Oracle® Internet Directory

管理者ガイド

10*g*（9.0.4）

部品番号 : B12375-02

2004 年 5 月

ORACLE®

Oracle Internet Directory 管理者ガイド , 10*g*（9.0.4）

部品番号 : B12375-02

原本名 : Oracle Internet Directory Administrator's Guide, 10*g* (9.0.4)

原本部品番号 : B12118-01

原本著者 : Richard Smith

原本協力者 : Jennifer Polk、Vasuki Ashok、Tridip Bhattacharya、Neelima Bawa、Ramakrishna Bollu、Margaret Chou、Saheli Dey、Rajinder Gupta、Ajay Keni、Ashish Kolli、Stephen Lee、David Lin、Michael Mesaros、Radhika Moolky、Hari Sastry、David Saslav、Ramaprakash Sathyanarayan、Bhupindra Singh、Gurudatt Shakshikumar、Amit Sharma、Jason Sharma、Daniel Shih、Saurabh Shrivastava、Uppili Srinivasan、Olaf Stullich、Dipankar Thakuria、Sivakumar Venugopa

目次

2 ディレクトリの概念およびアーキテクチャ

3 事前に実行するタスクと情報

4 ディレクトリ管理ツール

6 ディレクトリ・スキーマの管理

7 ディレクトリ・エントリの管理

8 ディレクトリの属性一意性

9 Oracle Internet Directory の動的および静的グループ

10 ディレクトリのロギング、監査および監視

11 ディレクトリのバックアップとリストア

第 III 部 ディレクトリのセキュリティ

12 ディレクトリ・セキュリティの概要

13 Secure Sockets Layer（SSL）とディレクトリ

14 ディレクトリ・アクセス制御

15 Oracle Internet Directory のパスワード・ポリシー

16 パスワード・ベリファイアのディレクトリ格納

17 Oracle テクノロジ配置のための権限の委任

第 IV 部　ディレクトリの配置

18　ディレクトリ配置の考慮事項

19 Oracle Identity Management レルムの配置

20 ディレクトリの容量計画

21 ディレクトリのチューニングに関する考慮事項

22 Oracle Internet Directory におけるガベージ・コレクション

23 他のディレクトリからのデータの移行

第 V 部 ディレクトリ・レプリケーションおよび高可用性

24 ディレクトリ・レプリケーションの概要

26 高可用性とフェイルオーバーに関する考慮事項

27 ラックマウント型ディレクトリ・サーバー構成

28 コールド・フェイルオーバー・クラスタ構成

29 Oracle9*i* Real Application Clusters 環境でのディレクトリ

Vol.2

第 VI 部　Oracle Internet Directory での委任およびセルフ・サービス管理

30 Oracle Delegated Administration Services

31 Oracle Internet Directory セルフ・サービス・コンソール

第 VII 部 Oracle Directory Integration and Provisioning Platform

32 Oracle Directory Integration and Provisioning Platform の概要とコンポーネント

33 Oracle Directory Synchronization Service

34 Oracle Directory Provisioning Integration Service

35 Oracle Directory Integration and Provisioning Server の管理

39 Oracle Human Resources との同期化

40 Oracle E-Business Suite へのデータ・プロビジョニングの統合

41 サード・パーティ・ディレクトリとの統合に関する考慮事項

42 SunONE（iPlanet）Directory Server との統合

43 Microsoft Windows 環境との統合

44 サード・パーティのメタディレクトリ・ソリューションとの同期

第 IX 部　付録

A　LDIF およびコマンドライン・ツールの構文

B Oracle Internet Directory のスキーマ要素

C Oracle Internet Directory Graphical User Interface（GUI）の要素

D LDAP フィルタ定義

E アクセス制御ディレクティブ書式

F データベース・コピー・プロシージャを使用したディレクトリ・ノードの追加

図目次

表目次

はじめに

『Oracle Internet Directory 管理者ガイド』では、Oracle Internet Directory の機能、アーキテクチャおよび管理について説明します。インストールに関する情報は、使用しているオペレーティング・システムのインストール・マニュアルを参照してください。

この章では、次の項目について説明します。

対象読者

『Oracle Internet Directory 管理者ガイド』は、Oracle Internet Directory の管理タスクを実行するすべての管理者を対象としています。管理者は、コマンドライン・モードのコマンドや例を理解するために、UNIX オペレーティング・システムまたは Microsoft Windows オペレーティング・システムのいずれかをよく理解している必要があります。コマンドライン・モードのコマンドを使用すると、すべてのタスクを実行できます。また、大部分のタスクは、オペレーティング・システムに依存しない Oracle Directory Manager から実行できます。

このマニュアルを使用するには、**Lightweight Directory Access Protocol（LDAP）**をある程度理解している必要があります。

このマニュアルの構成

このマニュアルは、次の各章と付録で構成されています。インストールおよびメンテナンスを実行する前に、第 I 部に記載されている概念的およびその他の基礎的な説明を読むことをお薦めします。

管理ロールに従って、実行するタスクに関連するその他の部の説明も参照してください。

- ルーチン管理の詳細は、次の部を参照してください。
  - 第 I 部 : スタート・ガイド
  - 第 II 部 : 基本的なディレクトリ管理
- 企業およびホスティングされた環境でのディレクトリ計画と配置の詳細は、次の部を参照してください。
  - 第 III 部 : ディレクトリのセキュリティ
  - 第 IV 部 : ディレクトリ配置
  - 第 V 部 : ディレクトリ・レプリケーションおよび高可用性
  - 第 VI 章 : Oracle Internet Directory の委任およびセルフ・サービス管理
- Oracle Internet Directory と他のディレクトリの相互作用の詳細は、次の部を参照してください。
  - 第 VII 部 : Oracle Directory Integration and Provisioning Platform
- プラグインの使用による Oracle Internet Directory の機能拡張の詳細は、次の部を参照してください。
  - 第 VIII 部 : Oracle Internet Directory プラグイン

第 I 部 : スタート・ガイド

第 I 部では、この製品とその機能の概要およびディレクトリの構成と管理に必要な概念的な基礎知識について説明します。

第 1 章「LDAP および Oracle Internet Directory の概要」

この章では、ディレクトリ、LDAP および Oracle Internet Directory の機能の概要について説明します。

第 2 章「ディレクトリの概念およびアーキテクチャ」

この章では、オンライン・ディレクトリと LDAP の概要について説明します。また、ディレクトリ・エントリ、属性、オブジェクト・クラス、ネーミング・コンテキスト、スキーマ、分散ディレクトリ、セキュリティおよびグローバリゼーション・サポートの概念についても説明します。さらに、Oracle Internet Directory のアーキテクチャについても説明します。

第 3 章「事前に実行するタスクと情報」

この章では、構成と使用のためのディレクトリの準備方法について説明します。OID モニターの開始および停止、Oracle ディレクトリ・サーバーと Oracle ディレクトリ・レプリケーション・サーバーのインスタンスの起動および停止の方法を説明します。また、デフォルトのセキュリティ構成の再設定の必要性、Oracle Internet Directory の以前のリリースからのアップグレード方法および他の LDAP 準拠のディレクトリからのデータの移行方法についても説明します。

第 4 章「ディレクトリ管理ツール」

この章では、様々な管理ツール（Oracle Directory Manager、コマンドライン・ツール、バルク・ツール、カタログ管理ツール、OID データベース・パスワード・ユーティリティ、レプリケーション・ツールおよびデータベース統計収集ツール）の使用方法を説明します。

第 II 部 : 基本的なディレクトリ管理

第 II 部では、Oracle Internet Directory の構成とメンテナンスに必要なタスクを紹介します。

第 5 章「Oracle ディレクトリ・サーバーの管理」

この章では、サーバーの構成設定エントリの管理、システム操作属性の設定、ネーミング・コンテキストとパスワード暗号化の管理、検索の構成、スーパー・ユーザー、ゲスト・ユーザーおよびプロキシ・ユーザーの管理、デバッグ・ロギング・レベルの設定、監査ログの使用、アクティブ・サーバー・インスタンスの情報の表示および Oracle データベース・サーバー接続時のパスワードの変更について説明します。

第 6 章「ディレクトリ・スキーマの管理」

この章では、ディレクトリ・スキーマ、オブジェクト・クラスおよび属性についてそれぞれ説明します。Oracle Directory Manager とコマンドライン・ツールを使用して Oracle Internet Directory のスキーマを管理する方法を説明します。

第 7 章「ディレクトリ・エントリの管理」

この章では、Oracle Directory Manager とコマンドライン・ツールを使用して、エントリを検索、表示、追加、変更および管理する方法について説明します。

第 8 章「ディレクトリの属性一意性」

この章では、識別名以外の属性を一意キーとして使用するために、アプリケーションと Oracle Internet Directory との同期化を可能にする属性一意性機能について説明します。

第 9 章「Oracle Internet Directory の動的および静的グループ」

この章では、静的および動的グループの概要、および Oracle Internet Directory でこれらのグループを管理する方法について説明します。

第 10 章「ディレクトリのロギング、監査および監視」

この章では、Oracle Internet Directory で提供される、ディレクトリのデバッグ、監査および監視に使用可能な包括的フレームワークについて説明します。

第 III 部 : ディレクトリのセキュリティ

第 III 部では、ディレクトリ自体に格納されているデータおよび企業内のディレクトリ配置に格納されたデータの保護方法について説明します。

第 11 章「ディレクトリのバックアップとリストア」

この章では、小さいディレクトリおよび大きいディレクトリのバックアップ方法とリストア方法について説明します。

第 12 章「ディレクトリ・セキュリティの概要」

この章では、Oracle Internet Directory で利用できるセキュリティ機能を示し、管理業務を委任するためのディレクトリ配置方法について説明します。

第 13 章「Secure Sockets Layer（SSL）とディレクトリ」

この章では、Secure Sockets Layer（SSL）の機能を構成する方法について説明します。

第 14 章「ディレクトリ・アクセス制御」

この章では、アクセス制御ポリシーの概要およびディレクトリ・アクセスの管理方法について説明します。

第 15 章「Oracle Internet Directory のパスワード・ポリシー」

この章では、パスワード・ポリシー（パスワードの使用方法を管理する規則のセット）について説明します。ユーザーがディレクトリへのバインドを試みると、ディレクトリ・サーバーはパスワード・ポリシーを使用して、ユーザーのパスワードがパスワード・ポリシーの要件に適合するかを確認します。

第 16 章「パスワード・ベリファイアのディレクトリ格納」

この章では、Oracle コンポーネントでアプリケーション・セキュリティ資格証明を Oracle Internet Directory に格納してエンド・ユーザーと管理者が容易に管理できるようにし、企業に対するセキュリティ上の主な脅威に対処する方法を説明します。

第 17 章「Oracle テクノロジ配置のための権限の委任」

この章では、ユーザー、グループおよびサービスに関するすべてのデータを 1 つのリポジトリに格納する方法、およびこれらのデータの管理を複数の管理者に委任する方法について説明します。また、Oracle Internet Directory でのデフォルトのセキュリティ構成についても説明します。

第 IV 部 : ディレクトリ配置

第 IV 部では、ディレクトリ配置で考慮する必要のある重要な内容について説明します。これには、容量計画、高可用性、チューニングなどがあります。

第 18 章「ディレクトリ配置の考慮事項」

この章では、Oracle Internet Directory を配置するときに考慮する必要がある一般的な問題について説明します。この章は企業内のディレクトリの要件を評価し、効果的な配置を選択するのに役立ちます。

第 19 章「Oracle Identity Management レルムの配置」

Oracle の多くのコンポーネントは、様々な目的で Oracle Internet Directory を使用します。その場合、Oracle コンポーネントは、整理統合された Oracle Internet Directory のスキーマとデフォルトのディレクトリ情報ツリー（DIT）に依存します。この章では、次の項目について説明します。

- 様々なコンポーネントで使用される整理統合された Oracle Internet Directory スキーマ
- Oracle の様々なコンポーネントを使用する際のデフォルトのディレクトリ情報ツリー構造

第 20 章「ディレクトリの容量計画」

この章では、アプリケーションのディレクトリ・アクセス要件を評価する方法および許容速度で要求を処理するための十分なコンピュータ・リソースが Oracle Internet Directory にあることを確認する方法について説明します。

第 21 章「ディレクトリのチューニングに関する考慮事項」

この章では、組み合せたハードウェアとソフトウェアで、必要なレベルのパフォーマンスが得られることを確認するためのガイドラインを示します。

第 22 章「Oracle Internet Directory におけるガベージ・コレクション」

「ガベージ」とは、ディレクトリで、不要になっているが領域を使用しているデータを指します。ディレクトリからこの不要なデータを削除する処理を、ガベージ・コレクションと呼びます。この章では、Oracle Internet Directory で使用可能な事前定義済ガベージ・コレクタの概要およびこれらのコレクタの変更方法について説明します。

第 23 章「他のディレクトリからのデータの移行」

この章では、LDAP バージョン 3 互換のディレクトリとアプリケーション固有のディレクトリから Oracle Internet Directory へデータを移行する手順について説明します。

第 V 部 : ディレクトリ・レプリケーションおよび高可用性

第 V 部では、レプリケーションとその管理方法について詳しく説明します。

第 24 章「ディレクトリ・レプリケーションの概要」

この章では、第 2 章「ディレクトリの概念およびアーキテクチャ」で説明したレプリケーションについて、さらに詳しく説明します。

第 25 章「Oracle ディレクトリ・レプリケーションの管理」

この章では、初めて Oracle ディレクトリ・レプリケーション・サーバー・ソフトウェアをインストールおよび初期化する方法、ソフトウェアがすでにインストールされている環境に新規ノードをインストールする方法について説明します。

第 26 章「高可用性とフェイルオーバーに関する考慮事項」

この章では、Oracle Internet Directory のテクノロジ・スタックにおける様々なコンポーネントの可用性とフェイルオーバー機能について説明し、一般的なディレクトリ配置に関してこれらの製品を最適な状態で活用する方法を示します。

第 27 章「ラックマウント型ディレクトリ・サーバー構成」

この章では、ディレクトリ・サーバーに高可用性を提供するラックマウント型ディレクトリ・サーバー構成について説明します。この構成では、複数のディレクトリ・サーバーのインスタンスを異なるハードウェア・ノードで実行します。ディレクトリ・サーバーは、同一ディレクトリ・ストアに接続されます。このディレクトリ・ストアは、Oracle9*i* データベース・サーバーです。

第 28 章「コールド・フェイルオーバー・クラスタ構成」

この章では、クラスタ環境で（物理ホストではなく）論理ホスト（物理ホストとは異なるものです）を使用することによって、高可用性を得る方法について説明します。

第 29 章「Oracle9i Real Application Clusters 環境でのディレクトリ」

この章では、Oracle9*i* Real Application Clusters システムで Oracle Internet Directory を実行する方法について説明します。

第 VI 章 : Oracle Internet Directory の委任およびセルフ・サービス管理

第 30 章「Oracle Delegated Administration Services」

この章では、Oracle Delegated Administration Services について説明します。Oracle Delegated Administration Services は、管理コンソールおよびセルフ・サービス・コンソールを構築するための事前定義済 Web ベース・ユニットで構成されるフレームワークです。委任管理者およびユーザーは、これらのコンソールを使用して、指定したディレクトリ操作を実行できます。

第 31 章「Oracle Internet Directory セルフ・サービス・コンソール」

この章では、Oracle Internet Directory セルフ・サービス・コンソールについて説明します。Oracle Internet Directory セルフ・サービス・コンソールは、Oracle Delegated Administration Services を使用して作成された既製のアプリケーションです。

第 VII 部 : Oracle Directory Integration and Provisioning Platform

第 VIII 部では、Oracle Directory Integration and Provisioning Platform の概念、アーキテクチャおよびコンポーネントについて説明し、これを構成および使用して複数のディレクトリを Oracle Internet Directory と同期させる方法を示します。

第 32 章「Oracle Directory Integration and Provisioning Platform の概要とコンポーネント」

この章では、Oracle Directory Integration and Provisioning Platform とそのコンポーネント、アーキテクチャおよび管理ツールについて説明します。

第 33 章「Oracle Directory Synchronization Service」

この章では、同期プロファイルと、Oracle Internet Directory と接続ディレクトリをリンクするコネクタについて説明します。

第 34 章「Oracle Directory Provisioning Integration Service」

この章では、Oracle Internet Directory からのプロビジョニング情報をアプリケーションで受信できる Oracle Directory Provisioning Integration Service について説明します。

第 35 章「Oracle Directory Integration and Provisioning Server の管理」

この章では、Oracle Directory Integration and Provisioning Server について説明し、その構成方法および管理方法を示します。

第 36 章「Oracle Directory Integration and Provisioning Platform におけるセキュリティ」

この章では、Oracle Directory Integration and Provisioning Platform のセキュリティにおける最も重要な事項について説明します。

第 37 章「Oracle Directory Integration and Provisioning Platform におけるディレクトリのブートストラップ」

この章では、Oracle Directory Integration and Provisioning Platform を使用する前に実行する必要がある初期設定タスクについて説明します。

第 38 章「リレーショナル・データベースの表との同期」

この章では、リレーショナル・データベース内の表のデータを Oracle Internet Directory と同期させる方法について説明します。同期は、増分（たとえば、データベース表の行単位）またはすべてのデータベース表を一括で実行できます。

第 39 章「Oracle Human Resources との同期化」

Oracle Internet Directory に格納した従業員データを Oracle Human Resources で作成、変更および削除する場合は、この 2 つの間でデータが同期化されていることを確認する必要があります。この章では、この操作を可能にする Oracle Human Resources エージェントについて説明します。

第 40 章「Oracle E-Business Suite へのデータ・プロビジョニングの統合」

Oracle Internet Directory 10*g*（9.0.4）では、Oracle Directory Provisioning Integration Service を使用して、ユーザー・アカウントと Oracle E-Business Suite からの他のユーザー情報を同期させることができます。

第 41 章「サード・パーティ・ディレクトリとの統合に関する考慮事項」

サード・パーティのディレクトリを Oracle Internet Directory に統合する前に、統合環境の構成方法を決定する必要があります。この章では、決定する必要がある基本的な事項について説明します。決定後、後続のブートストラップおよびディレクトリ間のデータの同期を設定する手順を実行できます。

第 42 章「SunONE（iPlanet）Directory Server との統合」

この章では、SunONE コネクタを使用して、Oracle Internet Directory と SunONE Directory Server を同期化する方法について説明します。

第 43 章「Microsoft Windows 環境との統合」

この章では、Oracle Application Server Infrastructure を Microsoft Windows オペレーティング・システムと統合する方法について説明します。この統合は、Oracle Directory Integration and Provisioning Platform で Active Directory Connector を使用して行います。

第 44 章「サード・パーティのメタディレクトリ・ソリューションとの同期」

Oracle Internet Directory は、サポートするサード・パーティのメタディレクトリ・ソリューションとの同期を可能にするために変更ログを使用します。この章では、変更ログ情報の生成方法と、サポートするソリューションでの変更ログ情報の使用方法について説明します。また、サード・パーティのメタディレクトリ・ソリューションを Oracle Internet Directory と同期化できるように、サード・パーティのメタディレクトリ・ソリューションのディレクトリ統合エージェントを使用可能にする方法を示します。

第 VIII 部 : Oracle Internet Directory プラグイン

第 45 章「Oracle Internet Directory プラグイン・フレームワーク」

この章では、オラクル社またはサード・パーティ・ベンダーが開発したプラグインを使用して、Oracle ディレクトリ・サーバーの機能を拡張する方法について説明します。

第 46 章「Oracle Internet Directory のパスワード・ポリシー・プラグイン」

Oracle Internet Directory は、プラグインを使用して、パスワード値のチェックを他のパスワード・ポリシー管理機能に追加します。このプラグインを使用すると、追加または変更されたパスワードが、指定された最小文字数以上であるかどうかなどを確認できます。個別の要件に合わせて、パスワード値チェックをカスタマイズできます。この章では、パスワード・ポリシーのプラグインとその使用例について説明します。

第 47 章「カスタマイズされた外部認証プラグインの設定」

ユーザー・セキュリティ資格証明を Oracle Internet Directory 以外のリポジトリ（データベースや他の LDAP ディレクトリなど）に格納し、Oracle コンポーネントに対するユーザー認証に使用できます。資格証明を Oracle Internet Directory に格納し、同期させておく必要はありません。外部リポジトリに格納された資格証明によるユーザー認証を、外部認証と呼びます。この章では、外部認証プラグインとその使用例について説明します。

第 IX 部 : 付録

付録 A「LDIF およびコマンドライン・ツールの構文」

この付録では、LDAP Data Interchange Format と LDAP コマンドライン・ツールに関する構文、使用方法および例を紹介します。

付録 B「Oracle Internet Directory のスキーマ要素」

この付録では、Oracle Internet Directory でサポートされているスキーマ要素について説明します。

付録 C「Oracle Internet Directory Graphical User Interface（GUI）の要素」

この付録では、Oracle Directory Manager および Oracle Internet Directory セルフ・サービス・コンソールの様々なフィールドおよび制御デバイスについて説明します。

付録 D「LDAP フィルタ定義」
この付録（Internet Engineering Task Force（IETF）の許可によりコピー）では、読取りおよび更新のアクセス権を提供するディレクトリ・アクセス・プロトコルについて説明します。

付録 E「アクセス制御ディレクティブ書式」
この付録では、アクセス制御情報アイテム（ACI）の書式（構文）について説明します。

付録 F「データベース・コピー・プロシージャを使用したディレクトリ・ノードの追加」
この付録では、ディレクトリが非常に大きい場合に、レプリケート・ディレクトリ・システムにノードを追加するための代替方法について説明します。

付録 G「ディレクトリにおけるグローバリゼーション・サポート」
この付録では、Oracle Internet Directory で使用されるグローバリゼーション・サポートについて説明します。

付録 H「ユーザーおよびグループの作成ベースおよび検索ベースに対するアクセス制御の設定」
この付録では、ユーザーおよびグループの作成ベースおよび検索ベースに対するアクセス制御について説明します。

付録 I「トラブルシューティング」
この付録では、発生する可能性がある障害とエラー・コードおよび考えられる原因について説明します。

関連ドキュメント

詳細は、次の Oracle ドキュメントを参照してください。

- Oracle Directory Manager、Oracle Delegated Administration Services および Oracle Enterprise Manager を介して使用可能なオンライン・ヘルプ。
- Oracle Application Server および Oracle9*i* データベース・サーバーのドキュメント・セット。特に次のマニュアルを参照してください。
  - 『Oracle Internet Directory アプリケーション開発者ガイド』
  - 『Oracle Identity Management 概要および配置プランニング・ガイド』
  - 『Oracle9*i* データベース管理者ガイド』
  - 『Oracle9*i* アプリケーション開発者ガイド - 基礎編』
  - 『Oracle Application Server 10*g* 管理者ガイド』
  - 『Oracle9*i* Net Services 管理者ガイド』

- 『Oracle9*i* Real Application Clusters 管理』
- 『Oracle9*i* アドバンスト・レプリケーション』
- 『Oracle Advanced Security 管理者ガイド』

リリース・ノート、インストール関連ドキュメント、ホワイト・ペーパーまたはその他の関連ドキュメントは、OTN-J（Oracle Technology Network Japan）から、無償でダウンロードできます。OTN-J を使用するには、オンラインでの登録が必要です。登録は、次の Web サイトから無償で行えます。

`http://otn.oracle.co.jp/membership/`

すでに OTN-J のユーザー名およびパスワードを取得している場合は、次の URL で OTN-J Web サイトのドキュメントのセクションに直接接続できます。

`http://otn.oracle.co.jp/document/`

詳しい情報は、次のドキュメントを参照してください。

- 『Chadwick, David,Understanding X.500 - The Directory.Thomson Computer Press, 1996』
- 『Howes, Tim and Mark Smith, LDAP: Programming Directory-enabled Applications with Lightweight Directory Access Protocol.Macmillan Technical Publishing, 1997』
- 『Howes, Tim, Mark Smith and Gordon Good, Understanding and Deploying LDAP Directory Services.Macmillan Technical Publishing, 1999』
- `http://www.iana.org`（Internet Assigned Numbers Authority のホームページ。オブジェクト識別子に関する情報）
- `http://www.ietf.org` で入手可能な次の Internet Engineering Task Force（IETF）のドキュメント
  - LDAPEXT の Charter および LDAP の Draft
  - LDUP の Charter および Draft
  - RFC 2254、「The String Representation of LDAP Search Filters」
  - RFC 1823、「The LDAP Application Program Interface」
- `http://www.openldap.org`（OpenLDAP Community）

表記規則

この項では、このマニュアルの本文およびコード例で使用される表記規則について説明します。この項の内容は次のとおりです。

- 本文の表記規則
- コード例の表記規則
- Microsoft Windows オペレーティング・システム環境での表記規則

本文の表記規則

本文では、特定の項目が一目でわかるように、次の表記規則を使用します。次の表に、その規則と使用例を示します。

規則	意味	例
太字	太字は、本文中で定義されている用語および用語集に記載されている用語を示します。	この句を指定すると、**索引構成表**が作成されます。
固定幅フォントの大文字	固定幅フォントの大文字は、システム指定の要素を示します。このような要素には、パラメータ、権限、データ型、Recovery Manager キーワード、SQL キーワード、SQL*Plus またはユーティリティ・コマンド、パッケージおよびメソッドがあります。システム指定の列名、データベース・オブジェクト、データベース構造、ユーザー名およびロールも含まれます。	`NUMBER` 列に対してのみ、この句を指定できます。 `BACKUP` コマンドを使用して、データベースのバックアップを作成できます。 `USER_TABLES` データ・ディクショナリ・ビューの `TABLE_NAME` 列を問い合せます。 `DBMS_STATS.GENERATE_STATS` プロシージャを使用します。
固定幅フォントの小文字	固定幅フォントの小文字は、実行可能ファイル、ファイル名、ディレクトリ名およびサンプルのユーザーが指定する要素を示します。このような要素には、コンピュータ名とデータベース名、ネット・サービス名および接続識別子があります。ユーザーが指定するデータベース・オブジェクトとデータベース構造、列名、パッケージとクラス、ユーザー名とロール、プログラム・ユニットおよびパラメータ値も含まれます。 **注意 :** プログラム要素には、大文字と小文字を組み合せて使用するものもあります。これらの要素は、記載されているとおりに入力してください。	`sqlplus` と入力して、SQL*Plus をオープンします。 パスワードは、`orapwd` ファイルで指定します。 `/disk1/oracle/dbs` ディレクトリ内のデータ・ファイルおよび制御ファイルのバックアップを作成します。 `hr.departments` 表には、`department_id`、`department_name` および `location_id` 列があります。 `QUERY_REWRITE_ENABLED` 初期化パラメータを `true` に設定します。 `oe` ユーザーとして接続します。 `JRepUtil` クラスが次のメソッドを実装します。

規則	意味	例
固定幅フォントの小文字のイタリック	固定幅フォントの小文字のイタリックは、プレースホルダまたは変数を示します。	*parallel_clause* を指定できます。 U*old_release*.SQL を実行します。ここで *old_release* とは、アップグレード前にインストールしたリリースを示します。

コード例の表記規則

コード例は、SQL、PL/SQL、SQL*Plus またはその他のコマンドライン文の例です。次のように固定幅フォントで表示され、通常のテキストと区別されます。

```
SELECT username FROM dba_users WHERE username = 'MIGRATE';
```

次の表に、コード例で使用される表記規則とその使用例を示します。

規則	意味	例
[ ]	大カッコは、大カッコ内の項目を任意に選択することを表します。大カッコは、入力しないでください。	DECIMAL (*digits* [, *precision*])
{ }	中カッコは、カッコ内の項目のうち、1 つが必須であることを表します。中カッコは、入力しないでください。	{ENABLE | DISABLE}
|	縦線は、大カッコまたは中カッコ内の複数の選択項目の区切りに使用します。項目のうちの 1 つを入力します。縦線は、入力しないでください。	{ENABLE | DISABLE} [COMPRESS | NOCOMPRESS]
...	水平の省略記号は、次のいずれかを示します。	
	■ 例に直接関連しないコードの一部が省略されている。	CREATE TABLE ... AS *subquery*;
	■ コードの一部を繰り返すことができる。	SELECT *col1*, *col2*, ... , *coln* FROM employees;
. . .	垂直の省略記号は、例に直接関連しない複数の行が省略されていることを示します。	SQL> SELECT NAME FROM V$DATAFILE; NAME ---------- /fsl/dbs/tbs_01.dbf /fs1/dbs/tbs_02.dbf . . . /fsl/dbs/tbs_09.dbf 9 rows selected.

規則	意味	例
その他の表記	大カッコ、中カッコ、縦線および省略記号以外の記号は、記載されているとおりに入力する必要があります。	`acctbal NUMBER(11,2);` `acct CONSTANT NUMBER(4) := 3;`
イタリック体	イタリック体は、特定の値を指定する必要があるプレースホルダや変数を示します。	`CONNECT SYSTEM/`*`system_password`* `DB_NAME =` *`database_name`*

大文字	大文字は、システム指定の要素を示します。これらの用語は、ユーザー定義の要素と区別するために大文字で示されます。大カッコ内にないかぎり、表示されているとおりの順序および綴りで入力します。ただし、大 / 小文字が区別されないため、小文字でも入力できます。	`SELECT last_name, employee_id FROM employees;`
		`SELECT * FROM USER_TABLES;`
		`DROP TABLE hr.employees;`

小文字	小文字は、ユーザー指定のプログラム要素を示します。たとえば、表名、列名またはファイル名などです。
	注意 : プログラム要素には、大文字と小文字を組み合せて使用するものもあります。これらの要素は、記載されているとおりに入力してください。
		`SELECT last_name, employee_id FROM employees;`
		`sqlplus hr/hr`
		`CREATE USER mjones IDENTIFIED BY ty3MU9;`

Microsoft Windows オペレーティング・システム環境での表記規則

次の表に、Microsoft Windows オペレーティング・システム環境での表記規則とその使用例を示します。

規則	意味	例
「スタート」> を選択	プログラムの起動方法。	Database Configuration Assistant を起動するには、「スタート」>「プログラム」>「Oracle - *HOME_NAME*」>「Configuration and Migration Tools」>「Database Configuration Assistant」を選択します。
ファイル名およびディレクトリ名	ファイル名およびディレクトリ名は大 / 小文字が区別されません。特殊文字の左山カッコ（<）、右山カッコ（>）、コロン（:）、二重引用符（"）、スラッシュ（/）、縦線（|）およびハイフン（-）は使用できません。円記号（¥）は、引用符で囲まれている場合でも、要素のセパレータとして処理されます。Windows では、ファイル名が ¥¥ で始まる場合、汎用ネーミング規則が使用されていると解釈されます。	`c:¥winnt"¥"system32` は `C:¥WINNT¥SYSTEM32` と同じです。

規則	意味	例
Windows コマンド・プロンプト	Windows コマンド・プロンプトには、カレント・ディレクトリが表示されます。コマンド・プロンプトのエスケープ文字はカレット（^）です。このマニュアルでは、コマンド・プロンプトと呼びます。	C:¥oracle¥oradata>
特殊文字	Windows コマンド・プロンプトで二重引用符（"）のエスケープ文字として円記号（¥）が必要な場合があります。丸カッコおよび一重引用符（'）にはエスケープ文字は必要ありません。エスケープ文字および特殊文字の詳細は、Windows オペレーティング・システムのドキュメントを参照してください。	C:¥>exp scott/tiger TABLES=emp QUERY=¥"WHERE job='SALESMAN' and sal<1600¥" C:¥>imp SYSTEM/*password* FROMUSER=scott TABLES=(emp, dept)
HOME_NAME	Oracle ホームの名前を表します。ホーム名には、英数字で 16 文字まで使用できます。ホーム名に使用可能な特殊文字は、アンダースコアのみです。	C:¥> net start Oracle*HOME_NAME*TNSListener
ORACLE_HOME および *ORACLE_BASE*	Oracle8*i* より前のリリースでは、Oracle コンポーネントをインストールすると、すべてのサブディレクトリが最上位の *ORACLE_HOME* ディレクトリの直下に置かれました。*ORACLE_HOME* ディレクトリの名前は、デフォルトでは次のとおりです。 ■ C:¥orant（Windows NT の場合） このリリースは、Optimal Flexible Architecture（OFA）のガイドラインに準拠しています。*ORACLE_HOME* ディレクトリの下に配置されないサブディレクトリもあります。最上位のディレクトリは、*ORACLE_BASE* と呼ばれ、デフォルトでは C:¥oracle です。他の Oracle ソフトウェアがインストールされていないコンピュータに Oracle9*i* リリース 2（9.2）をインストールした場合、Oracle ホーム・ディレクトリは、デフォルトで C:¥oracle¥ora*nn*（*nn* は最新リリース番号）です。Oracle ホーム・ディレクトリは、*ORACLE_BASE* の直下に配置されます。 このマニュアルに示すディレクトリ・パスの例は、OFA の表記規則に準拠しています。	%*ORACLE_HOME*%¥rdbms¥admin ディレクトリにアクセスします。

Oracle Internet Directory の新機能

この章では、Oracle Internet Directory の最新リリースで導入された新機能について簡単に説明します。各項目には、関連項目が記載されています。次の項目について説明します。

Oracle Internet Directory 10*g*（9.0.4）で導入された新機能

- **Microsoft Windows 環境との統合**: Oracle Application Server Infrastructure を Microsoft Windows オペレーティング・システム（Microsoft Active Directory や Microsoft Windows NT 4.0 を含む）と統合できます。この統合は、Oracle Directory Integration and Provisioning Platform の Active Directory コネクタおよびプラグインを使用して実現されます。

  関連項目： 第 43 章「Microsoft Windows 環境との統合」

- **外部認証サポート**: Oracle Internet Directory 以外のリポジトリにユーザー・セキュリティ資格証明を格納できます。たとえば、データベースや、Microsoft Active Directory、SunONE Directory Server などの LDAP ディレクトリです。これらの資格証明をユーザー認証に使用できます。

  関連項目：

  - 第 47 章「カスタマイズされた外部認証プラグインの設定」
  - 41-6 ページの「パスワードの格納場所の選択」

- **動的グループ**: メンバーシップがリストで管理されるのではなく、指定されたアサーションに基づいてその場で計算される動的グループを作成し、使用できます。

  関連項目： 第 9 章「Oracle Internet Directory の動的および静的グループ」

- **問合せ最適化**: 検索の際、一部の属性ではその値によって応答時間が大幅に異なります。パフォーマンスを向上させるため、そのような属性について検索操作の応答時間を統一できます。

  関連項目： 21-11 ページの「検索の最適化」

- **ガベージ・コレクション・フレームワーク**: ガベージ・コレクタは、使用されなくなったデータをディレクトリから削除するバックグラウンドのデータベース・プロセスです。Oracle Internet Directory ガベージ・コレクション・フレームワークには、ガベージ・コレクタの標準セットがあります。このフレームワークにより、これらのコレクタを変更できます。

関連項目： 第 22 章「Oracle Internet Directory におけるガベージ・コレクション」

- **簡易認証セキュリティ・レイヤー（SASL）のサポート**: Oracle Internet Directory は、接続ベースのプロトコルに対して認証サポートを追加する方法として、SASL の使用をサポートします。SASL を使用するために、プロトコルには、ユーザーを識別してサーバーに対して認証を行うコマンドが含まれます。また、オプションで、以降のプロトコル対話の保護を規定するコマンドも含まれます。SASL の使用が規定されると、プロトコルと接続の間にセキュリティ・レイヤーが挿入されます。

  関連項目： 12-4 ページの「Oracle Internet Directory での認証」

- **ロギングの拡張**: このリリースの Oracle Internet Directory では、ロギングとトレースについて次の機能が追加されています。
  - スレッドおよび接続識別子に関連付けられた操作に対するオブジェクト・ベースのトレースの実行。これにより、マルチスレッド環境での各 LDAP 操作に関する連続した一貫性のあるロギングを容易に行えます。
  - 操作ディメンションの使用による選択した操作に対する選択的トレース
  - スレッド識別子や重大性などの補足情報を含む構造化されたわかりやすいトレース・メッセージ

  関連項目： 第 10 章「ディレクトリのロギング、監査および監視」

- **OID 移行ツール（ldifmigrator）の拡張**: このツールを使用して、既存のディレクトリにあるデータを調整し、Oracle Internet Directory に直接ロードできます。

  関連項目：
  - 23-5 ページの「ユーザー・データのアプリケーション固有リポジトリからの移行」
  - A-132 ページの「OID 移行ツール（ldifmigrator）の構文」

- **クライアント側の参照キャッシング**: この新機能により、クライアントは参照情報をキャッシュし、それを使用して参照処理を高速化できます。

  関連項目:

  - 7-18 ページの「クライアント側の参照キャッシング」
  - 『Oracle Internet Directory アプリケーション開発者ガイド』の `ldap_set_option` および `ldap_get_option`

- **ファンアウト・レプリケーションおよび部分レプリケーションのサポート**: Oracle Internet Directory は、現在、次の機能をサポートします。
  - 部分レプリケーション: ディレクトリ情報ツリー全体ではなく、1 つ以上のネーミング・コンテキストを別のノードに伝播します。
  - ファンアウト・レプリケーション: サプライヤから変更を受信したコンシューマは、その変更を 1 つ以上の別のコンシューマにレプリケートできます。ファンアウト・レプリケーションには完全レプリケーションと部分レプリケーションがあります。

  関連項目:

  - 第 24 章「ディレクトリ・レプリケーションの概要」
  - 第 25 章「Oracle ディレクトリ・レプリケーションの管理」

- **パスワード・ポリシーの拡張**: Oracle Internet Directory のパスワード・ポリシーには、次の新機能があります。
  - パスワード履歴
  - アカウントのロック解除
  - 初回ログイン時におけるパスワード変更の強制
  - アカウント・ロックアウトやパスワードを忘れた場合のパスワードの自己再設定
  - IP ベースのアカウント・ロックアウト
  - パスワード・ポリシー・エントリで単一値属性を使用することによるパスワード・ポリシーの有効化または無効化

  関連項目: 第 15 章「Oracle Internet Directory のパスワード・ポリシー」

- **セキュリティ資格証明ストレージの拡張**: Oracle Internet Directory のセキュリティ資格証明ストレージには、次の新機能があります。
  - エンタープライズ・ユーザーのための O3logon ベリファイアの生成
  - アプリケーション・ブートストラップのためのデフォルトのベリファイア・セットの生成
  - ディレクトリ認証のための SASL/MD5 ベリファイアの生成

  関連項目： 第 16 章「パスワード・ベリファイアのディレクトリ格納」

- **レプリケーション環境管理ツール**: このツールによって、Oracle9*i* Advanced Replication をディレクトリ・レプリケーションのために適切に構成することができます。ディレクトリ・レプリケーション障害が発生した場合、このツールはよく発生する問題を調査し、修正方法を検証します。問題を解決できない場合は、問題の性質に関するレポートを作成し、考えられる解決方法を示します。

  関連項目： A-62 ページの「レプリケーション環境管理ツール」

- **DNS の使用によるサーバー検出**: この機能により、分散環境にあるディレクトリ・サーバーの位置を、ドメイン・ネーム・システム（DNS）を使用して動的に検出できます。サーバーの位置情報を、クライアントの `ldap.ora` ファイルに静的に格納するのではなく、その情報を中央のドメイン・ネーム・サーバーに格納し、管理します。クライアントは、要求を処理するときに、ドメイン・ネーム・サーバーからこの情報を取得します。

  関連項目： A-62 ページの「レプリケーション環境管理ツール」

- **バルク・ロード・ツールの拡張**: 大量のエントリを空でないディレクトリに追加するために、bulkload を使用できます。たとえば、すでに 100 万件のエントリを持つディレクトリに 100 万件のエントリを追加できます。また、中規模数のエントリを大きなディレクトリに増分的に追加できます。たとえば、すでに 500 万件のエントリを持つディレクトリに、一度に 50,000 件ずつエントリを追加できます。

  関連項目： A-45 ページの「bulkload の構文」

- **ラックマウント型のディレクトリ・サーバー構成のサポート**: この構成は、異なるハードウェア・ノードで複数のディレクトリ・サーバー・インスタンスを実行することにより、ディレクトリ・サーバーの可用性を高めます。ディレクトリ・サーバーは、基礎となる同一のデータ・ストア、すなわち Oracle9*i* データベース・サーバーに接続されます。

  関連項目： 第 27 章「ラックマウント型ディレクトリ・サーバー構成」

- **Oracle Internet Directory と他のアプリケーション・ディレクトリ間の双方向プロビジョニング**: Oracle Directory Provisioning Integration Service は、Oracle Internet Directory と他のアプリケーションとの間で、双方向にプロビジョニング・イベントの通知を送信できます。

  関連項目： 34-7 ページの「アプリケーションが Oracle Internet Directory からプロビジョニング情報を受信する方法」

  34-8 ページの「Oracle Internet Directory がアプリケーションからプロビジョニング情報を受信する方法」

- **プロビジョニング・データと Oracle E-Business Suite の統合**: Oracle Directory Provisioning Integration Service を使用することにより、ユーザー・アカウントや Oracle E-Business Suite からの他のユーザー情報を Oracle Internet Directory に対して同期化できます。

  関連項目： 第 40 章「Oracle E-Business Suite へのデータ・プロビジョニングの統合」

- **Oracle9*i* Real Application Clusters における Oracle Internet Directory のインストール**: Oracle9*i* Real Application Clusters に Oracle Internet Directory をインストールできます。これを行う場合、Oracle Internet Directory のソフトウェアとスキーマは、いずれもプライマリ・ノードにインストールされますが、ソフトウェアだけはセカンダリ・ノードにインストールされます。

  関連項目： Oracle Internet Directory のこのリリース用のインストール・ドキュメント

- **Oracle Directory Manager の拡張** : Oracle Directory Manager では、次の項目を管理できます。
  - 属性一意性
  - プラグイン
  - ガベージ・コレクション
  - 変更ログ
  - レプリケーション
  - 問合せ最適化
  - 従来より細分化されたデバッグ・ロギング
  - ACL の拡張
- **Oracle Internet Directory セルフ・サービス・コンソールの拡張** : Oracle Internet Directory セルフ・サービス・コンソールは、Oracle Delegated Administration Services ユニットで構築されたグラフィカル管理ツールです。次の項目を管理できます。
  - レルム
  - サービス
  - アカウント
  - パスワードの再設定

  また、Oracle Internet Directory セルフ・サービス・コンソールにより、管理者は組織チャートの表示を、ユーザーは自分のプロファイルの編集を行うことができます。

  関連項目： 第 31 章「Oracle Internet Directory セルフ・サービス・コンソール」

- **アップグレード手順**

  関連項目： Oracle Internet Directory の以前のバージョンからアップグレードする方法の詳細は、Oracle Application Server 10*g* のアップグレード・ガイドを参照してください。

Oracle Internet Directory リリース 9.2 の概要

この項では、Oracle Internet Directory の機能を利用する重要な新機能について説明します。また、リリース 9.0.2 以降での変更点についても説明します。

- **Oracle Internet Directory へのデータベース・ユーザーのバルク移行に使用するユーザー移行ユーティリティ**: このユーティリティは Oracle Advanced Security リリース 2（9.2）でリリースされ、ユーザーをローカル・データベースまたは外部データベースから Oracle Internet Directory に移行できます。このユーティリティを使用すると、数千人のユーザーを Oracle Internet Directory に格納して集中管理できます。

  関連項目：『Oracle Advanced Security 管理者ガイド』の、ローカル・ユーザーまたは外部ユーザーをエンタープライズ・ユーザーに移行させる方法に関する章を参照してください。

注意：

- Oracle Internet Directory リリース 9.2 からは、Oracle Delegated Administration Services とそのツールは、Oracle9*i* データベース・サーバーではなく、Oracle Application Server のコンポーネントとなっています。Web と Oracle Application Server アプリケーションのためのセルフ管理ツールを確実に入手し、これらのツールが中間層環境と適切に統合されることを保証するため、オラクル社では、Oracle Application Server に含まれるバージョンの Oracle Internet Directory を使用することをお薦めします。Oracle Delegated Administration Services ベースのツールの開発と配置には、Oracle Application Server の Java およびセキュリティ・インフラストラクチャを使用することをお薦めします。
- Oracle Internet Directory リリース 9.2 には、Oracle Internet Directory インスタンス上でシステム診断を実行するための Enterprise Manager 統合機能は組み込まれていません。

Oracle Internet Directory リリース 9.0.2 で導入された新機能

この項では、Oracle Internet Directory リリース 9.0.2 で導入された新機能について説明します。

- **サーバー側のエントリ・キャッシング**: この機能によって、LDAP クライアントのディレクトリ問合せ待機時間が短縮されます。Oracle Internet Directory では、ネーミング・コンテキスト、クライアントの識別情報またはその他の使用可能なパラメータに基づいてサーバー側のエントリ・キャッシュを構成することによって、以前に取得したエントリとその属性を共有メモリーに保存し、後続のデータ要求で使用できるようにします。以前に構成したパラメータに適合する問合せは、フィルタに一致するエントリの小さいサブセット・データ、つまり内部 Global Unique Identifier（GUID）をディレクトリから取得するだけで済みます。戻されたこれらの GUID は、キャッシュ内のエントリと属性データの高速検索メカニズムとして使用され、クライアントに戻されます。

  関連項目： 21-10 ページの「エントリ・キャッシング」

- **新しいディレクトリ統合機能**: Oracle Internet Directory リリース 9.0.2 では、（Oracle および Oracle 以外で作成された）他のアプリケーションやリポジトリとの新しい種類の接続性が導入されました。新しい Oracle Directory Provisioning Integration Service および Oracle Directory Synchronization Service は、Oracle Directory Integration and Provisioning Platform（Oracle8*i* の Oracle Internet Directory リリース 2.1.1.1 で導入）上に構築されます。

  - **Oracle Directory Provisioning Integration Service**: プロビジョニングとは、ビジネス・ルールに基づいて、アプリケーション・リソースに対するユーザーのアクセス権を付与または取り消すプロセスです。ユーザーとは、人間であるエンド・ユーザーまたはアプリケーションの場合があります。

    Oracle Directory Provisioning Integration Service によって、サブスクライバ・アプリケーションやビジネス・エンティティは、ローカル・リポジトリの同期を維持するために、Oracle Internet Directory の更新に常に注意を払うことができます。Oracle Internet Directory を真のソースとして使用することによって、アプリケーション固有のローカルな情報を同期化できます。

  - **Oracle Directory Synchronization Service と LDAP コネクタ**: Oracle Directory Synchronization Service を使用すると、ERP システムや CRM システム、サード・パーティの LDAP ディレクトリ、NOS ユーザー・リポジトリなど、以前に配置したインフラストラクチャをほぼ完全に活用できます。このサービスによって、企業ディレクトリと Oracle Internet Directory との間の情報を同期化できます。集中的なデータ管理が可能になるため、管理コストを削減できます。企業内のデータは、最新かつ一貫性のある状態に維持されます。

関連項目： 第 32 章「Oracle Directory Integration and Provisioning Platform の概要とコンポーネント」

- **エンタープライズ・パスワード・ポリシー管理の拡張** : 次の機能を使用して、パスワード・ポリシーを構成できるようになりました。
  - 有効期限
  - 猶予期間
  - パスワードの必要最小限の長さ
  - 許可されるパスワード構文および再試行制限
  - ディレクトリ・サービスへの不正なアクセス試行のロックアウト（指定した回数を超えてアクセスに失敗した場合）

  ハッシング・アルゴリズムとして salted SHA を使用できるようになりました。この結果、次の各種ハッシング・アルゴリズムを使用できます。

  - **MD4**: 128 ビットのハッシュを生成する一方向ハッシュ関数です。
  - **MD5**: MD4 が改善された、より複合的なバージョンです。
  - **SHA**: Secure Hash Algorithm。MD5 よりも長い 160 ビットのハッシュを生成します。このアルゴリズムは MD5 よりも若干速度が遅くなりますが、大きなメッセージ・ダイジェストによって、総当り攻撃や反転攻撃に対処できます。
  - salted SHA も使用できます。salt は、ハッシュ値に追加され、ハッシュ値とともに格納される乱数です。このソルトは、当初のハッシュ値のリカバリに極端にコストがかかるようにすることで、事前に算出されたディクショナリ・アタックを回避します。
  - **UNIX Crypt**: UNIX 暗号化アルゴリズムです。
  - ハッシングなし

  関連項目：

  - 概念の説明は、12-8 ページの「ディレクトリ認証用ユーザー・パスワードの保護」を参照してください。
  - パスワード・ハッシングの設定方法は、第 15 章「Oracle Internet Directory のパスワード・ポリシー」を参照してください。

- **属性一意性** : 以前の Oracle Internet Directory アーキテクチャでは、属性一意性を規定する唯一の方法は、属性をユーザーの識別名の一部にすることでした。この方法は、ユーザー識別子（相対識別名として使用されている場合）には有効でしたが、必ずしも適切かつ簡単に構成できるわけではありませんでした。属性は、ツリー分岐の 1 レベル内で一意性を保証されていました。たとえば、識別名が `uid=dlin, ou=people, o=oracle` の場合、相対識別名 dlin は `ou=people,o=oracle` の直下で一意のディレクトリになります。ただし、別の分岐（たとえば、`uid=dlin, ou=others, o=oracle`）では、同じユーザー識別子を使用できました。つまり、属性一意性は、指定された分岐の 1 レベル内でのみ保証されていました。

  dn 以外の属性は、Oracle Internet Directory と同期するアプリケーションの一意キーとして使用できます。属性一意性を規定する Oracle Internet Directory のこの機能によって、すべてのアプリケーションは、それぞれ独自のユーザーに関する認識を持ち、そのユーザー・ベースを企業の Oracle Internet Directory サーバーに格納されているユーザー・リポジトリと同期化することができます。

  関連項目： 第 8 章「ディレクトリの属性一意性」

- **複数パスワード・ベリファイアのサポート** : Oracle Internet Directory では、複数のアプリケーションやプロトコルに対するパスワードを格納できるようになりました。たとえば、ボイスメールの 4 桁の個人識別番号（PIN）を、同一のユーザーに対し、より長い英数字のシングル・サインオン・パスワードと X.509 v3 のデジタル証明書とともに保持できます。この新機能によって、アプリケーション開発者には、ディレクトリ対応の製品スタックについて高い柔軟性が与えられます。

  関連項目： 第 16 章「パスワード・ベリファイアのディレクトリ格納」

- **拡張されたプロキシ・ユーザー機能** : この新機能によって、開発者は中間層の能力をより有効に活用できます。ユーザーは、独立した、ディレクトリとは無関係なセッションを確立する必要はありません。中間層が Oracle Application Server などからプロキシ・ユーザーのバインド方法を、多数のクライアントにかわって連続して起動する場合、実際のバインドを行うエージェントが全体にわたって変わらないときにも、Oracle Internet Directory は、各クライアントの資格証明と権限をそれぞれ考慮します。

  関連項目：

  - 第 12 章「ディレクトリ・セキュリティの概要」
  - 5-11 ページの「スーパー・ユーザー、ゲスト・ユーザーおよびプロキシ・ユーザーの管理」

- **Oracle Application Server のコンポーネントとの統合** : Oracle Directory Provisioning Integration Service を介して、Oracle Internet Directory リリース 9.0.2 は Oracle Application Server の中央コンポーネントとして機能します。Oracle Application Server の各コンポーネントは、有効なユーザー識別子とそのパスワードなど、共通のコンポーネント間メタデータの格納に Oracle Internet Directory を使用するようになりました。

  関連項目： 第 19 章「Oracle Identity Management レルムの配置」

- **Oracle Enterprise Manager（OEM）の統合** : 新しく拡張された標準の Enterprise Manager コンソールを使用して、Oracle Internet Directory インスタンスを起動、停止および監視できます。実行中の Oracle Internet Directory インスタンスに対してシステム診断を実施し、現在のパフォーマンスおよび負荷がピークとなる時間帯を判断するためのパフォーマンス・グラフを作成できます。

  関連項目： 10-17 ページの「Oracle Internet Directory サーバーの監視」

- **Oracle Directory Manager の拡張** : Oracle Internet Directory のスタンドアロンで 100% Java の管理コンソールである Oracle Directory Manager は、様々な面で進化しました。Oracle Directory Manager を使用すると、次の操作を行うことができます。
  - レルムの構成
  - パスワード・ポリシーの構成
  - Oracle Directory Synchronization Service および Oracle Internet Directory のコネクタとエージェントの構成

  通常、高水準の Oracle Enterprise Manager の Graphical User Interface（GUI）では対応できなかったディレクトリ固有の構成タスクまたはメンテナンス・タスクを、Oracle Internet Directory が提供するコマンドライン・インタフェースと同様に Oracle Directory Manager を介して実行できるようになりました。

  関連項目： 第 4 章「ディレクトリ管理ツール」

- **サーバー側のプラグイン・フレームワーク** : この新機能によって、ディレクトリ・アプリケーションは、LDAP オブジェクトの参照整合性 / 連鎖的削除、ディレクトリ・クライアントの外部認証、ブローカ・アクセスおよび外部リレーショナル表との同期など、高度な機能を展開できます。このプラグインは、従来これらのテクノロジに存在したリスクなしで、LDAP コマンドの発行前後に実行できます。

関連項目： 第 45 章「Oracle Internet Directory プラグイン・フレームワーク」

- **エントリ別名の間接参照** : LDAP バージョン 3 の標準では、ディレクトリ内のすべてのエントリには、識別名と呼ばれている Global Unique Identifier（GUID）が必要です。一般的に、GUID は相当長く、使用するには厄介です。Oracle Internet Directory が提供するこの新機能では、完全修飾された LDAP 識別名を指し示すための、IETF 規格の別名オブジェクトを自動的に間接参照します。たとえば、「DavesServer1」は、エントリ別名、つまり実際のディレクトリ・エントリ名 `dc=server1, dc=us, dc=oracle, dc=com` へのポインタとして使用できます。Oracle Internet Directory は、クライアント側の完全な透過性を提供するために、別名参照すべてを格納、解析および追跡します。

  関連項目： 5-14 ページの「別名エントリの間接参照」

- **Delegated Administration Services**

  Oracle Delegated Administration Services は、Oracle Delegated Administration Services ユニットと呼ばれる個々の事前定義済サービスのセットで、ユーザーのかわりにディレクトリ操作を実行します。このサービスによって、Oracle Internet Directory を使用する Oracle のディレクトリ対応アプリケーションおよびその他のディレクトリ対応アプリケーションの管理ソリューションを容易に開発および配置できます。

  管理者は、Oracle Delegated Administration Services とその付属コンソールを使用して、次の操作を行うことができます。

  – 他の領域または部門の管理者の作成

  – 特定の領域または部門のユーザーを管理する特定の委任権限の付与

  Oracle Internet Directory セルフ・サービス・コンソール : これは、Oracle Delegated Administration Services の新規コンポーネントです。この新機能によって、中央のチームから、または分散化と委任によって、アプリケーション、レルムおよびエンド・ユーザーを柔軟に管理できます。このコンポーネントでは、次の機能が提供されます。

  – ディレクトリ管理者、ディレクトリ・サービス・サブスクライバおよびエンド・ユーザー用に統一されたリソース

  – 許可されたエンド・ユーザーが、パーソナライズされた作業環境の表示および Oracle Application Server Single Sign-On パスワードの更新を行うための機能

  – 個人および他のディレクトリ・ベースのリソース情報を Oracle Internet Directory で検索するための直観的なユーザー・インタフェース

Oracle Internet Directory セルフ・サービス・コンソールを使用すると、Oracle Internet Directory に格納されているオブジェクト・クラス、ユーザー・グループ、権限およびディレクトリ情報メタデータのその他の要素を構成できます。

関連項目： 第 31 章「Oracle Internet Directory セルフ・サービス・コンソール」

- **アップグレード手順**

  このアップグレード手順によって、Oracle Internet Directory リリース 2.1.1 およびリリース 3.0.1 からアップグレードできます。

Oracle Internet Directory リリース 3.0.1 で導入された新機能

この項では、Oracle Internet Directory リリース 3.0.1 で導入された新機能について説明します。

- **クラスタ構成でのフェイルオーバー**

  この新機能によって、クラスタ化された環境で物理ホストではなく論理ホストを使用することにより、可用性を高めることができます。

  関連項目： 第 28 章「コールド・フェイルオーバー・クラスタ構成」

- **Oracle9*i* Real Application Clusters 環境でのフェイルオーバー**

  Oracle9*i* Real Application Clusters は、複数の、相互接続されたコンピュータの処理能力を活用するコンピューティング環境です。Oracle9*i* Real Application Clusters は、クラスタと呼ばれるハードウェアの集合とともに、各コンポーネントの処理能力を、単一の強力なコンピューティング環境にまとめます。クラスタは、ノードとも呼ばれる 2 つ以上のコンピュータで構成されます。

  Oracle9*i* Real Application Clusters システムで Oracle Internet Directory を実行できます。

  関連項目： 第 29 章「Oracle9i Real Application Clusters 環境でのディレクトリ」

- **論理ホストのサポート** : Oracle Internet Directory リリース 3.0.1 では、物理ホストではなく論理ホストをクラスタ化された環境で使用することによって、可用性を高めることができます。論理ホストは、1 つ以上のディスク・グループ、およびホスト名と IP アドレスのペアから構成されます。論理ホストは、クラスタ内の物理ホストにマップされます。この物理ホストは、論理ホストのホスト名と IP アドレスに対応します。

  このパラダイムでは、ディレクトリ・サーバーは物理ホストではなく論理ホストにバインドされます。ディレクトリ・サーバーは、論理ホストが新規物理ホストにフェイルオーバーしてもこの接続を維持します。

  クライアントは、ディレクトリ・サーバーの論理ホスト名およびアドレスを使用してディレクトリ・サーバーに接続します。論理ホストが新規物理ホストにフェイルオーバーした場合は、このフェイルオーバーはクライアントに対して透過的です。

  関連項目： 第 28 章「コールド・フェイルオーバー・クラスタ構成」

- **同一のホストで複数の Oracle Internet Directory のインスタンスを実行する機能**

  この新機能によって、1 つのホストで複数の Oracle Internet Directory をインストールして実行できます。複数の Oracle Internet Directory 間でレプリケーションを実行したり、フェイルオーバー手法の一部として使用できます。

  関連項目： 18-6 ページの「1 つのホストにおける複数の Oracle Internet Directory インストール」

- **Oracle Directory Integration and Provisioning Platform**

  この新機能によって、多数のディレクトリを Oracle Internet Directory と同期させることができます。また、サード・パーティのメタディレクトリ・ベンダーと開発者にとって、独自の接続エージェントの開発と配置が容易になります。

  関連項目： 第 VII 部 :「Oracle Directory Integration and Provisioning Platform」

- **パスワード・ポリシーの管理**

  パスワード・ポリシーの管理によって、パスワード使用規則の確立と強化が可能になります。

  関連項目：

  - 12-8 ページの「Oracle Internet Directory のパスワード・ポリシー」
  - 第 15 章「Oracle Internet Directory のパスワード・ポリシー」

- **パフォーマンスとスケーラビリティの強化**
- **アップグレード手順**

  これらの手順によって、Oracle Internet Directory リリース 2.1.1 からアップグレードできます。

- **UTF8 制限の削除**

  Oracle ディレクトリ・サーバーとデータベース・ツールの実行を UTF8 データベース上に限定する制限はなくなりました。ただし、クライアント要求とディレクトリ・サーバーのデータベース・リポジトリに含まれるデータのキャラクタ・セットが異なり、クライアント・データをデータベース・キャラクタ・セットにマップできない場合は、追加、削除、変更または識別名の変更操作中にデータが消失する可能性があります。Oracle ディレクトリ・サーバーの基礎となるデータベースが AL32UTF8 または UTF8 でない場合は、文字コードが同じかどうかにかかわらず、クライアント・キャラクタ・セットにある文字がすべてデータベース・キャラクタ・セットに含まれているかどうかを確認してください。

Oracle Internet Directory リリース 2.1.1 で導入された新機能

この項では、Oracle Internet Directory リリース 2.1.1 で導入された新機能について説明します。

- **属性オプション（言語コードを含む）**

  属性オプションを使用すると、検索または比較操作でその属性の値をどのように使用できるかを指定できます。たとえば、ある従業員がロンドンとニューヨークという 2 つの住所を持っているとします。その従業員の `address` 属性のオプションを使用すると、両方の住所を格納できます。ユーザーはいずれの住所も検索できます。

  属性オプションは言語コードを含むことができます。たとえば、John Doe の `givenName` 属性のオプションを使用すると、彼の名前をフランス語と日本語の両方で格納できます。ユーザーは、この名前をいずれの言語でも検索できます。

関連項目：

- 2-7 ページの「属性オプション」
- 7-8 ページの「Oracle Directory Manager を使用した属性オプション付きエントリの管理」
- 7-12 ページの「コマンドライン・ツールを使用した属性オプション付きエントリの管理」

- **変更ログの削除機能の拡張**

  これらの拡張によって、使用を停止する変更ログのタイプを、変更番号ベースまたは時間ベースで指定できます。

  関連項目：

  - 22-7 ページの「マルチマスター・レプリケーションの変更ログの削除」
  - 25-35 ページの「ディレクトリ・レプリケーション・サーバーの構成パラメータの表示および変更」

- **creatorsName、createTimestamp、modifiersName、modifyTimestamp の各操作属性の拡張サポート**

  この拡張サポートを使用して、これらの属性を 1 つ以上、検索に使用できます。

  関連項目：

  - 2-4 ページの「属性情報の種類」
  - `createTimestamp` 属性を使用した検索操作の例は、A-43 ページの「例 7: 全ユーザー属性および指定した操作属性の検索」を参照してください。

- **他の LDAP 準拠のディレクトリからの移行**

  この新機能によって、他の LDAP バージョン 3 準拠のディレクトリから Oracle Internet Directory へデータを移行できます。

  関連項目： 第 23 章「他のディレクトリからのデータの移行」

- **オブジェクト・クラスの増加**

  オブジェクト・クラスが増加したため、エントリに対する操作の追加や実行が、そのエントリに関連するスーパークラスの階層全体を指定せずに可能になります。

  関連項目： この機能をオブジェクト・クラスの追加で使用する方法は、6-3 ページの「オブジェクト・クラスの追加のガイドライン」を参照してください。

- **OID データベース統計収集ツール**

  このツールは容量計画を支援するものです。様々なデータベース・スキーマ・オブジェクトを分析して統計を見積もる場合に役立ちます。

  関連項目： A-131 ページの「OID データベース統計収集ツール（oidstats.sh）の構文」

- **パスワード保護機能の拡張**

  この新機能は、パスワードをハッシュ値として格納することによって、利用できるパスワード保護を強化するものです。パスワードを暗号値ではなく一方向ハッシュ値として格納することによって、パスワードのセキュリティが向上します。これは、悪意のあるユーザーにはこれらの値を読むことも復号化することもできないためです。次のハッシュ・アルゴリズムのいずれかを選択できます。

  - **MD4**: 128 ビットのハッシュを生成する一方向ハッシュ関数です。
  - **MD5**: MD4 が改善された、より複合的なバージョンです。
  - **SHA**: Secure Hash Algorithm。MD5 よりも長い 160 ビットのハッシュを生成します。このアルゴリズムは MD5 よりも若干速度が遅くなりますが、大きなメッセージ・ダイジェストによって、総当り攻撃や反転攻撃に対処できます。
  - **UNIX Crypt**: UNIX 暗号化アルゴリズムです。
  - ハッシングなし

  関連項目：

  - 12-8 ページの「ディレクトリ認証用ユーザー・パスワードの保護」
  - パスワード・ハッシングの設定方法は、第 15 章「Oracle Internet Directory のパスワード・ポリシー」を参照してください。

- **レプリケーション・ツール**

  次の新しいレプリケーション・ツールが追加されました。

  - **管理者操作キュー操作ツール**

    管理者操作キューからリトライ・キューかパージ・キューへ、変更を移動できます。

  - **OID 調停ツール**

    このツールを使用して、レプリケートされた環境で発生する変更の競合を同期化できます。

    関連項目：

    - 4-14 ページの「コマンドラインツールの使用方法」
    - 25-21 ページの「管理者操作キュー操作ツールの概要」
    - 25-21 ページの「OID 調停ツールの概要」

- **レプリケーション・ノードの削除**

  この新機能を使用して、ディレクトリ・レプリケーション・グループからノードを削除できます。

  関連項目： 25-18 ページの「マルチマスター・レプリケーション・グループからのノードの削除」

- **メタディレクトリ環境での複数ディレクトリとの同期（リリース 2.1.1 のみ）**

  メタディレクトリ環境で作業している場合は、この新機能を使用して、複数ディレクトリを Oracle Internet Directory と同期化して単一の仮想ディレクトリを構成できます。

  注意： この機能は、リリース 3.0.1 で Oracle Directory Integration and Provisioning Platform に置き換えられました。詳細は、第 32 章「Oracle Directory Integration and Provisioning Platform の概要とコンポーネント」を参照してください。

- **アップグレード手順（リリース 2.1.1 のみ）**

  この新しい手順を使用して、Oracle Internet Directory リリース 2.0.4.x またはリリース 2.0.6 からアップグレードできます。リリース 2.1.1.1 またはリリース 3.0.1 では、この機能はサポートされていません。

第I部

スタート・ガイド

第 I 部では、Oracle Internet Directory の概要と使用する前に知っておく必要のある概念について説明します。第 I 部は次の各章で構成されています。

- 第 1 章「LDAP および Oracle Internet Directory の概要」
- 第 2 章「ディレクトリの概念およびアーキテクチャ」
- 第 3 章「事前に実行するタスクと情報」
- 第 4 章「ディレクトリ管理ツール」

1

LDAP および Oracle Internet Directory の概要

この章では、オンライン・ディレクトリ、Lightweight Directory Access Protocol（LDAP）バージョン 3 の概要、および Oracle Internet Directory 固有の機能と利点について説明します。

この章では、次の項目について説明します。

ディレクトリとは

ディレクトリとは、複雑な情報を編成する方法であり、検索を簡単にします。ディレクトリには、リソース（たとえば、人、図書館の本、百貨店の商品など）をリストし、それぞれに関する詳細情報を設定します。ディレクトリは、オフライン（たとえば、電話帳、百貨店のカタログ）、オンラインのいずれでも使用できます。

オンライン・ディレクトリは、分散コンピュータ・システムを持つ企業が、迅速な検索、ユーザーとセキュリティに対する費用効果の高い管理および複数のアプリケーションとサービスの中央統合の目的で使用しています。オンライン・ディレクトリは、E-Business およびホスティングされた環境の双方にとっても重要なものになりつつあります。

次の項目について説明します。

- 拡大するオンライン・ディレクトリの役割
- 問題点 : 特別な用途を指定されたディレクトリが多すぎる場合

拡大するオンライン・ディレクトリの役割

オンライン・ディレクトリは、オブジェクトに関する一連の情報を格納し検索する特殊なデータベースです。このような情報で、管理を必要とするあらゆるリソースを表現できます。これらのリソースには、従業員の氏名、役職およびセキュリティ資格証明、パートナの情報、会議室やプリンタなどの共有ネットワーク・リソースに関する情報などがあります。

オンライン・ディレクトリは様々なユーザーやアプリケーションによって、次のような様々な用途で使用されます。

- 従業員は、メール・クライアントを使用して、会社のインターネットのアドレス帳から電子メール・アドレスを調べます。
- メッセージ転送エージェントのようなアプリケーションが、ユーザーのメール・サーバーの位置を特定します。
- データベース・アプリケーションは、ユーザーのロール情報を識別します。

オンライン・ディレクトリはデータベース（データの構造化された集合）ですが、**リレーショナル・データベース**にはなっていません。次の表はオンライン・ディレクトリをリレーショナル・データベースと対比しています。

表 1-1 オンライン・ディレクトリとリレーショナル・データベースの比較

オンライン・ディレクトリ	リレーショナル・データベース
主に読取りを目的としています。一般的な使用例では、データの更新が比較的少なく、検索が多い傾向があります。	**主に書込みを目的としています。**一般的な使用例では、トランザクションが連続的に記録され、検索が比較的少ない傾向があります。

表 1-1 オンライン・ディレクトリとリレーショナル・データベースの比較（続き）

オンライン・ディレクトリ	リレーショナル・データベース
比較的小規模な単位のデータで比較的単純なトランザクションを処理するように設計されています。たとえば、アプリケーションがディレクトリを使用して、電子メール・アドレス、電話番号またはデジタル画像の格納および検索のみを行う場合があります。	**大規模な単位のデータで多数の操作を利用しながら、多様で大量のトランザクションを処理するように設計されています。**
ロケーションに依存しないように設計されています。ディレクトリ対応アプリケーションは、問合せ中のサーバーに関係なく、配置環境全体にわたって常に同じ情報を参照していると想定しています。問合せ先のサーバーにローカルの情報が格納されていない場合、そのサーバーはその情報を取り出すか、クライアント・アプリケーションにその情報を透過的に示す必要があります。	**一般的にはロケーション固有に設計されています。**リレーショナル・データベースは分散が可能ですが、通常は特定のデータベース・サーバーに常駐します。
情報をエントリに格納するように設計されています。これらのエントリは、従業員、E-Commerce パートナ、会議室、プリンタのような共有ネットワーク・リソースなど、管理が必要なリソースを表します。各エントリには、多数の属性が対応付けられます。それぞれの属性には 1 つ以上の値が割り当てられる場合があります。たとえば、person エントリの一般的な属性は、姓名、電子メール・アドレス、デフォルトのメール・サーバーのアドレス、パスワードまたは他のログイン資格証明、デジタル化された顔写真などです。	**リレーショナル表に行として情報を格納するように設計されています。**

問題点 : 特別な用途を指定されたディレクトリが多すぎる場合

ある見積りによると、世界規模の企業は平均 180 種類のディレクトリを作成しており、それぞれに特別な用途を指定しています。様々なエンタープライズ・アプリケーションには、ユーザー名を割り当てた固有のディレクトリがあるため、それら専用ディレクトリの実際の数はさらに増えます。

専用のディレクトリを多数管理していると、次のような問題が発生する可能性があります。

- 高い管理費用 : 管理者は、複数の場所で基本的には同じ情報をメンテナンスする必要があります。たとえば、ある企業が新しい従業員を雇用するとき、管理者は新しいユーザー ID をネットワークに作成し、新しい電子メール・アカウントを作成し、そのユーザーを従業員データベースに追加し、そして従業員が必要とするすべてのアプリケーション（開発、テストおよび本番データベース・システムのユーザー・アカウントなど）を設定する必要があります。その従業員が退社した場合は、管理者はこれらのユーザー・アカウントをすべて無効にするために逆の処理を行う必要があります。

- 一貫性のないデータ : 大きな管理オーバーヘッドのため、複数のシステムに冗長な情報を入力している複数の管理者にとっては、この従業員の情報をすべてのシステムで同期化させることが困難な場合があります。結果として、企業内で一貫性のないデータが発生することになります。
- セキュリティの問題 : 各ディレクトリには、独自のパスワード・ポリシーがあります。これは、異なるシステムで、ユーザーが様々なユーザー名とパスワードのために混乱する可能性があることを意味します。

今日の企業には、様々なアプリケーションとサービスをサポートするために、共通の規格に基づいた汎用性の高いディレクトリのインフラストラクチャが必要です。

Lightweight Directory Access Protocol（LDAP）とは

LDAP は、標準的で拡張可能なディレクトリ・アクセス・プロトコルです。LDAP は、LDAP クライアントとサーバーが通信を行うための共通言語です。

この項では、次の項目について説明します。

LDAP と単純化されたディレクトリ管理

LDAP は、国際標準化機構（ISO）のディレクトリ・サービスに関する X.500 規格の、インターネットに対応する軽量実装として考え出されました。クライアント側に必要なネットワーキング・ソフトウェアを最小限に抑えられるため、インターネット・ベースの Thin クライアント・アプリケーションには特に理想的です。

LDAP 規格は、ディレクトリ情報の管理を次の 3 つの方法で単純化します。

- 拡張可能な単一のディレクトリ・サービスに対し、正しく定義された単一の標準インタフェースを、企業内のすべてのユーザーとアプリケーションに提供します。これによって、ディレクトリに対応したアプリケーションの迅速な開発と配置が簡単になります。
- 企業内に散在する複数のサービスへの、冗長な情報の入力と調整の必要性を低減します。
- 正しく定義されたプロトコルと一連のプログラム・インタフェースによって、ディレクトリを活用するインターネット対応のアプリケーションの配置がより実用的になります。

LDAP バージョン 3

最新バージョンの LDAP バージョン 3 は、1997 年 12 月、**Internet Engineering Task Force（IETF）**によって、標準のインターネット勧告として承認されました。LDAP バージョン 3 では、次のいくつかの重要な領域において LDAP バージョン 2 の内容が改善されています。

- グローバリゼーション・サポート : LDAP バージョン 3 では、世界中の言語で使用されている文字を、サーバーとクライアントの両方でサポートできます。
- ナレッジ参照（参照とも呼ばれる）: LDAP バージョン 3 の参照機能によって、サーバーは、ディレクトリ問合せの結果として、参照を他のサーバーに戻すことができます。これにより、**ディレクトリ情報ツリー**を複数の LDAP サーバーにわたってパーティション化して、ディレクトリをグローバルに分散できます。
- セキュリティ : LDAP バージョン 3 では、**Simple Authentication and Security Layer（SASL）**をサポートするための標準機能が追加され、データ・セキュリティに関する総合的で拡張可能なフレームワークが提供されています。
- スケーラビリティ : LDAP バージョン 3 では、ベンダーは、コントロールと呼ばれるメカニズムを使用して既存の LDAP 操作を拡張できます。
- 機能およびスキーマの開示 : LDAP バージョン 3 では、他の LDAP サーバーやクライアントに役立つ情報（サポートされる LDAP プロトコルやディレクトリ・スキーマの説明など）を公開できます。

関連項目：

- IETF の RFC（Requests for Comments）2251 ～ 2256。次の URL で入手可能です。`http://www.ietf.org`
- LDAP に関する参考資料のその他のリストは、xlviii ページの「関連ドキュメント」を参照してください。
- ディレクトリ情報ツリーおよびナレッジ参照の概念の説明は、第 2 章「ディレクトリの概念およびアーキテクチャ」を参照してください。

Oracle Internet Directory とは

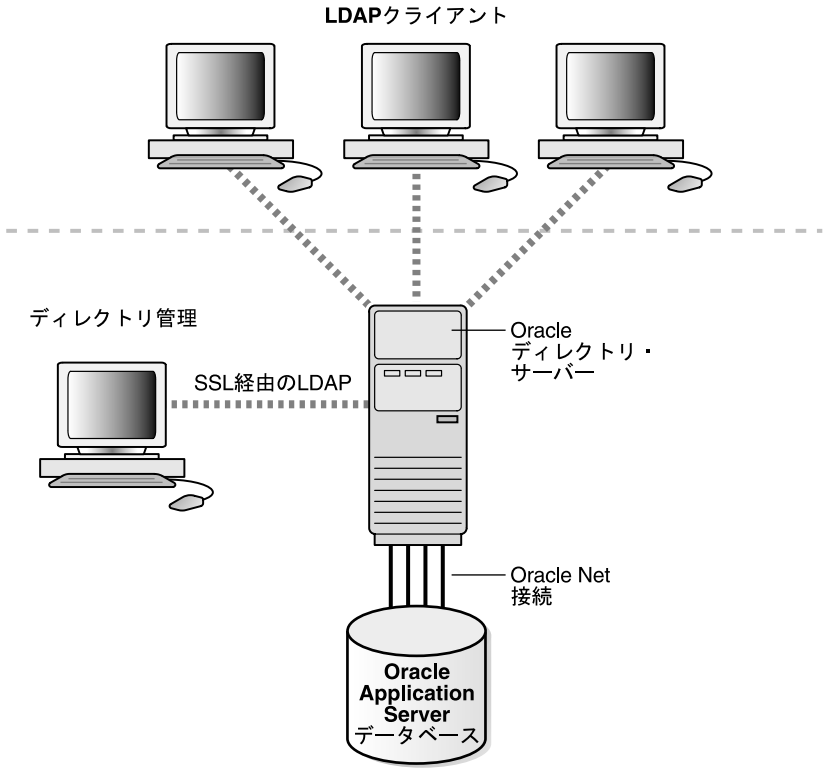
Oracle Internet Directory は、分散ユーザーやネットワーク・リソースに関する迅速な情報検索および情報の中央管理を可能にする、汎用ディレクトリ・サービスです。**Lightweight Directory Access Protocol（LDAP）**バージョン 3 と Oracle9*i* のすぐれたパフォーマンス、スケーラビリティ、耐久性および可用性を組み合せたものです。

この項では、次の項目について説明します。

Oracle Internet Directory のアーキテクチャ

Oracle Internet Directory は Oracle9*i* 上のアプリケーションとして動作します。オペレーティング・システムに依存しない Oracle のデータベース接続ソリューションである Oracle Net Services を使用して、データベース（オペレーティング・システムが異なっていてもかまいません）と通信します。図 1-1 に、この関係を示します。

図 1-1 Oracle Internet Directory のアーキテクチャ



Oracle Internet Directory のコンポーネント

Oracle Internet Directory のコンポーネントは、次のとおりです。

- Oracle ディレクトリ・サーバー。人員とリソースの情報に関するクライアントの要求に応答します。また、TCP/IP を介し、複数層アーキテクチャを直接使用して、その情報を更新します。
- Oracle ディレクトリ・レプリケーション・サーバー。Oracle ディレクトリ・サーバー間で、LDAP データをレプリケートします。
- ディレクトリ管理ツールには、次の内容が含まれます。
  - Oracle Directory Manager。Java ベースの Graphical User Interface（GUI）を使用してディレクトリの管理を簡素化します。
  - 各種のコマンドライン管理ツールとデータ管理ツール。これらは LDAP クライアントから呼び出されます。
  - Oracle Enterprise Manager Application Server Control 内のディレクトリ・サーバー管理ツール。これらの管理ツールにより、次のことが可能になります。
    * 標準的なブラウザからリアルタイム・イベントや統計の監視
    * これらのデータを新しいリポジトリに収集するプロセスの開始
- Oracle Internet Directory Software Developer's Kit

  関連項目： Oracle Internet Directory Software Developer's Kit の詳細は、『Oracle Internet Directory アプリケーション開発者ガイド』を参照してください。

Oracle Internet Directory の利点

Oracle Internet Directory の大きな利点は、スケーラビリティ、高可用性、セキュリティおよび Oracle 環境との緊密な統合です。

スケーラビリティ

Oracle Internet Directory は、Oracle9*i* の高機能を活用して、数テラバイト（TB）に及ぶディレクトリ情報のサポートを可能にします。さらに、共有 LDAP サーバーやデータベース接続プーリングなどのテクノロジによって、千単位の同時クライアントであっても、わずかな検索応答時間を実現します。

Oracle Internet Directory は、Oracle Directory Manager や様々なコマンドライン・ツールなど、大量の LDAP データを操作するためのデータ管理ツールも提供します。

高可用性

Oracle Internet Directory は、各種の基幹アプリケーションのニーズを満たすように設計されています。たとえば、ディレクトリ・サーバー間における完全なマルチマスター・レプリケーションをサポートします。レプリケーション・コミュニティ内のサーバーの 1 つが使用できなくなった場合、ユーザーは別のサーバーからデータにアクセスできます。サーバー上にあるディレクトリのデータの変更情報は、Oracle9*i* データベース上の専用の表に格納されます。この表は、堅牢なレプリケーション方式である **Oracle9i Advanced Replication** によって、ディレクトリ環境全体にわたってレプリケートされます。

Oracle Internet Directory は、Oracle9*i* の可用性機能もすべて活用しています。ディレクトリ情報は、Oracle9*i* データベースに安全に格納されるため、Oracle のバックアップ機能によって保護されます。また、Oracle9*i* データベースは、大規模なデータストアおよび高負荷で実行されていても、システム障害からすぐにリカバリできます。

セキュリティ

Oracle Internet Directory は、広範囲にわたる柔軟なアクセス制御を提供します。管理者は、特定のディレクトリ・オブジェクトまたはディレクトリ・サブツリー全体に対するアクセス権限を付与または制限できます。さらに、Oracle Internet Directory は、匿名、パスワード・ベースおよび **Secure Sockets Layer（SSL）** バージョン 3 を使用した証明書ベースという 3 つのレベルのユーザー認証を実装し、認証アクセスおよびデータ・プライバシが保障されています。

Oracle 環境との統合

Oracle Internet Directory は、Oracle Directory Integration and Provisioning Platform を介して、Oracle 環境と他のディレクトリ（NOS ディレクトリ、サード・パーティのエンタープライズ・ディレクトリ、アプリケーション固有のユーザー・リポジトリなど）の間で 1 箇所の統合ポイントを提供します。

Oracle Identity Management

Oracle Internet Directory は、Oracle Identity Management のコンポーネントの 1 つで、Oracle 製品や他のエンタープライズ・アプリケーションに対して分散セキュリティ・サービスを提供する統合インフラストラクチャです。Oracle Internet Directory の他、Oracle Identity Management インフラストラクチャは、次のコンポーネントと機能を含みます。

- Oracle Directory Integration and Provisioning Platform: このコンポーネントは、Oracle Internet Directory と次の機能を同期化します。
  - 他のディレクトリおよびユーザー・リポジトリ
  - Oracle コンポーネントおよびアプリケーションのための自動プロビジョニングサービス
  - サード・パーティのアプリケーション

- Oracle Delegated Administration Services: このコンポーネントは、ユーザーおよびアプリケーション管理者による、信頼できるプロキシ・ベースのディレクトリ情報管理を提供します。
- Oracle Application Server Single Sign-On: Oracle アプリケーションとサード・パーティのアプリケーションへのシングル・サインオン・アクセスを提供します。
- Oracle Application Server Certificate Authority: 強力な認証方式をサポートする X.509 V3 PKI 証明書を生成し、公開します。

エンタープライズ・アプリケーションの配置をサポートするため、通常は、単一の Oracle Identity Management インフラストラクチャが企業に配置されます。高可用性、情報ローカライゼーション、コンポーネントの委任管理を提供するため、複数のサーバーとコンポーネント・インスタンスを含めることができます。企業で追加する各アプリケーションは、認証管理サービスのために共有インフラストラクチャを活用します。この配置モデルには、次のような多数の利点があります。

- 認証管理インフラストラクチャの計画策定と実装は、エンタープライズ・アプリケーションを配置するたびに必要な作業ではなく、1 回のみ必要です。したがって、ポータル、J2EE アプリケーション、E-Business アプリケーションなどの新しいアプリケーションを迅速に配置できます。
- 識別情報は、複数の場所で管理可能であると同時に、集中管理され、すべてのエンタープライズ・アプリケーションに対してすぐに利用できます。
- 一元化されたセキュリティ・インフラストラクチャにより、ユーザーはエンタープライズ・アプリケーションに対してシングル・サインオンを利用できます。
- 一元化された認証管理インフラストラクチャは、エンタープライズ Oracle 環境と他の認証管理システムを 1 箇所で統合します。したがって、point-to-point 統合のために、複数のカスタム・ソリューションを用意する必要はありません。

関連項目：

- Oracle Identity Management インフラストラクチャの計画策定、配置および使用方法の詳細は、『Oracle Identity Management 概要および配置プランニング・ガイド』を参照してください。
- Oracle Identity Management に関連する Oracle Internet Directory の役割の詳細は、第 19 章「Oracle Identity Management レルムの配置」を参照してください。

Oracle コンポーネントにおける Oracle Internet Directory の使用方法

Oracle コンポーネントは、より容易な管理、厳重なセキュリティ、簡単な複数のディレクトリの統合を実現するために Oracle Internet Directory を使用します。

この項では、次の項目について説明します。

簡単で対費用効果の高いアプリケーション管理

OracleAS Portal により、Oracle Internet Directory に一般ユーザーとグループの属性を格納する、セルフ・サービスの統合されたエンタープライズ・ポータルを実現できます。Oracle Portal 管理ツールは、特定のタスクに対して Oracle Delegated Administration Services も活用します。

Oracle Collaboration Suite は、次の目的で Oracle Internet Directory を使用します。

- ユーザーとグループに関する情報の集中管理
- Provisioning Oracle Collaboration Suite コンポーネント。Oracle Internet Directory のデータに重要な変更が行われた場合のユーザーとグループへの通知
- 他のディレクトリと Oracle Collaboration Suite コンポーネントを接続しているエンタープライズの集中的な統合

Oracle Net Services は、データベース・サービスと単純な名前（ネット・サービス名と呼ばれ、サービスを表すために使用できる）の格納と解決に Oracle Internet Directory を使用します。

集中化されたセキュリティ・ポリシー管理による厳重なセキュリティ

Oracle9*i* は、Oracle Internet Directory を使用してユーザー名とパスワードを格納します。また、Oracle Internet Directory を使用して各ユーザーのエントリとともにパスワード・ベリファイアを格納します。

Oracle Application Server Single Sign-On は、Oracle Internet Directory を使用してユーザー・エントリを格納します。また、パートナ・アプリケーションのユーザーを Oracle Internet Directory エントリのユーザー・エントリにマップし、LDAP メカニズムを使用して認証します。

Oracle Advanced Security は、Oracle Internet Directory を使用して次の操作を実行します。

- ユーザー認証資格証明の集中管理

  Oracle Advanced Security は、ユーザーのデータベース・パスワードをそのユーザーのユーザー・エントリの属性として、各データベースではなくディレクトリに格納します。

- ユーザー認可の集中管理

  Oracle Advanced Security は、エンタープライズ・ロールと呼ばれるディレクトリ・エントリを使用して、指定のスキーマ（共有または所有）内でエンタープライズ・ユーザーに付与されている権限を判断します。エンタープライズ・ロールは、データベース固有のグローバル・ロールのコンテナです。たとえば、あるユーザーをエンタープライズ・ロールの事務担当に割り当て、このロールに、人事管理データベースに対するグローバル・ロールの人事担当とその補佐の権限、および給与管理データベースに対するグローバル・ロールの分析担当とその補佐の権限を含めることができます。

- 共有スキーマへのマッピング

  Oracle Advanced Security は、マッピング（個別のアカウントではなく、データベース上の共有アプリケーション・スキーマをエンタープライズ・ユーザーに指し示すディレクトリ・エントリ）を使用します。たとえば、複数のエンタープライズ・ユーザーを、ユーザー名の個別のアカウントではなく、スキーマ `sales_application` に対してマップできます。

- 単一パスワード認証

  Oracle9*i* では、Oracle Advanced Security によって、エンタープライズ・ユーザーは、集中管理された単一のパスワードを使用して複数のデータベースに対する認証を実行できます。パスワードは、ユーザーのエントリの属性としてディレクトリに格納され、暗号化とアクセス制御リスト（ACL）によって保護されます。この機能によって、クライアントでの Secure Sockets Layer（SSL）の設定に関係するオーバーヘッドを削減し、複数のパスワードを記憶する必要性からユーザーを解放します。

- エンタープライズ・ユーザー・セキュリティ

  集中管理されたパスワードによる認証に代わる方法として、SSL を介した PKI ベースのエンタープライズ・ユーザー・セキュリティの使用があります。単一パスワード認証と同様に、この機能はディレクトリのユーザー・エントリに依存します。ユーザーの Wallet は、そのユーザーのエントリの属性として格納する必要があります。

- PKI 資格証明の集中格納

  Oracle9*i* データベース・サーバーと Oracle Application Server では、ユーザー Wallet をユーザーのエントリの属性としてディレクトリに格納できます。この機能によって、モバイル・ユーザーは、Enterprise Login Assistant を使用して Wallet を取得およびオープンできます。Wallet のオープン中は、認証は透過的に行われます。つまり、ユーザーは、スキーマを所有または共有しているデータベースに、再認証せずにアクセスできます。

分散ディレクトリの統合

Oracle Directory Integration and Provisioning Platform は、インタフェースとサービスの集合で、Oracle Internet Directory といくつかの関係するプラグインやコネクタを使用して複数のディレクトリを統合します。

Oracle Directory Integration and Provisioning Platform には、次の利点があります。

- すべての Oracle コンポーネントでは、Oracle Internet Directory を使用することが事前に認証されています。
- サード・パーティの各ディレクトリを Oracle Internet Directory に統合することによって、Oracle 環境全体をサード・パーティ・ディレクトリに簡単に統合できます。したがって、各アプリケーションを各ディレクトリと統合するという複雑な作業から解放されます。

2

ディレクトリの概念およびアーキテクチャ

この章では、Oracle Internet Directory の基本要素の概念および Oracle Internet Directory のアーキテクチャについて説明します。

この章では、次の項目について説明します。

> **関連項目：** LDAP 準拠のディレクトリに関する参考文献のリストは、xlviii ページの「関連ドキュメント」を参照してください。

エントリ

オンライン・ディレクトリでは、オブジェクトに関する情報の集合は**エントリ**と呼ばれます。エントリには、社員、会議室、E-Commerce パートナ、プリンタなどの共有ネットワーク・リソースに関する情報が含まれます。

識別名（DN）とディレクトリ情報ツリー（DIT）

オンライン・ディレクトリ内の各エントリは、**識別名**で一意に識別されます。識別名は、ディレクトリ階層におけるそのエントリの位置を正確に伝えます。この階層は、**ディレクトリ情報ツリー**で示されます。

識別名とディレクトリ情報ツリーとの関係を理解するには、図 2-1 を参照してください。

図 2-1 ディレクトリ情報ツリー

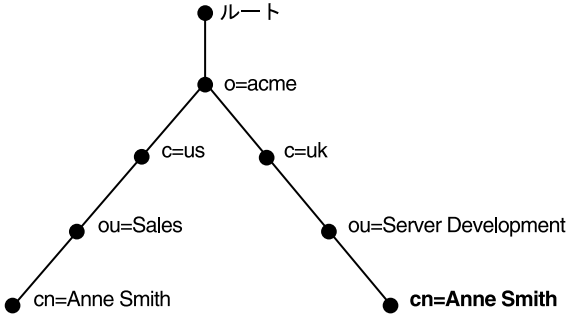


図 2-1 のディレクトリ情報ツリーは、どちらも Acme Corporation に所属する、Anne Smith という同名の 2 人の従業員のエントリを図示しています。この図のディレクトリ情報ツリーは、地理的および組織的な系統に従って構造化されています。左の分岐の Anne Smith は米国の Sales 部門に勤務し、もう一方の Anne Smith は英国の Server Development 部門に勤務しています。

右の分岐の Anne Smith は、Anne Smith という一般名（cn）を持っています。彼女は、組織（o）が Acme、国（c）が英国（uk）で、Server Development という組織単位（ou）に勤務しています。

この Anne Smith エントリの識別名（DN）は次のとおりです。

```
cn=Anne Smith,ou=Server Development,c=uk,o=acme
```

識別名の慣習的な書式では、左から最下位のディレクトリ情報ツリー・コンポーネント、続いてその次の上位コンポーネントを記述し、ルートのコンポーネントまで順に記述することに注意してください。

識別名内の最下位コンポーネントは**相対識別名**と呼ばれます。たとえば、前述の Anne Smith のエントリの相対識別名は `cn=Anne Smith` です。同様に、Anne Smith の相対識別名のすぐ上のエントリに対応する相対識別名は `ou=Server Development`、`ou=Server Development` のすぐ上のエントリに対応する相対識別名は `c=uk` です。したがって、DN は DIT での親子関係を反映した RDN の連結です。DN 内では、RDN はカンマで区切ります。

ディレクトリ情報ツリー全体の中で特定エントリの位置を識別するために、クライアントは、その相対識別名のみではなく、エントリの完全な識別名を使用することによってそのエントリを一意に示します。たとえば、図 2-1 のグローバル組織内でこの 2 人の Anne Smith を混同しないように、それぞれの完全な識別名を使用できます（同一組織単位内に同じ名前の従業員が 2 人いる可能性がある場合は、一意の識別番号で各従業員を識別するなど、他の方法を使用してください）。

エントリ・キャッシング

エントリに対して迅速で効率的な操作を行うために、Oracle Internet Directory はエントリ・キャッシングを使用します。この機能を有効にした場合、Oracle Internet Directory は、各エントリに一意の識別子を割り当て、指定された数の識別子をキャッシュ・メモリーに格納します。ユーザーがエントリに対する操作を行うと、ディレクトリ・サーバーは、キャッシュ内でエントリ識別子を検索し、対応するエントリをディレクトリから取得します。この方法によって、Oracle Internet Directory のパフォーマンスが強化されます。小規模から中規模の企業では特に有効です。

注意： Oracle Internet Directory 10*g*（9.0.4）では、単一サーバー、単一インスタンスの Oracle Internet Directory ノードの場合にのみ、エントリ・キャッシングを使用できます。

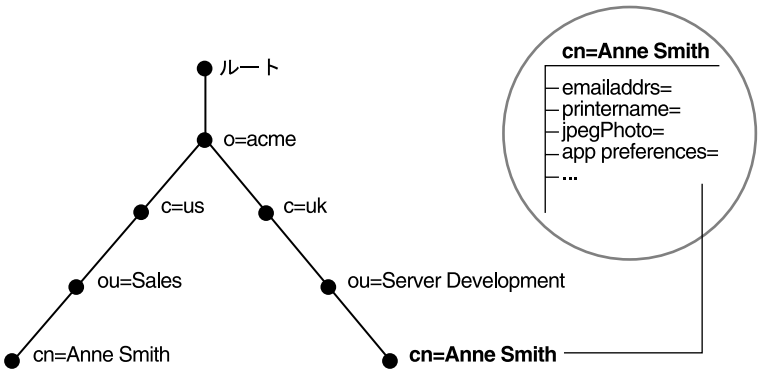
関連項目： 第 7 章「ディレクトリ・エントリの管理」

属性

一般的な電話帳の場合、個人に関する**エントリ**には住所や電話番号などの情報項目が含まれます。オンライン・ディレクトリでは、このような情報項目は**属性**と呼ばれます。一般的な従業員エントリの属性には、役職名、電子メール・アドレス、電話番号などがあります。

たとえば、図 2-2 では、英国（uk）の Anne Smith に関するエントリには、その個人の固有な情報を提供する各種の属性があります。これらの属性はツリーの右側の円の中にリストされています。`emailaddrs`、`printername`、`jpegPhoto` および `app preferences` などの情報が記述されています。さらに、図 2-2 の各黒丸も属性を持つエントリですが、ここではそれぞれの属性は示されていません。

図 2-2 Anne Smith のエントリの属性



各属性は、属性の型と 1 つ以上の属性値で構成されます。**属性の型**とは、その属性に含まれている情報の種類（例：`jobTitle`）を指します。**属性値**は、そのエントリに含まれる情報の具体的な内容です。たとえば、`jobTitle` 属性に対する値には `manager` があります。

この項では、次の項目について説明します。

- 属性情報の種類
- 単一値と複数値の属性
- 属性オプション
- 一般的な LDAP 属性
- 属性の構文
- 属性の一致規則

属性情報の種類

属性には 2 種類の情報があります。

- アプリケーション属性

  この情報は、ディレクトリ・クライアントによってメンテナンスおよび取出しが行われ、ディレクトリの操作には影響しません。例として電話番号があります。

- 操作属性

  この情報は、ディレクトリ自体の操作に関係します。一部の操作情報は、サーバーを制御するためにディレクトリによって指定されます。たとえば、エントリの作成や変更のタイムスタンプ、エントリを作成または変更したユーザーの名前などです。アクセス情報などのその他の操作情報は、管理者が定義し、ディレクトリ・プログラムの処理時に、そのプログラムによって使用されます。

エントリがディレクトリに追加されると、エントリを検索する機能を拡張するために Oracle Internet Directory が自動的にいくつかのシステム操作属性を作成します。たとえば次のようなものです。

属性	説明
creatorsName	エントリ作成者の名前
createTimestamp	**UTC（Coordinated Universal Time）**でのエントリの作成時間
modifiersName	エントリ変更者の名前
modifyTimestamp	UTC でのエントリの変更時間

ユーザーがエントリを変更すると、Oracle Internet Directory は自動的に modifiersName 属性をエントリを変更したユーザーの名前に、modifyTimestamp 属性を UTC で表したエントリ変更時間にそれぞれ更新します。

> **関連項目：** システム操作属性の構成方法は、5-9 ページの「システム操作属性の設定」を参照してください。

単一値と複数値の属性

属性には、単一値または複数値のいずれかを設定できます。単一値の属性には 1 つの値のみ設定でき、複数値の属性には複数の値を設定できます。複数値の属性の例には、グループ全員の名前を載せたグループ・メンバーシップ・リストがあります。

一般的な LDAP 属性

Oracle Internet Directory は、標準的な LDAP 属性をすべて実装しています。表 2-1 に、Internet Engineering Task Force（IETF）の RFC 2798 に定義されている、一般的な LDAP 属性の一部を示します。

表 2-1 一般的な LDAP 属性

属性の型	属性の文字列	説明
commonName	cn	エントリの一般的な名前（Anne Smith など）。
domainComponent	dc	ドメイン・ネーム・システム（DNS）にあるコンポーネントの識別名 （dc=uk、dc=acme、dc=com など）。
jpegPhoto	jpegPhoto	JPEG フォーマットの写真イメージ。バイナリ形式で格納されます。
organization	o	組織の名前（my_company など）。
organizationalUnitName	ou	組織内の単位の名前（Server Development など）。

表 2-1 一般的な LDAP 属性（続き）

属性の型	属性の文字列	説明
owner	owner	エントリの所有者を識別する名前（cn=Anne Smith、ou=Server Development、o=Acme、c=uk など）。
surname、sn	sn	ユーザーの姓（Smith など）。
telephoneNumber	telephoneNumber	電話番号（(650) 123-4567、6501234567 など）。

関連項目： Oracle Internet Directory で使用できる属性のリストは、付録 B「Oracle Internet Directory のスキーマ要素」を参照してください。

属性の構文

属性の構文とは、各属性にロード可能なデータの形式のことです。たとえば、telephoneNumber 属性の構文の場合、電話番号は空白やハイフンを含む一続きの数値であることが必要です。しかし、別の属性の構文では、そのデータに日付書式が必要かどうか、または数値データかどうかを指定することが必要な場合もあります。各属性には必ず 1 つの構文を付加する必要があります。

Oracle Internet Directory は、**Internet Engineering Task Force（IETF）**の RFC 2252 で指定されているほとんどの構文を認識するため、そのドキュメントに記述されている構文の大部分を属性に関連付けることができます。Oracle Internet Directory は、RFC 2252 構文の認識に加え、一部の LDAP 構文も適用します。Oracle Internet Directory ですでにサポートされているこれらの構文以外に、新規の構文を追加することはできません。

関連項目： B-43 ページの「LDAP 構文」

属性の一致規則

ディレクトリ・サーバーは、クライアントの要求に応じて、検索と比較の操作を実行します。この操作時に、ディレクトリ・サーバーは関連する**一致規則**を調査し、検索対象の属性値と、格納されている属性値との間の等価性を判断します。たとえば、telephoneNumber 属性に関連付けられた一致規則では、(650) 123-4567 を (650) 123-4567 または 6501234567 のいずれか、あるいはその両方と一致させることができます。属性の作成時に、その属性を一致規則と対応付けることができます。

Oracle Internet Directory は、標準的な LDAP 一致規則をすべて実装しています。Oracle Internet Directory ですでにサポートされているこれらの一致規則以外に、新規の一致規則を追加することはできません。

関連項目： B-46 ページの「一致規則」

属性オプション

属性の型には様々なオプションがあり、検索または比較操作でその属性の値をどのように使用できるかを指定できます。たとえば、ある従業員がロンドンとニューヨークという 2 つの住所を持っているとします。その従業員の address 属性のオプションを使用すると、両方の住所を格納できます。

さらに、属性オプションは言語コードを含むことができます。たとえば、John Doe の givenName 属性のオプションを使用すると、彼の名前をフランス語と日本語の両方で格納できます。

オプション付きの属性とその基本属性は、明確に区別できます。オプションがない場合、両者は同じ属性です。たとえば、givenName;lang-fr=Jean では、基本属性は givenName であり、この基本属性のフランス語の値は givenName;lang-fr=Jean です。

1 つ以上のオプションを持つ属性は、そのベース属性のプロパティ（一致規則、構文など）を継承します。前述の例では、オプション付きの属性 givenName;lang-fr=Jean が、givenName のプロパティを継承しています。

注意： 属性オプションは識別名内では使用できません。たとえば、識別名 givenName;lang-fr=Jean, ou=sales,o=acme,c=uk は不適切です。

関連項目：

- 7-8 ページの「Oracle Directory Manager を使用した属性オプション付きエントリの管理」
- 7-12 ページの「コマンドライン・ツールを使用した属性オプション付きエントリの管理」

オブジェクト・クラス

オブジェクト・クラスはエントリの構造を定義する属性のグループです。ディレクトリ・**エントリ**を定義するときは、そのエントリに 1 つ以上のオブジェクト・クラスを割り当てます。これらのオブジェクト・クラスでは、一部の属性の指定は必須で、値を指定する必要がありますが、それ以外の属性はオプションで、空にできます。

たとえば、organizationalPerson オブジェクト・クラスには、必須属性の commonName（cn）と surname（sn）が含まれています。また、オプション属性として、telephoneNumber、uid、streetAddress および userPassword が含まれています。organizationalPerson オブジェクト・クラスを使用してエントリを定義するときは、commonName（cn）および surname（sn）に値を定義する必要があります。しかし、telephoneNumber、uid、streetAddress および userPassword に値を指定する必要はありません。

この項では、次の項目について説明します。

サブクラス、スーパークラスおよび継承

サブクラスは、別のオブジェクト・クラスから導出されたオブジェクト・クラスです。サブクラスが導出されるオブジェクト・クラスは、その**スーパークラス**と呼ばれます。たとえば、オブジェクト・クラス organizationalPerson は、オブジェクト・クラス person のサブクラスです。逆に、オブジェクト・クラス person は、オブジェクト・クラス organizationalPerson のスーパークラスです。

サブクラスは、そのスーパークラスの属性をすべて**継承**します。たとえば、サブクラス organizationalPerson は、そのスーパークラス person の属性を継承しています。エントリも、そのスーパークラスが継承した属性を継承します。

注意： オブジェクト・クラス自体に値は含まれていません。値を持つのは、オブジェクト・クラスのインスタンス、つまりエントリのみです。サブクラスがスーパークラスから属性を継承するときは、スーパークラスの属性定義のみを継承します。

---

top と呼ばれる、スーパークラスを持たない特別なオブジェクト・クラスが 1 つあります。このオブジェクト・クラスは、ディレクトリ内のすべてのオブジェクト・クラスのスーパークラスの 1 つで、その属性定義はすべてのエントリに継承されます。

オブジェクト・クラスの型

オブジェクト・クラスには次の 3 つの型があります。

- 構造型
- 補助型
- 抽象型

構造型オブジェクト・クラス

構造型オブジェクト・クラスは、オブジェクトの基本的側面を記述します。使用するオブジェクト・クラスの大部分は構造型オブジェクト・クラスであり、すべてのエントリは少なくとも 1 つの構造型オブジェクト・クラスに属している必要があります。構造型オブジェクト・クラスの例としては、person や groupOfNames があります。

これらのオブジェクト・クラスは、実社会のエンティティと、その物理的属性および論理的属性をモデルとしています。たとえば、人、プリンタ、データベース接続などがあります。

構造型オブジェクト・クラスは、構造規則を使用して、特定のオブジェクト・クラスの下に作成可能なオブジェクトの種類に制限を与えます。たとえば、構造規則では、organization（o）オブジェクト・クラスの下にあるすべてのオブジェクトは organizational units（ou）であることが要求されます。この規則に従うと、person オブジェクトを organization オブジェクト・クラスのすぐ下に入力することはできません。同様に、構造規則では、person オブジェクトの下に organizational unit（ou）オブジェクトを置くことはできません。

補助型オブジェクト・クラス

補助型オブジェクト・クラスは、オプションの属性をグループ化したもので、エントリ内の既存の属性リストを拡張します。構造型オブジェクト・クラスと異なり、エントリを格納する場所に関する制限はなく、DIT でのそのエントリの位置にかかわらず、任意のエントリに接続できます。

注意： Oracle Internet Directory は、構造規則を施行していません。したがって、構造型オブジェクト・クラスと補助型オブジェクト・クラスは同様に処理されます。

抽象型オブジェクト・クラス

抽象型オブジェクト・クラスは、仮想のオブジェクト・クラスです。これは、オブジェクト・クラス階層の最上位レベルを指定する際にのみ使用されます。エントリに対する唯一のオブジェクト・クラスにはできません。たとえば、オブジェクト・クラス top は抽象型オブジェクト・クラスです。これは、構造型オブジェクト・クラスすべてに対するスーパークラスとして必要ですが、単独では使用できません。

top オブジェクト・クラスには、必須属性である objectClass の他に、次のオプション属性があります。top 内のオプション属性は次のとおりです。

- orclGuid: エントリが移動しても変わらないグローバル識別子
- creatorsName: オブジェクト・クラス作成者の名前
- createTimestamp: オブジェクト・クラスが作成された時間
- modifiersName: オブジェクト・クラスを最後に変更したユーザーの名前
- modifyTimestamp: オブジェクト・クラスが最後に変更された時間
- orclACI: この属性が定義されている**アクセス制御ポリシー・ポイント**の下のサブツリーにあるすべてのエントリに適用される**アクセス制御リスト**ディレクティブ
- orclEntryLevelACI: 特殊なユーザーなどの特定のエンティティのみに関連するアクセス制御ポリシー

関連項目：

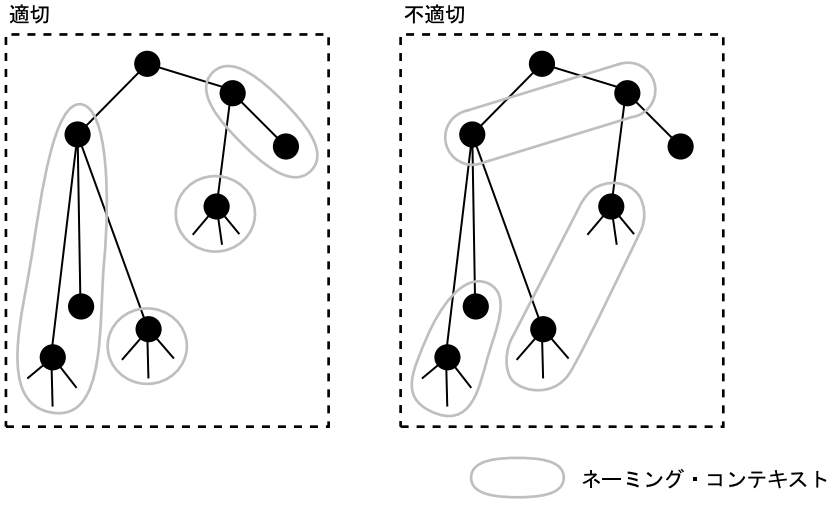
- アクセス制御ポリシーおよび ACL の詳細は、2-12 ページの「グローバリゼーション・サポート」を参照してください。
- エントリにコンテンツを追加する方法の詳細は、6-20 ページの「エントリと関連付けられた属性数の拡大方法」を参照してください。

ネーミング・コンテキスト

ネーミング・コンテキストは、その全体が 1 つのサーバーに常駐しているサブツリーです。このサブツリーは完全である必要があります。つまり、サブツリーの最上位の役割を果たす**エントリ**から始まり、下位のリーフ・エントリまたは従属ネーミング・コンテキストへの参照までを範囲とする必要があります。単一のエントリから **DIT** 全体までをその範囲とすることができます。

図 2-3 に、適切なネーミング・コンテキストと不適切なネーミング・コンテキストを示します。左側の適切なコンテキストは連続しており、右側の不適切なコンテキストは連続していないことに注意してください。

図 2-3 適切なネーミング・コンテキストと不適切なネーミング・コンテキスト



ユーザーが特定のネーミング・コンテキストを検出できるようにするには、Oracle Directory Manager または ldapmodify を使用して、Oracle Internet Directory でそれらのネーミング・コンテキストを公開する必要があります。

関連項目： ネーミング・コンテキストの公開方法は、5-9 ページの「ネーミング・コンテキストの管理」を参照してください。

セキュリティ

Oracle Internet Directory は、Oracle Identity Management インフラストラクチャの重要な要素です。これを使用すると、複数の Oracle コンポーネントを Oracle Internet Directory の共有インスタンスや関連付けられたインフラストラクチャの各部分に対して機能するように配置できます。この共有により、企業はすべてのアプリケーションでセキュリティ管理を単純化できます。

Oracle Identity Management インフラストラクチャで果たす役割に加えて、Oracle Internet Directory は情報を保護するための多数の強力な機能を提供します。

Oracle Internet Directory 自体に、次のようなセキュリティ機能があります。

- データ整合性 : 伝送中のデータが改ざんされないことを保証します。
- データ・プライバシ : ネットワーク内で Oracle Internet Directory と他のコンポーネントとの間の伝送中にデータが不正に覗かれないように保証します。
- 認証 : ユーザー、ホストおよびクライアントの識別情報が正しく検証されていることを保証します。
- 認可 : ユーザーが権限を持つ情報のみを読取りまたは更新することを保証します。
- パスワード・ポリシー : パスワードの定義方法と使用方法に関する規則を確立し、適用することを保証します。
- パスワード保護 : 第三者がパスワードを簡単に解読できないことを保証します。

企業またはホスティングされた環境では、これらの機能をすべて使用して、Oracle Internet Directory を使用できる複数のアプリケーションに一貫したセキュリティ・ポリシーを施行できます。このためには、管理業務の委任を行うためのディレクトリを配置します。この配置によって、たとえば、グローバル管理者は、部門にあるアプリケーションのメタデータに対するアクセスをその部門の管理者に委任できます。その結果、部門の管理者が自部門のアプリケーションへのアクセスを制御できるようになります。

関連項目：

- Oracle Internet Directory のセキュリティ機能の詳細は、第 12 章「ディレクトリ・セキュリティの概要」を参照してください。
- Oracle Identity Management インフラストラクチャと Oracle Internet Directory の関係については、第 19 章「Oracle Identity Management レルムの配置」を参照してください。
- 大企業やホスティングされた環境でアプリケーションを保護する方法の詳細は、第 17 章「Oracle テクノロジ配置のための権限の委任」を参照してください。
- Oracle Directory Integration and Provisioning Platform 環境におけるセキュリティの詳細は、第 36 章「Oracle Directory Integration and Provisioning Platform におけるセキュリティ」を参照してください。
- Oracle Identity Management インフラストラクチャの詳細は、『Oracle Identity Management 概要および配置プランニング・ガイド』を参照してください。

グローバリゼーション・サポート

Oracle Internet Directory は、LDAP バージョン 3 国際化（I18N）規格に準拠しています。この規格では、ディレクトリ・データを格納するデータベースで **UTF-8**（Unicode Transformation Format 8-bit）キャラクタ・セットを使用する必要があります。（Oracle キャラクタ・セット名は AL32UTF8 です。）この規格に従って、Oracle Internet Directory は、Oracle グローバリゼーション・サポートがサポートするほとんどすべての言語の文字データを格納できます。また、Oracle Internet Directory の実装では異なる **Application Program Interface（API）**がいくつか含まれていますが、Oracle Internet Directory では、各 API に正しい文字エンコーディングが使用されることを保証しています。

グローバリゼーション・サポートとは、シングルバイト文字とマルチバイト文字の双方をサポートすることを意味します。シングルバイト文字は、1 バイトのメモリーで表されます。たとえば、ASCII テキストはシングルバイト文字を使用します。一方、マルチバイト文字は、複数バイトで表すことができます。たとえば、簡体字中国語はマルチバイト文字を使用します。簡体字中国語のディレクトリ・エントリ定義の ASCII 表現は次のとおりです。

```
dn: o=¥274¥327¥271¥307¥316¥304,c=¥303¥300¥271¥372
objectclass: top
objectclass: organization
o: ¥274¥327¥271¥307¥316¥304
```

属性値は、簡体字中国語のディレクトリ・エントリ定義の ASCII 表現に対応します。

デフォルトでは、Oracle Internet Directory の主なコンポーネントである OID モニター（OIDMON）、OID 制御ユーティリティ（OIDCTL）、Oracle ディレクトリ・サーバー（OIDLDAPD）、Oracle ディレクトリ・レプリケーション・サーバー（OIDREPLD）および Oracle Directory Integration and Provisioning Server（ODISRV）は、常に UTF-8 キャラクタ・セットを使用します。Oracle キャラクタ・セット名は AL32UTF8 です。

Oracle ディレクトリ・サーバーとデータベース・ツールの実行を UTF8 データベース上に限定していた、従来の制限はなくなりました。ただし、Oracle Internet Directory サーバーの基礎となるデータベースが AL32UTF8 または UTF8 でない場合は、クライアント・キャラクタ・セットにある文字がすべて（文字コードが同じかどうかにかかわらず）データベース・キャラクタ・セットに含まれていることを確認してください。異なるキャラクタ・セットの場合は、クライアント・データをデータベース・キャラクタ・セットにマップできない場合に、LDAP の追加、変更または識別名の変更操作でデータが消失する可能性があります。

Java ベースのツールである Oracle Directory Manager は、内部的に **Unicode**（固定幅の 16 ビット Unicode である **UTF-16**）を使用します。Oracle Directory Manager は国際化キャラクタ・セットをサポートできます。

関連項目：

- Oracle Internet Directory の主なコンポーネントの詳細は、2-13 ページの「Oracle Internet Directory のアーキテクチャ」を参照してください。
- Oracle Internet Directory におけるグローバリゼーション・サポートの使用方法は、付録 G「ディレクトリにおけるグローバリゼーション・サポート」を参照してください。
- グローバリゼーション・サポートの詳細は、『Oracle グローバリゼーション・ガイド』を参照してください。

Oracle Internet Directory のアーキテクチャ

この項では、次の項目について説明します。

Oracle Internet Directory のノード

Oracle Internet Directory のノードは、同じディレクトリ・ストアに接続された 1 つ以上のディレクトリ・サーバー・インスタンスで構成されます。ディレクトリ・ストア、すなわちディレクトリ・データのリポジトリは、Oracle9*i* データベース・サーバーです。

2-15 ページの図 2-4 に、単一ノード上で稼働している様々なディレクトリ・サーバー・コンポーネントと、それらの関係を示します。

Oracle データベース・サーバーと次のものとの接続には、いずれも Oracle Net Services が使用されます。

- **OID 制御ユーティリティ**
- Oracle ディレクトリ・サーバー・インスタンス 1 非 SSL ポート 389
- Oracle ディレクトリ・サーバー・インスタンス 2SSL 対応ポート 636
- **OID モニター**

LDAP は、非 SSL ポート 389 上のディレクトリ・サーバー・インスタンス 1 と次のものとの間の接続に使用されます。

- Oracle Directory Manager
- Oracle ディレクトリ・レプリケーション・サーバー

2 つの Oracle ディレクトリ・サーバー・インスタンスと Oracle ディレクトリ・レプリケーション・サーバーは、オペレーティング・システム経由で OID モニターに接続します。

図 2-4 一般的な Oracle Internet Directory のノード

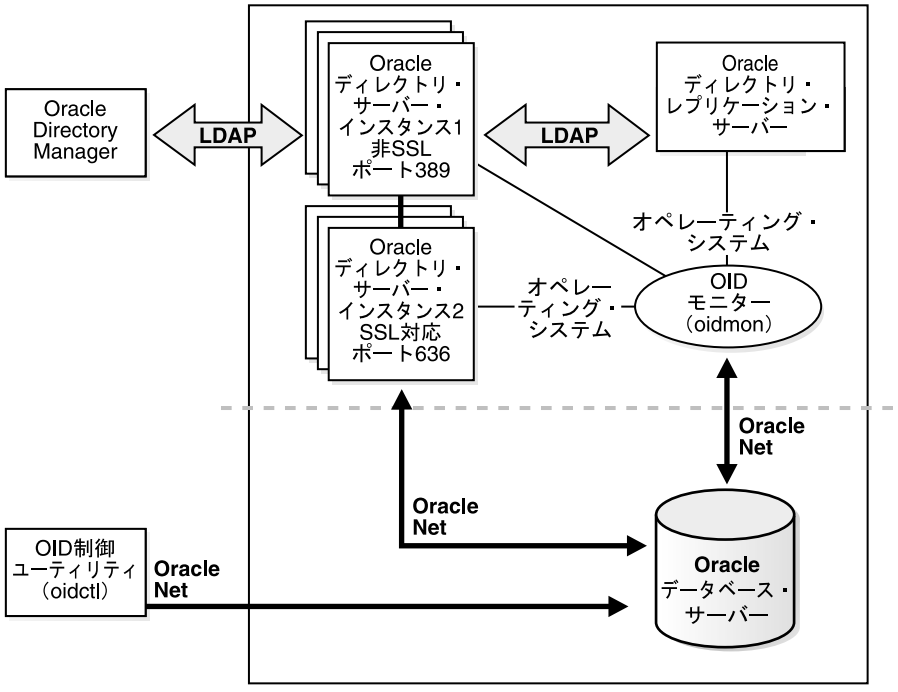


図 2-4 に示すとおり、Oracle Internet Directory のノードには、次の主なコンポーネントがあります。

表 2-2 Oracle Internet Directory のノードのコンポーネント

コンポーネント	説明
Oracle ディレクトリ・サーバー・インスタンス	LADP サーバー・インスタンスまたはディレクトリ・サーバー・インスタンスとも呼ばれ、特定の TCP/IP ポートでリスニングする単一の Oracle Internet Directory ディスパッチャ・プロセスを介して、ディレクトリ要求に応答します。それぞれが異なるポートをリスニングする複数のディレクトリ・サーバー・インスタンスをノードに持つことができます。
Oracle ディレクトリ・レプリケーション・サーバー	レプリケーション・サーバーとも呼ばれ、他の Oracle Internet Directory システム内のレプリケーション・サーバーの変更を追跡し、その内容を送信します。1 つのノード上に設定できるレプリケーション・サーバーは 1 つのみです。レプリケーション・サーバーを構成するかどうかは選択できます。

表 2-2 Oracle Internet Directory のノードのコンポーネント（続き）

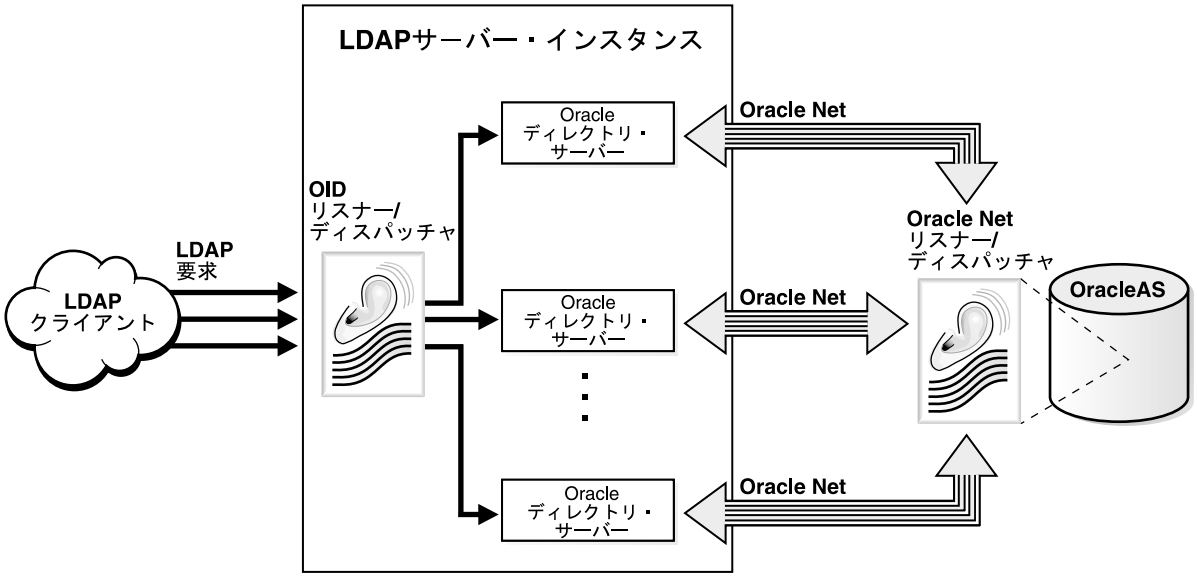
コンポーネント	説明
Oracle データベース・サーバー	ディレクトリ・データを格納します。データベースをこのディレクトリ専用に使用することをお薦めします。データベースは、ディレクトリ・サーバー・インスタンスと同じノードに常駐できます。
OID モニター（OIDMON）	LDAP のサーバー・プロセスを開始、モニターおよび終了します。レプリケーション・サーバーをインストールするように選択した場合、レプリケーション・サーバーは OID モニターによって制御されます。ディレクトリ・サーバー・インスタンスを起動または停止するために OID 制御ユーティリティ（OIDCTL）を介してコマンドを発行すると、そのコマンドはこのプロセスによって解析されます。 OID モニターは、管理者が OID 制御ユーティリティで行う LDAP サーバー・インスタンスの起動と停止の要求を処理します。また、OID モニターはサーバーを監視し、例外的な理由で実行が停止した場合に再起動させます。 サーバー・インスタンスが起動すると、OID モニターは、ディレクトリ・インスタンスのレジストリにエントリを追加し、プロセス表内のデータを更新します。ディレクトリ・サーバー・インスタンスが停止すると、レジストリ・エントリおよびその特定のサーバー・インスタンスに対応しているデータをプロセス表から削除します。OID モニターが異常終了したサーバーを再起動する場合は、そのサーバーの起動時間でレジストリ・エントリを更新します。 OID モニターのアクティビティはすべて、ファイル *$ORACLE_HOME*/ldap/log/oidmon.log に記録されます。このファイルは、Oracle Internet Directory のサーバー・ファイル・システム上にあります。 OID モニターは、オペレーティング・システムに用意されているメカニズムを通して、サーバーの状態をチェックします。
OID 制御ユーティリティ（OIDCTL）	Oracle Internet Directory のサーバー表にメッセージ・データを格納することによって、OID モニターと通信します。このメッセージ・データには、各 Oracle ディレクトリ・サーバー・インスタンスの実行に必要な構成パラメータが含まれています。

Oracle ディレクトリ・レプリケーション・サーバーは LDAP を使用して、Oracle ディレクトリ（LDAP）サーバー・インスタンスと通信します。データベースとの通信には、すべてのコンポーネントが OCI/Oracle Net Services を使用します。Oracle Directory Manager とコマンドライン・ツールは、LDAP を介して Oracle ディレクトリ・サーバーと通信します。

Oracle ディレクトリ・サーバー・インスタンス

各 Oracle ディレクトリ・サーバー・インスタンスは LDAP サーバー・インスタンスとも呼ばれ、図 2-5 のようになります。

図 2-5 Oracle ディレクトリ・サーバー・インスタンスのアーキテクチャ



1 つのインスタンスは、1 つのディスパッチャ・プロセスと 1 つ以上のサーバー・プロセスで構成されます。デフォルトでは、インスタンスごとに 1 つのサーバー・プロセスがありますが、これは増やすことができます。Oracle Internet Directory ディスパッチャとサーバー・プロセスは、複数のスレッドを使用して、負荷を分散できます。LDAP クライアントは LDAP 要求を、そのポートで LDAP コマンドをリスニングしている Oracle Internet Directory リスナー / ディスパッチャ・プロセスに送信します。

OID リスナー / ディスパッチャは、その LDAP 要求を Oracle ディレクトリ・サーバーに送信し、サーバー・プロセスを作成します。サーバー・プロセスは、LDAP 操作要求を処理し、Oracle データベース・インスタンスに接続して、ディレクトリ・ストアにアクセスします。ディレクトリ・サーバーは、各操作に対して 1 つのサーバー・プロセスを生成することにより、クライアント要求を処理します。

マルチ・サーバー・プロセスによって、Oracle Internet Directory はマルチ・プロセッサ・システムを利用できます。作成されるサーバー・プロセス数は、構成パラメータ ORCLSERVERPROCS で決まります。デフォルトは 1 です。

構成パラメータ ORCLMAXCC に設定された数値に応じて、各サーバー・プロセスとデータベースとの間に必要な数の接続が生成されます。このパラメータのデフォルト値は 10 です。サーバー・プロセスは、Oracle Net Services を介してデータ・サーバーと通信します。Oracle Net Services リスナー / ディスパッチャは、Oracle9*i* データベース・サーバーに要求を中継します。

ディレクトリ・メタデータ

ディレクトリ・メタデータは、ディレクトリ・サーバーが実行中に LDAP 要求を処理するために使用する情報です。ディレクトリ・メタデータは、基礎となるデータ・リポジトリに格納されます。起動中に、ディレクトリ・サーバーはこの情報を読み取り、ローカル・メタデータ・キャッシュに格納します。ディレクトリ・サーバーは、実行中にこのキャッシュを使用し、受信する LDAP 操作要求を処理します。

ディレクトリ・サーバーのローカル・メタデータ・キャッシュには、次の種類のメタデータが格納されます。

- ディレクトリ・スキーマ

  ディレクトリ・サーバーによりサポートされるオブジェクト・クラス、属性、一致規則の定義。ディレクトリ・サーバーは、ディレクトリ・オブジェクトの作成および変更時にこの情報を使用します。ディレクトリ・オブジェクトとは、オブジェクト・クラスおよびそれに関連付けられた属性と一致規則の集合です。

- アクセス制御ポリシー・ポイント（ACP）

  ドメインにある情報へのアクセスを定義し、制御するためのディレクトリ管理ドメイン。ディレクトリ・サーバーは、特定の LDAP 操作をユーザーが実行できるかどうかを判断するときに ACP を使用します。

- ルート DSE エントリ

  ルート DSE（DSA 固有のエントリ）には、ディレクトリ・サーバー自体に関する情報を格納する多数の属性が入っています。これらの属性には次のような情報項目を含みます。

  - ネーミング・コンテキスト識別名
  - サブ・スキーマ・サブエントリ識別名
  - 上位参照（参照）識別名
  - Oracle Internet Directory 構成コンテナやレジストリ・コンテナのような特殊なエントリ識別名
  - 変更ログ・コンテナや変更ステータス・コンテナのような特殊なエントリ識別名
  - レプリケーション承諾コンテナの識別名

- 権限グループ

  アクセス制御ポリシーで使用できるグループ。

  ディレクトリ・スキーマは、標準の groupofuniquenames オブジェクト・クラスと groupofnames オブジェクト・クラスによってディレクトリ・グループ・オブジェクトをサポートします。これらのオブジェクト・クラスは、配布リストやメーリング・リストのようなグループに関する情報を格納します。

  Oracle Internet Directory は、orclprivilegegroup と呼ばれる補助オブジェクト・クラスによって、これらの標準グループ・オブジェクトを拡張します。このオブジェクト・クラスは、アクセス制御ポリシーで使用できる権限グループをサポートし、ユーザーのグループに対するアクセスの許可や拒否を柔軟に行えるようにします。ディレクトリ・サーバーはこの情報を次の場合に使用します。

  – 特定のユーザーに関してサブスクライブされた権限グループを検索するための LDAP バインド操作
  – 権限が付与されたグループに対するアクセスを許可または拒否するディレクティブがポリシーにあるかどうかのアクセス制御ポリシーの評価

  オブジェクト・クラスとグループ・エントリの関連付けまたは関連付け解除については、7-7 ページの「Oracle Directory Manager を使用したエントリの変更」または 7-11 ページの「例 : ldapmodify を使用したユーザー・エントリの変更」を参照してください。

- カタログ・エントリ

  基礎となるデータベースで索引付けされた属性に関する情報を入れる特別なエントリ。ディレクトリは、ディレクトリ検索操作中にこの情報を使用します。

- 共通エントリ

  ホスティングされた企業に関する情報を入れる特別なエントリ。ホスティングされた企業とは、別の企業からサービスを提供される企業のことをいいます。このエントリのメタデータには、ホスティングされた企業の識別名、ユーザー検索ベース、ニックネームなどの属性が入っています。詳細は、第 19 章「Oracle Identity Management レルムの配置」を参照してください。

- プラグイン・エントリ

  プラグイン・イベントをトリガーする操作の種類と、操作のどの時点でそのプラグインをトリガーするかに関する情報を入れる特別なエントリ。詳細は、第 45 章「Oracle Internet Directory プラグイン・フレームワーク」を参照してください。

- パスワード検証エントリ

  暗号タイプと検証属性タイプに関する情報を入れる特別なエントリ。詳細は、第 16 章「パスワード・ベリファイアのディレクトリ格納」を参照してください。

- パスワード・ポリシー・エントリ

  ユーザー・パスワード資格証明についてディレクトリ・サーバーにより施行されるポリシーに関する情報の入った特別なエントリ。ディレクトリ・サーバーは、パスワード・ポリシーを施行するために実行時にこの情報を使用します。

構成設定エントリ

各 Oracle ディレクトリ・サーバー・インスタンスの構成パラメータは、構成設定エントリ（configset）と呼ばれるエントリに格納されます。管理者が OID 制御ユーティリティを使用してサーバーのインスタンスを起動すると、その起動コマンドにこの構成設定エントリの 1 つへの参照が含まれ、その中の情報が使用されます。

Oracle ディレクトリ・サーバーは、デフォルトの構成設定エントリ（`configset0`）でインストールされているので、ディレクトリ・サーバーはすぐに実行できます。要件を満たすパラメータによって、カスタマイズされた構成設定エントリを作成できます。

構成設定エントリを表示、追加および変更するには、**Oracle Directory Manager** または該当するコマンドライン・ツールを使用します。

関連項目：

- 5-2 ページの「サーバーの構成設定エントリの管理」
- 構成設定エントリの属性のリストは、B-5 ページの「構成設定エントリのスキーマ要素」を参照してください。

例 : Oracle Internet Directory の動作

この例では、Oracle Internet Directory がどのように検索要求を処理するかを示します。

1. ユーザーまたはクライアントが検索要求を入力します。検索条件は、次の 1 つ以上のオプションによって決まります。

   - SSL: クライアントとサーバーは、SSL の暗号化と認証または SSL の暗号化のみを使用するセッションを確立できます。SSL が使用されていない場合、クライアントのメッセージは平文で送信されます。
   - ユーザーのタイプ : ユーザーは、特定のユーザーまたは匿名ユーザーのいずれかでディレクトリにシーク・アクセスできます。要求する機能の実行に必要な権限を持っているかどうかによって、2 つのタイプのいずれかでアクセスします。
   - フィルタ : ユーザーは、1 つ以上の検索フィルタを使用して検索条件を絞り込むことができます。検索フィルタには、ブール条件 and、or、not の他に、greater than、equal to、less than などの演算子を使用します。

2. ユーザーまたはクライアントが Oracle Directory Manager を使用してコマンドを発行すると、Oracle Directory Manager は Java ネイティブ・インタフェースで問合せ関数を起動し、次に Java ネイティブ・インタフェースが C API で関数を起動します。ユーザーまたはクライアントがコマンドライン・ツールを使用した場合は、そのツールが直接 C API で C 関数をコールします。
3. C API は、LDAP プロトコルを使用して、ディレクトリへの接続要求をディレクトリ・サーバー・インスタンスに送信します。
4. ディレクトリ・サーバーはユーザーを認証します。このプロセスはバインドと呼ばれます。ディレクトリ・サーバーは、アクセス制御リスト（ACL）もチェックして、そのユーザーが、要求した検索の実行を許可されているかどうかを検証します。
5. ディレクトリ・サーバーは、LDAP からの検索要求を Oracle Call Interface（OCI）および Oracle Net Services に変換し、Oracle9*i* データベースに送信します。
6. Oracle9*i* データベースは、情報を取得し、ディレクトリ・サーバー、次に C API、最後にクライアントと連鎖的に戻していきます。

分散ディレクトリ

オンライン・ディレクトリは論理的に集中管理されていますが、物理的には複数のサーバーに分散できます。この分散によって、サーバーが 1 つのみの場合に実行する必要のある作業が削減され、ディレクトリにより多くのエントリを格納できるようになります。

分散ディレクトリは、レプリケートまたはパーティション化できます。情報がレプリケートされると、同じネーミング・コンテキストが複数のサーバーに格納されます。情報がパーティション化されると、他と重複しない 1 つ以上のネーミング・コンテキストが各ディレクトリ・サーバーに格納されます。分散ディレクトリでは、情報の一部がパーティション化されたりレプリケートされる場合があります。

この項では、次の項目について説明します。

- ディレクトリ・レプリケーション
- ディレクトリ・パーティション化

ディレクトリ・レプリケーション

レプリケーションは、複数のディレクトリ・サーバーに同じネーミング・コンテキストをコピーし、管理するプロセスです。問合せの処理に複数のサーバーで備えることによってパフォーマンスを向上させ、シングル・ポイント障害に伴うリスクを排除して信頼性を向上させます。

レプリケーションには、完全レプリケーションと部分レプリケーションがあります。

完全レプリケーションでは、DIT 全体を別のノードに伝播します。

部分レプリケーションでは、DIT 全体ではなく 1 つ以上のサブツリーを別のノードに伝播します。

指定したネーミング・コンテキストのレプリケーションの対象となるディレクトリ・サーバーは、ディレクトリ・レプリケーション・グループ（DRG）と呼ばれるグループを形成します。DRG を構成するディレクトリ・サーバー間の関係は、各ノード上でレプリケーション承諾と呼ばれる特別なディレクトリ・エントリによって表されます。

サーバー内に格納されているネーミング・コンテキストの各コピーは、レプリカと呼ばれます。レプリカは、読取り専用または更新可能（あるいはその両方）です。更新可能レプリカを保持するサーバーは、サプライヤと呼ばれます。このレプリカを変更すると、コンシューマと呼ばれる他のサーバーに伝播されます。

ディレクトリ・レプリケーション・グループは、単一マスター、マルチマスター、ファンアウトのいずれかです。

単一マスター・レプリケーション・グループには、1 つ以上のコンシューマに変更をレプリケートするサプライヤが 1 つのみ存在します。更新できるのはサプライヤのみで、コンシューマは読取り専用です。

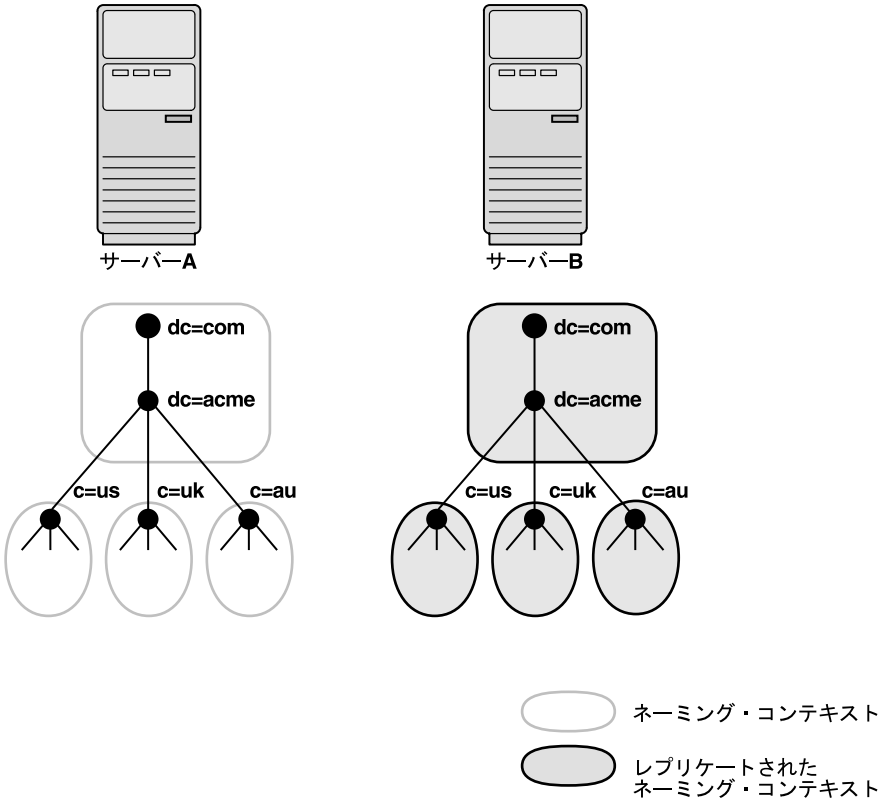
マルチマスター・レプリケーションは、peer-to-peer レプリケーションまたは *n*-way レプリケーションとも呼ばれ、同等に機能する複数のサイトが、レプリケートされたデータのグループを管理できるようにします。マルチマスター・レプリケーション環境では、各ノードはサプライヤ・ノードであると同時にコンシューマ・ノードであり、各ノードでディレクトリ全体がレプリケートされます。

ファンアウト・レプリケーション・グループは、point-to-point レプリケーション・グループとも呼ばれ、コンシューマに直接レプリケートするサプライヤを持っています。そのコンシューマは、1 つ以上の別のコンシューマにレプリケートできます。レプリケーションには、完全レプリケーションと部分レプリケーションがあります。

ディレクトリ・レプリケーション・グループの場合、ノード間でデータを転送するプロトコルは、Oracle9*i* Advanced Replication または LDAP のいずれかに基づきます。

図 2-6 に、レプリケート・ディレクトリを示します。

図 2-6 レプリケート・ディレクトリ



注意： このリリースの Oracle Internet Directory では、ネーミング・コンテキスト・レベルでのレプリケーションが可能です。ネーミング・コンテキストの一部のレプリケーションはサポートされていません。

また、ディレクトリ・レプリケーションのインターネット規格はまだありませんが、IETF がこれに類する規格を開発中です。Oracle Internet Directory のレプリケーションは、ディレクトリ変更情報を**変更ログ**に記録する IETF 規格案に準拠しています。Oracle Internet Directory レプリカ間でこれらの変更ログを送信するためのトランスポートとして標準 LDAP を使用できます。

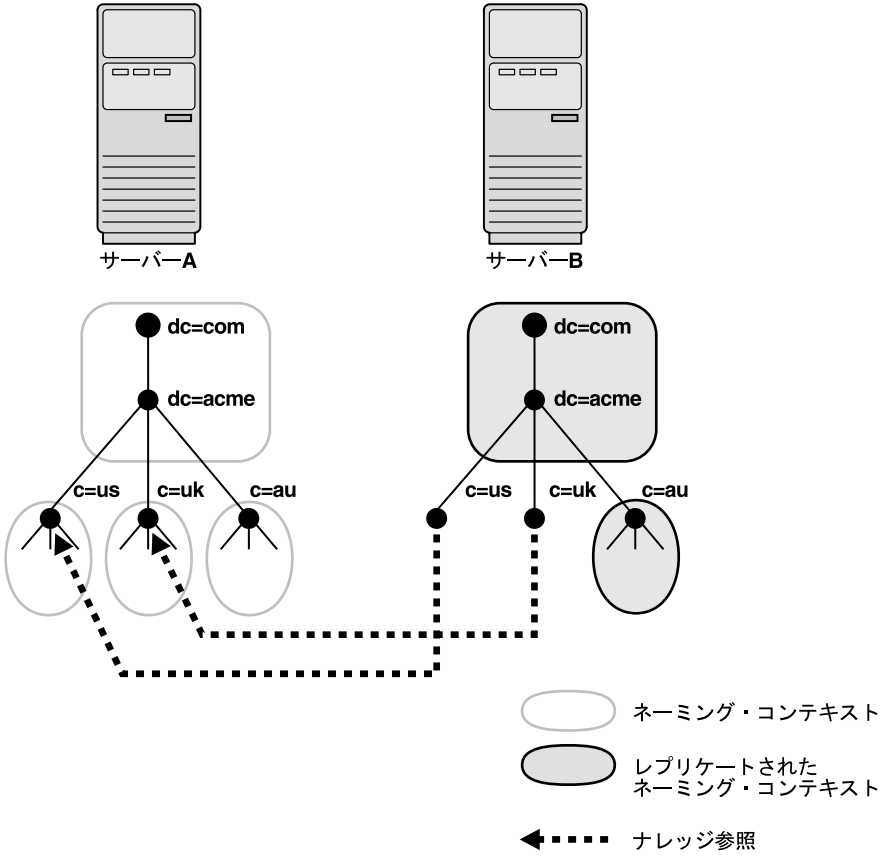
関連項目： レプリケーションの詳細は、第 24 章「ディレクトリ・レプリケーションの概要」を参照してください。これには、Oracle9*i* Advanced Replication のアーキテクチャ、LDAP ベースのレプリケーション、変更ログの削除、競合の解決、レプリケーションのプロセスが含まれています。

ディレクトリ・パーティション化

パーティション化は、ディレクトリ情報を分散するもう 1 つの方法です。パーティション化では、他と重複しないネーミング・コンテキストが 1 つ以上、各ディレクトリ・サーバーに格納されます。

図 2-7 に、異なるサーバーにいくつかのネーミング・コンテキストが常駐している、パーティション化されたディレクトリを示します。

図 2-7 パーティション化されたディレクトリ



2-24 ページの図 2-7 では、サーバー A に次の 4 つのネーミング・コンテキストが常駐しています。

- `dc=acme,dc=com`
- `c=us,dc=acme,dc=com`
- `c=uk,dc=acme,dc=com`
- `c=au,dc=acme,dc=com`

サーバー A にある次の 2 つのネーミング・コンテキストは、サーバー B にレプリケートされています。

- `dc=acme,dc=com`
- `c=au,dc=acme,dc=com`

ディレクトリは、サーバー B に要求した情報がサーバー A に常駐している場合に、1 つ以上の**ナレッジ参照**を使用して情報を検索します。次にディレクトリは、この情報を**参照**のフォームでクライアントに渡します。

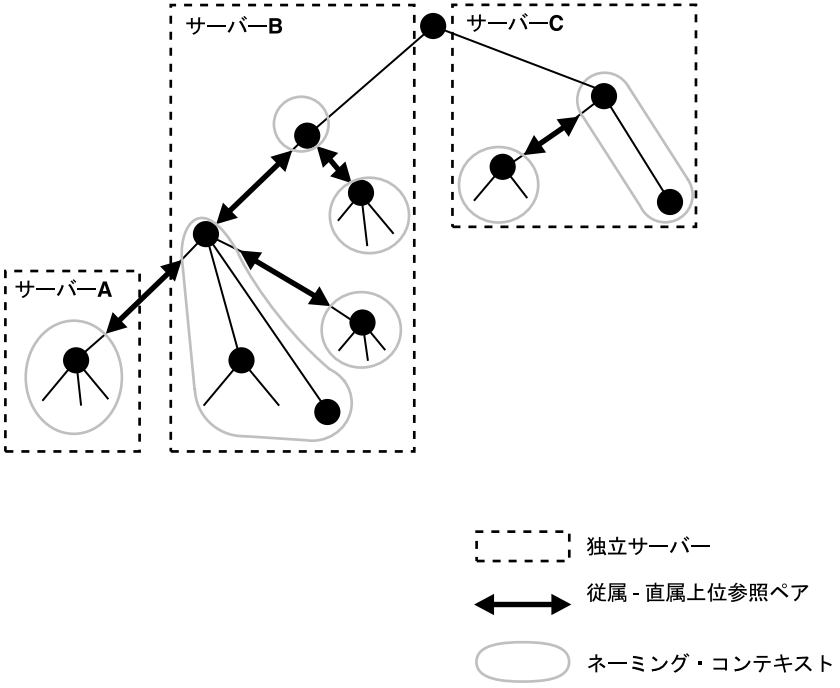
ナレッジ参照と参照

ナレッジ参照は、別のパーティションに保持されている様々なネーミング・コンテキストの名前とアドレスを提供します。たとえば、2-24 ページの図 2-7 で、サーバー B は、ナレッジ参照を使用して、サーバー A 上のネーミング・コンテキスト `c=us` と `c=uk` を指し示します。サーバー B がサーバー A に常駐している情報の要求を受けると、サーバー B は 1 つ以上のサーバー A への参照を戻します。クライアントはこれらの参照を使用してサーバー A と通信できます。

一般的に、各ディレクトリ・サーバーには、上位ナレッジ参照と従属ナレッジ参照の両方があります。上位ナレッジ参照では、ディレクトリ情報ツリー内でルートに向かう上位方向が指し示されます。この参照は、パーティション化されたネーミング・コンテキストをその親に結び付けます。従属ナレッジ参照では、ディレクトリ情報ツリー内で他のパーティションへの下位方向が指し示されます。

たとえば、2-26 ページの図 2-8 では、サーバー B に 4 つのネーミング・コンテキストがあり、そのうちの 2 つは他のネーミング・コンテキストの上位にあります。この 2 つの上位ネーミング・コンテキストは、従属ナレッジ参照を使用して、その従属ネーミング・コンテキストを指し示しています。逆に、サーバー A 上のネーミング・コンテキストは、サーバー B に常駐している直属の上位ネーミング・コンテキストを持っています。したがって、サーバー A は、上位ナレッジ参照を使用してサーバー B 上の親を指し示しています。

図 2-8 ナレッジ参照を使用したネーミング・コンテキストへの指示



当然のことですが、ディレクトリ情報ツリーの最上位で始まるネーミング・コンテキストは、上位ネーミング・コンテキストへのナレッジ参照を持つことはできません。

注意： ナレッジ参照の有効性を実施するためのインターネット規格は現在ありません。また、このことは、Oracle Internet Directory でも同様です。エンタープライズ・ネットワーク内で複数ナレッジ参照間の一貫性を確保する責任は管理者にあります。

ナレッジ参照エントリの管理権限は、スキーマやアクセス制御などの他の重要な権限管理機能と同様に制限することをお薦めします。

参照には次の 2 つの種類があります。

- スマート参照

  これらは、ナレッジ参照エントリが検索の有効範囲内にあるときにクライアントに戻されます。スマート・ナレッジ参照は、要求された情報が格納されているサーバーをクライアントに示します。

たとえば、次のような場合があります。

- サーバー A には、ネーミング・コンテキスト ou=server development,c=us,o=acme があり、さらにサーバー B へのナレッジ参照があります。
- サーバー B には、ネーミング・コンテキスト ou=sales,c=us,o=acme があります。

ou=sales,c=us,o=acme にある情報の要求をクライアントがサーバー A に送信すると、サーバー A はサーバー B への参照をユーザーに提供します。

- デフォルト参照

  デフォルト参照は、ベース・オブジェクトがディレクトリになく、さらに操作が別のサーバー上のネーミング・コンテキストで実行されたときに戻されます。デフォルト参照では、通常、ディレクトリ・パーティション化配置に関するより多くの情報を持つサーバーにクライアントを送信します。

  たとえば、サーバー A が次のものを保持するとします。

  - ネーミング・コンテキスト c=us,o=acme
  - ディレクトリ・パーティション化配置全般についてより多くのナレッジを持つサーバー PQR へのナレッジ参照

  クライアントが c=uk,o=acme にある情報を要求したとします。サーバー A は、c=uk,o=acme ネーミング・コンテキストを持っていないことを認識すると、そのクライアントにサーバー PQR への参照を提供します。クライアントは、要求したネーミング・コンテキストを保持しているサーバーをそこから検索できます。

関連項目： 7-16 ページの「ナレッジ参照と参照の管理」

Oracle Delegated Administration Services と Oracle Internet Directory セルフ・サービス・コンソール

Oracle Delegated Administration Services は、ユーザーのかわりにディレクトリ操作を実行するために事前定義された Web ベースのユニットのセットです。この一連のサービスは、ディレクトリ管理者が他の管理者やエンド・ユーザーに対して特定の機能を委任できるようにすることによって、ディレクトリ管理の日常的な作業からディレクトリ管理者を解放します。この一連のサービスによって、ディレクトリ対応アプリケーションに必要な大部分の機能が提供されます。たとえば、ユーザー・エントリの作成、グループ・エントリの作成、エントリの検索、ユーザー・パスワードやその他の従業員固有のデータの変更などがあります。

Oracle Delegated Administration Services を使用して、ディレクトリ内のアプリケーション・データを管理するための独自のツールを開発できます。また、Oracle Internet Directory セルフ・サービス・コンソールを使用することもできます。これは、Oracle Internet Directory ですぐに使用できる Oracle Delegated Administration Services に基づいたツールです。このコンソールは、委任管理を提供するためにいくつかの Oracle コンポーネントで使用されます。

関連項目：

- 第 30 章「Oracle Delegated Administration Services」
- 第 31 章「Oracle Internet Directory セルフ・サービス・コンソール」

Oracle Directory Integration and Provisioning Platform

Oracle Directory Integration and Provisioning Platform によって、企業ではアプリケーションやその他のディレクトリを Oracle Internet Directory に統合できます。これは、Oracle Internet Directory のデータとエンタープライズ・アプリケーションや接続ディレクトリのデータとの一貫性を維持するために必要なインタフェースとインフラストラクチャのすべてを提供します。また、サード・パーティ・ベンダーや開発者にとっては、独自の接続エージェントの開発と配置が容易になります。

たとえば、企業では人事管理データベースの従業員レコードと Oracle Internet Directory との同期が必要な場合があります。また、変更が Oracle Internet Directory に適用されるたびに通知が必要な LDAP 対応のアプリケーション（OracleAS Portal など）が配置されている可能性もあります。

統合の特性に基づいて、Oracle Directory Integration and Provisioning Platform は 2 つの異なるサービスを提供します。

- 同期化統合サービスは、接続ディレクトリと中央の Oracle Internet Directory との一貫性を維持します。
- プロビジョニング統合サービスは、ユーザーやグループなど、エントリに対する重要な変更を反映するために、ターゲット・アプリケーションに通知を送信します。

関連項目：「Oracle Directory Integration and Provisioning Platform」

Oracle Internet Directory と Oracle Identity Management

認証管理とは、組織でネットワーク・エンティティのセキュリティ・ライフサイクル全体を管理するプロセスです。Oracle Internet Directory は、Oracle Identity Management インフラストラクチャの重要な要素であり、すべてのアプリケーションにわたってセキュリティ管理を簡素化できます。これを行うには、Oracle Internet Directory と他の Oracle Identity Management コンポーネントとの共有インスタンスに対して、複数の Oracle コンポーネントを配置します。それには、Oracle Internet Directory 配置が企業のセキュリティ要件を満たすように慎重に計画を策定する必要があります。

この項では、次の項目について説明します。

認証管理の概要

認証管理とは、最も一般的には、組織のアプリケーション・ユーザーの管理です。セキュリティ・ライフサイクルの手順には、アカウント作成、一時停止、権限変更、アカウント削除があります。管理対象エンティティには、デバイス、プロセス、アプリケーション、ネットワーク環境で対話するために必要なその他のものが含まれます。組織外のユーザー、顧客、取引先、Web サービスなども含まれることがあります。

認証管理は、管理コストを削減しながら、同時にセキュリティを向上できるため、IT 配置にとって重要です。

Oracle Identity Management インフラストラクチャによって、企業内のすべてのエンタープライズ ID と各種アプリケーションに対する各 ID のアクセスを集中的かつ安全に管理できます。認証管理は、次のタスクで構成されています。

- 企業全体で単一のコンソールを使用したエンタープライズ ID の作成および ID の共有プロパティの管理
- エンタープライズ ID のグループの作成
- 企業で利用できる各種サービスでのこれらの ID のプロビジョニング。次のサービスが含まれます。
  - アカウント作成
  - アカウント一時停止
  - アカウント削除
- これらの ID に関連付けられたポリシーの管理。次のポリシーが含まれます。
  - 認可ポリシー
  - 認証ポリシー
  - 既存 ID に委任された権限

Oracle Identity Management インフラストラクチャの概要

Oracle Identity Management は、分散セキュリティのために Oracle 製品が利用する統合インフラストラクチャです。これは、他の Oracle 製品同様、Oracle Application Server Infrastructure の一部です。2-30 ページの図 2-9 に、Oracle Identity Management インフラストラクチャのコンポーネントおよびこれらを利用する各種の Oracle 製品およびサード・パーティ製品を示します。

図 2-9 Oracle Identity Management インフラストラクチャおよび他のコンポーネント

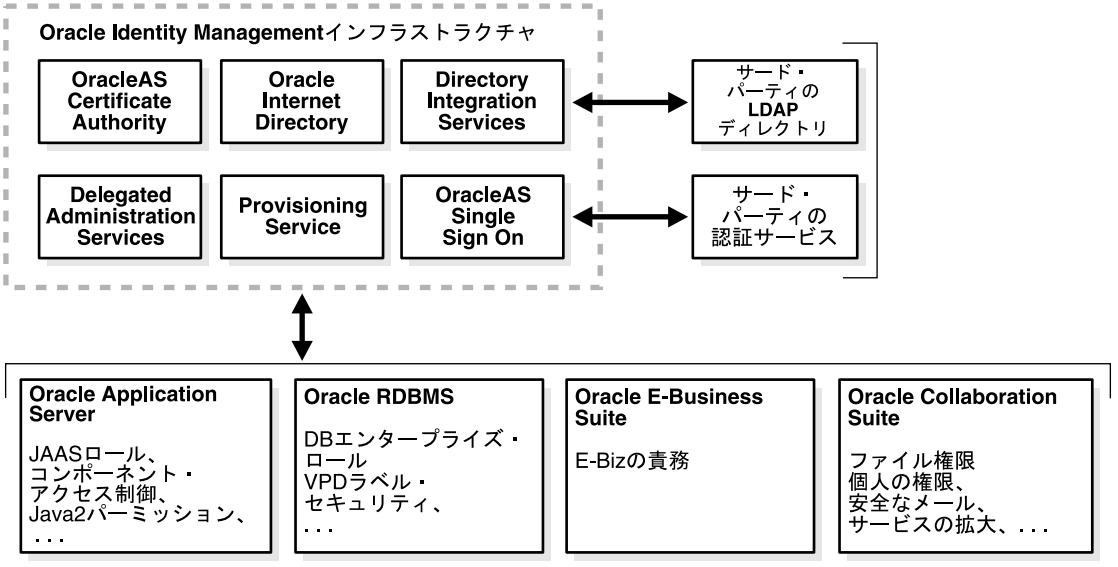


図 2-9 に示すとおり、Oracle Identity Management インフラストラクチャは次のコンポーネントと機能を含んでいます。

- Oracle Internet Directory: Oracle9*i* データベース・サーバーに実装されたスケーラブルで堅牢な LDAP V3 準拠のディレクトリ・サービス。
- Oracle Directory Integration and Provisioning Platform: Oracle Internet Directory、他のディレクトリ、ユーザー・リポジトリを同期させ、Oracle コンポーネントやアプリケーションとサード・パーティのアプリケーションで、標準インタフェースを使用した自動プロビジョニング・サービスを可能にします。
- Oracle Delegated Administration Services: ユーザーおよびアプリケーション管理者による、信頼できるプロキシ・ベースのディレクトリ情報管理を提供します。

- Oracle Application Server Single Sign-On: Oracle アプリケーションとサード・パーティの Web アプリケーションへのシングル・サインオン・アクセスを提供します。
- Oracle Application Server Certificate Authority: 強力な認証方式をサポートする X.509 V3 PKI 証明書を生成し、公開します。

Oracle Identity Management は、Oracle 製品のためのエンタープライズ・インフラストラクチャを提供するために設計されたものですが、ユーザー作成アプリケーションおよびサード・パーティのエンタープライズ・アプリケーションのために、汎用の認証管理ソリューションとしても使用できます。サード・パーティのアプリケーション、ハードウェア、およびネットワーク・オペレーティング・システムのために、堅牢でスケーラブルな企業全体の認証管理プラットフォームを提供します。カスタム・アプリケーションは、一連のドキュメント、サポートされるサービス、API により Oracle Identity Management を活用できます。次のようなサービスがあります。

- Oracle Internet Directory は、C、Java および PL/SQL のための LDAP API を提供します。他の LDAP SDK と互換性があります。
- Oracle Delegated Administration Services は、サード・パーティのアプリケーションをサポートするようにカスタマイズできるコア・セルフ・サービス・コンソールを提供します。また、ディレクトリ・データを操作するカスタマイズされた管理インタフェースを構築するための多数のサービスも提供します。
- Oracle Directory Synchronization Service は、Oracle Internet Directory とサード・パーティ・ディレクトリおよび他のユーザー・リポジトリとの同期のためのカスタム・ソリューションの開発と配置を容易にします。
- Oracle Directory Provisioning Integration Service は、サード・パーティのアプリケーションをプロビジョニングし、Oracle 環境を他のプロビジョニング・システムと統合できます。
- Oracle Application Server Single Sign-On は、他の Oracle Web アプリケーションとシングル・サインオン・セッションを共有するパートナ・アプリケーションを開発および配置するための API を提供します。
- JAAS 規格の Oracle の実装である JAZN によって、Web 用に開発されたアプリケーションで、Oracle の J2EE 環境を使用して Oracle Identity Management インフラストラクチャを認証と認可に活用できます。

また、オラクル社はサード・パーティのアプリケーション・ベンダーと共同で、それらのアプリケーションが Oracle Identity Management を直接活用できるようにしています。

> **関連項目：** Oracle Identity Management インフラストラクチャの詳細は、『Oracle Identity Management 概要および配置プランニング・ガイド』を参照してください。

認証管理レルム

認証管理レルムは、ある認証管理ポリシーが配置により定義され、施行されるときの企業内での範囲を定義します。次の要素で構成されます。

- 有効範囲の定義されたエンタープライズ ID の集合 − たとえば、US ドメインのすべての従業員
- これらの ID に関連付けられた認証管理ポリシーの集合。認証管理ポリシーの例としては、すべてのユーザー・パスワードに少なくとも 1 文字の英数字を含む必要があることなどがあります。
- グループの集合、すなわち ID の集合 − 認証管理ポリシーの設定を簡素化します

同じ Oracle Identity Management インフラストラクチャ内で複数の認証管理レルムを定義できます。したがって、ユーザーの集団を区別し、各レルムで異なる認証管理ポリシー（パスワード・ポリシー、ネーミング・ポリシー、自己変更ポリシーなど）を施行できます。

各認証管理レルムには、他のレルムと区別するために固有の名前が付けられます。また、レルムに対して完全な管理制御を行うために、レルム固有の管理者も決められます。

デフォルト認証管理レルム

すべての Oracle コンポーネントが機能するには、認証管理レルムが必要です。Oracle Internet Directory のインストール中に作成される特別なレルムは、デフォルト認証管理レルムと呼ばれます。これは、レルムの名前が指定されていない場合に、Oracle コンポーネントが、ユーザー、グループおよび関連付けられたポリシーを検索する場所です。

デフォルト認証管理レルムは、ディレクトリに 1 つのみです。配置に、複数の認証管理レルムが必要である場合、その 1 つをデフォルトとして選択する必要があります。

認証管理ポリシー

Oracle Identity Management インフラストラクチャは、一連の柔軟な管理ポリシーをサポートします。これは、次の要素で構成されます。

- ディレクトリ構造ポリシーとネーミング・ポリシー。これにより次のことが可能になります。
  - 配置に合せて Oracle Internet Directory のディレクトリ構造をカスタマイズ
  - 各種 ID が置かれる場所と、それを一意に識別する方法を指定
- Oracle Identity Management インフラストラクチャによりサポートされる認証方式とプロトコルを指定できる認証ポリシー
- 権限のある特定のサービスへのアクセスと必要に応じて管理委任を制御できる認証管理認可

注意： Oracle Internet Directory リリース 9.0.2 で使用した「サブスクライバ」は、「認証管理レルム」と同じ用語です。

リソース情報

Oracle コンポーネントの中には、ユーザーの要求を実行するために、様々なリポジトリおよびサービスからデータを収集するものがあります。データを収集するために、これらのコンポーネントでは次の情報が必要です。

- データの収集元となるリソースのタイプを識別する情報。たとえば、Oracle データベースなどです。これは、リソース・タイプ情報と呼ばれます。
- リソースに対するユーザーの接続および認証に関する情報。これは、リソース・アクセス情報と呼ばれます。

この項では、次の項目について説明します。

リソース・タイプ情報

ユーザーの要求を実行するためにアプリケーションが使用するリソースの情報をリソース・タイプ情報と呼びます。リソース・タイプには、Oracle9*i* データベース・サーバーや交換可能な Java Database Connectivity データ・ソースなどがあります。リソース・タイプ情報には、ユーザーの認証に使用するクラス、ユーザー識別子、パスワードなどの項目が含まれます。

Oracle Internet Directory セルフ・サービス・コンソールを使用して、リソース・タイプ情報を指定します。

リソース・アクセス情報

データベースに対するユーザーの接続および認証に関する情報を、リソース・アクセス情報と呼びます。この情報は、様々な Oracle コンポーネントで取得および共有できるリソース・アクセス記述子（RAD）と呼ばれるエントリに格納されます。

たとえば、販売レポートに関するユーザーの要求を実行するために、Oracle Application Server Reports Services は複数のデータベースを問い合せます。データベースへの問合せでは、次の処理が実行されます。

1. RAD からの必要な接続情報の取得
2. 取得した情報を使用した、データベースへの接続およびデータを要求しているユーザーの認証

この処理が終了すると、レポートがコンパイルされます。

Oracle Internet Directory セルフ・サービス・コンソールを使用して、リソース・アクセス情報を指定します。各ユーザーに対してリソース・アクセス情報を個別に指定したり、すべてのユーザーに対して共通に指定することもできます。後者の場合、指定されたアプリケーションに接続するすべてのユーザーは、デフォルトで同じ情報を使用して必要なデータベースに接続します。たとえば、各ユーザーが一意のシングル・サインオン・ユーザー名でアプリケーション内に定義されている場合など、アプリケーションに独自の統合アカウント管理がある場合は、デフォルトのリソース・アクセス情報を定義することをお薦めします。

DIT 内のリソース情報の位置

図 2-10 に、DIT 内のリソース情報の位置を示します。

図 2-10 DIT 内のリソース・アクセス情報およびリソース・タイプ情報の配置

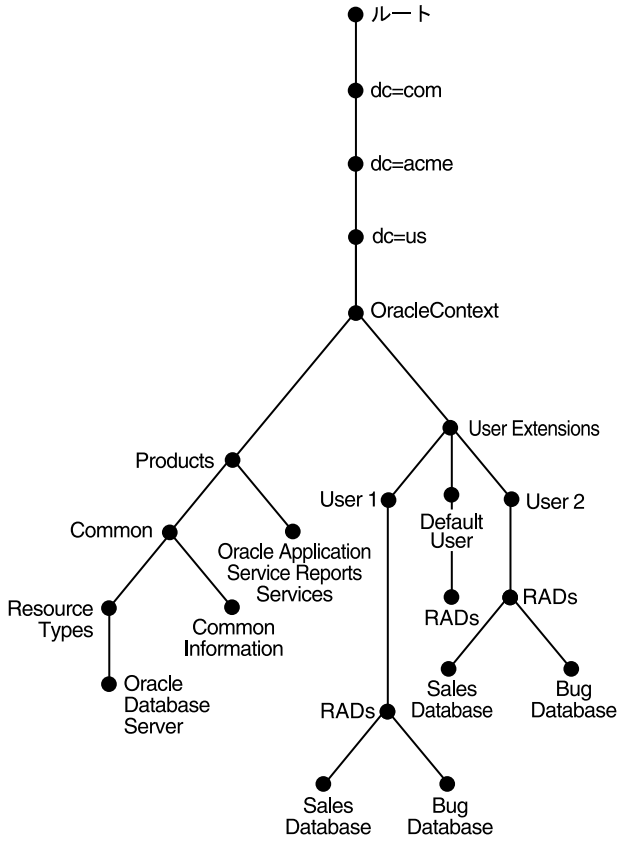


図 2-10 に示すとおり、リソース・アクセス情報およびリソース・タイプ情報は、Oracle コンテキストに格納されます。

各ユーザーのリソース・アクセス情報は、Oracle コンテキスト内の cn=User Extensions ノードに格納されます。この例では、cn=User Extensions ノードには、デフォルトのユーザーおよび特定のユーザーの両方のリソース・アクセス情報が含まれています。後者の場合、リソース・アクセス情報には、Sales データベースおよび Bug データベースの両方へのアクセスで必要な情報が含まれます。

各アプリケーションのリソース・アクセス情報は、アプリケーション名で識別されるオブジェクトに格納されます。たとえば、cn=Oracle Application Server Reports Services、cn=Products、cn=Oracle Context、dc=us、dc=acme、dc=com などです。これは、その製品に固有のユーザー情報です。

リソース・タイプ情報は、コンテナ cn=resource types、cn=common、cn=products、cn=Oracle Context に格納されます。

関連項目：

- エンド・ユーザーによるリソース・アクセス情報の指定手順については、31-9 ページの「リソース・アクセス情報の管理」を参照してください。
- 管理者によるユーザー・エントリ作成時のリソース・アクセス情報の指定手順については、31-16 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用したユーザー・エントリの作成」を参照してください。
- すべてのユーザーが自動的に継承する使用済リソースを管理者が定義する一般的な手順については、31-24 ページの「デフォルトのリソース・アクセス情報の構成」を参照してください。
- 管理者によるリソース・タイプの指定手順については、31-24 ページの「リソース・タイプ情報の構成」を参照してください。
- B-31 ページの「プラグインのスキーマ要素」
- 『Oracle Application Server Reports Services レポート Web 公開ガイド』

3

事前に実行するタスクと情報

Oracle Internet Directory を構成して使用する前に、この章で説明するタスクを実行する必要があります。この章では、様々な Oracle Internet Directory コンポーネントのログ・ファイルの位置のリストも示します。

次の項目について説明します。

タスク 1: OID モニターの起動

サーバーの起動と停止を行うコマンドを処理するには、OID モニターが実行中であることが必要です。

関連項目： OID モニターの開始方法と停止方法は、A-4 ページの「OID モニター（oidmon）構文」を参照してください。

タスク 2: サーバー・インスタンスの起動

OID モニターの実行後は、Oracle Enterprise Manager Application Server Control または OID 制御ユーティリティでサーバー・インスタンスを起動します。

関連項目：

- 10-23 ページの「Oracle Enterprise Manager Application Server Control を使用した新規ディレクトリ・サーバー・インスタンスの起動」
- A-4 ページの「Oracle Internet Directory サーバーの起動、停止、再起動および監視」
- A-9 ページの「ディレクトリ・サーバー・インスタンスの起動に関するトラブルシューティング」

注意： ディレクトリ・サーバーが同じコンピュータ上にある場合は、複数のインスタンスを実行できます。たとえば、1 つのインスタンスを SSL モードで実行し、別のインスタンスを Non-SSL モードで実行できます。

タスク 3: デフォルトのセキュリティ構成の再設定

ご使用の環境に合わせるには、デフォルトのセキュリティ構成をカスタマイズする必要があります。表 3-1 に、カスタマイズで必要なタスクとその説明を示します。

表 3-1 デフォルトのセキュリティ構成を再設定するためのタスク

タスクの領域	説明
subSchemaSubEntry サブエントリとその子エントリの保護	ディレクトリに関する情報は、サブエントリ subSchemaSubEntry とその子エントリに格納されます。オラクル社では、これらのオブジェクトへのアクセスを制御することをお薦めします。
エントリへのアクセスの確立	ディレクトリ・エントリをロードすると、ディレクトリ・エントリの階層が作成されます。このため、次の項目を設定する必要があります。 ■ この階層にエントリをロードするための権限 ■ ディレクトリ・エントリに対する読取り、変更および書込みの各アクセス権限を必要とするクライアントを対象としたディレクトリ・アクセス権限
デフォルト・アクセス・ポリシーの変更	Oracle Internet Directory は、第 17 章「Oracle テクノロジ配置のための権限の委任」で説明する、デフォルトのセキュリティ構成でインストールされます。ディレクトリの使用を開始する前に、使用する環境に合せてこのデフォルトの構成を変更し、各ユーザーが適切な認可を確実に持つようにすることができます。
デフォルト・パスワード・ポリシーの変更	パスワード・ポリシーとは、パスワードの使用方法を管理する規則のセットです。Oracle Internet Directory は、デフォルト・パスワード・ポリシーとともにインストールされます。これは、環境に合せて変更できます。

関連項目：

- Oracle Internet Directory のセキュリティ機能と Oracle Internet Directory を使用する Oracle コンポーネントのデフォルト DIT の概要は、第 2 章「ディレクトリの概念およびアーキテクチャ」を参照してください。
- アクセス制御のオプションの説明およびセキュリティの設定方法は、第 14 章「ディレクトリ・アクセス制御」を参照してください。
- Oracle コンテキスト・スキーマの詳細は、第 19 章「Oracle Identity Management レルムの配置」を参照してください。
- デフォルト・パスワード・ポリシーの詳細は、15-2 ページの「デフォルトのパスワード・ポリシー」を参照してください。

注意： Oracle コンテキストでデフォルト ACL を変更する場合は注意が必要です。変更により、ご使用の環境内で Oracle コンポーネントのセキュリティが無効になることがあります。Oracle コンテキストでデフォルト ACL を安全に変更できるかどうかの詳細は、各コンポーネントのドキュメントを参照してください。

タスク 4: データベースのデフォルト・パスワードの再設定

Oracle Internet Directory は、Oracle データベースへの接続時にパスワードを使用します。Oracle Internet Directory が使用するデフォルトのパスワードは、インストール時に Oracle Application Server 管理者（ias_admin）に対して指定されたパスワードと同じです。OID データベース・パスワード・ユーティリティを使用すると、このパスワードを変更できます。

関連項目： 構文と使用方法は、A-129 ページの「OID データベース・パスワード・ユーティリティ（oidpasswd）構文」を参照してください。

タスク 5: OID データベース統計収集ツールの実行

バルク・ロード・ツール（`bulkload.sh`）以外の方法でデータをディレクトリにロードする場合は、ロード後に OID データベース統計収集ツールを実行する必要があります。Oracle のオプティマイザが LDAP 操作に対応する問合せについて最適の実行計画を選択するには、統計収集が必要です。OID データベース統計収集ツールは、OID デーモンを停止せずに必要に応じて実行できます。

注意： Windows オペレーティング・システムでシェル・スクリプト・ツールを実行するには、次のいずれかの UNIX エミュレーション・ユーティリティが必要です。

- Cygwin 1.3.2.2-1 以上
  サイト：`http://sources.redhat.com`
- MKS Toolkit 6.1
  サイト：`http://www.datafocus.com/`

関連項目： A-131 ページの「OID データベース統計収集ツール（oidstats.sh）の構文」

ログ・ファイルの位置

Oracle Internet Directory の各コンポーネントは、ログ情報とトレース情報を *ORACLE_HOME* 環境のログ・ファイルに出力します。表 3-2 に、各コンポーネントと対応するログ・ファイルの位置を示します。

表 3-2 ログ・ファイルの位置

コンポーネント	ログ・ファイル名
バルク・ローダー（bulkload.sh）	`$ORACLE_HOME/ldap/log/install.log`
カタログ管理ツール（catalog.sh）	`$ORACLE_HOME/ldap/log/catalog.log`
ディレクトリ統合エージェント	`$ORACLE_HOME/ldap/odi/log/`*`AgentName`*`.err`（*`AgentName`* にはエージェント名が入ります）
Oracle Directory Integration and Provisioning Server（odisrv）	`$ORACLE_HOME/ldap/log/odisrv`*`XX`*`.log`（*`XX`* には Oracle Directory Integration and Provisioning Server インスタンス番号が入ります）
ディレクトリ・レプリケーション・サーバー（oidrepld）	`$ORACLE_HOME/ldap/log/oidrepld00.log`
ディレクトリ・サーバー（oidldapd）	`$ORACLE_HOME/ldap/log/oidldapdXXs`*`pid`*`.log`（*`pid`* にはサーバー・プロセス識別子が入ります） `$ORACLE_HOME/ldap/log/oidstack<instance_identifier><dispatcher | server><PID>.log` **注意：** oidstack ログ・ファイルは、SIGSEGV/SIGBUS 追跡に関係します。また、ディレクトリ・インスタンスの起動時に空ファイルがこの名前で作成されますが、無視できます。
LDAP ディスパッチャ（oidldapd）	`$ORACLE_HOME/ldap/log/oidldapd`*`XX`*`.log`（*`XX`* にはサーバー・インスタンス番号が入ります）
OID モニター（oidmon）	`$ORACLE_HOME/ldap/log/oidmon.log`
レプリケーション設定（ldaprepl.sh）	`$ORACLE_HOME/ldap/admin/LOGS/ldaprepl.log`

4

ディレクトリ管理ツール

この章では、Oracle Internet Directory の様々な管理ツールについて説明します。Oracle Directory Manager と呼ばれるオンライン管理ツールの起動方法とナビゲート方法、およびこのツールでディレクトリ・サーバーに接続する方法を説明します。また、LDAP、バルクおよびカタログの各操作に関するコマンドライン・ツールについても説明します。

この章では、次の項目について説明します。

- Oracle Directory Manager の使用方法
- コマンドラインツールの使用方法
- 定期的な管理タスクの一覧

Oracle Delegated Administration Services は、ユーザーのかわりにディレクトリ操作を実行するために事前定義された Web ベースのユニットのセットであり、これもディレクトリ管理に利用できます。これにより、ディレクトリ管理者は他の管理者やエンド・ユーザーに対して特定の機能を委任でき、ディレクトリ管理の日常的な作業から解放されます。たとえば、エンド・ユーザーが管理者の介入を必要とせずに自分の個人プロファイル情報（Oracle Application Server Single Sign-On パスワードなど）を変更できるようにするために使用できます。

Oracle Internet Directory セルフ・サービス・コンソールは、Oracle Delegated Administration Services を使用して作成されたツールの 1 つです。このすぐに使用可能なアプリケーションによって、委任された管理者やエンド・ユーザーがディレクトリのデータを管理するための単一のグラフィカル・インタフェースが提供されます。

関連項目：

- 第 30 章「Oracle Delegated Administration Services」
- 第 31 章「Oracle Internet Directory セルフ・サービス・コンソール」

Oracle Directory Manager の使用方法

Oracle Directory Manager は、Oracle Internet Directory を管理するための Java ベースのツールです。この項では、その基本機能のいくつかを説明します。各機能固有の詳細は、このマニュアルの中で、各種タスクの実行方法を説明している項に記載されています。

この項では、次の項目について説明します。

- Oracle Directory Manager の起動
- Oracle Directory Manager を使用したディレクトリ・サーバーへの接続
- Oracle Directory Manager のナビゲート
- Oracle Directory Manager を使用した追加のディレクトリ・サーバーへの接続
- Oracle Directory Manager を使用したディレクトリ・サーバーからの切断
- Oracle Directory Manager を使用した管理タスクの実行

注意： Oracle Directory Manager は、Oracle Internet Directory 以外の LDAP ディレクトリの管理には使用できません。

Oracle Directory Manager の起動

Oracle Directory Manager の起動前に、ディレクトリ・サーバー・インスタンスを実行しておく必要があります。

関連項目：

- サーバー・インスタンスの起動方法は、第 3 章「事前に実行するタスクと情報」を参照してください。
- ディレクトリ・サーバー・インスタンスの概念の説明は、2-13 ページの「Oracle Internet Directory のアーキテクチャ」を参照してください。

Oracle Directory Manager を起動するには、オペレーティング・システムごとに次の説明に従ってください。

オペレーティング・システム	参照先
Windows NT	「スタート」メニューから、「プログラム」>「*ORACLE_HOME*」>「Integrated Management」>「Oracle Directory Manager」をクリックします。
UNIX	パスを設定していない場合は、`$ORACLE_HOME/bin` に移動します。 コマンド・プロンプトで次のコマンドを入力します。 `oidadmin`

初めて Oracle Directory Manager を起動すると、サーバーに接続する必要があることを知らせるアラートが表示されます。「OK」をクリックします。「ディレクトリ・サーバーの接続」ダイアログ・ボックスが表示されます。

Oracle Directory Manager を使用したディレクトリ・サーバーへの接続

ディレクトリ・サーバーへ接続する手順は、次のとおりです。

1. 「ディレクトリ・サーバーの接続」ダイアログ・ボックスに、使用可能なサーバーの名前とポート番号を入力します。

   デフォルト・ポートは 389 です。ポートは必要に応じて変更できます。ただし、Oracle ディレクトリ・サーバーをデフォルトのポート以外で実行する場合は、そのサーバーを使用するすべてのクライアントに、正しいポートを必ず通知してください。

   「**OK**」を選択します。「Oracle Internet Directory の接続」ダイアログ・ボックスが表示されます。

2. 「**資格証明**」タブ・ページの各フィールドに、このサーバー・インスタンス固有の情報を、次の表の説明に従って入力します。

表 4-1「資格証明」タブ・ページのフィールド

フィールド	説明
ユーザー	初めてログインするときは、**スーパー・ユーザー**または匿名でログインします。このセッション中に SSL の機能を構成する場合は、スーパー・ユーザーでログインします。 スーパー・ユーザーでログインする場合は、「ユーザー」ボックスに `cn=orcladmin` と入力します。 匿名でログインする場合は、「ユーザー」ボックスを空白のままにします。 LDAP のコマンドライン・ツールを使用してユーザーのエントリをすでに設定している場合は、次の 2 つの方法いずれかでそのユーザーのエントリを入力できます。 ■ 「ユーザー」フィールドの右側のボタンを使用し、そのエントリを参照して選択します。 ■ そのユーザーのエントリに対する**識別名**を、次の例のように正しい書式で入力します。 `cn=Susie Brown,ou=HR,o=acme,c=us`
パスワード	スーパー・ユーザーでログインし、インストール時にスーパー・ユーザー用のパスワードを指定している場合は、そのパスワードを「**パスワード**」フィールドに入力します。パスワードを指定していない場合は、デフォルトのパスワード `welcome` を入力します。Oracle Directory Manager にログインし、ディレクトリ・サーバーに接続した後、ディレクトリを保護するためにこのパスワードを変更してください。 匿名でログインする場合は、「**パスワード**」フィールドを空白のままにします。 特定のディレクトリ・ユーザーとしてログインする場合は、対応するパスワードを入力してください。 **関連項目：**パスワードの変更方法は、5-11 ページの「スーパー・ユーザー、ゲスト・ユーザーおよびプロキシ・ユーザーの管理」を参照してください。

表 4-1「資格証明」タブ・ページのフィールド（続き）

フィールド	説明
サーバー	「**サーバー**」リストから、接続するディレクトリ・サーバーのあるホストを選択します。 ディレクトリ・サーバーにすでに接続している場合に、別のホストのディレクトリ・サーバーに接続する手順は、次のとおりです。 **1.** 「**サーバー**」リストの右側のボタンをクリックします。使用可能なサーバーのリストが、「ディレクトリ・サーバーの選択」ダイアログ・ボックスに表示されます。 **2.** サーバーを選択します。 **3.** 「**OK**」を選択します。 ディレクトリ・サーバーをリストに追加する手順は、次のとおりです。 **1.** 「ディレクトリ・サーバーの選択」ダイアログ・ボックスで、「**追加**」を選択します。「ディレクトリ・サーバーの接続」ダイアログ・ボックスが表示されます。 **2.** 「**サーバー**」フィールドに、追加するディレクトリ・サーバーの名前を入力します。 **3.** 「**ポート**」フィールドに、追加するサーバーのポート番号を入力します。 **4.** 「**OK**」を選択します。追加したディレクトリが、「ディレクトリ・サーバーの選択」ダイアログ・ボックスのリストに表示されます。 リストにあるディレクトリ・サーバーを変更する手順は、次のとおりです。 **1.** 変更するディレクトリ・サーバーを選択します。 **2.** 「**編集**」を選択します。「ディレクトリ・サーバーの接続」ダイアログ・ボックスが表示されます。 **3.** 「**サーバー**」フィールドおよび「**ポート**」フィールドを変更して、「**OK**」を選択します。サーバーに対する変更が、「ディレクトリ・サーバーの選択」ダイアログ・ボックスのリストに表示されます。

表 4-1「資格証明」タブ・ページのフィールド（続き）

フィールド	説明
ポート	このフィールドには、デフォルト・ポート（389）が表示されます。同じホスト上に複数のディレクトリ・サーバー・インスタンスが存在している場合、各ディレクトリ・サーバー・インスタンスごとにポートが異なり、ディレクトリ・サーバー・インスタンスを選択すると、そのポート番号がこのフィールドに表示されます。 このポート番号を変更する手順は、次のとおりです。 1. 「**サーバー**」フィールドの右側のボタンを選択します。 2. 「ディレクトリ・サーバーの選択」ダイアログ・ボックスで、ディレクトリ・サーバーを選択します。 3. 「**編集**」を選択します。「ディレクトリ・サーバーの接続」ダイアログ・ボックスが表示されます。 4. 「ディレクトリ・サーバーの接続」ダイアログ・ボックスの「**ポート**」フィールドにポート番号を入力して、「**OK**」を選択します。
SSL 使用可能	このチェックボックスを選択すると、Oracle Directory Manager を使用して発行するすべてのコマンドが Secure Sockets Layer（SSL）を介して送信されます。 ディレクトリ・サーバーには、SSL の使用または SSL なしのいずれでも接続できます。SSL を使用して接続すると、Oracle Directory Manager は SSL クライアントになります。 この方法による接続は、次の 2 つの条件を満たしている場合に可能です。 ■ 接続先のサーバーが SSL を使用していること。接続先のサーバーが SSL を使用していない場合にこのチェックボックスを選択すると、認証に失敗します。 ■ 証明書と信頼できる証明書のリストを含んだ Wallet が作成済であること。

関連項目：

- SSL を使用可能にする方法は、第 13 章「Secure Sockets Layer（SSL）とディレクトリ」を参照してください。
- 識別名の書式に関する説明は、2-2 ページの「エントリ」を参照してください。
- ポートの変更方法とそのセキュリティへの影響については、13-3 ページの「SSL パラメータの構成」を参照してください。
- SSL の使用時に Oracle Wallet Manager を使用して Wallet を作成する手順は、『Oracle Advanced Security 管理者ガイド』を参照してください。

3. 「**資格証明**」タブ・ページの「**SSL 使用可能**」チェックボックスを選択した場合は、次に「**SSL**」タブを選択します。
4. 次の表の説明に従って、各フィールドに必要なデータを入力します。

表 4-2 「SSL」タブ・ページのフィールド

フィールド	説明
SSL 位置	クライアントとサーバーの認証に使用するクライアントの Wallet を指定します。クライアントの Wallet がローカル・マシン上にある場合は、その Wallet のパスとファイル名を次の構文で入力します。 `file:` *absolute_path_name* Wallet が別のマシン上にある場合は、その位置にリンクして、Wallet のリンク・パスとファイル名を入力します。
SSL パスワード	ユーザーの Wallet をオープンするパスワード。
SSL 認証	認証レベルを次の中から選択します。 ■ SSL 認証なし : クライアントとサーバーのいずれも、相手に対して自己認証を行いません。証明書の送信または交換は行われません。「資格証明」タブの「SSL 使用可能」チェックボックスを選択して、このオプションを選択した場合は、SSL 暗号化 / 復号化のみが使用されます。 ■ SSL クライアントとサーバーの認証 : クライアントとサーバーの認証。クライアントとサーバーは、証明書を交換します。 ■ SSL サーバー認証 : サーバー認証。ディレクトリ・サーバーがクライアントに証明書を送信することによって、ディレクトリ・サーバーからクライアントに対してサーバー認証を行います。

5. 「**ログイン**」を選択します。Oracle Directory Manager が表示されます。

Oracle Directory Manager のナビゲート

この項では、Oracle Directory Manager の概要を紹介し、メニュー・バーの項目とツールバーのボタンについて説明します。

Oracle Directory Manager の概要

ディレクトリと同様に、ナビゲータ・ペイン（ダブル・ウィンドウ・インタフェースの左側のウィンドウ）はツリー構造です。最初に Oracle Directory Manager をオープンしたときのナビゲータ・ペインには、ツリー項目「Oracle Internet Directory サーバー」のみが表示されます。ツリー項目の横のプラス記号（+）をクリックすると、そのツリー項目のサブコンポーネントが表示されます。

右側のペインで、一部のウィンドウには「適用」ボタンと「OK」ボタンがあります。「適用」を選択すると、変更内容がコミットされ、ウィンドウを開いたまま続けて他の変更操作を実行できます。「OK」をクリックすると、変更内容がコミットされ、ウィンドウが閉じます。

同様に、「回復」ボタンと「取消」ボタンがあります。「回復」をクリックすると、そのウィンドウで行った変更は適用されず、元の値が該当するフィールドに再び表示され、ウィンドウを開いたまま作業を継続できます。「取消」をクリックすると、そのウィンドウで行った変更は適用されないままウィンドウが閉じます。

Oracle Directory Manager のメニュー・バー

表 4-3 に、メニュー・バーからアクセスできるメニューを示します。各メニュー項目は、表示しているペインやタブ・ページによって、使用できる場合と使用できない場合があります。

表 4-3 Oracle Directory Manager のメニュー・バー

メニュー	メニュー項目
ファイル	**作成**: オブジェクトを追加します。
	類似項目の作成: ナビゲータ・ペインで選択したオブジェクトをテンプレートとして使用し、新規オブジェクトを追加します。
	接続: ナビゲータ・ペインで選択したディレクトリ・サーバーに接続します。
	切断: ナビゲータ・ペインで選択したディレクトリ・サーバーから切断します。
	終了: Oracle Directory Manager を終了します。
編集	**編集**: オブジェクトを変更します。
	削除: 選択したオブジェクトを削除します。
	オブジェクト・クラスの検索または**属性の検索**: コンテキストに応じて、オブジェクト・クラスまたは属性を検索します。ナビゲータ・ペインで「**Oracle Internet Directory**」>**ディレクトリ・サーバー・インスタンス**>「**サーバー管理**」>「**オブジェクト・クラス**」の順にナビゲートすると、このメニュー項目でオブジェクト・クラスを検索できます。「**Oracle Internet Directory**」>**ディレクトリ・サーバー・インスタンス**>「**サーバー管理**」>「**属性**」の順にナビゲートすると、属性を検索できます。

表 4-3 Oracle Directory Manager のメニュー・バー（続き）

メニュー	メニュー項目
ビュー	**更新**：メモリーに格納されているデータを更新し、データベースに変更内容を反映します。 **切離し**：Oracle Directory Manager の右側のペインに表示されているフィールドと値を含むセカンダリ・ダイアログを生成します。2 つの情報を比較する場合に便利です。
操作	**オブジェクト・クラスの作成**：新規オブジェクト・クラスの追加に使用する「新規オブジェクト・クラス」ウィンドウを表示します。 **属性の作成**：エントリへの新規属性の追加に使用する「新規属性の型」ダイアログ・ボックスを表示します。 **アクセス制御ポイントの作成**：新規**アクセス制御ポリシー・ポイント**の追加に使用する「新規アクセス制御ポイント」ダイアログ・ボックスを表示します。 **エントリの作成**：新規ディレクトリ・エントリの追加に使用する「新規エントリ」ダイアログ・ボックスを表示します。 **エントリの更新**：メモリーに格納されているエントリのデータを更新し、データベースに変更内容を反映します。 **サブツリー・エントリの更新**：メモリーに格納されているエントリの子を更新し、データベースに変更内容を反映します。 **検索フィルタの構成**：指定されたフィルタに応じてナビゲータ・ペインが表示するエントリの範囲を狭くします。 **索引の削除**：属性から索引を削除します。この項目を選択すると、削除の確認を要求するアラートが表示されます。 **検索**：ACP 検索の構成を可能にします。 **ユーザー設定項目**：次の操作のためのダイアログ・ボックスを表示します。 ■ エントリ検索結果の表示の構成 ■ ACP の表示を Oracle Directory Manager の実行のたびに行うか、検索の結果としてのみ行うかの設定
ヘルプ	**目次**：ヘルプ・ナビゲータの「目次」タブ・ページを表示します。 **トピックの検索**：オンライン・ヘルプ・ガイドのワード検索に使用する「ヘルプ・ナビゲータ」ダイアログ・ボックスを表示します。 バージョン情報：Oracle Internet Directory のバージョン情報を表示します。

Oracle Directory Manager のツールバー

図 4-1 に、Oracle Internet Directory のツールバーを示します。このツールバーについて左から順番に表 4-4 で説明します。各ボタンは、Oracle Directory Manager に表示しているペインやタブ・ページによって、使用できる場合と使用できない場合があります。

図 4-1 Oracle Directory Manager のツールバー

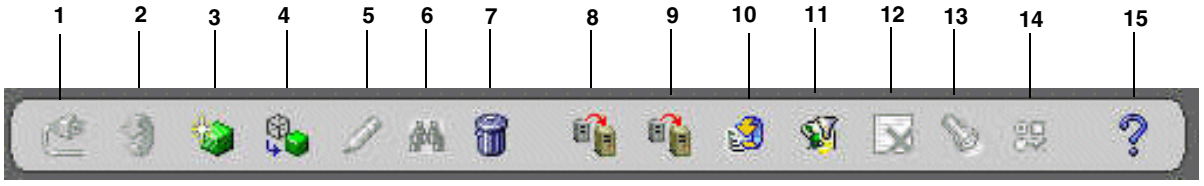


表 4-4 Oracle Directory Manager のツールバー

ボタン	用途
1	「**接続**」: ナビゲータ・ペインで選択したディレクトリ・サーバーに接続します。または選択したディレクトリ・サーバーから切断します。
2	**更新**: メモリーに格納されているエントリ以外のオブジェクトのデータを更新し、データベースに変更内容を反映します。
3	**作成**: 新規オブジェクトを追加します。
4	**類似項目の作成**: 別のオブジェクトをテンプレートとして使用して、新規オブジェクトを追加します。
5	**編集**: オブジェクトを変更します。
6	**オブジェクト・クラスの検索または属性の検索**: コンテキストに応じて、オブジェクト・クラスまたは属性を検索します。ナビゲータ・ペインで「Oracle Internet Directory」>ディレクトリ・サーバー・インスタンス>「サーバーの管理」>「オブジェクト・クラス」の順にナビゲートすると、このボタンでオブジェクト・クラスを検索できます。「Oracle Internet Directory」>ディレクトリ・サーバー・インスタンス>「サーバーの管理」>「属性」の順にナビゲートすると、属性を検索できます。
7	**削除**: オブジェクトを削除します。
8	**オブジェクト・クラスの追加**: 既存エントリにオブジェクト・クラスを追加します。
9	**エントリの更新**: メモリーに格納されているエントリのデータを更新し、データベースに変更内容を反映します。
10	**サブツリー・エントリの更新**: メモリーに格納されているエントリの子を更新し、データベースに変更内容を反映します。

表 4-4 Oracle Directory Manager のツールバー（続き）

ボタン	用途
11	**検索フィルタの構成**: 指定されたフィルタに応じてナビゲータ・ペインが表示するエントリの範囲を狭くします。
12	**索引の削除**: 属性から索引を削除します。このボタンをクリックすると、削除の確認を要求するアラートが表示されます。
13	**検索**: ACP 検索の構成を可能にします。
14	**ユーザー設定項目**: 検索操作のエントリと同様に、ナビゲータ・ペインの ACP の表示を構成できるようにします。
15	**ヘルプ**: ヘルプ・システムを表示します。

Oracle Directory Manager を使用した追加のディレクトリ・サーバーへの接続

一度に複数のディレクトリ・サーバーに接続し、各ディレクトリ・サーバーのデータ、スキーマおよびセキュリティを表示して変更できます。複数のサーバーに接続すると、「Oracle Internet Directory サーバー」の下のナビゲータ・ペインに、各サーバーがリストされます。

追加のディレクトリ・サーバーに接続する手順は、次のとおりです。

1. ナビゲータ・ペインで「**Oracle Internet Directory サーバー**」を選択します。
2. 右側のペインの「**新規作成**」をクリックします。
3. 4-3 ページの「Oracle Directory Manager を使用したディレクトリ・サーバーへの接続」で説明している手順に従ってログインします。

Oracle Directory Manager を使用したディレクトリ・サーバーからの切断

Oracle Directory Manager を使用してディレクトリ・サーバーから切断するには、「**ファイル**」メニューから「**切断**」を選択します。また、Oracle Directory Manager を終了すると、すべてのディレクトリ・サーバーとディレクトリ間の接続が自動的に切断されます。

すべての接続情報は、ファイル `osdadmin.ini` のユーザーのホーム・ディレクトリに格納されます。

Oracle Directory Manager を再起動すると、今までに接続したすべてのサーバー接続が、ディレクトリ・サーバーの「ログイン」ダイアログ・ボックスに表示されます。

Oracle Directory Manager での検索の表示と期間の構成

検索の結果として Oracle Directory Manager に表示されるエントリの最大数と検索の期間を指定できます。Oracle Directory Manager またはディレクトリ・サーバー、あるいはその両方でこれらの構成を行えます。

Oracle Directory Manager とディレクトリ・サーバーの両方で構成を行い、Oracle Directory Manager での構成がディレクトリ・サーバーでの構成と一致しない場合、この矛盾を Oracle Internet Directory が次のように解決します。

- Oracle Directory Manager での設定値がディレクトリ・サーバーでの設定値より大きい場合は、ディレクトリ・サーバーの構成が採用されます。たとえば、検索期間を、Oracle Directory Manager では 2 分間、ディレクトリ・サーバーでは 3 分間に設定した場合、実際の検索期間は 3 分になります。
- Oracle Directory Manager での設定値がディレクトリ・サーバーでの設定値より小さい場合は、Oracle Directory Manager の構成が採用されます。たとえば、検索期間を Oracle Directory Manager では 2 分間、ディレクトリ・サーバーでは 3 分間に設定した場合、実際の検索期間は 2 分になります。

Oracle Directory Manager で検索の表示と期間を構成する手順は、次のとおりです。

1. ナビゲータ・ペインで「**Oracle Internet Directory サーバー**」を展開して、構成するサーバーを選択します。
2. ツールバーから「**ユーザー設定項目**」を選択します。「ユーザー設定項目」ダイアログ・ボックスが表示されます。
3. 「**エントリ管理の構成**」タブ・ページの「**1 レベルのサブツリー・エントリの最大数**」フィールドに、検索により返されるエントリの最大数を入力します。
4. 「**最大の検索時間**」フィールドに、検索完了までの最大時間を秒単位で入力します。デフォルトは 3600 です。
5. 「**OK**」を選択します。

Oracle ディレクトリ・サーバーで検索の表示と期間を構成する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」を展開して、ディレクトリ・サーバー・インスタンスを選択します。そのサーバーに対応するタブ・ページが右側のペインに表示されます。
2. 「**システム操作属性**」タブ・ページの「**問合せエントリの返送制限**」フィールドに、検索によって戻されるエントリの最大数を入力します。デフォルトは 1000 です。
3. 「**サーバー処理の制限時間**」フィールドに、検索完了までの最大時間を秒単位で入力します。デフォルトは 3600 です。
4. 「**適用**」を選択します。

Oracle Directory Manager を使用した管理タスクの実行

Oracle Directory Manager を使用すると、Oracle Internet Directory の大部分の管理タスクを実行できます。Oracle Directory Manager で実行できないタスクには、OID モニター（oidmon）の起動と停止やサーバー・インスタンスの起動と停止などの実行プロセスがあります。Oracle Directory Manager で実行できないタスクの実行には、対応する LDAP コマンドライン・ツールを使用します。

関連項目：

- 4-14 ページの「コマンドラインツールの使用方法」
- 付録 A「LDIF およびコマンドライン・ツールの構文」

次の表に、Oracle Directory Manager を使用して管理できるタスクの領域、および各領域に関する説明の参照先を示します。

表 4-5 Oracle Directory Manager でのタスクの領域

タスクの領域	参照先
アクセス制御の管理	14-17 ページの「Oracle Directory Manager を使用したアクセス制御の管理」 14-48 ページの「コマンドライン・ツールを使用したアクセス制御の管理」
属性一意性の管理	第 8 章「ディレクトリの属性一意性」
監査ログの管理	第 10 章「ディレクトリのロギング、監査および監視」
変更ログの管理	24-19 ページの「ディレクトリ・レプリケーションの変更ログ」 第 25 章「Oracle ディレクトリ・レプリケーションの管理」 32-6 ページの「Oracle Directory Synchronization Service」 33-3 ページの「同期の使用例」 35-6 ページの「Oracle Directory Integration and Provisioning Server の管理」
エントリの管理	7-2 ページの「Oracle Directory Manager を使用したエントリの管理」
ガベージ・コレクションの管理	第 22 章「Oracle Internet Directory におけるガベージ・コレクション」
パスワード・ポリシーの管理	第 15 章「Oracle Internet Directory のパスワード・ポリシー」
パスワード・ベリファイアの管理	第 16 章「パスワード・ベリファイアのディレクトリ格納」

表 4-5 Oracle Directory Manager でのタスクの領域（続き）

タスクの領域	参照先
プラグインの管理	第 VIII 部「ディレクトリ・プラグイン」
レプリケーションの管理	第 25 章「Oracle ディレクトリ・レプリケーションの管理」
スキーマの管理	6-2 ページの「ディレクトリのオブジェクト・クラス」 6-11 ページの「ディレクトリの属性」
サーバーの管理	第 5 章「Oracle ディレクトリ・サーバーの管理」

コマンドラインツールの使用方法

Oracle Internet Directory には、ディレクトリ・エントリと属性を操作するために、次のような数種類のコマンドライン・ツールが用意されています。

- LDAP ツールー LDAP Data Interchange Format（LDIF）で記述されたテキスト・ファイル内のオブジェクトを変更します。
- カタログ管理ツールー既存の属性を索引付きの属性にします。
- 社内の複数のディレクトリを同期化するための各種ツール。

多くのコマンドライン・ツールは、LDAP Data Interchange Format（LDIF）で記述されたテキスト・ファイルのオブジェクトに有効です。

注意： コマンドライン・ツールを使用するには、次の環境変数を設定します。

- *ORACLE_HOME*
- ORACLE_*SID* または適切な TNS CONNECT 文字列
- NLS_LANG（*APPROPRIATE_LANGUAGE*.AL32UTF8）。インストール時のデフォルトの言語設定は、AMERICAN_AMERICA です。
- PATH および CLASSPATH。環境変数 PATH および CLASSPATH では、UNIX バイナリ・ディレクトリの前に Oracle LDAP バイナリ（*ORACLE_HOME*/bin）を指定します。

関連項目： LDIF ファイルのフォーマット方法は、A-2 ページの「LDAP Data Interchange Format（LDIF）の構文」を参照してください。

この項では、次の項目について説明します。

- Oracle Internet Directory サーバーの起動、停止、監視のためのコマンドライン・ツール
- エントリと属性の管理のためのコマンドライン・ツール
- バルク操作を実行するためのコマンドライン・ツール
- レプリケーション管理のためのコマンドライン・ツール
- ディレクトリの同期化とプロビジョニングの管理のためのコマンドライン・ツール
- OID 移行ツール（ldifmigrator）
- OID データベース統計収集ツール（oidstats.sh）
- OID データベース・パスワード・ユーティリティ（oidpasswd）

Oracle Internet Directory サーバーの起動、停止、監視のためのコマンドライン・ツール

表 4-6 に、Oracle Internet Directory サーバーを起動、停止および監視するための各種コマンドライン・ツールとその詳細情報の参照先を示します。

表 4-6　Oracle Internet Directory サーバーの起動、停止、監視のためのツール

ツール	説明	詳細情報の参照先
OID 制御ユーティリティ（OIDCTL）	このツールは、サーバーを起動および停止するときに使用します。コマンドは、OID モニター・プロセスによって解析され、実行されます。	概念の説明は、2-13 ページの「Oracle Internet Directory のアーキテクチャ」を参照してください。 構文と使用方法は、A-6 ページの「OID 制御ユーティリティ（oidctl）の構文」を参照してください。
OID モニター（OIDMON）	このツールは、LDAP サーバー・プロセスを開始、監視および終了するときに使用します。レプリケーション・サーバーをインストールする場合、レプリケーション・サーバーは OID モニターによって制御されます。ディレクトリ・サーバー・インスタンスを起動または停止するために OID 制御ユーティリティ（OIDCTL）を介してコマンドを発行すると、そのコマンドはこのプロセスによって解析されます。	概念の説明は、2-13 ページの「Oracle Internet Directory のアーキテクチャ」を参照してください。 構文と使用方法は、A-4 ページの「OID モニター（oidmon）構文」を参照してください。

エントリと属性の管理のためのコマンドライン・ツール

表 4-7 に、エントリと属性を管理するためのコマンドライン・ツールとその詳細情報の参照先を示します。

表 4-7　エントリの管理のためのツール

ツール	説明	詳細情報の参照先
カタログ管理ツール（catalog.sh）	Oracle Internet Directory は、索引を使用して属性を検索できるようにしています。Oracle Internet Directory のインストール時に、エントリ cn=catalogs に、検索で使用できる属性がリストされます。等価の一致規則を持つ属性のみが索引付けできます。 その他の属性を検索フィルタで使用する場合は、使用する属性をカタログ・エントリに追加する必要があります。この操作は、Oracle Directory Manager を使用して属性を作成するときに実行できます。ただし、すでに存在している属性への索引付けに使用できるのは、カタログ管理ツールのみです。 索引の作成と削除に便利です。	構文と使用方法は、A-19 ページの「カタログ管理ツール（catalog.sh）構文」を参照してください。 6-19 ページの「コマンドライン・ツールを使用した属性の索引付け」 6-16 ページの「Oracle Directory Manager を使用した属性の索引付け」
ldapadd	このツールは、一度に 1 つずつエントリを追加するときに使用します。	A-21 ページの「ldapadd の構文」
ldapaddmt	これは共有サーバー・ツールであり、同時に複数のエントリを追加するときに使用します。	A-23 ページの「ldapaddmt の構文」
ldapbind	このツールは、ディレクトリ・サーバーに対してユーザーまたはクライアントを認証するときに使用します。	A-25 ページの「ldapbind の構文」
ldapcompare	このツールは、指定した属性値がエントリに含まれているかどうかを調べるときに使用します。	A-26 ページの「ldapcompare の構文」
ldapdelete	このツールは、エントリを削除するときに使用します。	A-28 ページの「ldapdelete の構文」
ldapmoddn	このツールは、エントリの識別名または相対識別名の変更、エントリまたはサブツリーの名前の変更、エントリまたはサブツリーの新しい親への移動を行うときに使用します。	A-30 ページの「ldapmoddn の構文」
ldapmodify	このツールは、エントリの属性データを作成、更新および削除するときに使用します。	A-32 ページの「ldapmodify の構文」
ldapmodifymt	これは共有サーバー・ツールであり、同時に複数のエントリを変更するときに使用します。	A-37 ページの「ldapmodifymt の構文」
ldapsearch	このツールは、ディレクトリ・エントリを検索するときに使用します。	A-39 ページの「ldapsearch の構文」

バルク操作を実行するためのコマンドライン・ツール

表 4-8 に、バルク操作を実行するためのコマンドライン・ツールとその詳細情報の参照先を示します。

表 4-8 バルク操作を実行するためのコマンドライン・ツール

ツール	説明	詳細情報の参照先
bulkdelete	このツールは、サブツリーを効率的に削除するときに使用します。	A-44 ページの「bulkdelete の構文」
bulkload	このツールは、LDIF ファイルを使用して Oracle Internet Directory に大量のエントリをロードし、追加するときに使用します。	A-45 ページの「bulkload の構文」
bulkmodify	このツールは、既存の多数のエントリを効率的に変更するために使用します。	A-52 ページの「bulkmodify の構文」
ldifwrite	このツールは、ディレクトリ情報ベースのデータを、LDAP 準拠のディレクトリ・サーバーで読取り可能な LDIF ファイルにコピーするために使用します。ldifwrite は、bulkload と組み合せて使用できます。ldifwrite を使用して、ディレクトリの一部またはすべての情報をバックアップすることもできます。	A-54 ページの「ldifwrite の構文」

レプリケーション管理のためのコマンドライン・ツール

表 4-9 に、レプリケーションを管理するためのコマンドライン・ツールとその詳細情報の参照先を示します。

表 4-9 レプリケーション管理のためのコマンドライン・ツール

ツール	説明	詳細情報の参照先
レプリケーション環境管理ツール	このツールは、Oracle9*i* Advanced Replication がディレクトリ・レプリケーションのために正しく構成されることを保証します。ディレクトリ・レプリケーション障害が発生した場合、このツールは問題を調査し、修正方法を検証します。問題を解決できない場合は、問題の性質に関するレポートを作成し、考えられる解決方法を示します。	構文と例は、A-62 ページの「レプリケーション環境管理ツール」を参照してください。

表 4-9 レプリケーション管理のためのコマンドライン・ツール（続き）

ツール	説明	詳細情報の参照先
OID 調停ツール	レプリケーションの競合が発生すると、Oracle ディレクトリ・レプリケーション・サーバーは変更をリトライ・キューに入れ、そこからの変更の適用を指定された回数だけ再試行します。指定された失敗回数に達した後、レプリケーション・サーバーは変更を管理者操作キューに入れます。レプリケーション・サーバーはそこから長い間隔で変更適用プロセスを繰り返すと同時に、管理者によるアクションを待ちます。 この時点で、次の操作を行う必要があります。 1. 管理者操作キューの変更を検証します。 2. OID 調停ツールを使用して、サプライヤでの変更と競合しているコンシューマでの変更を調停します。 3. 変更をリトライ・キューに戻すか、パージ・キューに入れます。	25-21 ページの「OID 調停ツールの概要」 OID 調停ツールの構文と動作の説明は、A-59 ページの「OID 調停ツール」を参照してください。
管理者操作キュー操作ツール	OID 調停ツールを使用して、競合している変更を調停した後に、管理者操作キュー操作ツールを使用して、変更を管理者操作キューからリトライ・キューまたはパージ・キューに移動できます。パージ・キューへの変更の移動は、変更ログ・エントリの再適用を以降は試みないということを意味します。	25-21 ページの「管理者操作キュー操作ツールの概要」 構文の説明は、A-56 ページの「管理者操作キュー操作ツール」を参照してください。

ディレクトリの同期化とプロビジョニングの管理のためのコマンドライン・ツール

表 4-10 に、ディレクトリの同期化とプロビジョニングを管理するためのコマンドライン・ツールとその詳細情報の参照先を示します。

表 4-10 ディレクトリの同期化とプロビジョニングの管理のためのコマンドライン・ツール

ツール	説明	詳細情報の参照先
Directory Integration and Provisioning Assistant	このツールは、Oracle Directory Integration and Provisioning Platform でのすべての操作の実行を支援します。	A-106 ページの「Directory Integration and Provisioning Assistant」
プロビジョニング・サブスクリプション・ツール	このツールを使用して、作成、無効化、有効化、削除、監視およびエラーの消去など、ディレクトリ内のプロビジョニング・プロファイル・エントリを管理します。	A-125 ページの「プロビジョニング・サブスクリプション・ツール（oidprovtool）の構文」
ldapuploadagentfile.sh	このツールを使用して、ディレクトリを同期化するときにマッピングおよび構成情報をロードします。	A-118 ページの「ldapUploadAgentFile.sh ツールの構文」

表 4-10 ディレクトリの同期化とプロビジョニングの管理のためのコマンドライン・ツール（続き）

ツール	説明	詳細情報の参照先
ldapcreateconn.sh	このツールを使用して、同期プロファイルを作成します。	A-119 ページの「ldapCreateConn.sh ツール構文」
oidmdelp	このツールを使用して、同期プロファイルの登録を解除します。	A-121 ページの「ldapDeleteConn.sh ツール構文」
stopodis	モニターおよび oidctl ツールを使用できないクライアントのみのインストール環境では、oidctl ツールを使用せずに Oracle Directory Integration and Provisioning Server を起動できます。	A-122 ページの「StopOdiServer.sh ツールの構文」
schemasync	このツールを使用して、Oracle ディレクトリ・サーバーとサード・パーティの LDAP ディレクトリの間で、スキーマ要素（属性とオブジェクト・クラス）を同期化します。	A-123 ページの「schemasync ツールの構文」

OID 移行ツール（ldifmigrator）

アプリケーション固有のリポジトリから Oracle Internet Directory へデータを移行するには、このツールを使用します。

関連項目： このツールの使用方法は、A-132 ページの「OID 移行ツール（ldifmigrator）の構文」を参照してください。

OID データベース統計収集ツール（oidstats.sh）

このツールを使用し、様々なデータベースの ods スキーマ・オブジェクトを分析して統計を見積ります。ディレクトリへのデータの初回ロードを含め、ディレクトリ・データに大幅な変更がある場合は、このユーティリティを実行する必要があります。

バルク・ロード・ツール（bulkload.sh）以外の手段でデータをディレクトリにロードする場合は、ロード後に OID データベース統計収集ツールを実行する必要があります。Oracle のオプティマイザが LDAP 操作に対応する問合せについて最適の実行計画を選択するには、統計収集が必要です。OID データベース統計収集ツールは、OID デーモンを停止せずに必要に応じて実行できます。

関連項目： A-131 ページの「OID データベース統計収集ツール（oidstats.sh）の構文」

OID データベース・パスワード・ユーティリティ（oidpasswd）

OID データベース・パスワード・ユーティリティを使用して、次の操作を実行できます。

- Oracle Internet Directory データベースへのパスワードを変更します。

  Oracle Internet Directory は、Oracle データベースへの接続時にパスワードを使用します。このパスワードのデフォルトは、Oracle Application Server 管理者のパスワードとしてインストール時に指定した値と同じです。OID データベース・パスワード・ユーティリティを使用すると、このパスワードを変更できます。

- Oracle Internet Directory データベース・パスワード用の oidlpwdldap1 という Wallet、および Oracle ディレクトリ・レプリケーション・サーバー・パスワード用の `oidpwdr`*`sid`* という Wallet を作成します。

  `sid` は環境変数 *`SID`* からではなく、接続データベースから取得されます。

  `create_wallet=true` オプションを使用して、ODS Wallet を生成する前に、ODS データベースに対して自己認証を行うための ODS パスワードを指定する必要があります。デフォルトの ODS パスワードは Oracle Application Server 管理者のパスワードと同じです。

- ロックされているディレクトリ・スーパー・ユーザー・アカウント（`cn=orcladmin`）のロックを解除します。

関連項目： A-129 ページの「OID データベース・パスワード・ユーティリティ（oidpasswd）構文」

定期的な管理タスクの一覧

Oracle Internet Directory の定期的な管理タスクの説明は、このマニュアル全体にわたって記述されています。次の表に、一般的なタスクの一部について必要な情報を示します。

表 4-11 定期的な管理タスク

タスク	情報
属性の管理	-
コマンドライン・ツールを使用した属性の追加、変更または削除	6-17 ページの「コマンドライン・ツールを使用した属性の管理」
Oracle Directory Manager を使用した属性の追加、変更または削除	6-11 ページの「ディレクトリの属性」
エントリの管理	-
コマンドライン・ツールを使用したディレクトリ・エントリの追加、変更または削除	7-9 ページの「コマンドライン・ツールを使用したエントリの管理」

表 4-11 定期的な管理タスク（続き）

タスク	情報
Oracle Directory Manager を使用したディレクトリ・エントリの追加、変更または削除	7-2 ページの「Oracle Directory Manager を使用したエントリの管理」
大量のデータ・ファイルのインポート	A-45 ページの「bulkload の構文」 A-2 ページの「LDAP Data Interchange Format（LDIF）の構文」
エントリのディレクトリ情報ツリー階層の表示	7-2 ページの「Oracle Directory Manager を使用したエントリの管理」
オブジェクト・クラスの管理	-
コマンドライン・ツールを使用したオブジェクト・クラスの追加、変更または削除	6-9 ページの「コマンドライン・ツールを使用したオブジェクト・クラスの管理」
Oracle Directory Manager を使用したオブジェクト・クラスの追加、変更または削除	6-2 ページの「ディレクトリのオブジェクト・クラス」
レプリケーションの管理	-
レプリケーションの設定	第 25 章「Oracle ディレクトリ・レプリケーションの管理」
レプリケーション変更の競合の解消	25-20 ページの「手動でのマルチマスター・レプリケーション・グループ内の競合の解消」
レプリケーション変更の管理者操作キューからリトライ・キューかパージ・キューへの移動	25-21 ページの「管理者操作キュー操作ツールの概要」
セキュリティの管理	-
アクセス制御ポリシー・ポイント（ACP）の設定	第 14 章「ディレクトリ・アクセス制御」
SSL の設定	第 13 章「Secure Sockets Layer（SSL）とディレクトリ」
サーバーの管理	-
コマンドライン・ツールを使用したサーバー・インスタンス・パラメータの構成	5-7 ページの「コマンドライン・ツールを使用したサーバー構成設定エントリの管理」
Oracle Directory Manager を使用したサーバー・インスタンス・パラメータの構成	5-4 ページの「Oracle Directory Manager を使用したサーバーの構成設定エントリの管理」
Oracle Directory Manager を使用したディレクトリへの接続	4-3 ページの「Oracle Directory Manager を使用したディレクトリ・サーバーへの接続」 4-11 ページの「Oracle Directory Manager を使用した追加のディレクトリ・サーバーへの接続」

表 4-11 定期的な管理タスク（続き）

タスク	情報
ディレクトリ・サーバー・プロセスの起動	第 3 章「事前に実行するタスクと情報」
ディレクトリ・サーバー・プロセスの停止	第 3 章「事前に実行するタスクと情報」
システム操作属性の表示	5-9 ページの「Oracle Directory Manager を使用したシステム操作属性の設定」

第 II 部

基本的なディレクトリ管理

第 II 部では、Oracle Internet Directory の構成とメンテナンスに必要なタスクについて説明します。第 II 部は次の各章で構成されています。

- 第 5 章「Oracle ディレクトリ・サーバーの管理」
- 第 6 章「ディレクトリ・スキーマの管理」
- 第 7 章「ディレクトリ・エントリの管理」
- 第 8 章「ディレクトリの属性一意性」
- 第 9 章「Oracle Internet Directory の動的および静的グループ」
- 第 10 章「ディレクトリのロギング、監査および監視」

5

Oracle ディレクトリ・サーバーの管理

この章では、Oracle Directory Manager とコマンドライン・ツールを使用して Oracle ディレクトリ・サーバーを管理する方法について説明します。

この章では、次の項目について説明します。

- サーバーの構成設定エントリの管理
- システム操作属性の設定
- ネーミング・コンテキストの管理
- スーパー・ユーザー、ゲスト・ユーザーおよびプロキシ・ユーザーの管理
- アクティブ・サーバー・インスタンスの情報の表示
- アイドル状態の LDAP 接続のクローズ
- Oracle Internet Directory データベース・サーバー接続時のパスワードの変更
- 別名エントリの間接参照
- 分散環境でのディレクトリ・サーバーの位置の特定

> **関連項目：** ディレクトリ・サーバー・インスタンスの起動および停止方法は、第 3 章「事前に実行するタスクと情報」を参照してください。

サーバーの構成設定エントリの管理

OID 制御ユーティリティを使用して Oracle ディレクトリ・サーバーを起動すると、その起動メッセージはサーバー・パラメータを含む**構成設定エントリ**を参照します。構成設定エントリを追加、変更および削除するには、Oracle Directory Manager または対応するコマンドライン・ツールを使用します。

この項では、次の項目について説明します。

- 構成設定エントリ管理のための事前の考慮事項
- Oracle Directory Manager を使用したサーバーの構成設定エントリの管理
- コマンドライン・ツールを使用したサーバー構成設定エントリの管理

関連項目：

- 構成設定エントリの概要は、2-20 ページの「構成設定エントリ」を参照してください。
- OID 制御ユーティリティを使用したサーバーの起動方法は、3-2 ページの「タスク 2: サーバー・インスタンスの起動」を参照してください。

構成設定エントリ管理のための事前の考慮事項

構成設定エントリ `configset0` はデフォルトで、すべての新規構成設定エントリのテンプレートとして使用されます。このデフォルト構成設定の値は変更できますが、すべての変更が、新規に作成するすべての構成設定エントリに影響します。

すべてのサーバー・インスタンスに対しては有効でない値を変更するには、新しい構成設定エントリを作成することをお薦めします。ただし、この方法は、Oracle ディレクトリ・サーバーおよび Oracle Directory Integration and Provisioning Server のインスタンスにのみ適用されます。Oracle ディレクトリ・レプリケーション・サーバーがサポートする構成設定は 1 つのみです。

異なる値を使用して、ディレクトリ・サーバーの別のインスタンスを設定できます。この値を使用するユーザーを限定する場合は、新規の構成設定エントリを設定してから、特別なニーズを持つグループ用に、その構成設定エントリを示す個別のサーバー・インスタンスを実行してください。

図 5-1 に、それぞれ異なる値を持つ、3 つのディレクトリ・サーバー・インスタンスを示します。

図 5-1 複数の構成設定エントリを示すディレクトリ・エントリ階層

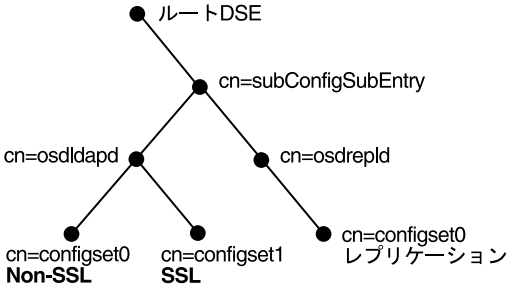


図 5-1 は、次のものを表しています。

- 次のインスタンスを含む Oracle ディレクトリ・サーバー（`cn=osdldap`）
  - デフォルト・ポートでリスニングし、SSL が使用禁止状態の `configset0` を使用している 1 つのインスタンス
  - SSL ポートでリスニングし、SSL が使用可能な状態の `configset1` を使用している 2 番目のインスタンス
- `configset0` を使用しているレプリケーション・サーバー・インスタンス（`cn=osdrepld`）

注意： ディレクトリ・サーバーが同じコンピュータ上にある場合は、複数のインスタンスを実行できます。たとえば、1 つのインスタンスを SSL モードで実行し、別のインスタンスを Non-SSL モードで実行できます。

関連項目：

- SSL の構成パラメータの詳細は、第 13 章「Secure Sockets Layer（SSL）とディレクトリ」を参照してください。
- レプリケーションの構成パラメータの詳細は、第 25 章「Oracle ディレクトリ・レプリケーションの管理」を参照してください。
- ディレクトリ・サーバー・インスタンスの構成に使用する、属性の全セットのリストとその説明は、B-5 ページの「構成設定エントリのスキーマ要素」を参照してください。

Oracle Directory Manager を使用したサーバーの構成設定エントリの管理

Oracle Directory Manager を使用して、構成設定エントリの表示、追加、変更および削除ができます。

重要： アクティブ・インスタンスのパラメータは直接変更できません。かわりに、構成設定エントリのパラメータを変更し、保存する必要があります。構成設定エントリの保存後に、OID 制御ユーティリティの restart コマンドを使用して現行の Oracle ディレクトリ・サーバー・インスタンスの停止と再起動を行ってください。

構成設定エントリを変更して、新規パラメータを使用する新しいインスタンスを起動できます。変更前に起動した実行中のインスタンスには、そのインスタンスを再起動するまで変更内容が適用されません。

ディレクトリ・サーバー・インスタンスを再起動する方法は、A-16 ページの「Oracle Internet Directory サーバー・インスタンスの再起動」を参照してください。

Oracle Directory Manager を使用した構成設定エントリの表示

構成設定エントリを表示する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**、「**サーバー管理**」の順に展開します。
2. 「**ディレクトリ・サーバー**」、「**レプリケーション・サーバー**」または「**統合サーバー**」を選択します。アクティブ・インスタンスのパラメータが、右側のペインに表示されます。
3. 右側のペインで、インスタンスを選択した後、「**プロパティの表示**」を選択します。「サーバー・プロセス」ダイアログ・ボックスが表示されます。

   ダイアログ・ボックス上部のタブを選択すると、インスタンスのパラメータをすべて参照できます。ただし、このダイアログ・ボックスではパラメータの値を変更できません。変更するには、基となっている構成設定エントリを変更する必要があります。

   関連項目： 5-6 ページの「Oracle Directory Manager を使用した構成設定エントリの変更」

Oracle Directory Manager を使用した構成設定エントリの追加

初めて構成設定エントリを追加するときには、次の操作が可能です。

- デフォルトの構成設定を新規構成設定エントリ用のテンプレートとして使用できます。以降は、デフォルトの構成設定のコピーを使用して構成設定を作成できます。
- 既存の構成設定エントリからコピーせずに、新規に追加できます。

デフォルトの構成設定エントリのコピーを使用した構成設定エントリの追加 デフォルトの構成設定エントリのコピーを使用して構成設定エントリを追加する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**、「**サーバー管理**」、「**ディレクトリ・サーバー**」の順に展開します。
2. 「**デフォルト構成設定**」を選択します。
3. ツールバーの「**類似項目の作成**」ボタンを選択します。「構成設定」ダイアログ・ボックスに「**一般**」タブ・ページが表示されます。
4. 「**一般**」タブ・ページの各フィールドに情報を入力します。詳細は、C-25 ページの表 C-32 を参照してください。
5. 「**SSL 設定**」タブを選択し、各フィールドに情報を入力します。詳細は、C-26 ページの表 C-33 を参照してください。
6. 「**適用**」を選択します。
7. コマンドを有効にするために、サーバー・インスタンスを再起動します。

関連項目：

- A-16 ページの「Oracle Internet Directory サーバー・インスタンスの再起動」
- Oracle Wallet Manager を使用して Oracle Wallet の位置と Oracle Wallet パスワードを設定する手順は、『Oracle Advanced Security 管理者ガイド』を参照してください。
- 10-6 ページの「デバッグ・ロギング・レベルの設定」

既存の構成設定エントリのコピーを使用しない構成設定エントリの追加 既存の構成設定のコピーを使用せずに、新しい構成設定エントリを作成する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**、「**サーバー管理**」、「**ディレクトリ・サーバー**」の順に展開します。
2. 「**デフォルト構成設定**」を選択します。
3. ツールバーの「**作成**」ボタンを選択します。「構成設定」ダイアログ・ボックスに「**一般**」タブ・ページが表示されます。
4. 「**一般**」タブ・ページの各フィールドに情報を入力します。詳細は、C-25 ページの表 C-32 を参照してください。
5. 「**SSL 設定**」タブを選択し、各フィールドに情報を入力します。これらのフィールドについては、C-26 ページの表 C-33 を参照してください。
6. 「**OK**」を選択します。

Oracle Directory Manager を使用した構成設定エントリの変更

構成設定エントリを変更する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「**ディレクトリ・サーバー・インスタンス**」、「**サーバー管理**」、「**ディレクトリ・サーバー**」の順に展開します。
2. 変更する構成設定を選択します。右側のペインのタブ・ページに、構成設定が表示されます。
3. 「**一般**」タブ・ページの各フィールドの情報を変更します。詳細は、C-25 ページの表 C-32 を参照してください。変更内容を保存するには、「**適用**」を選択します。
4. 「**SSL 設定**」タブを選択し、各フィールドの情報を変更します。詳細は、C-26 ページの表 C-33 を参照してください。変更内容を保存するには、「**適用**」を選択します。
5. コマンドを有効にするために、サーバー・インスタンスを再起動します。

関連項目：

- A-16 ページの「Oracle Internet Directory サーバー・インスタンスの再起動」
- Oracle Wallet Manager を使用して Oracle Wallet の位置と Oracle Wallet パスワードを設定する手順は、『Oracle Advanced Security 管理者ガイド』を参照してください。

Oracle Directory Manager を使用した構成設定エントリの削除

構成設定エントリを削除する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**サーバー管理**」、「**ディレクトリ・サーバー**」の順に展開します。
2. 削除する構成設定を選択します。
3. ツールバーの「**削除**」を選択します。
4. コマンドを有効にするために、サーバー・インスタンスを再起動します。

関連項目： A-16 ページの「Oracle Internet Directory サーバー・インスタンスの再起動」

コマンドライン・ツールを使用したサーバー構成設定エントリの管理

構成設定エントリの変更には Oracle Directory Manager を使用する方法をお薦めしますが、利用可能なコマンドライン・ツールを使用する方が便利な場合があります。たとえば、複数の Oracle ディレクトリ・サーバーに同じ変更を加える場合などがそうです。

コマンドライン・ツールを使用して構成設定エントリを追加または変更する場合、新規構成設定エントリの追加用の入力ファイルは、**LDAP Data Interchange Format（LDIF）**で作成する必要があります。インストール時のデフォルトと異なる属性と値のみ記述してください。ディレクトリ・サーバーは、新規構成設定エントリに設定された属性値で、該当する属性の既存値をオーバーライドします。

> **関連項目：** LDIF の詳細は、A-2 ページの「LDAP Data Interchange Format（LDIF）の構文」を参照してください。

ldapadd を使用した構成設定エントリの追加

新しい Oracle ディレクトリ・サーバー・インスタンスを追加する場合は、既存の構成設定エントリを使用するか、新しいインスタンス用に新規の構成設定エントリを追加します。

新規構成設定エントリを追加するには、入力ファイルを作成して、そのファイルを ldapadd でロードします。次の手順で行ってください。

1. テキスト・エディタで入力ファイルを作成します。

   入力ファイルは LDIF フォーマットで作成する必要があります。入力ファイルを作成するときは、その構成設定エントリの現行の値と異なる属性のみ定義（記述）する必要があります。

   この例では、パラメータ `configset2` は新規エントリの相対識別名（ローカル名）、Wallet の位置は `/HOME/test/wallet` です。

   ```
   dn:cn=configset2, cn=osdldapd, cn=subconfigsubentry
   cn:configset2
   objectclass:orclConfigSet
   objectclass:orclLDAPSubConfig
   objectclass:top
   orclsslauthentication:1
   orclsslenable:1
   orclsslport:5000
   orclsslversion:3
   orclsslwalleturl:file:/HOME/test/wallet
   ```

2. 入力ファイルを使用して ldapadd を実行します。

   コマンド・プロンプトで、入力ファイルを追加するコマンドを入力します。

   ```
   ldapadd [options] -f LDIF_file_name
   ```

関連項目：

- A-2 ページ「LDAP Data Interchange Format（LDIF）の構文」
- このコマンドで使用できるオプションの詳細は、A-21 ページの「ldapadd の構文」を参照してください。
- 構成設定エントリの属性の説明は、B-5 ページの「構成設定エントリのスキーマ要素」を参照してください。

ldapmodify を使用した構成設定エントリの変更と削除

既存の構成設定エントリを変更または削除するには、変更する属性のみを含む入力ファイルを作成して、その入力ファイルを ldapmodify コマンドでロードします。次の手順で行ってください。

1. 入力ファイルを作成します。

   入力ファイルを作成するとき、インストール時のデフォルトと異なる属性のみ定義（記述）します。

   入力ファイルは LDIF フォーマットで作成する必要があります。

   次に示す例では、パラメータ `cn=configset2,cn=osdldapd,cn=subconfigsubentry` が、既存の構成設定エントリの識別名（ローカル名）です。この例は、orclsslport パラメータを 7000 に変更する方法を示しています。

   ```
   dn:cn=configset2,cn=osdldapd,cn=subconfigsubentry
   changetype: modify
   replace: orclsslport
   orclsslport: 7000
   ```

2. 入力ファイルを参照する ldapmodify を実行します。

   コマンド・プロンプトで、入力ファイルを参照するコマンドを入力します。

   ```
   ldapmodify [options] -f LDIF_file_name
   ```

   関連項目：

   - A-2 ページの「LDAP Data Interchange Format（LDIF）の構文」
   - ldapmodify の詳細とそのオプションのリストは、A-32 ページの「ldapmodify の構文」を参照してください。
   - 構成設定エントリの属性の説明は、B-5 ページの「構成設定エントリのスキーマ要素」を参照してください。

システム操作属性の設定

操作**属性**は、アプリケーション属性とは異なり、ディレクトリ自体の操作に関係します。一部の操作情報（エントリのタイムスタンプなど）は、サーバーを制御するためにディレクトリによって指定されます。アクセス情報などのその他の操作情報は、管理者が定義し、ディレクトリ・プログラムの処理時に、そのプログラムによって使用されます。システム操作属性を設定するには、スーパー・ユーザー権限を持っている必要があります。

この項では、次の項目について説明します。

- Oracle Directory Manager を使用したシステム操作属性の設定
- ldapmodify を使用したシステム操作属性の設定

関連項目： 2-4 ページの「属性情報の種類」

Oracle Directory Manager を使用したシステム操作属性の設定

接続している各 Oracle ディレクトリ・サーバーの操作属性の一部は、**Oracle Directory Manager** を使用して表示および設定できます。この操作を実行するには、ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」を展開して、ディレクトリ・サーバーを選択します。右側のペインにシステム操作属性が表示されます。

Oracle Directory Manager に表示されるシステム操作属性フィールドの説明は、C-27 ページの表 C-34 を参照してください。

ldapmodify を使用したシステム操作属性の設定

システム操作属性を変更するには、ldapmodify を使用します。変更可能なシステム操作属性については、B-40 ページの表 B-34 を参照してください。

関連項目： ldapmodify の詳細とそのオプションのリストは、A-32 ページの「ldapmodify の構文」を参照してください。

ネーミング・コンテキストの管理

ユーザーが特定のネーミング・コンテキストを検索できるように、それらのネーミング・コンテキストを公開できます。この項では、次の項目について説明します。

- Oracle Directory Manager を使用したネーミング・コンテキストの公開
- ldapmodify を使用したネーミング・コンテキストの公開

ネーミング・コンテキストを公開するには、各ネーミング・コンテキストの最上位エントリを、ルート DSE の namingContexts 属性の値として指定します。たとえば、3 つの主なネーミング・コンテキストを持ったディレクトリ情報ツリーがあり、それらの最上位エントリが c=uk、c=us および c=de であるとします。これらのエントリが namingContexts 属性の値として指定されている場合、適切なフィルタを指定することによって、ユーザーはルート DSE の検索によってそれらの情報を検索できます。ユーザーは、特に c=de ネーミング・コンテキストに絞り込むなど、検索条件を詳細に指定できます。

ネーミング・コンテキストの公開には、Oracle Directory Manager または ldapmodify を使用できます。namingContexts 属性は複数値なので、複数のネーミング・コンテキストを指定できます。

公開されたネーミング・コンテキストを検索するには、検索フィルタとして objectClass =* を指定して、ルート DSE でベース検索を実行します。検索された情報には、namingContexts 属性で指定したエントリが含まれています。

ネーミング・コンテキストを公開する前に、次のことを確認してください。

- 自分がルート DSE への必要なアクセスを持ったディレクトリ管理者であること
- そのネーミング・コンテキストの最上位エントリがディレクトリに存在すること

Oracle Directory Manager を使用したネーミング・コンテキストの公開

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」を展開して、ネーミング・コンテキストを指定するディレクトリ・サーバーを選択します。そのディレクトリ・サーバーに対応するタブ・ページが右側のペインに表示されます。
2. 「**システム操作属性**」タブ・ページの「**ネーミング・コンテキスト**」フィールドに、公開するネーミング・コンテキストの最上位識別名を入力します。「**参照**」を選択して検索ウィンドウを開くこともできます。
3. 「**適用**」を選択します。

ldapmodify を使用したネーミング・コンテキストの公開

次のサンプル LDIF ファイルは、ネーミング・コンテキストとしてエントリ c=uk を指定しています。

```
dn:
changetype: modify
add: namingcontexts
namingcontexts: c=uk
```

スーパー・ユーザー、ゲスト・ユーザーおよびプロキシ・ユーザーの管理

スーパー・ユーザーは、一般的にはディレクトリ情報へのあらゆるアクセスが可能な、特別なディレクトリ管理者です。スーパー・ユーザーのデフォルトのユーザー名は `orcladmin`、デフォルトのパスワードは `welcome` です。オラクル社は、このパスワードをすぐに変更することをお薦めします。

ゲスト・ユーザーは、匿名ユーザーではなく、特定のユーザー・エントリも持っていないユーザーです。ゲスト・ユーザーのデフォルトのユーザー名は `guest`、デフォルトのパスワードは `guest` です。

通常、**プロキシ・ユーザー**は、ファイアウォール、Oracle Delegated Administration Services のようなアプリケーション、RADIUS サーバーなどの中間層を持つ環境で使用されます（12-5 ページの「間接認証」を参照）。プロキシ・ユーザーのデフォルトのユーザー名は `proxy`、デフォルトのパスワードは `proxy` です。

Oracle Directory Manager または ldapmodify を使用すると、スーパー・ユーザー、ゲスト・ユーザーおよびプロキシ・ユーザーのユーザー名とパスワードを管理できます。

> **関連項目：** アクセス権限の設定方法は、第 14 章「ディレクトリ・アクセス制御」を参照してください。

> **注意：** ユーザー名またはパスワードを指定せずに Oracle Directory Manager にログインすることもできます。この場合、匿名ユーザーに指定されている権限が与えられます。匿名ユーザーには、最小限の権限が与えられます。

この項では、次の項目について説明します。

- Oracle Directory Manager を使用したスーパー・ユーザー、ゲスト・ユーザーおよびプロキシ・ユーザーの管理
- ldapmodify を使用したスーパー・ユーザー、ゲスト・ユーザーおよびプロキシ・ユーザーの管理

Oracle Directory Manager を使用したスーパー・ユーザー、ゲスト・ユーザーおよびプロキシ・ユーザーの管理

> **注意：** スーパー・ユーザー、ゲスト・ユーザーおよびプロキシ・ユーザーのパスワードは、デフォルトで暗号化されます。クリア・テキストで送信するために、これらのパスワードを変更することはできません。

Oracle Directory Manager を使用して、スーパー・ユーザー、ゲスト・ユーザーまたはプロキシ・ユーザーのユーザー名またはパスワードを設定する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」を展開して、ディレクトリ・サーバーを選択します。そのサーバーに対応するタブ・ページが右側のペインに表示されます。
2. 「**システム・パスワード**」タブを選択します。このページに、各タイプのユーザーに対するカレント・ユーザー名とパスワードが表示されます。各パスワードは、パスワードのフィールドには表示されないことに注意してください。
3. C-32 ページの表 C-35 で説明するとおり、「**システム・パスワード**」タブ・ページ内の該当するフィールドを編集します。変更内容を保存するには、「**適用**」を選択します。

ldapmodify を使用したスーパー・ユーザー、ゲスト・ユーザーおよびプロキシ・ユーザーの管理

スーパー・ユーザー、ゲスト・ユーザーまたはプロキシ・ユーザーのユーザー名またはパスワードを変更するには、ldapmodify を使用して該当する属性を変更します。

表 5-1 スーパー・ユーザー、ゲスト・ユーザーおよびプロキシ・ユーザーのユーザー名、パスワードおよび属性

ユーザー名	パスワード	属性
スーパー・ユーザーの名前	orclsupassword	orclsuname
ゲスト・ユーザーの名前	orclgupassword	orclguname
プロキシ・ユーザーの名前	orclprpassword	orclprname

たとえば、スーパー・ユーザーのパスワードを *superuserpassword* に変更するには、ldapmodify で、次のように記述した LDIF ファイルを使用して**ディレクトリ固有のエントリ**（DSE）を変更します。

```
dn:
changetype:modify
replace:orclsupassword
orclsupassword:superuserpassword
```

> **関連項目：** ldapmodify の構文と使用方法は、A-32 ページの「ldapmodify の構文」を参照してください。

アクティブ・サーバー・インスタンスの情報の表示

任意のアクティブ・ディレクトリ・サーバー・インスタンスに関する情報（タイプ、インスタンス番号、デバッグ・レベル、ホスト名および構成パラメータなど）を表示するには、**Oracle Directory Manager** を使用します。この手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」を展開して、ディレクトリ・サーバーを選択します。そのディレクトリ・サーバー・インスタンスに対応するタブ・ページが右側のペインに表示されます。
2. 「**サーバー管理**」タブを選択します。ここには、すべてのアクティブ・ディレクトリ・サーバー・インスタンスの基本的な情報（タイプ、インスタンス番号、デバッグ・レベルおよびホスト名）が表示されます。
3. 特定のディレクトリ・サーバー・インスタンスの構成パラメータを参照するには、そのディレクトリ・サーバー・インスタンスを選択して、「**プロパティの表示**」を選択します。「サーバー・プロセス」ダイアログ・ボックスに、選択したディレクトリ・サーバー・インスタンスの構成パラメータが表示されます。このダイアログ・ボックスでは、構成パラメータを変更できないことに注意してください。変更するには、基となっている構成設定エントリを変更する必要があります。

> **関連項目：** 構成設定エントリの変更方法は、5-4 ページの「Oracle Directory Manager を使用したサーバーの構成設定エントリの管理」を参照してください。

アイドル状態の LDAP 接続のクローズ

アイドル状態の LDAP 接続がクローズするまでのアイドル時間を分単位で指定できます。この処理を行うには、B-40 ページの表 B-34 で説明する `orclLDAPconnTimeout` 属性に値を設定します。

Oracle Internet Directory データベース・サーバー接続時のパスワードの変更

Oracle Internet Directory は、独自に指定された Oracle データベースへの接続時にパスワードを使用します。Oracle Internet Directory インストール時のこのパスワードのデフォルトは、Oracle Application Server 管理者のパスワードと同じです。**OID データベース・パスワード・ユーティリティ**を使用すると、このパスワードを変更できます。

関連項目： A-129 ページの「OID データベース・パスワード・ユーティリティ（oidpasswd）構文」

別名エントリの間接参照

エントリに非常に長く複雑な識別名が付いている場合があるため、Oracle Internet Directory では、別名オブジェクトを使用してエントリの管理を簡単にできます。別名を使用してオブジェクトを検索（参照）すると、別名が間接参照され、その別名が指し示すオブジェクトが戻されます。たとえば、別名 `Server1` は、完全修飾された識別名 `dc=server1,dc=us,dc=myCompnay,dc=com` を指し示すように間接参照できます。この機能によって、厳密には階層構造でない構造も開発できます。

この項では、別名エントリを追加、検索および変更する方法の例について説明し、メッセージのリストを示します。この項では、次の項目について説明します。

- 別名エントリの概要
- 例 : 別名エントリ間接参照の使用方法
- 成功メッセージとエラー・メッセージ

別名エントリの概要

別名エントリは、オブジェクト・クラス `alias` を使用して、ディレクトリ内のオブジェクト・エントリと区別します。このオブジェクト・クラスの定義は次のとおりです。

```
(2.5.6.1 NAME 'alias' SUP top STRUCTURAL MUST aliasedObjectName)
```

別名エントリには、`aliasedObjectName` 属性も含まれます。この属性には、別名が指し示すオブジェクトの識別名が入ります。この属性の定義は次のとおりです。

```
(2.4.5.1 NAME 'aliasedObjectName" EQUALITY distinguishedNmameMatch SYNTAX
1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE)
```

図 5-2 およびその後に続く説明では、別名エントリの間接参照の例を示します。

図 5-2 別名エントリの例

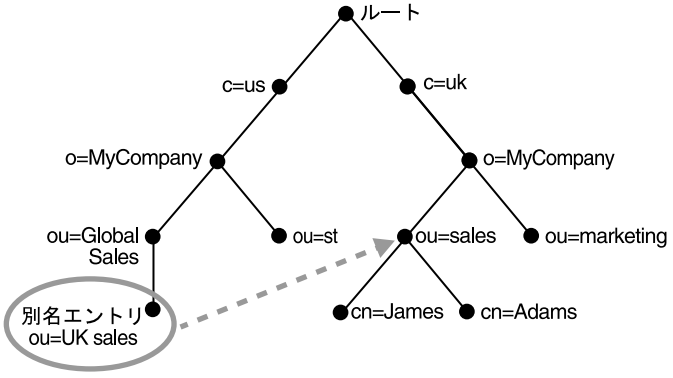


図 5-2 で、`ou=uk sales,ou=global sales,o=myCompany,c=us` は、`ou=sales,o=myCompany,c=uk` エントリを指し示す別名エントリです。

`ou=uk sales,ou=global sales,o=oracle,c=us` を参照すると、その参照は、ディレクトリ・サーバーによって実際のエントリ `ou=sales,o=oracle,c=uk` に自動的に変更されます。

例 : 別名エントリ間接参照の使用方法

この項では、次の項目について説明します。

- 例 : 別名エントリの追加
- 例 : 別名エントリによるディレクトリの検索
- 例 : 1 レベルの検索
- 例 : サブツリーの検索
- 例 : 別名エントリの変更

例 : 別名エントリの追加

別名エントリを追加するには、LDIF の通常のエントリ、および実際のエントリを指し示す別名エントリを作成します。この例の手順を実行すると、5-17 ページの図 5-3 に示すツリーが生成されます。

1. 次のエントリを持つサンプル LDIF ファイル My_file.ldif を作成します。

```
dn: c=us
c: us
objectclass: country

dn: o=oracle, c=us
o: oracle
objectclass:organization

dn: ou=Area1, c=us
objectclass: alias
aliasedObjectName: o=oracle, c=us

dn: cn=John Doe, o=oracle, c=us
cn: John Doe
objectclass: person

dn: cn=President, o=oracle, c=us
objectclass: alias
aliasedobjectname:  cn=John Doe, o=oracle, c=us
```

2. 次のコマンドを使用して、これらのエントリをディレクトリに追加します。

```
ldapadd -p port -h host -f  My_file.ldif
```

注意 : 親が別名エントリである別名エントリを追加すると、ディレクトリ・サーバーはエラーを戻します。

関連項目 : エラー・メッセージは、5-19 ページの「エントリ別名間接参照メッセージ」を参照してください。

図 5-3 My_file.ldif の作成結果を示すツリー

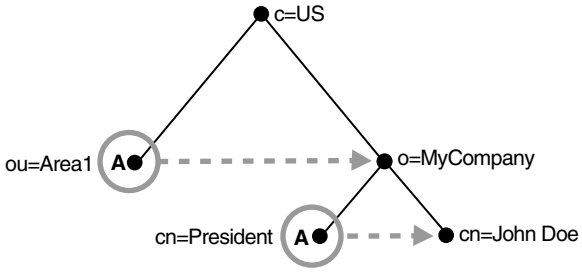


図 5-3 の文字 A は、別名エントリを表します。

- ou=Area1 は、o=MyCompany を指し示す別名です。
- cn=President は、cn=John Doe を指し示す別名です。

例 : 別名エントリによるディレクトリの検索

指定する検索ごとに設定できるフラグがあります。検索は、指定したフラグに基づいて実行されます。

別名の間接参照に関係するフラグは、-a never および -a find です。

デフォルトでは、ldapsearch の間接参照フラグは -a never で、ディレクトリ・サーバーは別名エントリに対する間接参照を行いません。

例 : ベースの検索 ベース検索は、指定した別名エントリの最上位レベルを検索します。

次の例は、間接参照フラグを -a find に設定し、フィルタとして "objectclass=*" を使用して ou=Area1,c=us のベース検索を行う場合を示しています。

```
ldapsearch -p port -h host -b "ou=Area1,c=us"  -a find -s base "objectclass=*"
```

ディレクトリ・サーバーは、ベース検索時に、検索要求に指定されたベースを検索し、その位置をユーザーに戻します。ただし、この例のようにベースが別名エントリで、検索要求に -a find が指定されている場合、ディレクトリ・サーバーは、別名エントリを自動的に間接参照し、その別名エントリが指し示すエントリを戻します。この例では、検索で ou=Area1,c=us（別名エントリ）が間接参照され、o=MyCompany,c=us が戻されます。

例 : 1 レベルの検索 1 レベル検索では、指定したベース・レベルに対する子のみを検索します。

次の例は、間接参照フラグを -a find に設定し、フィルタとして "objectclass=*" を使用して "ou=Area1,c=us" の 1 レベル検索を行う場合を示しています。

```
ldapsearch -p port -h host -b "ou=Area1,c=us"  -a find -s one "objectclass=*"
```

ディレクトリ・サーバーは、2 つの手順で検索を実行します。

1. 検索要求に指定されたベースを検索します。
2. ベースの位置を特定すると、このベース下のすべての 1 レベル・エントリを検索して、フィルタ基準と一致するエントリを戻します。

この例では、検索要求に -a find が指定されているため、ディレクトリ・サーバーは、ベースの検索（最初の手順）中に自動的に間接参照しますが、ベース下の 1 レベルの別名エントリは間接参照しません。したがって、この検索では ou=Area1,c=us（別名エントリ）が間接参照され、o=MyCompany,c=us 下の 1 レベル・エントリが検索されます。1 レベル・エントリの 1 つは、間接参照されずにそのまま戻される cn=President,o=MyCompany,c=us です。

したがって、この検索では、cn=President,o=MyCompany,c=us および cn=John Doe,o=MyCompany,c=us が戻されます。

例 : サブツリーの検索 サブツリー検索は、ベース、子および孫を検索します。

次の例は、間接参照フラグを -a find に設定し、フィルタとして "objectclass=*" を使用して "ou=Area1,c=us" のサブツリー検索を行う場合を示しています。

```
ldapsearch -p port -h host -b "ou=Area1,c=us" -a find -s one "objectclass=*"
```

ディレクトリ・サーバーは、2 つの手順で検索を実行します。

1. 検索要求に指定されたベースを検索します。
2. ベースの位置を特定すると、このベース下のすべてのエントリを検索して、フィルタ基準と一致するエントリを戻します。

この例では、検索要求に -a find が指定されているため、ディレクトリ・サーバーは、ベースの検索（最初の手順）中に自動的に間接参照しますが、ベース下の別名エントリは間接参照しません。したがって、検索では、ou=Area1,c=us（別名エントリ）が間接参照され、o=MyCompany,c=us 下のエントリが検索されます。エントリの 1 つは、間接参照されずにそのまま戻される cn=President,o=MyCompany,c=us です。

したがって、この検索では次の情報が戻されます。

- o=MyCompany,c=us
- cn=john doe,o=MyCompany,c=us
- cn=President,o=MyCompany,c=us

例 : 別名エントリの変更

次の例は、別名エントリを変更する方法を示しています。次のエントリを持つサンプル LDIF ファイル My_file.ldif を作成します。

```
dn: cn=President, o=MyCompany, c=us
changetype : modify
replace: aliasedobjectname
aliasedobjectname:  cn=XYZ, o=MyCompany, c=us
```

次のコマンドを使用して、別名エントリを変更します。

```
ldapmodify -p port -h host -f My_file.ldif
```

成功メッセージとエラー・メッセージ

説明列に示した別名の問題が見つかると、次のメッセージが戻ります。

表 5-2 エントリ別名間接参照メッセージ

メッセージ	意味
別名に問題があります	次のいずれかの問題が発生しました。 ■ 別名を間接参照しましたが、その別名がディレクトリ情報ツリー内のエントリを指し示していません。 ■ 親が別名である別名エントリを追加しようとしました。
別名の間接参照に問題があります	アクセス制御上の問題であるため、別名を間接参照できません。
該当するオブジェクトがありません	検索要求に指定されたベース識別名をサーバーで検索できません。
識別名の構文に誤りがあります	aliasedObjectName に指定された値に無効な識別名の構文が含まれている場合に別名エントリを追加または変更すると、ディレクトリ・サーバーがクライアントにこのエラー・メッセージを戻します。
成功しました	クライアント操作が正常に完了しました。 間接参照ターゲットが見つかり、検索要求に指定したフィルタと一致しない場合、サーバーは一致エントリなしで成功メッセージを戻します。
不十分なアクセス権限	ユーザーが間接参照されたエントリへのアクセス権限を持っていません。

分散環境でのディレクトリ・サーバーの位置の特定

特定のエントリに対して操作を実行するには、クライアントが、そのエントリが常駐するサーバーを検出できる必要があります。分散環境では、サーバーの位置に関する情報は、次の 2 通りの方法で入手できます。

- 静的には、クライアント・ホストに格納されているディレクトリ・サーバー構成ファイル（ldap.ora）を使用。
- 動的には、ドメイン・ネーム・システム（DNS）を使用。この場合、サーバーの位置に関する情報は、中央ドメイン・ネーム・サーバーに格納され、管理されます。クライアントは、要求処理時に、ドメイン・ネーム・サーバーからこの情報を動的に取り出します。

この項では、サーバー情報の位置を特定する 2 通りの方法について説明します。この項では、次の項目について説明します。

- ディレクトリ・サーバー構成ファイル（ldap.ora）を使用した静的ディレクトリ・サーバーの検出
- ドメイン・ネーム・システム（DNS）を使用した動的ディレクトリ・サーバーの検出

関連項目： http://www.ietf.org の Michael P. Armijo 氏他による「Discovering LDAP Services with DNS」（draft-ietf-ldapext-locate-08.txt）

http://www.ietf.org の Internet RFC 2782 の「A DNS RR for specifying the location of services (DNS SRV)」を参照してください。

ディレクトリ・サーバー構成ファイル（ldap.ora）を使用した静的ディレクトリ・サーバーの検出

この方法では、クライアントは、ディレクトリ・エントリに対して操作を実行する場合、クライアント・ホストに格納されているディレクトリ・サーバー構成ファイル（ldap.ora）からディレクトリ・サーバーの位置情報を取得します。このファイルには、次の要件を指定する構成パラメータが含まれています。

- ディレクトリ・サーバーのタイプ（Oracle Internet Directory、Microsoft Active Directory、SunONE Directory Server など）
- ディレクトリ・サーバーの位置
- クライアントまたはサーバーが、データベース・サービス接続用の接続識別子の検索または構成に使用するデフォルトのディレクトリ・エントリ

ファイル ldap.ora は LDAP クライアントのファイル・システムに常駐しています。クライアントがこのファイルを検索する場合、次の優先順位に従います。

- まず、環境変数 LDAP_ADMIN によって指し示されるファイル・システム・ディレクトリを検索します。
- 次に、ディレクトリ *ORACLE_HOME*/ldap/admin（Microsoft Windows NT では *ORACLE_HOME*¥ldap¥admin）を検索します。
- 次に、環境変数 TNS_ADMIN によって指し示されるファイル・システム・ディレクトリを検索します。
- 最後に、ディレクトリ *ORACLE_HOME*/network/admin（Microsoft Windows NT では *ORACLE_HOME*¥network¥admin）を検索します。

ファイル ldap.ora が複数の位置に存在する場合、優先順位の高い位置を使用します。

静的方法を使用してディレクトリ・サーバーを検出すると、管理オーバーヘッドが増加する場合があります。たとえば、ldap.ora ファイルがクライアント・ホストに格納されているため、管理者は、ディレクトリ・サーバーのホスト名やポート番号を変更するたびに、すべてのクライアント上でそのファイルを更新する必要があります。このオーバーヘッドの増加を回避するには、アプリケーションでドメイン・ネーム・システム（DNS）を使用して、動的にディレクトリ・サーバーを検出します。

ドメイン・ネーム・システム（DNS）を使用した動的ディレクトリ・サーバーの検出

ドメイン・ネーム・システム（DNS）は、ドメイン名の位置を特定し、それをコンピュータの実際のアドレスに変換する動的方法です。この変換プロセスは、ディレクトリ・サーバーの位置に関する情報が格納されている中央ドメイン・ネーム・サーバーによって処理されます。

ネットワーク管理者がディレクトリ・サーバーの位置に関する必要な情報をドメイン・ネーム・サーバーに入力すると、クライアントは、ldap.ora ファイルからではなく、そのサーバーから情報を取り出すことができます。

クライアントが DNS を使用してディレクトリ・サーバーの位置を特定する場合は、次の手順を完了しておく必要があります。

- ネットワーク管理者がドメイン・ネーム・サーバーに DNS サービス・ロケーション・レコード（SRV）を入力しておく必要があります。
- クライアント・アプリケーションで識別名をドメイン名にマッピングできるようにしておく必要があります。

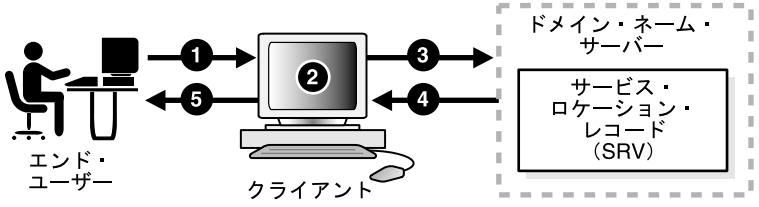
クライアントが DNS を使用してディレクトリ・サーバーの位置を特定する方法

クライアントは、エントリが常駐するディレクトリ・サーバーを検出するためにドメイン・ネーム・サーバーと通信します。具体的には、ドメイン・ネーム・サーバーにドメイン名を提供します。ドメイン名は、必要なディレクトリ・サーバーが配置されている場所を指定します。

クライアントは、ドメイン名を生成するためにユーザーが入力した識別名からドメイン・コンポーネントを抽出します。たとえば、識別名 `cn=John Doe,ou=accounting,dc=example,dc=net` の場合、ドメイン・コンポーネントは `dc=example,dc=net` です。このドメイン・コンポーネントは、要求したエントリが常駐するサーバーを表します。次に、クライアントは、そのドメイン名コンポーネントをドメイン・ネーム・サーバーが認識する形式（`example.net`）のドメイン名に変換します。

図 5-4 とその後の説明で、クライアントの視点からディレクトリ・サーバーの位置を特定するプロセスを示します。

図 5-4 DNS を使用してディレクトリ・サーバーの位置を特定するクライアント



1. ディレクトリ・エントリに対して操作を実行するユーザーは、エントリの識別名（DN）をクライアントに入力します。たとえば、`cn=John Doe,ou=accounting,dc=example,dc=net` です。
2. クライアントは、ドメイン・ネーム・サーバーと通信するために、識別名のドメイン・コンポーネントをドメイン名に変換します。ここで使用している例では、クライアントはその識別名のドメイン・コンポーネント `dc=example,dc=net` をドメイン名 `example.net` に変換します。
3. クライアントは、指定したドメイン名を持つ SRV リソース・レコードについてドメイン・ネーム・サーバーに問い合せます。
4. ドメイン・ネーム・サーバーは、指定したドメイン名と一致する SRV リソース・レコードを戻します。これらのリソース・レコードには、要求したエントリを含むディレクトリ・サーバーのホスト名情報が格納されています。ドメイン・ネーム・サーバーによって一致する SRV リソース・レコードを検出できない場合は、エラー・メッセージが戻されます。

5. クライアントは、このレコードを解析します。これらのレコードからディレクトリ・ホスト名情報を抽出し、ユーザーに戻します。

関連項目：

- `http://www.ietf.org` の P. Mockapetris 氏による「Domain Names: Concepts and Facilities (RFC 1034)」を参照してください。
- `http://www.ietf.org` の P. Mockapetris 氏による「Domain Names—Implementation and Specification (RFC 1035)」を参照してください。

注意： ドメイン・ネーム・サーバーは、必要なすべての SRV レコードをローカルに格納するか、または他のドメイン・ネーム・サーバーから取得します。また、要求された情報を検出できない場合は、エラー・メッセージを戻します。別のドメイン・ネーム・サーバーに対する参照は戻しません。

ドメイン・ネーム・システムへのディレクトリ・サーバーの登録

ディレクトリ・サーバーに関するサーバーの位置情報を登録するには、DNS サービス・ロケーション・レコード（SRV）をドメイン・ネーム・サーバーに入力します。SRV レコードには次の情報が格納されています。

- LDAP サービスを提供するサーバーの DNS 名
- 対応するポート番号
- クライアントが複数のサーバーから該当するサーバーを選択できるようにするパラメータ

SRV リソース・レコードによって、管理者は、1 つのドメインに対して複数のサーバーを使用し、サービスをホスト間で簡単に移動し、一部のホストをサービス用のプライマリ・サーバーとして、残りをバックアップとして指定することができます。

SRV レコードは、Oracle Internet Directory サーバーに固有の形式または標準形式にできます。Oracle Internet Directory サーバーに関する情報の場合は、Oracle Internet Directory 固有の形式をお薦めします。クライアントは、初めてドメイン・ネーム・サーバーに問い合せる場合、Oracle Internet Directory 固有の形式を持つ SRV レコードを検索します。この形式のレコードを検出できない場合は、標準形式の SRV レコードを問い合せます。

SRV レコード用の Oracle Internet Directory 固有の形式

Oracle Internet Directory 固有の形式は、次のとおりです。

```
_Service._Proto._product.Domain TTL Class Type Priority Weight Port Target
```

表 5-3 に引数を示します。次に、Oracle Internet Directory 固有の形式を使用した SRV レコードの例を示します。

```
_ldap._tcp._oid.acme.com 0 IN SRV 0 1 389 ldap.acme.com
```

SRV レコード用の標準形式

標準形式は、次のとおりです。

```
_Service._Proto.Domain TTL Class Type Priority Weight Port Target
```

表 5-3 に引数を示します。次に、非 SSL ベースのディレクトリ・サーバー用の標準形式を使用した SRV レコードの例を示します。

```
_ldap._tcp.acme.com 0 IN SRV 0 1 389 ldap.acme.com
```

表 5-3 サービス・ロケーション・レコード（SRV）の引数

引数	説明
Service	非 SSL ベースのサーバーの場合、この引数の値は `ldap` です。SSL ベースのサーバーの場合は、`ldaps` です。
Proto	常に、値は `tcp` です。
Product	常に、値は `oid` です。
Domain	ドメイン名。通常は、ディレクトリ・サーバーによって作成されたネーミング・コンテキストの DN をドメイン名に変換して取得されます。 **関連項目：**5-22 ページの「クライアントが DNS を使用してディレクトリ・サーバーの位置を特定する方法」を参照してください。
TTL	有効期間。この引数は標準 DNS の意味を持っています。情報のソースを再度問い合せるまでリソース・レコードをキャッシュしておくことができる時間を指定します。
Class	この引数は標準 DNS の意味を持っています。SRV レコードは IN クラスで発生します。
Type	すべての SRV レコードで、この引数の値は SRV です。
Priority	ディレクトリ・サーバーの優先順位。クライアントは、優先順位番号が一番小さいターゲット・ホストと通信する必要があります。

表 5-3 サービス・ロケーション・レコード（SRV）の引数（続き）

引数	説明
Weight	サーバー選択メカニズム。この引数は、同じ優先順位を持つエントリに対して相対的な重みを指定します。複数の SRV が同じ優先順位を持っている場合は、次のプロトコルに従って順位付けされます。 **1.** 次に通信するターゲットを選択するために、順位付けされていないすべての SRV リソース・レコードを任意の順序で並べます。ただし、重み 0 のレコードはすべてリストの先頭に置きます。 **2.** これらのリソース・レコードの重みの合計を計算します。また、各リソース・レコードには、選択した順序での重みの累計を関連付けます。 **3.** 0 から計算した合計までの間の一様乱数を選択し、選択した順序で、重みの累計値が初めて選択した乱数以上となるリソース・レコードを選択します。選択した SRV リソース・レコードに指定されているターゲット・ホストが、クライアントによって次に通信されるホストです。 **4.** 順位付けされていない SRV リソース・レコードのセットから、この SRV リソース・レコードを削除します。 **5.** 順序付けされていない SRV リソース・レコードに前述のアルゴリズムを適用して、次のターゲット・ホストを選択します。 **6.** 順位付けされていない SRV リソース・レコードがなくなるまで、この順位付けプロセスを続けます。 **7.** このプロセスを各優先順位に対して繰り返します。
Port	ディレクトリ・サービス用のターゲット・ホストのポート。
Target	ディレクトリ・サーバーが稼働しているホストのドメイン名。

注意： ディレクトリ・サーバーが別のホストに移動された場合、または別のポートで稼働している場合は、対応する SRV リソース・レコードをそれに応じて更新する必要があります。

6

ディレクトリ・スキーマの管理

この章では、Oracle Internet Directory のオブジェクト・クラスと属性を管理する方法を説明します。

この章では、次の項目について説明します。

ディレクトリ・スキーマの概要

ディレクトリ・スキーマには、次の機能があります。

- ディレクトリに格納できるオブジェクトの種類に関する規則を含んでいます。
- 検索などの処理時にディレクトリ・サーバーとクライアントが情報を扱う方法の規則を含んでいます。
- ディレクトリに格納されているデータの整合性と品質をメンテナンスするのに役立ちます。
- データの重複を削減します。
- ディレクトリに対応したアプリケーションがディレクトリ・オブジェクトにアクセスしたり変更したりするための、予測可能な方法を提供します。

ディレクトリ・**スキーマ**には、ディレクトリ情報ツリー内のデータを組織する方法に関するすべての情報（**オブジェクト・クラス**、**属性**、**一致規則**、構文などのメタデータ）が含まれています。この情報は、**サブエントリ**と呼ばれる特別なクラスのエントリに格納されます。Oracle Internet Directory は、LDAP バージョン 3 の規格に従って、`subSchemaSubentry` と呼ばれるサブエントリにこの情報を格納します。

`subSchemaSubentry` を変更することによって新規のオブジェクト・クラスとオブジェクトを追加できます。ただし、Oracle Internet Directory ですでにサポートされているもの以外に、新規の一致規則や構文を追加することはできません。

ディレクトリのオブジェクト・クラス

この項では、次の項目について説明します。

- オブジェクト・クラス管理
- Oracle Directory Manager を使用したオブジェクト・クラスの管理
- コマンドライン・ツールを使用したオブジェクト・クラスの管理

オブジェクト・クラス管理

この項では、**オブジェクト・クラス**の追加方法と変更方法を説明します。ディレクトリ内のベース・スキーマの追加または変更を行う前に、ディレクトリのコンポーネントの基本概念を理解しておいてください。

関連項目：

- オブジェクト・クラスの概要は、2-7 ページの「オブジェクト・クラス」を参照してください。
- Oracle Internet Directory とともにインストールされるスキーマ要素のリストは、付録 B「Oracle Internet Directory のスキーマ要素」を参照してください。

オブジェクト・クラスの追加のガイドライン

ディレクトリ・エントリを追加する場合は、そのディレクトリ・エントリを 1 つ以上のオブジェクト・クラスと関連付けます。各オブジェクト・クラスには、新規エントリと関連付ける属性が含まれています。たとえば、従業員に関するエントリを作成する場合は、そのエントリを person オブジェクト・クラスと関連付けることができます。このオブジェクト・クラスには、その従業員エントリと関連付ける多くの属性（名前、住所、電話番号など）が含まれています。

継承 各オブジェクト・クラスは、スーパークラスの階層から派生し、これらのスーパークラスからの属性を継承します。デフォルトでは、すべてのオブジェクト・クラスは top オブジェクト・クラスから継承します。オブジェクト・クラスをエントリに割り当てると、エントリは、そのオブジェクト・クラスとそのオブジェクト・クラスのスーパークラスの両方の属性をすべて継承します。

オブジェクト・クラスの必須属性とオプション属性 エントリがスーパークラスから**継承**する属性は、必須またはオプションのいずれかです。オプション属性の値は、ディレクトリ・エントリに存在している必要はありません。

オブジェクト・クラスに対して、属性が必須であるか、オプションであるかを指定できます。ただし、この指定は、そのオブジェクト・クラスにのみバインドされます。同じ属性を別のオブジェクト・クラスに割り当てる場合は、そのオブジェクト・クラスに対して必須であるか、オプションであるかを指定しなおすことができます。次の操作が可能です。

- 既存の標準オブジェクト・クラスからの選択
- 標準以外の新規オブジェクト・クラスの追加と既存属性の割当て
- 既存のオブジェクト・クラスの変更、異なる属性のセットへの割当て
- 既存の属性の追加と変更

関連項目： 6-11 ページの「属性管理の概要」

上位から下位の順序でのエントリの追加 エントリは上位から下位の順序で追加する必要があります。エントリを追加する場合は、そのすべての親エントリがディレクトリに存在している必要があります。同様に、オブジェクト・クラスと属性を参照するエントリを追加するときは、参照先のオブジェクト・クラスと属性が、ディレクトリ・スキーマにすでに存在している必要があります。ディレクトリ・サーバーには標準のディレクトリ・オブジェクトの完全なセットが用意されているため、通常、問題は発生しません。

オブジェクト・クラスの増加 エントリに操作を追加または実行する場合、そのエントリに対応付けられたスーパークラスの階層全体を指定する必要はありません。オブジェクト・クラスの増加と呼ばれるこの機能によって、リーフ・オブジェクト・クラスの指定のみで済みます。Oracle Internet Directory は、リーフ・オブジェクト・クラスの階層を解決して、情報モデル制約を規定します。たとえば、`inetOrgPerson` オブジェクト・クラスは、そのスーパークラスとして、`top`、`person` および `organizationalPerson` を持っています。ある人物を表すエントリを作成する場合、オブジェクト・クラスとして指定する必要があるのは `inetOrgPerson` のみです。Oracle Internet Directory は、対応するスーパークラス `top`、`person` および `organizationalPerson` によって定義されたスキーマ制約を規定します。

オブジェクト・クラスを追加するときは、次のガイドラインに注意してください。

- すべての構造型オブジェクト・クラスには、スーパークラスとして `top` を設定する必要があります。
- オブジェクト・クラスの名前とオブジェクト識別子は、すべてのスキーマ・コンポーネントを通して一意であることが必要です。
- オブジェクト・クラスで参照されるスキーマ・コンポーネント（スーパークラスなど）は、すでに存在している必要があります。
- 抽象型オブジェクト・クラスの場合は、スーパークラスも抽象型であることが必要です。
- スーパークラスの必須属性は、新規オブジェクト・クラスでオプション属性に再定義することが可能です。同様に、スーパークラスのオプション属性は、新規オブジェクト・クラスで必須属性に再定義できます。

注意： Oracle Internet Directory のスキーマ・オブジェクトには、それぞれ特定の制限があります。たとえば、一部のオブジェクトは変更できません。これらの制限事項は、ここでは制約や規則として説明しています。

関連項目： これらの用語の概念の説明は、2-8 ページの「サブクラス、スーパークラスおよび継承」を参照してください。

オブジェクト・クラスの変更のガイドライン

この項では、既存のオブジェクト・クラスに対して実行できる変更のタイプについて説明します。変更は、Oracle Directory Manager およびコマンドライン・ツールを使用して実行できます。

オブジェクト・クラスに対しては、次の変更を実行できます。

- 必須属性からオプション属性への変更
- オプション属性の追加
- スーパークラスの追加
- 抽象型オブジェクト・クラスから構造型または補助型オブジェクト・クラスへの変換（その抽象型オブジェクト・クラスが、別の抽象型オブジェクト・クラスのスーパークラスではない場合）

オブジェクト・クラスを変更するときは、次のガイドラインに注意してください。

- 標準の LDAP スキーマの一部であるオブジェクト・クラスは変更できません。ユーザー定義のオブジェクト・クラスは変更できます。
- 必要な属性が既存のオブジェクト・クラスに設定されていない場合は、補助型オブジェクト・クラスを作成して、必要な属性をそのオブジェクト・クラスに関連付けることができます。
- 既存のオブジェクト・クラスに、必須属性を追加できません。
- ベース・スキーマのオブジェクト・クラスは変更できません。
- 既存のオブジェクト・クラスから属性またはスーパークラスを削除できません。
- 構造型オブジェクト・クラスは、他の型のオブジェクト・クラスに変換できません。
- エントリがすでに関連付けられているオブジェクト・クラスは変更しないでください。

関連項目：

- 6-2 ページの「ディレクトリのオブジェクト・クラス」
- 6-9 ページの「コマンドライン・ツールを使用したオブジェクト・クラスの管理」

オブジェクト・クラスの削除のガイドライン

オブジェクト・クラスの削除に関しても、いくつかの制限事項があります。

- ベース・スキーマからオブジェクト・クラスを削除できません。
- ベース・スキーマ内にないオブジェクト・クラスは、他のスキーマ・コンポーネントから直接または間接的に参照されていないかぎり削除できます。たとえば、このようなオブジェクト・クラスを参照するディレクトリ・エントリがいくつか存在するとします。このオブジェクト・クラスを削除すると、これらのエントリにはアクセスできなくなります。

注意： Oracle Internet Directory は、前述の規則を強制していません。ここでは、ガイドラインとして紹介します。

Oracle Directory Manager を使用したオブジェクト・クラスの管理

この項では、Oracle Directory Manager を使用して、オブジェクト・クラスの検索、そのプロパティの表示、オブジェクト・クラスの追加、変更および削除を行う方法を説明します。

Oracle Directory Manager を使用したオブジェクト・クラスの検索

次の方法でオブジェクト・クラスを検索できます。

- オブジェクト・クラスのプロパティを選択する方法。たとえば、名前やオブジェクト識別子を選択します。
- 選択したプロパティの値を入力する方法。
- 選択したオブジェクト・クラスのプロパティと入力値との関連を指定する検索フィルタを選択する方法。「次の文字で始まる」または「完全に一致する」などのフィルタがあります。

この項では、オブジェクト・クラスの検索の入力方法を説明します。

オブジェクト・クラスを検索する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開します。
2. 「スキーマ管理」を選択します。「スキーマ管理」タブ・ページが、右側のペインに表示されます。
3. 右側のペインの右下の「**オブジェクト・クラスの検索**」ボタンを選択するか、メニュー・バーから「**編集**」を選択してから「**オブジェクト・クラスの検索**」を選択します。「検索 : オブジェクト・クラス」ダイアログ・ボックスが表示されます。

4. 検索基準バーの一番左のメニューから、検索するオブジェクト・クラスのプロパティを選択します。オプションのリストと説明は、C-16 ページの表 C-20 を参照してください。

   注意： 各オブジェクト・クラスでは、すべての属性が使用されているわけではありません。指定する属性が、探しているオブジェクト・クラス内の属性と実際に一致していることを確認してください。一致する属性がない場合は、検索に失敗します。

5. 検索基準バーの中央のメニューから、検索に使用するフィルタを選択します。オプションのリストと説明は、C-17 ページの表 C-21 を参照してください。
6. 検索基準バーの一番右のテキスト・ボックスに、検索するオブジェクト・クラスのプロパティの値を入力します。たとえば、名前が `orcl` で始まるすべてのオブジェクト・クラスを検索するには、検索基準バーの一番右のテキスト・ボックスに orcl と入力します。
7. 「**基準**」フィールドの下に、その次の表で説明する 5 つのボタンがあります。これらのボタンを使用すると、検索基準をさらに詳細に指定できます。
8. 「**検索**」を選択します。検索結果が、「検索 : オブジェクト・クラス」ダイアログ・ボックスの下部のウィンドウに表示されます。

Oracle Directory Manager を使用したオブジェクト・クラスのプロパティの表示

スキーマ内のすべてのオブジェクト・クラスを表示する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開します。
2. 「**スキーマ管理**」を選択します。
3. 右側のペインで、「**オブジェクト・クラス**」タブ・ページを選択します。

   個々のオブジェクト・クラスとその属性を調べるには、「**オブジェクト・クラス**」タブ・ページでオブジェクト・クラスを選択します。選択したオブジェクト・クラスのプロパティが、「オブジェクト・クラス」ダイアログ・ボックスに表示されます。

Oracle Directory Manager を使用したオブジェクト・クラスの追加

Oracle Directory Manager を使用してオブジェクト・クラスを追加する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開します。
2. 「**スキーマ管理**」を選択します。

3. 右側のペインで「**オブジェクト・クラス**」タブを選択し、ツールバーの「**作成**」ボタンをクリックします。「新規オブジェクト・クラス」ダイアログ・ボックスが表示されます。

   または、「**オブジェクト・クラス**」タブ・ページで、作成するオブジェクト・クラスに類似しているオブジェクト・クラスを選択した後、「**類似項目の作成**」を選択する方法もあります。「新規オブジェクト・クラス」ダイアログ・ボックスに選択したオブジェクト・クラスの属性が表示されます。選択したオブジェクト・クラスをテンプレートとして使用して、新規のオブジェクト・クラスを作成できます。

4. 「新規オブジェクト・クラス」ダイアログ・ボックスで、フィールドに情報を入力します。詳細は、C-19 ページの表 C-23 を参照してください。

5. 「**OK**」を選択します。

関連項目：

- 2-8 ページの「オブジェクト・クラスの型」
- 2-8 ページの「サブクラス、スーパークラスおよび継承」
- オブジェクト・クラスを追加する方法の詳細は、Oracle Directory Manager のオンライン・ヘルプを参照してください。

Oracle Directory Manager を使用したオブジェクト・クラスの変更

オブジェクト・クラスを変更する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開します。

2. 「**スキーマ管理**」を選択します。

3. 右側のペインで「**オブジェクト・クラス**」タブを選択した後、変更するオブジェクト・クラスを選択します。「オブジェクト・クラス」ダイアログ・ボックスが表示されます。

4. 「オブジェクト・クラス」ダイアログ・ボックスのフィールドで、情報を変更または追加します。詳細は、C-19 ページの表 C-23 を参照してください。

5. 「**OK**」を選択します。

関連項目：

- 2-8 ページの「オブジェクト・クラスの型」
- 2-8 ページの「サブクラス、スーパークラスおよび継承」

注意： 属性は、補助型オブジェクト・クラスまたはユーザー定義の構造型オブジェクト・クラスに追加できます。

関連項目：補助型オブジェクト・クラスへの属性の追加例は、6-10 ページの「例 : 補助型またはユーザー定義のオブジェクト・クラスへの新規属性の追加」を参照してください。

Oracle Directory Manager を使用したオブジェクト・クラスの削除

注意： ベース・スキーマからはオブジェクト・クラスを削除しないことをお薦めします。エントリの参照先であるオブジェクト・クラスを削除すると、そのエントリにアクセスできなくなります。

ベース・スキーマからオブジェクト・クラスを削除する場合は、使用中または将来使用する可能性があるオブジェクト・クラスを削除しないように注意してください。

Oracle Directory Manager を使用してオブジェクト・クラスを削除する手順は、次のとおりです。

1. ナビゲータ・ペインで「**スキーマ管理**」を選択します。
2. 右側のペインで「**オブジェクト・クラス**」タブ・ページを選択し、削除するオブジェクト・クラスを選択します。
3. 「**削除**」を選択します。

コマンドライン・ツールを使用したオブジェクト・クラスの管理

ディレクトリ・スキーマへのオブジェクト・クラスの追加や、既存のオブジェクト・クラスの変更にコマンドライン・ツールを使用できます。コマンドライン・ツールでは、入力ファイルが使用できます。さらに、いくつかのコマンドをスクリプトにまとめて、バッチ処理することもできます。

スキーマ・コンポーネントを追加または変更するには、ldapmodify を使用します。

関連項目： A-32 ページの「ldapmodify の構文」

例 : 新規オブジェクト・クラスの追加

この例では、LDIF 入力ファイル new_object_class.ldi に、次のようなデータが含まれています。

```
dn: cn=subschemasubentry
changetype: modify
add: objectclasses
objectclasses: ( 1.2.3.4.5 NAME 'myobjclass' SUP top STRUCTURAL MUST ( cn $ sn )
MAY ( telephonenumber $ givenname $ myattr ) )
```

左右のカッコとオブジェクト識別子の間には、必ず空白を入れてください。

このファイルをロードするには、次のコマンドを入力します。

```
ldapmodify -h myhost -p 389 -f new_object_class.ldi
```

この例は、myobjclass という名前の構造型オブジェクト・クラスを、オブジェクト識別子に 1.2.3.4.5、スーパークラスとして top、必須属性として cn と sn、オプション属性として telephonenumber、givenname および myattr を指定して追加しています。記述されている属性すべてが、コマンドの実行前に存在している必要があることに注意してください。

抽象型オブジェクト・クラスを作成する場合は、前述の例の STRUCTURAL を ABSTRACT に置き換えてください。

例 : 補助型またはユーザー定義のオブジェクト・クラスへの新規属性の追加

補助型オブジェクト・クラスまたはユーザー定義の構造型オブジェクト・クラスに新規属性を追加するには、ldapmodify を使用します。この例では、複合変更操作で、古いオブジェクト・クラス定義を削除して新規の定義を追加します。変更はディレクトリ・サーバーによって 1 回のトランザクションでコミットされます。既存のデータは影響されません。入力ファイルには次のように指定します。

```
dn: cn=subschemasubentry
changetype: modify
delete: objectclasses
objectclasses: old value
-
add: objectclasses
objectclasses: new value
```

たとえば、既存のオブジェクト・クラス country に属性 changes を追加する場合、入力ファイルは次のようになります。

```
dn: cn=subschemasubentry
changetype: modify
delete: objectclasses
objectclasses:  ( 2.5.6.2 NAME 'country' SUP top STRUCTURAL MUST c MAY
( searchGuide $ description  )  )
-
add: objectclasses
objectclasses:  ( 2.5.6.2 NAME 'country' SUP top STRUCTURAL MUST c MAY
( searchGuide $ description  $ changes )  )
```

ディレクトリの属性

この項では、次の項目について説明します。

- 属性管理の概要
- Oracle Directory Manager を使用した属性の管理
- コマンドライン・ツールを使用した属性の管理

関連項目：

- 属性オプションの詳細は、2-7 ページの「属性オプション」を参照してください。
- 属性オプションを追加する方法と削除する方法および属性オプションを含むエントリの検索方法は、7-8 ページの「Oracle Directory Manager を使用した属性オプション付きエントリの管理」および 7-12 ページの「コマンドライン・ツールを使用した属性オプション付きエントリの管理」を参照してください。
- 属性値のサイズを指定する構文の使用方法の詳細は、B-46 ページの「属性値のサイズ」を参照してください。

属性管理の概要

属性を扱う操作を実行する前に、概念的な観点から属性を理解する必要があります。

多くの場合、ベース・スキーマにある属性で、ユーザーの組織のニーズを満たすことができます。ベース・スキーマにない属性を使用する場合は、新規属性の追加または既存属性の変更が可能です。

デフォルトでは、属性は複数値です。Oracle Directory Manager またはコマンドライン・ツールを使用して、属性を単一値に指定できます。

> **関連項目：** 属性の概念の説明は、2-3 ページの「属性」を参照してください。

属性の追加に関する規則

属性の追加に関しては、次の規則があります。

- 属性の名前とオブジェクト識別子は、すべてのスキーマ・コンポーネントを通して一意であることが必要です。
- 構文と一致規則は、整合性がとれている必要があります。
- スーパー属性はすでに存在している必要があります。

属性の変更に関する規則

属性の変更に関しては、次の規則があります。

- 属性の名前とオブジェクト識別子は、すべてのスキーマ・コンポーネントを通して一意であることが必要です。
- 属性の構文は変更できません。
- 単一値の属性は複数値の属性に変更できますが、複数値の属性を単一値の属性に変更することはできません。
- ベース・スキーマの属性は、変更したり、削除することはできません。

属性の削除に関する規則

属性の削除に関しては、次の規則があります。

- 削除できるのはユーザー定義属性のみです。ベース・スキーマの属性は削除しないでください。
- 他のスキーマ・コンポーネントから直接または間接的に参照されていない属性は、削除することができます。

  エントリの参照先である属性を削除すると、そのエントリはディレクトリ操作に使用できなくなります。

> **関連項目：** 属性値のサイズを指定する構文の使用方法の詳細は、B-46 ページの「属性値のサイズ」を参照してください。

Oracle Directory Manager を使用した属性の管理

この項では、Oracle Directory Manager を使用して、属性の検索、表示、追加、変更、削除および索引付けを行う方法を説明します。

Oracle Directory Manager を使用したすべてのディレクトリ属性の表示

Oracle Directory Manager を使用して属性を表示する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開します。
2. 「**スキーマ管理**」を選択します。
3. 右側のペインで、「**属性**」タブ・ページを選択します。このタブ・ページには、属性プロパティを含む表が表示されます。この表の列の説明は、C-19 ページの表 C-24 を参照してください。

関連項目： 特定のエントリの属性を表示する方法は、7-4 ページの「Oracle Directory Manager を使用した特定エントリの属性の表示」を参照してください。

Oracle Directory Manager を使用した属性の検索

Oracle Directory Manager を使用して属性を検索する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開します。
2. 「**スキーマ管理**」を選択します。対応するタブ・ページが、右側のペインに表示されます。
3. 「**属性**」タブ・ページを選択します。
4. 右下隅の「**属性の検索**」ボタンをクリックします。「検索 : 属性」ダイアログ・ボックスが表示されます。
5. 検索基準バーの一番左のメニューから、検索する属性のプロパティを選択します。オプションの説明は、C-19 ページの表 C-24 を参照してください。
6. 検索基準バーの中央のメニューから、検索に使用するフィルタを選択します。オプションの説明は、C-20 ページの表 C-25 を参照してください。
7. 検索基準バーの一番右のテキスト・ボックスに、検索する属性の値または値の一部を入力します。たとえば、名前が `orcl` で始まる属性をすべて検索するには、検索基準バーの一番右のテキスト・ボックスにこの文字を入力して、「名前」「次の文字で始まる」「`orcl`」という句を作成します。
8. 検索をさらに詳細に指定するには、「**検索基準**」ボックスのボタンを使用して検索基準バーを拡張します。詳細は、C-21 ページの表 C-26 を参照してください。

9. 「**検索**」を選択します。検索結果が、「属性の検索」ダイアログ・ボックスの下部のウィンドウに表示されます。

Oracle Directory Manager を使用した属性の追加

新しい属性の作成や既存の属性からのコピーが可能です。

> **ヒント：** 等価、構文および一致規則は数が多く複雑であるため、これらの特性は、類似の既存属性からコピーすると作業が簡単になります。詳細は、6-14 ページの「Oracle Directory Manager を使用した既存の属性からの新規属性の作成」を参照してください。

Oracle Directory Manager を使用した新規属性の追加 新規属性を追加する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開します。
2. 「**スキーマ管理**」を選択します。
3. 右側のペインで「**属性**」タブを選択し、ツールバーの「**作成**」ボタンをクリックします。「新規属性の型」ダイアログ・ボックスが表示されます。そこには、「**一般**」と「**拡張**」の 2 つのタブ・ページがあります。これらの各フィールドでは、値を入力するかまたはメニューから選択します。
4. 「**一般**」タブの各フィールドに値を入力します。詳細は、C-21 ページの表 C-27 を参照してください。
5. 「**拡張**」タブを選択し、各フィールドに値を入力します。詳細は、C-22 ページの表 C-28 を参照してください。
6. 「**OK**」を選択します。

注意： この属性を使用するには、オブジェクト・クラスに対する属性セットの一部であることを必ず宣言してください。宣言は、ナビゲータ・ペインで「スキーマ管理」を選択した後、右側のペインで「オブジェクト・クラス」タブ・ページを選択して行います。詳細は、6-5 ページの「オブジェクト・クラスの変更のガイドライン」を参照してください。

Oracle Directory Manager を使用した既存の属性からの新規属性の作成 既存属性を利用して属性を追加する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開します。
2. 「**スキーマ管理**」を選択します。

3. 右側のペインで「**属性**」タブを選択します。
4. 「**属性**」タブ・ページで、コピーする属性を選択します。
5. 「**類似項目の作成**」を選択します。その属性の「新規属性の型」ダイアログ・ボックスが表示されます。このダイアログ・ボックスには、「**一般**」と「**拡張**」の 2 つのタブ・ページがあります。
6. 「**一般**」タブを選択し、各フィールドに値を入力します。詳細は、C-21 ページの表 C-27 を参照してください。識別名は、新規属性の識別名に必ず変更する必要があります。
7. 「**拡張**」タブを選択し、各フィールドに値を入力します。詳細は、C-22 ページの表 C-28 を参照してください。
8. 「**OK**」を選択します。

注意： この属性を使用するには、オブジェクト・クラスに対する属性セットの一部であることを必ず宣言してください。宣言は、ナビゲータ・ペインで「スキーマ管理」を選択した後、右側のペインで「オブジェクト・クラス」タブ・ページを選択して行います。詳細は、6-5 ページの「オブジェクト・クラスの変更のガイドライン」を参照してください。

Oracle Directory Manager を使用した属性の変更

Oracle Directory Manager を使用して属性を変更する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開します。
2. 「**スキーマ管理**」を選択します。
3. 右側のペインで「**属性**」タブを選択して、リストの中から編集可能な属性を選択します。
4. 「**編集**」を選択します。「属性」ダイアログ・ボックスには、「**一般**」と「**拡張**」の 2 つのタブ・ページが表示されます。これらの各フィールドには値を直接入力するか、メニューから値を選択します。
5. 「**一般**」タブを選択し、各フィールドに値を入力します。詳細は、C-21 ページの表 C-27 を参照してください。
6. 「**拡張**」タブを選択し、各フィールドに値を入力します。詳細は、C-22 ページの表 C-28 を参照してください。
7. 「**OK**」を選択します。

Oracle Directory Manager を使用した属性の削除

> **注意：** 削除できるのはユーザー定義属性のみです。ベース・スキーマの属性は削除しないでください。

属性を削除する方法は次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開します。
2. 「**スキーマ管理**」を選択します。
3. 右側のペインで「**属性**」タブを選択して、リストの中から編集可能な属性を選択します。
4. 「**削除**」を選択します。

Oracle Directory Manager を使用した属性の索引付け

Oracle Internet Directory は、索引を使用して属性を検索できるようにしています。Oracle Internet Directory のインストール時に、特定の属性はすでに索引付けされています。その他の属性を検索フィルタで使用する場合は、使用する属性に索引を付ける必要があります。

> **注意：** Oracle Directory Manager では、属性の作成時にのみ索引を付けることができます。Oracle Directory Manager を使用して、既存の属性に索引を付けることはできません。既存の属性に索引を付けるには、6-19 ページの「コマンドライン・ツールを使用した属性の索引付け」で説明するカタログ管理ツールを使用します。
>
> 次の条件を満たす属性のみ索引を付けることができます。
>
> - 等価の一致規則を持つ
> - Oracle Internet Directory でサポートされる一致規則を持つ（B-46 ページの「一致規則」を参照）
> - 属性名が 127 文字以下

Oracle Directory Manager を使用した索引付き属性の表示 索引付き属性を表示する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開します。
2. 「**スキーマ管理**」を選択します。

3. 右側のペインで「**属性**」タブ・ページを選択します。このタブ・ページに、スキーマ内のすべての属性が表示されます。「索引付け」列のチェックボックスが選択されている場合は、索引付き属性であることを示しています。

Oracle Directory Manager を使用した属性への索引の追加 属性に索引を追加する手順は、次のとおりです。

1. 属性を作成します（6-14 ページの「Oracle Directory Manager を使用した属性の追加」を参照）。
2. 「新規属性の型」ダイアログ・ボックスの「**拡張**」タブ・ページで、「**索引付け**」チェックボックスを選択します。

Oracle Directory Manager を使用した属性からの索引の削除 属性から索引を削除する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開します。
2. 「**スキーマ管理**」を選択します。
3. 右側のペインで「**属性**」タブを選択します。
4. 索引付き属性を選択します。選択する属性は編集可能である必要があります。編集可能かどうかは、属性名の左にアイコンで示されています。
5. 「**索引の削除**」をクリックします。

コマンドライン・ツールを使用した属性の管理

この項では、コマンドライン・ツールを使用した属性の追加、変更および索引付けについて説明します。

ldapmodify を使用した属性の追加と変更

ldapmodify コマンドを使用して新規属性をスキーマに追加するには、コマンド・プロンプトで次のようなコマンドを入力します。

```
ldapmodify -h host -p port -f ldif_file_name
```

LDIF ファイルには、次のようなデータが含まれています。

```
dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: ( 1.2.3.4.5 NAME 'myattr' SYNTAX
                 '1.3.6.1.4.1.1466.115.121.1.38' )
```

属性を単一値として指定するには、LDIF ファイルの属性定義エントリに、空白で囲んだキーワード SINGLE-VALUE を含めます。

Oracle Directory Manager または ldapsearch コマンドライン・ツールを使用して、指定した構文のオブジェクト ID を検索できます。

関連項目：

- ldapmodify とそのオプションの詳細は、A-32 ページの「ldapmodify の構文」を参照してください。
- Oracle Directory Manager または ldapsearch を使用した構文の表示方法は、6-26 ページの「ディレクトリの構文」を参照してください。

ldapmodify を使用した属性の削除

注意： 削除できるのはユーザー定義属性のみです。ベース・スキーマの属性は削除しないでください。

ldapmodify を使用して属性を削除するには、システム・プロンプトで次のようなコマンドを入力します。

```
ldapmodify -h host -p port -f ldif_file_name
```

LDIF ファイルには、次のようなデータが含まれています。

```
dn: cn=subschemasubentry
changetype: modify
delete: attributetypes
attributetypes: ( 1.2.3.4.5 NAME 'myattr' SYNTAX
                '1.3.6.1.4.1.1466.115.121.1.38' )
```

Oracle Directory Manager または ldapsearch コマンドライン・ツールを使用して、指定した構文のオブジェクト ID を検索できます。

関連項目：

- ldapmodify とそのオプションの詳細は、A-32 ページの「ldapmodify の構文」を参照してください。
- Oracle Directory Manager または ldapsearch を使用した構文の表示方法は、6-26 ページの「ディレクトリの構文」を参照してください。

コマンドライン・ツールを使用した属性の索引付け

Oracle Internet Directory は、索引を使用して属性を検索できるようにしています。Oracle Internet Directory のインストール時に、エントリ `cn=catalogs` に、検索で使用できる属性がリストされます。

その他の属性を検索フィルタで使用する場合は、使用する属性をカタログ・エントリに追加する必要があります。次の条件を満たす属性のみ索引を付けることができます。

- 等価の一致規則を持つ
- Oracle Internet Directory でサポートされる一致規則を持つ（B-46 ページの「一致規則」を参照）
- 属性の名前が 128 文字以下

新しい属性（ディレクトリにデータが存在していない属性）に、ldapmodify を使用して索引を付けることができます。ディレクトリにデータがすでに存在している属性に索引を付けるには、カタログ管理ツールを使用します。属性から索引を削除するには、ldapmodify を使用することもできますが、オラクル社ではカタログ管理ツールを使用することをお薦めします。

ldapmodify を使用した、データが存在していない属性の索引付け スキーマに新規属性を定義した後、ldapmodify を使用してその属性をカタログ・エントリに追加できます。

ディレクトリ・データが存在していない属性に ldapmodify を使用して索引を付けるには、ldapmodify で LDIF ファイルをインポートします。たとえば、すでにスキーマに定義されている属性 `foo` に索引を付けるには、ldapmodify で次の LDIF ファイルをインポートします。

```
dn: cn=catalogs
changetype: modify
add: orclindexedattribute
orclindexedattribute: foo
```

この方法は、ディレクトリにデータが存在している属性に索引を付ける場合には使用しないでください。データが存在している属性に索引を付けるには、カタログ管理ツールを使用します。

ldapmodify を使用した属性からの索引の削除 ldapmodify を使用して属性から索引を削除するには、LDIF ファイルで `delete` を指定します。たとえば、次のように入力します。

```
dn: cn=catalogs
changetype: modify
delete: orclindexedattribute
orclindexedattribute: foo
```

関連項目： A-32 ページの「ldapmodify の構文」

カタログ管理ツールを使用した、データが存在している属性の索引付け データがすでに存在している属性に対する索引付けおよび属性からの索引の削除には、カタログ管理ツールを使用します。

関連項目： A-19 ページの「カタログ管理ツール（catalog.sh）構文」

注意： Oracle Internet Directory でインストールされたベース・スキーマによって作成された索引ではないことが確信できない場合は、catalog.sh `-delete` オプションを使用して属性から索引を削除しないように注意してください。ベース・スキーマ属性から索引を削除すると、Oracle Internet Directory の操作に悪影響を及ぼす場合があります。

エントリと関連付けられた属性数の拡大方法

エントリの属性数を拡大できます。使用する方法は、エントリがすでに存在するかどうかによって異なります。

既存エントリの場合、関連付ける属性数の拡大方法には 2 通りあります。1 つは、各エントリの `objectclass` 属性のリストにオブジェクト・クラスの名前を追加する方法です。ディレクトリが比較的小さい場合は、属性に基づいてエントリを検索できるため、この方法が適しています。一方、ディレクトリが大きい場合は、`objectclass` 属性へのオブジェクト・クラスの名前の入力が、非常に複雑な作業になる場合があります。この場合、もう 1 つの方法として、コンテンツ規則を使用する方法で、より効率的にエントリのコンテンツを拡大できます。

この項では、次の項目について説明します。

- ディレクトリでエントリを作成する前の属性数の拡大
- 補助型オブジェクト・クラスの作成による既存エントリの属性数の拡大
- コンテンツ規則の作成による既存エントリの属性数の拡大

ディレクトリでエントリを作成する前の属性数の拡大

Oracle Internet Directory は、インストール時に、標準的な LDAP オブジェクト・クラスといくつかの専用オブジェクト・クラスを用意します。この事前に定義されたオブジェクト・クラスに属している属性のセットには、必須属性を追加できません。エントリに必要なすべての属性が所定のオブジェクト・クラスに含まれていない場合には、次のうちのいずれかを行います。

- 新規の（ベース）オブジェクト・クラスの定義
- オブジェクト・サブクラスの定義

関連項目：

- Oracle Internet Directory とともにインストールされるスキーマに含まれるオブジェクト・クラスのリストは、付録 B「Oracle Internet Directory のスキーマ要素」を参照してください。
- 新規のオブジェクト・クラスまたはオブジェクト・サブクラスを定義する方法については、6-3 ページの「オブジェクト・クラス管理」を参照してください。

補助型オブジェクト・クラスの作成による既存エントリの属性数の拡大

エントリに必要な追加属性を含む補助型オブジェクト・クラスを作成し、その補助型オブジェクト・クラスをエントリと関連付けることができます。補助型オブジェクト・クラスをエントリと関連付けるには、エントリの `objectclass` 属性でそれを指定します。

関連項目：

- 補助型オブジェクト・クラスの作成方法の詳細は、6-3 ページの「オブジェクト・クラス管理」を参照してください。
- オブジェクト・クラスをエントリと関連付ける方法の詳細は、第 7 章「ディレクトリ・エントリの管理」を参照してください。

コンテンツ規則の作成による既存エントリの属性数の拡大

コンテンツ規則は、仕様に従って、特定の構造型オブジェクト・クラスと関連付けられたエントリで使用されるコンテンツの種類を決定します。たとえば、`person` オブジェクト・クラスと関連付けられたエントリは、そのオブジェクト・クラスの属性だけでなく、他の属性も持つ必要があることを指定できます。追加属性は、補助型オブジェクト・クラスの必須またはオプションの属性にできます。また、このようなエントリに、1 つ以上の特定の属性に対する値が含まれないように指定することもできます。

エントリには補助型クラスをリストする必要があります（これはかなりの管理負荷になることがあります）が、コンテンツ規則をリストする必要はありません。

コンテンツ規則には、コンテンツ規則が適用される構造型オブジェクト・クラスだけでなく、次のものも含めることができます。

- 規則によって制御されるエントリで使用可能な補助型オブジェクト・クラス
- 構造型および補助型オブジェクト・クラスに必要な属性に加え、ディレクトリ情報ツリー・コンテンツ規則によって制御されるエントリで必要な必須属性
- 構造型および補助型オブジェクト・クラスに必要な属性に加え、ディレクトリ情報ツリーのコンテンツ規則によって制御されるエントリで使用可能なオプション属性
- エントリの構造型および補助型オブジェクト・クラスの属性のうち、規則によって制御されるエントリから除外するオプション属性

コンテンツ規則を作成および変更するための規則

コンテンツ規則は、サブスキーマ・サブエントリ（cn=subschemasubentry）の DITContentRule 属性の値として定義されます。コンテンツ規則は、次の規則に準拠する必要があります。

- エントリの構造型オブジェクト・クラスは、エントリに適用可能なコンテンツ規則を識別します。構造型オブジェクト・クラスに対するコンテンツ規則が存在しない場合、そのオブジェクト・クラスと関連付けられたエントリには、構造型オブジェクト・クラス定義によって許可された属性のみが含まれます。
- コンテンツ規則は構造型オブジェクト・クラスと関連付けられるため、同じ構造型オブジェクト・クラスのすべてのエントリが、ディレクトリ情報ツリーでの位置に関係なく、同じコンテンツ規則を持ちます。
- エントリのコンテンツは、そのエントリの objectClass 属性にリストされたオブジェクト・クラスの一貫性を維持している必要があります。具体的には、次の条件を満たしている必要があります。
  - objectClass 属性にリストされたオブジェクト・クラスの必須属性は、常にエントリ内に存在する必要があります。
  - コンテンツ規則で指定された補助型オブジェクト・クラスのオプション属性は、objectClass 属性にそれらの補助型オブジェクト・クラスがリストされていない場合でも存在できます。

    関連項目： コンテンツ規則の作成と管理の詳細は、6-23 ページの「コンテンツ規則の管理」を参照してください。

コンテンツ規則使用時のスキーマ制約

スキーマ整合性についてオブジェクトを検証する場合、ディレクトリ・サーバーはエントリの構造型オブジェクト・クラスのコンテンツ規則を使用します。またエントリにリストされた他のすべてのオブジェクト・クラスも使用します。

オブジェクト・クラスに複数のコンテンツ規則が存在する場合は、エントリの追加または変更時、あるいはデータのバルク・ロード時に、次の規則が適用されます。

- エントリには、各種コンテンツ規則にリストされたすべての補助型オブジェクト・クラスからの属性を含めることができます。コンテンツ規則にオブジェクト・クラスが指定されていない場合、クライアントは、制限なくディレクトリ・エントリの補助型オブジェクト・クラスを明示的に追加できます。
- エントリには、次のものにリストされたすべての必須属性の値を含める必要があります。
  - コンテンツ規則
  - エントリと関連付けられたオブジェクト・クラス
  - エントリに適用可能なコンテンツ規則にリストされた補助型オブジェクト・クラス

- オプションで、次のものにリストされたオプション属性の一部またはすべての値をエントリに含めることができます。
  - コンテンツ規則
  - エントリにリストされたオブジェクト・クラス
  - エントリに適用可能なコンテンツ規則にリストされた補助型オブジェクト・クラス
- 必須と指定された属性は、その属性をオプションと定義する他のすべての定義をオーバーライドします。

コンテンツ規則にリストされたオブジェクト・クラスの検索

コンテンツ規則にリストされた補助型オブジェクト・クラスは、エントリの objectclass 属性にリストされないため、それらのオブジェクト・クラスをエントリ検索時にフィルタとしてリストすることはできません。かわりに、関連する構造型オブジェクト・クラスに基づいて検索します。補助型オブジェクト・クラスに基づいて検索する必要がある場合は、その補助型オブジェクト・クラスをユーザー・オブジェクトの objectclass 属性に明示的に追加します。

たとえば、構造型オブジェクト・クラス inetOrgPerson のコンテンツ規則は、補助型オブジェクト・クラス orclUser を指定できます。ただし、これは、ディレクトリ内のすべての inetOrgPerson エントリに orclUser が objectclass 属性の値として含まれることを意味しません。したがって、フィルタ objectclass=orclUser を使用した検索は失敗します。コンテンツ規則に含まれる補助型オブジェクト・クラスを問い合せるかわりに、objectclass=inetOrgPerson などの構造型オブジェクト・クラスを問い合せる必要があります。

objectclass=orcluser に基づいて検索するには、各エントリの objectclass 属性の値の 1 つとして orclUser を追加します。

この注意事項は、アクセス制御ポリシーで使用するフィルタにも適用されます。追加の補助型オブジェクト・クラスと関連付けられたコンテンツ規則を使用している場合、検索フィルタでは構造型オブジェクト・クラスのみを使用します。

コンテンツ規則の管理

この項では、Oracle Directory Manager およびコマンドライン・ツールを使用してコンテンツ規則を管理する方法を説明します。

Oracle Directory Manager を使用したコンテンツ規則の管理 この項では、Oracle Directory Manager を使用してコンテンツ規則の作成と変更を行う方法を説明します。

Oracle Directory Manager を使用したコンテンツ規則の作成

コンテンツ規則を作成する手順は次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開します。
2. 「**スキーマ管理**」を選択します。
3. 右側のペインで「**コンテンツ・ルール**」タブを選択します。
4. 「**作成**」を選択します。「新規コンテンツ・ルール」ダイアログ・ボックスが表示されます。
5. 「新規コンテンツ・ルール」ダイアログ・ボックスの適切なフィールドに値を入力します。フィールドについては、C-23 ページの表 C-30 を参照してください。
6. 「**OK**」を選択します。

Oracle Directory Manager を使用したコンテンツ規則の変更

コンテンツ規則を変更する手順は次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開します。
2. 「**スキーマ管理**」を選択します。
3. 右側のペインで「**コンテンツ・ルール**」タブを選択します。
4. 変更するコンテンツ規則を選択し、「**編集**」をクリックします。「コンテンツ・ルール」ダイアログ・ボックスが表示されます。
5. 「コンテンツ・ルール」ダイアログ・ボックスの適切なフィールドに値を入力します。このダイアログ・ボックスのフィールドの説明は、C-24 ページの表 C-31 を参照してください。
6. 「**OK**」を選択します。

コマンドライン・ツールを使用したコンテンツ規則の管理 コンテンツ規則の形式は次のとおりです。

```
DITContentRule  ::=  SEQUENCE  {
    oids                                ALPHA-NUMERIC-OID,
    structuralObjectClass       OBJECT-CLASS,
    LABEL                               CONTENT-LABELOPTIONAL,
    auxiliaries                         SET (1..MAX) OF OBJECT-CLASSOPTIONAL,
    mandatory                           SET (1..MAX) OF ATTRIBUTEOPTIONAL,
    optional                            SET (1..MAX) OF ATTRIBUTEOPTIONAL,
```

表 6-1 に、パラメータを示します。属性およびオブジェクト・クラスの名前では、大 / 小文字が区別されることに注意してください。

表 6-1 コンテンツ規則のパラメータ

パラメータ	説明
oids	コンテンツ規則の一意のオブジェクト識別子（oid）。オブジェクト・クラスまたは属性定義のオブジェクト識別子と同様です。値が一意であれば、数字または英数字を使用できます。
LABEL	ディレクトリで適用されるコンテンツ規則のコンテンツ・ラベル。
structuralObjectClass	コンテンツ規則が適用される構造型オブジェクト・クラス。
auxiliaries	コンテンツ規則が適用されるエントリで使用可能な補助型オブジェクト・クラス。
mandatory	コンテンツ規則が適用されるエントリに含まれるユーザー属性タイプ。これは、指定された構造型および補助型オブジェクト・クラスとの関連付けの結果としてエントリに含まれる必須属性に対する追加の属性です。
optional	コンテンツ規則が適用されるエントリに含めることができるユーザー属性タイプ。これは、指定された構造型および補助型オブジェクト・クラスとの関連付けの結果としてエントリに含めることができる属性に対する追加の属性です。

新しいコンテンツ規則の定義中に、ディレクトリ・サーバーは構文を検証し、コンテンツ規則にリストされた属性およびオブジェクト・クラスがディレクトリで定義済であることを確認します。

コンテンツ規則は、構造型オブジェクト・クラスに対してのみ指定できます。オブジェクト・クラスの名前では、大 / 小文字が区別されます。

各構造型オブジェクト・クラスに複数のコンテンツ規則を指定できます。ただし、コンテンツ規則は、オブジェクト・クラスごとに異なるラベルで関連付ける必要があります。

コンテンツ規則の既存の定義を変更する場合、クライアントは既存の定義を削除した後で、新しい定義を追加する必要があります。`replace` コマンドを使用してコンテンツ規則を単純に置き換えることはできません。

コンテンツ規則を削除する場合、クライアントは構造型オブジェクト・クラスおよびコンテンツ規則の英数字のオブジェクト識別子のみを指定する必要があります。オプションで、削除するコンテンツ規則の関連バージョンを指定することもできます。

ディレクトリの一致規則

この項では、次の項目について説明します。

- Oracle Directory Manager を使用した一致規則の表示
- ldapsearch を使用した一致規則の表示

注意： 一致規則は変更できません。

Oracle Directory Manager を使用した一致規則の表示

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開し、「**スキーマ管理**」を選択します。
2. 右側のペインで「**一致規則**」タブを選択します。このタブ・ページのフィールドは列見出しとして表示されます。詳細は、C-22 ページの表 C-29 を参照してください。

ldapsearch を使用した一致規則の表示

サブエントリ `cn=subSchemaSubentry` で ldapsearch を使用します。

関連項目： A-39 ページの「ldapsearch の構文」

ディレクトリの構文

この項では、次の項目について説明します。

- Oracle Directory Manager を使用した構文の表示
- ldapsearch を使用した構文の表示

注意： 構文は変更できません。

Oracle Directory Manager を使用した構文の表示

Oracle Directory Manager を使用して構文を表示する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開します。
2. 「**スキーマ管理**」を選択します。

3. 右側のペインで「**構文**」タブを選択します。このタブ・ページのフィールドは列見出しとして表示されます。これには次のようなものがあります。
   - **説明** : 属性構文の名前
   - **オブジェクト ID**: この構文の一意の識別子

ldapsearch を使用した構文の表示

サブエントリ `cn=subSchemaSubentry` で ldapsearch を使用します。

関連項目： A-39 ページの「ldapsearch の構文」

7

ディレクトリ・エントリの管理

この章では、エントリを表示、追加、変更および削除する方法について説明します。

この章では、次の項目について説明します。

- Oracle Directory Manager を使用したエントリの管理
- コマンドライン・ツールを使用したエントリの管理
- バルク・ツールを使用したエントリの管理
- ナレッジ参照と参照の管理

> **関連項目：** ディレクトリ・エントリ、ディレクトリ情報ツリー、識別名および相対識別名の概要は、第 2 章「ディレクトリの概念およびアーキテクチャ」を参照してください。

Oracle Directory Manager を使用したエントリの管理

この項では、次の項目について説明します。

Oracle Directory Manager を使用したエントリの検索

すべてのエントリの表示にはナビゲータ・ペインを、1 つ以上の特定のエントリの検索には Oracle Directory Manager の検索機能を使用できます。

ナビゲータ・ペインにエントリを表示するには、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**、「**エントリ管理**」の順に展開します。

ツリーのルートが最初にリストされ、次に第 2 レベル、第 3 レベルというように、左から右へ移動してリストされます。サブツリーには、各エントリの **RDN** が階層順にリストされます。サブツリー内の下位レベルのエントリを表示するには、親エントリの横のプラス記号（+）をクリックします。

ディレクトリ・エントリを検索する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**、「**エントリ管理**」の順に展開します。右側のペインに「**検索**」フィールドが表示されます。
2. 「**検索のルート**」フィールドに、検索のルートの **DN** を入力します。

   たとえば、Americas にある IMC 組織の Manufacturing 部門に勤務する従業員を検索するとします。検索のルートの識別名は、次のようになります。

   ```
   ou=Manufacturing,ou=Americas,o=IMC,c=US
   ```

   この識別名を「**検索のルート**」テキスト・ボックスに入力します。

   ディレクトリ情報ツリー（DIT）を参照して検索のルートを選択することもできます。この手順は、次のとおりです。

   a. 「**検索のルート**」フィールドの右側の「**参照**」をクリックします。「識別名（DN）パスの選択 : ツリー表示」ダイアログ・ボックスが表示されます。

   b. 「ツリー・ビュー」の横のプラス記号（+）をクリックして、そのエントリを表示します。

c. 検索のルートのレベルを表すエントリまで、ナビゲートします。

d. そのエントリを選択して、「**OK**」をクリックします。検索のルートの識別名が、右側のペインの「**検索のルート**」テキスト・ボックスに表示されます。

3. 「**最大結果件数**」ボックスに、検索で取り出すエントリの最大数を入力します。デフォルトは 200 です。ここで設定できるディレクトリ・サーバーのエントリ数は、最大 1000 です。

4. 「**最長検索時間**」ボックスに、検索の最大時間を秒数で入力します。ここで入力する値は、少なくともデフォルト値の 25 以上にする必要があります。ここで指定できるディレクトリ・サーバーの最大検索時間は、1 時間です。

5. 「**検索の深さ**」のリストで、検索するディレクトリ情報ツリーのレベルを選択します。

   オプションは次のとおりです。

   - **ベース** : 特定のディレクトリ・エントリを取り出します。この検索レベルの場合は、検索基準バーを使用して、属性 `objectClass` とフィルタ「存在」を選択します。
   - **1 レベル** : 検索のルートの 1 レベル下のすべてのエントリに検索を制限します。
   - **サブツリー** : 検索のルートを含め、サブツリー全体のエントリを検索します。

6. 「**検索基準**」ボックスで、検索基準バーのリストとテキスト・フィールドを使用して、検索基準をさらに詳細に指定します。

   a. 検索基準バーの一番左のリストから、検索するエントリの属性を選択します。各エントリですべての属性が使用されているわけではないため、指定した属性が、検索しているエントリの属性に実際に一致していることを確認する必要があります。一致する属性がない場合は、検索に失敗します。

   b. 検索基準バーの中央のリストから、フィルタを選択します。オプションの説明は、C-33 ページの表 C-37 を参照してください。

   c. 検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。たとえば、選択した属性が `cn` の場合は、検索する個々の一般名を入力します。

7. 検索をさらに詳細に指定するには、「**検索基準**」ボックスのボタンを使用して検索基準バーを拡張します。これらのフィールドの説明は、C-34 ページの表 C-38 を参照してください。

8. 「**検索**」をクリックします。検索結果は「**識別名**」ボックスに表示されます。

関連項目： 検索で表示するエントリ数と検索の制限時間の設定方法は、5-13 ページの「アクティブ・サーバー・インスタンスの情報の表示」を参照してください。

Oracle Directory Manager を使用した特定エントリの属性の表示

検索結果の表示後、属性を参照するエントリをクリックします。「エントリ」ダイアログ・ボックスに、そのエントリの属性が表示されます。

一部の属性は、識別名である可能性もあります。たとえば、指定した従業員の 1 つの属性がその従業員のマネージャで、そのマネージャに識別名がある場合があります。この場合、従業員の「エントリ」ダイアログ・ボックスを表示すると、「**マネージャ**」テキスト・ボックスの横に「**参照**」ボタンが表示されます。そのマネージャの情報を検索するには、「**参照**」をクリックして「ディレクトリ : エントリ管理」ダイアログ・ボックスを表示し、7-2 ページの「Oracle Directory Manager を使用したエントリの検索」の手順に従って検索してください。

> **関連項目：** ディレクトリの属性をすべて表示する方法は、6-13 ページの「Oracle Directory Manager を使用したすべてのディレクトリ属性の表示」を参照してください。

Oracle Directory Manager を使用したエントリの追加

この項では、個々のエントリおよびグループ・エントリを追加する方法を説明します。

注意： エントリを追加または削除する場合、Oracle ディレクトリ・サーバーではエントリ属性値の構文検証は行われません。

Oracle Directory Manager を使用した新規エントリの追加

Oracle Directory Manager でエントリを追加または削除するには、親エントリに対する書込みアクセス権限があり、新規エントリの識別名を認識している必要があります。

新規エントリを追加する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開します。
2. 「**エントリ管理**」を選択します。
3. ツールバーの「**作成**」ボタンをクリックします。「新規エントリ」ダイアログ・ボックスが表示されます。
4. 「**識別名**」フィールドに、完全な識別名を入力します。「**参照**」をクリックして、追加するエントリの親の識別名の位置を識別して選択することもできます。選択したエントリが「**識別名**」フィールドに表示されます。その親の識別名の左に新規エントリの相対識別名を入力し、その後にカンマを付けます。
5. 新規エントリのオブジェクト・クラスを指定するには、「**オブジェクト・クラス**」ボックスの横の「**追加**」をクリックします。「スーパー・クラス・セレクタ」ダイアログ・ボックスが表示されます。

6. 「スーパー・クラス・セレクタ」ダイアログ・ボックスでオブジェクト・クラスを選択して、「**選択**」をクリックします。オブジェクト・クラス・リストからオブジェクト・クラスを選択すると、「新規エントリ」ダイアログ・ボックスの下半分のタブ・ページにあるウィンドウに、必須属性とオプション属性が表示されます。必須属性のフィールドには、値を入力する必要があります。オプション属性のフィールドには、値を必ずしも入力する必要はありません。
7. オブジェクト・クラスを選択して、対応する属性に値を入力した後、「**OK**」をクリックします。

Oracle Directory Manager の既存エントリを利用したエントリの追加

Oracle Directory Manager では、既存エントリをコピーしてその識別名を変更する方法で、新規エントリを作成できます。この操作を行う場合は、名前やアドレスなどの属性も、新規識別名に対応するように変更してください。エントリを追加するには、その親に対する書込みアクセス権限が必要です。

> **ヒント：** 検索ペインで他の類似エントリを参照して、新規識別名用のテンプレートを検索できます。

既存エントリを利用してエントリを追加する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開します。
2. 「**エントリ管理**」を選択します。
3. 右側のペインに「検索」インタフェースが表示されます。このペインで、テンプレートとして使用するエントリを検索します。
4. 取り出したエントリから、テンプレートとして使用するエントリをダブルクリックします。そのエントリに対応する「エントリ」ダイアログ・ボックスが表示されます。
5. 「エントリ」ダイアログ・ボックスで、「**類似項目の作成**」をクリックします。「新規エントリ : 類似項目の作成」ダイアログ・ボックスが表示されます。
6. このエントリを作成するエントリに調整するために、重要なフィールドを変更します。この操作で、識別名と一般名は必ず変更する必要があります。変更しないと、新規エントリのデータは保存されません。たとえば、Henri Latour のエントリをテンプレートとして使用して Henri Latrobe のエントリを作成する場合は、識別名の `cn=Henri Latour` を `cn=Henri Latrobe` に変更する必要があります。また、この他にも従業員番号や電話番号など、一意であることが必要な属性をすべて変更する必要があります。
7. 「**OK**」をクリックして、変更内容を保存します。

> **関連項目：** フィールドに情報を追加する方法は、このダイアログ・ボックスのオンライン・ヘルプを参照してください。

例 : Oracle Directory Manager を使用したユーザー・エントリの追加

この例では、Anne Smith というユーザーを作成し、パスワードを割り当てます。

1. administrator でログインします。
2. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開します。
3. 「**エントリ管理**」を選択します。
4. ツールバーの「**作成**」ボタンをクリックします。「新規エントリ」ダイアログ・ボックスが表示されます。
5. 「**識別名**」フィールドに、完全な識別名を入力します。「**参照**」ボタンをクリックして、このエントリの親の識別名を探し、親の識別名の左に相対識別名、つまり `cn=Anne Smith` を入力して、その後にカンマを付けることもできます。
6. 「オブジェクト・クラス」ボックスの右の「**追加**」をクリックします。「スーパー・クラス・セレクタ」ダイアログ・ボックスが表示されます。
7. 「スーパー・クラス・セレクタ」ダイアログ・ボックスで `person` オブジェクト・クラスを選択して、「**選択**」をクリックします。「新規エントリ」ダイアログ・ボックスに戻ります。
8. 「新規エントリ」ダイアログ・ボックスで「**オプション・プロパティ**」タブをクリックし、「ユーザー・パスワード」ウィンドウまでスクロールします。
9. Anne Smith 用のパスワードを入力します。

関連項目 :

- 検索ペインの使用方法は、7-2 ページの「Oracle Directory Manager を使用したエントリの検索」を参照してください。
- 9-7 ページの「グループ・エントリの管理」
- グループ・エントリのアクセス制御ポリシーの設定方法の詳細は、14-3 ページの「セキュリティ・グループ」を参照してください。
- アクセス権限の詳細は、2-12 ページの「グローバリゼーション・サポート」および第 14 章「ディレクトリ・アクセス制御」を参照してください。

Oracle Directory Manager を使用したエントリの変更

既存エントリに補助型オブジェクト・クラスを追加できます。

すでにエントリで使用されているオブジェクト・クラスには、オプション属性は追加できますが、必須属性は追加できません。エントリですでに使用されているオブジェクト・クラスにオプション属性を追加する場合、特別な規則は適用されません。オプション属性は、空の属性としてこれらのエントリに追加されます。

注意： エントリを追加または削除する場合、Oracle ディレクトリ・サーバーではエントリ属性値の構文検証は行われません。

エントリを変更する手順は、次のとおりです。

1. 7-2 ページの「Oracle Directory Manager を使用したエントリの検索」の説明に従って、変更するエントリの検索を実行します。
2. 右側のペインの「**識別名**」ボックスで、変更するエントリを選択します。
3. 「**編集**」をクリックします。「エントリ」ダイアログ・ボックスが表示されます。
4. 該当するフィールドを変更し、「**プロパティの選択**」タブ・ページを選択します。追加または変更する属性が表示されない場合は、タブ・ページの一番上にある「**プロパティの表示 : すべて**」を選択します。
5. 「**プロパティ**」タブ・ページで、編集可能な属性の値を変更します。
6. 「**OK**」を選択します。

例 : Oracle Directory Manager を使用したユーザー・エントリの変更

この例では、7-6 ページの「例 : Oracle Directory Manager を使用したユーザー・エントリの追加」の項で Anne Smith 用に作成したエントリ用のパスワードを変更します。

1. Anne Smith エントリの検索を実行します。
2. 右側のペインの「**識別名**」ボックスで、Anne Smith のエントリを選択します。
3. 「**編集**」をクリックします。
4. 「エントリ」ダイアログ・ボックスで、「ユーザー・パスワード」ウィンドウまでスクロールしてその値を変更します。
5. 「**OK**」をクリックします。

Oracle Directory Manager を使用した属性オプション付きエントリの管理

この項では、属性オプションを追加、変更および削除する方法を説明します。

> **関連項目：** 属性オプション付きエントリの検索方法は、7-2 ページの「Oracle Directory Manager を使用したエントリの検索」を参照してください。

Oracle Directory Manager を使用した、既存エントリへの属性オプションの追加

> **注意：** Oracle Internet Directory 10*g*（9.0.4）の Oracle Directory Manager では、エントリを作成した時点で、そのエントリに属性オプションを追加することはできません。すでに存在しているエントリに対してのみ、Oracle Directory Manager を使用して属性オプションを追加できます。

既存のエントリに属性オプションを追加する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**、「**エントリ管理**」の順に展開します。
2. 属性オプションを追加するエントリを選択します。対応するタブ・ページが、右側のペインに表示されます。
3. 右側のペインにある「**プロパティ**」タブ・ページの「**プロパティの表示**」フィールドで、「**拡張**」を選択します。この操作に伴って、「**プロパティ**」タブ・ページが変わります。
4. 「**属性**」フィールドで、オプションを追加する属性（たとえば、`ou`）を選択します。
5. 「**属性オプション**」フィールドで、属性オプション（たとえば、`lang-en`）を入力します。
6. 「**属性値**」フィールドで、指定する属性オプションの値（たとえば、`Server Technologies`）を入力します。指定した属性オプションに複数の値を追加するには、各値をセミコロンで区切ります。
7. 「**適用**」をクリックします。

Oracle Directory Manager を使用した属性オプションの変更

属性オプションを変更する手順は次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**、「**エントリ管理**」の順に展開します。

2. 変更する属性オプションのエントリを選択します。対応するタブ・ページが、右側のペインに表示されます。
3. 「**プロパティ**」タブ・ページの「**プロパティの表示**」フィールドで、「**NULL 以外の値のみ**」または「**すべて**」を選択します。
4. 変更する属性オプションを含むフィールドまでスクロールします。
5. フィールドの値を変更します。
6. 「**適用**」をクリックします。

Oracle Directory Manager を使用した属性オプションの削除

属性オプションを削除する手順は次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**、「**エントリ管理**」の順に展開します。
2. 属性オプションを削除するエントリを選択します。対応するタブ・ページが、右側のペインに表示されます。
3. 「**プロパティ**」タブ・ページの「**プロパティの表示**」フィールドで、「**NULL 以外の値のみ**」または「**すべて**」を選択します。
4. 削除する属性オプションを含むフィールドまでスクロールします。
5. フィールドの値を削除します。
6. 「**適用**」をクリックします。

コマンドライン・ツールを使用したエントリの管理

この項では、エントリの管理に使用できるコマンドライン・ツールについて説明します。また、コマンドライン・ツールを使用したエントリ管理の例もいくつか紹介します。この項では、次の項目について説明します。

- エントリ管理のためのコマンドライン・ツール
- 例 : ldapadd を使用したユーザー・エントリの追加
- 例 : ldapmodify を使用した属性オプションの追加
- 例 : ldapmodify を使用したユーザー・エントリの変更
- コマンドライン・ツールを使用した属性オプション付きエントリの管理

エントリ管理のためのコマンドライン・ツール

次の表に、各コマンドライン・ツールと、それぞれのツールの構文と使用方法の参照先を示します。

表 7-1　エントリ管理のためのコマンドライン・ツール

ツール	タスク	構文と使用方法
ldapadd	エントリを一度に 1 つずつ追加します。 新規構成設定エントリを追加します。 入力ファイルを使用してサーバーを構成します。	A-21 ページの「ldapadd の構文」
ldapaddmt	この共有サーバー・ツールは、同時に複数のエントリを追加するときに使用します。	A-23 ページの「ldapaddmt の構文」
ldapbind	ディレクトリ・サーバーに対して、ユーザーまたはクライアントを認証します。 クライアントをサーバーに接続できるかどうかを検証します。	A-25 ページの「ldapbind の構文」
ldapcompare	ユーザーが指定した属性値とディレクトリ・エントリ内の属性値を比較します。	A-26 ページの「ldapcompare の構文」
ldapdelete	エントリを削除します。	A-28 ページの「ldapdelete の構文」
ldapmoddn	エントリの識別名または相対識別名を変更します。 エントリまたはサブツリーの名前を変更します。 エントリまたはサブツリーを新しい親の下に移動します。	A-30 ページの「ldapmoddn の構文」
ldapmodify	エントリの属性データを作成、更新および削除します。 構成設定エントリを変更します。 エントリの識別名または相対識別名を変更します。	A-32 ページの「ldapmodify の構文」
ldapmodifymt	この共有サーバー・ツールは、同時に複数のエントリを変更するときに使用します。	A-37 ページの「ldapmodifymt の構文」
ldapsearch	ディレクトリ・エントリを検索します。	A-39 ページの「ldapsearch の構文」

例 : ldapadd を使用したユーザー・エントリの追加

次の例では、John という従業員のエントリを追加するため、entry.ldif という名前の LDIF ファイルを示します。

```
dn: cn=john, c=us
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
cn: john
cn;lang-fr:Jean
cn;lang-en-us:John
sn: Doe
jpegPhoto: /photo/john.jpg
userpassword: welcome
```

このファイルには、cn、sn、jpegPhoto および userpassword の各属性が含まれています。

cn 属性には、2 つのオプションを指定します。cn;lang-fr と cn;lang-en-us です。これらのオプションは、French（フランス語）または American English（米語）での一般名を戻します。

jpegPhoto 属性では、エントリの属性として組み込む、対応する JPEG イメージのパスとファイル名を指定しています。

注意 : エントリを追加または削除する場合、Oracle ディレクトリ・サーバーではエントリ属性値の構文検証は行われません。

例 : ldapmodify を使用したユーザー・エントリの変更

次の例では、Audrey というユーザーのパスワードを、welcome から audreyspassword に変更します。前述の例と同様に、このユーザー・エントリ用のデータは entry.ldif ファイルに記述されています。このファイルの内容は次のとおりです。

```
dn: cn=audrey,c=us
changetype: modify
replace: userpassword
userpassword: audreyspassword
```

ファイルを変更するには、次のコマンドを発行します。

```
ldapmodify -p 389 -v  -f entry.ldif
```

-v は冗長モードを指定します。

注意： エントリを追加または削除する場合、Oracle ディレクトリ・サーバーではエントリ属性値の構文検証は行われません。

コマンドライン・ツールを使用した属性オプション付きエントリの管理

この項では、属性オプションを追加する例と削除する例、および属性オプション付きエントリを検索する例を紹介します。

例 : ldapmodify を使用した属性オプションの追加

John のエントリのスペイン語属性を追加するとします。また、このユーザー・エントリ用のデータは entry.ldif ファイルに記述されているとします。このファイルの内容は次のとおりです。

```
dn: cn=john,c=us
changeType: modify
add: cn;lang-sp
cn;lang-sp: Juan
```

ファイルを変更するには、次のコマンドを発行します。

```
ldapmodify -p 389 -v  -f entry.ldif
```

例 : ldapmodify を使用した属性オプションの削除

次の例では、John のエントリから cn;lang-fr 属性オプションを削除します。前述の例と同様に、このユーザー・エントリ用のデータは entry.ldif ファイルに記述されています。このファイルの内容は次のとおりです。

```
dn: cn=john, c=us
changetype: modify
delete: cn;lang-fr
cn;lang-fr: Jean
```

ファイルを変更するには、次のコマンドを発行します。

```
ldapmodify -p 389 -v  -f entry.ldif
```

例 : ldapsearch を使用した属性オプション付きエントリの検索

次の例では、言語コード属性オプションを指定するオプションのある一般名（cn）属性を使用して、エントリを取り出します。この例の場合には、一般名がフランス語で、R で始まるエントリを取り出します。

```
ldapsearch -p 389 -h myhost -b "c=US" -s sub "cn;lang-fr=R*"
```

John のエントリで、cn;lang-it 言語コード属性オプションに値が設定されていないと想定します。この場合、次の例は失敗します。

```
ldapsearch -p 389 -h myhost -b "c=us" -s sub "cn;lang-it=Giovanni
```

関連項目： 2-7 ページの「属性オプション」

バルク・ツールを使用したエントリの管理

この項では、バルク・ツールで実行する一般的なタスクの一部を説明します。

この項では、次の項目について説明します。

- bulkload を使用した LDIF ファイルのインポート
- ディレクトリ・データの LDIF への変換
- 多数のエントリの変更
- 多数のエントリの削除

注意： ディレクトリへの移入に bulkload ユーティリティを使用しない場合は、oidstats.sh ツールを実行して、検索パフォーマンスの深刻な低下を回避する必要があります。

関連項目：

- oidstats.sh ツールの説明と構文は、A-131 ページの「OID データベース統計収集ツール（oidstats.sh）の構文」を参照してください。
- これらのツールの概要は、4-14 ページの「コマンドラインツールの使用方法」を参照してください。

bulkload を使用した LDIF ファイルのインポート

LDIF ファイルをインポートするには、bulkload ユーティリティを使用します。この項では、bulkload で LDIF ファイルを処理するタスクについて説明します。

注意： bulkload ユーティリティは、空のディレクトリを想定しています。ディレクトリに既存のエントリがあると、bulkload ユーティリティは失敗するか、既存のエントリを上書きします。

バルク・ロードを実行する前に、Oracle Internet Directory プロセスを停止してください。ディレクトリ・サーバー・インスタンスの停止方法は、第 3 章「事前に実行するタスクと情報」を参照してください。

注意： Windows オペレーティング・システムでシェル・スクリプト・ツールを実行するには、次のいずれかの UNIX エミュレーション・ユーティリティが必要です。

- Cygwin 1.3.2.2-1 以上
  サイト：`http://sources.redhat.com`
- MKS Toolkit 6.1
  サイト：`http://www.datafocus.com/`

この項では、次の項目について説明します。

タスク 1: Oracle データベース・サーバーのバックアップ

ファイルをインポートする前に、安全対策として Oracle データベース・サーバーをバックアップします。

関連項目：『Oracle Database バックアップおよびリカバリ基礎』

タスク 2: Oracle Internet Directory のパスワードの準備

bulkload および `.sh` で終わるコマンドを持つ他のシェル・スクリプト・ツールを使用するには、Oracle Internet Directory のパスワードを準備する必要があります。デフォルトのパスワードは `ods` ですが、このパスワードは、**OID データベース・パスワード・ユーティリティ**を使用して、システム管理者が変更できます。

関連項目： A-129 ページの「OID データベース・パスワード・ユーティリティ（oidpasswd）構文」

タスク 3: スキーマ違反とデータ整合性違反に関する入力のチェック

UNIX では、bulkload.sh ファイルは通常は次の場所にあります。

$*ORACLE_HOME*/ldap/bin

Windows NT では、このファイルは通常は次の場所にあります。

ORACLE_HOME¥ldap¥bin

入力ファイルをチェックするには、次のように入力します。

```
bulkload.sh -connect connect_string -check path_to_ldif-file_name
```

すべてのスキーマ違反が $*ORACLE_HOME*/ldap/log/schemacheck.log に記録されます。

入力ファイルに違反が検出された場合は、ASCII テキスト・ファイル・エディタを使用してその違反を修正または削除してください。エントリが重複している場合、その識別名は $*ORACLE_HOME*/ldap/log/duplicate.log に記録されます。

タスク 4: SQL*Loader 用の入力ファイルの生成

入力ファイルのエラー修正後、次の例のように -generate オプションを指定して bulkload を再実行します。この手順で、LDIF データは SQL*Loader 固有の形式に変換されます。

```
bulkload.sh -connect connect_string -generate ldif-file_name
```

ロード時のエラーはすべて $*ORACLE_HOME*/ldap/log に記録されます。

このコマンドが正常に完了すると、SQL*Loader が -load モードで使用する *.dat ファイルが、$ORACLE_HOME/ldap/load ディレクトリに生成されます。このファイルは変更できません。

タスク 5: 入力ファイルのロード

入力ファイルの生成後、-load オプションを指定して bulkload を再実行します。この手順で、Oracle SQL*Loader 固有の形式の *.dat ファイルがデータベースにロードされ、属性の索引が作成されます。構文は次のとおりです。

```
bulkload.sh -connect connect_string -load
```

バルク・ロードに失敗した場合

ロード時のエラーはすべて、$*ORACLE_HOME*/ldap/log/directory にファイル拡張子 .bad で記録されます。

バルク・ロードに失敗した場合は、データベースが一貫性のない状態のままになっている可能性があります。バルク・ロードを操作する前の状態にデータベースをリストアする必要がある場合があります。

ディレクトリ・データの LDIF への変換

LDIF ライターを使用してディレクトリ・データを LDIF に変換すると、レプリケート・ディレクトリの新規ノードまたはバックアップ保管用の別のノードにロードするために使用できます。

関連項目： A-54 ページの「ldifwrite の構文」

多数のエントリの変更

bulkmodify ユーティリティを使用すると、多数の既存エントリを効率的に変更できます。

関連項目： A-52 ページの「bulkmodify の構文」

多数のエントリの削除

bulkdelete ユーティリティを使用すると、サブツリー全体を効率的に削除できます。

関連項目： A-44 ページの「bulkdelete の構文」

ナレッジ参照と参照の管理

ナレッジ参照は**参照**とも呼ばれ、特定のタイプの**エントリ**としてディレクトリ内で表されます。ナレッジ参照エントリを作成するときには、`referral` **オブジェクト・クラス**および `extensibleObject` オブジェクト・クラスにそのエントリを対応付けます。通常、ナレッジ参照エントリは、パーティションを確立する **DIT** 内の場所に作成されます。

ナレッジ参照は、LDAP URL を含む参照をユーザーに提供します。この URL を、`ref` 属性の値として入力してください。任意のナレッジ参照エントリに複数の `ref` 属性が指定されている場合があります。同様に、ディレクトリ情報ツリーに複数のナレッジ参照エントリがある場合もあります。

関連項目： ナレッジ参照の概要、**スマート・ナレッジ参照**および**デフォルト・ナレッジ参照**の説明は、2-24 ページの「ディレクトリ・パーティション化」を参照してください。

この項では、次の項目について説明します。

- スマート参照の構成
- デフォルト参照の構成
- クライアント側の参照キャッシング

スマート参照の構成

検索結果には、ナレッジ参照とともに通常のエントリも含まれる場合があります。ユーザーが検索操作を実行すると、Oracle Internet Directory は指定された検索の適用範囲内でナレッジ参照エントリを探します。ナレッジ参照が見つかった場合、Oracle Internet Directory は参照をクライアントに戻します。

ユーザーがナレッジ参照エントリの下に置かれたエントリに対して追加、削除または変更操作を実行すると、Oracle Internet Directory は参照を戻します。

たとえば、ディレクトリ・サーバーの地理的な場所に基づいたディレクトリ情報ツリーを分割するとします。この例では、次のように仮定します。

- c=us ネーミング・コンテキストは、米国のサーバー A とサーバー B にローカルに保持されています。
- c=uk ネーミング・コンテキストは、英国のサーバー C とサーバー D にローカルに保持されています。

ここで、この 2 つのネーミング・コンテキスト間のナレッジ参照を、次のように構成するとします。

1. 米国のサーバー A で、サーバー C とサーバー D の c=uk オブジェクトのナレッジ参照を構成します。

```
dn: c=uk
c: uk
ref: ldap://host C:389/c=uk
ref: ldap://host D:686/c=uk
objectclass: top
objectclass: referral
objectClass: extensibleObject
```

2. 同様に英国のサーバー C で、サーバー A とサーバー B の c=us オブジェクトのナレッジ参照を構成します。

```
dn: c=us
c: us
ref: ldap://host A:4000/c=us
ref: ldap://host B:5000/c=us
objectclass: top
objectclass: referral
objectClass: extensibleObject
```

結果は、次のようになります。

- サーバー A にベース o=foo,c=uk で問い合せるクライアントは、参照を受信します。
- サーバー C にベース o=foo,c=us で問い合せるクライアントは、参照を受信します。
- サーバー A またはサーバー B での o=foo,c=uk の追加操作は失敗します。かわりに、Oracle Internet Directory は参照を戻します。

デフォルト参照の構成

Oracle Internet Directory は、サーバーによってローカルに保持されているすべての**ネーミング・コンテキスト**を、**DSE** の namingcontext 属性を使用して判断します。namingContext 属性には、ネーミング・コンテキスト情報を正しく反映させてください。

DSE エントリの ref 属性の値を入力して、デフォルト参照を指定します。ref 属性が DSE エントリにない場合は、デフォルト参照は戻されません。

デフォルト参照を構成するときは、LDAP URL の識別名を指定しないでください。

たとえば、サーバー A の DSE エントリに、次の namingContext 値が含まれているとします。

```
namingcontext: c=us
```

さらに、デフォルト参照が次のとおりと仮定します。

```
Ref: ldap://host PQR:389
```

ユーザーが、サーバー A でネーミング・コンテキスト c=canada にベース識別名を持つ操作を入力したとします。たとえば、次のとおりです。

```
ou=marketing,o=foo,c=canada
```

このユーザーはホスト PQR への参照を受信することになります。これは、サーバー A が c=canada ベース識別名を保持しておらず、その DSE の namingContext 属性が値 c=canada を保持していないためです。

> **関連項目：** ナレッジ参照の概要は、2-25 ページの「ナレッジ参照と参照」を参照してください。

クライアント側の参照キャッシング

参照キャッシングとは、参照情報へのアクセスを簡単に繰り返すことができるように、その情報を格納するプロセスです。クライアントがサーバー A に問い合せ、サーバー A がサーバー B に参照を戻すとします。クライアントはこの参照を追跡して、操作を実行し、クライアントに結果を戻すサーバー B と通信します。参照キャッシングが行われていない場合、クライアントが次回同じ問合せをサーバー A に対して行うと、手順全体が繰り返され、時間とシステム・リソースを必要以上に消費することになります。

参照情報をキャッシュできる場合は、以降の各問合せで、参照情報をキャッシュから取り出し、サーバー B と直接通信できます。これによって、操作にかかる時間を短縮できます。

クライアント側の参照キャッシングによって、各クライアントは、参照情報をキャッシュして使用し、参照処理にかかる時間を短縮できます。

クライアント側の参照キャッシングの動作方法

参照エントリは、クライアントの構成ファイルに格納されます。クライアントは、セッション確立時に、この構成ファイルから参照情報を読み取ってキャッシュに格納します。このキャッシュは静的状態を保持し、セッション中に更新の追加は行われません。これ以降、クライアントは、操作を行うたびにキャッシュ内の参照情報を検索します。

クライアントが使用するこの構成ファイルは、ディレクトリ管理者が準備します。

注意： 構成ファイルは、クライアントにとってはオプションです。ファイルが存在しない場合でも、参照に関係するクライアント操作は正常に行われます。したがって、このファイルの準備は、管理者の必須作業ではありません。構成ファイルを使用する利点は、参照に関係するクライアント / サーバーの操作時間を短縮できることです。

構成ファイルは、1 つ以上の参照セットで構成されます。それぞれの参照セットは、次の要素で構成されます。

- 特定のディレクトリ・サーバーが稼働しているホスト名
- そのサーバーに常駐する 1 つ以上のエントリ

各参照エントリは一連の行で構成され、それぞれの行は 1 つの参照 URL に対応します。行セパレータは、CR LF または LF です。

```
ref_file=ref_file_content
ref_file_content=1*(referral_set)
referral_set=hostname      SEP      ref_entry_set   SEP
ref_entry_set=ref_entry     *(SEP      ref_entry)
ref_entry=1*(referralurl     SEP)
SEP=CR LF / LF
CR=0x0D
LF=0x0A
```

たとえば、ホスト・サーバー X で稼働しているディレクトリ・サーバーに次の 2 つの参照エントリがあるとします。

```
dn: dc=acme, dc=com
ref: ldap://serverA:389/dc=acme, dc=com
ref: ldap://serverB:389/dc=acme, dc=com
```

```
dn: dc=oracle, dc=com
ref: ldap://serverC:389/dc=oracle, dc=com
ref: ldap://serverD:389/dc=oracle, dc=com
```

ホスト・サーバー Y で稼働しているディレクトリ・サーバーには、次の参照エントリがあるとします。

```
dn: dc=fiction, dc=com
ref: ldap://serverE:389/dc=fiction, dc=com
```

対応する referral.ora ファイルは、次のようになります。

```
ServerX
ldap://serverA:389/dc=acme, dc=com
ldap://serverB:389/dc=acme, dc=com

ldap://serverC:389/dc=oracle, dc=com
ldap://serverD:389/dc=oracle, dc=com

ServerY
ldap://serverE:389/dc=fiction, dc=com
```

8

ディレクトリの属性一意性

この章では、Oracle Internet Directory の属性一意性について説明します。次の項目について説明します。

- 属性一意性の概要
- 属性一意性作成の結果
- 属性一意性の管理
- Oracle Internet Directory 10g（9.0.4）での属性一意性の制限事項

属性一意性の概要

属性一意性機能は、属性値の追加時および変更時に属性値が重複しないようにします。たとえば、すでに別の従業員に割り当てられている識別子を新しい従業員に割り当てることを防止します。かわりに、ディレクトリ・サーバーは操作を中止し、エラー・メッセージを戻します。

次の属性一意性を定義できます。

- ディレクトリ全体を対象

  たとえば、mail 属性を持つディレクトリ内のすべてのエントリが、その属性に対して一意の値を保持するためには、mail と関連付けられた属性一意性のインスタンスを作成します。

- 属性ごとの 1 つのサブツリー対象

  たとえば、MyCompany が SubscriberCompany1 と SubscriberCompany2 用のディレクトリをホスティングしている場合は、SubscriberCompany1 のみに属性一意性を適用できます。

- 1 つのオブジェクト・クラス対象

  たとえば、ID は、machine オブジェクト・クラスと person オブジェクト・クラスの両方で属性となっています。属性一意性を有効にすると、ディレクトリ・サーバーは、同じ ID を持つ 2 台のマシンまたは 2 人のユーザーの追加を防止します。ただし、machine の ID 属性に、person の ID 属性と同じ値を指定することは可能です。

属性一意性を実装するには、表 8-1 に示す属性を指定して属性一意性制約エントリを作成します。

表 8-1 属性一意性制約エントリ

属性名	必須	有効値	デフォルト値	デフォルト有効範囲
orcluniqueattrname	はい	任意の文字列	該当なし	該当なし
orcluniquescope	いいえ	次のいずれかの値 ■ base: ルート・エントリのみを検索 ■ onelevel: 1 レベルのみを検索 ■ sub: ディレクトリ全体を検索	sub	ディレクトリ全体を検索

表 8-1 属性一意性制約エントリ（続き）

属性名	必須	有効値	デフォルト値	デフォルト有効範囲
orcluniqueenable	いいえ	0（無効）または 1（有効）	0	属性一意性を無効化
orcluniquesubtree	いいえ	任意の文字列	" "	ディレクトリ全体を検索
orcluniqueobjectclass	いいえ	任意の文字列	" "	すべてのオブジェクト・クラスを検索

エントリを作成し、属性を指定した場合、ディレクトリ・サーバーは、エントリに対する操作を実行する前に次のことを行います。

- 属性一意性制約を使用したすべての更新操作のチェック
- 監視対象の属性、サブツリーまたはオブジェクト・クラスに操作を適用するかどうかの決定

監視対象の属性、接尾辞またはオブジェクト・クラスに操作を適用して、2 つのエントリに同じ属性値が含まれた場合、ディレクトリ・サーバーは操作を中止し、制約違反エラー・メッセージをクライアントに戻します。

注意： 属性一意性機能は、索引付き属性でのみ機能します。

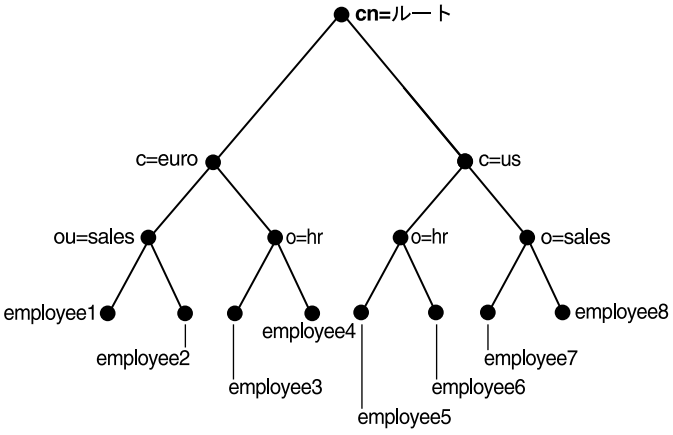
属性一意性作成の結果

この項では、属性一意性制約の作成時に適用される規則について、例を使用して説明します。この項では、次の項目について説明します。

- 属性一意性制約での複数の属性名の指定
- 属性一意性制約での複数のサブツリーの指定
- 属性一意性制約での複数の有効範囲の指定
- 属性一意性制約での複数のオブジェクト・クラスの指定
- 属性一意性制約での複数のサブツリー、有効範囲およびオブジェクト・クラスの指定

この項の例を理解するには、図 8-1 を参照してください。

図 8-1 ディレクトリ情報ツリーの例



属性一意性制約での複数の属性名の指定

複数の属性一意性制約で orcluniqueattrname の値が異なる場合、その有効性は互いに独立しています。

たとえば、ユーザーが、次のような 2 つの属性一意性制約を定義するとします。

制約 1:

```
orcluniqueattrname: employee_id
```

制約 2:

```
orcluniqueattrname: email_id
```

この例で、制約 1 と制約 2 は、それぞれの属性一意性の有効範囲内で指定された属性に対して一意性を適用します。制約 1 と制約 2 は、互いに独立しています。

属性一意性制約での複数のサブツリーの指定

複数の属性一意性制約で、orcluniqueattrname、orcluniquescope および orcluniqueobjectclass の値が同一で、orcluniquesubtree の値が異なる場合は、それらの属性一意性制約で指定されたサブツリーの有効範囲を結合したものがチェックされます。

たとえば、8-4 ページの図 8-1 を参照してください。ユーザーが、次のような 2 つの属性一意性制約を定義するとします。

制約 1:

```
orcluniqueattrname: employee_id
orcluniquesubtree: o=sales, c=us, cn=root
orcluniquescope: onelevel
```

制約 2:

```
orcluniqueattrname: employee_id
orcluniquesubtree: o=hr, c=euro, cn=root
orcluniquescope: onelevel
```

この例で、employee_id の属性一意性は、サブツリー o=sales,c=us,cn=root および o=hr,c=euro,cn=root の下にあるすべてのエントリに対して適用されます。ディレクトリ・サーバーは、employee_id 属性の一意の値を employee1、employee2、employee5 および employee6 に対して適用します。

属性一意性制約での複数の有効範囲の指定

複数の属性一意性制約で、orcluniqueattrname、orcluniquesubtree および orcluniqueobjectclass の値が同一で、orcluniquescope の値が異なる場合は、最大の検索有効範囲を持つ属性一意性制約が有効となります。

たとえば、8-4 ページの図 8-1 で、ユーザーが、次のような 2 つの属性一意性制約を定義するとします。

制約 1:

```
orcluniqueattrname: employee_id
orcluniquesubtree: c=us, cn=root
orcluniquescope: onelevel
```

制約 2:

```
orcluniqueattrname: employee_id
orcluniquesubtree: c=us, cn=root
orcluniquescope: sub
```

この例で、employee_id の属性一意性は、サブツリー c=us,cn=root の下にあるすべてのエントリおよびエントリ c=us,cn=root 自体に対して適用されます。これは、ユーザーが制約 2 のみを定義した場合と同じです。

属性一意性制約での複数のオブジェクト・クラスの指定

複数の属性一意性制約で、orcluniqueattrname、orcluniquesubtree および orcluniquescope の値が同一で、orcluniqueobjectclass の値が異なる場合は、それらのオブジェクト・クラスに属する属性を結合したものがチェックされます。

たとえば、8-4 ページの図 8-1 で、ユーザーが、次のような 2 つの属性一意性制約を定義するとします。

制約 1:

```
orcluniqueattrname: employee_id
orcluniquesubtree: c=us, cn=root
orcluniqueobjectclass: person
```

制約 2:

```
orcluniqueattrname: employee_id
orcluniquesubtree: c=us, cn=root
```

この例で、employee_id の属性一意性は、エントリが属するオブジェクト・クラスに関係なく、サブツリー c=us,cn=root の下にあるすべてのエントリと、エントリ c=us,cn=root 自体に対して適用されます。制約 2 は orcluniqueobjectclass 属性を指定していません。これはすべてのオブジェクト・クラスを指定した場合と同じです。

属性一意性制約での複数のサブツリー、有効範囲およびオブジェクト・クラスの指定

複数の属性一意性制約で、orcluniqueattrname の値が同一で、orcluniquesubtree、orcluniquescope および orcluniqueobjectclass の値が異なる場合は、異なる制約の属性一意性の有効範囲に属するエントリを結合したものがチェックされます。

たとえば、8-4 ページの図 8-1 で、ユーザーが、次のような 2 つの属性一意性制約を定義するとします。

制約 1:

```
orcluniqueattrname: employee_id
orcluniquesubtree: o=sales, c=us, cn=root
orcluniquescope: onelevel
orcluniqueobjectclass: person
```

制約 2:

```
orcluniqueattrname: employee_id
orcluniquesubtree: c=euro, cn=root
orcluniquescope: sub
orcluniqueobjectclass: organization
```

この例で、employee_id の属性一意性は次のエントリに対して適用されます。

- オブジェクト・クラスが person に属しているサブツリー `o=sales,c=us,cn=root` の下のすべてのエントリ
- オブジェクト・クラスが `organization` に属しているサブツリー `c=euro,cn=root` の下のすべてのエントリおよびエントリ `c=euro,cn=root` 自体

属性一意性の管理

この項では、次の項目について説明します。

属性一意性エントリの位置

属性一意性制約エントリは、
`cn=unique,cn=Common,cn=Products,cn=OracleContext` の下に格納されます。

Oracle Directory Manager を使用した属性一意性の管理

Oracle Directory Manager を使用して、属性一意性制約エントリの作成、変更および削除を実行できます。

属性一意性制約エントリの作成

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**、「**属性一意性管理**」の順に展開します。「属性一意性管理」ウィンドウが表示され、右側のペインに既存の属性一意性制約エントリがリストされます。
2. ツールバーの「**作成**」ボタンを選択します。「新規制約」ウィンドウが表示されます。

   「新規制約」ウィンドウの各フィールドに値を入力します。詳細は、C-4 ページの表 C-6 を参照してください。
3. 「**OK**」を選択します。「属性一意性管理」ウィンドウに戻ります。作成したエントリが、属性一意性制約エントリのリストに表示されます。
4. 「**適用**」を選択します。

Oracle Directory Manager を使用した属性一意性制約エントリの変更

属性一意性制約エントリを変更する手順は次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**、「**属性一意性管理**」の順に展開します。「属性一意性管理」ウィンドウが表示され、右側のペインに既存の属性一意性制約エントリがリストされます。
2. 「属性一意性管理」ウィンドウで、変更する属性一意性制約エントリを選択した後、「**編集**」を選択します。その属性の「属性一意性制約」ウィンドウが表示されます。
3. 「属性一意性制約」ウィンドウで、該当するフィールドに変更する値を入力した後、「**OK**」を選択します。「属性一意性管理」ウィンドウに戻ります。
4. 「**適用**」を選択します。

Oracle Directory Manager を使用した属性一意性制約ポリシーの削除

属性一意性制約ポリシーを削除する手順は次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**、「**属性一意性管理**」の順に展開します。「属性一意性管理」ウィンドウが表示され、右側のペインに既存の属性一意性制約エントリがリストされます。
2. 「属性一意性管理」ウィンドウで、削除する属性一意性制約エントリを選択した後、「**編集**」を選択します。この属性の「属性一意性制約」ウィンドウが表示されます。
3. 「**削除**」を選択し、確認を求めるプロンプトで削除を確認します。「属性一意性制約」ウィンドウに戻ります。削除したエントリは、属性一意性制約エントリのリストに表示されなくなります。

コマンドライン・ツールを使用した属性一意性の管理

この項では、次の項目について説明します。

コマンドライン・ツールを使用した属性一意性の有効化および無効化

既存の属性一意性制約エントリに対する属性一意性を有効または無効にできます。

既存の属性一意性制約エントリに対する属性一意性を有効にする手順は、次のとおりです。

1. ldapmodify を使用して、`orcluniqueenable` 属性を `1` に設定します。
2. ディレクトリ・サーバーを再起動して、ポリシーを有効にします。

属性一意性を無効化する手順は、次のとおりです。

1. ldapmodify を使用して、orcluniqueenable 属性を 0 に設定します。
2. ディレクトリ・サーバーを再起動して、ポリシーを無効にします。

コマンドライン・ツールを使用した属性一意性制約エントリの作成

属性一意性を有効にするには、8-2 ページの表 8-1 に示した属性を持つ属性一意性制約エントリを指定します。

コマンドライン・ツールを使用したディレクトリ全体を対象とする属性一意性の作成 ディレクトリ全体を対象とする属性一意性のインスタンスを作成するには、値の一意性を適用する属性名を指定します。

たとえば、MyCompany の米国の全従業員に対して一意の従業員識別子を作成する手順は、次のとおりです。

1. 次のように、属性一意性制約エントリを（LDIF フォーマットで）作成します。

```
dn: cn=constraint1, cn=unique, cn=common, cn=products, cn=oraclecontext
objectclass: orclUniqueConfig
orcluniqueattrname: employeenumber
orcluniquesubtree: o=MyCompany, c=US
orcleuniqueobjectclass: person
```

2. 属性一意性機能を適用するには、次のような属性一意性制約エントリをロードします。

```
ldapadd -h host -p port -D DN -w password -f constraint1.dat
```

3. ディレクトリ・サーバーを再起動します。

コマンドライン・ツールを使用した 1 つのサブツリーを対象とする属性一意性の作成 1 つ以上のサブツリーを対象とする属性一意性のインスタンスを作成するには、次の項目を指定します。

- 値の一意性を適用する属性名
- 一意性制約を適用するサブツリーの位置

たとえば、MyCompany が SubscriberCompany1 と SubscriberCompany2 をホスティングしていて、SubscriberCompany1 のみに従業員識別子属性の一意性を適用するとします。uid=dlin,ou=people,o=SubscriberCompany1,dc=MyCompany, dc=com などのエントリを追加する場合は、o=SubscriberCompany1,dc=MyCompany,dc=com サブツリーでのみ一意性を適用する必要があります。これを行うには、属性一意性制約の構成で、サブツリーの識別名を明示的に列挙します。

この場合、LDIF ファイルは次のようになります。

```
dn: cn=constraint1, cn=unique, cn=common, cn=products, cn=oraclecontext
objectclass: orclUniqueConfig
orcluniqueattrname: employeenumber
orcluniquesubtree: o=SubscriberCompany1,dc=MyCompany,dc=com
```

コマンドライン・ツールを使用した 1 つのオブジェクト・クラスを対象とする属性一意性の作成 1 つのオブジェクト・クラスを対象とする属性一意性のインスタンスを作成するには、次の項目を指定します。

- 値の一意性を適用する属性名
- オブジェクト・クラス名

この場合、LDIF ファイルは次のようになります。

```
dn: cn=constraint1, cn=unique, cn=common, cn=products, cn=oraclecontext
objectclass: orclUniqueConfig
orcluniqueattrname: employeenumber
orcleuniqueobjectclass: person
```

コマンドライン・ツールを使用した属性一意性制約エントリの変更

属性一意性エントリを変更するには、エントリの LDIF ファイルを作成し、その後 ldapmodify を使用してそのファイルをディレクトリにアップロードします。

たとえば、次のような既存の属性一意性制約エントリがあるとします。

```
dn: cn=constraint1, cn=unique, cn=common, cn=products, cn=oraclecontext
objectclass: orclUniqueConfig
orcluniqueattrname: employeenumber
orcluniquesubtree: o=MyCompany, c=US
orcleuniqueobjectclass: person
```

この制約を o=MyCompany ではなく c=US に適用する手順は、次のとおりです。

1. LDIF エントリを作成して、orcluniquenesssubtree エントリを次のように変更します。

   ```
   dn: cn=constraint1, cn=unique, cn=common, cn=products, cn=oraclecontext
   changetype: modify
   replace: orcluniquesubtree
   orcluniquesubtree: o=Oracle Corporation, c=US
   ```

2. ldapmodify を使用して、この変更をディレクトリ・サーバーに適用します。

   ```
   ldapmodify -p port -D user -w password -f file_name
   ```

3. ディレクトリ・サーバーを再起動して、この変更を有効にします。

コマンドライン・ツールを使用した属性一意性制約エントリの削除

属性一意性制約ポリシーを削除するには、ldapdelete コマンドライン・ツールを使用します。

1. ldapdelete を使用して、ディレクトリから属性一意性制約エントリを削除します。

```
ldapdelete -p port -D bind_DN -w password
"cn=constraint1,cn=unique,cn=common,cn=products,cn=oraclecontext"
```

2. ディレクトリ・サーバーを再起動して、この変更を有効にします。

Oracle Internet Directory 10*g*（9.0.4）での属性一意性の制限事項

属性一意性制約が Oracle Internet Directory レプリケーション環境にある場合は、各サーバーでの属性一意性制約の構成は慎重に行ってください。この項では、次の項目について説明します。

- 単純なレプリケーション使用例
- マルチマスター・レプリケーション使用例

単純なレプリケーション使用例

クライアント・アプリケーションによる変更はすべてサプライヤ・サーバーで実行されます。したがって、サプライヤ・サーバーの属性一意性制約を使用可能に設定してください。コンシューマ・サーバーで属性一意性制約を使用可能にする必要はありません。コンシューマ・サーバーの属性一意性制約を使用可能にしても、ディレクトリ・サーバーの正しい動作を妨害することはありませんが、パフォーマンスが低下する可能性があります。

マルチマスター・レプリケーション使用例

マルチマスター・レプリケーション使用例では、ノードが同じレプリカのサプライヤとコンシューマの両方として機能します。マルチマスター・レプリケーションでは、ゆるやかな一貫性を持つレプリケーション・モデルを使用します。

1 台のサーバーの属性一意性制約を使用可能にしても、指定された時間に両方のマスターで属性値が一意であることは保証されません。1 台のサーバーのみで属性一意性制約を使用可能にすると、各レプリカに保持されているデータに不整合が発生する可能性があります。

属性一意性制約は、両方のマスターで使用可能にする必要があります。ただし、それでも不整合な状態になる可能性があります。たとえば、両方のマスターで、それぞれのエントリを同じ属性値に変更することができます。ただし、後で変更が別のノードにレプリケートされる際、競合が明白になります。この種の競合解消も考慮する必要があります。競合解消がレプリケーション・サーバー側の問題によるものであるかどうかを調査してください。

9

Oracle Internet Directory の動的および静的グループ

この章では、Oracle Internet Directory で静的グループと動的グループの両方を管理する方法について説明します。この章では、次の項目について説明します。

- グループの概要
- Oracle Internet Directory 10g（9.0.4）での動的グループの制限事項
- グループ・エントリの管理

グループの概要

Oracle Internet Directory では、静的グループと動的グループでメンバーシップの割当ておよび管理を実行できます。各タイプのグループは、それぞれ異なる目的に適しています。

この項では、次の項目について説明します。

- 静的グループ
- 動的グループ
- 階層
- グループ・エントリの問合せ
- 使用するグループを検討する場合の考慮事項
- Oracle Internet Directory 10g（9.0.4）での動的グループの制限事項

静的グループ

静的グループは、明示的に管理するメンバーのリストを含むエントリで構成されるグループです。

静的グループに対しては、管理者がそのメンバーシップを明示的に管理する必要があります。たとえば、メンバーが名前を変更した場合、管理者はそのメンバーが属する各グループでそのユーザーの識別名を変更する必要があります。このため、静的グループは、メンバーシップの変更が頻繁に行われないグループに適しています。また、静的グループにはメンバーの識別名のリストが含まれているため、ディレクトリ内でのフットプリントがそのメンバーシップ・リストによって増加します。このため、静的グループは、エントリがディレクトリの領域を取らないグループに適しています。

静的グループ作成のためのスキーマ要素

この種のグループのエントリを作成する場合は、エントリを `groupOfNames` オブジェクト・クラスまたは `groupOfUniqueNames` オブジェクト・クラスのいずれかと関連付けます。

いずれのオブジェクト・クラスにも、グループ・メンバーの名前を格納するための複数値属性があります。ユーザーをグループのメンバーとして割り当てるには、各メンバーの識別名を対応する複数値属性に追加します。逆に、グループからメンバーを削除するには、そのメンバーの識別名を対応する属性から削除します。この複数値属性は、`groupOfNames` オブジェクト・クラスでは `member` で、`groupOfUniqueNames` オブジェクト・クラスでは `uniqueMember` です。

動的グループ

動的グループは、そのメンバーシップがリストで管理されるのではなく、指定した規則およびアサーションに基づいてその場で計算されるグループです。たとえば、ou=americas ネーミング・コンテキストのすべてのユーザーに電子メールを送信するとします。これを行うには、対象のネーミング・コンテキストとして ou=americas を指定した動的グループを作成します。また、電子メール・アドレスのみが戻されるように指定します。電子メール・アプリケーションがその特定のグループについてディレクトリに問い合せると、ディレクトリ・サーバーはメンバーシップを動的に計算し、対応する電子メール・アドレスのリストを戻します。

別の例として、Anne Smith という名前のマネージャの部下であるすべての従業員に電子メールを送信するとします。この場合は、前述の例のようなネーミング・コンテキストは指定しません。かわりに、Anne Smith の部下であるすべての従業員の電子メール・アドレスを取得するように指定した動的グループを作成します。前述の例と同様に、電子メール・アプリケーションがその特定のグループについてディレクトリに問い合せると、ディレクトリ・サーバーはメンバーシップを動的に計算し、対応する電子メール・アドレスのリストを戻します。

注意： この例で、電子メール・アプリケーションは、メンバーシップ・リストではなく、メンバーの特定の属性を読み取ることをディレクトリ・サーバーに対して指定します。これは、コントロール 2.16.840.1.113894.1.8.5 を渡すことによって行われます。

また、ユーザーが属するグループを問い合せる場合、アプリケーションは、静的グループに加えて動的グループも問合せ対象とすることができます。このような状況が発生した場合は、コントロール 2.16.840.1.113894.1.8.7 が渡されます。このコントロールが渡されない場合は、静的グループのみが問合せ対象となります。

関連項目：『Oracle Internet Directory アプリケーション開発者ガイド』の第 7 章「Oracle Internet Directory の C API」

動的グループ作成のためのスキーマ要素

動的グループを作成する場合も、静的グループの作成と同様に、まず、エントリを groupOfNames オブジェクト・クラスまたは groupOfUniqueNames オブジェクト・クラスのいずれかと関連付けます。次に、そのオブジェクト・クラスを補助型オブジェクト・クラス orclDynamicGroup と関連付けます。この補助型オブジェクト・クラスには、グループのメンバーシップを動的に計算するための 2 つの方法のいずれかを指定する各種属性があります。

この 2 つの方法は、次のとおりです。

- labeledURI 属性を使用する方法

  この方法を使用する場合、ディレクトリ・サーバーはディレクトリ情報ツリーの階層構造に基づいて通常の検索を実行します。この検索を実行するには、orclDynamicGroup オブジェクト・クラスの属性の 1 つ labeledURI に対して値を設定する必要があります。この属性には、問合せのベース、フィルタ、その他の必要なすべての属性を指定します。たとえば、labeledURI 属性に次のような値を入力したとします。

  ```
  labeledURI:ldap://host name/"ou=MyOrganizationalUnit,o=MyCompany,c=US"??sub"
  (objectclass=person)
  ```

  この方法を使用した場合、エントリの検索では、グループのすべてのメンバーのエントリが戻されます。

  > **関連項目：** labeledURI 属性などで LDAP URL を表示する方法については、『The LDAP URL Format (Request for Comments 2255)』（T. Howes、M. Smith 著、1997 年 12 月）を参照してください。Web サイト http://www.ietf.org で入手可能です。

- CONNECT BY アサーションの使用

  この方法は、前述の方法と異なり、ディレクトリ情報ツリーの階層構造ではなく、エントリを暗黙に相互接続している属性を利用します。これはディレクトリ情報ツリー内での位置に関係しません。たとえば、manager 属性は、従業員のエントリをその上司のエントリと接続します。この接続は、ディレクトリ情報ツリー内での従業員の位置に関係なく適用されます。この方法では、CONNECT BY 句を使用して、階層を作成するために使用する属性（manager など）およびそのような階層の開始値（cn=Anne Smith など）を指定します。

  この方法を使用するには、表 9-1 に示す各単一値属性の値を orclDynamicGroup オブジェクト・クラスに指定します。

表 9-1 Connect By アサーションのための orclDynamicGroup 属性

属性	説明
orclConnectByAttribute	問合せのフィルタとして使用する属性。例 : manager
orclConnectByStartingValue	orclConnectByAttribute 属性に指定した属性の識別名。例 : Anne Smith

たとえば、米国の MyOrganizational Unit の Anne Smith の部下であるすべての従業員のエントリを取得するには、前述の属性に対して次のような値を設定します。

```
orclConnectByAttribute=manager
orclConnectByStartingValue=
"cn=Anne Smith,ou=MyOrganizationalUnit,o=MyCompany,c=US"
```

また、すべてのメンバーの特定の属性（email 属性など）の値を取得することを指定するアプリケーションを開発することもできます。

関連項目： 特定の属性の値を取得するアプリケーションを開発する方法の詳細は、『Oracle Internet Directory アプリケーション開発者ガイド』を参照してください。

階層

階層は、明示的または暗黙的のいずれかにできます。

明示的階層では、ディレクトリ情報ツリーのエントリの位置によって関係が決まります。たとえば、グループ A はディレクトリ情報ツリーでグループ B より上位にあります。

暗黙的階層では、エントリ間の関係は、ディレクトリ情報ツリー内の位置によってではなく、特定の属性の値によって決まります。たとえば、John Doe のエントリが Anne Smith と同じレベルの階層にあるディレクトリ情報ツリーがあるとします。ただし、John Doe のエントリでは、manager 属性に Anne Smith が彼の上司として指定されているとします。この場合、ディレクトリ情報ツリーでの両方の位置は同レベルですが、Anne Smith は John Doe の上司として指定されているため、階層のランクは同一ではありません。

注意： 階層グループを作成する場合は、真の階層となるように注意してください。たとえば、真の階層では、グループ A はグループ B のメンバーとなることができますが、グループ B が同時にグループ A のメンバーとなることはできません。後者の関係は循環的であるため、グループ A のメンバーの検索は失敗します。

暗黙的階層に基づく問合せでは、クライアントは検索要求にコントロール 2.16.840.1.113894.1.8.3 を指定できます。この問合せのフィルタは、暗黙的階層の作成に使用する属性を指定します。たとえば、(manager=cn=john doe,o=foo) と指定すると、John Doe が直接的または間接的に管理するすべての人が問い合されます。暗黙的階層は、manager 属性に基づいたものとなります。このような問合せでは、検索のベースは無視されます。

関連項目： 『Oracle Internet Directory アプリケーション開発者ガイド』の第 7 章「Oracle Internet Directory の C API」

グループ・エントリの問合せ

アプリケーションは、いずれかのグループに問い合せて、次の操作を実行できます。

- グループのすべてのメンバーをリスト
- あるユーザーがメンバーであるすべてのグループをリスト
- あるユーザーが特定のグループのメンバーであるかどうかをチェック

また、指定するメンバー属性について、動的グループに問合せできますが、静的グループには問合せできません。

使用するグループを検討する場合の考慮事項

使用するグループについて検討する場合は、管理の容易性とパフォーマンスの効率を考慮する必要があります。たとえば、動的グループは管理が簡単ですが、パフォーマンスが低下します。表 9-2 に、静的グループまたは動的グループの使用を検討する場合の考慮事項を示します。

表 9-2　静的グループと動的グループについての考慮事項

考慮事項	静的グループ	動的グループ
管理の容易性	グループのメンバーシップが大きく、頻繁に変更がある場合は管理が困難になる	特に、グループのメンバーシップが大きく、頻繁に変更がある場合に有効
パフォーマンス	メンバーシップ・リストを明示的に管理するため、比較的高パフォーマンス	メンバーシップはその場で検索されるため、比較的低パフォーマンス
ディレクトリ内でのフットプリントのサイズ	グループ・メンバーシップのサイズによっては、フットプリントが大きい	グループ・メンバーシップのサイズに関係なく、フットプリントが小さい

Oracle Internet Directory 10*g*（9.0.4）での動的グループの制限事項

このバージョンの Oracle Internet Directory は、アクセス制御リストでの動的グループの使用をサポートしていません。`orclACPgroup` オブジェクト・クラスまたは `orclPrivilegeGroup` オブジェクト・クラスのいずれにも、動的グループを関連付けることはできません。

メンバーの必須の属性について動的グループに問い合せる場合、このリリースは、メンバーシップ・リストに明示的にリストされていないメンバーの属性の読取りのみをサポートします。また、この場合、メンバーシップに基づく ldapsearch フィルタ（`member` または `uniqueMember`）は、動的グループ・オブジェクトに適用できません。

階層グループ解決の問合せは、静的グループに対してのみ機能します。動的グループが静的グループのメンバーである場合、グループの階層全体を解決するための問合せは、動的グループを評価しません。したがって、静的グループ A が別の静的グループ B のメンバーであり、グループ B が静的グループ C のメンバーである場合、あるユーザー（静的グループ A のメンバーであると仮定）がメンバーであるすべてのグループを検出する問合せは、正常にグループ A、B、C を戻します。ただし、グループ C が動的グループである場合、同じ問合せはグループ A と B のみを戻します。

暗黙的階層を解決するための CONNECT BY 問合せは、等価フィルタでのみ機能します。この種の問合せの実行中、検索のベースは使用されません。

グループ・エントリの管理

この項では、次の項目について説明します。

- Oracle Directory Manager を使用した静的グループ・エントリの管理
- コマンドライン・ツールを使用した静的グループ・エントリの管理
- Oracle Directory Manager を使用した動的グループの管理
- コマンドライン・ツールを使用した動的グループの管理

注意： グループの階層を作成する場合は、9-5 ページの「階層」で説明したとおり、必ず真の階層としてください。

関連項目：

- グループ・エントリのアクセス制御ポリシーの設定方法の詳細は、14-3 ページの「セキュリティ・グループ」を参照してください。
- アクセス権限の詳細は、2-12 ページの「グローバリゼーション・サポート」および第 14 章「ディレクトリ・アクセス制御」を参照してください。

Oracle Directory Manager を使用した静的グループ・エントリの管理

Oracle Directory Manager を使用して、静的グループ・エントリの作成と変更の両方を実行できます。

Oracle Directory Manager を使用した静的グループ・エントリの作成

エントリが groupOfNames オブジェクト・クラスに属する場合は、複数値属性 member に識別名を追加してグループのメンバーシップを決定します。エントリが groupOfUniqueNames オブジェクト・クラスに属する場合は、複数値属性 uniqueMember に識別名を追加してグループのメンバーシップを決定します。

静的グループ・エントリを追加する手順は、次のとおりです。

1. 「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開します。
2. 「**エントリ管理**」を選択します。
3. ツールバーの「**作成**」ボタンを選択します。「新規エントリ」ダイアログ・ボックスが表示されます。
4. 「**識別名**」フィールドに、完全な識別名を入力します。「**参照**」を使用して、追加するエントリの親の識別名を検索し、親の識別名の左側にカンマで区切って新規エントリの相対識別名を入力することもできます。
5. 新規エントリに使用するオブジェクト・クラスを指定するには、「**オブジェクト・クラス**」ボックスの右の「**追加**」を選択します。「スーパー・クラス・セレクタ」ダイアログ・ボックスが表示されます。
   a. 「スーパー・クラス・セレクタ」ダイアログ・ボックスで、次のオブジェクト・クラスを選択します。
      * `top`
      * `groupOfNames` または `groupOfUniqueNames`
   b. 「**選択**」を選択します。「新規エントリ」ダイアログ・ボックスの「**オブジェクト・クラス**」ウィンドウに、選択したオブジェクト・クラスが表示されます。
6. グループ・エントリの必須属性とオプション属性を入力します。

   「`groupOfNames`」オブジェクト・クラスを選択した場合は、いくつかのフィールド、たとえば「**必須プロパティ**」タブ・ページの「メンバー」フィールドの横に、「**参照**」ボタンが表示されます。参照によって必須プロパティを入力する手順は、次のとおりです。
   a. 「**参照**」を選択します。「ディレクトリ : エントリ管理」ダイアログ・ボックスが表示されます。
   b. このダイアログ・ボックスを使用して、リストに追加する特定のエントリを検索します。
   c. 「ディレクトリ : エントリ管理」ダイアログ・ボックスの「**識別名**」ウィンドウで、エントリを選択した後、「**OK**」を選択します。「新規エントリ」ダイアログ・ボックスに戻ります。選択したエントリが、「メンバー」ウィンドウのリストに追加されています。
7. 「**OK**」を選択します。

Oracle Directory Manager を使用した静的グループ・エントリの変更

グループ・エントリのメンバー・リストを変更する手順は、次のとおりです。

1. 変更するグループ・エントリを検索します。
2. 右側のペインの「**識別名**」ボックスで、変更するグループ・エントリを選択します。
3. 「**編集**」を選択します。
4. 「エントリ」ダイアログ・ボックスで、member 属性のテキスト領域までスクロールして、その値を変更します。
5. 「**OK**」を選択します。

コマンドライン・ツールを使用した静的グループ・エントリの管理

この項では、静的グループ・エントリを作成および変更する方法の例を示します。

ldapadd を使用した静的グループ・エントリの作成

LDIF ファイルの構文は、次のとおりです。

```
dn: DN_of_group_entry
objectclass: top
objectclass: [groupOfNames] [groupOfUniqueNames]
member: DN of member 1
member: DN of member 2
.
.
.
member: DN of member N
```

次のコマンドは、この LDIF ファイルをディレクトリに追加します。

```
ldapadd -p port_number -h host -f file_name.ldif
```

例 : ldapadd を使用した静的グループ・エントリの作成　次の例は、MyStaticGroup というグループのエントリ用の myStaticGroup.ldif という LDIF ファイルを示しています。

```
dn: cn=myStaticGroup,c=us
objectclass: top
objectclass: groupOfNames
member: cn=John Doe
member: cn=Anne Smith
```

次のコマンドは、この LDIF ファイルをディレクトリに追加します。

```
ldapadd -p 389 -h myhost -f myStaticGroup.ldif
```

ldapmodify を使用した静的グループの変更

グループにメンバーを追加する場合、LDIF ファイルの構文は次のようになります。

```
dn: DN_of_group_entry
changetype: modify
add:member
member:DN of member entry
```

グループからメンバーを削除する場合、LDIF ファイルの構文は次のようになります。

```
dn: DN of group entry
changetype: modify
delete:member
member:DN of member entry
```

ファイルを変更するには、次のコマンドを発行します。

```
ldapmodify -p 389 -v  -f file_name.ldif
```

-v は冗長モードを指定します。

例 : ldapmodify を使用した静的グループの変更　次の例は、John Doe を MyStaticGroup というグループに追加します。前述の例と同様に、このユーザー・エントリに関するデータは myStaticGroup.ldif ファイルに記述されています。このファイルの内容は次のとおりです。

```
dn: cn=myStaticGroup,c=us
changetype: modify
add:member
member: cn=John Doe
```

ファイルを変更するには、次のコマンドを発行します。

```
ldapmodify -p 389 -v  -f myStaticGroup.ldif
```

-v は冗長モードを指定します。

注意 :　エントリを追加または変更する場合、Oracle ディレクトリ・サーバーではエントリの存在は検証されません。ただし、属性値に識別名を含める必要がある場合、ディレクトリ・サーバーは識別名が指定されていることを検証します。

Oracle Directory Manager を使用した動的グループの管理

Oracle Directory Manager を使用して、静的グループ・エントリの作成と変更の両方を実行できます。

Oracle Directory Manager を使用した動的グループ・エントリの作成

エントリが groupOfNames オブジェクト・クラスに属する場合は、複数値属性 member に識別名を追加してグループのメンバーシップを決定します。エントリが groupOfUniqueNames オブジェクト・クラスに属する場合は、複数値属性 uniqueMember に識別名を追加してグループのメンバーシップを決定します。

動的グループ・エントリを追加する手順は、次のとおりです。

1. 「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開します。
2. 「**エントリ管理**」を選択します。
3. ツールバーの「**作成**」ボタンを選択します。「新規エントリ」ダイアログ・ボックスが表示されます。
4. 「**識別名**」フィールドに、完全な識別名を入力します。「**参照**」を使用して、追加するエントリの親の識別名を検索し、親の識別名の左側にカンマで区切って新規エントリの相対識別名を入力することもできます。
5. 新規エントリに使用するオブジェクト・クラスを指定するには、「**オブジェクト・クラス**」ボックスの右の「**追加**」を選択します。「スーパー・クラス・セレクタ」ダイアログ・ボックスが表示されます。
   a. 「スーパー・クラス・セレクタ」ダイアログ・ボックスで、次のオブジェクト・クラスを選択します。
      * top
      * orcldynamicgroup
      * groupOfNames または groupOfUniqueNames
   b. 「**選択**」を選択します。「新規エントリ」ダイアログ・ボックスの「**オブジェクト・クラス**」ウィンドウに、選択したオブジェクト・クラスが表示されます。

6. グループ・エントリの必須属性とオプション属性を入力します。

   「**オプション・プロパティ**」タブ・ページの「labeledURI」フィールドで、次のように指定します。

   ldap:*ldap_URL*

   たとえば、次のように入力します。

   ```
   ldap://my_host/ou=MyNeworganizationalUnit,o=MyCompany,c=US??sub?
   (objectclass=person)
   ```

   「orclConnectByAttribute」フィールドで、問合せのフィルタとして使用する属性（manager など）を指定します。

   「orclConnectByStartingValue」フィールドで、orclConnectByAttribute 属性で指定した属性の識別名（cn=Anne Smith など）を指定します。

   「**オプション・プロパティ**」タブ・ページに表示される他の属性の指定については、付録 B「Oracle Internet Directory のスキーマ要素」を参照してください。

   「groupOfNames」オブジェクト・クラスを選択した場合は、いくつかのフィールド、たとえば「**必須プロパティ**」タブ・ページの「メンバー」フィールドの横に、「**参照**」ボタンが表示されます。「参照」を選択すると、「ディレクトリ：エントリ管理」ダイアログ・ボックスが表示されます。このダイアログ・ボックスを使用して、リストに追加する特定のエントリを検索します。次に、「ディレクトリ：エントリ管理」ダイアログ・ボックスの「**識別名**」ウィンドウで、エントリを選択した後、「**OK**」を選択します。「新規エントリ」ダイアログ・ボックスに戻ります。選択したエントリが、「メンバー」ウィンドウのリストに追加されています。

7. 「**OK**」を選択します。

Oracle Directory Manager を使用した動的グループ・エントリの変更

動的グループ・エントリのメンバー・リストを変更する手順は、次のとおりです。

1. 変更するグループ・エントリを検索します。
2. 右側のペインの「**識別名**」ボックスで、変更するグループ・エントリを選択します。
3. 「**編集**」を選択します。
4. 「エントリ」ダイアログ・ボックスで、member 属性のテキスト領域までスクロールして、その値を変更します。
5. 「**OK**」を選択します。

コマンドライン・ツールを使用した動的グループの管理

この項では、コマンドライン・ツールを使用して動的グループを作成および変更する方法について説明します。

ldapadd を使用した動的グループ・エントリの作成

labeledURI 属性を使用する場合、LDIF ファイルの構文は次のようになります。

```
dn: DN_of_group_entry
objectclass: top
objectclass: [groupOfNames] [groupOfUniqueNames]
objectclass: orcldynamicgroup
labeledURI:ldap:ldap_URL
member: DN of member 1
member: DN of member 2
.
.
.
member: DN of member N
```

次のコマンドは、この LDIF ファイルをディレクトリに追加します。

```
ldapadd -p port_number -h host -f file_name.ldif
```

CONNECT BY 文字列を使用する場合、LDIF ファイルの構文は次のようになります。

```
dn: DN_of_group_entry
objectclass: top
objectclass: [groupOfNames] [groupOfUniqueNames]
objectclass: orclDynamicGroup
orclConnectByAttribute: attribute_name
orclConnectByStartingValue: DN_of_attribute
member: DN_of_member_1
```

この構文でエントリを指定する場合は、識別名を二重引用符で囲まないでください。

例 : ldapadd を使用した動的グループ・エントリの作成

次の例は、動的グループのエントリ用の LDIF ファイルを示しています。

```
dn: cn=myDynamicGroup,c=us
objectclass: top
objectclass: groupOfNames
objectclass: orcldynamicgroup
labeledURI:ldap:
//my_host/ou=MyNeworganizationalUnit,o=MyCompany,c=US??sub?(objectclass=person)
member: cn=John Doe
member: cn=Anne Smith
```

次のコマンドは、この LDIF ファイルをディレクトリに追加します。

```
ldapadd -p 389 -h myhost -f myDynamicGroup.ldif
```

例 : ldapmodify を使用した動的グループの変更

前述の例で作成したグループの組織単位を変更する場合、LDIF ファイルの構文は次のようになります。

```
dn: DN_of_group_entry
changetype: modify
replace:labeledURI
labeledURI:ldap:
//my_host/ou=MyNeworganizationalUnit,o=MyCompany,c=US??sub?(objectclass=person)
```

注意 : エントリを追加または削除する場合、Oracle ディレクトリ・サーバーではエントリ属性値の構文検証は行われません。

10

ディレクトリのロギング、監査および監視

Oracle Internet Directory には、ディレクトリのデバッグ、監査および監視を行うための包括的フレームワークが用意されています。この章では、次の項目について説明します。

- デバッグ・ロギングの使用
- 監査ログの使用方法
- Oracle Internet Directory サーバーの監視

デバッグ・ロギングの使用

この項では、次の項目について説明します。

Oracle Internet Directory デバッグ・ロギングの概要

Oracle Internet Directory では、次のことが可能になります。

- ディレクトリ・サーバー、ディレクトリ・レプリケーション・サーバー、Oracle Directory Integration and Provisioning Server に関するロギング情報の表示
- ロギング・レベルの設定
- ロギングする操作の指定
- 致命的エラーおよび重大エラーに対する対処方法を調べるための標準形式のメッセージの検索
- 重大度と重要性の度合いによるトレース・メッセージの表示
- エントリの識別名、ACP 評価、操作のコンテキストなどに関する関連情報の入ったトレース・メッセージを調べることによる Oracle Internet Directory コンポーネントの診断

ログ・メッセージの概要

この項では、特定の LDAP 操作と関連付けられたログ・メッセージおよび関連付けられていないログ・メッセージについて説明します。トレース・ログの例と、その解釈方法を示します。

特定の LDAP 操作に関するログ・メッセージ

特定の操作に関するログ・メッセージは、トレース・オブジェクトとして格納されます。このオブジェクトは、各種の Oracle Internet Directory モジュールにわたって、操作の開始から終了までを追跡します。これは、次のいずれかの状態が発生した場合に記録されます。

- LDAP 操作が完了したとき
- 優先度の高いメッセージが記録されたとき
- トレース・メッセージ・バッファが一杯になったとき

各スレッドは、各操作に連続する情報のブロックを持ち、そのブロックは明確に区切られます。したがって、共有サーバー環境でも、異なるスレッド、操作、接続に関するメッセージの追跡が容易です。

内部メッセージ・バッファ・オーバーフローのため、1 つのトレース・オブジェクトに 1 つの操作に関する情報をすべて格納できない場合、情報は複数のトレース・オブジェクトに分散されます。分散された情報の各部分は明確に区切られており、共通のヘッダーが付けられます。操作の進行を追跡するには、トレース・オブジェクトとその共通ヘッダーを最後までたどります。最後は、「操作が完了しました。」というトレース・メッセージで識別できます。

特定の LDAP 操作と関連付けられていないログ・メッセージ

どの LDAP 操作とも関連付けられていないメッセージは、オブジェクト・ベースではない単純な形式で表示されます。これは、操作が完了したとき、または優先度の高いメッセージが発生したときにログ・ファイルに記録されます。

例 : Oracle Internet Directory サーバー・ログ・ファイル内のトレース・メッセージ

```
2003/01/28:13:44:27 * Main:1 * Starting up the OiD Server, on node dthakuri-sun

2003/01/28:13:44:27 * Main:1 * Oid Server Connected to DB store via inst1 connect
string.
2003/01/28:13:44:27 * Main:1 * OiD LDAP server started.

2003/01/28:13:44:31 * ServerController:1 * INFO * slsfctSpawnDispatcher * Entry
2003/01/28:13:44:31 * ServerController:1 * INFO * gslsfctSpawnDispatcher * Spawned
server dispatcher thread successfully. Thread id : 1
2003/01/28:13:44:31 * ServerController:1 * INFO * gslsfctSpawnDispatcher * Exit


2003/01/28:13:44:31 * ServerWorker:6 * INFO : ServerWorker : Entry
2003/01/28:13:44:31 * ServerWorker:6 * INFO : gslsfccRegisterThread : Entry
2003/01/28:13:44:31 * ServerWorker:6 * INFO : gslsfccRegisterThread : Exit
2003/01/28:13:44:31 * ServerWorker:6 * INFO * gslfsfAStr2Filter *
Filter="(|(objectclass=referral))"
2003/01/28:13:44:31 * ServerWorker:6 * INFO * gslfsfAStr2Filter *
Filter="(objectclass=referral)"
2003/01/28:13:44:31 * ServerWorker:6 * INFO * gslfsfCStr2Simple *
Filter="objectclass=referral"
2003/01/28:13:44:31 * ServerWorker:6 * INFO * gslsbnrNormalizeString() String to
Normalize: "objectclass"
2003/01/28:13:44:31 * ServerWorker:6 * INFO * gslsbnrNormalizeString() Normalized
value: "objectclass"
```

```
BEGIN
2003/01/28:13:45:49 * ServerWorker:6 * ConnID:0 * OpId:0 * OpName:bind
13:45:49 * INFO * gslfbiADoBind * Entry
13:45:49 * INFO * gslfbiGetControlInfo * Entry
13:45:49 * INFO * gslfbiGetControlInfo * Exit
13:45:49 * INFO * gslfbiADoBind * connID=0 opID=0 Version=3 BIND dn="" method=128
13:45:49 * INFO * gslfrsBSendLdapResult * Entry
13:45:49 * INFO * gslfrsASendLdapResult2 * Entry
13:45:49 * INFO * sgslunwWrite * Entry
13:45:49 * INFO * sgslunwWrite * Exit
13:45:49 * INFO * gslfrsASendLdapResult2 * Exit
13:45:49 * INFO * gslfrsBSendLdapResult * Exit
13:45:49 * INFO * gslfbiADoBind * Exit
13:45:49 * INFO * Total Bind operation time for dn=2588  micro sec and Total Worker
time=3434  micro sec
END

2003/01/28:13:45:49 * ServerWorker:6 * INFO * ServerWorker * Operation Complete

2003/01/28:13:44:31 * ServerWorker:7 * INFO * ServerWorker : Entry
2003/01/28:13:44:31 * ServerWorker:7 * INFO * gslsfccRegisterThread : Entry
2003/01/28:13:44:31 * ServerWorker:7 * INFO * gslsfccRegisterThread : Exit


BEGIN
2003/01/28:13:48:53 * ServerWorker:13 * ConnID:0 * OpId:0 * OpName:bind
13:48:14 * INFO * gslfbiADoBind * Entry
13:48:53 * INFO * gslfbiGetControlInfo * Entry
13:48:53 * INFO * gslfbiGetControlInfo * Exit
13:48:53 * INFO * gslfbiADoBind * conn=0 op=0 Version=3 BIND dn="cn=proxy"
method=128
13:48:53 * INFO * gslsbbBind * Entry
13:48:53 * INFO * gslsbnrNormalizeString * String to Normalize: "proxy"
13:48:53 * INFO * gslsbnrNormalizeString * Normalized value: "proxy"
13:48:53 * INFO * gslfrsBSendLdapResult * Entry
13:48:53 * INFO * gslfrsASendLdapResult2 * Entry
13:48:53 * INFO * sgslunwWrite * Entry
13:48:53 * INFO * sgslunwWrite * Exit
13:48:53 * INFO * gslfrsASendLdapResult2 * Exit
13:48:53 * INFO * gslfrsBSendLdapResult * Exit
13:48:53 * INFO * gslsbbBind * Exit
13:48:53 * INFO * gslfbiADoBind:Exit
13:48:53 * INFO * Total Bind operation time for dn = cn=proxy is  3710  micro sec
 Total Worker time = 4767  micro sec
END

2003/01/28:13:48:53 * ServerWorker:13 * INFO * ServerWorker * Operation Complete
```

```
2003/01/28:14:05:56 * ServerWorker:6 * FATAL * ServerWorker * Processing shutdown
notification
2003/01/28:14:05:56 * ServerWorker:6 * WARNING * ServerWorker * Shutting down worker
ID :  6
```

ログ・ファイル内のトレース・メッセージの解釈方法

前述のメッセージ例に示したとおり、ログ情報は、操作を実行するスレッド、または操作を実行しないスレッドのいずれかと関連付けることができます。操作を実行するスレッドのログのヘッダーには、次の項目が格納されます。

- 日時
- 特定の接続のスレッド名と識別子
- 接続識別子
- 関連付けられた操作の名前と識別子

操作を実行しないスレッドでは、通常のトレース・メッセージが記録されます。そのヘッダーには、日時とスレッド識別子が格納されます。接続および操作に関係する情報は含まれません。

トレース・オブジェクトは、キーワード `BEGIN` で始まり、キーワード `END` で終わります。

表 10-1 に、トレース・メッセージ内の各フィールドを示します。

表 10-1 トレース・メッセージ内のフィールド

フィールド 1	フィールド 2	フィールド 3	フィールド 4	フィールド 5	フィールド 6
オブジェクトに基づかないメッセージの場合 : 日時 オブジェクトに基づくメッセージの場合 : 時刻のみ	非オブジェクト・ベースのトレース・メッセージのみの場合、スレッド識別子	トレース・メッセージの重大性。次の 4 つの値があります。 ■ FATAL ■ ERROR ■ WARN（警告） ■ INFO（通知）	機能名	実行された操作に関する情報。この情報は、問題の診断のために使用できます。	エラー・コード（該当する場合）。エラー・コードには、オペレーティング・システム、Oracle データベースまたは LDAP に関するものがあります。

デバッグ・ロギング・レベルの設定

Oracle Directory Manager または **OID 制御ユーティリティ**を使用して、デバッグ・ロギング・レベルを設定できます。

Oracle Directory Manager を使用したデバッグ・ロギング・レベルの設定

デバッグ・ロギング・レベルを設定する手順は、次のとおりです。

1. ナビゲータ・ペインで、「Oracle Internet Directory サーバー」を展開して、サーバーのインスタンスを選択します。そのサーバーに対応するタブ・ページが右側のペインに表示されます。
2. 「**デバッグ・フラグ**」タブを選択します。
3. 「**デバッグ・フラグ**」を選択します。

   通常、このタブ・ページのチェックボックスは選択する必要がありません。ただし、特定の問題に関するログを生成するには、このタブ・ページでデバッグ・ロギング・レベルを指定します。

OID 制御ユーティリティを使用したデバッグ・ロギング・レベルの設定

OID 制御ユーティリティを使用してデバッグ・ロギング・レベルを設定するには、LDAP サーバーの場合は `-debug` フラグを、レプリケーション・サーバーの場合は `-d` フラグを使用して、Oracle ディレクトリ・サーバーを再起動します。10-7 ページの表 10-2 に基づいて、デバッグ・レベルの数値を設定します。

デバッグ・レベルは加算方式であるため、アクティブ化する機能を表す数値を加算し、その合計値をコマンドライン・オプションに使用する必要があります。

デフォルトでは、デバッグ・ログは記録されません。デバッグ・ログを記録するには、**ディレクトリ固有のエントリ**（DSE）属性 `orcldebugflag` を必要なレベルに変更します。デバッグ・レベルは、次のレベルのいずれかに構成できます。

OID 制御ユーティリティによって生成されたデバッグ・ログ・ファイルを見るには、`$ORACLE_HOME/ldap/log` にナビゲートします。

表 10-2 に、デバッグ・ロギング・レベルの全リストを示します。

表 10-2 デバッグ・ロギング・レベル

ロギング・レベルの値	提供される情報
1	大容量トレースのデバッグ
128	パケット・ハンドリングのデバッグ
256	接続管理（ネットワーク・アクティビティ関連）
512	検索フィルタの処理
1024	エントリの解析
2048	構成ファイルの処理
8192	アクセス制御リストの処理
491520	バックエンド（つまり、データベース）との通信のログ
524288	スキーマ関連の操作
4194304	レプリケーション固有の操作
8388608	各接続に関するエントリ、操作および結果のログ
16777216	ファンクション・コール引数のトレース
67108863	潜在的なすべての操作 / データ

たとえば、検索フィルタ処理（512）とアクティブな接続管理（256）をトレースするには、次のようにデバッグ・レベルとして 768（512 + 256 = 768）を入力します。

```
oidctl server=oidldapd instance=1 flags='-debug 768' restart
oidctl server=oidrepld instance=1 flags='-h my_host -p 389 -d 768' restart
```

この例では、デバッグ・フラグを付けて、Oracle ディレクトリ・サーバーと Oracle ディレクトリ・レプリケーション・サーバーを再起動しています。

操作デバッグ・ディメンションの設定

ロギングの対象を絞り込むには、デバッグ・レベルと組み合せてデバッグ・ディメンションを使用します。たとえば、ロギングを特定のディレクトリ・サーバー操作に限定するには、それらの操作に対してデバッグ・ディメンションを指定します。

表 10-3 に、これらのディメンションを示します。

表 10-3 LDAP 操作に関するデバッグ・ディメンション値

操作デバッグ・ディメンション値	提供される情報
1	ldapbind
2	ldapunbind
4	ldapadd
8	ldapdelete
16	ldapmodify
32	ldapmodrdn
64	ldapcompare
128	ldapsearch
256	ldapabandon
511	すべての LDAP 操作

デバッグ・ディメンションの設定には、Oracle Directory Manager または ldapmodify のいずれかを使用できます。

Oracle Directory Manager を使用した操作デバッグ・ディメンションの設定

操作デバッグ・ディメンションを設定する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」を展開して、サーバー・インスタンスを選択します。そのサーバーに対応するタブ・ページが右側のペインに表示されます。
2. 「**デバッグ・フラグ**」タブを選択します。
3. 「**デバッグ操作フラグ**」を選択します。

デフォルトでは、すべての操作が選択されます。ただし、特定の操作に関するログを生成するには、対応する操作を選択します。複数の操作を選択できます。

ldapmodify を使用した操作デバッグ・ディメンションの設定

複数の操作を記録するには、そのディメンションの値を加算します。たとえば、ldapbind（1）、ldapadd（4）および ldapmodify（16）の操作をトレースする場合、orcldebugop 属性を 21（1 + 4 + 16 = 21）に設定した LDIF ファイルを作成します。この LDIF ファイルは、次のようになります。

```
dn:
changetype:modify
replace:orcldebugop
orcldebugop:21
```

このファイルをロードするには、次のように入力します。

```
ldapmodify -h host_name -p port_number -f file_name
```

ログ・ファイルへのトレース情報のフラッシュの強制

I/O 操作のパフォーマンス・オーバーヘッドを最小限にするため、デバッグ・メッセージは、メッセージがディレクトリ・サーバーに記録されるたびにではなく、定期的にログ・ファイルにフラッシュされます。ログ・ファイルへの書込みは、次のいずれかの状態が発生した場合に実行されます。

- LDAP 操作が完了したとき
- 優先度の高いメッセージが記録されたとき
- トレース・メッセージ・バッファが一杯になったとき

ただし、場合によっては、定期的なフラッシュを待たずに、トレース・メッセージが記録されたときにログ・ファイルでそれを検証する必要があります。これを行うには、DSA 構成属性 orcldebugforceflush を 1 に設定します。次の例に示すとおり、ldapmodify を使用して、これを行います。

ldapmodify を使用して強制フラッシュを使用可能にするには、次のような LDIF ファイルを作成します。

```
dn: cn=dsaconfig,cn=configsets,cn=oracle internet directory
changetype: modify
replace: orcldebugforceflush
orcldebugforceflush: 1
```

このファイルをロードするには、次のように入力します。

```
ldapmodify -h host_name -p port_number -f file_name
```

注意：

- 強制フラッシュが使用可能な場合、各操作のトレース・メッセージ・オブジェクトの形式は断片化されたものになります。
- デフォルトでは、強制フラッシュは使用禁止です。必要な情報をログ・ファイルにフラッシュした後は、強制フラッシュを使用禁止にしてください。

関連項目： `orcldebugforceflush` 属性の詳細は、B-7 ページの表 B-6 を参照してください。

監査ログの使用方法

監査ログには、Oracle ディレクトリ・サーバーに関するセキュリティ上および操作上重要なイベントが記録されています。ログはディレクトリ・サーバーのイベントによって生成されるため、管理者による監査ログ・エントリの作成はできません。監査ログ・エントリを作成できるのはディレクトリ・サーバー自体のみです。

監査ログは、通常のディレクトリ・エントリで構成されています。イベントごとに 1 つのエントリがあります。監査ログは ldapsearch を使用して問い合せることができ、監査ログ・エントリは Oracle Directory Manager を使用して表示できます。

デフォルトでは、監査ログは使用禁止です。監査ログを使用可能にするには、ディレクトリ固有のエントリ（DSE）属性の `orclauditlevel` を必要なレベルに変更します。監査レベルは、選択したイベントのみを監査するように構成できます。

関連項目：

- 監査レベルのリストは、10-12 ページの「監査可能なイベント」を参照してください。
- 監査レベルの指定は、10-13 ページの「監査レベルの設定」を参照してください。
- 10-16 ページの「Oracle Directory Manager を使用した監査ログ・エントリの検索」
- 10-17 ページの「ldapsearch を使用した監査ログ・エントリの検索」
- A-28 ページの「ldapdelete の構文」

監査ログ・エントリの構造

各監査ログ・エントリには、orclAuditoc **オブジェクト・クラス**が含まれています。他のすべての構造型オブジェクト・クラスと同様に、orclAuditoc は、top から属性を継承します。その属性は次のとおりです。

表 10-4 オブジェクト・クラスの属性

属性	説明
orclsequence	エントリ名の作成に使用されます。名前は、データベース順序を使用して生成されます。
orcleventtype	発生したイベントのタイプを指定します。この属性はカタログ化されています。
orcleventtime	イベントを発生させる時刻を指定します。時刻は、**UTC (Coordinated Universal Time)** 形式です。UTC 形式であることは、値の最後の z によって示されます。例 : orcleventtime: 199811281010z
orcluserdn	操作を実行するために Oracle ディレクトリ・サーバーにログインしたユーザーの識別子を指定します。これはカタログ化属性です。
orclopresult	操作の結果を指定します。操作が無事終了した場合は「SUCCESS」、失敗の場合はその理由を示します。
orclauditmessage	テキスト・メッセージを指定します。この属性はカタログ化されていません。
objectclass	値は top と orclauditoc に事前設定されています。

検索フィルタが問合せ基準を満たしている場合でも、通常の検索の結果セットには監査ログ・エントリは含まれません。たとえば、検索条件が objectclass=top の場合、監査ログ・エントリは結果として戻されません。検索のベースとして cn=auditlog を指定した場合のみ、監査ログ・エントリが検索できます。

注意 : デフォルトでは、属性 orcleventtype と orcluserdn は、Oracle Internet Directory のインストール時に索引付けされています。これらの属性から索引を削除すると、この 2 つの属性の検索はできなくなります。索引を再作成するには、カタログ管理ツールを使用します。詳細は、6-19 ページの「コマンドライン・ツールを使用した属性の索引付け」を参照してください。

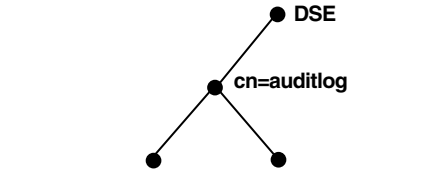
関連項目：

- カタログ化属性の詳細は、A-19 ページの「カタログ管理ツール（catalog.sh）構文」を参照してください。
- `top` の詳細は、2-8 ページの「オブジェクト・クラスの型」を参照してください。

ディレクトリ情報ツリーにおける監査ログ・エントリの位置

監査ログのコンテナは DSE の一部です。そのエントリは DSE の子として保持され、`orclsequence` 属性に従って構成されています。詳細は、図 10-1 を参照してください。

図 10-1 DSE 下のサンプル監査ログ



orclsequence: 1
orcleventtime: 199811281010z
orclauditmessage: Adding Attribute: (1.2.32.43.3.NAME 'myattr' SYNTAX '1.2.3.4.5.6.7')
orcleopresult: Invalid syntax.
orcluserdn: cn=orcladmin
objectclass: top
objectclass: orclauditoc

監査可能なイベント

表 10-5 に、監査可能なイベントとその監査レベルを示します。3 列目の「監査レベル」は 16 進の値です。複数のイベントを監査するには、この列のそれぞれのイベントに対応する値を加算します。

表 10-5 監査可能なイベント

イベント	説明	監査レベル
スーパー・ユーザー・ログイン	スーパー・ユーザーのサーバーへのバインド（成功または失敗）	0x0001
スキーマ要素の追加 / 置換	新規スキーマ要素の追加（成功または失敗）	0x0002
スキーマ要素の削除	スキーマの削除（成功または失敗）	0x0004

表 10-5 監査可能なイベント（続き）

イベント	説明	監査レベル
バインド	バインドの失敗	0x0008
アクセス違反	アクセス制御ポリシー・ポイントで否認されたアクセス	0x0010
ディレクトリ固有のエントリの変更	DSE に対する変更（成功または失敗）	0x0020
レプリケーション・ログイン	レプリケーション・サーバーの認証（成功または失敗）	0x0040
ACL の変更	アクセス制御リスト（ACL）の変更	0x0080
ユーザー・パスワードの変更	ユーザー・パスワード属性の変更	0x0100
追加	ldapadd 操作（成功または失敗）	0x0200
削除	ldapdelete 操作（成功または失敗）	0x0400
変更	ldapmodify 操作（成功または失敗）	0x0800
識別名の変更	ldapModifyDN 操作（成功または失敗）	0x1000

監査レベルの設定

DSE 属性 `orclauditlevel` の設定は、現行の監査レベルを示します。前述の項で説明したイベントを使用可能または使用禁止にできます。属性の値が `0`（ゼロ）の場合（これがデフォルトです）、監査は使用禁止です。

監査レベルの設定には、Oracle Directory Manager または ldapmodify のいずれかを使用します。この項では、両方の方法について説明します。

Oracle Directory Manager を使用した監査レベルの設定 Oracle Directory Manager を使用して監査レベルを設定する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」を展開して、ディレクトリ・サーバー・インスタンスを選択します。

2. 右側のペインで、「**監査マスク・レベル**」タブ・ページを選択します。このタブ・ページには、次の表で説明する監査可能イベントがリストされます。

表 10-6 監査マスク・レベル

監査レベル	説明
スーパー・ユーザー・ログイン	スーパー・ユーザーのサーバーへのバインド（成功または失敗）
スキーマ要素の追加 / 置換	新規スキーマ要素の追加（成功または失敗）
スキーマ要素の削除	スキーマの削除（成功または失敗）
バインド	バインドの失敗
アクセス違反	ACP で否認されたアクセス
DSE の変更	DSE エントリに対する変更（成功または失敗）
レプリケーション・ログイン	レプリケーション・サーバーの認証（成功または失敗）
ACL の変更	ACP に対する変更
ユーザー・パスワードの変更	ユーザー・パスワード属性の変更
追加	ldapadd 操作（成功または失敗）
削除	ldapdelete 操作（成功または失敗）
変更	ldapmodify 操作（成功または失敗）
識別名の変更	ldapModifyDN 操作（成功または失敗）

3. 使用する監査レベルを選択します。

4. 「**適用**」を選択します。

成功したイベントと失敗したイベントが選択されている場合は、次の場合を除き、両方が監査ログに記録されます。

- バインド : バインドに失敗した例のみをログに記録します。
- アクセス違反 : ACP によってアクセスが拒否されたイベントのみをログに記録します。

変更を有効にするために、ディレクトリ・サーバー・インスタンスを再起動します。

> **関連項目：** ディレクトリ・サーバーを再起動する方法は、A-16 ページの「Oracle Internet Directory サーバー・インスタンスの再起動」を参照してください。

ldapmodify を使用した監査レベルの設定 複数のイベントを監査するには、その監査マスクの値を加算します。たとえば、10-15 ページの表 10-7 のイベントを監査するとします。

表 10-7 例：監査レベルの設定

イベント	監査レベル	値
スキーマ要素の削除	0x0004	4
DSE の変更	0x0020	32
追加	0x0200	512
合計		548

監査レベルの合計値は 548 です。したがって、ldapmodify コマンドは、次のようになります。

```
ldapmodify -p port -h host << EOF
dn:
changetype:modify
replace: orclauditlevel
orclauditlevel: 548
EOF
```

`orclauditlevel` に変更を加えた場合は、変更内容を有効にするためにディレクトリ・サーバー・インスタンスを再起動してください。

> **関連項目：** ディレクトリ・サーバーを再起動する方法は、A-16 ページの「Oracle Internet Directory サーバー・インスタンスの再起動」を参照してください。

監査ログ・エントリの検索

Oracle Directory Manager または ldapsearch を使用して、監査ログ・エントリを検索できます。

Oracle Directory Manager を使用した監査ログ・エントリの検索

Oracle Directory Manager を使用して監査ログ・エントリを表示する手順は次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「**ディレクトリ・サーバー・インスタンス**」の順に展開し、「**監査ログの管理**」を選択します。対応する右側のペインが表示されます。
2. 「**最大結果件数**」フィールドに、検索で取り出すエントリの最大数を入力します。デフォルトは 200 です。ここで指定できるディレクトリ・サーバーのエントリ数は、最大 1000 です。
3. 「**最長検索時間**」ボックスに、検索の最大時間を秒数で入力します。ここで入力する値は、少なくともデフォルト値の 25 以上にする必要があります。ここで指定できるディレクトリ・サーバーの最大検索時間は、1 時間です。
4. 「**検索基準**」ボックスで、検索基準バーのリストとテキスト・フィールドを使用して、検索基準をさらに詳細に指定します。
   a. 検索基準バーの一番左のリストから、検索するエントリの属性を選択します。各エントリですべての属性が使用されているわけではないため、指定した属性が、検索しているエントリの属性に実際に一致していることを確認する必要があります。一致する属性がない場合は、検索に失敗します。
   b. 検索基準バーの中央のリストから、フィルタを選択します。詳細は、C-33 ページの表 C-37 を参照してください。
   c. 検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。たとえば、選択した属性が cn の場合は、検索する個々の一般名を入力します。
5. 検索をさらに詳細に指定するには、「**検索基準**」ボックスのボタンを使用して検索基準バーを拡張します。詳細は、C-34 ページの表 C-38 を参照してください。
6. 「**検索**」を選択します。検索結果は「識別名」ボックスに表示されます。
7. 特定の監査ログ・エントリのプロパティを表示するには、そのプロパティを「**識別名**」ボックスで選択し、Oracle Internet Directory サーバー管理機能の機能を使用するように選択します。「監査ログ・エントリ」ダイアログ・ボックスに、選択した監査ログのプロパティが表示されます。

関連項目： 検索で表示するエントリ数と検索の制限時間の設定方法は、4-12 ページの「Oracle Directory Manager での検索の表示と期間の構成」を参照してください。

ldapsearch を使用した監査ログ・エントリの検索 監査ログのコンテナの **DN** は、cn=auditlog です。監査ログ・エントリを検索するには、検索のベースとしてコンテナ・オブジェクト cn=auditlog を指定し、サブツリー検索または 1 レベルの検索を実行します。

関連項目： A-39 ページの「ldapsearch の構文」

監査ログの削除

bulkdelete を使用して、コンテナ cn=auditlog の下の監査ログ・オブジェクトを削除できます。次のコマンドを実行します。

```
bulkdelete.sh -connect connect_string -base "cn=auditlog"
```

Oracle Internet Directory サーバーの監視

Oracle Internet Directory サーバー管理機能により、Oracle Internet Directory サーバーに関する様々なタイプの情報を監視できます。この項では、次の項目について説明します。

- Oracle Internet Directory サーバー管理機能の機能
- Oracle Internet Directory サーバー管理機能のアーキテクチャとコンポーネント
- Oracle Internet Directory サーバー管理機能の構成情報の位置
- Oracle Internet Directory サーバー管理機能の構成
- 重要なイベントの構成
- Oracle Enterprise Manager Application Server Control を介した Oracle Internet Directory サーバー管理機能フレームワークの使用

Oracle Internet Directory サーバー管理機能の機能

Oracle Internet Directory サーバー管理機能フレームワークにより、次のディレクトリ・サーバー統計を監視できます。

- LDAP 要求キュー、メモリー、LDAP セッションおよびデータベース・セッションに関するサーバー健全性統計。たとえば、ある期間のアクティブなデータベース・セッションの数を表示できます。
- 特定のサーバー操作（追加、変更、削除などの操作）に関する一般統計。たとえば、ある期間のディレクトリ・サーバー操作の数を表示できます。

- ディレクトリおよび各操作を実行するユーザーに対する、成功および失敗したバインドおよび比較操作を含むユーザー統計
- システム・リソースとセキュリティに関する重要なイベント（ユーザーがパスワードをまちがえた場合や、操作の実行に十分なアクセス権限を持っていない場合など）
- ディレクトリ・サーバーとディレクトリ・レプリケーション・サーバーのステータス情報（ディレクトリ・レプリケーション・サーバーが呼び出された日時など）
- Oracle Directory Integration and Provisioning Server と統合プロファイルのステータス情報（Oracle Directory Integration and Provisioning Server が失敗した回数や、統合プロファイルが使用可能かどうかなど）

関連項目： 第 32 章「Oracle Directory Integration and Provisioning Platform の概要とコンポーネント」

Oracle Enterprise Manager Application Server Control を使用すると、監視対象の情報を表示できます。

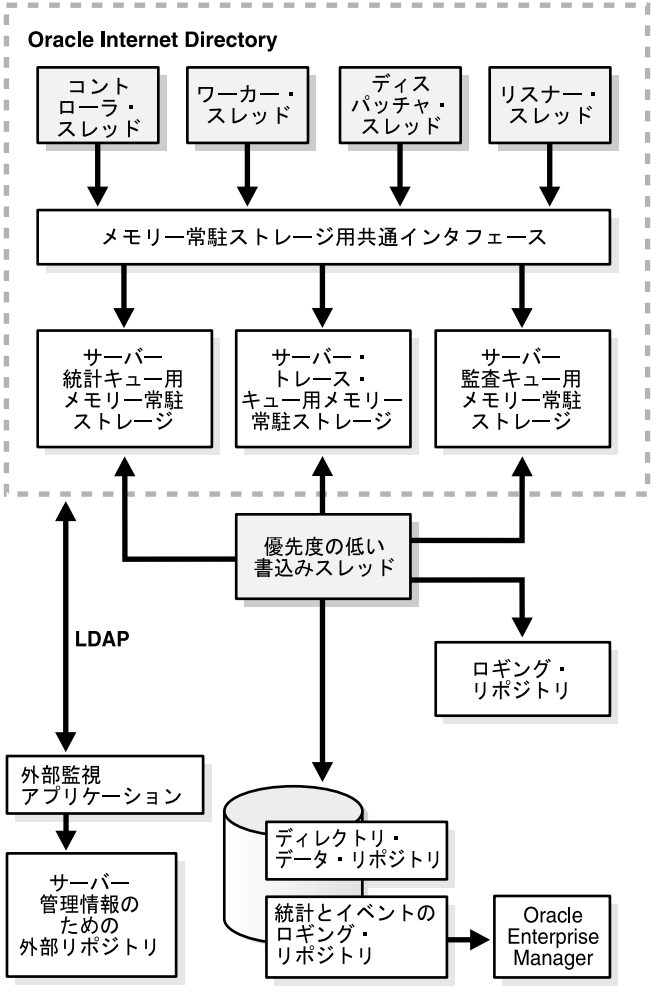
関連項目：

- Oracle Enterprise Manager Application Server Control のオンライン・ヘルプ
- 『Oracle Application Server 10*g* 管理者ガイド』の管理ツールに関する章

Oracle Internet Directory サーバー管理機能のアーキテクチャとコンポーネント

図 10-2 とその後の説明で、ディレクトリ・サーバー管理機能の各種コンポーネント間の関係について説明します。

図 10-2 Oracle Internet Directory サーバー管理機能のアーキテクチャ



Oracle Internet Directory ディレクトリ・サーバーは、クライアントからのディレクトリ要求に応答します。コントローラ、ワーカー、ディスパッチャ、リスナーの 4 種類の機能スレッドがあります。ディレクトリ・サーバーは、クライアントからの LDAP 要求を受信し、処理した後、LDAP 応答をクライアントに返信します。

Oracle Internet Directory サーバー管理機能フレームワークを使用して実行時監視機能を設定すると、サーバーの 4 種類の機能スレッドが指定された情報を記録し、それをローカル・メモリーに格納します。

> **関連項目：** ディレクトリ・サーバーの詳細は、2-17 ページの「Oracle ディレクトリ・サーバー・インスタンス」を参照してください。

メモリー常駐ストレージ これは、ローカル・プロセス・メモリーです。Oracle Internet Directory サーバー管理機能フレームワークは、統計、トレース、監査にそれぞれ 1 つのストレージを割り当てます。それぞれのストレージは、ローカル・メモリー・ストレージで管理される独自のデータ構造を持ちます。

優先度の低い書込みスレッド これらの書込み専用スレッドは、サーバー統計、監査ロギングおよびトレース情報をリポジトリに書き込むサーバー機能スレッドとは異なります。システム・オーバーヘッドを少なくするため、その優先度は低く保たれます。

外部監視アプリケーション このモジュールは独自のもので、サーバー管理機能フレームワークの外部にあります。これは、集められた統計をディレクトリ・サーバーの標準 LDAP インタフェースを通じて収集し、それを専用のリポジトリに格納します。

サーバー管理情報のための外部リポジトリ これは、収集されたディレクトリ・サーバー統計を格納するために監視エージェントが使用するリポジトリです。監視エージェントがこのリポジトリの実装方法を決定します。

Oracle Enterprise Manager Application Server Control Application Server Control は、統計とイベントのリポジトリから監視されたデータを抽出し、それを Web ベースの Graphical User Interface（GUI）で表示します。ユーザーは通常のブラウザでデータを表示できます。リポジトリは、収集されたデータを一般問合せとカスタム問合せのために格納できます。

ロギング・リポジトリ（ファイル・システム）このリポジトリは、ファイル・システムを使用して、ディレクトリ・サーバーの各種モジュールでトレースされた情報を格納します。この目的のためにファイル・システムを使用することにより、Oracle Internet Directory サーバー管理機能フレームワークはオペレーティング・システムの機能とセキュリティを使用できます。

ディレクトリ・データ・リポジトリ このリポジトリには、ユーザーが入力したすべてのデータ（ユーザー・エントリやグループ・エントリなど）が格納されます。

統計とイベントのリポジトリ このリポジトリは、ファイル・システムにではなく、ディレクトリ・データ・リポジトリと同じデータベースに情報を格納する点を除き、トレース・リポジトリと同じです。この方法で、Oracle Internet Directory サーバー管理機能フレームワークは次の機能を使用できます。

- 通常の LDAP 操作による情報の格納と取得
- 既存のアクセス制御ポリシーによる収集済情報のセキュリティの管理

ディレクトリ管理機能フレームワークは、この 2 つを別々に格納することにより、収集された情報をディレクトリ・データから分離します。

Oracle Internet Directory サーバー管理機能の構成情報の位置

Oracle Internet Directory サーバー管理機能フレームワークは、サーバー統計、サーバー・トレース、サーバー監査のための 3 つのモジュールすべてに関する構成パラメータを、ディレクトリの DSE ルートに格納します。収集する情報の周期、量、レベルを指定するには、これらのパラメータに対して適切な値を設定する必要があります。

Oracle Internet Directory サーバー管理機能の構成

Oracle Internet Directory サーバー管理機能フレームワークを構成するには、ldapmodify を使用して、ルート DSE の各種属性に対して正の整数値を設定します。

- 健全性統計と一般統計を使用可能にするには、`orclStatsFlag` 属性と `orclStatsPeriodicity` 属性を設定します。
- ユーザー統計を使用するには、次の設定を行います。
  - `orclstatslevel` 属性を `1` に設定します。
  - `orclStatsPeriodicity` 属性を設定します。
- 重要なイベントを使用可能にするには、`OrclEventLevel` 属性を設定します。
- スーパー・ユーザー、プロキシ・ユーザーおよびレプリケーション管理者以外のログインのイベントを使用可能にするには、次のように設定します。
  - `OrclEventLevel` 属性を適切な値に設定します。
  - `orclStatsFlag` を `1` に設定します。

関連項目： Oracle Internet Directory サーバー管理機能を使用する場合に設定する各属性の詳細は、B-24 ページの「Oracle Internet Directory サーバー管理機能の属性」を参照してください。

たとえば、Oracle Internet Directory サーバー管理機能フレームワークを使用可能にするには、次のような LDIF ファイルを作成します。

```
dn:
changetype: modify
replace: orclstatsflag
orclstatsflag:1
```

このファイルをアップロードするには、次のコマンドを入力します。

```
ldapmodify -h host -p port_number -D bind_DN -w bind_DN_password -f file_name
```

ここで、サーバー管理機能構成を実行する権限を持つバインド識別名は、`cn=emd admin,cn=oracle internet directory` です。

> **関連項目：** Oracle Internet Directory サーバー管理機能を使用した Oracle Internet Directory サーバーの監視と管理の詳細は、Oracle Enterprise Manager Application Server Control のオンライン・ヘルプを参照してください。

重要なイベントの構成

重要なイベントを構成するには、ldapmodify を使用し、`OrclEventLevel` 属性に表 10-8 に示すイベント・レベルを 1 つ以上設定します。

表 10-8 重要なイベントのレベル

レベル値	重要なイベント	提供される情報
1	スーパー・ユーザー・ログイン	スーパー・ユーザーのバインド（成功または失敗）
2	プロキシ・ユーザー・ログイン	プロキシ・ユーザーのバインド（失敗）
4	レプリケーション・ログイン	レプリケーションのバインド（失敗）
8	追加アクセス	追加アクセス違反
16	削除アクセス	削除アクセス違反
32	書込みアクセス	書込みアクセス違反
64	ORA 3113 エラー	ORA 3113 エラー
128	ORA 3114 エラー	ORA 3114 エラー
255	すべての重要なイベント	

Oracle Enterprise Manager Application Server Control を介した Oracle Internet Directory サーバー管理機能フレームワークの使用

Oracle Internet Directory サーバー管理機能の機能を使用するには、Oracle Enterprise Manager Application Server Control を使用します。この項では、その手順を示します。

Oracle Enterprise Manager Application Server Control を使用した情報収集の有効化

Oracle Enterprise Manager Application Server Control を使用して情報収集を可能にする手順は、次のとおりです。

1. Oracle Internet Directory メイン・ウィンドウで、「**LDAP メトリック**」を選択します。「LDAP 診断収集構成」ページが表示されます。
2. 「**メトリックの収集**」をチェックします。
3. 「**間隔**」を選択します。
4. 必要なパスワードを入力します。
5. 「**適用**」を選択します。

> **注意：** 重要なイベントを使用可能にするには、ldapmodify を使用して `orclEventLevel` 属性を適切な値に設定します。

Oracle Enterprise Manager Application Server Control を使用した新規ディレクトリ・サーバー・インスタンスの起動

サーバーを起動する手順は、次のとおりです。

1. 「Oracle Internet Directory」メイン・ウィンドウで、「**新規インスタンスの開始**」を選択します。「新規 LDAP サーバー・インスタンスの開始」ウィンドウに、構成設定を選択できる表が表示されます。

表 10-9「新規 LDAP サーバー・インスタンスの開始」ウィンドウのフィールド

列	説明
セット番号	ディレクトリ・サーバー・インスタンスの構成設定番号
デフォルト・ポート	ディレクトリ・サーバー・インスタンスのデフォルト・ポート番号
使用可能なポート	デフォルト・ポートが使用可能かどうかのインジケータ
最大データベース接続数	このディレクトリ・インスタンスで使用可能なデータベース接続の数

表 10-9「新規 LDAP サーバー・インスタンスの開始」ウィンドウのフィールド（続き）

列	説明
サーバー・プロセス	サーバー・プロセスの数
ポート番号	デフォルト・ポート番号を使用しない場合にディレクトリ・サーバー・インスタンスに割り当てるポート番号

2. 「**セット番号**」列で、使用する構成設定を選択します。

   デフォルト・ポートを使用できない場合は、「**ポート番号**」列にポート番号を指定します。

3. 「**起動**」を選択します。

Oracle Enterprise Manager Application Server Control を使用したディレクトリ・サーバー・インスタンスの停止

ディレクトリ・サーバー・インスタンスを停止する手順は、次のとおりです。

1. 「Oracle Internet Directory」メイン・ウィンドウの「**ディレクトリ・サーバー・インスタンス**」セクションで、停止するディレクトリ・サーバー・インスタンスを選択します。
2. 「**停止**」を選択します。

Oracle Enterprise Manager Application Server Control を使用したディレクトリ・サーバー・インスタンスの再起動

ディレクトリ・サーバー・インスタンスを再起動する手順は、次のとおりです。

1. 「Oracle Internet Directory」メイン・ウィンドウの「**ディレクトリ・サーバー・インスタンス**」セクションで、再起動するサーバーを選択します。
2. 「**再起動**」を選択します。「LDAP サーバー・インスタンスの再起動」ウィンドウに次の表が表示されます。

表 10-10「LDAP サーバー・インスタンスの再起動」ウィンドウのフィールド

列	説明
セット番号	ディレクトリ・サーバー・インスタンスの構成設定番号
デフォルト・ポート	ディレクトリ・サーバー・インスタンスのデフォルト・ポート番号
使用可能なポート	デフォルト・ポートが使用可能かどうかのインジケータ
最大データベース接続数	このディレクトリ・インスタンスで使用可能なデータベース接続の数

表 10-10「LDAP サーバー・インスタンスの再起動」ウィンドウのフィールド（続き）

列	説明
サーバー・プロセス	サーバー・プロセスの数
ポート番号	デフォルト・ポート番号を使用しない場合にディレクトリ・サーバー・インスタンスに割り当てるポート番号

3. 構成を選択します。デフォルト・ポートを使用できない場合は、「**ポート番号**」列にポート番号を入力します。
4. 「**起動**」を選択します。

Oracle Enterprise Manager Application Server Control を使用したディレクトリ・サーバー・アクティビティの表示

ディレクトリ・サーバー・アクティビティ情報を表示する手順は、次のとおりです。

1. 「ディレクトリ・サーバー」メイン・ウィンドウで、情報を表示するディレクトリ・サーバー・インスタンスを選択します。
2. 「**ロードの表示**」を選択します。「LDAP ロード」ウィンドウが表示されます。
3. 「**ロード特性の選択**」のリストから、このインスタンスについて表示する情報を選択します。オプションは次のとおりです。
   - **LDAP リポジトリ・データベース・セッション**: このオプションは、2 つのグラフを表示します。最初のグラフは、オープン中のデータベース・セッションに関する情報を示します。もう 1 つのグラフは、アクティブなデータベース・セッションに関する情報を示します。これは、統計収集の指定された期間終了時の情報です。
   - **レスポンス時間と LDAP 操作**: このオプションを選択すると、2 つのグラフが表示されます。最初のグラフは、指定された期間の統計情報の LDAP 操作応答時間の平均を示します。もう 1 つのグラフは、その期間終了時に進行中であった操作の数を示します。
   - **アクティブ LDAP セッションと新規 LDAP セッション**: このオプションを選択すると、2 つのグラフが表示されます。最初のグラフは、アクティブな LDAP セッション（統計収集の指定された期間終了時にオープンしていたセッション）の数を表示します。2 番目のグラフは、新規 LDAP セッション（統計収集の指定された期間中にオープンされたセッション）の数を表示します。
4. 選択した後、「**実行**」をクリックします。

Oracle Enterprise Manager Application Server Control を使用したディレクトリ・サーバー操作の表示

Application Server Control を使用して、統計収集の指定された期間中のディレクトリ・サーバー操作を表示できます。この手順は、次のとおりです。

1. 「ディレクトリ・サーバー」メイン・ウィンドウで、情報を表示するディレクトリ・サーバー・インスタンスを選択します。
2. 「**操作の表示**」を選択します。すべての LDAP 操作に関するチャートが表示されます。チャートをクリックすると、チャートが拡大表示されます。

11

ディレクトリのバックアップとリストア

この章では、小さいディレクトリおよび大きいディレクトリのバックアップ方法とリストア方法について説明します。次の項目について説明します。

- 小さいディレクトリまたはディレクトリ内の特定のネーミング・コンテキストのバックアップとリストア
- 大きいディレクトリのバックアップとリストア

小さいディレクトリまたはディレクトリ内の特定のネーミング・コンテキストのバックアップとリストア

小さいディレクトリまたはディレクトリ内の特定のネーミング・コンテキストのバックアップとリストアを行う手順は、次のとおりです。

1. ldifwrite ユーティリティを使用してノードをバックアップします。次のコマンドを入力します。

   ```
   ldifwrite -connect connect_string  -b naming_context -f backup.ldif
   ```

2. 次のコマンドを入力して、新規ノードでディレクトリ・サーバーを起動します。

   ```
   oidctl connect= connect_string  server=oidldapd instance=1
   flags= '-p port_number' start
   ```

3. ldapaddmt ユーティリティを使用して、新規ノードにデータをロードします。次のコマンドを入力します。

   ```
   ldapaddmt -h host_name -p port_number -v -f backup.ldif
   ```

大きいディレクトリのバックアップとリストア

大きいディレクトリのバックアップとリストアについては、『Oracle Application Server 10*g* 管理者ガイド』を参照してください。

第 III 部

ディレクトリのセキュリティ

第 III 部では、ディレクトリ内のデータを保護する機能について説明します。また、企業およびホスティングされた環境にあるアプリケーションを管理するアクセス制御を確立する方法についても説明します。第 III 部は次の各章で構成されています。

- 第 12 章「ディレクトリ・セキュリティの概要」
- 第 13 章「Secure Sockets Layer（SSL）とディレクトリ」
- 第 14 章「ディレクトリ・アクセス制御」
- 第 15 章「Oracle Internet Directory のパスワード・ポリシー」
- 第 16 章「パスワード・ベリファイアのディレクトリ格納」
- 第 17 章「Oracle テクノロジ配置のための権限の委任」

12

ディレクトリ・セキュリティの概要

Oracle Internet Directory は、Oracle Identity Management インフラストラクチャの重要な要素です。これを使用すると、複数の Oracle コンポーネントを Oracle Internet Directory の共有インスタンスや関連付けられたインフラストラクチャの各部分に対して機能するように配置できます。この共有により、企業はすべてのアプリケーションでセキュリティ管理を単純化できます。

Oracle Identity Management インフラストラクチャで果たす役割に加えて、Oracle Internet Directory は情報を保護するための多数の強力な機能を提供します。

この章では、Oracle Internet Directory セキュリティ機能の概要を示します。次の項目について説明します。

データの整合性と Oracle Internet Directory

Oracle Internet Directory は、Secure Sockets Layer（SSL）を使用して、送信時にデータの変更、削除または再現が行われないことを保証します。SSL は、暗号方式の保護メッセージ・ダイジェストを、**MD5** アルゴリズムまたは **Secure Hash Algorithm（SHA）**を使用する暗号チェックサムを使用して生成し、ネットワークを介して送信する各パケットに組み込みます。

> **関連項目：** SSL の詳細は、第 13 章「Secure Sockets Layer（SSL）とディレクトリ」を参照してください。

データのプライバシと Oracle Internet Directory

Oracle Internet Directory は、SSL とともに使用可能な**公開鍵暗号**を使用して、送信時にデータが開示されないことを保証します。公開鍵暗号では、メッセージの送信側が受信側の公開鍵を使用して、メッセージを暗号化します。メッセージが送達されると、受信側は、受信側の秘密鍵を使用して、メッセージを復号化します。Oracle Internet Directory では特に、SSL によって使用可能な次の 2 つのレベルの暗号化をサポートします。

- DES40

  DES40 アルゴリズムは **DES** の改良型で、国際的に使用可能な暗号化方式です。このアルゴリズムでは、秘密鍵を事前に処理して、40 ビットの有効**鍵**を提供します。DES40 は、米国およびカナダ以外で、DES ベースの暗号化アルゴリズムの使用を希望する顧客を対象に設計されています。この機能によって、顧客は地理的条件に関係なく使用するアルゴリズムを選択できます。

- RC4_40

  Oracle は、他の Oracle 製品が使用できる事実上すべての地域に対して、鍵のサイズが 40 ビットの RC4 データ暗号化アルゴリズムを輸出するライセンスを取得しています。この結果、国際企業は、高速暗号化を使用して事業全体を保護することが可能になります。

> **関連項目：** SSL の詳細は、第 13 章「Secure Sockets Layer（SSL）とディレクトリ」を参照してください。

Oracle Internet Directory での認可

認可とは、オブジェクトまたはオブジェクトのセットへのアクセスのためにユーザー、プログラムまたはプロセスに与えられる権限です。ディレクトリ・セッション中にディレクトリ操作が試行されると、ディレクトリ・サーバーによって、ユーザーにこれらの操作を実行するための権限があるかどうかが確認されます。ユーザーに権限がない場合、ディレクトリ・サーバーはこれらの操作を許可しません。ディレクトリ・サーバーはアクセス制御情報を使用して、ディレクトリ・ユーザーによる不正操作からディレクトリ・データを保護します。

アクセス制御情報アイテム（ACI）は、アクセス制御に関連する管理ポリシーを記録したディレクトリ・メタデータです。この情報は、ユーザーによる変更が可能な操作属性として、Oracle Internet Directory に格納されています。各属性は、**アクセス制御情報項目**（ACI）と呼ばれます。

通常、**アクセス制御リスト**（ACL）と呼ばれるこの ACI 属性値のリストは、ディレクトリ・オブジェクトと関連付けられています。このリストの属性値は、様々なディレクトリ・ユーザー・エンティティ（対象）が各オブジェクトに対して所有している権限を表しています。

ACI は次のコンポーネントで構成されています。

- アクセス権限を付与するオブジェクト
- アクセス権限を付与するエンティティ（対象）
- 付与するアクセス権限の種類

アクセス制御ポリシーは規定的です。つまり、そのセキュリティ・ディレクティブは、**ディレクトリ情報ツリー**（DIT）内のすべての下位エントリに適用されるように設定できます。アクセス制御ポリシーが施行される開始点は、**アクセス制御ポリシー・ポイント**（**ACP**）と呼ばれます。

ACI は、ディレクトリ内にテキスト文字列として記述され、格納されています。この文字列は、ACI ディレクティブ書式と呼ばれる、明確に定義された書式に従う必要があります。ACI 属性の各有効値は、個別のアクセス制御ポリシーを表します。

ホスティングされた環境で実行されているアプリケーションでは、ディレクトリ・アクセス制御の次の機能が使用できます。

- 規定のアクセス制御

  サービス・プロバイダは、ディレクトリ・オブジェクトの集合に対してアクセス制御リスト（ACL）を指定できます。個々のオブジェクトごとにポリシーを設定する必要はありません。この機能によって、アクセス制御の管理が簡素化されます。特に同じポリシーまたは同等のポリシーで管理されるオブジェクトが多数含まれる大きなディレクトリで有効です。

- 階層的なアクセス制御管理のモデル

  サービス・プロバイダは、ホスティングされた企業にディレクトリ管理を委任できます。必要に応じて、レルムからさらに委任することもできます。

- 委任ドメインに対する管理制御のオーバーライド

  サービス・プロバイダは、アカウントの意図しないロックアウトやセキュリティの不慮の露見に対する診断とリカバリを実行できます。

- アクセス制御エンティティの動的評価

  サブツリーの管理者は、対象とオブジェクトの双方を、その名前空間およびディレクトリのその他のオブジェクトとの関連の点で識別できます。たとえば、あるレルムの管理者は、ユーザーの上司のみに、そのユーザーの給与属性の更新を認めることができます。他のレルムの管理者は、給与属性に関して、これと異なるポリシーを確立して施行できます。

Oracle Internet Directory での認証

認証は、ディレクトリ・サーバーが、そのディレクトリに接続しているユーザーの正確な識別情報を設定するプロセスです。認証は、LDAP セッションが ldapbind 操作によって確立されたときに発生します。このようにして、すべてのセッションにユーザー ID が関連付けられます。

ユーザー、ホストおよびクライアントの識別情報を検証するために、Oracle Internet Directory では、3 種類の一般的な認証を使用できます。それらについて、次の項目で説明します。

- 直接認証
- 間接認証
- 外部認証

直接認証

この項では、Oracle Internet Directory 内で使用可能な 3 種類の認証と、SASL 対応クライアントがディレクトリ・サーバーに対して認証を行う方法について説明します。

直接認証オプション

3 種類の直接認証オプションがあります。

- 匿名認証

  匿名で認証する場合、ユーザーは、ユーザー名とパスワードのフィールドを空白のままにしてログインします。各匿名ユーザーは、匿名ユーザーに付与されている権限すべてを使用できます。

- 簡易認証

  簡易認証を使用する場合、クライアントは、ネットワーク上を暗号化されずに送信される識別名とパスワードによって、サーバーに対して自己認証を行います。

- Simple Authentication and Security Layer（SASL）を使用した認証

  これは、接続ベースのプロトコルに認証サポートを追加する方法です。SASL を使用するために、プロトコルには、ユーザーを識別してサーバーに対して認証を行うコマンドが含まれます。また、オプションで、以降のプロトコル対話の保護を規定するコマンドも含まれます。SASL の使用が正常に規定されると、プロトコルと接続の間にセキュリティ・レイヤーが挿入されます。

  Oracle Internet Directory は、SASL を使用する 2 種類の認証メカニズムをサポートします。

  – MD5 ダイジェスト : LDAP バージョン 3 内では必須の認証メカニズムです（RFC 2829）。MD5 ハッシュ関数を使用して、任意の長さのメッセージを、クライアント / サーバー認証のベリファイアとして使用できる 128 ビットのメッセージ・ダイジェストに変換します。

  – 外部認証 : たとえば、SSL があります。この場合、クライアントは、ユーザー名とパスワードを使用するかわりに、外部認証メカニズムにより要求される証明書、トークンまたは他のデバイスによって、サーバーに対して認証します。

    関連項目：

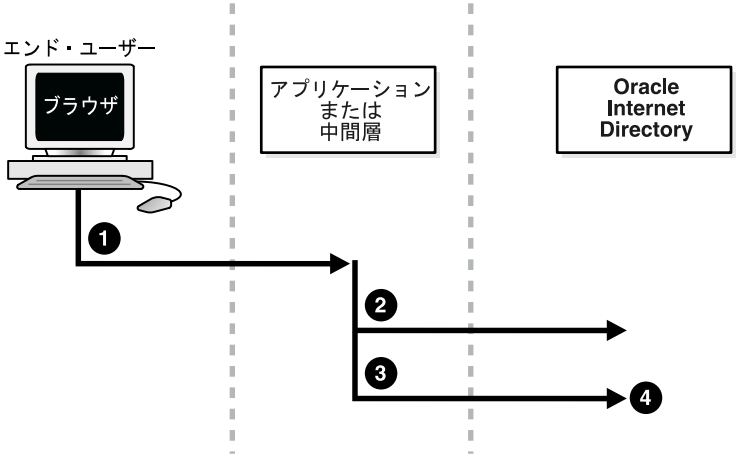
    - 12-8 ページの「Simple Authentication and Security Layer（SASL）を使用した認証」
    - http://www.ietf.org にある Internet Engineering Task Force（IETF）の Web サイトで、RFC 2829（LDAP バージョン 3 サーバーで必要な認証メカニズムとしての SASL Digest-MD5 を指定）、RFC 2831（Digest-MD5 メカニズムの説明）、RFC 2617（SASL Digest-MD5 がベースとしている HTTP Digest 認証メカニズムの説明）の各 RFC を参照してください。

間接認証

間接認証は、ディレクトリに資格証明を保持するエンティティ（Oracle Internet Directory セルフ・サービス・コンソールのようなアプリケーション、ファイアウォールや RADIUS サーバーのような中間層など）を介して発生します。アプリケーションや中間層は、**プロキシ・ユーザー**となります。プロキシ・ユーザーは、エンド・ユーザーの代理となる権限を持ち、そのユーザーが権限を持つ操作をユーザーにかわって実行します。

次の図 12-1 および図に続く説明は、間接認証がどのように実行されるかを示しています。

図 12-1 間接認証



間接認証は、次の手順で行われます。

1. エンド・ユーザーが、Oracle Internet Directory への問合せが含まれている要求をアプリケーションまたは中間層に送信します。アプリケーションまたは中間層がエンド・ユーザーを認証します。
2. アプリケーションまたは中間層がディレクトリにバインドします。
3. アプリケーションまたは中間層は、エンド・ユーザーの識別名を使用して、2 回目のバインドを実行します。この場合、エンド・ユーザーのパスワードは入力しません。
4. ディレクトリ・サーバーは、アプリケーションまたは中間層がエンド・ユーザーの ID に切り替えようとしているものとして、この 2 回目のバインドを認識します。ディレクトリ・サーバーは、アプリケーションまたは中間層によってエンド・ユーザーに付与された認証を受け入れます。ただし、アプリケーションまたは中間層に、このユーザーのプロキシとなる権限があるかどうかを検証する必要があります。ディレクトリ・サーバーは、エンド・ユーザーのエントリを管理する ACP によって、このエンド・ユーザーに対するプロキシ権限がこのアプリケーションまたは中間層に付与されているかどうかをチェックします。
    * エンド・ユーザーのエントリにより、アプリケーションまたは中間層に必要なプロキシ権限が提供された場合、ディレクトリ・サーバーは、認可識別情報をエンド・ユーザーの認可識別情報に変更します。後続するすべての操作は、そのエンド・ユーザーがサーバーに直接接続して直接認証された場合と同様に行われます。

* エンド・ユーザーのエントリが、アプリケーションまたは中間層に必要なプロキシ権限を提供しない場合、ディレクトリ・サーバーは、「アクセス権限が不十分です。」というエラー・メッセージを戻します。

関連項目： 14-11 ページの「操作 : 付与するアクセス権の種類」

ディレクトリ・サーバーは同一セッションで、その他のエンド・ユーザーを認証および許可できます。また、セッションをエンド・ユーザーから、そのセッションをオープンしたアプリケーションまたは中間層に切り替えることもできます。

セッションをクローズするには、アプリケーションまたは中間層がバインド解除要求をディレクトリ・サーバーに送信します。

たとえば、次の場合を想定します。

- `cn=User1` でディレクトリにバインドする中間層には、ディレクトリ全体に対するプロキシ・アクセス権限があります。
- `cn=User2` でディレクトリにバインドできるエンド・ユーザーがいます。

このエンド・ユーザーが、ディレクトリに対する問合せが含まれている要求をアプリケーションまたは中間層に送信すると、アプリケーションまたは中間層がエンド・ユーザーを認証します。その後、中間層サービスは、そのサービスの ID である `cn=User1` を使用してディレクトリにバインドし、次に、エンド・ユーザーの識別名 `cn=User2` のみを使用して 2 回目のバインドを実行します。この 2 回目のバインドは、Oracle ディレクトリ・サーバーでは、プロキシ・ユーザーがエンド・ユーザーの代理になろうとしているものと認識されます。ディレクトリ・サーバーは、`cn=user1` にプロキシ・アクセス権限があることを確認した後、この 2 回目のバインドの実行を許可します。パスワードなど、エンド・ユーザー識別名の妥当性をさらに要求することはありません。このセッションでは、これ以降すべての LDAP 操作は、`cn=User2` が実行しているかのようにアクセス制御されます。

あるユーザーがアプリケーションからサービスを受け、続いて別のユーザーが同じアプリケーションのサービスを要求した場合、アプリケーションは、先行ユーザーのセッションを中断せずに、新規接続を確立して前述のとおりに処理を進めることができます。ただし、まだサービスを受けている先行ユーザーがいない場合は、新しい接続を確立することなく、既存の確立済接続を何度も使用できます。

外部認証

多くの企業では、ユーザー・セキュリティ資格証明を Oracle Internet Directory 以外のリポジトリ（データベースや他の LDAP ディレクトリなど）に格納しています。Oracle Internet Directory の外部認証プラグインとパスワード変更プラグインにより、ユーザー認証用のこれらの資格証明を Oracle コンポーネントに対して使用できます。資格証明を Oracle Internet Directory に格納する必要はなく、常に同期化させる必要はありません。

ディレクトリ認証用ユーザー・パスワードの保護

Oracle Internet Directory では、ユーザーのディレクトリ・パスワードを一方向ハッシュ値として userPassword 属性に格納することで、そのパスワードを保護します。管理者は、使用するハッシング・アルゴリズムを選択します。パスワードを暗号値ではなく一方向ハッシュ値として格納することによって、パスワードのセキュリティが向上します。これは、悪意のあるユーザーにはこれらの値を読むことも復号化することもできないためです。

関連項目： 「Oracle Internet Directory に対する認証用パスワード・ベリファイアの格納および管理」

Oracle Internet Directory のパスワード・ポリシー

パスワード・ポリシーとは、パスワードの使用方法を定めた一連の規則のことです。ユーザーがディレクトリへのバインドを試みると、ディレクトリ・サーバーは、ユーザーのパスワードがパスワード・ポリシーの様々な要件に適合するかを確認します。

パスワード・ポリシーを確立する際は、次のような規則を設定します。なお、この規則はほんの一部です。

- 指定されたパスワードの有効期限
- パスワードの最小必須文字数
- パスワードに必要な数字の文字数

関連項目： パスワード・ポリシーの確立で設定する規則の詳細は、第 15 章「Oracle Internet Directory のパスワード・ポリシー」を参照してください。

Simple Authentication and Security Layer（SASL）を使用した認証

12-4 ページの「直接認証」の項では、Oracle Internet Directory 環境での SASL の使用について説明しました。この項では、SASL の動作について詳細に説明します。この項では、次の項目について説明します。

- SASL 対応クライアントが Digest-MD5 を使用してディレクトリ・サーバーに対して認証する方法
- SASL 対応クライアントが外部認証を使用してディレクトリ・サーバーに対して認証する方法

SASL 対応クライアントが Digest-MD5 を使用してディレクトリ・サーバーに対して認証する方法

SASL 対応クライアントがサーバーに対して Digest-MD5 認証を求める場合、その認証プロセスは次のとおりです。

1. ディレクトリ・サーバーは、サポートする各種認証オプションと特別なトークンを含むデータを LDAP クライアントに送信します。
2. クライアントは、認証オプションを選択し、選択したオプションを示す応答をサーバーに送信します。応答は暗号化されるため、クライアントがそのパスワードを知ることはありません。
3. ディレクトリ・サーバーは、クライアント応答を復号化し、検証します。

SASL 対応クライアントが外部認証を使用してディレクトリ・サーバーに対して認証する方法

Oracle Internet Directory では、クライアントおよびサーバーの両方が相互に証明書を提供して認証する SSL 接続を介して SASL 外部認証を提供します。識別名は、SSL ネットワーク規定で使用されたクライアント証明書から作成されます。

クライアントが、SSL のような外部認証メカニズムを使用してディレクトリ・サーバーに認証を求める場合、その認証プロセスは次のとおりです。

1. クライアントは、認可識別情報の入った初期メッセージを送信します。
2. ディレクトリ・サーバーは、SASL の外部にある情報を使用して、クライアントが認可識別情報として正当に認証できるかどうかを判断します。クライアントが正当に認証できる場合、ディレクトリ・サーバーは認証通信が成功して完了したことを示します。そうでない場合、ディレクトリ・サーバーは失敗を示します。

IPsec や SSL/TLS などのシステムにより外部情報が提供されます。クライアントが認可識別情報として空の文字列を送信した場合、認可識別情報は外部認証を提供するシステムのクライアント認証資格証明（SSL 証明書など）から作成されます。

13

Secure Sockets Layer（SSL）とディレクトリ

この章では、Oracle Internet Directory で使用するために Secure Sockets Layer（SSL）を構成する方法について説明します。SSL を使用すると、厳密認証、データ整合性およびデータ・プライバシも構成できます。

この章では、次の項目について説明します。

- サポートされている Cipher Suite
- SSL クライアントの使用例
- SSL パラメータの構成
- Oracle Internet Directory 10g（9.0.4）での SSL の使用制限事項

関連項目： Oracle Internet Directory に関連した SSL の概要は、2-11 ページの「セキュリティ」を参照してください。

サポートされている Cipher Suite

Cipher Suite は、ネットワーク・ノード間でのメッセージ交換に使用される認証、暗号化およびデータ整合性アルゴリズムのセットです。SSL ハンドシェイク時に、2 つのノード間で折衝し、メッセージを送受信するときに使用する Cipher Suite を確認します。

Oracle Internet Directory では、次の SSL Cipher Suite がサポートされています。

表 13-1 Oracle Internet Directory でサポートされている SSL Cipher Suite

Cipher Suite	認証	暗号化	データ整合性
SSL_RSA_WITH_3DES_EDE_CBC_SHA	RSA	DES40	SHA
SSL_RSA_WITH_RC4_128_SHA	RSA	RC4_40	SHA
SSL_RSA_WITH_RC4_128_MD5	RSA	なし	MD5
SSL_RSA_WITH_DES_CBC_SHA	RSA	なし	SHA
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA	-	3DES_EDE_CBC	SHA
SSL_DH_anon_WITH_RC4_128_MD5	-	RC4_40	MD5
SSL_DH_anon_WITH_DES_CBC_SHA	-	DES_CBC	SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5	-	RC4_40	MD5
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	-	DES40	SHA
SSL_DH_anon_EXPORT_WITH_RC4_40_MD5	-	RC4_40	MD5
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA	-	DES40	SHA

SSL クライアントの使用例

Oracle Internet Directory のクライアントは、SSL 2.0 または SSL 3.0 を使用できます。SSL を使用するクライアントは、匿名または簡易認証あるいは厳密認証を使用してサーバーに接続できます。

クライアントとサーバーの双方が相互に自己認証を行うと、SSL は X.509 v3 デジタル証明書から必要な識別情報を取得します。

SSL パラメータの構成

ディレクトリ・サーバー・インスタンスの起動時に、SSL プロファイルのパラメータを含む 1 セットの構成パラメータがディレクトリに読み込まれます。SSL が使用可能な状態でこのディレクトリを実行する場合は、**構成設定エントリ**の SSL パラメータを確認する必要があります（多くの場合、再構成が必要です）。

サーバー・インスタンスを保護モードで実行するには、構成設定の「SSL 使用可能」パラメータを 1（デフォルトの保護ポートは 636）に設定します。同一のインスタンスを同時に非保護接続で実行できるようにするには、「SSL 使用可能」を 2（デフォルトの非保護ポートは 389）に設定します。

管理者は、異なる値を持つ複数の構成パラメータのセットを作成および変更し、Oracle Internet Directory のインスタンスごとに異なる構成設定エントリを使用できます。これは、セキュリティ要件の異なるクライアントを制御する便利な方法です。

SSL の値を変更するときは、デフォルトの構成設定にある SSL の値を変更するのではなく、別の構成設定を作成して、その SSL の値を変更する方法をお薦めします。デフォルトの構成設定は、技術的な問題を診断するときにオラクル社カスタマ・サポート・センターで必要となる場合があります。

関連項目：

- これらのパラメータの設定方法は、5-2 ページの「サーバーの構成設定エントリの管理」を参照してください。
- これらのパラメータの説明は、B-5 ページの「構成設定エントリのスキーマ要素」を参照してください。

Oracle Directory Manager を使用した SSL パラメータの構成

作成した各構成設定エントリおよび現在実行中の各サーバー・インスタンスの SSL 構成パラメータの値を、確認および変更できます。

注意： アクティブ・インスタンスのパラメータを直接変更することはできません。アクティブ・インスタンスのパラメータを変更する場合は、構成設定エントリ内のパラメータを変更して、それを保存してください。保存後は、現行のインスタンスを停止して、サーバーの起動メッセージ内にある新しく変更された構成設定を参照できます。

新規 SSL 構成設定の追加

注意： Oracle Directory Manager を使用して新規 SSL 構成設定を追加する前に、Oracle Wallet Manager を使用して次のことを行う必要があります。

- 新規 Wallet を作成します。
- 証明書要求を作成し、認証局に送付します。
- 認証局が Oracle Wallet Manager の信頼できる証明書のデフォルト・リストに含まれていない場合は、認証局の信頼できる証明書を Wallet にインポートしてください。
- 自動ログインを使用可能にして Wallet を保存します。

関連項目：『Oracle Advanced Security 管理者ガイド』の Oracle Wallet Manager の章を参照してください。

新規 SSL 構成設定を追加する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「**ディレクトリ・サーバー・インスタンス**」、「**サーバー管理**」の順に展開します。
2. 「**ディレクトリ・サーバー**」または「**レプリケーション・サーバー**」の適切な項目を展開します。選択した項目の下に、番号付きの構成設定が表示されます。
3. デフォルトの構成設定を選択します。
4. 「**類似項目の作成**」を選択します。「構成設定」ダイアログ・ボックスに「**一般**」タブ・ページが表示されます。
5. 「**一般**」タブ・ページで、非 SSL ポートの値をデフォルト（389 または 4032）以外に変更します。
6. 「**SSL 設定**」タブを選択し、適切なフィールドに値を入力します。フィールドについては、C-26 ページの表 C-33 を参照してください。

SSL 構成パラメータの表示と変更

SSL 構成パラメータを表示および変更する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**、「**サーバー管理**」の順に展開します。
2. 「**ディレクトリ・サーバー**」または「**レプリケーション・サーバー**」の適切な項目を展開します。選択した項目の下に、番号付きの構成設定が表示されます。
3. 検証する構成設定を選択します。その構成設定エントリに対応するタブ・ページが右側のペインに表示されます。
4. 「**SSL 設定**」タブ・ページを選択し、フィールドを変更し、保存します。フィールドについては、C-35 ページの表 C-39 を参照してください。

関連項目： 構成設定エントリのパラメータの変更方法は、5-4 ページの「Oracle Directory Manager を使用したサーバーの構成設定エントリの管理」を参照してください。

コマンドライン・ツールを使用した SSL パラメータの構成

関連項目：

- 5-7 ページの「コマンドライン・ツールを使用したサーバー構成設定エントリの管理」
- SSL を構成するための `-p` フラグ、`-U` フラグ、`-W` フラグの使用方法の詳細は、A-18 ページの「エントリおよび属性の管理コマンドライン・ツール構文」を参照してください。

SSL が使用可能な状態でのディレクトリ・サーバー・インスタンスの起動

注意： Oracle Internet Directory リリース 9.0.2 以上では、暗号化された（cwallet.sso）形式の Wallet のみがサポートされます。これは、SSL インスタンスを起動するには、その前に自動ログインを使用可能にした Oracle Wallet Manager を使用して Wallet をオープンする必要があることを意味します。リリース 9.0.2 より前のリリースの Oracle Internet Directory では、Wallet をオープンするためのパスワードを提供できます。

Windows オペレーティング・システムでは、SSL を使用可能にしてディレクトリ・サーバー・インスタンスを開始する前に、Oracle Directory Service のログオン・アカウントをローカル・システム・アカウントから Wallet を所有するユーザーに変更しておく必要があります。このユーザーは、管理者グループのメンバーである必要があります。

サービスを変更する手順は、次のとおりです。

- Windows 2000 の場合：「**スタート**」、「**設定**」、「**コントロール パネル**」、「**管理ツール**」、「**サービス**」の順に選択します。
- Windows NT の場合：「**スタート**」、「**設定**」、「**コントロール パネル**」、「**サービス**」の順に選択します。

「**Oracle Directory Service**」を右クリックし、「**プロパティ**」を選択します。

「**ログオン**」タブを選択します。

ローカル・システム・アカウントのラジオ・ボタンをクリアし、**このアカウント**を選択します。

Wallet を作成したときにログインしたアカウントを入力します。

サービスを停止して、再起動します。

OID 制御ユーティリティを使用して、SSL を使用可能にしたディレクトリ・サーバーを起動します。

この例では、SSL は Configset 1 で構成されます。ここでは、インスタンス ID が 2 であるディレクトリ・サーバー・インスタンスは、実行中ではないと仮定しています。次のコマンドを入力します。

```
oidctl connect=<et_service_name server=oidldapd instance=2 configset=1 start
```

Oracle Internet Directory 10*g*（9.0.4）での SSL の使用制限事項

同じホストで、SSL クライアントと非 SSL クライアントの両方をサポートする場合は、2 つの別々のサーバー・インスタンスを構成する必要があります。

Oracle Internet Directory 10*g*（9.0.4）では、Oracle ディレクトリ・レプリケーション・サーバーは、SSL 対応の Oracle ディレクトリ・サーバー・インスタンスとは直接通信できません。

関連項目： サーバー・インスタンスの構成方法は、第 5 章「Oracle ディレクトリ・サーバーの管理」を参照してください。

14

ディレクトリ・アクセス制御

この章では、アクセス制御ポリシーの概要および Oracle Directory Manager またはコマンドライン・ツール ldapmodify を使用してディレクトリのアクセス制御を管理する方法について説明します。

この章では、次の項目について説明します。

- アクセス制御ポリシーの管理の概要
- ACL 評価の動作
- Oracle Directory Manager を使用したアクセス制御の管理
- コマンドライン・ツールを使用したアクセス制御の管理

関連項目：

- アクセス制御ポリシーの実装と管理を開始する前に理解しておく必要がある概要については、2-11 ページの「セキュリティ」および第 12 章「ディレクトリ・セキュリティの概要」を参照してください。
- アクセス制御情報アイテム（ACI）の書式（構文）の詳細は、付録 E「アクセス制御ディレクティブ書式」を参照してください。

アクセス制御ポリシーの管理の概要

アクセス制御ポリシーは、対応するエントリ内の **ACI** 属性の値を構成して管理します。そのためには、Oracle Directory Manager または ldapmodify のいずれかを使用します。

この項では、次の項目について説明します。

- アクセス制御管理の構造体
- アクセス制御情報アイテム（ACI）のコンポーネント
- LDAP 操作のアクセス・レベル要件

アクセス制御管理の構造体

この項では、Oracle Internet Directory でアクセス制御に使用される構造について説明します。たとえば次のようなものです。

- アクセス制御ポリシー・ポイント（ACP）
- 規定のアクセス制御のための orclACI 属性
- エントリ・レベルのアクセス制御のための orclEntryLevelACI 属性
- 権限グループ

アクセス制御ポリシー・ポイント（ACP）

ACP は、`orclACI` 属性が指定されたエントリです。`orclACI` 属性の値は、エントリのサブツリーによって継承されるアクセス・ポリシーを示します。エントリのサブツリーは、そのサブツリーのルートとなる ACP から始まります。

ディレクトリ・サブツリー内に複数の ACP の階層が存在する場合、そのサブツリー内の従属エントリは、すべての上位 ACP からアクセス・ポリシーを継承します。継承結果のポリシーは、そのエントリより上位の ACP 階層内のポリシーを集約したものです。

たとえば、HR 部門のエントリに ACP が設定されており、HR 部門内に、Benefits、Payroll および Insurance グループのエントリがある場合、この 3 つのグループ内のエントリはいずれも、HR 部門のエントリに指定されたアクセス権を継承します。

ACP の階層内に競合するポリシーがある場合、ディレクトリは、集約したポリシーの評価には明確に定義された優先順位規則を適用します。

関連項目： 14-13 ページの「ACL 評価の動作」

規定のアクセス制御のための orclACI 属性

orclACI 属性には、規定のアクセス制御リスト（ACL）・ディレクティブが含まれています。つまりこのディレクティブは、この属性が定義されている ACP より下位のサブツリー内にあるすべてのエントリに適用されます。ディレクトリ内のあらゆるエントリに、この属性の値を含めることができます。この属性自体へのアクセスは、他の属性に対するアクセスと同様に制御されます。

注意： 単一のエントリ固有の ACL ディレクティブを orclACI 属性で示すことができます。ただし、その場合には、「エントリ・レベルのアクセス制御のための orclEntryLevelACI 属性」で説明する、管理が容易でパフォーマンス上のメリットもある orclEntryLevelACI の使用をお薦めします。これは、orclACI を介して示されるディレクティブの数によって LDAP 操作のオーバーヘッドが増加するためです。エントリ固有のディレクティブを orclACI から orclEntryLevelACI に移動すると、このオーバーヘッドを削減できます。

エントリ・レベルのアクセス制御のための orclEntryLevelACI 属性

あるポリシーが特定のエンティティ（例：特別のユーザー）のみに関係するとき、単一のエントリ内で、そのエントリに固有の ACL ディレクティブをメンテナンスできます。Oracle Internet Directory では、orclEntryLevelACI と呼ばれるユーザーが変更可能な操作属性を使用して前述のディレクティブを管理できます。orclEntryLevelACI 属性には、関連付けられたエントリにのみ適用される ACL ディレクティブが含まれます。

いずれのディレクトリ・エントリにも、この属性の値をオプションで設定できます。それは、Oracle Internet Directory が抽象型クラス top を拡張し、オプション属性として orclEntryLevelACI を組み込むからです。

orclEntryLevelACI 属性は複数値の属性で、構造は orclACI と類似しています。

> **関連項目：** orclEntryLevelACI 属性の構造の定義については、14-7 ページの「オブジェクト：アクセス権を付与するオブジェクト」を参照してください。

セキュリティ・グループ

Oracle Internet Directory 内のグループ・エントリは、groupOfNames オブジェクト・クラスまたは groupOfUniqueNames オブジェクト・クラスのいずれかと関連付けられます。グループ内のメンバーシップは、それぞれ member 属性または uniqueMember 属性の値として指定されます。

個人またはエンティティのグループにアクセス権を指定するには、セキュリティ・グループでそのグループを識別します。セキュリティ・グループには、ACP グループと権限グループの 2 つのタイプがあります。

ACP グループ 個人が ACP グループのメンバーである場合、ディレクトリ・サーバーは、その ACP グループに関連付けられている権限をその個人に単純に付与します。

ACP グループを使用して、ACP のレベルでアクセス権を解決します。たとえば、エントリを参照できるアクセス権を数百ものユーザーに付与すると仮定します。参照権限を各エントリに個別に付与することもできますが、この作業には相当な管理オーバーヘッドが必要となります。さらに、後日その権限の変更が決定した場合は、各エントリを個々に修正する必要があります。より効率的な解決策は、権限を集合的に割り当てることです。そのためには、グループ・エントリを作成して ACP グループとして指定し、必要な権限をそのグループに割り当てた後、ユーザーをそのグループのメンバーに割り当てます。その後、アクセス権を変更する場合は、個々のユーザーに対してではなく、グループに対して 1 箇所で変更を行います。同様に、権限を削除する場合は、多数の各エントリにアクセスするのではなく、グループから権限を削除することによって、複数のユーザーから権限を削除できます。

ACP グループは、`orclacpgroup` オブジェクト・クラスに関連付けられています。

権限グループ 権限グループは、上位レベルのアクセス・グループです。同様の権限を持つユーザーを管理する点では、ACP グループと類似しています。ただし、権限グループは、単一の ACP 以外に追加チェックを提供します。たとえば、ある ACP によってアクセスが制限される場合、ディレクトリ・サーバーは、アクセスを制限されるユーザーがいずれかの権限グループに属しているかどうかをユーザー・エントリの属性によって判断します。権限グループに属している場合、このユーザーには上位管理レベルで別途の権限があるため、ディレクトリ情報ツリーで上位管理レベルすべてがチェックされます。要求したオブジェクトへのアクセス権を権限グループに付与することを示す上位 ACP が見つかった場合、ディレクトリ・サーバーは、下位 ACP による制限を無視してアクセス権をユーザーに付与します。

通常は、ACP グループのみを実装します。権限グループが提供する追加チェックは、パフォーマンスを低下させる可能性があります。下位レベルの標準的な制御よりも上位レベルのアクセス制御を優先させる権限が必要な場合にのみ、権限グループを使用します。

権限グループを使用して、ディレクトリ情報ツリーの下位 ACP では認識されない管理者に対して、アクセス権を付与します。たとえば、ホスティングされた環境のグローバル管理者が、レルムで操作を行う必要があると仮定します。グローバル管理者の識別情報はホスティングされた企業のレルムでは認識されないため、ディレクトリ・サーバーは、そのレルムの ACP のみに依存している場合必要なアクセスを拒否します。ただし、グローバル管理者が権限グループのメンバーである場合、ディレクトリ・サーバーは、ディレクトリ情報ツリーの上位で、そのサブツリーへのアクセス権をこの権限グループに付与している ACP を検索します。アクセス権を付与している ACP が見つかった場合、ディレクトリ・サーバーは、ホスティングされた企業のレルムにある ACP による制限を無視します。

権限グループは、`orclPrivilegeGroup` オブジェクト・クラスに関連付けられています。

両方のタイプのグループに属するユーザー ユーザーが ACP グループと権限グループの両方のメンバーの場合、ディレクトリ・サーバーは、各タイプのグループについて評価を行います。ディレクトリ・サーバーは、ディレクトリ情報ツリーで上位の ACP に注目して、権限グループのアクセス権を解決します。

概要 : グループへのアクセス権の付与 アクセス権をユーザーのグループに付与する手順は、次のとおりです。

1. 通常の方法でグループ・エントリを作成します。
2. グループ・エントリを `orclPrivilegeGroup` オブジェクト・クラスまたは `orclACPgroup` オブジェクト・クラスに関連付けます。
3. そのグループのアクセス・ポリシーを指定します。
4. メンバーをグループに割り当てます。

ディレクトリ・サーバーによるセキュリティ・グループ・メンバーシップの検出方法 エントリは、グループの直接のメンバーとなるか、またはグループをネストして権限グループの一群を形成し、他の ACP または権限グループの間接のメンバーとなることができます。与えられたレベルで指定されているアクセス・ポリシーは、そのレベル以下のすべてのメンバーに直接的または間接的に適用されます。

Oracle Internet Directory は、セキュリティ・グループのみをアクセス制御目的で評価するため、その他のタイプのグループに対してアクセス・ポリシーを設定できません。ユーザーが特定の識別名とバインドされると、Oracle Internet Directory は、セキュリティ・グループ内でそのユーザーの直接のメンバーシップを検出します。指定した識別名の第 1 レベルのグループを認識すると、Oracle Internet Directory は、この第 1 レベルのグループすべての、他のセキュリティ・グループに対するネストを検出します。この処理は、評価対象のネストされたグループがなくなるまで行われます。

各セキュリティ・グループ（ネストされているかどうかに関係なく）は、セキュリティ・グループのオブジェクト・クラス（`orclACPgroup` または `orclPrivilegeGroup`）に関連付けられている必要があります。グループがセキュリティ・グループのメンバーの場合でも、セキュリティ・グループのオブジェクト・クラスに関連付けられていないかぎり、ディレクトリ・サーバーではアクセス制御目的のグループとはみなされません。セキュリティ・グループ内でユーザーのメンバーシップが判断された場合、ディレクトリ・サーバーでは、セッションの存続期間にわたってその情報を使用します。

例 : セキュリティ・グループ・メンバーシップの検出 たとえば、次のエントリのグループを仮定します。group4 以外は、それぞれ権限グループ（objectclass:orclprivilegegroup）として指定されています。管理者は、group1、group2 および group3 のメンバーに適用されるアクセス制御ポリシーを設定できます。

group 1

```
dn: cn=group1, c=us
cn: group1
objectclass: top
objectclass: groupofUniquenames
objectclass: orclprivilegegroup
uniquemember: cn=mary smith, c=us
uniquemember: cn=joe smith, c=us
uniquemember: cn=bill smith, c=us
```

group 2

```
dn: cn=group2, c=us
cn: group2
objectclass: top
objectclass: groupofUniquenames
objectclass: orclprivilegegroup
uniquemember: cn=mary jones, c=us
uniquemember: cn=joe jones, c=us
uniquemember: cn=bill jones, c=us
```

group 3

```
dn: cn=group3, c=us
cn: group3
objectclass: top
objectclass: groupofUniquenames
objectclass: orclprivilegegroup
uniquemember: cn=group2, c=us
uniquemember: cn=group1, c=us
uniquemember: cn=group4, c=us
```

group 4

```
dn: cn=group4, c=us
cn: group4
objectclass: top
objectclass: groupofUniquenames
uniquemember: cn=john doe, c=uk
uniquemember: cn=jane doe, c=uk
uniquemember cn=anne smith, c=us
```

group 3、c=us には、次のネストされたグループが含まれています。

- cn=group2,c=us
- cn=group1,c=us
- cn=group4,c=us

group3 のアクセス制御ポリシーは、group3、group1 および group2 のメンバーに適用されます。これは、各グループが権限グループとして指定されているためです。この同じアクセス制御ポリシーは、group4 のメンバーには適用されません。これは、group4 は権限グループとして指定されていないためです。

たとえば、ユーザーが識別名 `cn=john smith,c=uk` で group4 のメンバーとして Oracle Internet Directory にバインドされている場合を考えてみます。group3 のメンバーに適用されるアクセス・ポリシーがこのユーザーに適用されることはありません。これは、このユーザーの唯一の直接メンバーシップが非権限グループに対するものであるためです。これに対して、ユーザーが `cn=john smith,c=us`、つまり、group1 と group2 のメンバーとしてバインドされている場合、そのアクセス権は group1、group2 および group3（group1 と group2 がネストされているため）のメンバーに対して設定されているアクセス・ポリシーで管理されます。これは、この 3 つのグループすべてがオブジェクト・クラス `orclPrivilegeGroup` と関連付けられているためです。

> **関連項目：** グループ・エントリを変更して、`orclPrivilegeGroup` または `orclACPgroup` オブジェクト・クラスに対して関連付けまたは関連付け解除を行う方法については、7-7 ページの「Oracle Directory Manager を使用したエントリの変更」または 7-11 ページの「例 : ldapmodify を使用したユーザー・エントリの変更」を参照してください。

アクセス制御情報アイテム（ACI）のコンポーネント

ACI とは、様々なエンティティまたは対象がディレクトリ内の指定されたオブジェクトに対して操作を行う必要がある権限を表します。したがって、ACI は次の 3 つのコンポーネントで構成されています。

- アクセス権限を付与するオブジェクト
- アクセス権限を付与するエンティティ（対象）
- 付与するアクセス権限の種類

オブジェクト : アクセス権を付与するオブジェクト

アクセス制御ディレクティブのオブジェクト部分は、そのアクセス制御が適用されるエントリと属性を決定します。エントリまたは属性のいずれかに適用できます。

ACI に関連付けられているエントリ・オブジェクトは、ACI 自体が定義されているエントリまたはサブツリーによって暗黙的に識別されます。属性のレベルにおけるその他の条件は、ACL 式で明示的に指定されます。

`orclACI` 属性においては、ACI のオブジェクトのエントリ識別名コンポーネントは、暗黙的に、最上位のエントリの ACP から始まるサブツリー内のエントリすべての識別名コンポーネントです。たとえば、`dc=com` が ACP の場合、その ACI で管理されるディレクトリ領域は次のようになります。

```
.*, dc=com
```

ただし、ディレクトリ領域は暗黙的であるため、この識別名コンポーネントは不要で、構文的にも許可されません。

orclEntryLevelACI 属性においては、ACL のオブジェクトのエントリ識別名コンポーネントは、暗黙的にエントリ自体の識別名コンポーネントです。たとえば、dc=acme,dc=com にエントリ・レベルの ACI が関連付けられている場合、その ACI が管理しているエントリは dc=acme,dc=com 自体です。ただし、これは暗黙的であるため、この識別名コンポーネントは不要で、構文的にも許可されません。

ACL のオブジェクト部分は、次のようにエントリ内の属性と一致させるフィルタによって、エントリをオプションで限定できます。

```
filter=(ldapFilter)
```

ldapFilter は、LDAP 検索フィルタの文字列を表しています。特別なエントリ・セレクタ * は、全エントリの指定に使用されます。

エントリ内の属性をポリシーに組み込むには、次のようにカンマで区切られた属性名のリストをオブジェクト・セレクタに組み込みます。

```
attr=(attribute_list)
```

エントリ内の属性をポリシーから除外するには、次のようにカンマで区切られた属性名のリストをオブジェクト・セレクタに組み込みます。

```
attr!=(attribute_list)
```

注意： エントリ自体に対するアクセス権は、特別なオブジェクト・キーワード ENTRY を使用して、付与または否認する必要があります。属性に対してアクセス権を付与するのみでは不十分で、ENTRY キーワードを指定してエントリ自体にアクセス権を付与する必要があることに注意してください。

関連項目： ACI の書式（構文）の詳細は、付録 E「アクセス制御ディレクティブ書式」を参照してください。

対象 : アクセス権を付与する対象

この項では、次の項目について説明します。

- アクセス権が付与されるエンティティ
- バインド・モード（そのエンティティ識別情報の検証に使用される認証モード）
- オブジェクト追加制約（アクセス権を付与されたユーザーが、親の下に追加できるオブジェクトの種類の制限）

エンティティ アクセス権は、エントリではなくエンティティに対して付与されます。エンティティ・コンポーネントは、アクセス権が付与されているエンティティを指定します。

直接または間接的にエンティティを指定できます。

エンティティの直接指定: この方法は、実際のエンティティ値の入力（たとえば、group=managers）を必要とします。次の要素を使用して値を入力します。

- 任意のエントリと一致するワイルド・カード文字（*）
- アクセス権によって保護されているエントリと一致するキーワード SELF
- エントリの識別名と一致する正規表現（たとえば、dn=regex）
- 権限グループ・オブジェクトのメンバー（group=dn）

エンティティの間接指定: これはエンティティを動的に指定する方法です。アクセス権を付与しているエントリの一部である識別名値属性を指定する必要があります。識別名値属性には次の 3 つのタイプがあります。

- dnattr: この属性を使用して、このエントリに対してアクセス権を付与または制限しているエンティティの識別名を指定します。
- groupattr: この属性を使用して、このエントリに対してアクセス権を付与または制限している管理グループの識別名を指定します。
- guidattr: この属性を使用して、このエントリに対してアクセス権を付与または制限するエントリのグローバル・ユーザー識別子（orclGUID）を指定します。

たとえば、Anne Smith のマネージャが彼女のエントリで給与属性を変更できるように指定する場合を想定します。マネージャの識別名を直接指定するかわりに、識別名値属性を指定します（dnattr=<manager>）。次に、John Doe が Anne の給与属性を変更しようとすると、ディレクトリ・サーバーでは次の処理が実行されます。

- Anne のマネージャ属性の値を参照し、John Doe であることを確認します。
- バインド識別名とマネージャ属性が一致することを確認します。
- 適切なアクセス権を John Doe に付与します。

バインド・モード バインド・モードは、対象が使用する認証と暗号化の方法を指定します。

認証には、次の 4 つのモードがあります。

- MD5 ダイジェスト
- PKCS12
- プロキシ
- 簡易 : パスワードベースの簡易認証。

暗号化には、次の 3 つのオプションがあります。

- SASL
- SSL 認証なし
- SSL 一方向

暗号化モードの指定はオプションです。未指定の場合は、選択した認証モードが PKCS12 でないかぎり暗号化は使用されません。PKCS12 を使用して送信したデータは、すべて暗号化されます。

認証の選択肢には次のような優先順位規則があります。

匿名 < プロキシ < 簡易 <MD5 ダイジェスト <PKCS12

この規則は次のことを意味します。

- プロキシ認証は、匿名アクセスをブロックします。
- 簡易認証は、プロキシおよび匿名アクセスの両方をブロックします。
- MD5 ダイジェスト認証は、簡易、プロキシおよび匿名アクセスをブロックします。
- PKCS12 認証は、MD5 ダイジェスト、簡易、プロキシおよび匿名アクセスをブロックします。

バインド・モードの構文は次のとおりです。

```
BINDMODE =(LDAP_AUTHENTICATION_CHOICE + [ LDAP_ENCRYPTION_CHOICE ] )
LDAP_AUTHENTICATION_CHOICE = Proxy | Simple | MD5Digest | PKCS12
LDAP_ENCRYPTION_CHOICE = SSLNoAuth | SSLOneway | SASL
```

LDAP_ENCRYPTION_CHOICE パラメータはオプションです。未指定の場合、ディレクトリ・サーバーでは、暗号化は使用されないとみなされます。

オブジェクト追加制約 親エントリに追加アクセス権がある場合、階層内の下位エントリとしてオブジェクトを追加できます。オブジェクト追加制約は、*ldapfilter* を指定することによって、追加アクセス権を制限するために使用できます。

> **関連項目：** 付録 E「アクセス制御ディレクティブ書式」および 付録 D「LDAP フィルタ定義」

操作 : 付与するアクセス権の種類

付与するアクセス権の種類は次のいずれかです。

- なし
- Compare/nocompare
- Search/nosearch
- Browse/nobrowse
- Proxy/noproxy
- Read/noread
- Selfwrite/noselfwrite
- Write/nowrite
- Add/noadd
- Delete/nodelete

各アクセス・レベルを個々に付与または否認できることに注意してください。no*xxx* という記述は、*xxx* 権限が否認されていることを意味します。

エントリに関連付けられているアクセス権と、属性に関連付けられているアクセス権があることに注意してください。

表 14-1 アクセスのタイプ

アクセス・レベル	説明	オブジェクトのタイプ
比較	属性値で比較操作を実行する権限。	属性
読取り	属性値を読み取る権限。属性に対して読取り権限が与えられている場合でも、エントリ自体に参照権限がないかぎり値は戻されません。	属性
検索	検索フィルタで属性を使用する権限。	属性
自己書込み	識別名のグループ・エントリ属性のリスト内で、ユーザー自身の追加 / 削除あるいは自身のエントリを変更を行う権限。このレベルを使用すると、メンバーがリスト上の自分自身をメンテナンスできます。たとえば、次のコマンドを実行すると、グループ内のユーザーが member 属性上で、自分自身の識別名のみを追加または削除できます。 `access to attr=(member) by dnattr=(member) (selfwrite)` `dnattr` セレクタは、member 属性にリストされているエンティティにアクセス権が適用されるように指定します。`selfwrite` アクセス権セレクタは、そのメンバーが、属性上で自分自身の識別名のみを追加または削除できるように指定します。	属性
書込み	エントリの属性を変更 / 追加 / 削除する権限。	属性

表 14-1 アクセスのタイプ（続き）

アクセス・レベル	説明	オブジェクトのタイプ
なし	アクセス権なし。対象とオブジェクトの組合せにアクセス権を付与しない場合、対象にとってオブジェクトがそのディレクトリに存在しないかのように見えるという効果があります。	エントリおよび属性
追加	ターゲットのディレクトリ・エントリの下にエントリを追加する権限。	エントリ
プロキシ	別のユーザーの代理となる許可。	エントリ
参照	検索結果に識別名を戻すための権限。X.500 のリスト権限と同等です。この権限は、クライアントがエントリの識別名を ldapsearch 操作でベース識別名として使用するときにも必要です。	エントリ
削除	ターゲットのエントリを削除する権限。	エントリ

エントリ・レベルのアクセス・ディレクティブは、オブジェクト・コンポーネント内のキーワード ENTRY で識別されます。

注意： デフォルトのアクセス制御ポリシーでは、エントリおよび属性の両方を対象に、すべての人に、エントリ内のすべての属性の読取り、検索、書込みおよび比較の各アクセス権が付与されており、自己書込み権限は未指定です。エントリが未指定の場合、アクセス権は、そのアクセス権が指定されている直近の上位レベルで判断されます。

LDAP 操作のアクセス・レベル要件

次の表に、LDAP 操作と、各操作の実行に必要なアクセス権を示します。

表 14-2 LDAP 操作および各操作の実行に必要なアクセス権

操作	必要なアクセス権
オブジェクトの作成	親エントリに対する追加アクセス権
変更	変更対象の属性に対する書込みアクセス権
識別名の変更	現行の親に対する削除アクセス権と新しい親に対する追加アクセス権
相対識別名の変更	ネーミング属性すなわち相対識別名属性に対する書込みアクセス権
オブジェクトの削除	削除対象のオブジェクトに対する削除アクセス権
比較	属性に対する比較アクセス権とエントリに対する参照アクセス権

表 14-2 LDAP 操作および各操作の実行に必要なアクセス権（続き）

操作	必要なアクセス権
検索	■ フィルタ属性での検索アクセス権およびエントリでの参照アクセス権（エントリ識別名が結果として戻される必要がある場合） ■ フィルタ属性での検索アクセス権、エントリでの参照アクセス権および属性での読取り権（その値が結果として戻される必要があるすべての属性について）

ACL 評価の動作

ユーザーが指定されたオブジェクトで操作を実行しようとすると、ディレクトリ・サーバーは、そのオブジェクト上で操作を実行するための適切なアクセス権がユーザーにあるかどうかを判断します。オブジェクトがエントリの場合、ディレクトリ・サーバーは、エントリおよびその各属性に対するアクセス権を系統的に評価します。

オブジェクト（エントリの属性も含む）へのアクセス権の評価は、そのオブジェクトの ACI ディレクティブすべての検証を必要とする場合があります。これは、ACP に階層的な特性があり、上位 ACP から従属 ACP にポリシーが継承されるためです。

ディレクトリ・サーバーは、最初にエントリ・レベル ACI（`orclEntryLevelACI`）の ACI ディレクティブを検証します。検証は最も近い ACP に進み、評価が完了するまで各上位 ACP を次々と考慮します。

ACL の評価時には、属性は次のいずれかの状態になります。

表 14-3 ACL 評価時の属性の状態

状態	説明
Resolved with permission	属性に対して要求されたアクセスは、ACI で付与されています。
否認による解決	属性に対して要求されたアクセスは、ACI で明示的に否認されています。
Unresolved	対象の属性に対して、適用可能な ACI がまだ見つかりません。

検索を除き、次の場合にはすべての操作の評価が停止します。

- エントリ自体に対するアクセス権が否認される
- 属性のいずれかが「否認による解決」の状態になる

この場合、操作は失敗し、ディレクトリ・サーバーはエラーをクライアントに戻します。

検索操作の場合は、すべての属性が「Resolved」の状態になるまで評価が続けられます。「否認による解決」の属性は戻されません。

この項では、次の項目について説明します。

ACL の評価に使用される優先順位規則

LDAP の操作では、LDAP セッションの BindDN（つまりサブジェクト）に、そのオブジェクト（エントリ自体およびエントリの個々の属性を含む）で操作を実行するための特定の権限が必要です。

通常は、アクセス制御の管理認可レベルの階層があります。ネーミング・コンテキストのルートから、継承する管理ポイント（または ACP）までが 1 つの階層です。ACP は、`orclACI` 属性の定義済の値を持つあらゆるエントリです。また、単一のエントリ固有のアクセス情報をそのエントリ（`orclEntryLevelACI`）内で示すこともできます。

ACL の評価には、LDAP 操作の実行に必要な権限が対象にあるかどうかを判別する処理が含まれています。通常、`orclentryLevelACI` または `orclACI` には、ACL の評価に必要な情報がすべて含まれているわけではありません。したがって、評価が完全に解決されるまで、使用可能なすべての ACL 情報が、一定の順序で処理されます。

処理の順序は次の規則に従います。

- エントリ・レベルの ACI が最初に検証されます。`orclACI` の ACI は、そのターゲット・エントリに一番近い ACP から順に上位方向に検証されます。
- 必要な権限が判別された時点で、評価は停止します。それ以外は評価が継続されます。
- 単一の ACI 内では、セッションの識別名と関連付けられているエンティティが、by 句で識別される複数の項目と一致している場合、有効なアクセス権が次のように評価されます。
  - 一致する by 句の項目内で付与された全権限の UNION

    次の場合の AND 検索
  - 一致する by 句の項目内で否認された全権限の UNION

エントリ・レベルにおける優先順位

エントリ・レベルにおける ACI は、次の順序で評価されます。

1. フィルタを使用している場合。たとえば、次のようになります。

```
access to entry filter=(cn=p*)
    by group1 (browse, add, delete)
```

2. フィルタを使用していない場合。たとえば、次のようになります。

```
access to entry
    by group1 (browse, add, delete)
```

属性レベルにおける優先順位

属性レベルにおいては、属性が指定されている ACI が未指定の ACI よりも優先されます。

1. 属性が指定されている ACI は、次の順序で評価されます。
   a. フィルタを使用しているもの。たとえば、次のようになります。

```
access to attr=(salary) filter=(salary > 10000)
by group1 (read)
```

   b. フィルタを使用していないもの。たとえば、次のようになります。

```
access to attr=(salary)
by group1 (search, read)
```

2. 属性が未指定の ACI は、次の順序で評価されます。
   a. フィルタを使用している場合。たとえば、次のようになります。

```
access to attr=(*) filter (cn=p*)
by group1 (read, write)
```

   b. フィルタを使用していない場合。たとえば、次のようになります。

```
access to attr=(*)
by group1 (read, write)
```

同一オブジェクトに対する複数 ACI の使用

Oracle Internet Directory リリース 9.0.4 から、オブジェクトの ACP 内に複数の ACI を定義できるようになりました。Oracle Internet Directory は、オブジェクトに関連付けられている各 ACI を処理して、内部 ACP キャッシュ内に単一 ACI として格納します。その後、ACP 内に指定された複数の ACI のすべての関連ポリシーを適用します。

この動作については、次の ACP の例を参照してください。

```
Access to entry by dn="cn=john" (browse,noadd,nodelete)
Access to entry by group="cn=admingroup" (browse,add,nodelete)
Access to entry by dn=".*,c=us" (browse,noadd,nodelete)
```

この ACP には、オブジェクト・エントリに対する 3 つの ACI があります。この ACP をロードする場合、Oracle Internet Directory は、内部 ACP キャッシュ内でこの 3 つの ACI を 1 つの ACI としてマージします。

ACI の構文は次のとおりです。

```
Access to <OBJECT> by <SUBJECT> <ACCESSLIST>
<OBJECT> = [ entry |  attr [EQ-OR-NEQ] ( * | <ATTRLIST> ) ]
[ filter = ( <LDAFILTER> ) ]
```

この構文は、次のオブジェクトのタイプを可能にします。

- entry
- entry + filter = （*LDAPFILTER*）
- attr =（*ATTRLIST*）
- attr =（*ATTRLIST*）+ filter =（*LDAPFILTER*）
- attr !=（*ATTRLIST*）
- attr !=（*ATTRLIST*）+ filter =（*LDAPFILTER*）
- attr =（*）
- attr =（*）+ filter =（*LDAPFILTER*）

前述のすべてのオブジェクトのタイプに対して、複数の ACI を定義できます。ACP の初期ロード時に、ディレクトリ・サーバーは、定義されたオブジェクト・タイプに基づいて ACI をマージします。ACI 内のオブジェクト文字列が完全一致の文字列かどうかを比較することが、一致基準となります。

1 つの ACI で `ATTR=(ATTRLIST)` と、別の `ATTR!=(ATTRLIST)` が指定されている場合、`ATTR=(*)` はエントリ内で ACI としては指定できません。また、ACI で ATTR=(ATTRLIST) が指定されている場合に、ATTRLIST にはない属性に対するアクセス権限を指定するには、ATTR!=(ATTRLIST) ではなく ATTR=(*) を使用する必要があります。ATTR=(*) は、ATTRLIST で指定されている属性以外のすべての属性を示します。

ディレクトリ・オブジェクトに対する排他的アクセス権

指定したオブジェクトに ACI が存在している場合は、そのオブジェクト以外のすべてのオブジェクトに対してアクセス権を指定できます。そのためには、アクセス権をすべてのオブジェクトに付与するか、または 1 つのオブジェクトに対するアクセス権を否認します。

次の例は、アクセス権をすべての属性に付与します。

```
access to attr=(*)
by group2 (read)
```

次の例は、userpassword 属性に対するアクセス権を否認します。

```
access to attr!=(userpassword)
by group2 (read)
```

グループの場合の ACL 評価

属性またはエントリ自体の操作が、ディレクトリ情報ツリー内の下位の ACP で明示的に否認されている場合、通常、ACL によるそのオブジェクトの評価は、否認による解決とみなされます。しかし、そのセッションのユーザー（bindDN）がグループ・オブジェクトのメンバーの場合、評価はまだ解決されていないかのように継続されます。グループの対象セレクタを介して、ツリー内の上位の ACP でセッションのユーザーに権限が付与されている場合、この権限付与はディレクトリ情報ツリー内の下位での否認よりも優先されます。

この例は、上位レベルの ACP の ACL ポリシーが、ディレクトリ情報ツリー内の下位の ACP ポリシーよりも優先される唯一のケースです。

Oracle Directory Manager を使用したアクセス制御の管理

ACP 内のアクセス制御情報アイテム（ACI）は、Oracle Directory Manager またはコマンドライン・ツールを使用して表示および変更できます。この項では、Oracle Directory Manager でこれらのタスクを実行する方法について説明します。

注意： Oracle Internet Directory のインストール直後に、3-3 ページの「タスク 3: デフォルトのセキュリティ構成の再設定」の説明に従ってデフォルトのセキュリティ構成を必ずリセットしてください。

この項では、次の項目について説明します。

- アクセス制御管理のための Oracle Directory Manager の構成
- Oracle Directory Manager を使用した ACP の表示
- Oracle Directory Manager を使用した ACP の追加
- Oracle Directory Manager の ACP 作成ウィザードを使用した ACP の追加
- Oracle Directory Manager を使用した ACP の変更
- Oracle Directory Manager を使用したエントリ・レベルのアクセス権の付与
- 例 : Oracle Directory Manager を使用した ACP の管理

> **関連項目 :** コマンドライン・ツールの説明は、付録 A「LDIF およびコマンドライン・ツールの構文」を参照してください。

アクセス制御管理のための Oracle Directory Manager の構成

Oracle Directory Manager での ACP の表示方法および ACP 検索の実行方法を構成できます。

Oracle Directory Manager の ACP の表示の構成

Oracle Directory Manager では、ナビゲータ・ペインですべての ACP を自動的に表示するか、検索の結果としてのみ表示するかを決められます。ACP の数が多い場合は、検索の結果としてのみ表示できます。

ACP の表示を構成する手順は、次のとおりです。

1. ナビゲータ・ペインで「**Oracle Internet Directory サーバー**」を展開して、構成するサーバーを選択します。
2. ツールバーの「**ユーザー設定項目**」をクリックします。「ユーザー設定項目」ダイアログ・ボックスが表示されます。
3. 「**アクセス制御ポリシー管理の構成**」タブ・ページを選択します。
4. 次のいずれかを選択します。
   - **「常にすべての ACP を表示」**
   - **「検索要求に基づく ACP のみ表示」**
5. 「**OK**」を選択します。
6. 変更内容を反映するには、Oracle Directory Manager を再起動します。

Oracle Directory Manager を使用する場合の ACP の検索の構成

Oracle Directory Manager では、ACP の検索に次の項目が指定できます。

- 検索のルート
- 取り出されるエントリの最大数
- 検索の制限時間
- 検索の深さ

ACP エントリの検索を構成する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」を展開して、ディレクトリ・サーバー・インスタンスを選択します。
2. ツールバーの「**ユーザー設定項目**」を選択します。「ユーザー設定項目」ダイアログ・ボックスが表示されます。
3. 「**エントリ管理の構成**」タブを選択します。
4. 「**1 レベルのサブツリー・エントリの最大数**」のラベルが付いているフィールドに、ACP 検索で取得するエントリ数を入力します。
5. 「**最大の検索時間**」フィールドに、検索の最大時間を秒単位で入力します。
6. 「**OK**」を選択します。「注意」ウィンドウには、「ACP 管理の変更を表示するには、Oracle Directory Manager を再起動する必要があります。」というメッセージが表示されます。
7. 「注意」ウィンドウの「OK」を選択します。
8. 最新のアクセス制御管理のエントリを表示するには、Oracle Directory Manager を切断し、すぐに再接続します。

Oracle Directory Manager を使用した ACP の表示

14-18 ページの「Oracle Directory Manager の ACP の表示の構成」の説明に従って常に ACP を表示するように Oracle Directory Manager を構成した場合、ACP の位置を特定および表示する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**、「**アクセス制御管理**」の順に展開します。定義したすべての ACP は、いずれもナビゲータ・ペインの「アクセス制御管理」ノードの下に表示されます。
2. ナビゲータ・ペインで「**アクセス制御管理**」の下の ACP を選択すると、その情報が右側のペインに表示されます。「アクセス制御管理」ペインのフィールドの説明は、C-2 ページの表 C-1 を参照してください。

14-18 ページの「Oracle Directory Manager の ACP の表示の構成」の説明に従って検索の結果としてのみ ACP を表示するように Oracle Directory Manager を構成した場合に、ACP の位置を特定して表示する手順は、次のとおりです。

1. 「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開して、「**エントリ管理**」を選択します。
2. ACP として指定したエントリの検索を実行します。検索結果が右側ペインの下半分の「**識別名**」ボックスに表示されます。
3. 「**識別名**」ボックスで、エントリをダブルクリックします。対応する「エントリ」ダイアログ・ボックスが表示されます。
4. この ACP のサブツリーのアクセス制御を表示するには、「**サブツリー・アクセス**」タブを選択します。

   この ACP のエントリ・レベルのアクセス制御を表示するには、「**ローカル・アクセス**」タブを選択します。

Oracle Directory Manager を使用した ACP の追加

ACP は、規定の、すなわち継承可能なアクセス制御情報アイテム（ACI）を含んだエントリです。この情報は、エントリ自体とその下位エントリすべてに影響を与えます。一般的に、サブツリー全体にわたる規模の大きいアクセス制御をブロードキャストする ACP を作成します。

Oracle Directory Manager を使用して ACP を追加するには、次の 3 つのタスクが必要です。

- タスク 1: ACP にするエントリを指定します。
- タスク 2: 構造型アクセス項目（エントリに関係する ACI）を構成します。
- タスク 3: コンテンツ・アクセス項目（属性に関係する ACI）を構成します。

タスク 1: ACP にするエントリの指定

1. 14-18 ページの「Oracle Directory Manager の ACP の表示の構成」の説明に従って常に ACP を表示するように Oracle Directory Manager を構成した場合は、次のように開始します。

   a. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開します。

   b. 「**アクセス制御管理**」を選択し、手順 2 に進みます。

14-18 ページの「Oracle Directory Manager の ACP の表示の構成」の説明に従って検索の結果としてのみ ACP を表示するように Oracle Directory Manager を構成した場合は、次のように開始します。

a. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**、「**アクセス制御管理**」の順に展開します。

b. ACP を常駐させるノードを選択します。構成された ACP が存在しない場合は、「DSE ルート」の下の ACP を選択できます。

2. ツールバーの「**作成**」ボタンを選択します。「新規アクセス制御ポイント」ダイアログ・ボックスが表示されます。

3. 「**エントリへのパス**」フィールドで、ACP に指定するエントリの識別名を入力します。また、識別名は、「**エントリへのパス**」フィールドの右側の「**参照**」を選択して検索することもできます。

タスク 2: 構造型アクセス項目の構成

1. 構造型アクセス項目（エントリに関係する ACI）を定義するには、「**構造型アクセス項目**」ウィンドウの下の「**作成**」を選択します。「構造型アクセス項目」ダイアログ・ボックスが表示されます。このダイアログ・ボックスには、「**エントリ・フィルタ**」、「**追加されたオブジェクト・フィルタ**」、「**責任者**」および「**アクセス権限**」の 4 つのタブがあります。

2. ACP では、定義されたアクセス権は、他のフィルタによりアクセスがそれ以上制限されないかぎり、このエントリおよびそのエントリのすべてのサブエントリに適用されます。

   ACP のすべての下位エントリを ACP で管理する場合は、「**エントリ・フィルタ**」タブ・ページには何も入力せず、次の手順に進みます。それ以外の場合は、この手順を実行します。

   適切な場合、「**エントリ・フィルタ**」タブ・ページを使用して、アクセスを指定するエントリを識別します。

   エントリへのアクセスを、このエントリの 1 つ以上の属性に基づいて制限できます。たとえば、役職名がマネージャで組織単位がアメリカであるすべてのエントリへのアクセスを制限できます。

   アクセスを指定するエントリを識別する手順は、次のとおりです。

   a. 検索基準バーの一番左のメニューから、属性タイプを選択します。

   b. バーの中央のメニューから、フィルタ・オプションのいずれかを選択します。これらのオプションの説明は、C-33 ページの表 C-37 を参照してください。

   c. 検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。

3. 「**追加されたオブジェクト・フィルタ**」タブ・ページを選択します。

   ACI を指定して、ユーザーが追加できるエントリの種類を制限できます。たとえば、ユーザーが `objectclass=country` を持つエントリのみを追加できるように、DSE ルート・エントリで ACI を指定できます。その後、ディレクトリ・サーバーによって、新規エントリがこのフィルタの制限に適合するかどうかが検証されます。

   ユーザーが追加できるエントリの種類を制限する手順は、次のとおりです。

   a. 検索基準バーの一番左のメニューから、属性タイプを選択します。

   b. バーの中央のメニューから、フィルタ・オプションのいずれかを選択します。これらのオプションの説明は、C-33 ページの表 C-37 を参照してください。

   c. 検索基準バーの右のテキスト・ボックスに、選択した属性の値を入力します。

4. 「**責任者**」タブ・ページを選択します。

   a. 「**認証の選択**」リストから、対象（アクセス権を要求しているエンティティ）が使用する認証のタイプを選択します。オプションの説明は、C-2 ページの表 C-2 を参照してください。

      認証方式を選択しない場合は、どの種類の認証も受け入れられます。あるノードで指定されている認証方式は、通信先のノードで指定されている認証方式と一致している必要があります。

      「**暗号化の選択**」リストで、使用される暗号化のタイプを選択します。オプションの説明は、C-3 ページの表 C-3 を参照してください。

   b. アクセス権を付与するエンティティを指定します。オプションの説明は、C-3 ページの表 C-4 を参照してください。

5. 「**アクセス権限**」タブ・ページを選択します。

   a. 付与する権限の種類を指定します。

      * **参照** : 対象にエントリの表示を許可します。
      * **追加** : 対象に、このエントリの下への他のエントリの追加を許可します。
      * **削除** : 対象にエントリの削除を許可します。
      * **プロキシ** : 対象に、別のユーザーの代理となることを許可します。

   b. 「**OK**」をクリックします。

タスク 3: コンテンツ・アクセス項目の構成

1. コンテンツ・アクセス項目（属性に関係する ACI）を定義するには、「**コンテンツ・アクセス項目**」ウィンドウの下の「**作成**」を選択します。「コンテンツ・アクセス項目」ダイアログ・ボックスが表示されます。各タブ・ページには、変更可能な項目が含まれています。

2. ACP のすべての下位エントリを ACP で管理する場合は、「**エントリ・フィルタ**」タブ・ページには何も入力せず、手順 3 に進みます。それ以外の場合は、この手順を実行します。

   ACP では、定義されたアクセス権は、他のフィルタによりアクセスがそれ以上制限されないかぎり、このエントリおよびそのエントリのすべてのサブエントリに適用されます。適切な場合、「**エントリ・フィルタ**」タブ・ページを使用して、アクセスを指定するエントリを識別します。

   エントリへのアクセスを、このエントリの 1 つ以上の属性に基づいて制限できます。たとえば、役職名がマネージャで組織単位がアメリカであるすべてのエントリへのアクセスを制限できます。

   アクセスを指定するエントリを識別する手順は、次のとおりです。

   a. 検索基準バーの一番左のメニューから、属性タイプを選択します。

   b. バーの中央のメニューから、フィルタ・オプションのいずれかを選択します。詳細は、C-33 ページの表 C-37 を参照してください。

   c. 検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。

3. 「**責任者**」タブ・ページを選択します。

   a. 「**認証の選択**」リストから、対象（アクセス権を要求しているエンティティ）が使用する認証のタイプを選択します。オプションの説明は、C-2 ページの表 C-2 を参照してください。

      認証方式を選択しない場合は、どの種類の認証も受け入れられます。あるノードで指定されている認証方式は、通信先のノードで指定されている認証方式と一致している必要があります。

      「**暗号化の選択**」リストで、使用される暗号化のタイプを選択します。オプションの説明は、C-3 ページの表 C-3 を参照してください。

   b. アクセス権を付与するエンティティを指定します。オプションの説明は、C-3 ページの表 C-4 を参照してください。

4. 「**属性**」タブ・ページを選択します。

   a. 右のメニューから、アクセス権を付与または否認する属性を選択します。

b. 左のメニューから、属性に対して実行する一致操作を選択します。選択肢は「EQ」（=）と「NEQ」（!=）です。

たとえば、「EQ」と「cn」を選択した場合は、付与したアクセス権が cn 属性に適用されます。「NEQ」と「cn」を選択した場合は、付与したアクセス権が cn 属性に適用されません。

5. 「**アクセス権限**」タブ・ページを選択して、権限を指定します。詳細は、C-4 ページの表 C-5 を参照してください。

6. 「**OK**」をクリックしてこのダイアログ・ボックスを閉じ、Oracle Directory Manager のメイン・ダイアログ・ボックスに戻ります。

Oracle Directory Manager の ACP 作成ウィザードを使用した ACP の追加

ACP 作成ウィザードを使用すると、ACP を追加するために必要なタスクを順に実行できます。次のタスクがあります。

- タスク 1: ACP にするエントリを指定します。
- タスク 2: 構造型アクセス項目（エントリに関係する ACI）を構成します。
- タスク 3: コンテンツ・アクセス項目（属性に関係する ACI）を構成します。

タスク 1: ACP にするエントリの指定

1. 14-18 ページの「Oracle Directory Manager の ACP の表示の構成」の説明に従って常に ACP を表示するように Oracle Directory Manager を構成した場合は、次のように開始します。

   a. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開します。

   b. ナビゲータ・ペインで「**アクセス制御管理**」を選択し、手順 2 に進みます。

   14-18 ページの「Oracle Directory Manager の ACP の表示の構成」の説明に従って検索の結果としてのみ ACP を表示するように Oracle Directory Manager を構成した場合は、次のように開始します。

   a. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**、「**アクセス制御管理**」の順に展開します。

   b. ナビゲータ・ペインで ACP を常駐させるノードを選択します。構成された ACP が存在しない場合は、「DSE ルート」の下の ACP を選択できます。

2. ツールバーの「**作成**」ボタンをクリックします。「新規アクセス制御ポイント」ダイアログ・ボックスが表示されます。

3. 「**エントリへのパス**」フィールドで、ACP に指定するエントリの識別名を入力します。「エントリ管理」の下のナビゲータ・ペインを探すか、または「参照」をクリックして、識別名を検索することもできます。

ACP では、定義されたアクセス権は、このエントリおよびそのエントリのすべてのサブエントリに適用されるか、または特定のエントリのみに適用されます。次に、両オプションでの ACP の構成方法を説明します。

タスク 2: ACP 作成ウィザードを使用した構造型アクセス項目の構成

1. 構造型アクセス項目（エントリに関係する ACI）を定義するには、「構造型アクセス項目」ウィンドウの下の「**ウィザードで作成**」をクリックします。最初の「構造型アクセス項目」ダイアログ・ボックスが表示されます。

2. 規範的な構造型アクセス項目を指定した場合は、ACP のすべての下位エントリをこの ACP が管理します。規範的な構造型アクセス項目を希望する場合は、この最初の「構造型アクセス項目」ダイアログ・ボックスには何も入力する必要がありません。

   ただし、特定のエントリに対してアクセス権を付与する場合には、この最初の「構造的アクセス項目」ダイアログ・ボックスで、次の手順を実行します。

   a. 検索基準バーの左のメニューから、属性タイプを選択します。

   b. バーの中央のメニューから、フィルタ・オプションのいずれかを選択します。詳細は、C-33 ページの表 C-37 を参照してください。

   c. 検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。

   d. 「**次へ**」をクリックします。ユーザーが追加できるエントリの種類を制限するための ACI の指定を要求する、2 番目の「構造型アクセス項目」ダイアログ・ボックスが表示されます。

3. ACI を指定して、ユーザーが追加できるエントリの種類を制限できます。たとえば、ユーザーが `objectclass=country` を持つエントリのみを追加できるように、DSE ルート・エントリで ACI を指定できます。その後、ディレクトリ・サーバーによって、新規エントリがこのフィルタの制限に適合するかどうかが検証されます。

   ユーザーが追加できるエントリの種類を制限する手順は、次のとおりです。

   a. 検索基準バーの一番左のメニューから、属性タイプを選択します。

   b. バーの中央のメニューから、フィルタ・オプションのいずれかを選択します。詳細は、C-33 ページの表 C-37 を参照してください。

   c. 検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。

   d. 「**次へ**」を選択します。ウィザードによって、認証方式と暗号化方式、およびアクセス権を付与する対象の指定が要求されます。

4. 認証方式の指定はオプションです。認証方式を設定しない場合は、どの種類の認証も受け入れられます。あるノードで指定されている認証方式は、通信先のノードで指定されているバインド・モードと一致している必要があります。

   a. 認証のタイプを指定するには、「**認証の選択**」リストから、対象（アクセス権を要求しているエンティティ）が使用する認証のタイプを選択します。オプションの説明は、C-2 ページの表 C-2 を参照してください。

   b. 暗号化のタイプを指定するには、「**暗号化の選択**」リストから暗号化方式を選択します。オプションの説明は、C-3 ページの表 C-3 を参照してください。

   c. アクセス権を付与するエンティティを指定します。オプションの説明は、C-3 ページの表 C-4 を参照してください。

   d. 「**次へ**」をクリックします。アクセス権情報の入力を要求する「構造型アクセス項目」ダイアログ・ボックスが表示されます。

5. 付与する権限の種類を指定します。

   - **参照** : 対象にエントリの表示を許可します。
   - **追加** : 対象に、このエントリの下への他のエントリの追加を許可します。
   - **削除** : 対象にエントリの削除を許可します。
   - **プロキシ** : パスワードを指定せずに、エンティティの代理となることを許可します。

6. 「**終了**」をクリックします。

タスク 3: ACP 作成ウィザードを使用したコンテンツ・アクセス項目の構成

1. ウィザードを使用してコンテンツ・アクセス項目（属性に関係する ACI）を定義するには、「**コンテンツ・アクセス項目**」ウィンドウの下の「**ウィザードで作成**」をクリックします。最初の「コンテンツ・アクセス項目」ダイアログ・ボックスが表示されます。

2. 規範的なコンテンツ・アクセス項目を指定した場合は、ACP のすべての下位エントリをこの ACP が管理します。規範的なコンテンツ・アクセス項目を希望する場合は、この最初の「コンテンツ・アクセス項目」ダイアログ・ボックスには何も入力する必要がありません。

   ただし、アクセスを指定する属性を識別する手順は、次のとおりです。

   a. 検索基準バーの一番左のメニューから、属性タイプを選択します。

   b. バーの中央のメニューから、フィルタ・オプションのいずれかを選択します。詳細は、C-20 ページの表 C-25 を参照してください。

   c. 検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。

d. 「**次へ**」をクリックします。アクセス権を付与する対象の指定を要求する、2 番目の「コンテンツ・アクセス項目」ダイアログ・ボックスが表示されます。

e. 「**次へ**」を選択します。ウィザードによって、認証方式と暗号化方式、およびアクセス権を付与する対象の指定が要求されます。

3. 認証方式の指定はオプションです。認証方式を設定しない場合は、どの種類の認証も受け入れられます。あるノードで指定されている認証方式は、通信先のノードで指定されているバインド・モードと一致している必要があります。

   a. 認証のタイプを指定するには、「**認証の選択**」リストから、対象（アクセス権を要求しているエンティティ）が使用する認証のタイプを選択します。オプションの説明は、C-2 ページの表 C-2 を参照してください。

   b. 暗号化のタイプを指定するには、「**暗号化の選択**」リストから暗号化方式を選択します。オプションの説明は、C-3 ページの表 C-3 を参照してください。

   c. アクセス権を付与するエンティティを指定します。オプションの説明は、C-3 ページの表 C-4 を参照してください。

   d. 「**次へ**」をクリックします。属性およびこの属性に対して実行する一致操作の選択を要求する、「コンテンツ・アクセス項目」ダイアログ・ボックスが表示されます。

4. 属性およびこの属性に対して実行する一致操作を選択する手順は、次のとおりです。

   a. 「コンテンツ・アクセス項目」ダイアログ・ボックスの「属性」フィールドで、アクセス権を付与または制限する属性を右のリストから選択します。

   b. 左のリストから、属性に対して実行する一致操作を選択します。選択肢は「EQ」（=）と「NEQ」（!=）です。

   c. 「**次へ**」をクリックします。アクセス権の指定を要求する「コンテンツ・アクセス項目」ダイアログ・ボックスが表示されます。

5. 付与する権限の種類を指定します。詳細は、C-4 ページの表 C-5 を参照してください。

6. 「**終了**」をクリックします。

Oracle Directory Manager を使用した ACP の変更

Oracle Directory Manager を使用して ACP を変更するには、次の 3 つのタスクが必要です。

- タスク 1: 変更するエントリを指定します。
- タスク 2: 構造型アクセス項目（エントリに関係する ACI）を変更します。
- タスク 3: コンテンツ・アクセス項目（属性に関係する ACI）を変更します。

タスク 1: 変更するエントリの指定

1. 14-18 ページの「Oracle Directory Manager の ACP の表示の構成」の説明に従って常に ACP を表示するように Oracle Directory Manager を構成した場合は、次のように開始します。

   a. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**および「**アクセス制御管理**」を展開します。「**アクセス制御管理**」を選択します。ナビゲータ・ペインの「**アクセス制御管理**」の下のリストに、定義済のすべての ACP が表示されます。同じ内容のリストが、右側のペインにも表示されます。

   b. 「**アクセス制御管理**」の下で、変更する ACP を選択します。その ACP の情報が右側のペインに表示されます。または、右側のペインの ACP をダブルクリックすると、独立したダイアログ・ボックスにデータが表示されます。

   14-18 ページの「Oracle Directory Manager の ACP の表示の構成」の説明に従って検索の結果としてのみ ACP を表示するように Oracle Directory Manager を構成した場合は、次のように開始します。

   a. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**、「**アクセス制御管理**」の順に展開します。

   b. 変更する ACP を選択します。その ACP の情報が右側のペインに表示されます。

タスク 2: 構造型アクセス項目の変更

新規構造型アクセス項目を追加、または既存の構造型アクセス項目を変更できます。

> **関連項目：** 構造型アクセス項目の追加の詳細は、14-21 ページの「タスク 2: 構造型アクセス項目の構成」を参照してください。

構造型アクセス項目を変更する手順は、次のとおりです。

1. 「**構造型アクセス項目**」ウィンドウで変更する項目を選択し、「**構造型アクセス項目**」ウィンドウの下の「**編集**」をクリックします。「構造型アクセス項目」ダイアログ・ボックスが表示されます。
2. 「**エントリ・フィルタ**」タブ・ページを使用して、アクセス権を付与するエントリのセットを絞り込みます。ACP のすべての下位エントリを ACP で管理する場合は、次の手順に進んでください。

   1 つ以上の属性に基づいてエントリを選択する場合があります。たとえば、title が secretary の個人をすべて検索したり、title が manager で organization unit が Americas の個人をすべて検索することができます。

「**エントリ・フィルタ**」タブ・ページの「**基準**」ウィンドウで、検索基準バーを使用して属性を選択し、その属性の値を入力し、さらに指定した属性と入力値との一致条件を示すフィルタを指定します。この手順は、次のとおりです。

a. 検索基準バーの一番左のメニューから、属性を選択します。

b. バーの中央のメニューから、フィルタ・オプションのいずれかを選択します。詳細は、C-20 ページの表 C-25 を参照してください。

c. 検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。

3. 「**追加されたオブジェクト・フィルタ**」タブ・ページを使用して、ユーザーが追加できるエントリの種類を制限する ACI を指定できます。たとえば、ユーザーが `objectclass=country` を持つエントリのみを追加できるように、DSE ルート・エントリで ACI を指定できます。その後、ディレクトリ・サーバーによって、新規エントリがこのフィルタの制限に適合するかどうかが検証されます。

ユーザーが追加できるエントリの種類を制限する手順は、次のとおりです。

a. 検索基準バーの一番左のメニューから、属性タイプを選択します。

b. バーの中央のメニューから、フィルタ・オプションのいずれかを選択します。詳細は、C-33 ページの表 C-37 を参照してください。

c. 検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。

4. 「**責任者**」タブ・ページを使用して、認証方式と暗号化方式、および ACI の対象（アクセス権を要求しているエンティティ）を指定します。

認証方式の指定はオプションです。認証方式を設定しない場合は、どの種類の認証も受け入れられます。あるノードで指定されている認証方式は、通信先のノードで指定されているバインド・モードと一致している必要があります。

a. 認証のタイプを指定するには、「**認証の選択**」リストから、対象（アクセス権を要求しているエンティティ）が使用する認証のタイプを選択します。オプションの説明は、C-2 ページの表 C-2 を参照してください。

b. 暗号化のタイプを指定するには、「**暗号化の選択**」リストから暗号化方式を選択します。オプションの説明は、C-3 ページの表 C-3 を参照してください。

c. アクセス権を付与するエンティティを指定します。オプションの説明は、C-3 ページの表 C-4 を参照してください。

5. 「**アクセス権限**」タブ・ページを選択します。

a. 付与する権限の種類を決定します。

- **参照** : 対象にエントリの表示を許可します。
- **追加** : 対象に、このエントリの下への他のエントリの追加を許可します。

- **削除**: 対象にエントリの削除を許可します。
- **プロキシ**: パスワードを指定せずに、エンティティの代理となることを許可します。

  エントリが未指定の場合、アクセス権は、そのアクセス権が指定されている直近の上位レベルで判断されます。

6. 「**OK**」をクリックします。

タスク 3: コンテンツ・アクセス項目の変更

新規コンテンツ・アクセス項目を追加、または既存のコンテンツ・アクセス項目を変更できます。

> **関連項目：** コンテンツ・アクセス項目の追加の詳細は、14-23 ページの「タスク 3: コンテンツ・アクセス項目の構成」を参照してください。

コンテンツ・アクセス項目を変更する手順は、次のとおりです。

1. 「**コンテンツ・アクセス項目**」ボックスで変更するコンテンツ・アクセス項目を選択し、「**コンテンツ・アクセス項目**」ウィンドウの下の「**編集**」をクリックします。「コンテンツ・アクセス項目」ダイアログ・ボックスが表示されます。各タブ・ページには、変更可能な項目が含まれています。
2. ACP のすべての下位エントリを ACP で管理する場合は、「**エントリ・フィルタ**」タブ・ページには何も入力せず、次の手順に進みます。

   ACP では、定義されたアクセス権は、他のフィルタによりアクセスがそれ以上制限されないかぎり、このエントリおよびそのエントリのすべてのサブエントリに適用されます。適切な場合、「**エントリ・フィルタ**」タブ・ページを使用して、アクセスを指定するエントリを識別します。

   エントリへのアクセスを、このエントリの 1 つ以上の属性に基づいて制限できます。たとえば、役職名がマネージャで組織単位がアメリカであるすべてのエントリへのアクセスを制限できます。

   アクセスを指定するエントリを識別する手順は、次のとおりです。

   a. 検索基準バーの一番左のメニューから、属性タイプを選択します。
   b. バーの中央のメニューから、フィルタ・オプションのいずれかを選択します。詳細は、C-33 ページの表 C-37 を参照してください。
   c. 検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。

3. 「**責任者**」タブ・ページを使用して、認証方式と暗号化方式、および ACI の対象（アクセス権を要求しているエンティティ）を指定します。

   認証方式の指定はオプションです。認証方式を設定しない場合は、どの種類の認証も受け入れられます。あるノードで指定されている認証方式は、通信先のノードで指定されているバインド・モードと一致している必要があります。

   a. 認証のタイプを指定するには、「**認証の選択**」リストから、対象（アクセス権を要求しているエンティティ）が使用する認証のタイプを選択します。オプションの説明は、C-2 ページの表 C-2 を参照してください。

   b. 暗号化のタイプを指定するには、「**暗号化の選択**」リストから暗号化方式を選択します。オプションの説明は、C-3 ページの表 C-3 を参照してください。

   c. アクセス権を付与するエンティティを指定します。オプションの説明は、C-3 ページの表 C-4 を参照してください。

4. 「**属性**」タブ・ページを選択します。

   a. 右のメニューから、アクセス権を付与または否認する属性を選択します。

   b. 左のメニューから、属性に対して実行する一致操作を選択します。選択肢は「EQ」（=）と「NEQ」（!=）です。

      たとえば、「EQ」と「cn」を選択した場合は、付与したアクセス権が cn 属性に適用されます。「NEQ」と「cn」を選択した場合は、付与したアクセス権が cn 属性に適用されません。

5. 「**アクセス権限**」タブ・ページを選択して、権限を指定します。詳細は、C-4 ページの表 C-5 を参照してください。

6. 「**OK**」をクリックします。

Oracle Directory Manager を使用したエントリ・レベルのアクセス権の付与

Oracle Directory Manager を使用してエントリ・レベルのアクセス権を付与する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**、「**エントリ管理**」の順に展開します。次のいずれかの方法で展開します。

   - ナビゲータ・ペインで、エントリを選択して右側のペインにそのプロパティを表示します。
   - 右側のペインでエントリを検索して、そのエントリをダブルクリックし、「エントリ」ダイアログ・ボックスを開きます。

2. 「**ローカル・アクセス**」タブ・ページを選択して、14-27 ページの「Oracle Directory Manager を使用した ACP の変更」に示すように、「**構造型アクセス項目**」ボックスと「**コンテンツ・アクセス項目**」ボックスで、ローカル ACI を作成および編集します。

3. 変更後、「**適用**」をクリックします。

> **注意：** 入力した情報をディレクトリ・サーバーに送信するには、「**適用**」をクリックする必要があります。「適用」をクリックしないと、情報は Oracle Directory Manager のキャッシュに保持されるだけです。

例 : Oracle Directory Manager を使用した ACP の管理

この例では、Oracle Directory Manager を使用して、ACI を含めた新規 ACP を作成する方法を紹介します。大企業の管理者が、ユーザー・パスワードに対するアクセス権を制限して、比較はすべての人が可能に、読取りと変更は各パスワードの所有者（ユーザー）のみ可能に設定する場合の例です。

この例では、新しい ACP を作成し、その ACP に次の各権限を設定する 4 つの ACI を移入します。

- すべての人による `userpassword` 属性に対する制限付きアクセス権
- ユーザー本人による同一 `userpassword` 属性への開かれたアクセス権
- すべての属性に対する開かれたアクセス権（すべての人による `userpassword` に対するアクセス権を除く）
- すべての人へのすべての属性に対する開かれたアクセス権

新規 ACP の作成

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開します。
2. 「**アクセス制御管理**」を選択します。ACP のリストが右側のペインに表示されます。
3. 右側のペインの下の「**作成**」ボタンをクリックします。「新規アクセス制御ポイント」ダイアログ・ボックスが表示されます。
4. 「**エントリへのパス**」フィールドで、ACP に指定する識別名を入力します。ACP 内の ACI は、すべての下位エントリ（その識別名も含めて）に適用されます。

構造型アクセス項目の構成 エントリに対するアクセス権を設定する手順は次のとおりです。

1. 「**構造型アクセス項目**」ボックスの下の「**作成**」をクリックします。「構造型アクセス項目」ダイアログ・ボックスが表示されます。このダイアログ・ボックスには、「**エントリ・フィルタ**」、「**追加されたオブジェクト・フィルタ**」、「**責任者**」および「**アクセス権限**」のタブがあります。

   ACP のすべての下位エントリに ACI を適用するため、「**エントリ・フィルタ**」タブ・ページは使用しません。

2. 「**追加されたオブジェクト・フィルタ**」タブ・ページを選択します。

   ACI を指定して、ユーザーが追加できるエントリの種類を制限できます。たとえば、ユーザーが `objectclass=country` を持つエントリのみを追加できるように、DSE ルート・エントリで ACI を指定できます。その後、ディレクトリ・サーバーによって、新規エントリがこのフィルタの制限に適合するかどうかが検証されます。

   ユーザーが追加できるエントリの種類を制限する手順は、次のとおりです。

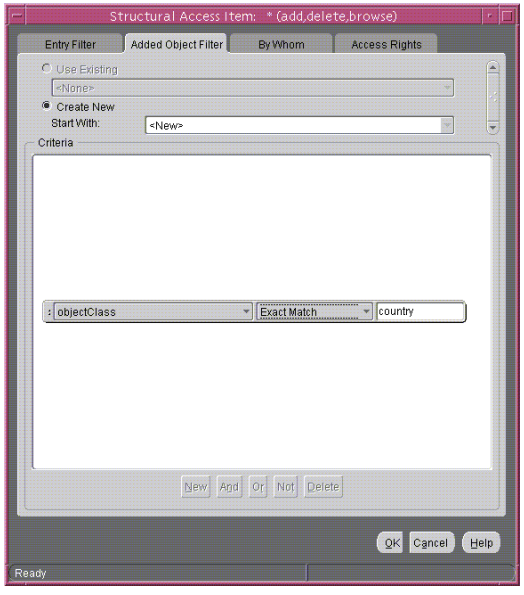
   a. 検索基準バーの一番左のメニューから、`objectclass` 属性タイプを選択します。

   b. バーの中央のメニューから「**完全一致**」を選択します。

   c. 検索基準バーの右のテキスト・ボックスに、`country` を入力します。

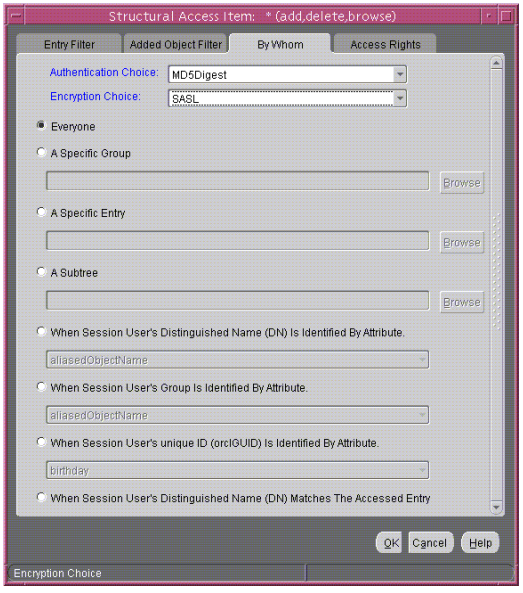
   ここで、「**追加されたオブジェクト・フィルタ**」タブ・ページは、図 14-1 のようになります。

図 14-1 構造型アクセス項目：「追加されたオブジェクト・フィルタ」タブ・ページ



3. 「**責任者**」タブ・ページを選択します。
   a. 「**認証の選択**」リストから、「**MD5 ダイジェスト**」を選択します。
   b. 「**暗号化の選択**」リストから、「**SASL**」を選択します。
   c. すべての人に対するアクセス権を作成するには、「**すべての人**」を選択します。「**責任者**」タブ・ページは、図 14-2 のようになります。

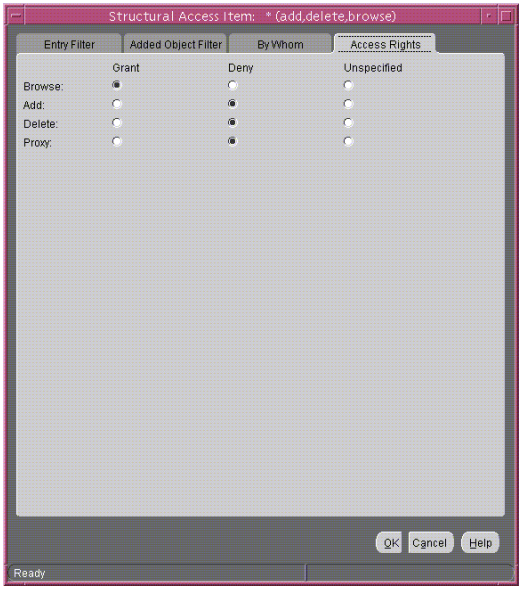
図 14-2 構造型アクセス項目：「責任者」タブ・ページ



4. 「**アクセス権限**」タブ・ページを選択します。デフォルトでは、すべての権限（「参照」、「追加」および「削除」）が付与されています。「プロキシ」は指定されません。

   a. すべての人が全エントリを参照でき、追加や削除はできないようにアクセス権を変更します。「**アクセス権限**」タブ・ページは、図 14-3 のようになります。

図 14-3 例 : 構造型アクセス項目 :「アクセス権限」タブ・ページ



   b. 「**OK**」をクリックします。

コンテンツ・アクセス項目の構成 この例の 4 つの ACI では、同じ構造型アクセス項目情報を使用します。これらは、許可するコンテンツ・アクセスのみが異なります。次に、ACI のコンテンツ・アクセスを作成する方法を説明します。

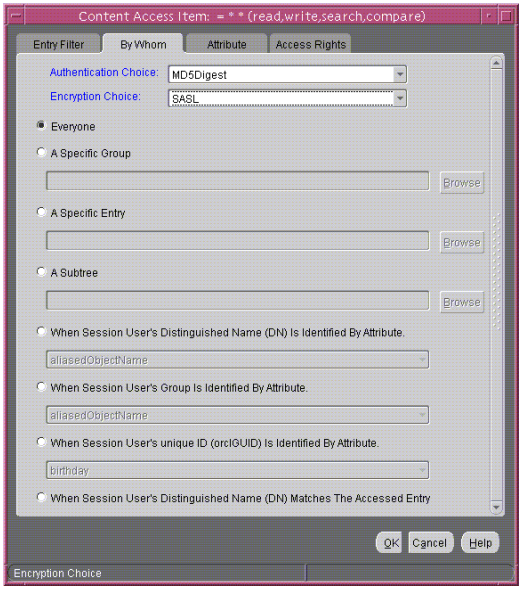
コンテンツ・アクセス項目を定義する手順は、次のとおりです。

1. 「**コンテンツ・アクセス項目**」ボックスの下の「**作成**」をクリックします。「コンテンツ・アクセス項目」ダイアログ・ボックスが表示されます。

   ACP のすべての下位エントリにこの ACI を適用するため、「**エントリ・フィルタ**」タブ・ページは使用しません。

2. 「**責任者**」タブ・ページを選択します。
   a. 「**認証の選択**」リストから、「**MD5 ダイジェスト**」を選択します。
   b. 「**暗号化の選択**」リストから、「**SASL**」を選択します。
   c. すべての人に対するアクセス権を作成するには、「**すべての人**」を選択します。「**責任者**」タブ・ページは、図 14-4 のようになります。

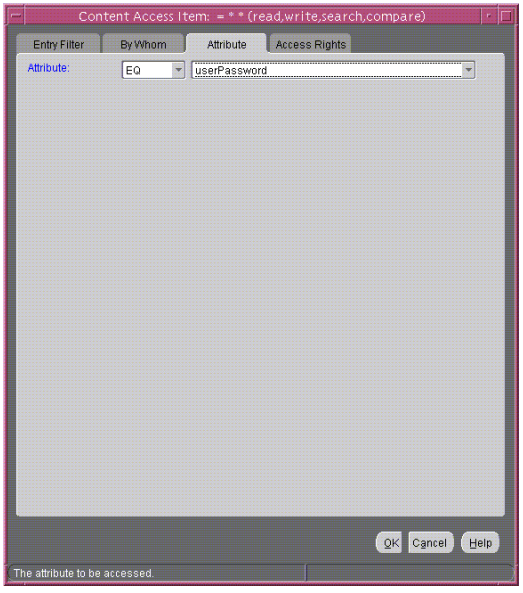
図 14-4 コンテンツ・アクセス項目：「責任者」タブ・ページ



3. 「**属性**」タブ・ページを選択します。このページには 2 つのフィールドがあります。最初のフィールドの選択肢は、「**EQ**」（等価）と「**NEQ**」（非等価）です。2 番目には、属性を設定します。

   「**EQ**」を選択して、「**`userPassword`**」を選択します。「**属性**」タブ・ページは、図 14-5 のようになります。

図 14-5 コンテンツ・アクセス項目：「属性」タブ・ページ



4. 「**アクセス権限**」タブ・ページを選択します。デフォルトでは、すべての権限が付与されています。読取り、検索、書込みおよび比較を否認するように権限を変更します。「**アクセス権限**」タブ・ページは、図 14-6 のようになります。

図 14-6 コンテンツ・アクセス項目：「アクセス権限」タブ・ページ

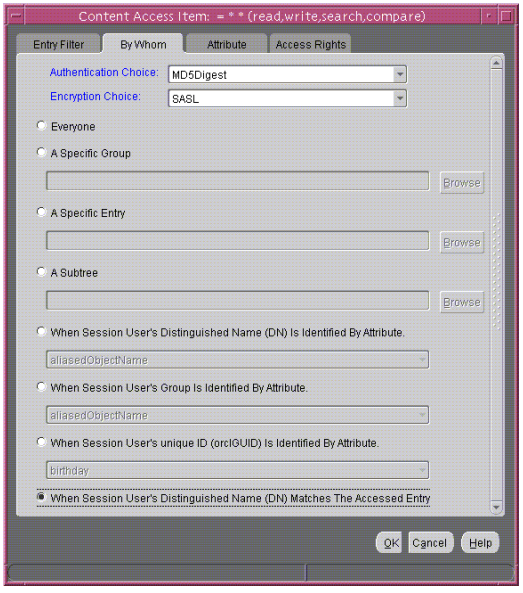
5. 「**OK**」をクリックします。

これで 1 番目の ACI の設定は完了です。

2 番目の ACI の作成 ユーザーに、本人のパスワードの読取り、書込み、検索および比較を許可する 2 番目の ACI を作成します。

1. 「**コンテンツ・アクセス項目**」ボックスの下の「**作成**」をクリックします。「コンテンツ・アクセス項目」ダイアログ・ボックスが表示されます。
2. 「**責任者**」タブ・ページを選択します。
   a. 「**認証の選択**」リストから、「**MD5 ダイジェスト**」を選択します。
   b. 「**暗号化の選択**」リストから、「**SASL**」を選択します。
   c. すべての人のアクセス権限を作成するには、「**セッション・ユーザーの識別名 (DN) がアクセス・エントリと一致する場合。**」を選択します。「責任者」タブ・ページは、図 14-7 のようになります。

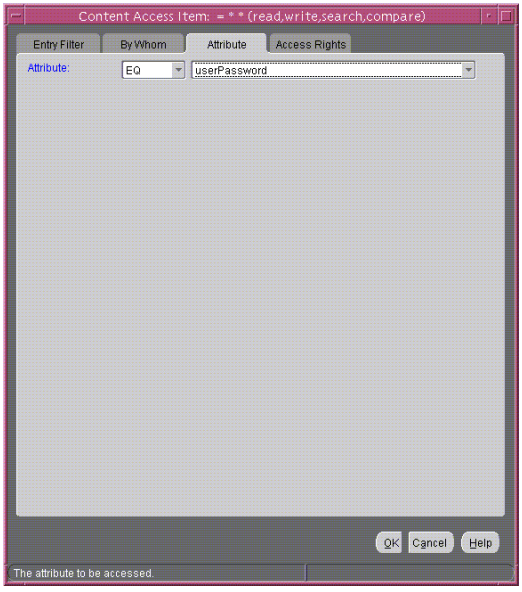
図 14-7 コンテンツ・アクセス項目：「責任者」タブ・ページ



3. 「**属性**」タブ・ページを選択します。このタブ・ページには、2 つのリストがあります。最初のリストの選択肢は、「**EQ**」（等価）と「**NEQ**」（非等価）です。2 番目には、属性を設定します。

   「**EQ**」と「**userPassword**」を選択します。「**属性**」タブ・ページは、図 14-8 のようになります。

図 14-8 コンテンツ・アクセス項目：「属性」タブ・ページ



4. 「**アクセス権限**」タブ・ページを選択します。

   読取り、検索、書込みおよび比較の各アクセス権を付与します。「自己書込み」は未指定のままにします。「**アクセス権限**」タブ・ページは、図 14-9 のようになります。

図 14-9 コンテンツ・アクセス項目：「アクセス権限」タブ・ページ

5. 「**OK**」をクリックします。

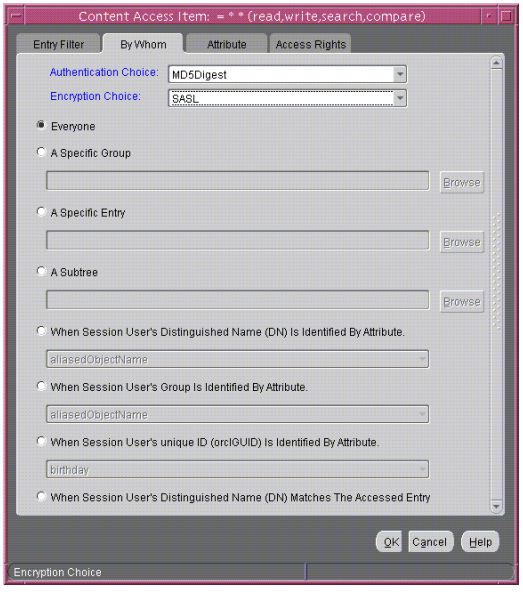
これで 2 つの ACI が作成されました。1 番目の ACI は、`userPassword` 属性の読取り、検索、書込みおよび比較の各アクセス権をすべての人に対して否認しています。2 番目の ACI は、パスワードの所有者に対して、その属性の読取り、検索、書込みおよび比較を許可しています

3 番目の ACI の作成

次の ACI は、userPassword を除くすべての属性の読取り、検索および比較の各アクセス権を、すべての人に付与します。書込みアクセス権は否認します。

1. 「**コンテンツ・アクセス項目**」ボックスの下の「**作成**」をクリックして、「コンテンツ・アクセス項目」ダイアログ・ボックスを表示します。
2. 「**責任者**」タブ・ページを選択します。
   a. 「**認証の選択**」リストから、「**MD5 ダイジェスト**」を選択します。
   b. 「**暗号化の選択**」リストから、「**SASL**」を選択します。
   c. すべての人に対するアクセス権を作成するには、「**すべての人**」を選択します。「**責任者**」タブ・ページは、図 14-10 のようになります。

図 14-10 コンテンツ・アクセス項目：「責任者」タブ・ページ

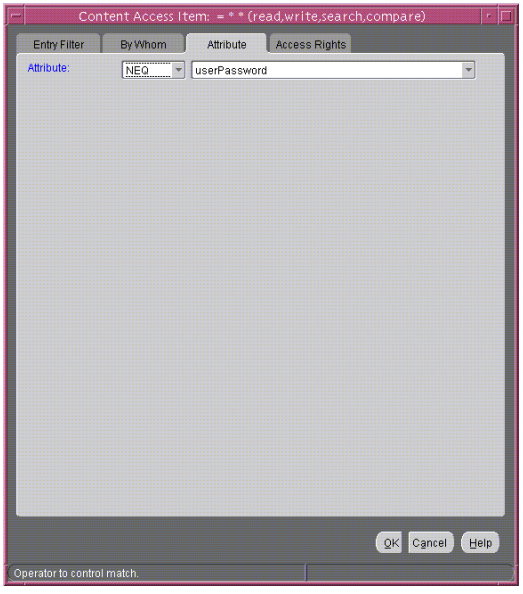


3. 「**属性**」タブ・ページを選択します。

   「**NEQ**」と「**userPassword**」を選択します。

   この組合せは、userpassword と等しくないあらゆる属性が、この ACI の権限の対象であることを示しています。「**属性**」タブ・ページは、図 14-11 のようになります。

図 14-11 コンテンツ・アクセス項目：「属性」タブ・ページ



4. 「**アクセス権限**」タブ・ページを選択します。

   読取り、検索および比較の各アクセス権を付与します。「書込み」アクセス権は否認します。「自己書込み」は未指定のままにします。「**アクセス権限**」タブ・ページは、図 14-12 のようになります。

図 14-12 コンテンツ・アクセス項目：「アクセス権限」タブ・ページ

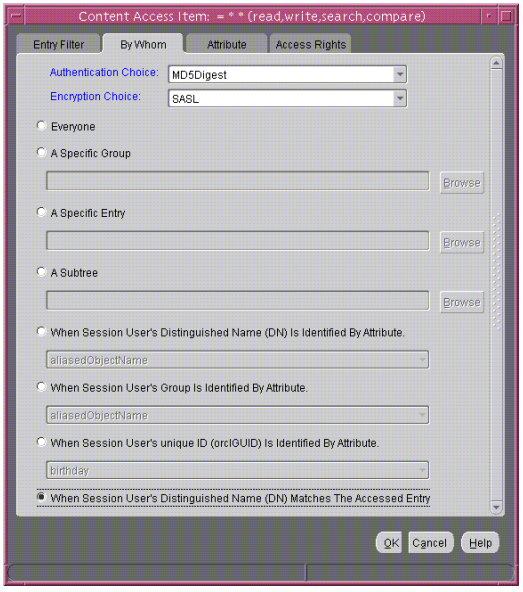
5. 「**OK**」をクリックしてこれらの権限を適用し、ダイアログ・ボックスを閉じます。

4 番目の ACI の作成

次の ACI は、userpassword を除くすべての属性の読取り、参照および書込みの各アクセス権を、その属性の所有者に付与します。この ACI を組み込むことによって、userPassword 以外の属性に対するアクセス権がその属性の所有者と他の人とで同じになるというあいまいさを排除できます。

1. 「**コンテンツ・アクセス項目**」ボックスの下の「**作成**」をクリックして、「コンテンツ・アクセス項目」ダイアログ・ボックスを表示します。
2. 「**責任者**」タブ・ページを選択します。
   a. 「**認証の選択**」リストから、「**MD5 ダイジェスト**」を選択します。
   b. 「**暗号化の選択**」リストから、「**SASL**」を選択します。
   c. すべての人のアクセス権限を作成するには、「**セッション・ユーザーの識別名 (DN) がアクセス・エントリと一致する場合。**」を選択します。「責任者」タブ・ページは、図 14-13 のようになります。

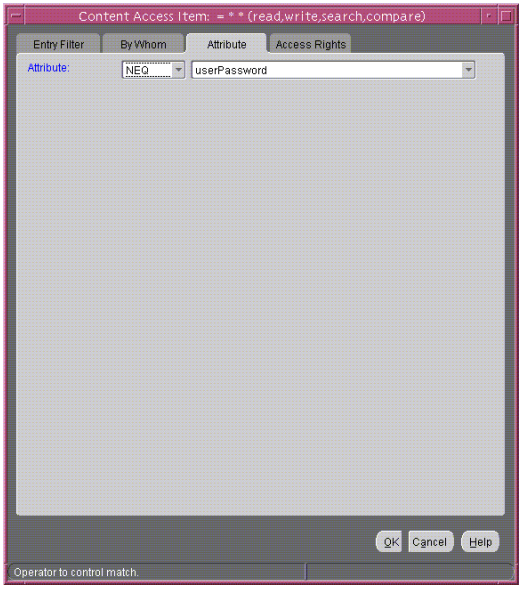
図 14-13 コンテンツ・アクセス項目：「責任者」タブ・ページ



3. 「**属性**」タブ・ページを選択します。

   リストから、「**NEQ**」と「**userPassword**」を選択します。この組合せは、userPassword 以外のすべての属性が、この ACI の権限の対象であることを示しています。「**属性**」タブ・ページは、図 14-14 のようになります。

図 14-14 コンテンツ・アクセス項目：「属性」タブ・ページ



4. 「**アクセス権限**」タブ・ページを選択します。

   読取り、検索および書込みの各アクセス権を付与します。「自己書込み」は未指定のままにします。「**アクセス権限**」タブ・ページは、図 14-15 のようになります。

図 14-15「アクセス権限」タブ・ページ

5. 「**OK**」をクリックしてこれらの権限を適用し、ダイアログ・ボックスを閉じます。

コマンドライン・ツールを使用したアクセス制御の管理

14-2 ページの「アクセス制御ポリシーの管理の概要」で説明したように、ディレクトリのアクセス制御ポリシーの情報は、ユーザーが変更可能な操作属性で表されます。したがって、ldapmodify を使用してこれらの属性の値を設定および変更して、ディレクトリのアクセス制御を管理できます。ldapmodify や ldapmodifymt などのツールがこのために使用できます。

付録 E「アクセス制御ディレクティブ書式」の説明に従って ACI を直接編集するには、ACI のディレクトリ表現の書式および構文を理解する必要があります。

関連項目：

- コマンドライン・モードのコマンドに必須の入力フォーマットである、**LDAP Data Interchange Format（LDIF）**を使用した入力ファイルのフォーマット方法は、A-2 ページの「LDAP Data Interchange Format（LDIF）の構文」を参照してください。
- ldapmodify の実行方法は、A-32 ページの「ldapmodify の構文」を参照してください。
- ACI の書式（構文）の詳細は、付録 E「アクセス制御ディレクティブ書式」を参照してください。

例 : ユーザーが追加できるエントリの種類の制限

ACI を指定して、ユーザーが追加できるエントリの種類を制限できます。たとえば、ユーザーが `objectclass=country` を持つエントリのみを追加できるように、DSE ルート・エントリで ACI を指定できます。追加できるエントリの種類を制限するには、`added_object_constraint` フィルタを使用します。その後、ディレクトリ・サーバーによって、新規エントリがこのフィルタの制限に適合するかどうかが検証されます。

次の制限を指定する例を示します。

- 対象 `cn=admin,c=us` は、`organization` エントリの下を参照、追加および削除できます。
- 対象 `cn=admin,c=us` は、`organization` エントリの下の `organizationalUnit` オブジェクトを追加できます。
- その他のすべては、`organization` エントリの下を参照できます。

```
access to entry filter=(objectclass=organization)
by group="cn=admin,c=us"
          constraintonaddedobject=(objectclass=organisationalunit)
          (browse,add,delete)
by * (browse)
```

例 : ldapmodify を使用した継承可能な ACP の設定

この例では、my_ldif_file という名前の LDIF ファイルを使用して、ルート DSE で orclACI にサブツリーのアクセス権を設定します。この例は orclACI 属性を参照しているため、このアクセス・ディレクティブはディレクトリ情報ツリーのエントリすべてを制御します。

```
ldapmodify -v -h $1 -D "cn=Directory Manager, o=IMC, c=US" -w "controller" -f my_
ldif_file
```

LDIF ファイル my_ldif_file は次のようになります。

```
dn:
changetype: modify
replace: orclaci
orclaci: access to entry
    by dn="cn=directory manager, o=IMC, c=us" (browse, add, delete)
    by * (browse, noadd, nodelete)
orclaci: access to attr=(*)
    by dn="cn=directory manager, o=IMC, c=us" (search, read, write, compare)
    by self (search, read, write, compare)
    by * (search, read, nowrite, nocompare)
```

例 : ldapmodify を使用したエントリ・レベルの ACI の設定

この例では、my_ldif_file という名前の LDIF ファイルを使用して、orclEntryLevelACI 属性にエントリ・レベルのアクセス権を設定します。この例は orclentrylevelACI 属性を参照しているため、このアクセス・ディレクティブは、それが常駐しているエントリのみを制御します。

```
ldapmodify -v -h myhost -D "cn=Directory Manager, o=IMC, c=US" -w "controller"
-f my_ldif_file
```

LDIF ファイル my_ldif_file は次のようになります。

```
dn:
changetype: modify
replace: orclentrylevelaci
orclentrylevelaci: access to entry
    by dn="cn=directory manager, o=IMC, c=us" (browse, add, delete)
    by * (browse, noadd, nodelete)
orclentrylevelaci: access to attr=(*)
    by dn="cn=directory manager, o=IMC, c=us" (search, read, write, compare)
    by * (search, read, nowrite, nocompare)
```

注意 : この例では、識別名の値が指定されていません。このことは、この ACI がルート DSE とその属性のみに関係していることを意味します。

例 : ワイルド・カードの使用方法

この例では、オブジェクトと対象指定子にワイルド・カード（*）を使用しています。acme.com ドメイン内のすべてのエントリに対して、すべてのユーザーが、すべての属性の読取り権限と検索権限およびすべてのエントリの参照権限を持つことになります。

dc=com の ACP 内の orclACI 属性

```
access to entry by * (browse)
access to attr=(*) by * (search, read)
```

属性の読取りを許可するには、エントリに参照権限を付与して、それらのエントリの属性に読取り権限を付与する必要があります。

例 : 識別名によるエントリの選択

この例では、2 つのアクセス・ディレクティブで識別名を使用してエントリを選択する際の正規表現の使用方法を示します。この例では、dc=acme, dc=com アクセス権より下位の address book 属性の読取り専用アクセス権を、すべての人に付与します。

dc=acme、dc=com の orclACI 属性

```
access to entry by * (browse)
access to attr=(cn, telephone, email) by * (search, read)
```

dc=us、dc=acme、dc=com の orclACI 属性

```
access to entry by * (browse)
access to attr=(*) by dn=".*,dc=us,dc=acme,dc=com" (search, read)
```

例 : 属性セレクタと対象セレクタの使用方法

この例では、特定の属性に対するアクセス権を付与する属性セレクタ、および様々な対象セレクタの使用方法を示します。この例は、dc=us、dc=acme、dc=com サブツリー内のエントリに適用されます。この ACI によって施行されるポリシーは次のとおりです。

- 管理者はサブツリー内のすべてのエントリに対する追加、削除および参照権限を所有しています。dc=us サブツリー内のその他のユーザーは、サブツリーの参照が可能ですが、サブツリー外部のユーザーはそのサブツリーにアクセスできません。
- salary 属性は、そのマネージャによる変更が可能で、本人は参照できます。その他のユーザーは salary 属性にアクセスできません。
- userPassword 属性は、パスワードの所有者と管理者による表示および変更が可能です。その他のユーザーは、この属性の比較のみ可能です。
- homePhone 属性は、本人による読取りおよび書込みが可能で、すべてのユーザーが参照できます。

- その他のすべての属性は、管理者のみ値の変更が可能です。その他のすべてのユーザーは、比較、検索、読取りは可能ですが、属性値の更新はできません。

dc=us、dc=acme、dc=com の orclACI 属性

```
access to entry
by dn="cn=admin, dc=us,dc=acme,dc=com" (browse, add, delete)
by dn=".*, dc=us,dc=acme,dc=com" (browse)
by * (none)


access to attr=(salary)
by dnattr=(manager) (read, write)
by self (read)
by * (none)


access to attr=(userPassword)
by self (search, read, write)
by dn="cn=admin, dc=us,dc=acme,dc=com" (search, read, write)
by * (compare)


access to attr=(homePhone)
by self (search, read, write)
by * (read)


access to attr != (salary, userPassword, homePhone)
by dn="cn=admin, dc=us,dc=acme,dc=com" (compare, search, read, write)
by * (compare, search, read)
```

例 : 読取り専用アクセス権の付与

この例では、dc=acme, dc=com より下位の address book 属性の読取り専用アクセス権を、すべての人に付与します。さらに、dc=us、dc=acme、dc=com サブツリー内のみのすべての属性に対する読取りアクセス権をすべての人に付与します。

dc=acme、dc=com の orclACI 属性

```
access to entry by * (browse)
access to attr=(cn, telephone, email) by * (search, read)
```

dc=us、dc=acme、dc=com の orclACI 属性

```
access to entry by * (browse)
access to attr=(*) by dn=".*,dc=us,dc=acme,dc=com" (search, read)
```

例 : グループ・エントリへの自己書込みアクセス権の付与

この例では、US ドメイン内のユーザーに、特定のグループ・エントリ（例 : mailing list）の member 属性に対して自分自身の名前（識別名）の追加または削除のみを行うアクセス権を許可します。

当該のグループ・エントリの orclEntryLevelACI 属性

```
access to attr=(member)
by dn=".*, dc=us,dc=acme,dc=com" (selfwrite)
```

15

Oracle Internet Directory のパスワード・ポリシー

この章では、パスワード・ポリシー（パスワードの使用方法を管理する規則のセット）について説明します。

この章では、次の項目について説明します。

- パスワード・ポリシーの概要
- パスワード・ポリシーの管理
- パスワード・ポリシーのエラー・メッセージ

パスワード・ポリシーの概要

この項では、次の項目について説明します。

パスワード・ポリシーとは

パスワード・ポリシーとは、パスワードの使用方法を管理する規則のセットです。たとえば、次のような規則を設定します。

- 指定されたパスワードの有効期限
- パスワードの最小必須文字数
- パスワードに必要な数字の文字数
- ユーザーによる定期的なパスワードの変更
- 以前使用したパスワードのユーザーによる再利用禁止
- 一定回数のログイン試行後のユーザーのロックアウト

デフォルトのパスワード・ポリシー

Oracle Internet Directory のデフォルトのパスワード・ポリシーは次のとおりです。

- パスワードの有効期限は 60 日とします。
- 10 回ログインに失敗すると、アカウントがロックアウトされます。スーパー・ユーザー・アカウントを除き、すべてのアカウントは、ディレクトリ管理者がパスワードを再設定するまで、24 時間ロックされたままになります。

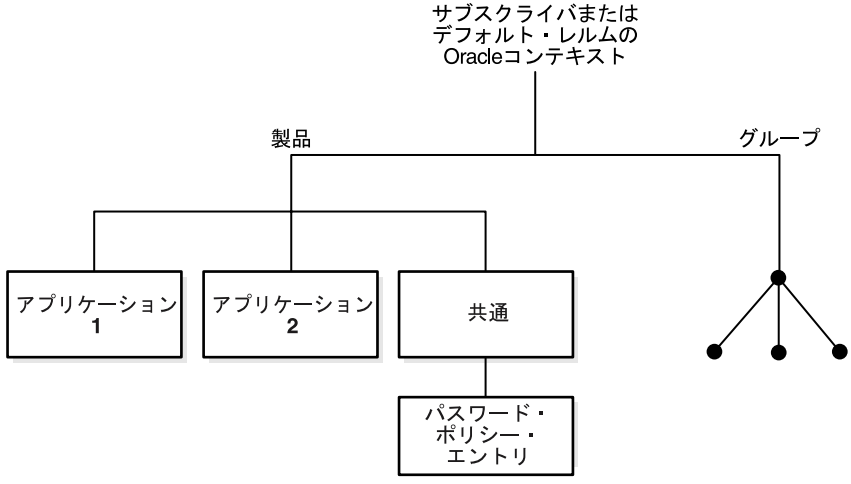
  スーパー・ユーザー・アカウントがロックされると、OID データベース・パスワード・ユーティリティを使用してロックを解除するまで、ロックされたままになります。このユーティリティでは、ODS ユーザー・パスワードの入力が要求されます。ODS パスワードを入力すると、アカウントのロックが解除されます。
- パスワードの最小文字数は 5 で、1 つ以上の数字を含める必要があります。
- パスワードの期限切れ後の猶予期間ログインは最大 3 とします。

Oracle Internet Directory リリース 9.0.4 からは、ルート Oracle コンテキストのパスワード・ポリシー・エントリがスーパー・ユーザーに適用されますが、アカウントのロックアウトを管理するパスワード・ポリシーのみがそのアカウントに施行されます。

Oracle Internet Directory のインストール時に、Oracle Universal Installer によって各認証管理レルムに対するパスワード・ポリシー・エントリが作成されます。このエントリには、このレルムのすべてのユーザーに適用できるすべてのパスワード・ポリシー情報が含まれます。

図 15-1 に示すように、このエントリは、製品エントリの下の共通エントリ直下に配置されます。この製品エントリは、認証管理レルムに固有の Oracle コンテキストの下にあります。

図 15-1 パスワード・ポリシー・エントリの位置



Oracle Internet Directory のパスワード・ポリシーは、シンプルなバインド（userpassword 属性に基づく）、userpassword 属性に対する比較操作および SASL バインドに適用され、SSL バインドおよびプロキシ・バインドには施行されません。

このパスワード・ポリシーを施行するには、レルム固有の Oracle コンテキストの共通エントリにある orclcommonusersearchbase 属性を適切な値に設定します。値を設定しなかった場合、パスワード・ポリシーの変更は有効になりません。

パスワード・ポリシー情報のディレクトリ・サーバー検証

ユーザー・パスワードが指定のポリシーの要件を満たしていることを確認する場合、ディレクトリ・サーバーは、次のことを検証します。

- パスワード・ポリシーが使用可能になっているかどうかの確認。この確認では、パスワード・ポリシー・エントリの orclpwdpolicyenable 属性の値がチェックされます。値 1 は、パスワード・ポリシーが使用可能になっていることを示します。値 0 は、パスワード・ポリシーが使用禁止になっていることを示します。
- パスワード・ポリシー構文情報（英数字の数、パスワード長など）の正確さ。ディレクトリ・サーバーは、ldapadd および ldapmodify の実行中に構文チェックを行います。
- パスワード・ポリシー状態情報。次に、その例を示します。
  - ユーザー・パスワードが作成または変更されたときのタイムスタンプ。
  - ユーザーが連続してログインに失敗したときのタイムスタンプ。
  - ユーザーのアカウントがロックされた日時。
  - パスワードが再設定されたため、最初の認証でユーザーがパスワードを変更する必要があることを示すインジケータ。
  - ユーザーが以前に使用したパスワードの履歴。
  - 猶予期間ログインのタイムスタンプ。

  ディレクトリ・サーバーは、ldapbind および ldapcompare の実行中に、状態情報をチェックしますが、このチェックは、orclpwdpolicyenable 属性が 1 に設定されている場合にのみ実行されます。

  パスワード値の構文チェックを使用可能にするには、パスワード・ポリシー・エントリの orclpwdpolicyenable および pwdchecksyntax 属性を TRUE に設定します。

概要 : 認証管理レルムに対するパスワード・ポリシーの設定

パスワード・ポリシーを設定する手順は、次のとおりです。

1. パスワード・ポリシー・エントリを作成し、それに pwdpolicy オブジェクト・クラスを関連付けてから、対応する属性を移入します。
2. pwdPolicy オブジェクト・クラスの値を設定します。このオブジェクト・クラスに、ディレクトリ全体のパスワード・ポリシー情報を格納します。この設定は、インストール中、このオブジェクト・クラスのエントリを作成するときに行います。
3. パスワード・ポリシー・エントリの orclpwdpolicyenable 属性が 1 に設定されていることを確認します。

関連項目： pwdPolicy オブジェクト・クラスの属性およびパスワード・ポリシーに関連する top オブジェクト・クラスのリストおよび説明は、B-25 ページの「パスワード・ポリシーのスキーマ要素」を参照してください。

パスワード・ポリシーの管理

この項では、次の項目について説明します。

- Oracle Directory Manager を使用したパスワード・ポリシーの管理
- コマンドライン・ツールを使用したパスワード・ポリシーの管理
- セルフ・サービス・コンソールを使用したパスワード・ポリシーの管理

表 15-1 に、パスワード・ポリシーに関連する管理タスク、各タスクの実行に使用するツールおよび対応する情報の参照先を示します。

表 15-1 パスワード・ポリシー管理のためのタスクおよびツール

タスク	ツール	参照先
アカウントの有効化と無効化	Oracle Internet Directory セルフ・サービス・コンソール ldapmodify	15-10 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用したアカウントの有効化と無効化」 15-8 ページの「例 : コマンドライン・ツールを使用したアカウントの有効化と無効化」
パスワードの強制変更	ldapmodify	15-9 ページの「例 : コマンドライン・ツールを使用したパスワードの強制変更」
認証管理レルムのパスワード・ポリシーの変更	Oracle Directory Manager ldapmodify	15-7 ページの「Oracle Directory Manager を使用した認証管理レルムのパスワード・ポリシーの変更」 15-8 ページの「例 : コマンドライン・ツールを使用した認証管理レルムのパスワード・ポリシーの変更」
パスワード・ポリシーの設定	ldapmodify	15-8 ページの「例 : コマンドライン・ツールを使用したパスワード・ポリシーの設定」

表 15-1 パスワード・ポリシー管理のためのタスクおよびツール（続き）

タスク	ツール	参照先
アカウントのロック解除	Oracle Internet Directory セルフ・サービス・コンソール ldapmodify	15-10 ページ「Oracle Internet Directory セルフ・サービス・コンソールを使用したアカウントのロック解除」 15-9 ページの「例 : コマンドライン・ツールを使用したアカウントのロック解除」
認証管理レルムのパスワード・ポリシーの表示	Oracle Directory Manager ldapsearch	15-6 ページの「Oracle Directory Manager を使用した認証管理レルムのパスワード・ポリシーの表示」 15-8 ページの「例 : コマンドライン・ツールを使用した認証管理レルムのパスワード・ポリシーの表示」

Oracle Directory Manager を使用したパスワード・ポリシーの管理

（Oracle Internet Directory のインストール時またはインストール後）認証管理レルムのベース・エントリを作成する場合は、そのレルムのパスワード・ポリシー・エントリも作成します。後で、Oracle Directory Manager を使用して、これらのポリシーを表示、更新および変更できます。

この項では、次の項目について説明します。

- Oracle Directory Manager を使用した認証管理レルムのパスワード・ポリシーの表示
- Oracle Directory Manager を使用した認証管理レルムのパスワード・ポリシーの変更

Oracle Directory Manager を使用した認証管理レルムのパスワード・ポリシーの表示

特定の認証管理レルムのパスワード・ポリシーを表示するには、ナビゲータ・ペインで「**Oracle Internet Directory サーバー**」、「**ディレクトリ・サーバー・インスタンス**」、「**パスワード・ポリシー管理**」の順に展開します。ナビゲータ・ペインに認証管理レルムのパスワード・ポリシー・エントリが表示されます。右側のペインに次の 2 つの列の表が表示されます。

- 「**パスワード・ポリシー・エントリへのパス**」列には、各パスワード・ポリシー・エントリの完全識別名がリストされます。
- 「**パスワード・ポリシー・エントリ**」列には、パスワード・ポリシーの対応する相対識別名がリストされます。

レルム固有のパスワード・ポリシーを最新の内容に更新するには、「**更新**」を選択します。

特定のレルムのパスワード・ポリシーを表示するには、ナビゲータ・ペインで、表示するレルム固有のパスワード・ポリシーを選択します。右側のペインにポリシーが表示されます。

> **関連項目：** Oracle Directory Manager で表示される各パスワード・ポリシーの説明は、C-6 ページの「Oracle Directory Manager のパスワード・ポリシーに関するフィールド」を参照してください。

Oracle Directory Manager を使用した認証管理レルムのパスワード・ポリシーの変更

特定の認証管理レルムのパスワード・ポリシーを変更する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「**ディレクトリ・サーバー・インスタンス**」、「**パスワード・ポリシー管理**」の順に展開します。
2. ナビゲータ・ペインで、変更するレルム固有のパスワード・ポリシーを選択します。対応するタブ・ページが、右側のペインに表示されます。
3. 必要に応じて、「**一般**」タブ・ページの編集可能な属性フィールドを変更します。フィールドについては、C-6 ページの表 C-8 を参照してください。
4. **アカウント・ロックアウト**のタブ・ページを選択した後、フィールドを変更する場合は「**グローバル・ロックアウト**」を選択します。必要に応じて、編集可能な属性フィールドを変更します。フィールドについては、C-7 ページの表 C-9 を参照してください。
5. 「**IP のロックアウト**」タブ・ページを選択した後、フィールドを変更する場合は「**IP のロックアウト**」を選択します。必要に応じて、編集可能な属性フィールドを変更します。フィールドについては、C-7 ページの表 C-10 を参照してください。
6. 「**パスワード構文**」タブ・ページを選択した後、フィールドを変更する場合は「**パスワード構文のチェック**」を選択します。必要に応じて、編集可能な属性フィールドを変更します。フィールドについては、C-8 ページの表 C-11 を参照してください。
7. 変更終了後、「**適用**」を選択します。

コマンドライン・ツールを使用したパスワード・ポリシーの管理

この項では、次の項目について説明します。

- 例 : コマンドライン・ツールを使用したパスワード・ポリシーの設定
- 例 : コマンドライン・ツールを使用した認証管理レルムのパスワード・ポリシーの管理
- 例 : コマンドライン・ツールを使用したアカウントの有効化と無効化
- 例 : コマンドライン・ツールを使用したアカウントのロック解除
- 例 : コマンドライン・ツールを使用したパスワードの強制変更

例 : コマンドライン・ツールを使用したパスワード・ポリシーの設定

次の例は、pwdLockout 属性を無効にして、その値をデフォルト設定（1）から変更します。

ファイル my_file.ldif の内容は、次のとおりです。

```
dn: cn=pwdpolicyentry,cn=common,cn=products,cn=OracleContext,o=my_company,dc=com
changetype:modify
replace: pwdlockout
pwdlockout: 0
```

次のコマンドでこのファイルをディレクトリにロードします。

```
ldapmodify -p 389 -h myhost -f my_file.ldif
```

例 : コマンドライン・ツールを使用した認証管理レルムのパスワード・ポリシーの管理

次に、コマンドライン・ツールを使用してレルムのパスワード・ポリシーを表示および変更する方法を示します。

例 : コマンドライン・ツールを使用した認証管理レルムのパスワード・ポリシーの表示 次の例は、特定のパスワード・ポリシー・エントリを取得します。

```
ldapsearch -p 389 -h my_host -b
"cn=pwdpolicyentry,cn=common,cn=products,cn=OracleContext,o=my_company,dc=com" -s
base "objectclass=*"
```

次の例は、すべてのパスワード・ポリシー・エントリを取得します。

```
ldapsearch -p 389 -h my_host -b "" -s sub "objectclass=pwdpolicy"
```

例 : コマンドライン・ツールを使用した認証管理レルムのパスワード・ポリシーの変更 次の例は、パスワード・ポリシー・エントリを変更します。

```
ldapmodify -p 389 -h my_host -v <<EOF
dn: cn=pwdpolicyentry,cn=common,cn=products,cn=OracleContext,o=my_company,dc=com
changetype: modify
replace: pwdMaxAge
pwdMaxAge: 100000
```

例 : コマンドライン・ツールを使用したアカウントの有効化と無効化

コマンドライン・ツールを使用して、ユーザー・アカウントを一時的に無効にし、その後再び有効にすることができます。

アカウントを永続的に無効にするには、orclisenabled 属性を DISABLED に設定します。この属性に他の値を設定すると、アカウントは有効になります。

アカウントを無効にした後、有効にするには、この属性をエントリから削除します。

特定の期間、アカウントを有効にするには、ユーザー・エントリ内の orclActiveStartDate および orclActiveEndDate 属性を、**UTC（Coordinated Universal Time）**書式による適切な値に設定します。たとえば、次のように入力します。

```
cn=John Doe,cn=users,o=my_company,dc=com
orclactivestartdate:20030101000000z
orclactiveenddate: 20031231000000z
```

この例で、John Doe は、2003 年 1 月 1 日から 2003 年 12 月 31 日までの期間ログインできます。2003 年 1 月 1 日より前、または 2003 年 12 月 31 日より後はログインできません。この期間 John Doe のアカウントを無効にする場合は、orclisenabled 属性を FALSE に設定する必要があります。

例 : コマンドライン・ツールを使用したアカウントのロック解除

セキュリティ管理者グループのメンバーの場合、アカウントがロックされると、ユーザーのパスワードを再設定せずに、アカウントのロックを解除できます。これによって、ユーザーに新規パスワードを明示的に知らせる必要がなくなります。ユーザーは、旧パスワードを使用してログインできます。

アカウントのロックを解除するには、orclpwdaccountunlock 属性を 1 に設定します。

次の例では、John Doe というユーザーのアカウントのロックを解除します。

```
ldapmodify -p port_number -h host_name -D cn=orcladmin -w welcome -v <<EOF
dn: cn=John Doe,cn=users,o=my_company,dc=com
changetype: modify
add: orclpwdaccountunlock
orclpwdaccountunlock: 1
```

例 : コマンドライン・ツールを使用したパスワードの強制変更

ユーザーが初めてログインする場合、ユーザーに対してパスワードの変更を強制できます。これを行うには、pwdpolicy エントリ内の pwdMustChange 属性を TRUE に設定し、パスワードを再設定します。この場合、ユーザーがログインしてパスワードを変更できるように、ユーザーに新しいパスワードを明示的に通知する必要があります。

> **関連項目 :** パスワードを再設定する方法については、15-11 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用したパスワードの再設定」を参照してください。

セルフ・サービス・コンソールを使用したパスワード・ポリシーの管理

この項では、次の項目について説明します。

- Oracle Internet Directory セルフ・サービス・コンソールを使用したアカウントの管理
- Oracle Internet Directory セルフ・サービス・コンソールを使用したアカウントの有効化と無効化
- Oracle Internet Directory セルフ・サービス・コンソールを使用したアカウントのロック解除
- Oracle Internet Directory セルフ・サービス・コンソールを使用したパスワードの再設定

Oracle Internet Directory セルフ・サービス・コンソールを使用したアカウントの管理

Oracle Internet Directory セルフ・サービス・コンソールを使用して、ユーザー・アカウントを有効または無効にしたり、ロック解除することができます。

Oracle Internet Directory セルフ・サービス・コンソールを使用したアカウントの有効化と無効化 Oracle Internet Directory セルフ・サービス・コンソールを使用して、ユーザー・アカウントを一時的に無効にし、その後再び有効にすることができます。

> **関連項目：** Oracle Internet Directory セルフ・サービス・コンソールを使用したアカウントの有効化および無効化の方法は、31-23 ページの「ユーザー・アカウントの有効化」および 31-23 ページの「ユーザー・アカウントの無効化」を参照してください。

Oracle Internet Directory セルフ・サービス・コンソールを使用したアカウントのロック解除
セキュリティ管理者グループのメンバーの場合、アカウントがロックされると、ユーザーのパスワードを再設定せずに、アカウントのロックを解除できます。これによって、ユーザーに新規パスワードを明示的に知らせる必要がなくなります。ユーザーは、旧パスワードを使用してログインできます。

> **関連項目：** Oracle Internet Directory セルフ・サービス・コンソールを使用してアカウントのロックを解除する方法は、31-23 ページの「ユーザー・アカウントのロック解除」を参照してください。

Oracle Internet Directory セルフ・サービス・コンソールを使用したパスワードの再設定

パスワードを忘れたり、アカウントがロックアウトされた場合は、パスワードを再設定できます。この場合、パスワード検証属性セットに値を入力して、サーバーに対して自己識別を行う必要があります。この操作は、以前回答を指定したパスワードのヒントの質問に答えるという形をとります。

> **関連項目：** Oracle Internet Directory セルフ・サービス・コンソールを使用してパスワードを再設定する方法は、31-8 ページの「パスワードを忘れた場合の再設定」を参照してください。

パスワード・ポリシーのエラー・メッセージ

パスワード・ポリシー違反が発生すると、ディレクトリ・サーバーはクライアントに様々なエラーおよび警告メッセージを送信します。Oracle Internet Directory10*g*（9.0.4）では、クライアントが ldapbind または ldapcompare 操作の一部としてパスワード・ポリシー・リクエスト・コントロールを送信する場合にのみ、ディレクトリ・サーバーはこれらのメッセージを LDAP コントロールとして送信できます。クライアントがリクエスト・コントロールを送信しない場合、ディレクトリ・サーバーは、レスポンス・コントロールを送信せず、追加情報の一部としてエラーおよび警告を送信します。

> **関連項目：** エラー・メッセージのリストおよびそれらのエラーを解決する方法は、I-9 ページの「パスワード・ポリシー違反のエラー・メッセージ」を参照してください。

16

パスワード・ベリファイアのディレクトリ格納

この章では、他の Oracle コンポーネントに対してユーザーを認証する場合に使用するパスワード・ベリファイアを Oracle Internet Directory で集中的に格納する方法について説明します。

この章では、次の項目について説明します。

ユーザー認証資格証明の集中格納の概要

退職または役職が変わったユーザーの権限は、その当日に変更して、古くなった未使用のアカウントや権限が誤使用されないようにする必要があります。ユーザー・アカウントとパスワードが複数のデータベースに分散される大企業では、パスワードが集中管理されていないと、管理者が万全なセキュリティに必要な速度で変更を実行できない可能性があります。

Oracle Internet Directory では、セキュリティ資格証明を集中的に格納して、エンド・ユーザーと管理者が簡単に管理できるようにします。このコンポーネントで格納される情報は、次のとおりです。

- ディレクトリ自体に対する認証ユーザーのパスワード
- その他の Oracle コンポーネントに対する認証ユーザーのパスワード・ベリファイア

Oracle 以外のアプリケーションがディレクトリ対応の場合、ユーザーは非 Oracle の認証資格証明を格納できます。これらのアプリケーションは、製品エントリの下に独自のコンテナを作成する必要があります。

Oracle Internet Directory に対する認証用パスワード・ベリファイアの格納および管理

Oracle Internet Directory では、ユーザーのディレクトリ・パスワードを `userPassword` 属性に格納します。Oracle Internet Directory でサポートされるハッシング・アルゴリズムの 1 つを使用して、パスワードを一方向ハッシュ値の BASE64 エンコーディング文字列で格納することで、このパスワードを保護できます。パスワードを暗号値ではなく一方向ハッシュ値として格納することによって、パスワードのセキュリティが向上します。これは、悪意のあるユーザーにはこれらの値を読むことも復号化することもできないためです。

Oracle Internet Directory リリース 9.0.4 からは、ユーザー・パスワードは、`orclrevpwd` という操作属性に可逆暗号化形式で格納されます。この属性は、パスワード・ポリシー・エントリの属性 `orclpwdencryptionenable` が `TRUE` に設定されている場合にのみ生成されます。`orclrevpwd` 属性は、SSL 一方向認証メカニズムおよび SSL 双方向認証メカニズムでのみ問合せが可能です。非 SSL セッションでは、この属性の問合せはできません。

この項では、次の項目について説明します。

- パスワード・ベリファイアおよびディレクトリに対する認証
- パスワード・ベリファイアを作成するためのハッシング・スキーム
- Oracle Directory Manager を使用したパスワード保護の管理
- ldapmodify を使用したパスワード保護の管理

パスワード・ベリファイアおよびディレクトリに対する認証

ディレクトリ・サーバーへの認証時、クライアントはパスワードをクリア・テキストでディレクトリ・サーバーに提供します。ディレクトリ・サーバーは、userpassword 属性に指定されているハッシング・アルゴリズムを使用して、このパスワードをハッシュします。次に、このハッシュされたパスワードをバインド・エントリの userPassword 属性に保存されているハッシュ済パスワードと照合します。ハッシュされたパスワードの値が一致した場合、サーバーはユーザーを認証します。ハッシュされたパスワードの値が一致しない場合、サーバーは「無効な資格証明」のエラー・メッセージをユーザーに送信します。

パスワード・ベリファイアを作成するためのハッシング・スキーム

インストール時に Oracle Universal Installer によって、ディレクトリに対するユーザーのパスワードを保護する一方向ハッシング・スキームの設定をユーザーに求めるプロンプトが表示されます。次のオプションがあります。

- **MD4**: 128 ビットのハッシュまたはメッセージ・ダイジェスト値を生成する一方向ハッシュ関数です。
- **MD5**: MD4 が改善された、より複合的なバージョンです。
- **SHA**: Secure Hash Algorithm。MD5 よりも長い 160 ビットのハッシュを生成します。このアルゴリズムは MD5 よりも若干速度が遅くなりますが、大きなメッセージ・ダイジェストによって、総当り攻撃や反転攻撃に対処できます。
- SSHA: Salted Secure Hash AlgorithmSHA と類似していますが、パスワードにランダムな salt 文字を使用して生成します。
- SMD5: Salted MD5.MD5 と類似していますが、パスワードにランダムな salt 文字を使用して生成します。
- **UNIX Crypt**: UNIX ハッシング・アルゴリズムです。

インストール時に指定するハッシング・アルゴリズムの値は、**ルート DSE** の orclCryptoScheme 属性に格納されます。その値を変更するには、Oracle Directory Manager または ldapmodify のいずれかを使用します。

Oracle Directory Manager を使用したパスワード保護の管理

Oracle Directory Manager を使用してパスワード保護を管理するには、スーパー・ユーザーである必要があります。

Oracle Directory Manager を使用してパスワード保護のタイプを変更する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」を展開して、パスワード・ハッシングをリセットするディレクトリ・サーバー・インスタンスを選択します。そのディレクトリ・サーバーに対応するタブ・ページが右側のペインに表示されます。

2. 「**システム操作属性**」タブ・ページの「**暗号化パスワード**」フィールドで、使用するパスワード保護のタイプを選択します。オプションは次のとおりです。
   - MD4
   - MD5
   - 暗号化なし
   - SHA
   - UNIX Crypt
   - SSHA
   - SMD5
3. 「**適用**」を選択します。

注意： 「暗号化なし」オプションを選択すると、ユーザー・パスワードがクリア・テキストで保存されます。

ldapmodify を使用したパスワード保護の管理

次の例は、my_ldif_file という名前の LDIF ファイルを使用してパスワード・ハッシング・アルゴリズムを SHA に変更します。

```
ldapmodify -D cn=orcladmin -w welcome -h myhost -p 389 -v -f my_ldif_file
```

LDIF ファイル my_ldif_file の内容は、次のとおりです。

```
dn:
changetype: modify
replace: orclcryptoscheme
orclcryptoscheme: SHA
```

関連項目： 12-8 ページの「ディレクトリ認証用ユーザー・パスワードの保護」

Oracle コンポーネントに対する認証用パスワード・ベリファイアの格納および管理

Oracle コンポーネントは、パスワードとパスワード・ベリファイアの両方を Oracle Internet Directory に格納します。この項では、次の項目について説明します。

Oracle コンポーネント用のパスワード・ベリファイアの概要

Oracle コンポーネントは、それぞれのコンポーネントのパスワード値をパスワード・ベリファイアとして Oracle Internet Directory に格納できます。パスワード・ベリファイアとは、クリア・テキストのパスワードをハッシュしたバージョンで、このバージョンは BASE64 エンコーディング文字列としてエンコードされます。

次のいずれかのハッシング・アルゴリズムを使用して、パスワード・ベリファイアを導出できます。

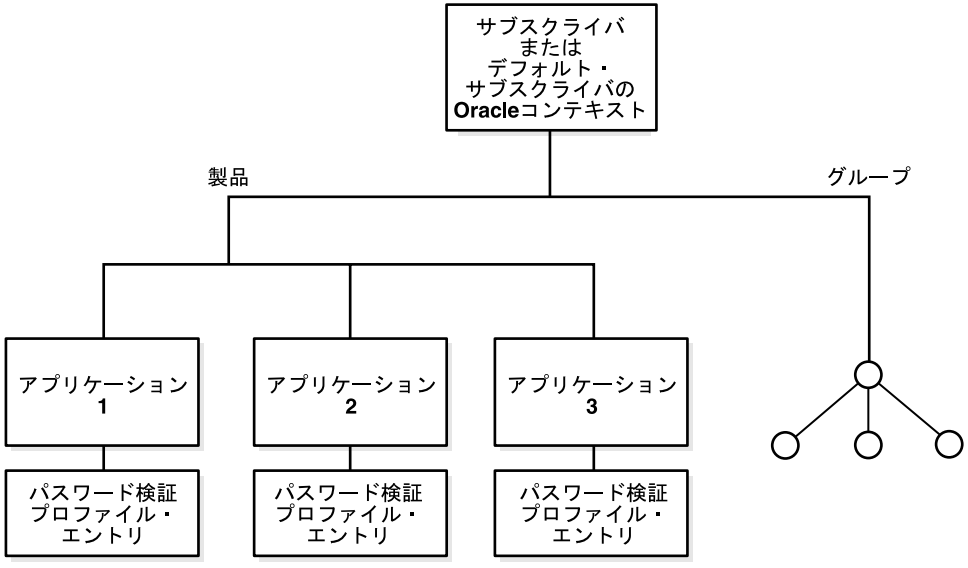
- **MD5**: MD4 が改善された、より複合的なバージョンです。
- **SHA**: Secure Hash Algorithm。**MD5** よりも長い 160 ビットのハッシュを生成します。このアルゴリズムは MD5 よりも若干速度が遅くなりますが、大きなメッセージ・ダイジェストによって、総当り攻撃や反転攻撃に対処できます。
- SSHA および SMD5
- **UNIX Crypt**: UNIX ハッシング・アルゴリズムです。
- SASL/MD5: Simple Authentication and Security Layer/MD5。接続ベースのプロトコルに認証サポートを追加し、要求 / 応答プロトコルを使用します。
- O3LOGON: ベリファイアを生成する Oracle 独自のアルゴリズムです。要求 / 応答プロトコルを使用する点で SASL/MD5 と似ています。
- ORCLWEBDAV: SASL/MD5 と同じ専用アルゴリズムで、`username@realm` の形式でユーザー名を取得します。

- ORCLLM: SMBLM アルゴリズムの Oracle 表現です。SMBLM アルゴリズムは、SMB/CIFS 要求 / 応答認証アルゴリズムの LM 改良型 Oracle 表現です。
- ORCLNT: SMBNT アルゴリズムの Oracle 表現です。SMBNT アルゴリズムは、SMB/CIFS 要求 / 応答認証アルゴリズムの NT 改良型 Oracle 表現です。

Oracle アプリケーションのインストール時に、Oracle Universal Installer は、そのアプリケーションに対して、必要なパスワード検証情報のすべてを含むパスワード検証プロファイル・エントリを作成します。16-6 ページの図 16-1 に示すように、このエントリは、レルム固有の Oracle コンテキストの下にある製品エントリ下のアプリケーション・エントリの直下に配置されます。

このベリファイア・プロファイル・エントリは、指定されたレルム内のユーザーのみに適用されます。ベリファイアの生成を適切に行うには、レルム固有の Oracle コンテキストの共通エントリの `orclcommonusersearchbase` 属性に適切な値を設定する必要があります。

図 16-1 パスワード検証プロファイル・エントリの位置



パスワード・ベリファイアを格納するための属性

ディレクトリと Oracle コンポーネントの両方とも、ユーザー・パスワードをユーザー・エントリに格納しますが、格納する属性は異なります。ディレクトリは、userPassword 属性にユーザー・パスワードを格納しますが、Oracle コンポーネントは、ユーザー・パスワード・ベリファイアを authPassword、orclPasswordVerifier または orclpassword 属性に格納します。Oracle コンポーネントで使用する各属性の説明は、表 16-1 を参照してください。

表 16-1 ユーザー・エントリにパスワード・ベリファイアを格納するための属性

属性	説明
authPassword	パスワードが、ディレクトリに対してユーザー認証を行うために使用するパスワード userpassword と同じ場合に、パスワードを Oracle コンポーネントに格納するための属性。この属性の値は、userpassword 属性の値と同期します。 複数の異なるアプリケーションで、ディレクトリに使用したクリア・テキスト・パスワードと同じパスワードの入力をユーザーに要求できます。ただし、各アプリケーションでは、異なるアルゴリズムを使用してそのパスワードがハッシュされる場合があります。この場合は、同じクリア・テキスト・パスワードが、複数の異なるパスワード・ベリファイアのソースとなります。 この属性は複数値の属性であるため、異なるアプリケーションがこのユーザーのクリア・テキスト・パスワードに対して使用する他のすべてのベリファイアを格納できます。userpassword 属性を変更すると、すべてのアプリケーションの authpasswords が再生成されます。
orclPasswordVerifier	パスワードが、ディレクトリに対してユーザー認証を行うために使用するパスワード userpassword と異なる場合に、パスワードを Oracle コンポーネントに格納するための属性。この属性の値は、userpassword 属性の値とは同期しません。 authPassword と同様に、この属性は複数値の属性であるため、異なるアプリケーションがこのユーザーのクリア・テキスト・パスワードに対して使用する他のすべてのベリファイアを格納できます。

表 16-1 ユーザー・エントリにパスワード・ベリファイアを格納するための属性（続き）

属性	説明
orclPassword	エンタープライズ・ユーザー用の 03LOGON ベリファイアのみを格納するための属性。03LOGON ベリファイアは、userpassword 属性と同期し、デフォルトでは、orcluserv2 オブジェクト・クラスに関連付けられたすべてのユーザー・エントリに対して生成されます。 Oracle Internet Directory をインストールすると、デフォルトではルート Oracle コンテキストにデータベース・セキュリティ・プロファイルのエントリが作成されます。このエントリの存在によって、orcluserv2 オブジェクト・クラスに関連付けられたユーザー・エントリを対象とする 03LOGON ベリファイアが生成されます。

これらの属性の型には、属性サブタイプとして appID があります。この属性サブタイプで特定のアプリケーションを一意に識別します。たとえば、appID はアプリケーション・エントリの ORCLGUID にできます。この属性サブタイプは、アプリケーションのインストール時に生成されます。

16-9 ページの図 16-2 では、様々な Oracle コンポーネントがそれぞれのパスワード・ベリファイアを Oracle Internet Directory に格納しています。Oracle Application Server Single Sign-On では、ディレクトリに対するパスワードと同じパスワードを使用するため、パスワードは authPassword 属性に格納されます。その他のアプリケーションでは、ディレクトリに対するパスワードとは異なるパスワードを使用するため、それぞれのベリファイアが orclPasswordVerifier 属性に格納されます。

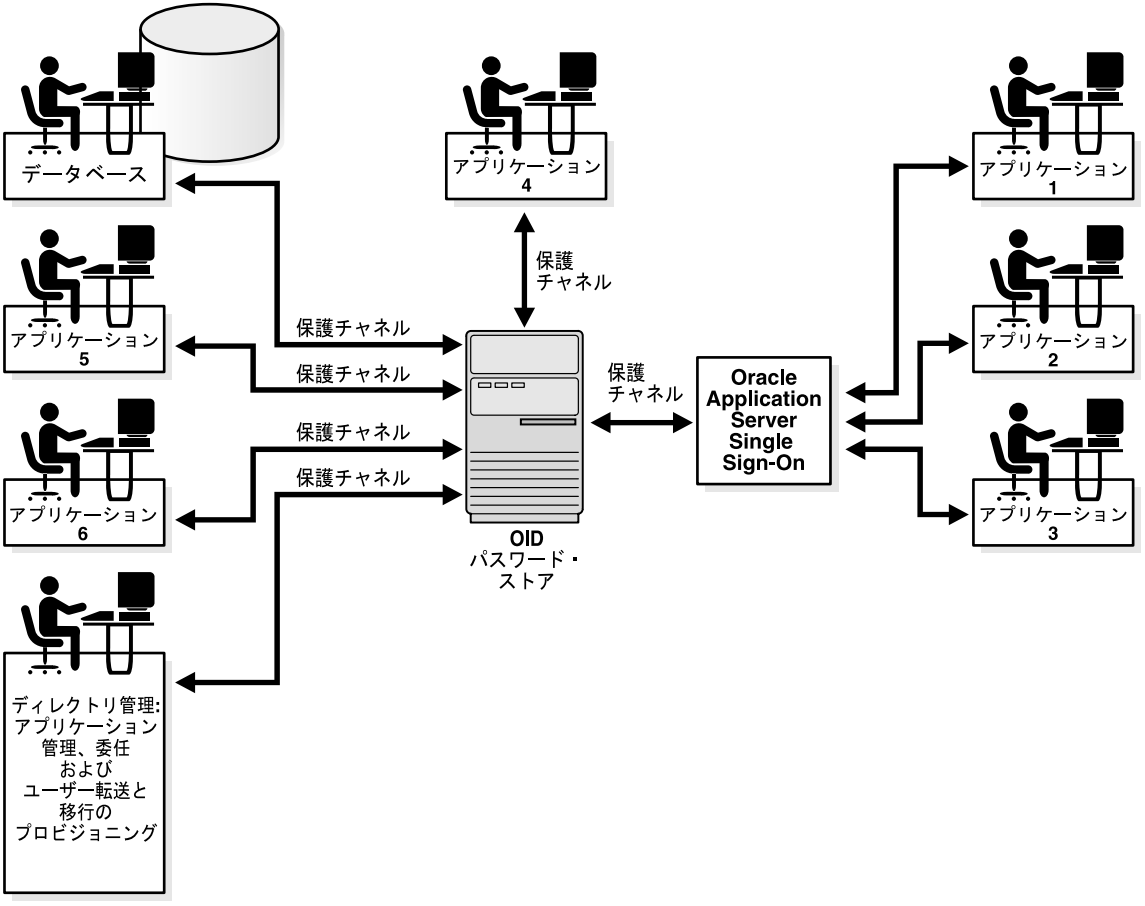
次の記述は、アプリケーション・ベリファイア・プロファイルの例です。

```
dn: cn=IFSVerifierProfileEntry,cn=IFS,cn=Products,cn=OracleContext,o=Oracle,dc=com
objectclass:top
objectclass:orclpwdverifierprofile
cn:IFSVerifierProfileEntry
orclappid:8FF2DFD8203519C0E034080020C34C50
orclpwdverifierparams;authpassword: crypto:SASL/MDS $ realm:dc=com
orclpwdverifierparams;orclpasswordverifier: crypto:ORCLLM
orclpwdverifierparams;authpassword: crypto:ORCLWEBDAV $ realm:dc=com
    $ usernameattribute: mail
    $ usernamecase: lower
    $ nodomain: TRUE
```

SASL/MD5 および ORCLWEBDAV ベリファイアは、ユーザー名、レルムおよびパスワードを使用して生成されます。使用するユーザー名属性は、ベリファイア・プロファイル・エントリで指定できます。ユーザー名は大文字でも小文字でも指定できます。ORLWEBDAV ベリファイアは、ユーザー名に認証管理レルムの名前を付加して生成されます。レルムの名前を付加して生成する必要がない場合、ベリファイア・プロファイル・エントリでは `nodomain: TRUE` を指定する必要があります。

前述の例では、ORCLWEBDAV ベリファイアは、レルムの名前を付加せずに `mail` 属性の値を使用して生成されます。また、ユーザー名はベリファイアが生成される前に小文字に変換されます。

図 16-2 認証モデル



Oracle コンポーネントのデフォルトのベリファイア

各 Oracle コンポーネントのプロファイルを作成する必要をなくし、すべてのコンポーネントでパスワード・ベリファイアを共有できるようにするために、Oracle Internet Directory にはパスワード・ベリファイアのデフォルト・セットが用意されています。デフォルトのベリファイアには、MD5、MD5-IFS（ユーザー名がニックネーム属性の値に設定され、レルムが Authorized_Users に設定された SASL/MD5）、WEBDAV、ORCLLM および ORCLNT のタイプがあります。

2 つのプロファイル・エントリが必要です。1 つは数値のみを使用する個人識別番号（PIN）を使用するアプリケーション用、もう 1 つは英数字のパスワードを使用するアプリケーション用です。

PIN ベースのアプリケーション用ベリファイア（たとえば、Oracle9*i* AS Unified Messaging のボイス・メール）は、`orclpasswordverifier` 属性に格納されます。英数字パスワード・ベースのアプリケーション用ベリファイア（たとえば、Oracle Internet File System）は、次のいずれかに格納されます。

- `authpassword` 属性 : アプリケーションがそのベリファイアと `userpassword` 属性を同期する必要がある場合
- `orclpasswordverifier` 属性 : `userpassword` 属性との同期が必要ない場合

これらのプロファイル・エントリには、サブスクライブ・アプリケーションのリストも含まれ、これらのアプリケーションは、プロファイル・エントリ内で `uniquemember` 属性の値として指定されます。デフォルトでは、Oracle Application Server Single Sign-On 識別情報の DN がサブスクライブ・アプリケーションの 1 つになっています。これは、Oracle Application Server Single Sign-On が、すべてのパートナ・アプリケーションのプロキシ・メンバーであることを示しています。Oracle Application Server Single Sign-On に基づいていないすべてのアプリケーションで、適切なプロファイル・エントリ内の `uniquemember` 属性に識別子（DN）を追加する必要があります。

次に、プロファイル・エントリの例を示します。

```
Cn=defaultSharedPwdProfileEntry, cn=common, cn=products, cn=oraclecontext
Objectclass: orclpwdverifierprofile
Cn: orclcommonpwdprofileentry
Orclappid: orclcommonpwd
Orclpwdverifierparams;authpassword: crypto:SASL/MD5 $ realm:Authorized_Users
Orclpwdverifierparams;authpassword: crypto:ORCLWEBDAV $ realm:Authorized_Users
Orclpwdverifierparams;authpassword: crypto:ORCLLM
Orclpwdverifierparams;authpassword: crypto:ORCLNT
Orclpwdverifierparams;orclpasswordverifier: crypto:SSHA
Uniquemember: cn=SSO,cn=Products,cn=OracleContext
Uniquemember: cn=IFS,cn=Products,cn=OracleContext

Cn=defaultSharedPINProfileEntry, cn=common, cn=products, cn=oraclecontext
Objectclass: orclpwdverifierprofile
Cn: orclcommonpinprofileentry
```

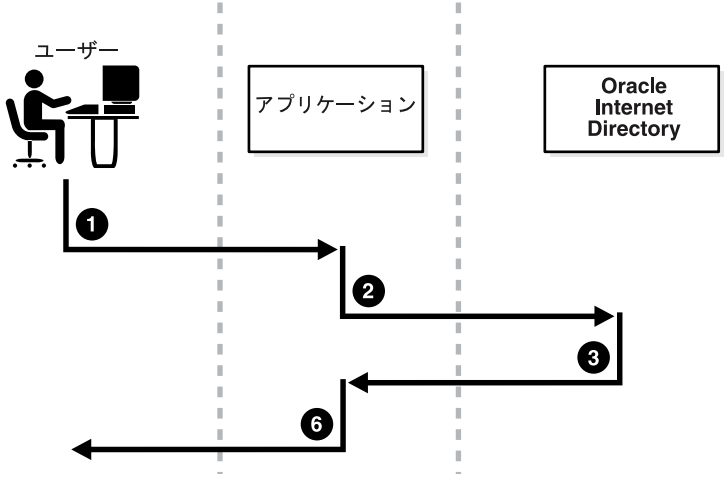
```
Orclappid: orclcommonpin
Orclpwdverifierparams;orclpasswordverifier: crypto:MD5
Orclpwdverifierparams;orclpasswordverifier: crypto:SSHA
Uniquemember: cn=SSO,cn=Products,cn=OracleContext
Uniquemember: cn=Unified Messaging,cn=Products,cn=OracleContext
```

PIN ベースのアプリケーションでは、`authpassword` はオプションではありません。`orclpasswordverifier` 属性が使用されます。

例 : Oracle コンポーネントに対するパスワード検証の動作

図 16-3 に、Oracle コンポーネントに対するパスワード検証の例を示します。この例の Oracle コンポーネントは、パスワード・ベリファイアをディレクトリに格納します。

図 16-3 パスワード検証の動作



1. ユーザーは、ユーザー名とクリア・テキスト・パスワードを入力して、アプリケーションへのログインを試みます。
2. アプリケーションは、クリア・テキスト・パスワードをディレクトリ・サーバーに送信します。アプリケーションは、パスワード・ベリファイアをディレクトリに格納した後、ディレクトリ・サーバーに対して、このパスワード値をディレクトリ内の対応するベリファイアと比較するように要求します。

3. ディレクトリ・サーバーは、次のように動作します。
   a. 特定のアプリケーションに指定されているハッシング・アルゴリズムを使用して、パスワード・ベリファイアを生成します。
   b. 次に、生成したパスワード・ベリファイアをディレクトリ内の対応するパスワード・ベリファイアと比較します。比較操作が成功した場合、アプリケーションは、ベリファイア属性のサブタイプとしてその appID を指定する必要があります。たとえば、次のようにします。

      ldapcompare -p389 -D "*DN_of_the_appplication_entity*" -w "*password*" -b "*DN_of_the_user*" -a orclpasswordverifier; *appID* -v *password_of_the_user*

   c. 比較操作の結果をアプリケーションに通知します。
4. アプリケーションは、ディレクトリ・サーバーからのメッセージに従って、ユーザーを認証または否認します。

アプリケーションは、比較操作を使用しない場合、次のように動作します。

1. ユーザーが入力したクリア・テキスト・パスワードをハッシュします。
2. ユーザーが入力したクリア・テキスト・パスワードのハッシュ値をディレクトリから取り出します。
3. クライアントが応答するユーザーへの要求を開始します。応答が適切な場合、アプリケーションはユーザーを認証します。

Oracle Directory Manager を使用した Oracle コンポーネント用パスワード検証プロファイルの管理

Oracle Directory Manager を使用して、パスワード検証プロファイル・エントリを表示および変更できます。

Oracle Directory Manager を使用した Oracle コンポーネント用パスワード検証プロファイルの表示と変更

アプリケーションのパスワード・ベリファイアを表示する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開します。
2. 「**パスワード検証管理**」を選択します。右側のペインに次の 2 つの列が表示されます。
   - 「**パスワード検証エントリへのパス**」列には、各パスワード検証プロファイル・エントリの完全識別名がリストされます。
   - 「**パスワード検証エントリ**」列には、各パスワード検証プロファイル・エントリの対応する相対識別名がリストされます。

3. 表示するパスワード・ベリファイアを選択します。選択したパスワード・ベリファイアが「パスワード検証プロファイル」ダイアログ・ボックスに表示されます。このダイアログ・ボックスのフィールドの説明は、C-8 ページの表 C-12 を参照してください。
4. パスワード・ベリファイアの生成に使用するハッシング・アルゴリズムを「パスワード検証プロファイル」ダイアログ・ボックスで変更するには、「**Oracle パスワード・パラメータ**」フィールドに新しい値を入力します。

コマンドライン・ツールを使用した Oracle コンポーネント用パスワード検証プロファイルの管理

コマンドライン・ツールを使用して、パスワード・ベリファイア・プロファイルを表示および変更できます。

コマンドライン・ツールを使用したパスワード検証プロファイルの表示

アプリケーションのパスワード・ベリファイアを表示するには、パスワード検証プロファイルの識別名を指定して検索を実行します。

例 : コマンドライン・ツールを使用したパスワード検証プロファイルの変更

この例では、アプリケーションのパスワード検証プロファイル・エントリのハッシング・アルゴリズムを変更します。このパスワード・ベリファイアは、ユーザーのディレクトリ・パスワードと同期しています。

```
ldapmodify -p 389 -h my_host -v <<EOF
dn: cn=MyAppVerifierProfileEntry,cn=MyApp,cn=Products,cn=OracleContext,o=my_
company,dc=com
changetype: modify
replace: orclPwdVerifierParams
orclPwdVerifierParams;authPassword: crypto:SASL/MD5 $ realm:dc=com
EOF
```

17

Oracle テクノロジ配置のための権限の委任

この章では、ユーザー、グループおよびサービスに関するすべてのデータを 1 つのリポジトリに格納する方法、およびこれらのデータの管理を複数の管理者に委任する方法について説明します。また、Oracle Internet Directory でのデフォルトのセキュリティ構成についても説明します。

この章では、次の項目について説明します。

Oracle Identity Management モデルでの委任

Oracle Identity Management を使用すると、ユーザー、グループおよびサービスのすべてのデータを 1 つのリポジトリに格納し、各データ・セットに特定の管理者を割り当てることができます。Oracle Identity Management は、集中型のリポジトリとカスタマイズされた委任アクセスの両方を提供するため、安全でスケーラブルです。

この項では、次の項目について説明します。

委任の動作

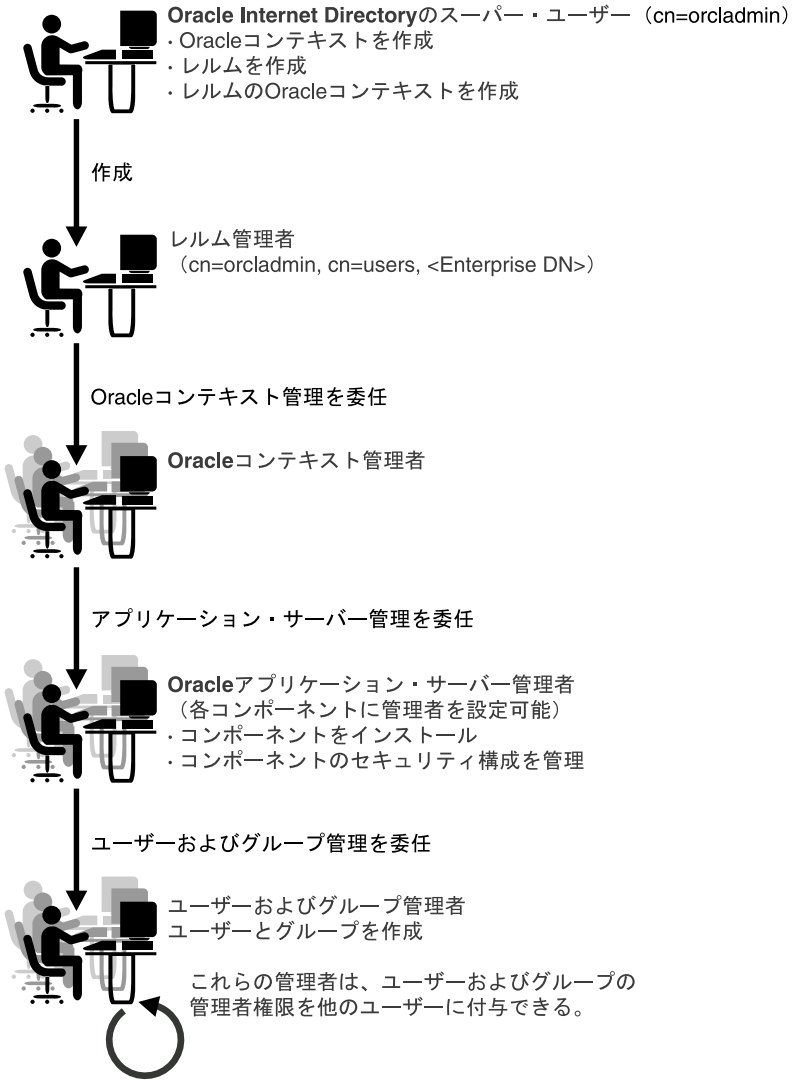
委任モデルを使用すると、グローバル管理者は、ホスティングされた企業の認証管理レルムを作成し、管理する権限をレルム管理者に委任できます。一方、レルム管理者は、アプリケーション用パスワード、個人データおよび作業環境を変更する権限をエンド・ユーザーおよびグループに委任できます。このようにして、各タイプのユーザーに、適切なレベルの権限を与えることができます。

必要な権限を委任するには、ユーザーを適切な管理グループに割り当てます。たとえば、エンタープライズ・ユーザーと電子メール・サービスに関するデータの両方をディレクトリに格納し、それぞれのデータ・セットに一意の管理者を割り当てる必要があるとします。ユーザーをエンタープライズ・ユーザーの管理者として指定するには、そのユーザーをエンタープライズ・ユーザー管理者グループなどに割り当てます。ユーザーを電子メール・サービスの管理者として指定するには、そのユーザーを電子メール・サービス管理者グループなどに割り当てます。

Oracle Application Server 環境での委任

図 17-1 に、Oracle Application Server 環境での委任の流れを示します。

図 17-1 Oracle Application Server 環境での委任の流れ



17-3 ページの図 17-1 に示すように、Oracle Application Server 環境では、ディレクトリのスーパー・ユーザーは次の項目を作成します。

- Oracle コンテキスト
- レルム
- レルム固有の Oracle コンテキスト
- レルム管理者用のエントリ

一方、レルム管理者は、Oracle コンテキスト管理者グループにユーザーを割り当てることで、Oracle コンテキストの管理を特定のユーザーに委任します。その後、Oracle コンテキスト管理者は、Oracle Application Server 管理者グループにユーザーを割り当てることで、Oracle Application Server の管理を 1 人以上のユーザーに委任します。これらの管理者は、Oracle Application Server コンポーネントをインストールおよび管理し、ユーザーやグループのデータ管理を他の管理者に委任します。この委任では、ユーザーおよびグループのデータ管理を他のユーザーに委任できます。

デフォルトの構成について

Oracle Internet Directory を初めてインストールすると、デフォルトの構成により、ディレクトリ情報ツリー（DIT）内の様々なポイントでアクセス制御ポリシーが確立されます。デフォルトのアクセス制御は、この章の後半で説明するとおり、ユーザーおよびグループのコンテナに配置されます。同様に、特定のディレクトリ・エンティティのデフォルトの権限についても、この章の後半で説明します。また、表 17-1 に示すように、特定のデフォルトの権限はすべての人および各ユーザーに付与されます。

表 17-1　すべての人および各ユーザーに付与されるデフォルトの権限

対象	デフォルトの権限
すべての人	ルート DSE での権限は次のとおりです。 ■ ユーザー・エントリを参照する権限 ■ userpkcs12、orcluserpkcs12hint、userpassword、orclpassword および orclpasswordverifier 以外のすべてのユーザー属性に対する検索、読取りおよび比較権限
各ユーザー	`userpassword`、`orclpassword` および `orclpasswordverifier` 属性を含む各ユーザー独自の属性に対する完全なアクセス権

企業のセキュリティ要件を満たすように、このデフォルト構成をカスタマイズできます。

概要 : Oracle テクノロジ・スタックの管理権限

表 17-2 に、Oracle テクノロジ・スタックの管理に必要な権限を示します。

表 17-2　Oracle テクノロジ・スタックの管理権限

必要な権限	説明	詳細情報の参照先
ユーザーおよびグループの管理権限	これらの権限は、認証管理インフラストラクチャを使用する Oracle コンポーネントまたはエンド・ユーザー自身のいずれかに委任されます。	17-6 ページの「ユーザーおよびグループの管理権限の委任」
配置時権限	この権限は、Oracle コンポーネントを配置するために必要です。ディレクトリ内部で適切なエントリを作成する権限や、共通リポジトリにメタデータを格納する権限を含む場合もあります。そのような権限は、OracleAS Portal 管理者などに与える必要があります。	17-12 ページの「Oracle コンポーネントの配置権限の委任」
実行時権限	この権限は、認証管理インフラストラクチャ内の Oracle コンポーネントの実行時の対話を円滑にするために必要な権限です。ユーザー属性の表示、新規ユーザーの追加、グループ・メンバーシップの変更のための権限が含まれます。そのような権限は、各 Oracle コンポーネントに固有な管理ツールが Oracle Internet Directory 内部でエントリにアクセスしたり、エントリを作成できるように、その管理ツールに対し与える必要があります。	17-15 ページの「コンポーネントの実行時権限の委任」

注意 : Oracle コンテキストでデフォルト ACL を変更する場合は注意が必要です。変更により、ご使用の環境内で Oracle コンポーネントのセキュリティが無効になることがあります。Oracle コンテキストでデフォルト ACL を安全に変更できるかどうかの詳細は、各コンポーネントのドキュメントを参照してください。

関連項目 : 既存のディレクトリ構造から Oracle Application Server 環境への移行を検討している場合は、23-9 ページの「デフォルトのディレクトリ構造への既存ディレクトリの移行」を参照してください。

ユーザーおよびグループの管理権限の委任

管理権限は、認証管理インフラストラクチャを使用する Oracle コンポーネントまたはエンド・ユーザー自身のいずれかに委任されます。権限は、識別情報（ユーザーやアプリケーションなど）、またはロールやグループに対して委任できます。

この項では、次の項目について説明します。

- ユーザーおよびグループのデータ管理権限の委任方法
- ユーザー・データを管理するためのデフォルトの権限
- グループ・データを管理するためのデフォルトの権限

ユーザーおよびグループのデータ管理権限の委任方法

管理権限を委任するには、Oracle Internet Directory スーパー・ユーザーは、次の作業を行います。

1. 認証管理レルムを作成します。
2. そのレルムでレルム管理者と呼ばれる特別なユーザーを識別します。
3. そのレルム管理者にすべての権限を委任します。

このレルム管理者は、Oracle 定義済ロール（Oracle Application Server 管理者など）に、Oracle コンポーネントが必要とする特定の権限を委任します。Oracle コンポーネントは、配置時にこれらのロールを受け取ります。

レルム管理者は、Oracle コンポーネント固有のロールに権限を委任する他に、配置に固有のロール（たとえば、ヘルプ・デスク管理者用のロール）を定義し、権限をこれらのロールに付与できます。委任された管理者は、これらのロールをさらにエンド・ユーザーに付与することができます。実際、ユーザー管理タスクの大部分はセルフ・サービス（電話番号の変更やアプリケーション固有の作業環境の指定など）に関係しているため、レルム管理者と Oracle コンポーネント管理者は、これらの権限をエンド・ユーザーに委任できます。

グループの場合、1 人以上の所有者（通常、エンド・ユーザー）を指定できます。これらの所有者に必要な管理権限が付与された場合、所有者は Oracle Internet Directory セルフ・サービス・コンソール、Oracle Directory Manager またはコマンドライン・ツールを使用してグループを管理できます。

ユーザー・データを管理するためのデフォルトの権限

ユーザーの管理には、次の権限が含まれます。

- ユーザー・エントリを作成および削除する権限
- ユーザー属性を変更する権限
- ユーザー管理を他のユーザーに委任する権限

ユーザーを作成するための**アクセス制御ポリシー・ポイント**（ACP）は、認証管理レルムのユーザー・コンテナにあります。

この項では、これらの権限について説明します。

レルムに対するユーザーの作成

レルムに対してユーザーを作成するには、管理者はサブスクライバ DAS ユーザー作成グループのメンバーである必要があります。表 17-3 に、このグループの特性を示します。

表 17-3　サブスクライバ DAS ユーザー作成グループの特性

特性	説明
デフォルト ACP	デフォルトのレルムのユーザー・コンテナにある ACL により、レルムの Oracle コンテキストのサブスクライバ DAS ユーザー作成グループは、ユーザー・コンテナの下でユーザーを作成できます。
管理者	Oracle Internet Directory スーパー・ユーザー Oracle コンテキスト管理者グループのメンバー ユーザー権限割当てグループのメンバー DAS 管理者グループのメンバー このグループの所有者
DN	`cn=oracleDASCreateUser,cn=groups,`*`Oracle_Context_DN`

ユーザー属性の変更

ユーザー属性を変更するには、管理者はサブスクライバ DAS ユーザー編集グループのメンバーである必要があります。表 17-4 に、このグループの特性を示します。

表 17-4　サブスクライバ DAS ユーザー編集グループの特性

特性	説明
デフォルト ACP	デフォルトの認証管理レルムのユーザー・コンテナにある ACL により、レルムの Oracle コンテキストのサブスクライバ DAS ユーザー編集グループは、ユーザーの各種属性を変更できます。
管理者	Oracle Internet Directory スーパー・ユーザー
	Oracle コンテキスト管理者グループのメンバー
	ユーザー権限割当てグループのメンバー
	DAS 管理者グループのメンバー
	このグループの所有者
DN	`cn=oracleDASEditUser,cn=groups,`*`Oracle_Context_DN`

ユーザーの削除

レルムでユーザーを削除するには、管理者は DAS ユーザー削除グループのメンバーである必要があります。表 17-5 に、このグループの特性を示します。

表 17-5　DAS ユーザー削除グループの特性

特性	説明
デフォルト ACP	デフォルトの認証管理レルムのユーザー・コンテナにある ACL により、レルムの Oracle コンテキストの DAS ユーザー削除グループは、レルムからユーザーを削除できます。
管理者	Oracle Internet Directory スーパー・ユーザー
	Oracle コンテキスト管理者グループのメンバー
	ユーザー権限割当てグループのメンバー
	DAS 管理者グループのメンバー
	このグループの所有者
DN	`cn=oracleDASDeleteUser,cn=groups,`*`Oracle_Context_DN`

ユーザー管理の委任

委任管理者は、ディレクトリで指定された操作を実行できます。また、前述のユーザー作成、ユーザー編集、ユーザー削除の各グループにユーザーを追加する権限を必要とします。

委任管理者にユーザー管理権限を付与するには、付与する管理者がユーザー権限割当てグループのメンバーである必要があります。表 17-6 に、このグループの特性を示します。

表 17-6 ユーザー権限割当てグループの特性

特性	説明
デフォルト ACP	前述の各グループの ACL ポリシーにより、ユーザー権限割当てグループのメンバーは、これらのグループでユーザーを追加または削除することができます。
管理者	Oracle Internet Directory スーパー・ユーザー Oracle コンテキスト管理者グループ このグループの所有者。これらの所有者の識別名は、グループの `owner` 属性の値としてリストされます。
DN	`cn=oracleDASUserPriv,cn=groups,`*`Oracle_Context_DN`*

グループ・データを管理するためのデフォルトの権限

ユーザーとグループの管理には、次の権限が含まれます。

- グループ・エントリを作成および削除する権限
- グループ属性を変更する権限
- グループ管理を他のユーザーに委任する権限

グループを作成するための ACP は、認証管理レルムのグループ・コンテナにあります。

グループの作成

Oracle Internet Directory でグループを作成するには、管理者はグループ作成グループのメンバーである必要があります。表 17-7 に、このグループの特性を示します。

表 17-7　グループ作成グループの特性

特性	説明
デフォルト ACP	レルムのグループ・コンテナにある ACL により、グループ作成グループは、レルムで新規グループを追加できます。
管理者	Oracle Internet Directory スーパー・ユーザー
	Oracle コンテキスト管理者グループのメンバー
	Oracle Application Server 管理者グループのメンバー
	グループ権限割当てグループのメンバー
	DAS 管理者グループのメンバー
	このグループの所有者
DN	`cn=oracleDASCreateGroup,cn=groups,`*`Oracle_Context_DN`*

グループ属性の変更

レルムのグループ・コンテナの下のグループ属性を変更するには、管理者はグループ変更グループのメンバーである必要があります。表 17-8 に、このグループの特性を示します。

表 17-8　グループ編集グループの特性

特性	説明
デフォルト ACP	レルムのグループ・コンテナにある ACL により、グループ編集グループは、レルムでグループの各種属性を変更できます。
管理者	Oracle Internet Directory スーパー・ユーザー
	Oracle コンテキスト管理者グループのメンバー
	Oracle Application Server 管理者グループのメンバー
	グループ権限割当てグループのメンバー
	DAS 管理者グループのメンバー
	このグループの所有者
DN	`cn=oracleDASEditGroup,cn=groups,`*`Oracle_Context_DN`*

グループの削除

グループを削除するには、管理者はグループ削除グループにメンバーであることが必要です。表 17-9 に、このグループの特性を示します。

表 17-9　グループ削除グループの特性

特性	説明
デフォルト ACP	レルムのグループ・コンテナにある ACL により、グループ削除グループは、レルムでグループを削除できます。
管理者	Oracle Internet Directory スーパー・ユーザー Oracle コンテキスト管理者グループのメンバー グループ権限割当てグループのメンバー DAS 管理者グループのメンバー このグループの所有者
DN	`cn=oracleDASDeleteGroup,cn=groups,`*Oracle_Context_DN*

グループ管理の委任

グループの管理を他のユーザーに委任する（つまり、前述のグループ作成、グループ編集またはグループ委任の各グループでユーザーを追加または削除する）には、管理者はグループ権限割当てグループのメンバーである必要があります。表 17-10 に、このグループの特性を示します。

表 17-10　グループ権限割当てグループのメンバーの特性

特性	説明
デフォルト ACP	グループ作成、グループ編集、グループ削除の各グループの ACL ポリシーにより、グループ権限割当てグループのメンバーは、これらのグループでユーザーを追加または削除することができます。
管理者	Oracle Internet Directory スーパー・ユーザー Oracle コンテキスト管理者グループのメンバー グループの所有者。これらの所有者の識別名は、グループの `owner` 属性の値としてリストされます。
DN	`cn=oracleDASUserPriv,cn=groups,`*Oracle_Context_DN*

Oracle コンポーネントの配置権限の委任

この項では、Oracle コンポーネントを配置するグループについて説明します。また、これらの管理者が実行するタスクと、付与できる権限についても説明します。次の項目について説明します。

- 配置権限の付与方法
- Oracle Application Server 管理者
- ユーザー管理アプリケーション管理者
- トラステッド・アプリケーション管理者

注意： Oracle Internet Directory のスーパー・ユーザーは、Oracle Application Server 管理者およびトラステッド・アプリケーション管理者のすべての権限を所有しています。また、Oracle Application Server 管理者グループのメンバーである必要があります。スーパー・ユーザーは、次の割当てを実行できます。

- ユーザーに対する Oracle Application Server 管理者ロールの割当て
- ユーザーに対するトラステッド・アプリケーション・ロールの割当て
- ユーザーに対するユーザー管理アプリケーション管理者ロールの割当て

配置権限の付与方法

管理者が Oracle コンポーネントを配置するには、スーパー・ユーザーは次の手順を実行します。

1. 特定の配置権限を Oracle Application Server 管理者グループなどの様々なグループに付与します。
2. 管理者をこれらの権限グループに追加します。

一方、委任管理者は、権限を他の管理者に委任できます。

Oracle Application Server 管理者

表 17-11 に、Oracle Application Server 管理者グループの特性を示します。

表 17-11　Oracle Application Server 管理者グループの特性

特性	説明
タスク	ディレクトリでリポジトリ・データベース登録エントリを作成する、リポジトリ・データベースのインストールの実行
	中間層インストールの実行。中間層をリポジトリと関連付けるには、ユーザーは特定のリポジトリ・データベースでの適切な権限が必要です。
	Oracle Internet Directory でアプリケーション・エンティティを作成する、Oracle Application Server コンポーネントのインストールと構成
	この項で後述するリストに示す実行時権限のコンポーネント・エンティティへの付与
	コンポーネントが更新通知を受信できるようにするための、コンポーネントに対するプロビジョニング・プロファイルの構成
このグループがコンポーネントに委任できる権限	パスワード、証明書および類似のセキュリティ資格証明以外の一般ユーザー属性を読み取る権限
	一般グループ属性を読み取る権限
	グループを作成、編集および削除する権限
	ユーザーを認証する権限
	アプリケーション・ベリファイアを読み取る権限
管理者	Oracle Internet Directory スーパー・ユーザー（super user）
	Oracle コンテキスト管理者
	このグループの所有者
DN	`cn=IASAdmins,cn=groups,`*`Oracle_Context_DN`*

ユーザー管理アプリケーション管理者

ユーザー管理アプリケーション管理者は、Oracle Application Server 管理者グループのメンバーである必要があります。

表 17-12 に、ユーザー管理アプリケーション管理者グループの特性を示します。

表 17-12 ユーザー管理アプリケーション管理者グループの特性

特性	説明
タスク	ユーザー管理アプリケーション管理者は、ユーザー管理操作を実行するためのインタフェースを持つ特定のアプリケーションをインストールします。たとえば、OracleAS Portal や Oracle Application Server Wireless などです。
このグループがコンポーネントに委任できる権限	ユーザー属性を作成、編集および削除する権限
管理者	Oracle Internet Directory スーパー・ユーザー（super user） Oracle コンテキスト管理者 このグループの所有者
DN	`cn=IAS & User Mgmt Admins,cn=groups,` *`Oracle_Context_DN`*

トラステッド・アプリケーション管理者

トラステッド・アプリケーション管理者は、Oracle Application Server 管理者グループのメンバーである必要があります。

表 17-13 に、トラステッド・アプリケーション管理者グループの特性を示します。

表 17-13 トラステッド・アプリケーション管理者グループの特性

特性	説明
タスク	特定の認証管理コンポーネントをインストールします。たとえば、Oracle Application Server Single Sign-On、Oracle Delegated Administration Services、Oracle Application Server Certificate Authority などです。
このグループがコンポーネントに委任できる権限	ユーザー・パスワードの読取り、比較、再設定を行う権限 エンド・ユーザーのプロキシとなる権限 ユーザーの証明書と SMIME 証明書の読取り、比較、変更を行う権限

表 17-13 トラステッド・アプリケーション管理者グループの特性（続き）

特性	説明
管理者	Oracle Internet Directory スーパー・ユーザー（super user） Oracle コンテキスト管理者 このグループの所有者
DN	`cn=Trusted Application Admins,cn=groups,` *`Oracle_Context_DN`*

コンポーネントの実行時権限の委任

多くの Oracle コンポーネントでは、Oracle Internet Directory でユーザー・エントリが管理されているため、それに対応する権限が必要です。次に例を示します。

- Oracle Application Server Single Sign-On Server がユーザーを認証する場合、そのサーバーには次の権限が必要です。
  - 独自の識別情報を使用して Oracle Internet Directory に接続する権限
  - ユーザーの入力したパスワードが、ディレクトリに格納されているそのユーザーのパスワードと一致するかどうかを検証する権限

  このためには、Oracle Application Server Single Sign-On Server はユーザー・パスワードを比較する権限を必要とします。Oracle Application Server Single Sign-On の Cookie を設定するには、ユーザー属性を読み取る権限が必要です。
- ユーザーにアクセス権を付与するには、OracleAS Portal はそのユーザーの属性を取得する必要があります。そのためには、アクセス権を必要とするユーザーにかわって、プロキシ・ユーザーとして Oracle Internet Directory にログインします。したがって、プロキシ・ユーザー権限が必要です。

通常、Oracle コンポーネントでは、次の権限が必要となる場合があります。

- ユーザー・パスワードの読取りと変更を行う権限
- ユーザー・パスワードの比較を行う権限
- アプリケーションにアクセスするユーザーのプロキシとなる権限
- すべての Oracle コンポーネントのメタデータが格納される Oracle コンテキストを管理する権限

ほとんどの Oracle コンポーネントには、事前定義された権限のセットを付属しています。これらの権限は、個々のビジネス要件を満たすように変更できます。たとえば、要件を満たすために、ユーザー・エントリを作成および削除するための権限を削除できます。

> **関連項目：** コンポーネント委任モデルの詳細は、『Oracle Application Server 10*g* セキュリティ・ガイド』を参照してください。

この項では、Oracle コンポーネントが必要とするセキュリティ権限を説明します。次の項目について説明します。

- ユーザー・パスワードの読取りおよび変更を行うためのデフォルトの権限
- ユーザー・パスワードを比較するためのデフォルトの権限
- パスワード・ベリファイアを比較するためのデフォルトの権限
- エンド・ユーザーのプロキシとなるためのデフォルトの権限
- Oracle コンテキストを管理するためのデフォルトの権限
- 共通ユーザー属性を読み取るためのデフォルトの権限
- 共通グループ属性を読み取るためのデフォルトの権限

ユーザー・パスワードの読取りおよび変更を行うためのデフォルトの権限

ユーザー・パスワードの読取りと変更は、ディレクトリにあるセキュリティ関係の属性（userPassword 属性など）に対する管理権限を必要とします。表 17-14 に示すユーザー・セキュリティ管理者グループでのメンバーである必要があります。

表 17-14 ユーザー・セキュリティ管理者グループの特性

特性	説明
デフォルト ACP	ルート（DSE エントリ）でのデフォルトの ACL ポリシーにより、ユーザー・セキュリティ管理者グループのメンバーは、ルート Oracle コンテキストで userpkcs12、orclpkcs12hint、userpassword、orclpassword および orclpasswordverifier の各属性の読取り、書込み、比較および検索を行えます。ただし、ディレクトリ管理者は、レルムの Oracle コンテキストのユーザー・セキュリティ管理者グループに同様の管理権限を付与することができます。
管理者	Oracle Internet Directory スーパー・ユーザー Oracle コンテキスト管理者グループのメンバー トラステッド・アプリケーション管理者グループのメンバー
DN	cn=oracleUserSecurityAdmins,cn=groups,*Oracle_Context_DN*

ユーザー・パスワードを比較するためのデフォルトの権限

ユーザー・パスワードの比較には、ユーザーの userPassword 属性を比較する権限が必要です。この操作は、Oracle Internet Directory に格納されたパスワードを使用してエンド・ユーザーを認証する Oracle Unified Messaging のようなコンポーネントにより実行されます。

ユーザー・パスワードを比較するには、表 17-15 に示す認証サービス・グループのメンバーである必要があります。

表 17-15 認証サービス・グループの特性

特性	説明
デフォルト ACP	デフォルトの認証管理レルムのユーザー・コンテナにある ACL ポリシーにより、認証サービス・グループは、ユーザーの userPassword 属性に対する比較操作を実行できます。
管理者	Oracle Internet Directory スーパー・ユーザー Oracle コンテキスト管理者グループのメンバー アプリケーション・サーバー管理者グループのメンバー このグループの所有者
DN	cn=authenticationServices,cn=groups,*Oracle_Context_DN*

パスワード・ベリファイアを比較するためのデフォルトの権限

パスワード・ベリファイアを比較するには、userpassword 属性を比較する権限が必要です。パスワード・ベリファイアを比較するには、表 17-16 に示すベリファイア・サービス・グループのメンバーである必要があります。

表 17-16 ベリファイア・サービス・グループの特性

特性	説明
管理者	Oracle Internet Directory スーパー・ユーザー Oracle コンテキスト管理者グループのメンバー アプリケーション・サーバー管理者グループのメンバー このグループの所有者
DN	cn=verifierServices,cn=groups,*Oracle_Context_DN*

エンド・ユーザーのプロキシとなるためのデフォルトの権限

プロキシ・ユーザーは、エンド・ユーザーの代理となる権限を持ち、そのユーザーが権限を持つ操作をユーザーにかわって実行します。Oracle Application Server 環境では、Oracle Delegated Administration Services がエンド・ユーザーのプロキシとなり、Oracle Internet Directory セルフ・サービス・コンソールを通じて、そのユーザーのかわりに操作を実行します。そのような場合、ディレクトリ・サーバーに対するアクセス制御がユーザーの実行できる操作を実質的に制御します。

エンド・ユーザーのプロキシには、表 17-17 に示すユーザー・プロキシ権限グループのメンバーである必要があります。

表 17-17 ユーザー・プロキシ権限グループの特性

特性	説明
デフォルト ACP	デフォルトの認証管理レルムのユーザー・コンテナでの ACL ポリシーにより、ユーザー・プロキシ権限グループは、エンド・ユーザーのプロキシとなることができます。
管理者	Oracle Internet Directory スーパー・ユーザー Oracle コンテキスト管理者グループのメンバー グループの所有者。これらの所有者の識別名は、Oracle Application Server 管理者グループのグループまたはメンバーの `owner` 属性の値としてリストされます。 トラステッド・アプリケーション管理者グループのメンバー
DN	`cn=userProxyPrivilege,cn=groups,`*`OracleContextDN`*

Oracle コンテキストを管理するためのデフォルトの権限

特定の Oracle コンテキストを管理するには、そのコンテキストへの完全なアクセス権が必要です。Oracle コンテキストを管理するには、表 17-18 に示す Oracle コンテキスト管理者グループのメンバーである必要があります。Oracle コンテキスト管理者グループは、Oracle コンテキストごとに存在し、特定の Oracle コンテキストでの管理権限を持ちます。

表 17-18 Oracle コンテキスト管理者グループの特性

特性	説明
デフォルト ACP	Oracle コンテキストのルート・ノードにある ACL ポリシーにより、Oracle コンテキスト管理者グループは、Oracle コンテキスト内ですべての管理操作を実行できます。そのようなポリシーは、ディレクトリで新しい Oracle コンテキストが作成されるときに設定されます。
管理者	Oracle Internet Directory スーパー・ユーザー Oracle コンテキスト管理者グループのメンバー

表 17-18 Oracle コンテキスト管理者グループの特性（続き）

特性	説明
DN	cn=oracleContextAdmins,cn=groups,*Oracle_Context_DN*

共通ユーザー属性を読み取るためのデフォルトの権限

共通ユーザー属性には、mail、orclguid、displayname、preferredlanguage、orcltime、gender、dateofbirth、telephonenumber および wirelessaccountnumber があります。これらの属性を読み取るには、表 17-19 に示す共通ユーザー属性グループのメンバーである必要があります。

表 17-19 共通ユーザー属性グループの特性

特性	説明
デフォルト ACP	デフォルト ACL は、レルム内のユーザー・コンテナ上にあり、共通ユーザー属性を読み取る権限を付与します。
管理者	Oracle Internet Directory スーパー・ユーザー アプリケーション・サーバー管理者グループのメンバー このグループの所有者
DN	cn=commonuserattributes,cn=users,*Oracle_Context_DN*

共通グループ属性を読み取るためのデフォルトの権限

共通グループ属性には、cn、uniquemember、displayname および description があります。これらの属性を読み取るには、表 17-20 に示す共通グループ属性グループのメンバーである必要があります。

表 17-20 共通グループ属性グループの特性

特性	説明
デフォルト ACP	デフォルト ACL は、レルム内のグループ・コンテナ上にあり、cn、uniquemember、displayname および description 属性を読み取る権限を付与します。
管理者	Oracle Internet Directory スーパー・ユーザー アプリケーション・サーバー管理者グループのメンバー このグループの所有者
DN	cn=commongroupattributes,cn=groups,*Oracle_Context_DN*

第 IV 部

ディレクトリの配置

第 IV 部では、配置に関する重要な考慮事項について説明します。第 IV 部は次の各章で構成されています。

- 第 18 章「ディレクトリ配置の考慮事項」
- 第 19 章「Oracle Identity Management レルムの配置」
- 第 20 章「ディレクトリの容量計画」
- 第 21 章「ディレクトリのチューニングに関する考慮事項」
- 第 22 章「Oracle Internet Directory におけるガベージ・コレクション」
- 第 23 章「他のディレクトリからのデータの移行」

18

ディレクトリ配置の考慮事項

この章では、Oracle Internet Directory を配置するときに考慮する必要がある問題について説明します。企業のディレクトリの要件を評価し、効果的な配置を選択するのに役立ちます。この章の推奨事項は、主に中規模および大規模の企業やインターネット・サービス・プロバイダ（ISP）のディレクトリに対するものですが、基本的な考え方は他の環境でも同様に適用できます。

この章では、次の項目について説明します。

- 拡大するディレクトリの役割
- ディレクトリ情報の論理編成
- 物理的な分散 : パーティション、レプリカおよび高可用性
- Oracle Directory Integration and Provisioning Platform
- 容量計画、サイズ設定およびチューニング
- 1 つのホストにおける複数の Oracle Internet Directory インストール

関連項目：

- 容量計画の詳細は、第 20 章「ディレクトリの容量計画」を参照してください。
- 高可用性の詳細は、第 26 章「高可用性とフェイルオーバーに関する考慮事項」を参照してください。
- チューニングの詳細は、第 21 章「ディレクトリのチューニングに関する考慮事項」を参照してください。
- クラスタ化された環境でのフェイルオーバーの詳細は、「ディレクトリ・レプリケーションおよび高可用性」を参照してください。

拡大するディレクトリの役割

現在、ほとんどの企業では、集中化および整理統合された LDAP 準拠のディレクトリを配置する傾向にあります。一部の企業では、非 LDAP 準拠のディレクトリ（例 : NDS または ISO X.500）を使用していましたが、現在は対応する LDAP 対応のバージョンに変換しています。これは、LDAP に依存するインターネット・クライアント（Web ブラウザに埋め込まれているものなど）に対応するため、あるいは増え続けるディレクトリ対応のプラットフォームやサービスを整理統合するためです。

LDAP 対応のアプリケーションの増加により、LDAP 準拠のディレクトリに対する可用性とパフォーマンスの要件が重要視されています。ほとんどの環境で配置を更新する必要があります。

企業は、次のような状況に対応するために、堅牢で柔軟な配置を計画する必要があります。

- ディレクトリ内の情報量の増加
- ディレクトリに依存するアプリケーションの数
- 同時アクセスやスループットなどのロード特性

ディレクトリがネットワークとそのサービスの運用の中心となるので、配置の選択が重要となります。

ディレクトリ情報の論理編成

Oracle Internet Directory は、Oracle Identity Management インフラストラクチャ全体の共有リポジトリとして機能します。ディレクトリの論理構造を慎重に計画することによって、次のことが可能になります。

- 配置の要件を満たすセキュリティ・ポリシーの施行
- ディレクトリ・サービスの効率的な物理的配置
- サード・パーティのディレクトリを Oracle Internet Directory と同期化させる場合の簡単な構成

関連項目： 19-5 ページの「認証管理を行うためのディレクトリ情報ツリーの計画」

物理的な分散 : パーティション、レプリカおよび高可用性

ディレクトリ・データを分散するには、次の 2 つの方法があります。

- サーバーのディレクトリ全体のメンテナンス
- 異なるサーバー上の異なるネーミング・コンテキストのホスティングおよびナレッジ参照によるネーミング・コンテキストの接続

関連項目： 2-21 ページの「分散ディレクトリ」

この項では、次の項目について説明します。

理想的な配置

中央の 1 つのディレクトリにすべてのネーミング・コンテキストを格納すると、より単純かつ安全であると考えられますが、この中央のディレクトリはシングル・ポイント障害の発生箇所になります。

1 つの解決策は、冗長な LDAP サーバーとそれに対応付けられたデータベースを実装することです。しかし、冗長性を持たせても、ほとんどのグローバルな組織がその地域やサイトすべてで必要とする、接続性、アクセス可能性およびパフォーマンスが提供されない場合があります。これらの要件を満たすには、企業の地理的な広がりに応じて、様々な地域にレプリカを物理的に配置する必要があります。

Oracle Internet Directory が単一のマスターによる構成しかサポートしない場合、ディレクトリの論理的な統合は困難なものとなります。各地域またはグループは、信頼できるネーミング・コンテキストのマスター・レプリカを格納することが必要となります。この方法では、管理者はパーティションごとに異なるデータ管理手順を使用する必要があるため、パーティションにわたる管理ポリシーに一貫性を欠くことになります。

マルチマスター・レプリケーションでは、どこでも更新可能な構成ができるため、ディレクトリの統合は、複数のパーティションをメンテナンスするより効率的で費用がかかりません。

堅牢で集中化された企業ディレクトリにするための、単純で実用的な推奨事項は次のとおりです。

- それぞれがすべてのネーミング・コンテキストを保持した、2 つ以上のディレクトリ・ノードを持つネットワークを確立します。これらのノードはマルチマスター構成で設定します。
- これらのノードをそれぞれ各地域に 1 つずつ、企業のデータ・ネットワーク接続に合うように配置します。たとえば、ある地域が遅いリンク方法でネットワークの他の地域と接続されている場合、その地域のクライアントが使用するための専用のディレクトリ・サーバーを設置する必要があります。
- フェイルオーバーとリカバリのために、各地域のサーバーを個々に構成します。

すべてのネーミング・コンテキストは整理統合されていますが、今までどおり様々な論理ネーミング・コンテキストに対して管理の自律性を実現できます。そのためには、適切なアクセス制御ポリシーを各ネーミング・コンテキストのルートで設定してください。

> **関連項目：** 冗長性の詳細は、18-6 ページの「高可用性に関する考慮事項」を参照してください。

パーティション化に関する考慮事項

パーティションが多すぎるディレクトリは、一般的に利点よりも管理上のオーバーヘッドのほうが大きくなります。これは、各パーティションごとに、バックアップ、リカバリおよびその他のデータ管理機能の計画が必要になるためです。

通常、パーティションをメンテナンスする理由は次のようなものです。

- パーティションが、独立したままのほうが、より管理の境界およびデータ所有権の境界に対応している。
- 企業ネットワークに、費用がかかる、あるいはスピードが遅いリンクと接続されている地域があり、多くのパーティションがローカル・アクセスのみを必要としている。
- パーティションの可用性の欠如が大きな影響を及ぼさない。
- 1 つの地域での企業全体のディレクトリのメンテナンスに、費用がかかりすぎる。

パーティション化する場合は、**ナレッジ参照**を使用して 1 つのパーティションを他のパーティションに接続します。

注意： LDAP では、LDAP サーバーによるナレッジ参照の自動連鎖をサポートしません。クライアント側の LDAP API のほとんどは、クライアント主導のナレッジ参照の追跡をサポートします。しかし、ナレッジ参照がすべての LDAP ツールでサポートされるという保証はありません。使用可能なツール全体で、一貫したナレッジ参照のサポートが欠如しているということは、パーティションの使用を決定する前の考慮事項です。

レプリケーションに関する考慮事項

LDAP ディレクトリ・レプリケーション・アーキテクチャは、緩和された一貫性モデルに基づいています。**レプリケーション承諾**内の 2 つのレプリケート・ノードが、リアルタイムで一貫しているという保証はありません。そのため、ディレクトリ・ネットワークの柔軟性と可用性が全般的に増加します。クライアントは相互接続されたすべてのノードが使用可能でなくても、データを変更できるためです。たとえば、1 つのノードが使用不可であるか、または負荷が高いとします。マルチマスター・レプリケーションでは、操作は代替のノードで実行され、後に相互接続されたすべてのノードが同期化します。

レプリケート・ネットワークを実装する理由の多くは、次のようなものです。

- ローカルなアクセス可能性とパフォーマンス要件

  多くの企業は世界中の様々な地域で活動しており、それらの活動には共通ディレクトリが必要です。複数の中継ルーターを含む、低帯域幅のリンクで各地域が相互接続されているとします。地域の外部からディレクトリ・サーバーにアクセスしているクライアントは、長い**待機時間**および不十分な**スループット**を体験します。

  このような場合には、地域レプリカ（更新を受信するために、マルチマスター・レプリケーションによって使用可能にされています）が必要です。さらに、基礎となる **Oracle9i Advanced Replication** に、閑散時のレプリケーション・データ転送をスケジュールできます。

- ロード・バランシング

  ディレクトリ・アクセスが既存のサーバーの容量を超えると、追加のサーバーが負荷を共有する必要があります。Oracle Internet Directory では、そのような 2 つのシステムをマルチマスター・レプリケーション・モードで配置できます。実際、特定の負荷見積りを満たすディレクトリ配置を計画する場合、1 つのハイエンド・システムよりも 2 つの比較的安価なシステムをメンテナンスするほうが、費用がかからない場合があります。ロード・バランシングに加えて、そのような構成も、システムの可用性を高めることに貢献します。

- 障害許容度とシステム全体の高可用性

  ディレクトリ・レプリケーションを実装する最も重要な理由の 1 つは、システム全体の可用性を増すことです。1 つのサーバーが使用できない場合、通信量は他の使用可能なサーバーに送られます。これはクライアントには透過的です。

> **関連項目：** レプリケート・ディレクトリ構成の詳細は、『Oracle Identity Management 概要および配置プランニング・ガイド』の Oracle Internet Directory の物理的配置計画についての項を参照してください。

高可用性に関する考慮事項

ディレクトリ・サービスは企業内で重要な機能を持っているので、配置する際に障害リカバリと高可用性を考慮する必要があります。各ノードのバックアップおよびリカバリ計画を作成することが必要です。

マルチマスター・レプリケーションに加えて、Oracle Internet Directory のインストール時に可能な配置について、次のフェイルオーバーおよび高可用性オプションを考慮します。

- インテリジェント・クライアントのフェイルオーバー

  Oracle Internet Directory に接続しているすべての LDAP クライアントは、指定したサーバー・インスタンスとの接続が突然切断された場合に接続する、Oracle Internet Directory の代替サーバー・インスタンスのリストをメンテナンスできます。

- インテリジェント・ネットワーク・レベルのフェイルオーバー

  Oracle Internet Directory を稼働させるシステムの障害を検出できる、ハードウェアおよびソフトウェアのソリューションがいくつかあります。これらのソリューションでは、以降の接続要求を代替サーバーにインテリジェントに変更できます。この中には、必要なフェイルオーバー機能も提供しながら、受信した接続要求の負荷を代替サーバーと調整するソリューションもあります。

- 1 つのホストにおける複数の Oracle Internet Directory インストール

  単一のホストで複数の Oracle Internet Directory のインストールを実行して、それらの間でレプリケートすることが可能です。自動バックアップにより、同一マシン上で最新のディレクトリ・データを提供するうえで、この方法は便利です。使用するノードを 2 つのみにすると、フェイルオーバーも可能になります。いずれかのノードに障害が発生しても、両方の Oracle Internet Directory のインスタンスは、もう一方のノード上で実行できます。

Oracle Internet Directory は Oracle9*i* のクライアントであるため、Oracle9*i* Real Application Clusters などの他のフェイルオーバー・テクノロジも使用可能です。

関連項目 :

- Oracle Internet Directory で使用可能な、高可用性およびフェイルオーバーのオプションの詳細は、第 26 章「高可用性とフェイルオーバーに関する考慮事項」を参照してください。
- ディレクトリの高可用性の詳細は、『Oracle Identity Management 概要および配置プランニング・ガイド』の Oracle Internet Directory の物理的配置計画についての項を参照してください。

Oracle Directory Integration and Provisioning Platform

サード・パーティの LDAP ディレクトリを含め、ディレクトリおよびアプリケーションを Oracle Internet Directory に統合することにより、管理作業に必要な時間とコストを削減できます。これは、Oracle Identity Management のコンポーネントである Oracle Directory Integration and Provisioning Platform によって実現します。たとえば、企業には次のようなニーズがあります。

- Oracle Human Resources と Oracle Internet Directory で従業員レコードの整合性を維持すること。Oracle Directory Integration and Provisioning Platform は Oracle Directory Synchronization Service によって、この同期化を行います。
- 変更が Oracle Internet Directory に適用されるたびに、OracleAS Portal などの LDAP 対応アプリケーションに通知されること。Oracle Directory Integration and Provisioning Platform は Oracle Directory Provisioning Integration Service によって、この通知を行います。

統合処理全体を通して、Oracle Directory Integration and Provisioning Platform は、アプリケーションとその他のディレクトリが確実な方法で必要な情報を受け取ったり提供することを保証します。

Oracle Directory Integration and Provisioning Platform は、Microsoft Active Directory や SunONE Directory Server など、様々なディレクトリに統合することができます。たとえば、Oracle Application Server 環境では、Oracle コンポーネントへのアクセスは、Oracle Internet Directory に格納されているデータに基づいて行います。この環境では、企業の中央ディレクトリとして Microsoft Active Directory も使用できます。これらのディレクトリのユーザーが Oracle コンポーネントにアクセスできるのは、Oracle Directory Integration and Provisioning Platform が、Microsoft Active Directory 内のデータを、Oracle Internet Directory 内のデータと同期化できるためです。

関連項目： 第 32 章「Oracle Directory Integration and Provisioning Platform の概要とコンポーネント」

容量計画、サイズ設定およびチューニング

ディレクトリの使用に際し、企業全体および地域の要件を見積もるときは、将来の必要性を計画します。レプリケーションとフェイルオーバーは他の構成の選択に依存するため、それぞれ独自の負荷と容量の要件を持つ複数のディレクトリ・ノードを必要とする場合があります。この場合、各ディレクトリ・ノードに対し個々にサイズを決める必要があります。

企業ではディレクトリの使用が増加しているので、Oracle Internet Directory を使用して要求を適時に処理する必要があるアプリケーションも増えています。Oracle Internet Directory のインストールが、それらのアプリケーションのパフォーマンスと容量の期待値にこたえられるかを確認します。

配置プロセスの 2 つのフェーズで、指定した Oracle Internet Directory のインストールの容量とパフォーマンスに影響を与えることができます。

- 計画フェーズ

  このフェーズで、ディレクトリのユーザーすべての要件を集めて、統一したパフォーマンスと容量の要件を確立します。これは、容量計画とシステム・サイズ設定で構成されます。

- 実装フェーズ

  ハードウェアの入手後、ハードウェア資源を最大限使用できるように、Oracle Internet Directory ソフトウェア・スタックをチューニングします。Oracle Internet Directory と LDAP クライアント・アプリケーションのパフォーマンスが改善されます。

この項では、次の項目について説明します。

容量計画

容量計画は、パフォーマンスと容量の要件を決定するプロセスです。企業のディレクトリ使用の一般的なモデルに基づいて行われます。

Oracle Internet Directory のインストールに必要な容量を見積もる場合の考慮事項は、次のとおりです。

- LDAP クライアント・アプリケーションのタイプ
- アプリケーションにアクセスするユーザー数
- アプリケーションが実行する LDAP 処理の特性
- ディレクトリ情報ツリー内のエントリ数
- Oracle ディレクトリ・サーバーに対して実行される操作のタイプ
- Oracle ディレクトリ・サーバーへの同時接続数
- Oracle ディレクトリ・サーバーで実行する必要がある、ピーク時の操作の実行率
- ピーク時の負荷条件で必要となる、操作の平均待機時間

これらの考慮事項を詳しく見積もる場合は、ディレクトリの使用が将来増加した場合に備えて余裕を持って見積もってください。

サイズ設定に関する考慮事項

基本となる容量とパフォーマンスの要件を確立した後、それをシステム要件に変換します。これはシステム・サイズ設定と呼ばれます。このフェーズでの考慮事項の詳細は次のとおりです。

- Oracle Internet Directory サーバー・コンピュータの CPU のタイプと数
- Oracle Internet Directory サーバー・コンピュータのディスク・サブシステムのタイプとサイズ
- Oracle Internet Directory サーバー・コンピュータに必要なメモリーの量
- クライアントからの LDAP メッセージに使用されるネットワークのタイプ

表 18-1 に、Oracle Internet Directory の様々な配置例に必要な CPU 能力の概算レベルを、現在の経験に基づいて示します。

表 18-1　様々な配置例に必要な CPU 能力

使用方法	アクティブな接続数	CPU の数	SPECint_rate95 ベースライン	システム
部門単位	0-500	2	60 ～ 200	Compaq AlphaServer 8400 5/300 (300MHz × 2)
組織単位	500-2000	4	200 ～ 350	IBM RS/6000 J50 (200MHz × 4)
会社単位	2000+	4+	350+	Sun Ultra 450 (296 MHz × 4)

Oracle Internet Directory のインストールに必要なディスク領域の量は、ディレクトリ情報ツリーに格納されるエントリ数に正比例します。表 18-2 に、様々なサイズのディレクトリ情報ツリーに必要なディスク領域要件の概算を示します。

表 18-2　様々なサイズのディレクトリ情報ツリーに必要なディスク領域要件の概算

ディレクトリ情報ツリー内のエントリ数	ディスク要件
100,000	450MB ～ 650MB
200,000	850MB ～ 1.5GB
500,000	2.5GB ～ 3.5GB
1,000,000	4.5GB ～ 6.5GB
1,500,000	6.5GB ～ 10GB
2,000,000	9GB ～ 13GB

この表のデータから、次のことが仮定されます。

- カタログ化属性が約 20 個であること
- 各エントリの属性が約 25 個であること
- 属性の平均サイズが約 30 バイトであること

Oracle Internet Directory に必要なメモリーの量は、配置サイトが要求するデータベース・バッファ・キャッシュの量によってほぼ決定されます。多くの場合、データベース・バッファ・キャッシュのサイズは、ディレクトリ情報ツリー内のエントリ数に比例します。表 18-3 に、様々なサイズのディレクトリ情報ツリーのメモリー要件の概算を示します。

表 18-3　様々なサイズのディレクトリ情報ツリーのメモリー要件の概算

ディレクトリのタイプ	エントリ数	最小メモリー
小	600,000 未満	512MB
標準	600,000 ～ 2,000,000	1GB
大	2,000,001 以上	2GB

関連項目： 第 20 章「ディレクトリの容量計画」

チューニングに関する考慮事項

本番環境で使用する前に、Oracle Internet Directory を正しくチューニングすることをお薦めします。チューニングする前に、実際の使用手順をシミュレートするための、十分なテスト手段とサンプル・データがディレクトリにあることを確認してください。テスト用のディレクトリに依存するアプリケーションを使用できます。

Oracle Internet Directory のパフォーマンスをテストするツールは、次のものの表示が可能である必要があります。

- 調べている包括的なスループット
- 操作の平均待機時間

このように、チューニング効果を確認し、チューニング作業全般に指示を与えるため、ツールではフィードバック・メカニズムを提供します。

Oracle Internet Directory のインストールで、一般的にチューニングされるプロパティには、次のようなものがあります。

- CPU 使用量

  次のものによって、ほぼ決定されます。

  - Oracle ディレクトリ・サーバーの数
  - 各サーバーによって開かれるデータベース接続の数

  Oracle ディレクトリ・サーバーとデータベース接続の数が多すぎると、使用可能な CPU リソースの競合が頻繁に発生します。また、Oracle ディレクトリ・サーバーとデータベース接続の数が少なすぎると、CPU の能力の大部分が十分に活用されないままとなります。使用可能な CPU リソースと想定されるピーク時の負荷に基づいて、これらの数を適正なレベルに調整することを考慮してください。

- メモリー使用量

  Oracle Internet Directory のインストールで主にメモリーを使用するのは、**SGA** の一部であるデータベース・バッファ・キャッシュです。大規模なデータベース・バッファ・キャッシュを割り当てることで、Oracle データ・ファイルのディスク I/O の多くを削減できる場合もあります。しかし、パフォーマンスに悪影響を及ぼすページングを発生させることにもなります。逆にデータベース・バッファ・キャッシュを小さくすると、ディスク I/O が多く発生して、パフォーマンスに悪影響を及ぼします。システム内のメモリーのコンシューマすべてが、ページングの使用を必要とせずに物理メモリーを取得できるように、システムのメモリー使用量をチューニングします。

- ディスク使用量

  Oracle Internet Directory によって処理されるデータはすべてデータベースの表領域に常駐しているので、I/O スループットを増加させるようなチューニングには注意してください。一般的なディスクのチューニング方法は、次のとおりです。

  - 異なる論理ドライブおよび物理ドライブにある表領域の均衡化
  - 論理ボリュームの複数の物理ボリュームへのストライプ化
  - ディスク・ボリュームの複数の I/O 制御装置への分散

  関連項目： 様々なチューニングのヒントと方法の詳細は、第 21 章「ディレクトリのチューニングに関する考慮事項」を参照してください。

19

Oracle Identity Management レルムの配置

この章では、認証管理レルムについて、企業内配置およびホスティングされた配置用に計画および構成する方法を説明します。

この章では、次の項目について説明します。

- 企業内配置における認証管理レルム
- ホスティングされた配置における認証管理レルム
- Oracle Internet Directory での認証管理レルムの実装
- 認証管理を行うためのディレクトリ情報ツリーの計画
- デフォルトのディレクトリ情報ツリーおよび認証管理レルム
- 認証管理レルムの管理

企業内配置における認証管理レルム

この項では、単一および複数の認証管理レルムを使用する配置について説明します。この項では、次の項目について説明します。

- 企業における単一認証管理レルム
- 企業における複数認証管理レルム

企業における単一認証管理レルム

すべての Oracle 製品のデフォルトの構成です。この場合、企業には、ユーザーの集団が 1 つあり、そのすべてのユーザーが同一の認証管理ポリシーによって管理されます。Oracle Internet Directory に存在するデフォルトの認証管理レルムは 1 つのみです。企業内のすべての Oracle コンポーネントが、デフォルトのレルム内のユーザーに対応しています。図 19-1 に、この使用方法を示します。

図 19-1 企業での使用例 : 単一認証管理レルム

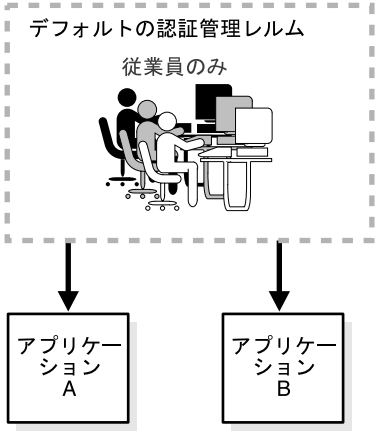


図 19-1 の例では、すべてのユーザーおよびグループが管理され、同じアプリケーションへのアクセスを共有する単一認証管理レルムがあります。

企業における複数認証管理レルム

同一の認証管理インフラストラクチャを使用して、内部ユーザーと外部の自己登録ユーザーの両方に対応する企業もあります。内部ユーザーと外部ユーザーでは認証管理ポリシーが異なるため、企業では、内部ユーザー用と外部ユーザー用にレルムを 1 つずつ配置できます。19-3 ページの図 19-2 に、その使用方法を示します。

図 19-2 企業での使用例 : 複数認証管理レルム

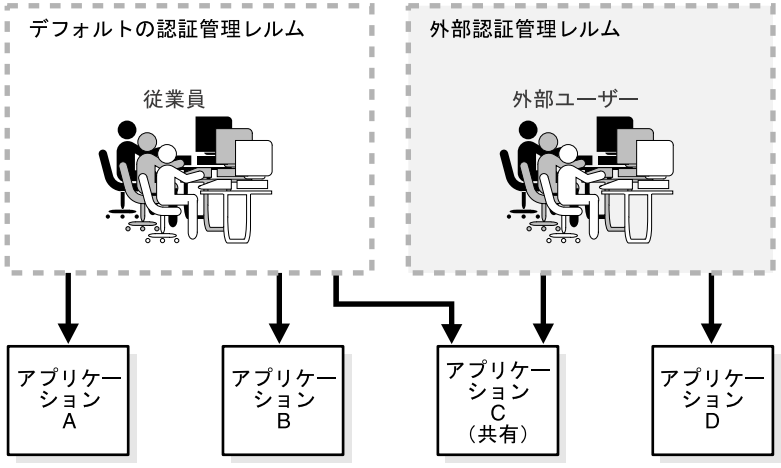


図 19-2 の例では、デフォルトの認証管理レルムが内部ユーザー（従業員）用です。内部ユーザーは、アプリケーション A、B および C へのアクセス権を所有しています。外部認証管理レルムは外部ユーザー用に使用されます。外部ユーザーは、アプリケーション C および D へのアクセス権を所有しています。

ホスティングされた配置における認証管理レルム

ホスティングされた配置では、アプリケーション・サービス・プロバイダ（ASP）が、1 社以上に認証管理サービスを提供し、これらの企業にかわってアプリケーションのホスティングを行います。ホスティングされた各企業は、その企業のユーザーが管理される個別の認証管理レルムに対応付けられます。アプリケーション・サービス・プロバイダに属するユーザーは、別のレルム（通常は、デフォルトのレルム）で管理されます。

図 19-3 に、ホスティングされた配置（2 社をホスティング）を示します。

図 19-3 ホスティングされた配置での使用例

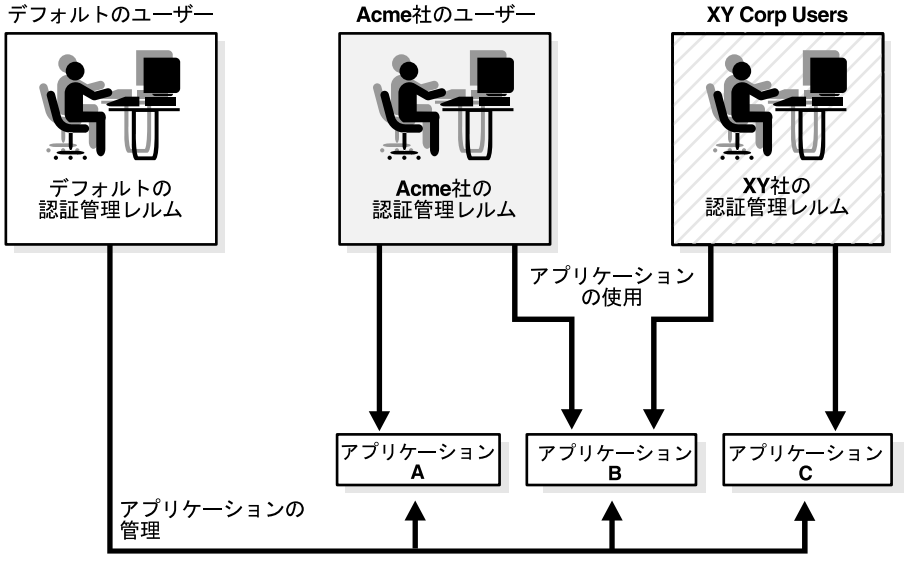


図 19-3 の例では、ASP ユーザーが行うのは、ホスティングされた企業にかわってホスティングする様々なアプリケーションの管理です。ホスティングされた各企業には、ユーザー、グループおよび関連するポリシーが ASP によって管理される認証管理レルムが関連付けられています。

Oracle Internet Directory での認証管理レルムの実装

表 19-1 に、Oracle Internet Directory ツリー内にある認証管理レルムの情報モデルについて説明します。

表 19-1 Oracle Identity Management オブジェクト

オブジェクト	説明
ルート Oracle コンテキスト	インフラストラクチャ内のデフォルトの認証管理レルムへのポインタが含まれます。単純な名前を指定して認証管理レルムの位置を特定する方法の詳細も含まれます。
認証管理レルム	特別なオブジェクト・クラスが関連付けられた Oracle Internet Directory ツリー内の通常のディレクトリ・エントリ。
認証管理レルム固有の Oracle コンテキスト	各レルムには、次の情報のコンテナがあります。 ■ 認証管理レルムのユーザー・ネーミング・ポリシー（ユーザーに名前を付け、配置する方法） ■ 必須認証属性 ■ 認証管理レルム内のグループの位置 ■ 認証管理レルムに対する権限の割当て（レルムにユーザーを追加する権限の割当てなど） ■ レルムに関するアプリケーション固有のデータ（認可など）

認証管理を行うためのディレクトリ情報ツリーの計画

Oracle Internet Directory は、Oracle Identity Management インフラストラクチャ全体の共有リポジトリとして機能します。ディレクトリの論理構造を慎重に計画することによって、次のことが可能になります。

- 配置の要件を満たすセキュリティ・ポリシーの施行
- ディレクトリ・サービスの効率的な物理的配置
- サード・パーティのディレクトリを Oracle Internet Directory と同期化させる場合の簡単な構成

Oracle Identity Management のディレクトリの論理編成の計画では、次の計画を実行します。

- ディレクトリ情報ツリー（DIT）全体の構造計画
- ユーザーおよびグループのディレクトリの格納およびネーミングの計画
- 認証管理レルムの計画

図 19-4 に、ディレクトリ情報ツリーにおけるこれらの手順を示します。

図 19-4 ディレクトリ情報ツリーの計画

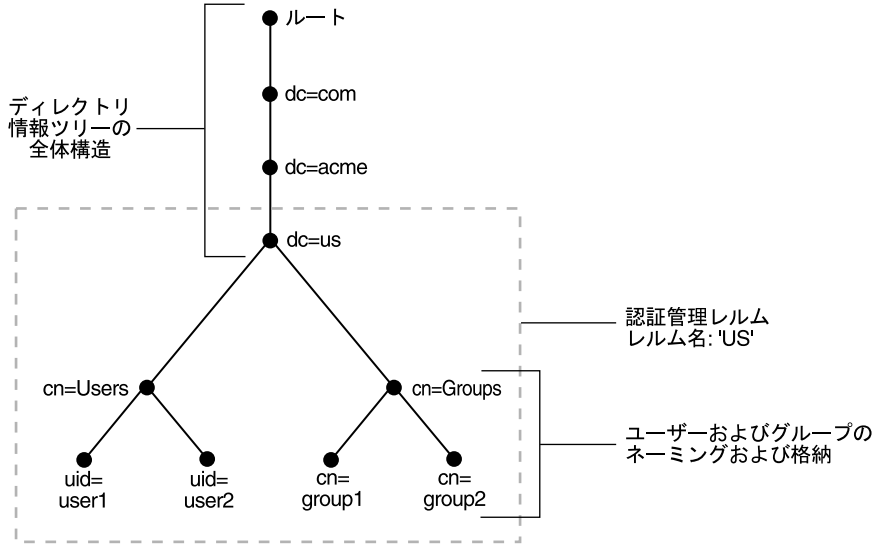


図 19-4 は、米国内の配置でのディレクトリの論理編成に関して次の事項を決定している Acme という仮想の会社について説明しています。

- ドメイン名ベースのスキームは、ディレクトリ情報ツリー階層全体を表す。認証管理インフラストラクチャが us ドメイン内で展開されるため、dc=us,dc=acme,dc=com がディレクトリ情報ツリーのルートとなる。
- 選択したネーミング・コンテキスト内部では、すべてのユーザーが cn=users というコンテナの下に表示される。このコンテナ内部では、すべてのユーザーが同一レベルで表示される。組織ベースの階層は存在しない。また、すべてのユーザーの一意の識別子として uid 属性を選択する。
- 選択したネーミング・コンテキスト内部では、すべての企業グループが cn=groups というコンテナの下に表示される。このコンテナ内部では、すべての企業グループが同一レベルで表示される。すべてのグループ・エントリのネーミング属性を cn とする。
- コンテナ dc=us を、認証管理レルムのルートとして選択する。この場合、レルムの名前は us とする。配置では、us レルムの範囲に該当するすべてのユーザーに対して、同様のセキュリティ・ポリシーを施行することを想定する。

この項では、ディレクトリ情報の論理編成を設計する場合の考慮事項の詳細を説明します。次の項目について説明します。

- ディレクトリ構造全体の計画
- ユーザーおよびグループのネーミングおよび格納の計画
- 認証管理レルムの計画

ディレクトリ構造全体の計画

このタスクでは、企業内のすべての認証管理統合アプリケーションで使用される基本的なディレクトリ情報ツリーを設計します。この設計を行う場合は、次の考慮事項に注意してください。

- ディレクトリ編成によって、明確で効果的なアクセス制御が簡単に実行できるようになる必要があります。完全レプリケーションまたは部分レプリケーションのいずれかのレプリケーションを計画した場合、ディレクトリ・レプリケーションに対して適切な境界およびポリシーを施行できるのは、ディレクトリ情報ツリーが分離するように設計された場合のみです。
- サード・パーティのディレクトリ・サーバーとの統合を行う企業では、Oracle Internet Directory のディレクトリ情報ツリーの設計と既存のディレクトリ情報ツリーを一致させることをお薦めします。この考慮事項は、現在 Oracle Internet Directory を展開し、後で別のディレクトリ（マイクロソフト社のソフトウェアの操作に必要な Microsoft Active Directory など）を展開する配置にも該当します。いずれの場合でも、サード・パーティのディレクトリ情報ツリーの設計とより一貫性のある Oracle Internet Directory のディレクトリ情報ツリーの設計を採用すると、Oracle Delegated Administration Services および他の中間層アプリケーションを使用した、ユーザー・オブジェクトおよびグループ・オブジェクトの管理をより簡単にできます。
- 単一企業の使用例では、企業の DNS ドメイン名と一致するディレクトリ情報ツリー設計を選択すると、十分な結果が得られます。たとえば、`acme.com` というドメイン名を持つ企業で Oracle Internet Directory を設定する場合は、`dc=acme,dc=com` というルートを持つディレクトリ構造を使用することをお薦めします。部門または組織レベルのドメイン・コンポーネント（`engineering.acme.com` の `engineering` など）は使用しないことをお薦めします。
- X500 ディレクトリ・サービスを使用し、他のサード・パーティの LDAP ディレクトリが本番環境に存在しない企業では、国ベースのディレクトリ情報ツリー設計を選択することをお薦めします。たとえば、`o=acme, c=US` というルートを持つディレクトリ情報ツリー設計は、すでに X.500 ディレクトリ・サービスを使用している企業に適しています。

- ディレクトリは、Oracle およびサード・パーティの複数のアプリケーションで使用できるため、ディレクトリ情報ツリーの構造全体を構成する相対識別名（RDN）で使用されるネーミング属性を、予約済属性に制限する必要があります。通常、次の属性は、ほとんどのディレクトリ対応アプリケーションで予約済です。
  - c: 国の名前
  - dc: DNS ドメイン名のコンポーネント
  - l: 地域（都市、国、その他の地域など）の名前
  - o: 組織の名前
  - ou: 組織単位の名前
  - st: 州またはその他の地方行政区画の名前
- 企業の部門構造または組織構造のいずれかを反映してディレクトリ情報ツリーを設計するのは、よくある間違いです。ほとんどの企業が組織および部門の再編成を頻繁に行うため、この方法はお薦めしません。企業のディレクトリは、できるかぎり組織変更とは無関係にしておくことが重要です。

ユーザーおよびグループのネーミングおよび格納の計画

ディレクトリ情報ツリー設計全体に適用される設計に関するほとんどの考慮事項は、ユーザーおよびグループのネーミングと格納にも適用されます。この項では、Oracle Internet Directory でユーザーおよびグループのモデリングを行う場合の追加の考慮事項について説明します。

ユーザーに関する考慮事項

Oracle Identity Management インフラストラクチャでは、すべてのユーザーの識別情報のリポジトリとして Oracle Internet Directory を使用します。企業内の複数のアプリケーションにアクセスするアカウントを持つユーザーの場合も、そのユーザーの識別情報を示すエントリは Oracle Internet Directory 内に 1 つのみです。ディレクトリ情報ツリー全体でのこれらのエントリの位置と内容は、Oracle Internet Directory および Oracle Identity Management インフラストラクチャの他のコンポーネントを配置する前に計画する必要があります。

- 前述のとおり、所属部門の関係や階層に基づいてユーザーを編成する傾向があります。ただし、ほとんどの企業は組織および部門の再編成を頻繁に行うため、この方法はお薦めしません。個人のディレクトリ・エントリの属性として個人の組織情報を捉えると、管理しやすくなります。
- 部門関係や管理系統に基づいた階層でユーザー編成を行った場合、パフォーマンスは向上しません。ユーザーを格納するディレクトリ情報ツリーは、できるかぎり浅い階層にしておくことをお薦めします。

- 配置に様々なユーザーの集団が含まれ、それぞれの集団が異なる組織によってメンテナンスおよび管理される場合は、それらの管理境界に基づいてユーザーをいくつかのコンテナに分けることをお薦めします。これによって、アクセス制御の設定が簡単になり、レプリケーションが必要になった場合に役立ちます。
- 検索操作でユーザーを一意に識別するためのデフォルトのニックネーム属性は、uid です。これはログインで使用するデフォルトの属性です。識別名を構成するためのデフォルトのネーミング属性は、cn です。
- 通常、ほとんどの企業には、従業員に一意の名前と番号を割り当てる規則を定める人事部門があります。ディレクトリ・エントリに対して一意のネーミング・コンポーネントを選択する場合、この管理インフラストラクチャを活用し、そのポリシーを使用するのが有効です。
- ディレクトリ内に作成するすべてのユーザー・エントリは、inetOrgPerson および orclUserV2 というオブジェクト・クラスのメンバーである必要があります。
- サード・パーティのディレクトリがすでに存在する場合、または統合する予定がある場合は、ユーザーのネーミングとディレクトリの格納を、後で発生する分散ディレクトリの管理と合わせることをお薦めします。

注意： Oracle Internet Directory リリース 9.0.2 では、nickname 属性のデフォルト値は cn でした。リリース 9.0.4 以上では、この属性のデフォルト値は uid です。

グループに関する考慮事項

Oracle Identity Management インフラストラクチャと統合されたアプリケーションの一部では、Oracle Internet Directory での配置によって作成された企業全体にわたるグループに基づいて認可を行うこともできます。ユーザー・エントリ同様、これらのグループ・エントリの位置と内容も慎重に計画する必要があります。グループ設計時の考慮事項は、次のとおりです。

- 部門関係や所有権に基づいた階層で企業グループ編成を行った場合、パフォーマンスは向上しません。グループを格納するディレクトリ情報ツリーは、できるかぎり浅い階層にしておくことをお薦めします。これによって、すべてのアプリケーションによるグループの検出が簡単になり、アプリケーション間でのこれらのグループの共有が促進されます。
- エントリの各セットに個別の管理ポリシーを適用できるように、ディレクトリ情報ツリー内のユーザーおよびグループを分けることをお薦めします。
- グループを一意に識別するには、cn または CommonName 属性を使用する必要があります。

- 企業がディレクトリ内に作成するすべてのグループは、groupOfUniqueNames および orclGroup というオブジェクト・クラスに属している必要があります。前者のオブジェクト・クラスは、グループを表すインターネット標準です。後者のオブジェクト・クラスは、Oracle Internet Directory セルフ・サービス・コンソールを使用してグループを管理する場合に有効です。
- 企業全体にわたるグループごとに新しいディレクトリ・アクセス制御を作成するのではなく、次のように対応することを検討してください。
  1. グループの owner 属性を使用して、グループの所有者であるユーザーを示します。
  2. owner 属性で示されたすべてのユーザーに、様々な操作を実行する特別な権限を付与する上位レベルのアクセス制御ポリシーを作成します。
- description 属性には、グループの目的をユーザーが理解できるように情報を書き込みます。
- オブジェクト・クラス orclGroup での displayName 属性の使用を検討します。これによって、Oracle Delegated Administration Services および Oracle Internet Directory セルフ・サービス・コンソールで、読みやすいグループ名を表示できます。
- 様々なグループのセットがあり、それぞれのセットが独自の管理ポリシーを持つ異なる組織によってメンテナンスおよび管理される場合は、それらの管理境界に基づいてグループをいくつかのコンテナに分けます。これによって、アクセス制御の設定が簡単になります。また、レプリケーションが必要な場合にも役立ちます。
- サード・パーティのディレクトリがすでに存在する場合、または将来それを統合する場合は、Oracle Internet Directory でのグループのネーミングとディレクトリの格納を、サード・パーティのディレクトリ内で使用されるものと一致させます。これによって、分散ディレクトリの同期化およびそれ以降の管理が簡単になります。

認証管理レルムの計画

前述の項では、ディレクトリ情報ツリー全体および配置対象のユーザーとグループの配置を構成する場合のガイドラインを示しました。これらのガイドラインを実装すると、膨大な数の配置構成を行うことになるため、配置の目的をディレクトリ自体にメタデータとして取得する必要があります。Oracle Identity Management インフラストラクチャに依存する Oracle ソフトウェアおよびサード・パーティのソフトウェアは、このメタデータによって配置の目的を認識し、カスタマイズされた環境で正常に機能できます。

Oracle Internet Directory では、配置の目的は、認証管理レルムに取得されます。このレルムは、前述の項で配置について説明したユーザーおよびグループに対して、認証管理ポリシーを設定する場合にも役立ちます。

認証管理レルムは、ディレクトリ内の適用範囲が明確な領域で、次の要素で構成されています。

- 適用範囲が明確な企業識別情報の集合（米国内のすべての従業員など）
- これらの識別情報に関連付けられた認証管理ポリシーの集合
- 認証管理ポリシーを設定しやすくするグループの集合（識別情報の集約）

ディレクトリ情報ツリー全体の構造およびユーザーとグループの配置を決定した後、認証管理レルムのルートとして機能するディレクトリ・エントリを識別する必要があります。このエントリによって、レルムに定義された認証管理ポリシーの施行範囲が決まります。デフォルトでは、認証管理レルムのルート下のディレクトリ・サブツリー全体が、この認証管理ポリシーの施行範囲になります。このエントリの下に、`OracleContext` という特別なエントリが作成されます。このエントリには、次の情報が含まれます。

- ユーザーおよびグループのネーミングおよび配置などの配置固有のディレクトリ情報ツリー設計（前述の項を参照）
- このレルムに関連付けられた認証管理ポリシー
- Oracle アプリケーション特有のレルム固有の追加情報

認証管理レルムを計画する場合は、次のことを考慮します。

- 企業のセキュリティ要件に基づいて、認証管理レルムのルートを選択する必要があります。通常、ほとんどの企業で必要なレルムは 1 つのみです。ただし、個別の認証管理ポリシーを使用して複数のユーザー集団を管理するときは、複数のレルムが必要になる場合があります。
- サード・パーティのディレクトリがすでに存在する場合、または将来それを統合する場合は、選択した認証管理レルムのルートを、サード・パーティのディレクトリのディレクトリ情報ツリー設計と一致させます。これによって、分散ディレクトリの同期化およびそれ以降の管理が簡単になります。
- 認証管理レルムを構成し管理するには、Oracle Internet Directory で提供される管理ツールを使用します。これらのツールには、Oracle Internet Directory セルフ・サービス・コンソール、コマンドライン・ツールなどが含まれます。
- Oracle Internet Directory ツールを使用して認証管理レルムを構成した後、配置によって行われたカスタマイズを反映するために、ディレクトリのネーミングおよび格納ポリシーの更新を計画します。この更新は、Oracle Identity Management インフラストラクチャを使用する他の Oracle コンポーネントをインストールして使用する前に行う必要があります。

図 19-5 に、Acme という会社の認証管理レルムの例を示します。

図 19-5 認証管理レルムの例

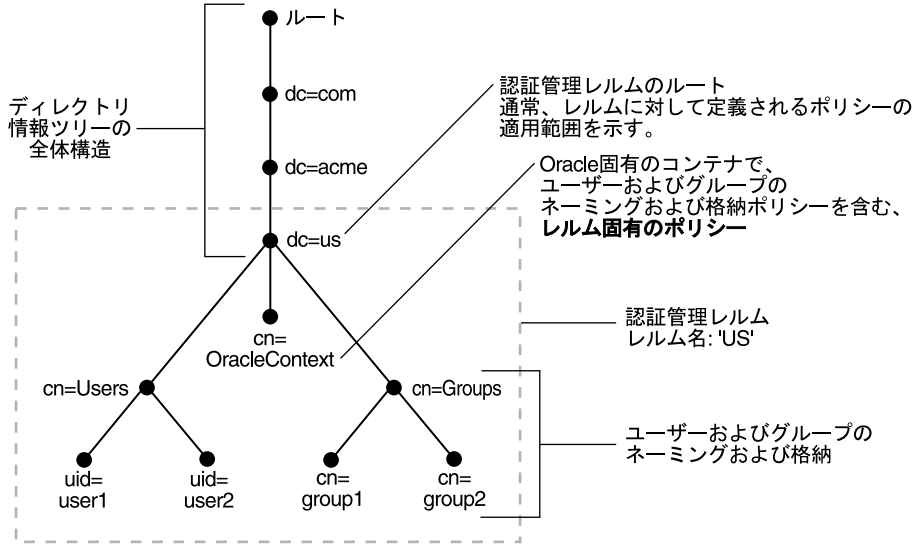


図 19-5 の例は、ドメイン名ベースのディレクトリ情報ツリー構造を使用する配置になっています。この場合、コンテナ dc=us,dc=acme,dc=com が、認証管理レルムのルートとして選択されています。その結果、デフォルトで、適用範囲が dc=us エントリ下のディレクトリ・サブツリー全体に限定される新しい認証管理レルムが作成されます。認証管理レルムの名前は US です。

デフォルトのディレクトリ情報ツリーおよび認証管理レルム

構成を簡単にするために、Oracle Internet Directory のインストール時に、デフォルトのディレクトリ情報ツリーが作成され、デフォルトの認証管理レルムが設定されます。オプションで、Oracle Internet Directory をインストールするコンピュータのドメインに基づいて、ディレクトリ情報ツリーを設定することもできます。たとえば、oidhost.us.mycompany.com というコンピュータにインストールすると、デフォルトの認証管理レルムのルートは dc=us,dc=mycompany,dc=com となります。Oracle Internet Directory によって、次のものが作成されます。

- デフォルトの認証管理レルムに関連付けられた Oracle コンテキスト。Oracle コンテキストには、レルム固有のすべてのポリシーとメタデータが格納されます。前述の例の場合は、cn=OracleContext,dc=us,dc=mycompany,dc=com という識別名を持つ Oracle コンテキストが作成されます。このエントリとその下にあるノードによって、Oracle ソフトウェアはレルム固有のポリシーと設定を検出できます。

- デフォルトの認証理レルムでのディレクトリ構造およびネーミング・ポリシー。これによって、Oracle コンポーネントが様々な識別情報を検索できるようになります。これらのデフォルト値は、次のとおりです。
  - すべてのユーザーは、認証管理レルムのベースの下にあるコンテナ cn=users に配置されます。この例では、cn=users,dc=us,dc=mycompany,dc=com がこのコンテナです。
  - Oracle Identity Management インフラストラクチャを使用して認証管理レルム内に作成した新規ユーザーは、コンテナ cn=users の下にも作成されます。
  - Oracle Identity Management インフラストラクチャを使用して認証管理レルム内に作成したすべての新規ユーザーは、オブジェクト・クラス orclUserV2 および inetOrgPerson に属します。
  - すべてのグループは、認証管理レルムのベースの下にあるコンテナ cn=groups に配置されます。この例では、cn=groups,dc=us,dc=mycompany,dc=com がこのコンテナです。
- 認証管理レルム管理者。cn=orcladmin と呼ばれるこのユーザーは、ユーザー・コンテナの下に配置されます。この例では、ブートストラップ・ユーザーの完全修飾された識別名は cn=orcladmin,cn=users,dc=us,dc=mycompany,dc=com です。
- 認証サービスで適切な処理を実行できるようにするデフォルトの認証ポリシー。次のポリシーが含まれます。
  - デフォルトのディレクトリ・パスワード・ポリシー（パスワードの長さ、ロックアウト、有効期限など）
  - ユーザーのプロビジョニングを行う際に自動生成される必要がある追加のパスワード・ベリファイア
- 認証管理の権限。これらの権限は、Oracle Internet Directory によって、Oracle Internet Directory セルフ・サービス・コンソールを介してこれらの権限を委任できるブートストラップ・ユーザーに付与されます。これらの権限の例は、次のとおりです。
  - 共通の認証管理操作権限（ユーザーの作成、ユーザー・プロファイルの変更、グループの作成など）
  - Oracle Identity Management インフラストラクチャを使用して新しい Oracle コンポーネントをインストールする権限
  - Oracle Internet Directory セルフ・サービス・コンソールを管理する権限

関連項目：

- `orclUserV2` オブジェクト・クラスの詳細は、17 ページの「orclUserV2 オブジェクト・クラスのオプション属性」を参照してください。
- Oracle Identity Management におけるデフォルトのアクセス制御ポリシーの詳細は、第 17 章「Oracle テクノロジ配置のための権限の委任」を参照してください。

認証管理レルムの管理

この項では、認証管理レルムに対して実行できる様々な管理タスクについて説明します。この項では、次の項目について説明します。

- 認証管理レルムのカスタマイズ
- 認証管理レルムの追加作成

認証管理レルムのカスタマイズ

レルムを作成した後、様々な要素をカスタマイズできます。表 19-2 に、カスタマイズできる要素、各種のカスタマイズで使用可能なツールおよび参照先を示します。

表 19-2 既存レルムのカスタマイズ

カスタマイズ可能な対象	ツール	情報
ディレクトリ構造およびネーミング・ポリシー	Oracle Delegated Administration Services Oracle Directory Manager コマンドライン・ツール	19-5 ページの「認証管理を行うためのディレクトリ情報ツリーの計画」 31-4 ページの「Oracle Internet Directory セルフ・サービス・コンソールの使用」
認証ポリシー	Oracle Directory Manager コマンドライン・ツール	第 15 章「Oracle Internet Directory のパスワード・ポリシー」
認証管理の権限	Oracle Delegated Administration Services Oracle Directory Manager コマンドライン・ツール	第 17 章「Oracle テクノロジ配置のための権限の委任」 31-4 ページの「Oracle Internet Directory セルフ・サービス・コンソールの使用」

注意： レルムを使用する Oracle コンポーネントをインストールする前に、必ずすべてのカスタマイズを完了してください。Oracle コンポーネントを配置した後、レルムのプロパティを変更すると、予測できない結果になる場合があります。

関連項目： Oracle Application Server Single Sign-On と統合している場合、『Oracle Application Server Single Sign-On 管理者ガイド』のディレクトリ変更を伴う Single Sign-On Server の更新に関する項を参照してください。

認証管理レルムの追加作成

Oracle Internet Directory セルフ・サービス・コンソールを使用して、認証管理レルムを追加作成できます。

注意： 複数の認証管理レルムでは、動作しないアプリケーションもあります。

レルムを追加する場合は、追加したレルムが既存アプリケーションで認識されるように手動で設定する必要があります。詳細は、アプリケーション固有のマニュアルを参照してください。

Oracle Identity Management インストラクチャでは、Single Sign-On Server に対し特別な管理手順で追加レルムが認識されるようにする必要があります。Oracle Application Server Single Sign-On で複数のレルムを使用可能にする手順については、『Oracle Application Server Single Sign-On 管理者ガイド』の複数レルムでの Single Sign-On に関する項を参照してください。

関連項目： 31-13 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用した認証管理レルムの作成」

20

ディレクトリの容量計画

容量計画は、アプリケーションのディレクトリ・アクセス要件を評価し、許容速度で要求を処理するための十分なコンピュータ・リソースが Oracle Internet Directory にあることを確認するプロセスです。この章では、容量計画を行うときに考慮する必要がある項目について説明します。Acme Corporation という仮想の会社における、電子メール・メッセージ・アプリケーションのディレクトリ配置例を使用して説明します。

この章では、次の項目について説明します。

容量計画の説明

Oracle Internet Directory とそれに対応する Oracle9*i* データベースが同じコンピュータ上で実行されている場合、容量計画の担当者が考慮する必要がある設定可能なリソースは次のとおりです。

- I/O サブシステム（タイプとサイズ）
- メモリー
- ネットワーク接続性
- CPU（スピードと数量）

Oracle Internet Directory 用のハードウェアを調達する場合は、すべてのコンポーネント（CPU、メモリー、I/O など）が、効果的に使用されることを確認してください。一般的に、適切なメモリーの使用と堅固な I/O サブシステムによって、CPU をビジー状態に保つことができます。

Oracle Internet Directory の新規インストール時には、次の 2 つの事項が整っている必要があります。

- インストールされたシステムに、負荷率のピーク時にユーザーの要求を満たすための十分なハードウェア・リソースが用意されていること。
- 使用可能なリソースを最大限に活用し、使用可能なハードウェアから最大のパフォーマンスを引き出すために適切にチューニングされたシステム（ハードウェアおよびソフトウェア）が用意されていること。

Acme Corporation という仮想の会社における、電子メール・メッセージ・アプリケーションのディレクトリ配置例を考察します。容量計画の各コンポーネントを検証し、Acme Corporation の例に対して推奨事項を適用していきます。

この章では次の用語が使用されます。

- スループット

  Oracle Internet Directory がディレクトリ操作を完了する包括的な率。通常、操作 / 秒（1 秒当りの操作件数）で表されます。

- 待機時間

  指定したディレクトリ操作が完了するまでのクライアントの待機時間。

- 同時クライアント

  Oracle Internet Directory とのセッションを確立しているクライアントの総数。

- 同時操作

  すべての同時クライアントの要求に基づいてディレクトリで実行されている同時操作の数。一部のクライアントではセッションがアイドル状態の可能性があるため、この数は同時クライアントの数と必ずしも同じではありません。

ディレクトリの使用パターンの理解 : 事例

Oracle Internet Directory の潜在的な負荷を評価することは、正確な容量計画を作成するために非常に重要です。Acme Corporation という仮想の会社で利用されている電子メール・メッセージ・ソフトウェアについて検証します。この例の電子メール・メッセージ・ソフトウェアは、Internet Message Access Protocol（IMAP）をベースにしています。Oracle Internet Directory にアクセスする主要なソフトウェアには、次の 2 種類があります。

- IMAP クライアント。IMAP サーバーにメールを送信する前に、会社内の電子メール・アドレスを検証します。このクライアントには、Netscape Messenger や Microsoft Outlook などのソフトウェア・プログラムが組み込まれています。
- メッセージ・ソフトウェア。メール転送エージェント（MTA）とも呼ばれます。ディレクトリを調べて、社内メールを会社全体の配布リストに送信し、外部からのメールを社内のメールボックスに送信します。

個々のユーザーのプライベート・エイリアスとプライベート配布リストもディレクトリに格納されていると仮定します。さらに、次の仮定を設けて、ディレクトリのサイズを推測できるようにします。

表 20-1 エントリのタイプとサイズについての前提事項

エントリ・タイプ	サイズ
ユーザー数の合計	40,000
ユーザーごとのプライベート・エイリアスの平均数	10
ユーザーごとのプライベート配布リストの平均数	10
パブリック配布リストの合計数	4000
社内におけるパブリック・エイリアスの合計数	1000
このアプリケーションに関連しているディレクトリ内の各エントリにある属性数	20
カタログ化属性の数	10

前述の仮定に基づくと、Oracle Internet Directory における全体的なエントリ件数は、次のように算出できます。

表 20-2 全体的なエントリ件数

エントリ・タイプ	サイズ
ユーザー・エントリ	40,000（このエントリはユーザー自身を表しています）
ユーザーのプライベート・エイリアス	40,000 × 10 = 400,000 エントリ
ユーザーのプライベート配布リスト	40,000 × 10 = 400,000 エントリ
会社全体の配布リスト	4000
会社全体のエイリアス	1000

前述の仮定から、ディレクトリに存在するエントリは約 100 万件であることがわかります。ユーザー数とディレクトリに存在するエントリ数が与えられたとして、パフォーマンス要件を導出するために、使用パターンを分析してみます。一般的なユーザーは、毎日平均 10 通の電子メールを送信し、外部から 1 日に平均 10 通の電子メールを受信します。ユーザーが送信する各メールに対して、平均 5 人の受信者がいると仮定すると、各メールごとに 5 回ずつディレクトリ参照が行われます。

次の表は、1 日に発生する可能性があるすべてのディレクトリ参照回数を要約したものです。

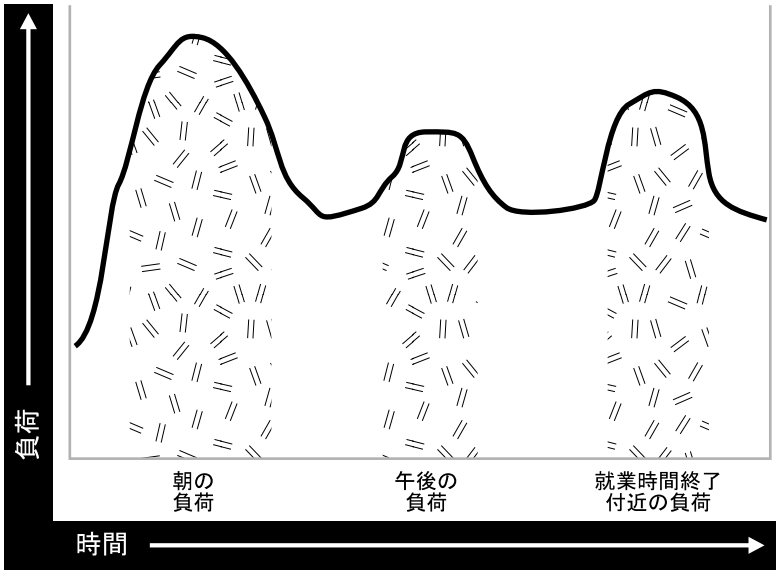
表 20-3 1 日のディレクトリ参照の数

ディレクトリ参照のタイプ	1 日のディレクトリ参照の数
各ユーザーからの送信メールを処理するメール転送エージェント（MTA）	5 × 10 × 40,000 = 2,000,000
外部からのメールを処理する MTA	10 × 40,000 = 400,000
その他のすべてのディレクトリ参照（IMAP クライアントによる特定のアドレスの検証など）	800,000

合計すると、毎日のディレクトリ参照の総数は約 3,200,000（320 万）となります。このディレクトリ参照が 1 日の範囲内で均一に分配されたとすると、毎秒約 37 ディレクトリ参照（毎時約 133,333 参照）が行われる必要があります。ただし、このように均一に分配されることは実際にはありません。

現行の電子メール・システムの使用状況を 24 時間にわたって分析すると、そのパターンは図 20-1 のようになります。

図 20-1 現行電子メール・システムの使用状況の分析



電子メール・システムおよび Oracle Internet Directory に最も負荷がかかるのは朝の時間帯です。その他に、昼食時と就業時間終了付近にもピークがあります。しかし、Oracle Internet Directory に最も負荷がかかるのは朝の時間帯です。

全ディレクトリ参照の 90 パーセントが通常の勤務時間内に発生すると仮定します。次に、1 日 8 時間の勤務時間内の負荷を次のカテゴリに分割します。

表 20-4 勤務時間内の負荷

負荷の時間帯	参照回数
朝の負荷	65%: 0.90 × 0.65 × 3,200,000 = 1,872,000 参照 /2 時間（936,000 参照 / 時）
昼食時の負荷	10%: 0.90 × 0.10 × 3,200,000 = 288,000 参照 /1 時間（288,000 参照 / 時）
就業時間終了付近の負荷	20%: 0.90 × 0.20 × 3,200,000 = 576,000 参照 /2 時間（288,000 参照 / 時）

これらの計算結果により、この場合の Oracle Internet Directory は、ピーク時の負荷である 1 時間当り 936,000 の参照を処理するように設計する必要があることが示されています。

データ・セットのサイズとパフォーマンス要件について理解したため、インストールの個々のコンポーネントを調べ、それぞれについて適切な値を見積もることができます。

I/O サブシステムの要件

この項では、次の項目について説明します。

I/O サブシステムの説明

I/O サブシステムは、CPU が負荷となる作業を実行できるように、CPU にデータを送り出すポンプにたとえることができます。I/O サブシステムには、データ記憶域を管理する役割もあります。I/O サブシステムの主なコンポーネントは、ディスク・コントローラによって制御される一連のディスク・ドライブです。

I/O サブシステムのサイズを決めるときは、記憶要件のみに基づいたサイズではなく、パフォーマンス要件を考慮することが重要です。ディスク・ドライブのサイズは増加していますが、スループット（ディスク・ドライブがデータを送り出す速度）は、比例して増加していません。I/O サブシステムのサイズを計算するときには、情報として次の要因を考慮する必要があります。

- データベースのサイズ
- システム上の CPU の数
- Oracle Internet Directory の作業負荷の初期見積り
- ディスクがデータを送出できる速度
- ロード前のデータ準備に必要な領域
- 索引作成とソート作業に必要な領域

様々な I/O サブシステムがある場合は、常にスループットが最大のドライブを選択してください。一般的に、次の技術を 1 つ以上使用すると、I/O スループットを最大にできます。

- I/O 操作で複数のディスク・スピンドルを使用するために、論理ボリュームをストライプ化
- 異なる表領域を、異なる論理ディスク・ボリュームと物理ディスク・ボリュームに格納
- ディスク・ボリュームを複数の I/O 制御装置に分散

Oracle Internet Directory 固有のデータ・ファイルを適切に動作させる方法のガイドラインは、第 21 章「ディレクトリのチューニングに関する考慮事項」を参照してください。ディスク障害の許容度によっては、異なるレベルの Redundant Arrays of Inexpensive Disks（RAID）を考慮することもできます。

可能なかぎり最良の I/O サブシステムを用意する決定が行われたと仮定して、次にディスク自体のサイズ設定を見積ります。

ディスク領域要件の概算

次の表を使用すると、全般的なディスク要件を概算で見積もることができます。

表 20-5　ディスク領域要件

ディレクトリ情報ツリー内のエントリ数	ディスク要件
100,000	450MB ～ 650MB
200,000	850MB ～ 1.5GB
500,000	2.5GB ～ 3.5GB
1,000,000	4.5GB ～ 6.5GB
1,500,000	6.5GB ～ 10GB
2,000,000	9GB ～ 13GB

この表のデータから、次の仮定が導出されます。

- カタログ化属性が約 20 個であること
- 各エントリの属性が約 25 個であること
- 属性の平均サイズが約 30 バイトであること

Acme Corporation の例に戻ると、ディレクトリに存在するエントリ数は約 100 万であるため、ディスク要件はおよそ 4.5GB ～ 6.5GB となります。カタログ化属性の数に関して Acme Corporation に設定した仮定は異なりますが、前述の表からサイズ要件の概算値を導出できます。

ディレクトリは、様々なアプリケーションに幅広く配置されている可能性があるため、これらの仮定は、考えられる状況すべてに対して必ずしも真である必要はありません。属性のサイズが大きい場合、エントリごとの属性の数が多い場合、アクセス制御情報アイテム（ACI）が広範囲で使用されている場合、またはカタログ化属性の数が非常に多い場合など、様々な状況が考えられます。このような場合の簡単な計算方法を、次項で提示します。この方法によって、計画担当者はディスク要件を詳細に把握できます。

ディスク領域要件の詳細な計算

Oracle Internet Directory はすべてのデータを Oracle9*i* データベースに格納するため、ディスク領域のサイズ設定では、主に基礎となるデータベースのサイズを設定します。Oracle Internet Directory は、データを次の表領域に格納します。

表 20-6 Oracle Internet Directory データを格納するために使用する表領域

表領域名	内容
OLTS_ATTR_STORE	ディレクトリ情報ツリー内にある全エントリのすべての属性を格納。
OLTS_CT_STORE	その他のすべてのカタログ（ユーザー定義カタログを含む）およびカタログに定義されている索引を格納。
OLTS_DEFAULT	Oracle Internet Directory の管理に関連するデータとレプリケーション・サポートに使用するデータをすべて格納。
OLTS_SVRMGSTORE	Oracle Internet Directory サーバー管理機能に必要なすべての表と索引を格納。
SYSTEM	各種の記録保持の目的で、Oracle9*i* データベースに必要。通常、このサイズは約 300MB で一定です。

この項では、前述の表に示した各表領域のサイズ要件を決定するための簡単な計算方法を提示します。すべてのサイズの計算は、次の変数に基づいて行われます。

表 20-7 サイズ計算に使用する変数

変数名	説明
num_entries	ディレクトリ内のエントリの合計数。
attrs_per_entry	ディレクトリ・エントリごとの属性の平均数。
avg_attr_size	属性値の平均サイズ（バイト）。
avg_dn_size	属性の識別名の平均サイズ（バイト）。
objectclass_per_entry	エントリが属しているオブジェクト・クラスの平均数。
objectclass_size	各オブジェクト・クラス名の平均サイズ（バイト）。
num_cataloged_attrs	エントリ内で使用されているカタログ化属性の数。
entries_per_catalog	カタログ表ごとのエントリの平均数。ディレクトリ情報ツリー内の全エントリにカタログ化属性が存在しているとはかぎらないため、この変数は必須です。
change_log_capacity	レプリケーション目的のためにバッファする変更の数。
num_acis	ディレクトリ内の ACI の全体数。

表 20-7 サイズ計算に使用する変数（続き）

変数名	説明
num_auditlog_entries	ディレクトリに格納する監査ログ・エントリの数。
db_storage_ovhd	表にデータを格納するときのオーバーヘッド。このオーバーヘッドは、オペレーティング・システム固有のオーバーヘッドと同時に、関係する構造体にも該当します。この変数の値が 1.3 の場合は、30% のオーバーヘッドがあることを示しています。この変数の最小値は 1 です。
db_index_ovhd	索引にデータを格納するときのオーバーヘッド。このオーバーヘッドは、オペレーティング・システム固有のオーバーヘッドと同時に、関係する構造体にも該当します。この変数の値が 5 の場合は、400% のオーバーヘッドがあることを示しています。この変数の最小値は 1 です。
factor_of_safety	データ量の増加および計算誤差に対応するための乗数。この変数の値が 1.3 の場合は、安全係数が 30% であることを示しています。この変数の最小値は 1 です。
initial_num_entries	ディレクトリに最初にバルク・ロードされるエントリの合計数。
avg_attrname_len	属性名の平均サイズ（バイト）。
num_stats_entries	ホスト DSF 属性 orclstatsflag が使用可能な場合に、OID サーバー管理機能によって生成される統計エントリの数。
attrs_per_stats_entry	統計エントリごとの属性の平均数。

表 20-7 に示す変数を使用すると、個々の表領域のサイズを次のように計算できます。

表 20-8 個々の表領域のサイズ

表が含まれている表領域	式
ATTRSTORE_INDEX_SIZE	num_entries*(attrs_per_entry+6) *10
CATALOG_INDEX_SIZE	entries_per_catalog*num_cataloged_attrs*avg_attr_size*db_index_ovhd +num_entries*objectclass_per_entry*objectclass_size*db_index_ovhd + num_acis*1.5*avg_dn_size*db_index_ovhd + num_auditlog_entries*2*avg_dn_size*db_index_ovhd
CN_SIZE	num_entries*avg_dn_size*db_storage_ovhd
DN_INDEX_SIZE	num_entries*2*(avg_dn_size * 3)
DN_SIZE	num_entries*2*(avg_dn_size+4)
OBJECTCLASSES_SIZE	num_entries*objectclass_per_entry*objectclass_size*db_storage_ovhd + num_auditlog_entries*2*avg_dn_size*db_storage_ovhd

表 20-8 個々の表領域のサイズ（続き）

表が含まれている表領域	式
OLTS_ATTR_STORE	(num_entries*(((attrs_per_entry)*(avg_attrname_len+avg_attr_size+22))+6*35)*db_storage_ovhd)+attrstore_index_size
OLTS_BATTRSTORE	6M+(((num_binary_attrs*avg_binval_length)+6*35)*db_storage_ovhd)
OLTS_CT_STORE	(cn_size+objectclasses_size+dn_size+catalog_index_size+dn_index_size)
OLTS_DEFAULT	(change_log_capacity*4*avg_attr_size*db_storage_ovhd*db_index_ovhd) + (initial_num_entries*2*(avg_dn_size+4))
OLTS_SVRMGSTORE	2M+num_stats_entries*((avg_attrname_len+avg_attr_size+20)*(2*attrs_per_stats_entry)*db_storage_ovhd*(orclstatsperiodicity/10)*12)
SYSTEM	300MB

この表の計算式は、Oracle Internet Directory の広範囲にわたる様々な配置例についての正確な領域要件を計算するために使用します。各表領域のサイズを合計すると、データベース全体のディスク要件がわかります。オプションで、その値に factor_of_safety 変数を乗算すると、予期せぬ事態にも対処可能な数値を算出できます。

Acme Corporation の例に戻り、前項に記述されている要件に基づいて各変数に値を代入します。次の表は、この項で紹介した各変数に、Acme Corporation の値を代入したものです。

表 20-9 サイズ計算に使用する変数の値

変数名	値
num_entries	1,000,000
attrs_per_entry	20
avg_attr_size	32 バイト
avg_dn_size	40 バイト
objectclass_per_entry	5（各エントリが平均 5 つのオブジェクト・クラスに所属）
objectclass_size	10 バイト
num_cataloged_attrs	10
entries_per_catalog	1,000,000
change_log_capacity	80,000 の変更（ユーザーごとに 2 つの変更）
num_acis	80,000 の ACI（ユーザーごとに 2 つの ACI）
num_auditlog_entries	1000
db_storage_ovhd	1.4（40% のオーバーヘッド）

表 20-9 サイズ計算に使用する変数の値（続き）

変数名	値
db_index_ovhd	5.0（400% のオーバーヘッド）
factor_of_safety	1.5（50% の安全係数）
initial_num_entries	1,000,000
num_stats_entries	5
attrs_per_stats_entry	12
'orclstatsperiodicity'	60（ルート DSE 属性）
avg_attrname_len	6

これらの値を前述の等式に代入すると、次の値が得られます。

表 20-10 表領域のサイズ

表領域名	サイズ（バイト）	サイズ（MB）
OLTS_ATTRSTORE	2,223,000,000	2182
OLTS_CT_STORE	2,328,512,000	274
OLTS_DEFAULT	159,680,000	156
OLTS_SVRMGSTORE	2,701,568	3
SYSTEM	314572800	300
合計サイズ	5038093862	4920

この表は、Acme Corporation のデータベースの見積りサイズが約 8.25GB であることを示しています。すべてのデータを一括してロードする場合、Oracle Internet Directory の bulkload ツールには、一時ファイルを格納するためにデータベースが使用する追加領域が 30% 必要です。Acme Corporation の場合は、領域要件の合計に約 2.5GB を追加します。

メモリー要件

メモリーは、Oracle Internet Directory などのあらゆるデータベース・アプリケーションが、多数の個別のタスク用に使用します。いずれかのタスクに対するメモリー・リソースが不十分な場合は、CPU の稼働率が低くなり、システム・パフォーマンスが低下します。また、メモリー使用量はデータベースへの同時接続数とディレクトリの同時ユーザー数に比例して増加します。容量計画の目的で、アクティブな接続は、クライアントがディレクトリとのバインドを要求したときに開始し、このバインドが完了したときに終了します。

処理に使用できるメモリーは、システム上の仮想メモリーから供給されます。これは、使用可能な物理メモリーよりもやや大きいメモリーです。全アクティブ・メモリー使用量の合計が、そのシステムで使用可能な物理メモリーを超えると、オペレーティング・システムは、ある程度のメモリー・ページをディスク上に格納する必要があります。この作業をページングと呼びます。使用可能な物理メモリーをはるかに超えるメモリーを使用すると、ページングによってパフォーマンスが低下することがあります。一般的に、物理メモリーの 20% を超えたメモリーは使用しないでください。ページングが発生した場合は、プロセスごとのメモリー使用量を減らすか、または物理メモリーを追加する必要があります。ただし、トレードオフに注意してください。追加できるメモリーには物理的な制限があり、プロセスごとのメモリー使用量を減らすとパフォーマンスが大幅に低下します。

メモリーを主に消費するのは、システム・グローバル領域（SGA）内のデータベース・バッファ・キャッシュおよび OID サーバー・エントリ・キャッシュ（使用可能な場合）です。バッファ・キャッシュおよびエントリ・キャッシュのヒット率を高くするには、各領域に十分なメモリーを割り当てる必要があります。次の計算式は、エントリ・キャッシュ内に 'N' 個のエントリをキャッシュするために必要な RAM の量の概算を示しています。

N * [150+ {attrs_per_entry + 6) * (avg_attrname_len + avg_attr_size + 40) }] * 1.3

> **関連項目：** SGA のチューニングの詳細は、第 21 章「ディレクトリのチューニングに関する考慮事項」を参照してください。

次の表に、異なるディレクトリ構成別に最小メモリー要件を示します。

表 20-11　ディレクトリ構成別最小メモリー要件

ディレクトリのタイプ	エントリ件数	最小メモリー
小	600,000 未満	512MB
標準	600,000 ～ 2,000,000	1GB
大	2,000,001 以上	2GB

Acme Corporation の例では、ディレクトリ内のエントリ数は約 1,000,000（100 万）です。パフォーマンスを最大にするには、2GB を選択してください。

ネットワーク要件

ほとんどの場合、ネットワークがボトルネックとなることはありません。ただし、容量計画の段階では、慎重に考慮する必要があります。クライアントが Oracle Internet Directory とのメッセージ送受信用に十分なネットワーク帯域幅を確保していない場合は、全体的なスループットが非常に低く感じられます。たとえば、毎秒 800 の検索を処理するように Oracle Internet Directory を構成しても、Oracle ディレクトリ・サーバーを実行しているコンピュータへのアクセスに使用できるのが 10Mbps のネットワーク（10-Base-T イーサネット）のみなので、使用可能な帯域幅が 60 パーセントの場合、クライアントは、スループットが毎秒 600 検索操作であると理解します（各検索操作で 1024 バイトがネットワークで移送されると仮定した場合）。次の表に、2 種類の操作（1024 バイトの転送を必要とする操作と 2048 バイトの転送を必要とする操作）について、10Mbps と 100Mbps の 2 つのタイプのネットワークで、帯域幅の使用可能率が異なる場合の最大可能スループット（操作 / 秒）を示します。

表 20-12　2 種類の操作についての最大可能スループット

使用可能な帯域幅（%）	操作 / 秒 1024 バイト		操作 / 秒 2048 バイト	
	10Mbps	100Mbps	10Mbps	100Mbps
30	300	3000	150	1500
40	400	4000	200	2000
50	500	5000	250	2500
60	600	6000	300	3000
70	700	7000	350	3500
80	800	8000	400	4000
90	900	9000	450	4500

場合によっては、クライアントから Oracle ディレクトリ・サーバーへのメッセージ送信時のネットワーク待機時間を考慮することが重要になります。WAN の環境によっては、ネットワーク待機時間が 500 ミリ秒になる場合があり、操作によっては、クライアントがタイムアウトとなる可能性があります。要約すると、各種ネットワーク・オプションがある場合は、常に帯域幅が最大で、待機時間が最短のネットワークを選択することをお薦めします。

Acme Corporation の例では、ピーク時の使用率は 1 時間当り 936,000 参照で、ディレクトリへの参照操作がこの回数実行されます。つまり、毎秒約 260 のディレクトリ操作が実行される必要があります。各操作で 2KB のデータがネットワーク上を転送されると仮定すると、100Mbps のネットワークを使用するか、または 10Mbps のネットワークで最低 60 パーセントの帯域幅を使用する必要があります。100Mbps のネットワークの方が通常待機時間が短いため、10Mbps のネットワークより優先して選択することになります。

CPU 要件

この項では、次の項目について説明します。

- CPU 構成
- CPU 要件の概算
- CPU 要件の詳細な計算

CPU 構成

Oracle Internet Directory に関する CPU のサイズ設定は、ユーザーの作業負荷に直接影響を与えます。CPU 構成は、次の要因によって決まります。

- サポートする同時操作の数。この数は、操作を同時に実行しているユーザー数に直接依存します。
- 各操作の許容待機時間。たとえば、電子メール・アプリケーションの場合、1 操作ごとの待機時間が 100 ミリ秒であることが理想的ですが、多くの場合、500 ミリ秒でも許容範囲内です。

作業負荷の増加に従って、システムに CPU リソースを追加できますが、CPU リソースを追加しても、すべての操作にそのままスケーラビリティがもたらされることはほとんどありません。これは、多くの操作が単に CPU のみに制限されるわけではないためです。このため、すべてのベンダーから一般的に入手可能なパフォーマンス特性（SPECint_rate95 ベースライン）によって、コンピュータの処理能力が分類されます。この数値は、一連の整数テストから導き出され、すべてのシステム・ベンダーおよび SPEC の Web サイト（http://www.spec.org）から入手可能です。

注意： SPECint_rate95 の数値を、通常の SPECint95 のパフォーマンス数値と混同しないでください。SPECint95 のパフォーマンス数値は、特定の CPU の整数処理能力に関する知識を提供します（CPU が複数あるシステムの場合、この数値は通常正規化されます）。SPECint_rate95 は、正規化を実行せずにシステム全体の整数処理能力を提供します。

Oracle Internet Directory は、SMP コンピュータで複数の CPU を効率的に使用しているため、SPECint_rate95 の数値に基づいてコンピュータを分類できます。SPECint_rate95 の範囲では、一般的に公表されている結果と異なるベースラインの数値が選択されています。これは、一般的に公表されている結果が、実際にはコンピュータのピーク時のパフォーマンスであるのに対して、ベースラインの数値は、通常の状況下のパフォーマンスを表しているためです。

CPU 要件の概算

Oracle Internet Directory は、通常 Oracle9*i* データベースと同じマシンに常駐しているため、少なくとも 2CPU のシステムをお薦めします。Oracle Internet Directory の使用レベルに基づいて、次のように概算で見積もることができます。

表 20-13 CPU 要件の概算

使用方法	CPU の数	SPECint_rate95 ベースライン	システム
部門単位	2	60 ～ 200	Compaq AlphaServer 8400 5/300（300MHz × 2）
組織単位	4	200 ～ 350	IBM RS/6000 J50（200MHz × 4）
会社単位	4+	350+	Sun Ultra 450（296 MHz × 4）

CPU 要件の詳細な計算

CPU の消費量はいくつかの要因によって変化するため、所定の配置サイトですべての操作に対する CPU 要件を判断することは困難です。次のような要因があります。

- 操作の種類（ベース検索、サブツリー検索、変更、追加など）。
- SSL モードを使用可能にしているかどうか（SSL を使用すると、15 ～ 20% 多く CPU リソースが消費されます）。
- Oracle Internet Directory サーバーのエントリ・キャッシュを使用可能にしているかどうか（ヒット率が CPU 使用量に影響を与えるため）。
- 検索で戻されるエントリの数。
- 検索操作中にチェックする必要があるアクセス制御ポリシーの数。

SSL を除くほとんどの場合、Oracle Internet Directory サーバー・プロセスとデータベースとの間にかなりの待機時間があることが予想されます。Oracle Internet Directory サーバー・プロセスのスレッドがデータベースの応答を待機しているときは、Oracle Internet Directory サーバー・プロセス内のその他のスレッドを、LDAP サーバー固有の処理が必要なその他のクライアント要求の作業に充てることができます。この結果、操作のいかなる組合せでも、同時クライアントと Oracle Internet Directory サーバー・プロセスの組合せが常に実現でき、CPU 使用率が 100% になります。この場合は、CPU がボトルネックとなります。

この事実を考慮し、メッセージング・タイプのサブツリー検索操作を採用し、操作のスループットを低下させずに、指定された数の同時操作をサポートするために必要な CPU リソースを算出しています。メッセージング検索操作には、サブツリー有効範囲、単純な完全一致フィルタおよび 1 つのエントリの結果セットが関係します。Oracle Internet Directory 10*g*（9.0.4）の場合は、次のようになります。

SPECint_rate95 ベースライン = 0.5 ×（ピーク時のスループットでの同時操作最大数）

これは、操作のスループットを低下させずに、600 の同時クライアントをサポートする必要がある場合は、（0.5 × 600）= 300 以上の SPECint_rate95 ベースライン評価のコンピュータが必要であることを意味します。

操作のスループットについては、Oracle Internet Directory 10*g*（9.0.4）の場合、次のようになります。

SPECint_rate95 ベースライン = 0.4 ×（サポートされる同時操作最大数での操作のスループット）

これは、サポートされる同時操作数として指定した最大数に、毎秒 750 操作のスループットが必要な場合は、（0.4 × 750）= 300 以上の SPECint_rate95 ベースライン評価のコンピュータが必要であることを意味します。

Oracle Internet Directory は、追加 CPU リソースを確実に調整することが証明されています。これは次のことを意味します。

- 指定した操作同時実行性については、CPU リソースを追加することによって、より高いスループット（待機時間がより短い）の操作を達成できます。
- 指定した操作スループット（待機時間）については、別途の CPU リソースを追加することによって、より高い操作同時実行性を達成できます。

Acme Corporation の例に戻り、各クライアントにわずかな待機時間を見込みながら、500 の同時メッセージング・タイプのサブツリー検索操作をサポートする適切な CPU リソースが必要であると仮定します。安全係数を 20% とすると、CPU 要件の仮見積りは、360 以上の SPECint_rate95 ベースラインを持つコンピュータとなります。

Acme Corporation の容量計画のまとめ

ここまでの各項で、容量計画に関係する様々なコンポーネントを説明するとともに、それぞれのコンポーネントを、Acme Corporation という仮想の会社における Oracle Internet Directory の配置に適用する方法も紹介しました。この項では、前述のすべての推奨事項を簡単に要約して示します。最初の仮定は次のとおりです。

- ディレクトリ全体のサイズ : 3,200,000 エントリ（320 万）
- ユーザー数 : 40,000
- アプリケーションのタイプ : IMAP メッセージング
- ピーク時の検索率 : 500 クライアントの同時実行性で 750 検索 / 秒

この要件とその他の仮定に基づいて、次の推奨事項を提示しました。

- ディスク領域 : 5GB ～ 8GB
- メモリー : 2GB
- ネットワーク : 100 Base-T
- CPU: SPECint_rate95 の数値が 360 以上の CPU

サイズ設定の計算を直観的に理解できるように、いくつか単純な仮定を使用しました。

21

ディレクトリのチューニングに関する考慮事項

第 20 章「ディレクトリの容量計画」の説明に従って容量計画を完了し、必要なハードウェアを用意した後は、ハードウェアとソフトウェアの組合せで必要なレベルのパフォーマンスが得られることを確認する必要があります。この章では、Oracle Internet Directory のチューニングに関するガイドラインを示します。次の項目について説明します。

- チューニングの概要
- パフォーマンス・チューニング用のツール
- CPU 使用量のチューニング
- メモリーのチューニング
- ディスクのチューニング
- データベースのチューニング
- エントリ・キャッシング
- 検索の最適化
- 制限時間モードの設定
- クライアント / サーバー間の接続のタイムアウトの設定
- パフォーマンスに関するトラブルシューティング

チューニングの概要

Oracle Internet Directory に関するパフォーマンスの主な測定方法は次の 2 つです。

- 最大負荷時における個々の操作の平均待機時間。

  この時間は、各操作が完了するまでの時間です。

- 最大負荷時における Oracle Internet Directory の包括的なスループット。1 秒当りの操作件数で表されます。

  このスループットは、Oracle Internet Directory のインスタンスがクライアントの操作を完了できる率です。

テストの結果、パフォーマンスの改善が必要と考えられる場合は、次の各項に記載されている情報で、パフォーマンスの問題点を識別して調整できます。

パフォーマンス・チューニング用のツール

Solaris および大部分の他の UNIX オペレーティング・システムを使用している場合は、次の各ツールを理解しておくことをお薦めします。

ツール	説明
top	システムにおいて CPU を最も多く消費しているタスクを表示します。
vmstat	Virtual Memory Manager など、システムの様々な部分の実行統計を示します。
mpstat	vmstat と同様の出力ですが、システム内の各種 CPU にわたって分割して示します。このユーティリティは Solaris でのみ使用可能です。
iostat	各種ディスク・コントローラからのディスク I/O 統計を示します。

Windows NT を使用している場合は、次のツールを理解しておくことをお薦めします。

ツール	説明
Windows NT Performance Monitor	システム内のイベントのカスタマイズされたビューを表示します。
Windows NT タスク・マネージャ	システムで実行されている主なタスクの最高レベルの出力（UNIX の top と同様）を提供します。

Oracle9*i* を使用する場合は、次のツールを理解しておくことをお薦めします。

- `utlbstat.sql` および `utlestat.sql`、または `Statspack`
- DBMS_STATS パッケージの ANALYZE ファンクション

関連項目：

- `utlbstat.sql` および `utlestat.sql` の詳細は、『Oracle Database リファレンス』を参照してください。
- statspack の詳細は、『Oracle Database パフォーマンス・チューニング・ガイド』を参照してください。
- DBMS_STATS パッケージの ANALYZE ファンクションの詳細は、『Oracle Database 概要』を参照してください。

オペレーティング・システム・ツール以外に、カスタマ環境で使用されている LDAP アプリケーションも待機時間やスループットの測定方法を提供しています。

さらに、様々なデータベース 'ods' スキーマ・オブジェクトを分析して統計を見積もるために、`$ORACLE_HOME/ldap/admin` にあるデータベース統計収集ツール（oidstats.sh）が提供されています。

注意： Windows オペレーティング・システムでシェル・スクリプト・ツールを実行するには、次のいずれかの UNIX エミュレーション・ユーティリティが必要です。

- Cygwin 1.3.2.2-1 以上
  サイト：`http://sources.redhat.com`
- MKS Toolkit 6.1
  サイト：`http://www.datafocus.com/`

関連項目： A-131 ページの「OID データベース統計収集ツール（oidstats.sh）の構文」

CPU 使用量のチューニング

CPU はおそらく、すべてのソフトウェアが使用する最も重要なリソースです。第 20 章「ディレクトリの容量計画」では、所定のアプリケーション負荷に対して必要となる CPU 能力の概算を示しましたが、十分にチューニングされていないと、CPU リソースが効率的に使用されない原因となります。次の各項目のいずれかに該当する場合は、CPU リソースのチューニングを考慮してください。

- 最大負荷時に CPU 稼働率が 100% の場合。
- 最大負荷時に CPU が十分に活用されていない場合。システムにかなりのアイドル時間があり、このアイドル時間が高負荷時でもなくならない場合。

内部的なベンチマークでは、CPU リソースの約 70 ～ 75% が Oracle Internet Directory のプロセスで消費され、残りの約 25 ～ 30% がデータベース接続に対応する Oracle のフォアグラウンド・プロセスで消費されている場合に、Oracle Internet Directory が最も効率よく実行されることが示されています。CPU 使用量を監視すると同時に、システム領域で使用されている時間とユーザー領域で使用されている時間の割合を監視することも重要です。内部的なベンチマークでは、約 85% がユーザー時間、約 15% がシステム時間の場合にスループット値が最大であることが示されています。

この項では、次の項目について説明します。

- Oracle Internet Directory のプロセスに関する CPU のチューニング
- Oracle のフォアグラウンド・プロセスに関する CPU のチューニング
- SMP システムにおけるプロセッサ親和性の利用
- CPU がボトルネックとなっているシステムに関するその他の方法

Oracle Internet Directory のプロセスに関する CPU のチューニング

CPU に対する Oracle Internet Directory プロセスの需要は、ORCLSERVERPROCS および ORCLMAXCC の各パラメータで制御できます。次の表に、様々なクライアント負荷に対応したパラメータの推奨値を示します。

ORCLSERVERPROCS	ORCLMAXCC	操作スループットの低下なしでサポートされる同時クライアントの数	接続を切断せずにサポートされるクライアントの数	必要な CPU の数
1	2	40		1
2	10	400	800	2
4	10	800	1600	4
8	10	1600	3200	8

同時クライアントの数が 500 で、ORCLSERVERPROCS の値が 4、ORCLMAXCC の値が 10 の場合を例にとると、次のような構成になります。

- 4 個のサーバー・プロセスが作成されます。
- 各サーバー・プロセスは、実際に作業するワーカー・スレッドを 10 個起動します。
- 各サーバー・プロセスは、ワーカー・スレッド間で共有される 11（10+1）個のデータベース接続のプールをメンテナンスします。

Oracle Internet Directory は、操作スループットおよびクライアント同時実行性の両面に関して、CPU リソースを確実に調整します。前述の表より、4 つの CPU があり、クライアント 'n' 台の同時実行性に対して、毎秒 'p' 件のピーク時操作スループットを維持できるとします。

CPU の数の追加またはより高速な CPU の使用によって、次の利点が得られます。

- クライアント 'n' 台の同じ同時実行性に対して、'p' 件を超える高いスループットを達成できます。
- 'n' 台を超える高い同時実行性に対して、同じ 'p' 件の操作スループットを維持できます。

最大負荷時の CPU 使用量が 100% 未満で、かなりの割合の時間（5% 以上）システムがアイドル状態の場合は、Oracle Internet Directory プロセスの構成数が少なく、CPU リソースを十分利用していないことを示しています。この問題を解決するためには、ORCLSERVERPROCS と ORCLMAXCC の値を計画的に増やして、CPU 稼働率が 100% になり、システム時間とユーザー時間が次の割合になるように調整してください。

- ユーザー時間 : 85% 以上
- システム時間 : 15% 以下

Oracle のフォアグラウンド・プロセスに関する CPU のチューニング

次の条件の両方に該当する場合のみ、Oracle のフォアグラウンド・プロセスに関する CPU リソースのチューニングを考慮してください。

- 最大負荷時の CPU 稼働率が 100% に近い場合
- Oracle のフォアグラウンド・プロセスが使用可能な全 CPU リソースの 30% 以上を消費している場合

Oracle のフォアグラウンド・プロセスが過度に CPU を消費している場合は、Oracle Internet Directory のデータベースに対する問合せが、多数の CPU サイクルを使用していることを示しています。データベースが実行するこの種の基本的な操作の場合は、ユーザーが制御できる部分はほとんどありませんが、次のことを試してください。

- データベース上の ODS ユーザーに関連付けられているすべての表と索引に関するデータベース統計を、`ANALYZE` コマンドを使用して収集します。この統計は、コストベースのオプティマイザが、Oracle Internet Directory で生成される問合せ用に、より適した実行計画を作成するために役立ちます。統計の収集には、`$ORACLE_HOME/ldap/admin/oidstats.sh` を使用できます。

- ANALYZE でよい結果が得られず、使用される LDAP 問合せに多数のフィルタが含まれている場合は、フィルタの指定順序を単純に再構成（最も特殊なフィルタを最初にし、最も一般的なフィルタを最後に指定）すると、Oracle フォアグラウンド・プロセスの CPU 消費削減に効果があります。

注意： Windows オペレーティング・システムでシェル・スクリプト・ツールを実行するには、次のいずれかの UNIX エミュレーション・ユーティリティが必要です。

- Cygwin 1.3.2.2-1 以上
  サイト：http://sources.redhat.com
- MKS Toolkit 6.1
  サイト：http://www.datafocus.com/

SMP システムにおけるプロセッサ親和性の利用

一部の対称型マルチ・プロセッサ（SMP）システムには、特定のプロセスを特定の CPU にバインドする機能があります。プロセスをプロセッサにバインドする方法は、通常はお薦めしませんが、次の条件に該当する場合は、この方法でパフォーマンスが向上する場合があります。

- システム全体の CPU 稼働率が 100% に近い場合
- コンピュータ上に複数の CPU が存在する場合

内部的なベンチマークでは、OID サーバー・プロセスと関連する Oracle シャドウ・プロセスを同じ CPU にバインドすることが、一般的に最大のパフォーマンスを上げると認められています。

CPU がボトルネックとなっているシステムに関するその他の方法

前述の項に記載されているヒントで CPU 関連のパフォーマンスの問題が解決されない場合は、次のオプションを使用してください。

- コンピュータの処理能力を増加させる方法。つまり、CPU を追加するか、または低速の CPU を高速の CPU に交換します。
- Oracle ディレクトリ・サーバーと Oracle9*i* データベースを別々のコンピュータに配置する方法。

メモリーのチューニング

CPU の次に、メモリーのチューニングが重要です。Oracle Internet Directory においてメモリーを主に消費しているのは、Oracle9*i* データベースです。バックエンド・データベースの SGA は、Oracle Internet Directory と Oracle プロセスがそのプライベート・スタックとヒープを操作するために必要な領域を確保しつつ、十分な大きさで作成する必要があります。この項では、SGA の様々なコンポーネントの判別に関して詳細に説明します。

この項では、次の項目について説明します。

- Oracle9i データベース・サーバー 用の SGA のチューニング
- メモリーがボトルネックとなっているシステムに関するその他の方法

Oracle9*i* データベース・サーバー 用の SGA のチューニング

SGA は、Oracle9*i* データベース・サーバー を実行しているシステムの使用可能な物理メモリーに基づいてサイズ設定してください。

> **関連項目：** SGA を適切なサイズに設定する方法の詳細は、『Oracle Database パフォーマンス・チューニング・ガイド』を参照してください。このマニュアルは、SGA サイズがページング・スワッピング・アクティビティを増やさないようにする方法について説明しています。後者はパフォーマンスに悪影響を及ぼします。

SGA の使用可能なサイズを設定した後、2 つの主なチューニング項目を考慮してください。

- 共有プール・サイズ
- バッファ・キャッシュ・サイズ

共有プール・サイズの初期見積りは、前項で決めた同時データベース接続ごとに 0.5MB です。

この見積りで、SGA 合計の 30% を超える領域を消費する場合は、SGA 合計の 30% を使用してください。

残りの使用可能な SGA サイズの 60% を、データベースに対するブロック・サイズで除算し、DB_BLOCK_BUFFERS の数にこの値を使用します。この 2 つの値は初期見積りであり、BSTAT/ESTAT やその他の RDBMS 監視ツールを使用してさらに詳細に見積もると、最大のパフォーマンスを得るための正確なサイズを設定できます。

メモリーがボトルネックとなっているシステムに関するその他の方法

データベースと Oracle ディレクトリ・サーバーを同じコンピュータ上で実行するためのメモリーが不足している場合は、データベースを別のコンピュータに配置できます。

ディスクのチューニング

ディスク I/O の均衡化は、RDBMS 全般、つまり Oracle Internet Directory のパフォーマンスにおいて重要な考慮事項です。一般的に、次の技術を 1 つ以上使用すると、I/O スループットを最大にできます。

- I/O 操作で複数のディスク・スピンドルを使用するために、論理ボリュームをストライプ化
- 異なる表領域を、異なる論理ディスク・ボリュームと物理ディスク・ボリュームに格納
- ディスク・ボリュームを複数の I/O 制御装置に分散

関連項目： ディスク I/O の均衡化とチューニングの概要は、『Oracle Database パフォーマンス・チューニング・ガイド』を参照してください。

データベースのチューニング

この項では、Oracle Internet Directory のインストールに有効な、その他のチューニング可能なパラメータについて説明します。

次の表は、様々なクライアント負荷に対する RDBMS パラメータの推奨値を一覧にしたものです。これらのパラメータは、初期化パラメータ・ファイルで設定可能です。

パラメータ	同時 LDAP クライアントの数が 500 の場合	同時 LDAP クライアントの数が 1000 の場合	同時 LDAP クライアントの数が 1500 の場合	同時 LDAP クライアントの数が 2000 の場合
OPEN_CURSORS	200	200	200	200
SESSIONS	225	600	800	1200
DATABASE_BLOCK_BUFFERS	200 ～ 250MB	200 ～ 250MB	200 ～ 250MB	200 ～ 250MB
DATABASE_BLOCK_SIZE	8192	8192	8192	8192
SHARED_POOL_SIZE	30 ～ 40MB	30 ～ 40MB	30 ～ 40MB	30 ～ 40MB
PROCESSES	400	800	1000	1500

この項では、チューニング可能な各 RDBMS パラメータについての詳細を説明します。この項では、次の項目について説明します。

- 必須パラメータ
- Oracle Internet Directory サーバーの構成に依存しているパラメータ
- ハードウェア・リソースに依存している SGA パラメータ

必須パラメータ

OPEN_CURSORS パラメータを次のように設定します。

```
OPEN_CURSORS=200
```

Oracle Internet Directory サーバーのカーソル・キャッシュを処理するには Oracle9*i* のデフォルト値（50 前後）では小さすぎます。この値は、他の Oracle Internet Directory サーバーのパラメータ（SERVERS の数や WORKERS の数など）に依存していません。値を 200 に設定すると、どのようなサイズのディレクトリ情報ツリーにも対応できます。

Oracle Internet Directory サーバーの構成に依存しているパラメータ

SESSIONS パラメータを次のように設定します。

```
PROCESSES = (# OID server processes for each instance) x
            (# DB Connections for each server + 1) x
            (# of OID instances) + 20
SESSIONS = 1.1 * PROCESSES + 5
```

各 Oracle Internet Directory サーバー・プロセスには、そのサーバーに構成されているワーカー・スレッドの数と等しい同時データベース接続数に 1 を加算した数が必要です。したがって、許容される同時データベース接続の合計数は、インスタンスごとのサーバー当りのこの数値になる必要があります。パラメータ値に追加されている 20 の接続数には、Oracle バックグラウンド・プロセスとその他の Oracle Internet Directory プロセス（OID モニター、OID 制御、Oracle ディレクトリ・レプリケーション・サーバーおよびバルク・ツールなど）が考慮されています。

共有サーバー・プロセスの使用

必要な同時データベース接続の合計数によっては、SESSIONS パラメータの設定で決められたように、共有サーバー・プロセスの使用がシステム全体の負荷をより均衡化するために役立つ場合があります。必要な同時データベース接続の合計数が 300 を超える場合は、共有サーバーを構成してください。必要なデータベース接続 10 ごとに、1 つの共有サーバーを構成してください。

注意： 必要な同時データベース接続数は、選択したハードウェアに依存します。共有サーバーの構成の詳細は、『Oracle9*i* Net Services 管理者ガイド』および『Oracle9*i* データベース管理者ガイド』を参照してください。

ハードウェア・リソースに依存している SGA パラメータ

SGA に関係する主なパラメータの説明は、21-7 ページの「メモリーのチューニング」に記載されています。その他のチューニング可能なパラメータを次にいくつか示します。

- ソート領域

  ディスク上でソートが行われないように、十分なソート領域を確保するために、262144（256K）に設定してください。

- REDO ログ・バッファ

  初期見積りとして 32768（32K）に設定してください。ログの書込みパフォーマンスがパフォーマンスの問題となる場合は、（REDO ログ領域要求 /REDO エントリ）> 1/5000 となるように十分に大きい値を使用して、LGWR プロセスが遅延しないようにしてください。この数値は全体でも、可変の SGA サイズにほとんど影響しないサイズであるため、この値の多少の増加が問題となることはありません。

エントリ・キャッシング

Oracle Internet Directory 10*g*（9.0.4）では、ディレクトリ・サーバーのエントリ・キャッシュは、単一のディレクトリ・サーバー・インスタンスでのみサポートされます。エントリ・キャッシングの利点は、エントリ・キャッシュのヒット率が非常に高い場合に最大化されます。次のような小中規模のディレクトリ配置では、エントリ・キャッシュの使用をお薦めします。

- ディレクトリ・エントリのワーキング・セットが合理的に完全にキャッシュできる場合
- クライアントの同時実行性が単一のディレクトリ・サーバー・インスタンスで処理できる場合

内部ベンチマークでは、エントリのワーキング・セットが数十万のエントリであるディレクトリ配置の場合、エントリ・キャッシュによって、最大 1000 の同時クライアントに対する操作のスループットが 2 倍になることが示されています。

より大規模なディレクトリ・エントリのワーキング・セットが存在し、クライアントの同時実行性が高いディレクトリ配置では、マルチプロセス・ディレクトリ・サーバー・インスタンスが使用され、Oracle のバッファ・キャッシュによって、スケーラビリティが増大します。

> **関連項目：** エントリ・キャッシングを使用可能にして構成するために設定する属性の詳細は、5-9 ページの「システム操作属性の設定」を参照してください。

検索の最適化

この項では、次の項目について説明します。

大きいグループ・エントリの検索の最適化

member または uniquemember 属性のいずれかの値が、数千個を超えるグループ・エントリの検索では、待機時間が長くなる可能性があります。member および uniquemember 以外の属性を持つ大きなグループ・エントリの検索で、待機時間が非常に長くなった場合は、次の操作を実行します。

1. dsaconfig エントリで、orclindexhints 属性を 1 に設定します。たとえば、UNIX では次のように設定します。

```
ldapmodify -D "cn=orcladmin" -w <passwd> -h ldaphost -p ldapport <<!
dn: cn=dsaconfig,cn=configsets,cn=oracle internet directory
changetype: modify
replace: orclindexhints
orclindexhints: 1
!
```

2. ODS ユーザーとして Oracle Internet Directory データベースにログインし、*$ORACLE_HOME*/ldap/admin/oidbmind.sql を実行します。これにより、ds_attrstore 表に、1 つの B ツリー索引ではなく、2 つのビットマップ索引が作成されます。
3. Oracle ディレクトリ・サーバーを再起動します。

スキュー属性の検索の最適化

通常の検索要求を処理する場合、ディレクトリ・サーバーは SQL 文を Oracle9*i* データベース・サーバーに送信します。指定された属性の応答時間が、属性の値によって大きく異なる場合、この属性はスキュー属性であるとみなされます。たとえば、my_attribute=value1 と my_attribute=value2 の検索で、応答時間が大きく異なる場合、my_attribute はスキュー属性であるとみなされます。

このような属性を、dsaconfig エントリにある orclskewedattribute 属性の値として追加することにより、検索時の応答時間を均一にできます。dsaconfig エントリの識別名は、cn=dsaconfig,cn=configsets,cn=oracle internet directory です。

デフォルトでは、objectclass 属性は、orclskewedattribute 属性内に値としてリストされます。

Oracle Directory Manager を使用したスキュー属性の検索の最適化

データベースへの問合せを最適化する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」を展開して、ディレクトリ・サーバー・インスタンスを選択します。
2. 右側のペインで「**問合せの最適化**」タブを選択します。このタブ・ページの各フィールドの説明は、C-32 ページの表 C-36 を参照してください。
3. 「**問合せの最適化**」タブ・ページの「**低カーディナリティの属性**」フィールドで、スキュー属性として指定する属性を入力します。
4. 「**適用**」を選択します。

ldapmodify を使用したスキュー属性の検索の最適化

スキュー属性の検索を最適化するには、ldapmodify を使用して、その属性を `orclskewedattribute` 属性の値として追加します。

たとえば、`my_attribute` を `orclskewedattribute` 属性に追加するには、次のように入力します。

```
ldapmodify -D "cn=orcladmin" -w password -h host -p port <<!
dn: cn=dsaconfig,cn=configsets,cn=oracle internet directory
changetype: modify
add: orclskewedattribute
orclskewedattribute: my_attribute
!
```

制限時間モードの設定

5-9 ページの「システム操作属性の設定」の説明に従って、サーバー処理の制限時間を設定する場合は、検索の完了までの最大時間（秒）を指定します。サーバーのパフォーマンスを調整する場合は、検索制限時間モードを厳密に設定するか、おおよその時間に設定することもできます。正確な時間に設定すると、検索は必ず指定した秒数で終了します。おおよその時間に設定すると、検索は指定した秒数から 2 秒の範囲内で終了します。作業負荷が低い場合は、後者の方がより高いパフォーマンスを得られます。

Oracle Directory Manager を使用した制限時間モードの設定

制限時間モードを設定する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」を展開して、ディレクトリ・サーバー・インスタンスを選択します。
2. 右側のペインで「**問合せの最適化**」タブを選択します。

3. 「**問合せの最適化**」タブ・ページの「時間制限モード」フィールドで、「**精度**」または「**近似**」を選択します。
4. 「**適用**」を選択します。

ldapmodify を使用した制限時間モードの設定

正確な時間か、おおよその時間のいずれかの検索制限時間モードを指定するには、orcltlimitmode 属性を設定します。値 0 は正確な時間で、値 1 はおおよその時間です。デフォルト値は 1 です。

クライアント / サーバー間の接続のタイムアウトの設定

クライアントとディレクトリ・サーバー間の接続のアイドル・タイムを指定できます。

Oracle Directory Manager を使用したクライアント / サーバー間の接続のタイムアウトの設定

クライアント / サーバー間の接続のタイムアウトを設定する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」を展開して、ディレクトリ・サーバー・インスタンスを選択します。
2. 右側のペインで「**問合せの最適化**」タブを選択します。
3. 「**問合せの最適化**」タブ・ページの「**LDAP 接続タイムアウト**」フィールドに、接続が終了するまで、ディレクトリ・クライアントがアイドル状態を維持できる最大秒数を入力します。デフォルトは 0 です。これはタイムアウトがないことを意味します。
4. 「**適用**」を選択します。

パフォーマンスに関するトラブルシューティング

この項では、一般的なパフォーマンス関連の問題を解決するための簡単な説明を示します。

LDAP 検索のパフォーマンスが悪い場合、次のことを確認してください。

- 検索対象の属性が索引付けされていること
- ODS ユーザーに関連付けられているスキーマが ANALYZED であること

  複数のフィルタ・オペランドを含む検索の場合は、フィルタの指定順序が、最も特殊な条件から最も一般的な条件の順であることを確認します。たとえば、
  &(c=US)(state=Illinois)(l=Chicago) は、
  &(l=Chicago)(state=Illinois)(c=US) と指定した方が効率的です。

LDAP 追加または変更のパフォーマンスが悪い場合、次のことを確認してください。

- データベースに十分な数の REDO ログ・ファイルがあること
- データベースの UNDO 表領域の大きさが十分であること
- ODS ユーザーに関連付けられているスキーマが ANALYZED であること

OID データベース統計収集ツールを使用して、様々なデータベース ods スキーマ・オブジェクトを分析し、統計を見積もることもできます。

> **関連項目：** OID データベース統計収集ツールの使用方法は、A-131 ページの「OID データベース統計収集ツール（oidstats.sh）の構文」を参照してください。

22

Oracle Internet Directory におけるガベージ・コレクション

「ガベージ」とは、ディレクトリで、不要になっているが領域を使用しているデータを指します。結果として、このような不要なデータや、古いデータで、ディスクが一杯になり、ディレクトリのパフォーマンスが低下します。ディレクトリからこの不要なデータを削除する処理を、ガベージ・コレクションと呼びます。

この章では、次の項目について説明します。

- Oracle Internet Directory ガベージ・コレクション・フレームワークの概要
- Oracle Internet Directory ガベージ・コレクタの変更
- Oracle Internet Directory ガベージ・コレクタのロギングの有効化と無効化

Oracle Internet Directory ガベージ・コレクション・フレームワークの概要

ガベージ・コレクタは、ディレクトリから不要なデータを削除する、バックグラウンドのデータベース・プロセスです。Oracle Internet Directory ガベージ・コレクション・フレームワークには、ガベージ・コレクタの標準セットがあります。このフレームワークにより、これらのコレクタを変更できます。

この項では、次の項目について説明します。

- Oracle Internet Directory ガベージ・コレクション・フレームワークのコンポーネント
- Oracle Internet Directory ガベージ・コレクションの動作
- ガベージ・コレクタ・エントリ
- マルチマスター・レプリケーションの変更ログの削除

Oracle Internet Directory ガベージ・コレクション・フレームワークのコンポーネント

この項では、Oracle Internet Directory ガベージ・コレクション・フレームワークを構成するコンポーネントであるガベージ・コレクション・プラグインおよびガベージ・コレクタについて説明します。

ガベージ・コレクション・プラグイン

Oracle Internet Directory のガベージ・コレクションは、ガベージ・コレクタの管理要求を受け取るガベージ・コレクション・プラグインを使用します。このプラグインは、Oracle Internet Directory とともにインストールされ、デフォルトで使用可能になります。このプラグインのエントリは、`cn=plugin,cn=subconfigsubentry` です。

このプラグインには、3 つのトリガーがあります。

- ガベージ・コレクション・ジョブの作成に使用するプラグイン・トリガー。識別名は、次のとおりです。
  `cn=Add PurgeConfig,cn=plugin,cn=subconfigsubentry`
- ガベージ・コレクション・ジョブの変更に使用するプラグイン・トリガー。識別名は、次のとおりです。
  `cn=Modify PurgeConfig,cn=plugin,cn=subconfigsubentry`

- ガベージ・コレクション・ジョブの削除に使用するプラグイン・トリガー。識別名は、次のとおりです。
  `cn=Delete PurgeConfig,cn=plugin,cn=subconfigsubentry`

  関連項目： ガベージ・コレクション・プラグインの属性のリストおよび説明は、B-16 ページの「Oracle Internet Directory ガベージ・コレクションのプラグイン」を参照してください。

ガベージ・コレクタ

ガベージ・コレクタは、ガベージ・コレクション・プラグインによって起動される、バックグラウンドのデータベース・プロセスです。次のガベージ・コレクタの動作を設定して管理できます。

- ガベージ・コレクタがデータを削除するサブツリー
- 起動時間
- 削除するデータの経過時間
- 実行頻度
- 削除するデータの種類
- 一度に削除するエントリの数

事前定義済ガベージ・コレクタ Oracle Internet Directory のデフォルトのインストールに含まれている事前定義済ガベージ・コレクタは、次のとおりです。

- 監査ログのガベージ・コレクタ : ディレクトリを監査するために作成されたエントリのうち、使用されなくなったものをクリーンアップします。このガベージ・コレクタのコンテナは、次のとおりです。
  `cn=auditlog purgeconfig,cn=purgeconfig,cn=subconfigsubentry`

  関連項目： B-9 ページの「監査ログのガベージ・コレクタ」

- 変更ログのガベージ・コレクタ : ディレクトリ内のコンシューム済変更ログ・エントリをクリーンアップします。このガベージ・コレクタのコンテナは、次のとおりです。
  `cn=changelog purgeconfig,`
  `cn=purgeconfig,cn=subconfigsubentry`

  関連項目： B-10 ページの「変更ログのガベージ・コレクタ」

- 一般統計のガベージ・コレクタ : ディレクトリの一般統計情報を監視するために Oracle Internet Directory サーバー管理機能により作成され、使用されなくなったエントリをクリーンアップします。このガベージ・コレクタのコンテナは、次のとおりです。
  ```
  cn=general stats purgeconfig,
  cn=purgeconfig,cn=subconfigsubentry
  ```
  関連項目 : B-11 ページの「一般統計のガベージ・コレクタ」

- 健全性統計のガベージ・コレクタ : ディレクトリの健全性統計情報を監視するために Oracle Internet Directory サーバー管理機能により作成され、使用されなくなったエントリをクリーンアップします。このガベージ・コレクタのコンテナは、次のとおりです。
  ```
  cn=health stats purgeconfig,
  cn=purgeconfig,cn=subconfigsubentry
  ```
  関連項目 : B-12 ページの「健全性のガベージ・コレクタ」

- セキュリティおよびリフレッシュ・イベントのガベージ・コレクタ : ディレクトリのセキュリティおよびリフレッシュ・イベントを監視するために Oracle Internet Directory サーバー管理機能により作成され、使用されなくなったエントリをクリーンアップします。このガベージ・コレクタのコンテナは、次のとおりです。
  ```
  cn=secrefresh events purgeconfig,
  cn=purgeconfig,cn=subconfigsubentry
  ```
  関連項目 : B-13 ページの「セキュリティと更新イベントのガベージ・コレクタ」

- システム・リソース・イベントのガベージ・コレクタ : ディレクトリのシステム・リソース・イベントを監視するために Oracle Internet Directory サーバー管理機能により作成され、使用されなくなったエントリをクリーンアップします。このガベージ・コレクタのコンテナは、次のとおりです。
  ```
  cn=sysresource events purgeconfig,
  cn=purgeconfig,cn=subconfigsubentry
  ```
  関連項目 : B-14 ページの「システム・リソース・イベントのガベージ・コレクタ」

- 削除済とマークされたエントリのガベージ・コレクタ : ディレクトリ内で削除済とマークされた、使用されなくなったエントリをクリーンアップします。このガベージ・コレクタのコンテナは、次のとおりです。
  `cn=tombstone purgeconfig, cn=purgeconfig,cn=subconfigsubentry`

  関連項目： B-15 ページの「削除済とマークされたエントリのガベージ・コレクタ」

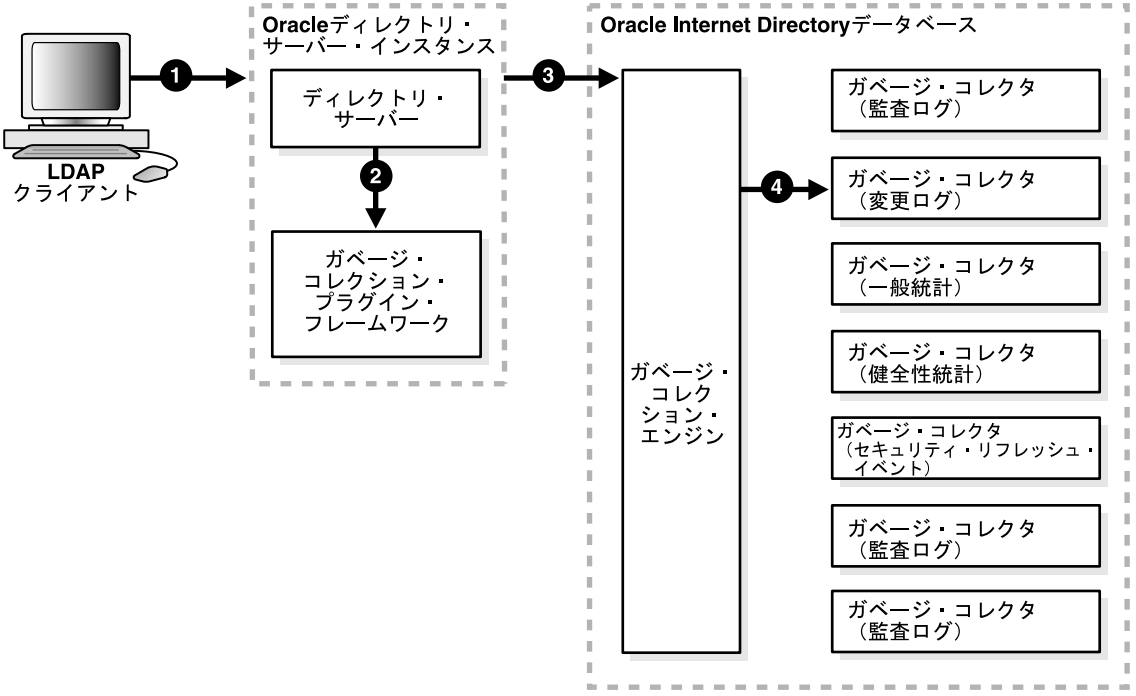
  注意： 事前定義済ガベージ・コレクタは削除しないことをお薦めします。これらのガベージ・コレクタを 1 つ以上削除すると、不要なデータが増加し、最終的には使用可能なすべてのディスク領域を使い果たすことになります。

  ただし、動作をカスタマイズするために、事前定義済ガベージ・コレクタを変更してもかまいません。

Oracle Internet Directory ガベージ・コレクションの動作

図 22-1 に、変更ログ・エントリを削除するガベージ・コレクタの動作の例を示します。

図 22-1 例 : 変更ログ・エントリのガベージ・コレクション



22-6 ページの図 22-1 の例に示すとおり、ガベージ・コレクション・プロセスは、次のように動作します。

1. LDAP クライアントが、特定のガベージ・コレクション操作要求をディレクトリ・サーバーに送信します。これらの操作には、削除されたとみなされるエントリ、変更ログのエントリ、監査ログのエントリの削除などがあります。
2. ディレクトリ・サーバーが、要求をガベージ・コレクション・プラグインに渡します。
3. ガベージ・コレクション・プラグインが、Oracle Internet Directory で指定されたデータベースのガベージ・コレクション・エンジンに要求を送信します。
4. ガベージ・コレクション・エンジンが、対応するガベージ・コレクタ（この場合は、変更ログのガベージ・コレクタ）をトリガーします。ガベージ・コレクタは、構成設定エントリに指定されているパラメータに基づいて、バックグラウンドのデータベース・プロセスとして動作します。

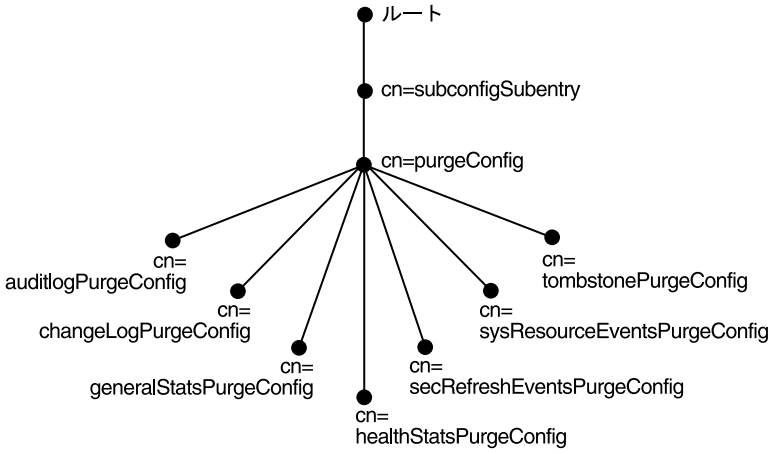
ガベージ・コレクタ・エントリ

各ガベージ・コレクタ・エントリは、動作を指定する属性を持ち、エントリ `cn=subconfigsubentry` の直下にあるエントリ `cn=purgeconfig` に存在します。

> **関連項目：** ガベージ・コレクタの各属性の詳細は、B-8 ページの表 B-8「ガベージ・コレクションの構成パラメータ」を参照してください。

図 22-2 に、これらのエントリの場所を示します。

図 22-2 ディレクトリ情報ツリー内のガベージ・コレクション・エントリ



マルチマスター・レプリケーションの変更ログの削除

Oracle Internet Directory の変更ログの削除は、次の 2 つの方法に従って発生します。

- 変更番号ベース

  これはデフォルトの方法です。レプリケーション・サーバーは、すでに DRG 内のすべてのノードに適用された変更内容を削除します。

- 時間ベース

  この方法を実行すると、変更番号ベースの削除を補強できます。この付加的な方法を使用するには、変更ログ・オブジェクトの存続期間を時間単位で指定するパラメータを設定します。たとえば、24 時間経過した変更ログ・オブジェクトをすべて削除するように、このパラメータを設定できます。変更ログが大きくなりすぎるのを防ぐには、この方法を使用してください。

  この方法は、常に変更ログを削除する規則に従うことに注意してください。指定された時間に変更が適用されていない場合、この方法によって変更ログが削除されることはありません。

  関連項目：

  - 25-35 ページの「ディレクトリ・レプリケーション・サーバーの構成パラメータの表示および変更」
  - 25-36 ページの「コマンドライン・ツールを使用したディレクトリ・レプリケーション・サーバーの構成パラメータの変更」

Oracle Internet Directory ガベージ・コレクタの変更

この項では、次の項目について説明します。

- Oracle Directory Manager を使用したガベージ・コレクタの変更
- コマンドライン・ツールを使用したガベージ・コレクタの変更

Oracle Directory Manager を使用したガベージ・コレクタの変更

ガベージ・コレクタを変更する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「**ディレクトリ・サーバー・インスタンス**」、「**ガベージ・コレクション管理**」の順に展開し、構成するガベージ・コレクタを選択します。右側のペインに「ガベージ・コレクタ」ウィンドウが表示されます。
2. 「**ガベージ・コレクタ**」ウィンドウで、このガベージ・コレクタの値を入力します。フィールドについては、C-5 ページの表 C-7 を参照してください。
3. 「**適用**」を選択します。

コマンドライン・ツールを使用したガベージ・コレクタの変更

この項では、コマンドライン・ツールを使用してガベージ・コレクタを変更する方法の例を示します。変更できるガベージ・コレクション属性は、B-9 ページの「事前定義されたガベージ・コレクタのスキーマ要素」を参照してください。

例 1: ガベージ・コレクタの変更

Tombstone ガベージ・コレクタをすぐに実行するとします。LDIF ファイルは次のようになります。

```
dn: cn=tombstone purgeconfig, cn=purge config, cn=subconfigsubentry
changetype:modify
replace: orclpurgerun
orclpurgerun: 1
```

ldapmodify を使用して、このエントリをロードします。

```
ldapmodify -h hostname -p port# -D username -w passwd -f  file_name_of_defined_entry
```

例 2: ガベージ・コレクタの変更ログの使用禁止

変更ログのガベージ・コレクタを使用禁止にするとします。

```
dn: cn=changelog purgeconfig, cn=purgeconfig, cn=subconfigsubentry
changetype: modify
replace: orclpurgeenable
orclpurgeenable: 0
```

ldapmodify を使用して、このエントリをロードします。

```
ldapmodify -h hostname -p port# -D username -w passwd -f  file_name_of_defined_entry
```

Oracle Internet Directory ガベージ・コレクタのロギングの有効化と無効化

この項では、次の項目について説明します。

- Oracle Internet Directory ガベージ・コレクタのロギングの有効化
- Oracle Internet Directory ガベージ・コレクタのロギングの無効化

Oracle Internet Directory ガベージ・コレクタのロギングの有効化

ガベージ・コレクタのロギングを有効にすると、ディレクトリ・サーバーは、ファイル・システム内のファイルに、情報を書き込みます。これには次の情報が含まれます。

- ジョブ識別子
- ガベージ・コレクタのジョブ説明
- 削除されたエントリ数

ガベージ・コレクション情報のロギングを有効にする手順は、次のとおりです。

1. `orclpurgedebug` 属性を 1 に設定します。
2. ログ・ファイルの有効なファイル名を `orclpurgefilename` 属性に設定します。
3. ログ・ファイルのあるディレクトリのパス名を `orclpurgefileloc` 属性に設定します。
4. PL/SQL I/O を有効にします。この手順は、次のとおりです。
   a. データベース初期化ファイルに、次の行を入力します。

      `UTL_FILE_DIR=`*`PATH_NAME`*

      PATH_NAME は、手順 3 で指定したパス名です。

   b. データベースを再起動します。

関連項目：『Oracle Database リファレンス』の UTL_FILE_DIR パラメータについての項を参照してください。

Oracle Internet Directory ガベージ・コレクタのロギングの無効化

ガベージ・コレクション情報のロギングを無効にするには、`orclpurgedebug` 属性を `0` に設定します。

23

他のディレクトリからのデータの移行

この章では、LDAP バージョン 3 準拠のディレクトリおよびアプリケーション固有のディレクトリから Oracle Internet Directory へのデータの移行方法を説明します。また、第 19 章「Oracle Identity Management レルムの配置」に説明したデフォルトのディレクトリ構成に、既存のディレクトリを移行する方法も説明します。

この章では、次の項目について説明します。

- LDAP 準拠のディレクトリからのデータの移行
- ユーザー・データのアプリケーション固有リポジトリからの移行
- デフォルトのディレクトリ構造への既存ディレクトリの移行

LDAP 準拠のディレクトリからのデータの移行

この項では、次の項目について説明します。

データ移行プロセスの概要

データを LDIF ファイルに保存することにより、サード・パーティ製の LDAP 準拠のディレクトリから Oracle Internet Directory にデータをインポートできます。LDIF は、LDAP 準拠のディレクトリのデータをファイルとして表現するための ASCII 交換フォーマットで、IETF による承認を受けています。すべての LDAP 準拠のディレクトリは、エクスポート時に、ディレクトリ情報ツリーを表す 1 つ以上の LDIF ファイルにその内容をエクスポートできます。

製品によっては、LDIF 出力にいくつかの独自の属性またはメタデータが含まれる場合があります。これらのディレクトリ固有のデータは、ファイルを Oracle Internet Directory にインポートする前に LDIF から削除する必要があります。この場合は、LDIF ファイルを Oracle Internet Directory にインポートする前に、追加手順を実行する必要があります。次の項では、これらの手順について説明します。

> **関連項目：** IETF の RFC 2849 は、`http://www.ietf.org` で入手可能です。

LDAP 準拠のディレクトリからデータを移行するためのタスク

LDAP 準拠のディレクトリからデータを移行するには、次のタスクを実行します。

- 非 Oracle Internet Directory サーバーから LDIF ファイル形式へのデータのエクスポート
- LDIF データで参照される必須スキーマの追加のための LDIF ユーザー・データの分析
- Oracle Internet Directory 内のスキーマの拡張
- LDIF ファイルからの独自のディレクトリ・データの削除
- LDIF ファイルからの操作属性の削除
- LDIF ファイルからの非互換の userPassword 属性値の削除
- bulkload.sh -check モードの実行とスキーマ違反または重複エラーが残っているかどうかの判断

タスク 1: 非 Oracle Internet Directory サーバーから LDIF ファイル形式へのデータのエクスポート

エクスポートの方法については、ベンダーが提供するマニュアルを参照してください。外部のディレクトリからデータをエクスポートするためのフラグまたはオプションが存在する場合は、必ず次の方法を選択してください。

- 最小の独自情報が含まれる LDIF 出力を生成する方法
- 23-2 ページの「データ移行プロセスの概要」に記載されている IETF Request for Comments 2849 に最も準拠している方法

タスク 2: LDIF データで参照される必須スキーマの追加のための LDIF ユーザー・データの分析

Oracle Internet Directory ベース・スキーマ内で検索できない属性については、LDIF ファイルをインポートする前に、Oracle Internet Directory ベース・スキーマの拡張が必要です。一部のディレクトリでは、そのベース・スキーマへの拡張を定義するための構成ファイルの使用をサポートしている場合があります（Oracle Internet Directory ではサポートしていません）。構成ファイルがある場合は、「タスク 3: Oracle Internet Directory 内のスキーマの拡張」において Oracle Internet Directory 内のベース・スキーマを拡張するためのガイドラインとしてそのファイルを使用できます。

タスク 3: Oracle Internet Directory 内のスキーマの拡張

Oracle Internet Directory におけるディレクトリ・スキーマの拡張方法に関するヒントは、第 6 章「ディレクトリ・スキーマの管理」を参照してください。この作業は、Oracle Directory Manager または SchemaSynch ツール（A-123 ページの「schemasync ツールの構文」を参照）を使用して実行できます。

タスク 4: LDIF ファイルからの独自のディレクトリ・データの削除

ACI 属性など、LDAP バージョン 3 規格の一部の要素は、まだ正式に承認されていません。その結果、様々なディレクトリ・ベンダーがベンダー間で正常に変換できない方法で、ACI ポリシー・オブジェクトを実装しています。

クリーンアップされた LDIF ファイルから Oracle Internet Directory に基本エントリ・データをインポートした後、Oracle Internet Directory 環境でセキュリティ・ポリシーを明示的に再適用する必要があります。この作業は、Oracle Directory Manager またはコマンドライン・ツールと、必要な **ACP** 情報を含む LDIF ファイルを使用して実行できます。

この他にもアクセス制御に関連しない独自のメタデータが含まれている場合があります。これも同様に削除する必要があります。様々な IETF RFC を理解することで、どのディレクトリ・メタデータが特定のベンダー独自のものであり、どれが LDAP 規格に準拠していて LDIF ファイルによって移植できるかを判断できます。

タスク 5: LDIF ファイルからの操作属性の削除

エントリが作成またはインポートされるたびに、標準の LDAP バージョン 3 操作属性のうち、creatorsName、createTimestamp、modifiersName および modifyTimestamp の 4 つの属性が、Oracle Internet Directory によって自動的に生成されます。たとえば、LDIF ファイルのインポートを使用して、既存のディレクトリ・データからこれらの値をインスタンス化することはできません。したがって、インポートする前にこれらの属性をファイルから削除する必要があります。

タスク 6: LDIF ファイルからの非互換の userPassword 属性値の削除

Oracle Internet Directory 10*g*（9.0.4）は、次の userPassword 属性のハッシュ・アルゴリズムをサポートしています。

- 暗号化を使用しない
- **MD4**
- **MD5**
- **SHA**
- **UNIX Crypt**

一部のベンダー製品で使用されている userPassword 属性のハッシュ値は、Oracle Internet Directory と互換性がありません。そのため、userPassword 属性と値に対応する行はすべて LDIF データ・ファイルから削除する必要があります。ただし、それらの行がプレーン・テキストで表されている場合、または値を含んでいない場合を除きます。LDIF データをインポートした後、手動で再入力するか、ハッシュされた userPassword 情報を別途ディレクトリにアップロードする必要があります。パスワードが Oracle Internet Directory パスワード・ポリシーに準拠し、クリア・テキストになっていることを確認します。

タスク 7: bulkload.sh -check モードの実行とスキーマ違反または重複エラーが残っているかどうかの判断

LDIF ファイルを生成してロードする前には、必ず bulkload ユーティリティのチェック・モードを使用して LDIF ファイルのチェックを実行してください。bulkload の出力によって、データの非一貫性がレポートされます。

注意： Windows オペレーティング・システムでシェル・スクリプト・ツールを実行するには、次のいずれかの UNIX エミュレーション・ユーティリティが必要です。

- Cygwin 1.3.2.2-1 以上
  サイト：http://sources.redhat.com
- MKS Toolkit 6.1
  サイト：http://www.datafocus.com/

関連項目： bulkload のチェック・モードの使用方法は、A-45 ページの「bulkload の構文」を参照してください。

ユーザー・データのアプリケーション固有リポジトリからの移行

ユーザー・データをアプリケーション固有のリポジトリから移行するには、次の処理が必要です。

- ユーザー・データをアプリケーション固有のリポジトリから収集し、ディレクトリが読み込める書式に設定します。
- ディレクトリ管理者がそのデータを使用できるようにします。ディレクトリ管理者は、次の作業を行う必要があります。
  - ディレクトリ内でデータを格納する場所を指定します。
  - データをディレクトリにインポートします。

中間テンプレート・ファイル

この移行を実行するには、Oracle Directory Provisioning Integration Service は、アプリケーション固有のリポジトリを使用して、そのデータを中間テンプレート・ファイルにエクスポートする必要があります。このテンプレート・ファイル内のレコードは、完全な LDIF にはなっていません。これらのレコードには、情報が最終的に格納されるディレクトリの場所などに関連する置換変数が入っています。これらの変数は未定義のまま残されるため、ディレクトリ管理者は後で定義できます。

ユーザー・データをこの中間テンプレート・ファイルから適切な LDIF に変換するには、OID 移行ツール（ldifmigrator）を使用します。LDIF に変換されたデータは、ディレクトリにロードできます。

要約すると、アプリケーション固有のリポジトリからデータを移行するには、通常、次の手順を実行します。

1. アプリケーション固有のデータを中間テンプレート・ファイルとしてエクスポートします。
2. ディレクトリ管理者は、OID 移行ツール（ldifmigrator）を使用して、不完全な LDIF エントリをテンプレート・ファイルからロードし、配置の選択に基づいて完全な LDIF エントリに変換します。
3. ディレクトリ管理者は、この完全な LDIF のデータを Oracle Internet Directory にロードします。
4. アプリケーションは、独自の仕様に従って移行処理を完了します。

アプリケーション・リポジトリ内のデータと Oracle Internet Directory に既存のデータとの調停

アプリケーション固有のリポジトリから移行しているデータが、Oracle Internet Directory にすでに存在している場合があります。この場合、OID 移行ツール（ldifmigrator）の調停機能を使用して、2 つのディレクトリ間の差分を調整できます。

関連項目：

- A-137 ページの「ロード機能」
- OID 移行ツールの調停機能の詳細は、A-137 ページの「調停機能」を参照してください。

アプリケーション固有のリポジトリからデータを移行するためのタスク

アプリケーション固有のリポジトリからデータを移行するには、中間テンプレート・ファイルを作成してから、OID 移行ツールを実行します。

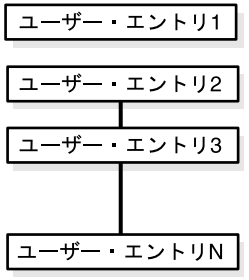
タスク 1: 中間テンプレート・ファイルの作成

各国語のデータを生成するアプリケーションでは、中間テンプレート・ファイルにデータを AL32UTF8 で格納する必要があります。詳細は、`http://www.ietf.org` で、IETF の RFC 2849「The LDAP Data Interchange Format（LDIF）- Technical Specification（LDAP Data Interchange Format（LDIF）ー 技術仕様）」を参照してください。

中間テンプレート・ファイルの生成時に、移行を実行するアプリケーションでは、RFC 2849 で定義されているレコード・セパレータを使用して、すべてのユーザー・レコードを順にリストする必要があります。OID 移行ツール（ldifmigrator）は、デフォルトの認証管理レルム（企業自体に対応しています）にすべてのユーザーを割り当てます。

図 23-1 に、ユーザー・エントリが格納される中間テンプレート・ファイルの全体構造を示します。

図 23-1 中間ユーザー・ファイルの構造



中間テンプレート・ファイルでは、次の形式を使用して、有効なユーザー・エントリが生成されます。**太字**の文字列は、すべてアプリケーション固有のリポジトリから提供されます。

```
dn: cn=UserID, %s_UserContainerDN%
sn: Last_Name
orclGlobalID: GUID_for_User
%s_UserNicknameAttribute%: UserID
objectClass: inetOrgPerson
objectClass: orclUserV2
```

このテンプレートの文字列 **%s_UserContainerDN%** と **%s_UserNicknameAttribute%** は置換変数で、OID 移行ツールによって値が提供されます。OID 移行ツールは、配置に固有な考慮事項に従ってこれらの値を判別します。引数は、アプリケーションが OID 移行ツールに渡すか、ツールがディレクトリから取得します。

例 : 中間テンプレート・ファイル内のユーザー・エントリ 次の中間テンプレート・ファイルには、アプリケーション固有の移行ロジックによって生成されたユーザー・エントリが格納されます。この例にある**太字**のデータは、すべてアプリケーション固有のユーザー・リポジトリから提供されます。

```
dn: cn=jdoe, %s_UserContainerDN%
sn: Doe
%s_UserNicknameAttribute%: jdoe
objectClass: inetOrgPerson
objectClass: orclUserV2
title: Member of Technical Staff
homePhone: 415-584-5670
homePostalAddress: 234 Lez Drive$ Redwood City$ CA$ 94402


dn: cn=jsmith, %s_UserContainerDN%
sn: Smith
%s_UserNicknameAttribute%: jsmith
objectClass: inetOrgPerson
objectClass: orclUserV2
title: Member of Technical Staff
homePhone: 650-584-5670
homePostalAddress: 232 Gonzalez Drive$ San Francisco$ CA$ 94404


dn: cn=lrider, %s_UserContainerDN%
sn: Rider
%s_UserNicknameAttribute%: lrider
objectClass: inetOrgPerson
objectClass: orclUserV2
title: Senior Member of Technical Staff
homePhone: 650-584-5670
```

中間ファイルの形式に変換されたすべてのユーザー・データは、さらに、OID 移行ツールによって、Oracle Internet Directory にロード可能な適切な LDIF ファイルに変換されます。

中間テンプレート・ファイルの例は、*$ORACLE_HOME*/ldap/schema/oid にあります。

ユーザー・エントリの属性 各ユーザー・エントリには、必須とオプションの属性があります。

表 23-1 に、ユーザー・エントリの必須属性を示します。

表 23-1 ユーザー・エントリの必須属性

属性	説明
dn	適切な置換変数を持つユーザー・エントリの識別名。エントリの相対識別名には、必ず cn 属性を含める必要があります。
sn	ユーザーの姓。
objectclass	エントリが最小限、属する必要があるオブジェクト・クラス。inetOrgPerson および orclUserV2 があります。

関連項目：

- inetOrgPerson オブジェクト・クラスの各属性については、http://www.ietf.org で、IETF の RFC2798「Definition of the inetOrgPerson LDAP Object Class（inetOrgPerson LDAP オブジェクト・クラスの定義）」を参照してください。
- B-17 ページの「orclUserV2 オブジェクト・クラスのオプション属性」

タスク 2: OID 移行ツールの実行

中間テンプレート・ファイルを設定すると、OID 移行ツールによって、すべての関連データがアプリケーション固有のリポジトリから Oracle Internet Directory に移行できます。データの移行後は、そのアプリケーションと Oracle Internet Directory を同期化することによって、アプリケーションに関連するあらゆるデータを更新できます。同期化には、Oracle Directory Synchronization Service を使用します。

関連項目： OID 移行ツールの使用方法は、A-132 ページの「OID 移行ツール（ldifmigrator）の構文」を参照してください。

デフォルトのディレクトリ構造への既存ディレクトリの移行

Oracle Internet Directory のインストール時に、Oracle Universal Installer によって、デフォルトのスキーマとディレクトリ情報ツリー（DIT）が作成されます。第 19 章「Oracle Identity Management レルムの配置」に説明したこのデフォルトのディレクトリ情報ツリー・フレームワークには柔軟性があるため、配置要件に応じて適切に変更できます。

すでに確立された構造を持つディレクトリが存在し、データをそのディレクトリからデフォルトのディレクトリ構造の環境に移行する場合は、この項の指示に従ってください。この項では、次の項目について説明します。

- デフォルトのディレクトリ構造
- デフォルトの認証管理レルムの Oracle コンテキスト内にあるユーザーまたはグループの位置の変更

デフォルトのディレクトリ構造

Oracle Internet Directory 10*g*（9.0.4）では、次のディレクトリ要素がデフォルトで作成されます。

- ルート Oracle コンテキスト（`cn=OracleContext`）－企業全体の構成データが Oracle 製品によって格納されるコンテナです。
- デフォルトの認証管理レルム（`dc=`*`dns_domain_of_host`*`,dc=com`）－ Oracle 製品による企業ユーザーおよびグループの検索対象となるコンテナです。企業の DIT 構造と似ています。たとえば、`my_computer.us.my_company.com` というホスト名のコンピュータに Oracle Internet Directory をインストールした場合、Oracle Internet Directory インストール時に作成されるデフォルトの認証管理レルムは、`dc=us,dc=my_company,dc=com` となります。Oracle 製品による検索対象となるのは、`cn=users,dc=us,dc=my_company,dc=com` の下のすべてのユーザーおよび `cn=groups,dc=us,dc=my_company,dc=com` の下のすべてのグループです。

このデフォルトの認証管理レルムは、すべての企業ユーザーを別のコンテナに格納するなど、配置要件に応じて変更してもかまいません。

デフォルトの認証管理レルムの Oracle コンテキスト内にあるユーザーまたはグループの位置の変更

Oracle コンテキスト内のユーザーまたはグループの位置を変更するには、デフォルトの認証管理レルム・エントリでポインタに適切な変更を加えます。次の LDIF ファイルの例では、Oracle コンテキスト内のユーザーまたはグループの位置を o=my_company,dc=com に変更します。

```
dn: cn=common,cn=products,cn=oracleContext,dc=default_subscriber_name,dc=com
changetype: modify
replace: orclCommonUserSearchBase
orclCommonUserSearchBase: o=my_company,dc=com
```

第 V 部

ディレクトリ・レプリケーションおよび高可用性

第V部では、レプリケーションおよび高可用性の詳細とその計画および管理方法について説明します。第V部は次の各章で構成されています。

- 第 24 章「ディレクトリ・レプリケーションの概要」
- 第 25 章「Oracle ディレクトリ・レプリケーションの管理」
- 第 26 章「高可用性とフェイルオーバーに関する考慮事項」
- 第 27 章「ラックマウント型ディレクトリ・サーバー構成」
- 第 28 章「コールド・フェイルオーバー・クラスタ構成」
- 第 29 章「Oracle9i Real Application Clusters 環境でのディレクトリ」

24

ディレクトリ・レプリケーションの概要

2-21 ページの「ディレクトリ・レプリケーション」では、レプリケーションの概要を説明しました。この章ではさらに詳しく説明します。次の項目について説明します。

- ディレクトリ・レプリケーションの概要
- 完全および部分ディレクトリ・レプリケーション
- ディレクトリ・レプリケーション・グループ
- レプリケーションに含まれるネーミング・コンテキストと除外されるネーミング・コンテキスト
- レプリケーション承諾
- ディレクトリ内のレプリケーション構成オブジェクト
- レプリケーションのセキュリティ
- ディレクトリ・レプリケーションの変更ログ
- マルチマスター・レプリケーション
- ファンアウトおよび部分レプリケーション
- 部分レプリケーションのフィルタ処理に関する規則

> **関連項目：** レプリケーションの管理方法は、第 25 章「Oracle ディレクトリ・レプリケーションの管理」を参照してください。

ディレクトリ・レプリケーションの概要

この項では、レプリケーションの基本的な概念について簡単に説明します。これらの概念の詳細は、この章の他の項で説明します。

レプリケーションは、複数のディレクトリ・サーバーに同じネーミング・コンテキストをコピーし、管理するプロセスです。問合せの処理に複数のサーバーで備えることによってパフォーマンスを向上させ、シングル・ポイント障害に伴うリスクを排除して信頼性を向上させます。

レプリケーションには、完全レプリケーションと部分レプリケーションがあります。

完全レプリケーションでは、DIT 全体を別のノードに伝播します。

部分レプリケーションでは、DIT 全体ではなく 1 つ以上のサブツリーを別のノードに伝播します。

指定したネーミング・コンテキストのレプリケーションの対象となるディレクトリ・サーバーは、ディレクトリ・レプリケーション・グループ（DRG）と呼ばれるグループを形成します。DRG を構成するディレクトリ・サーバー間の関係は、各ノード上でレプリケーション承諾と呼ばれる特別なディレクトリ・エントリによって表されます。

サーバー内に格納されているネーミング・コンテキストの各コピーは、レプリカと呼ばれます。レプリカは、読取り専用または更新可能（あるいはその両方）です。更新可能レプリカを保持するサーバーは、サプライヤと呼ばれます。このレプリカを変更すると、コンシューマと呼ばれる他のサーバーに伝播されます。

ディレクトリ・レプリケーション・グループは、単一マスター、マルチマスター、ファンアウトのいずれかです。

単一マスター・レプリケーション・グループには、1 つ以上のコンシューマに変更をレプリケートするサプライヤが 1 つのみ存在します。更新できるのはサプライヤのみで、コンシューマは読取り専用です。

マルチマスター・レプリケーションは、peer-to-peer レプリケーションまたは *n*-way レプリケーションとも呼ばれ、同等に機能する複数のサイトが、レプリケートされたデータのグループを管理できるようにします。マルチマスター・レプリケーション環境では、各ノードはサプライヤ・ノードであると同時にコンシューマ・ノードであり、各ノードでディレクトリ全体がレプリケートされます。

ファンアウト・レプリケーション・グループは、point-to-point レプリケーション・グループとも呼ばれ、コンシューマに直接レプリケートするサプライヤを持っています。そのコンシューマは、1 つ以上の別のコンシューマにレプリケートできます。レプリケーションには、完全レプリケーションと部分レプリケーションがあります。

ディレクトリ・レプリケーション・グループの場合、ノード間でデータを転送するプロトコルは、Oracle9*i* Advanced Replication または LDAP のいずれかに基づきます。

完全および部分ディレクトリ・レプリケーション

この項では、次の項目について説明します。

完全ディレクトリ・レプリケーション

完全レプリケーションでは、DIT 全体を別のノードに伝播します。このタイプのレプリケーションでは、ディレクトリ全体の高可用性が保証されます。このレプリケーションを使用して、ディレクトリ全体の操作を様々なノードに分散することもできます。

完全レプリケーションは、Oracle9*i* Advanced Replication または LDAP に基づきます。

部分ディレクトリ・レプリケーション

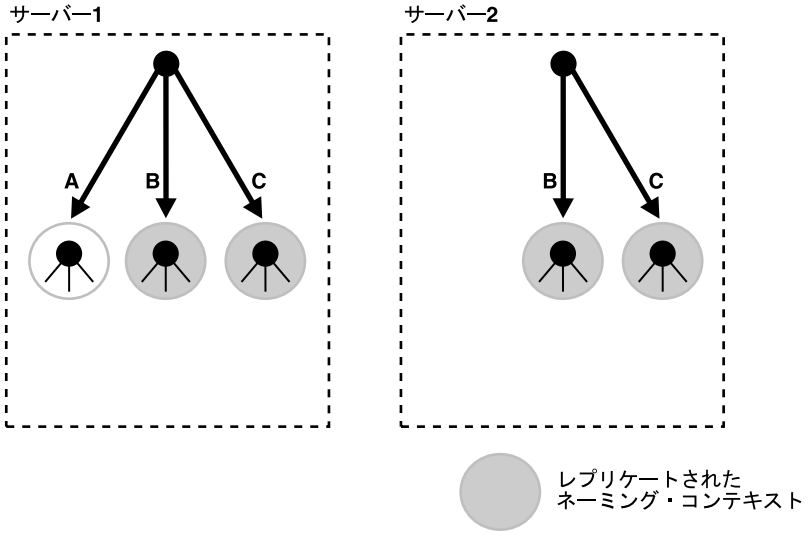
部分レプリケーションでは、DIT 全体ではなく、1 つ以上のサブツリーを別のノードに伝播できます。この方法でディレクトリを分散することによって、サーバー間の作業負荷を均衡化し、フォルト・トレランスおよびフェイルオーバー機能を備え、可用性に優れた分散ディレクトリを構築することができます。部分レプリケーションでは、データがクライアントに近づくため、応答時間が短くなり、パフォーマンスが向上します。部分レプリケーションは、レプリケーション環境管理ツールを使用して構成できます。

部分レプリケーションは、LDAP ベースのみです。Oracle9*i* Advanced Replication は使用しません。

関連項目： A-62 ページの「レプリケーション環境管理ツール」

図 24-1 に、部分レプリケーションの例を示します。

図 24-1 部分レプリケーションの例



部分レプリケーションの使用例では、ディレクトリ全体ではなく、1 つ以上のネーミング・コンテキストがレプリケートされます。たとえば、図 24-1 では、サーバー 1 に、A、B、C の 3 つのネーミング・コンテキストが含まれます。ネーミング・コンテキスト B および C は、サーバー 2 にレプリケートされますが、ネーミング・コンテキスト A はレプリケートされません。

表 24-1 に、2 つのタイプのレプリケーションの比較を示します。

表 24-1 完全および部分レプリケーションの比較

完全レプリケーション	部分レプリケーション
ディレクトリ全体を他のノードに伝播します。	ディレクトリの一部（すべてのネーミング・コンテキストではなく、1 つ以上のネーミング・コンテキスト）のみを他のノードに伝播します。
伝播先ノードの数は制限されます。	伝播先ノードの数は制限されません。
マルチマスター環境で、コンシューマは複数のサプライヤから変更を受け取ることができます。	単一マスター環境で、コンシューマは 1 つのサプライヤからのみ変更を受け取ることができます。

ディレクトリ・レプリケーション・グループ

この項では、次の項目について説明します。

- ディレクトリ・レプリケーション・グループでのノード間のデータ転送
- 単一マスター・レプリケーション・グループ
- マルチマスター・レプリケーション・グループ
- ファンアウト・レプリケーション・グループ
- ディレクトリ・レプリケーションの各タイプの比較
- ファンアウトを使用したマルチマスター・レプリケーション

関連項目： 24-12 ページの「レプリケーション承諾」

ディレクトリ・レプリケーション・グループでのノード間のデータ転送

ディレクトリ・レプリケーション・グループの場合、データを転送するためのプロトコルは、Oracle9*i* Advanced Replication または LDAP のいずれかに基づきます。表 24-2 に、各タイプによるレプリケーションの様々な機能の処理方法および詳細情報の参照先を示します。

表 24-2 ディレクトリ・レプリケーション・グループでのノード間のデータ転送のタイプ

機能	LDAP ベースのレプリケーション	Oracle9*i* Advanced Replication ベースのレプリケーション	詳細情報の参照先
変更の伝播	サプライヤからコンシューマへの変更の伝播は、LDAP を介して行われます。	サプライヤからコンシューマへの変更の伝播は、Oracle9*i* Advanced Replication を介して行われます。	24-19 ページの「ディレクトリ・レプリケーションの変更ログ」
サポートされるレプリカ・タイプ	読取り専用完全レプリカ 読取り専用部分レプリカ	読取り / 書込み可能完全レプリカ	24-3 ページの「完全ディレクトリ・レプリケーション」 24-3 ページの「部分ディレクトリ・レプリケーション」

表 24-2 ディレクトリ・レプリケーション・グループでのノード間のデータ転送のタイプ（続き）

機能	LDAP ベースのレプリケーション	Oracle9*i* Advanced Replication ベースのレプリケーション	詳細情報の参照先
サポートされる構成	単一マスター・レプリケーション ファンアウト・レプリケーション	マルチマスター・レプリケーション 単一マスター・レプリケーション（マルチマスター構成内の 1 つを除く他のすべてのマスターを読取り専用モードに切り替えた場合）	24-6 ページの「単一マスター・レプリケーション・グループ」 24-7 ページの「マルチマスター・レプリケーション・グループ」 24-8 ページ「ファンアウト・レプリケーション・グループ」

単一マスター・レプリケーション・グループ

単一マスター・レプリケーション・グループには、1 つ以上のコンシューマに変更を提供するサプライヤのレプリカが 1 つのみ存在します。クライアントは、マスター・レプリカのみ更新できます。また、任意のコンシューマのデータの読取りのみ可能です。

図 24-2 に、単一マスター・レプリケーション環境を示します。

図 24-2 単一マスター・レプリケーションの例

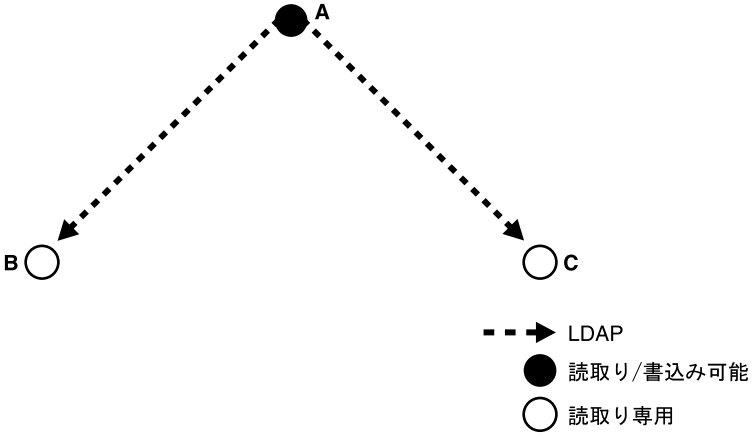


図 24-2 にある各黒丸は、Oracle Internet Directory のノードを表しています。ノード A は、コンシューマ・ノード B および C をレプリケートするサプライヤで、ノード A は読取り / 書込み可能、ノード B および C は読取り専用です。データ転送プロトコルは LDAP です。

マルチマスター・レプリケーション・グループ

マルチマスター・レプリケーションは、peer-to-peer レプリケーションまたは *n*-way レプリケーションとも呼ばれ、同等に機能する複数のノードが、レプリケートされたデータのグループを管理できるようにします。マルチマスター・レプリケーション・グループでは、各ディレクトリ・サーバーは、変更のサプライヤであると同時にコンシューマであり、各ノードでディレクトリ全体がレプリケートされます。

図 24-3 の例に、マルチマスター・レプリケーション・グループ内で相互に更新する 3 つのノード（A、B、C）を示します。

図 24-3 マルチマスター・レプリケーションの例

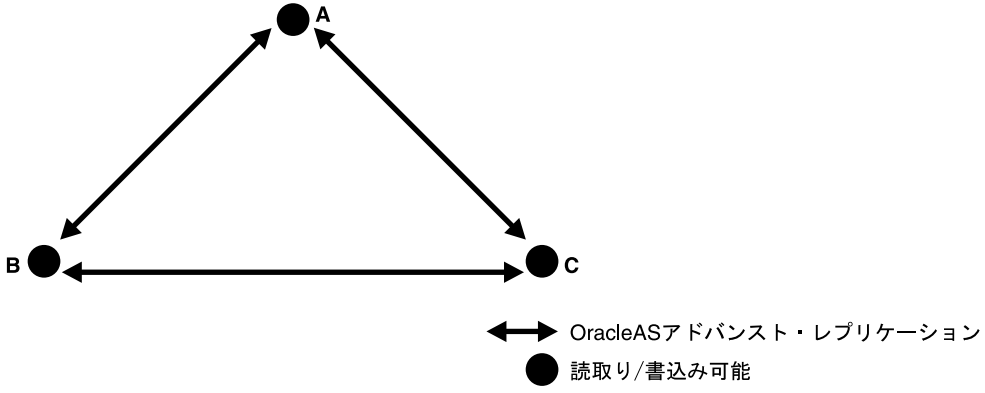


図 24-3 では、各ノードは読取り / 書込み可能で、データ転送プロトコルは、Oracle9*i* Advanced Replication に基づきます。

注意： 『Oracle Application Server Single Sign-On 管理者ガイド』の高可用性に関する章のレプリケーションのための Oracle Application Server Single Sign-On の構成に関する項に説明されているとおり、Oracle Application Server Single Sign-On でサポートされているレプリケーション方式は、マルチマスター・レプリケーションのみです。

関連項目： マルチマスター・レプリケーションの詳細は、24-19 ページの「マルチマスター・レプリケーション」を参照してください。

ファンアウト・レプリケーション・グループ

ファンアウト・レプリケーション・グループは、point-to-point レプリケーション・グループとも呼ばれ、コンシューマに直接レプリケートするサプライヤを持っています。そのコンシューマは、1 つ以上の別のコンシューマに同一データを提供できます。レプリケーションには、完全レプリケーションと部分レプリケーションがあります。

図 24-4 に、ファンアウト・レプリケーション環境を示します。

図 24-4 単一マスター・レプリケーションの例

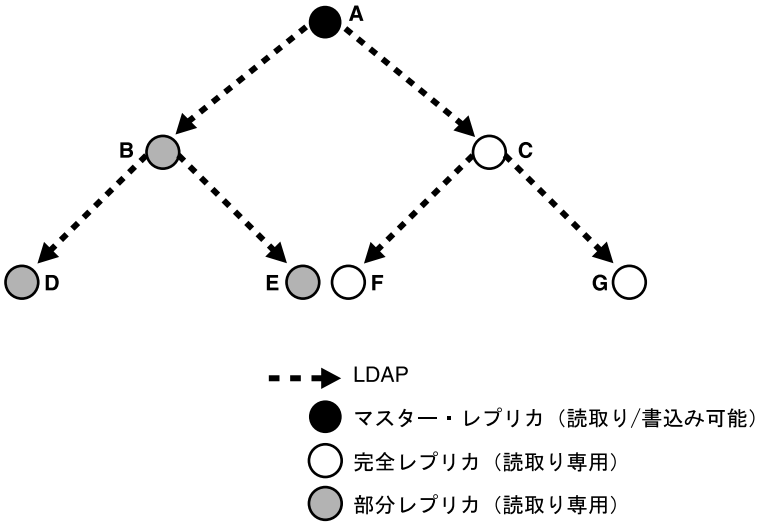


図 24-4 では、サプライヤ A は、B および C の 2 つのコンシューマをレプリケートします。コンシューマ・ノード B には、A の部分レプリカがあり、コンシューマ・ノード C には、A の完全レプリカがあります。コンシューマ・ノード B および C は読取り専用です。

これらの各ノードが、データを他の 2 つのコンシューマにレプリケートするサプライヤとして機能します。ノード B はノード D および E に対して部分レプリケーションを行い、ノード C はノード F および G に対して完全レプリケーションを行います。

ファンアウト・レプリケーションでは、ノードは LDAP を使用してデータを転送します。

ディレクトリ・レプリケーションの各タイプの比較

表 24-3 に、マルチマスター、単一マスターおよびファンアウト・レプリケーションの比較を示します。

表 24-3 マルチマスター、単一マスターおよびファンアウト・レプリケーションの比較

マルチマスター・レプリケーション	単一マスター・レプリケーション	ファンアウト・レプリケーション
Oracle9*i* Advanced Replication のみを使用します。	LDAP ベースのレプリケーションを使用します。	LDAP ベースのレプリケーションを使用します。
サプライヤまたはコンシューマに関係なく、すべてのノードが更新の対象になります。	更新の対象となるのは、サプライヤのみです。コンシューマの変更は、他のファンアウト・コンシューマに伝播されますが、サプライヤに戻されることはありません。	更新の対象となるのは、サプライヤのみです。コンシューマの変更は、他のファンアウト・コンシューマに伝播されますが、サプライヤに戻されることはありません。LDAP ベースのレプリカ・ノードが読み書き可能な場合も同様です。

ファンアウトを使用したマルチマスター・レプリケーション

Oracle Internet Directory リリース 9.0.4 では、マルチマスター・レプリケーション・グループ内のすべてのノードが、データのすべてまたは一部を読取り専用コンシューマに提供できます。このコンシューマは、ファンアウト構成の他のコンシューマにデータを提供できます。マルチマスター・レプリケーション承諾内では、ノード間のデータ転送は Oracle9*i* Advanced Replication を介して行われます。ファンアウト・レプリケーション承諾内では、サプライヤからコンシューマへのデータ転送は LDAP を介して行われます。

注意： LDAP ベースのレプリカが読取り / 書込み可能な場合、このノードに対する変更は、コンシューマには伝播されますが、サプライヤには伝播されません。

図 24-5 に、ファンアウト・レプリケーションと組み合せて使用するマルチマスター・レプリケーションの例を示します。

図 24-5 ファンアウトを使用するマルチマスター・レプリケーションの例

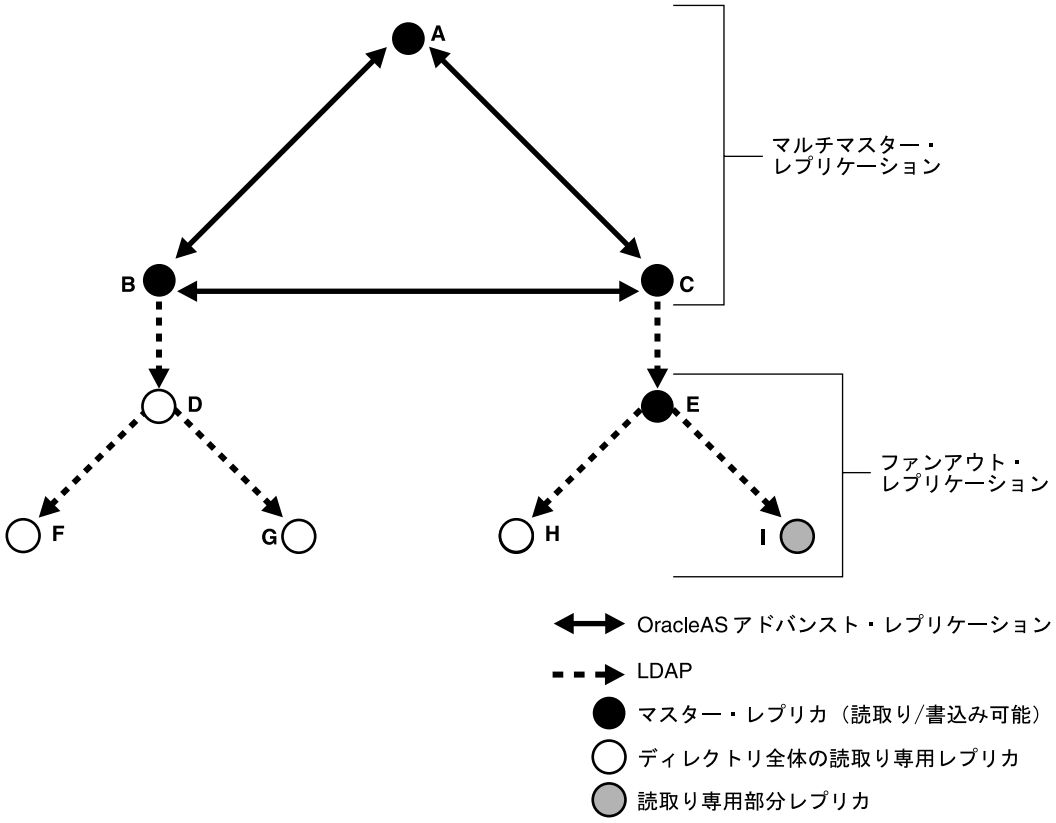


図 24-5 の例では、3 つのノード（A、B、C）が、マルチマスター・レプリケーション・グループを形成しています。これらのノード間では、Oracle9*i* Advanced Replication を使用してデータを転送します。

ノード B は、ディレクトリ全体の読取り専用レプリカであるノード D に変更を提供します。ノード D は、LDAP ベースのレプリケーションを使用して、ノード F および G に変更を提供します。ノード F および G は、ディレクトリ全体の読取り専用レプリカです。同様に、ノード C も、ディレクトリ全体の読み書き可能レプリカであるノード E に変更を提供します。ノード E は、LDAP ベースのレプリケーションを使用して、ディレクトリ全体の読取り専用レプリカであるノード H および読取り専用の部分レプリカであるノード I に変更を提供します。

関連項目： ファンアウト・レプリケーションの詳細は、24-31 ページの「ファンアウトおよび部分レプリケーション」を参照してください。

レプリケーションに含まれるネーミング・コンテキストと除外されるネーミング・コンテキスト

レプリケーションでは特定のネーミング・コンテキストを指定し、そのネーミング・コンテキスト内の 1 つ以上のサブツリーをレプリケーションから除外できます。ネーミング・コンテキスト内の 1 つ以上の属性もレプリケーションから除外できます。

LDAP ベースのレプリケーションでは、デフォルトでネーミング・コンテキストがレプリケーションから除外されます。

Oracle9*i* Advanced Replication ベースのレプリケーションでは、デフォルトでネーミング・コンテキストが含まれます。レプリケーションからネーミング・コンテキストを除外するには、レプリケーション承諾 `orclagreementid=000001` 内の `orclexcludednamingcontext` 属性にネーミング・コンテキストを指定します。

24-11 ページの図 24-6 およびその後に続く説明では、ネーミング・コンテキスト・コンテナおよびそのオブジェクトの使用例を示します。

図 24-6 ネーミング・コンテキスト・コンテナおよびオブジェクトの例

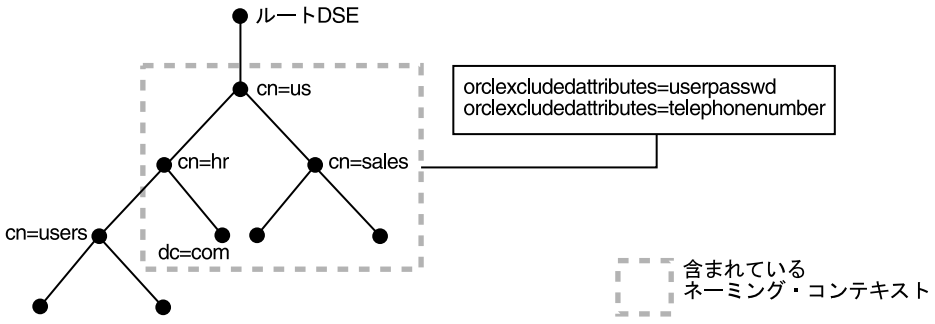


図 24-6 では、レプリケーションに含まれるネーミング・コンテキストは `cn=us` です。このネーミング・コンテキスト内では、1 つのサブツリー（`cn=users,cn=hr,cn=us`）がレプリケーションから除外されています。さらに、ネーミング・コンテキスト `cn=us` の `userpassword` および `telephonenumber` という 2 つの属性がレプリケーションから除外されています。

関連項目： 24-14 ページの「レプリケーションのネーミング・コンテキスト・コンテナ・エントリ」

レプリケーション承諾

レプリケーション承諾は、DRG 内のサーバー間の関係に関する情報を含む特別なエントリです。Oracle Internet Directory の場合、これらのすべてのエントリは、ルート DSE にあるコンテナ・エントリ cn=replication configuration 内に常駐しています。このエントリは、DRG 内の各ノードに常駐し、それぞれのノードに関するすべてのレプリケーション情報を含んでいます。

レプリケーション承諾には、マルチマスター・レプリケーション・グループ用と単一マスター・レプリケーション・グループ用の 2 つの種類があります。

この項では、次の項目について説明します。

マルチマスター・レプリケーション承諾

マルチマスター・レプリケーション・グループの場合、レプリケーション承諾は、Oracle9*i* Advanced Replication に基づきます。各ノードのレプリケーション承諾に、グループ内のすべてのノードが示されます。レプリケーション承諾は各ノードで同一ですが、ローカル・ディレクトリ・サーバー上にパーティション化されたネーミング・コンテキストなどのローカル・オプションは異なります。

このタイプのレプリケーション承諾のエントリは、コンテナ・エントリ cn=replication configuration の直下に常駐しています。たとえば、このような承諾の DN は、orclagreementID=000001,cn=replication configuration のようになります。

単一マスター・レプリケーション承諾

マルチマスター・レプリケーション・グループ用のレプリケーション承諾とは異なり、単一マスター・レプリケーション・グループ用のレプリケーション承諾は、LDAP ベースです。各ファンアウト・レプリケーション・グループに対して、サプライヤとコンシューマ間の関係ごとにレプリケーション承諾が 1 つ存在します。

このタイプのレプリケーション承諾のエントリは、サプライヤとして機能するノードの直下に常駐しています。したがって、サプライヤ・ノードに対するレプリケーション承諾は、次のようになります。

```
orclagreementID=unique_identifier_of_the_replication_agreeement,
orclReplicaID=unique_identifier_of_supplier_node,
cn=replication configuration
```

同様に、コンシューマ・ノードに対するレプリケーション承諾は、次のようになります。

```
orclagreementID=unique_identifier_of_the_replication_agreeement,
orclReplicaID=unique_identifier_of_supplier_node,
cn=replication configuration
```

ファンアウト・レプリケーション承諾の場合、親ノードを調べることで、承諾エントリと関連付けられているノードを識別できます。次に、レプリケーション承諾エントリの例を示します。

```
orclagreementID=000002,orclReplicaID=node_A,cn=replication
configuration
```

この例では、orclagreementID=000002 で表されたレプリケーション承諾がノード A と関連付けられていることを確認できます。これは、orclagreementID=000002 の親が orclReplicaID=node_A であるためです。

注意： コンテナ・エントリ cn=replication configuration は、すべてのノードでレプリケートされますが、すべてのノードで同一ではない場合があります。

関連項目： 24-14 ページの「レプリケーションのネーミング・コンテキスト・コンテナ・エントリ」

ディレクトリ内のレプリケーション構成オブジェクト

この項では、レプリケーション構成情報を含むディレクトリ内のオブジェクトについて説明します。この項では、次の項目について説明します。

- レプリケーション構成コンテナ
- レプリカ・サブエントリ
- レプリケーション承諾エントリ
- レプリケーションのネーミング・コンテキスト・コンテナ・エントリ
- ディレクトリ内のレプリケーション構成オブジェクトの例

レプリケーション構成コンテナ

ノードに関するすべてのレプリケーション情報は、ルート DSE にあるコンテナ cn=replication configuration 内に常駐しています。このエントリは、DRG 内の各ノードに常駐します。

レプリカ・サブエントリ

このサブエントリは、インストール時にレプリケーション構成コンテナの下に作成されます。このサブエントリには、関連するノードの特性を識別し定義する属性が含まれています。

このサブエントリは、orclReplicaSubentry オブジェクト・クラスに関連付けられています。このサブエントリには、レプリカ・サブエントリの名前を指定する値を持つ orclreplicaID 属性が含まれています。これは、各ディレクトリ・ノード固有の属性で、ルート DSE にある orclreplicaID 属性の値と一致します。たとえば、24-17 ページの図 24-9 では、レプリカ・サブエントリは orclReplicaID=*UID_of_node_D*,cn=replication configuration で表されています。

> **関連項目：** レプリカ・サブエントリの属性の詳細は、B-36 ページの表 B-31 を参照してください。

レプリケーション承諾エントリ

このエントリには、コンシューマとサプライヤ間のレプリケーション承諾を定義する属性が含まれています。このエントリは、レプリケーション構成エントリの下に常駐し、orclReplAgreementEntry オブジェクト・クラスに関連付けられています。このエントリのネーミング属性は、orclagreementID です。たとえば、24-17 ページの図 24-9 では、レプリケーション承諾エントリは orclagreementID=000003,orclReplicaID=*UID_of_node_D*,cn=replication configuration で表されています。

> **関連項目：** レプリケーション承諾エントリの属性の詳細は、B-37 ページの表 B-32 を参照してください。

レプリケーションのネーミング・コンテキスト・コンテナ・エントリ

このエントリには、LDAP ネーミング・コンテキストのすべてのオブジェクトが含まれています。これらのオブジェクトは、LDAP ベースの部分レプリカに対するレプリケーションに含むものまたはこのレプリケーションから削除するものを指定します。

このエントリには、相対識別名（RDN）cn=replication namecontext が含まれています。この相対識別名は、インストール時に orclagreementID エントリの下に作成されます。

レプリケーションのネーミング・コンテキストには、次のオブジェクトが含まれています。

- orclincludednamingcontexts: レプリケートされるネーミング・コンテキストのルート。
- orclexcludednamingcontexts: レプリケーションに含まれるネーミング・コンテキスト内で、レプリケーションから除外されるサブツリーのルート。

- `orclexcludedattributes`: 包含対象ネーミング・コンテキスト内で、レプリケーションから除外される属性。

  関連項目： レプリケーションのネーミング・コンテキスト・コンテナ・エントリの属性の詳細は、B-39 ページの表 B-33 を参照してください。

ディレクトリ内のレプリケーション構成オブジェクトの例

この項で説明するレプリケーション・オブジェクトの例は、図 24-7 に示すレプリケーション環境に依存します。

図 24-7 例 : マルチマスター・レプリケーションおよびファンアウト・レプリケーション

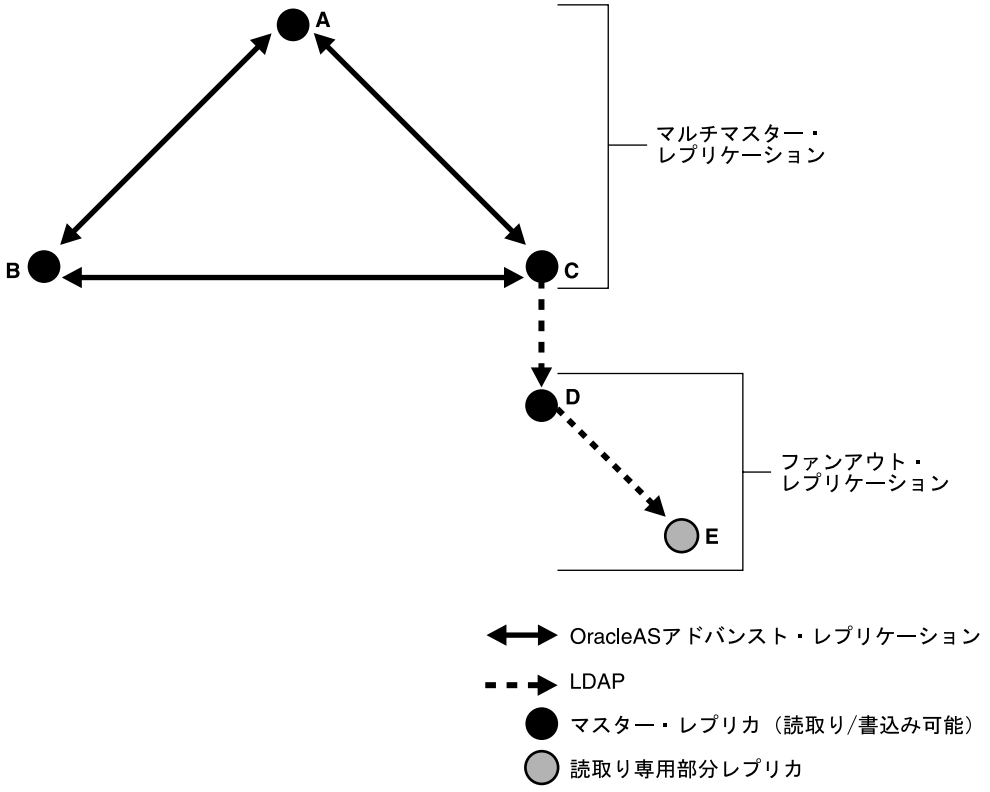


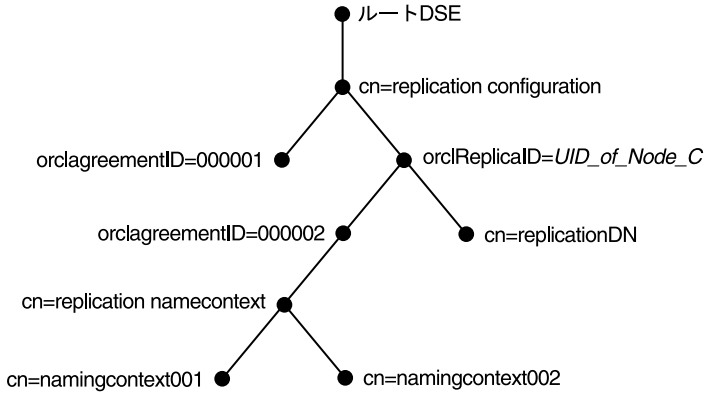
図 24-7 では、3 つのノード（A、B、C）が、マルチマスター・レプリケーション・グループを形成しています。ノード C は、4 番目のノード D に対してレプリケーションを行い、ノード D はノード E にファンアウトします。

この環境のレプリケーション承諾は、次のとおりです。

- ノード A には、ノード B および C とのマルチマスター関係を表す 1 つのレプリケーション承諾があります。
- ノード B には、ノード A および C とのマルチマスター関係を表す 1 つのレプリケーション承諾があります。
- ノード C には、2 つのレプリケーション承諾があります。1 つは、ノード A および B とのマルチマスター関係を表し、もう 1 つは、ノード C がサプライヤでノード D がコンシューマというノード D との関係を表しています。
- ノード D には、2 つのレプリケーション承諾があります。1 つは、変更情報の消費元のサプライヤ・ノード C との関係を表し、もう 1 つは、ノード D がサプライヤとなるコンシューマ・ノード E との関係を表しています。

図 24-8 に、24-15 ページの図 24-7 のノード C に関連する DIT 内のレプリケーション・オブジェクトを示します。

図 24-8 例 : ノード C についてのレプリケーション構成エントリ



ノード C の場合、ルート DSE にあるエントリ `cn=replication configuration` には、次の RDN が含まれています。

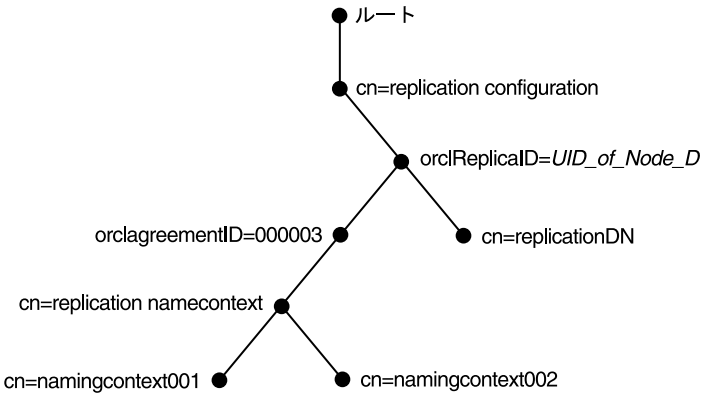
- `orclagreementID=000001`: ノード C がノード A および B とともにメンバーになっているマルチマスター・レプリケーション承諾。
- `orclReplicaID=`*`UID_of_node_C`*: ノード情報が含まれているノード C の一意識別子。
- `orclagreementID=000002`: サプライヤ・ノード C とコンシューマ・ノード D 間の関係についての一意識別子。この場合、ノード C が親になっているため、`orclagreementID=000002` がサプライヤ・ノード C のレプリケーション承諾です。

  このエントリには、`orclreplicaDN` 属性が含まれています。この属性の値は、レプリケーション承諾がノード C に含まれているコンシューマ・ノード D の DN です。

- cn=replicationDN: ノード C 上のディレクトリ・レプリケーション・サーバーが、ディレクトリ・サーバーにバインドする場合に使用するバインド識別名。
- cn=replication namecontext: レプリケーションに含まれるネーミング・コンテキストに関する情報のコンテナ。
- cn=namingcontext001 および cn=namingcontext002: レプリケーションに含まれているか、またはレプリケーションから除外されている実際のオブジェクト。レプリケーションに含まれるネーミング・コンテキストには、レプリケーションから除外する 1 つ以上のサブツリーを指定できます。また、レプリケーションから除外する特定の属性も指定できます。

図 24-9 に、24-15 ページの図 24-7 のノード D に関連する DIT 内のレプリケーション承諾エントリを示します。

図 24-9 例 : ノード D についてのレプリケーション構成エントリ



ノード D の場合、ルート DSE にあるエントリ cn=replication configuration には、次の RDN が入っています。

- orclReplicaID=*UID_of_node_D*: ノード情報が含まれているノード D の一意識別子。
- orclagreementID=000003: サプライヤ・ノード D とコンシューマ・ノード E 間の関係についての一意識別子。この場合、ノード D が親になっているため、orclagreementID=000003 がサプライヤ・ノード D のレプリケーション承諾です。

  このエントリには、orclreplicaDN 属性が含まれています。この属性の値は、レプリケーション承諾がノード D に含まれているコンシューマ・ノード E の DN です。
- cn=replicationDN: ノード D 上のディレクトリ・レプリケーション・サーバーが、ディレクトリ・サーバーにバインドする場合に使用するバインド識別名。
- cn=replication namecontext: レプリケーションに含まれるネーミング・コンテキストに関する情報のコンテナ。

- cn=namingcontext001 および cn=namingcontext002: レプリケーションに含まれるネーミング・コンテキストを指定するオブジェクト。レプリケーションに含まれるネーミング・コンテキストには、レプリケーションから除外する 1 つ以上のサブツリーまたは特定の属性を指定できます。

レプリケーションのセキュリティ

この項では、次の項目について説明します。

- 認証およびディレクトリ・レプリケーション・サーバー
- Secure Sockets Layer（SSL）と Oracle Internet Directory レプリケーション

認証およびディレクトリ・レプリケーション・サーバー

認証は、Oracle ディレクトリ・レプリケーション・サーバーが、ディレクトリ・サーバーへの接続時に、サーバー自身の正確な識別情報を取得するプロセスです。認証は、LDAP セッションが ldapbind 操作によって確立されたときに発生します。

ディレクトリ・レプリケーション・サーバーが、ディレクトリへのアクセスを許可される前に適切に認証されることが重要です。

ディレクトリ・レプリケーション・サーバーは、一意識別子とパスワードを使用して、ディレクトリ・サーバーに対する認証を行います。ディレクトリ・レプリケーション・サーバーの識別情報は、cn=replication dn,orclreplicaid=*unique_identifier_of_node*,cn=replication configuration の形式をとります。

ディレクトリ・レプリケーション・サーバーは、起動時、Oracle Internet Directory の安全な Wallet から識別情報とパスワードを読み取り、これらの資格証明を使用して認証を行います。レプリケーションのバインド識別名を変更する場合は、レプリケーション環境管理ツールの -pchgpwd オプションを使用する必要があります。

関連項目： A-62 ページの「レプリケーション環境管理ツール」

Secure Sockets Layer（SSL）と Oracle Internet Directory レプリケーション

Oracle Internet Directory レプリケーションは、SSL の使用に関係なく配置できます。

SSL 暗号化を使用するように LDAP ベースのレプリケーションを構成するには、サプライヤ連絡先情報が含まれている orclReplicaURI 属性に、SSL ポートのポート番号を指定します。

SSL 暗号化を使用するように Oracle9*i* Advanced Replication を構成するには、Oracle Advanced Security を使用します。

関連項目： SSL 暗号化を使用するように Oracle9*i* Advanced Replication を構成する方法は、『Oracle Advanced Security 管理者ガイド』を参照してください。

ディレクトリ・レプリケーションの変更ログ

Oracle Internet Directory は、各変更をエントリとして変更ログ・ストアに記録します。コンシューマのディレクトリ・レプリケーション・サーバーは、サプライヤの変更ログ・ストアにある変更内容を取り出し、それをコンシューマに適用します。

変更ログ・ストアの各エントリ（各変更ログ・オブジェクト）には、一意の変更番号が含まれています。コンシューマは、最後に適用した変更の番号を記録しておき、その番号よりも大きい番号を持つ変更のみをサプライヤから取得します。

- LDAP ベースのレプリケーション承諾では、ディレクトリ・レプリケーション・サーバーによって、最後に適用された変更番号がレプリケーション承諾エントリの `orclclastappliedchangenumber` 属性に格納されます。
- Oracle9*i* Advanced Replication ベースのレプリケーション承諾では、ディレクトリ・レプリケーション・サーバーによって、最後に適用された変更番号が `changestatus` エントリの `changenumber` 属性に格納されます。このエントリは、`changenumber=`*`last_applied_change_number`*`, supplier=`*`supplier_node`*`,consumer=`*`consumer_node`* のようになります。たとえば、コンシューマが最後に適用した変更の番号が 250 の場合、それ以降サプライヤから取得する変更の番号は、250 より大きい番号である必要があります。

マルチマスター・レプリケーション

この項では、マルチマスター・レプリケーションの詳細を説明します。マルチマスター・ディレクトリ・レプリケーション・グループには、レプリケートされたデータのグループを管理する機能と同様に機能する複数のノードが存在します。この項では、次の項目について説明します。

- Oracle9i Advanced Replication
- マルチマスター・レプリケーションのアーキテクチャ
- マルチマスター・レプリケーションにおける競合の解消
- マルチマスター・レプリケーション・プロセス

関連項目： レプリケーション承諾の構成方法は、25-35 ページの「レプリケーションの管理」を参照してください。

Oracle9*i* Advanced Replication

Oracle Internet Directory レプリケーションでは、レプリケーション承諾がなされたノード間における更新情報の転送は、Oracle9*i* で使用可能な Oracle9*i* Advanced Replication の蓄積転送機能によって管理されます。アドバンスト・レプリケーションを使用すると、2 つの Oracle データベース間で、データベース表を同期化させることができます。

Oracle9*i* Advanced Replication の機能は、次のとおりです。

- ローカルの変更内容を蓄積し、コンシューマに定期的にまとめて伝播します。コンシューマ・レプリケーション・サーバーは、リモートの変更内容をサーバー固有のローカルのディレクトリ・サーバーに適用し、ローカル・ストアから適用済のリモートの変更内容を削除します。
- Oracle9*i* レプリケーション・グループ内のどこにあるディレクトリ表に対しても読取りおよび更新アクセスできるようにします。一般的なアドバンスト・レプリケーション構成では、行レベル・レプリケーションが使用されます。
- 実証済のネットワーク・トレランスを提供し、データ移送は、Oracle Enterprise Manager Application Server Control で制御および監視できます。このような管理機能によって、データ移送のスケジュール方法に高度な柔軟性を与えることができます。

注意： Oracle Internet Directory と同じデータベース内に常駐する Oracle Application Server Single Sign-On のデータベース・スキーマも、Oracle9*i* Advanced Replication を使用してレプリケートします。

関連項目：

- 『Oracle Application Server Single Sign-On 管理者ガイド』の高可用性に関する章のレプリケーションのための Oracle Application Server Single Sign-On の構成に関する項を参照してください。
- Oracle9*i* Advanced Replication の詳細は、『Oracle9*i* アドバンスト・レプリケーション』を参照してください。

マルチマスター・レプリケーションのアーキテクチャ

一般的なアドバンスト・レプリケーション構成では、サプライヤが変更内容を変更ログに書き込み、バッチ処理された変更を他のコンシューマに定期的に送信する非同期データ伝播を使用します。コンシューマは変更ログ・データを受信し、変更内容をローカルに適用します。

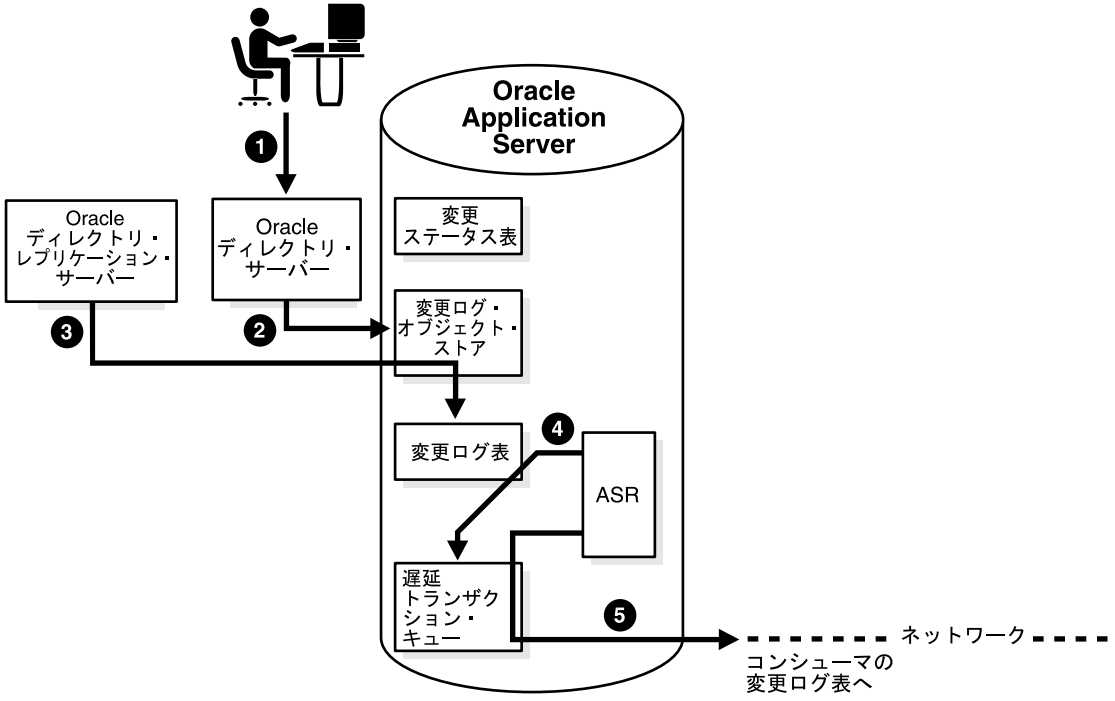
レプリケーションを構成する場合は、レプリケーション・グループ内で変更を共有するノードを指定します。レプリケーションの基本アーキテクチャは、レプリケーション環境に導入するノードの数に関係なく一定です。ローカル変更は、レプリケーション・サーバーがクライアントとして機能し、コンシューマを実行するディレクトリ・サーバーにコマンドを送信する**リモート・マスター・サイト**に配布されます。

次にこのレプリケーション・プロセスを、サプライヤとコンシューマの両方の観点から大まかに説明します。

サプライヤ側のマルチマスター・レプリケーション・プロセス

図 24-10 およびその後に続く説明では、マルチマスター・レプリケーション・プロセス中のサプライヤ側の動作を示します。

図 24-10 サプライヤ側のマルチマスター・レプリケーション・プロセス



1. LDAP クライアントがディレクトリ変更を発行します。
2. Oracle ディレクトリ・サーバーが変更ログ・オブジェクト・ストアに変更ログ・オブジェクトを生成します。
3. スケジュールされた時間に、Oracle ディレクトリ・レプリケーション・サーバーがアウトバウンド変更ログの処理スレッドを起動します。このスレッドは、変更ログ・オブジェクトを変更ログ表の行（変更エントリなど）に変換します。
4. 変更エントリが変更ログ表にコミットされると、Oracle9*i* Advanced Replication はその変更内容を遅延トランザクション・キューへすぐにコピーします。

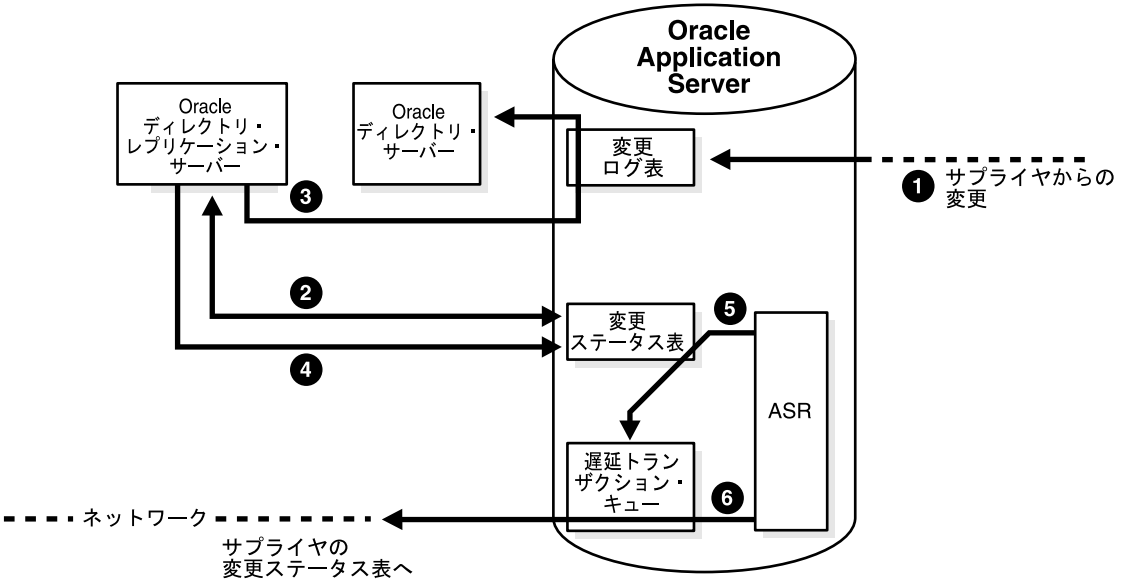
5. スケジュールされた間隔が経過すると、Oracle9*i* Advanced Replication は、遅延トランザクション・キューから保留トランザクションを抽出し、ネットワークを介してコンシューマの変更ログ表に送信します。

注意： シングル・サインオン管理者アプリケーションによって Oracle Application Server Single Sign-On 表に加えられたすべての変更も、Oracle9*i* Advanced Replication によってレプリケートされます。

コンシューマ側のマルチマスター・レプリケーション・プロセス

図 24-11 およびその後に続く説明では、コンシューマ側のマルチマスター・レプリケーション・プロセスを示します。

図 24-11 コンシューマ側のマルチマスター・レプリケーション・プロセス



1. コンシューマの変更ログ表にサプライヤから変更が到着します。
2. Oracle ディレクトリ・レプリケーション・サーバーは、スケジュールされたレプリケーション・サイクルに従って、各サプライヤの変更ログの処理スレッドを起動します。このスレッドは、まずサプライヤからコンシューマに適用された最終変更を変更ステータス表で調べます。

3. Oracle ディレクトリ・レプリケーション・サーバーは、次に変更ログ表から新規変更をすべてフェッチして、Oracle ディレクトリ・サーバーに適用します。
4. Oracle ディレクトリ・レプリケーション・サーバーは、次に変更ステータス表を更新し、サプライヤから適用された最終変更を記録してから終了します。
5. Oracle9*i* Advanced Replication は、変更ステータスの更新内容を遅延トランザクション・キューにコピーします。
6. スケジュールされた Oracle9*i* Advanced Replication の間隔が経過すると、Oracle9*i* Advanced Replication は遅延トランザクション・キューから保留変更ステータス更新を抽出し、サプライヤの変更ステータス表に送信します。

前の 2 つの表ではサプライヤとコンシューマの役割が分割されていますが、実際のマルチマスター・レプリケーション環境においては、各ディレクトリ・サーバーがサプライヤであり、コンシューマでもあります。このような環境では、適用済のエントリや候補の変更に従って削除されたエントリのパージが定期的に発生します。ローカルの変更ログ表にあるリモート変更の記録は、その変更がローカルで適用されると、ガベージ・コレクション・スレッドによってパージされます。ローカルの変更ログ表にあるローカル変更の記録は、その変更がすべてのコンシューマに配布されると、ガベージ・コレクション・スレッドによってパージされます。

関連項目： レプリケーションの構成方法は、25-35 ページの「レプリケーションの管理」を参照してください。

マルチマスター・レプリケーションにおける競合の解消

マルチマスター・レプリケーションを使用すると、複数のディレクトリ・サーバーを更新できます。競合は、ディレクトリ・レプリケーション・サーバーがサプライヤからコンシューマにリモートの変更を適用しようとして失敗した場合、常に発生します。

レプリケーション・プロセスで変更が適用できないことがあります。たとえば、サプライヤのノード A がコンシューマに変更を送信し、その直後にサプライヤのノード B が同じエントリの更新をコンシューマ送信したとします。このとき、なんらかの問題が発生して、サプライヤのノード A からのエントリ送信が遅れたが、サプライヤのノード B からの更新送信にはそのような問題が発生しなかったとします。この結果、サプライヤのノード B からの更新が、エントリの変更よりも先にコンシューマに到着することになります。この場合、レプリケーション・サーバーは、指定された回数まで変更の適用を試みます。指定された回数に達しても変更が適用できなかった場合、レプリケーション・サーバーは変更内容を管理者操作キューに移動し、それ以降は指定した間隔よりも少ない頻度で定期的に適用を試みます。

次の 4 種類の LDAP 操作が競合を引き起こす可能性があります。

- 追加
- 削除
- 変更
- 相対識別名または識別名の変更

レプリケーション競合が発生するレベル

競合には次の 2 つのタイプがあります。

- エントリ・レベルの競合
- 属性レベルの競合

表 24-4 レプリケーション競合のタイプ

レプリケーション競合のレベル	説明
エントリ・レベルの競合	エントリ・レベルの競合は、ディレクトリ・レプリケーション・サーバーが、コンシューマに変更を適用するときに発生します。次のいずれかのタイプの変更がコンシューマで発生する可能性があります。 ■ すでに存在しているエントリの追加 ■ 存在していないエントリの削除 ■ 存在していないエントリの変更 ■ 存在していない識別名に対する識別名の変更操作 これらの競合は、解消するのが難しい場合があります。たとえば、次のような原因の場合は競合を解消するのが不可能な可能性があります。 ■ エントリが別の位置に移動 ■ エントリがサプライヤから未到着 ■ エントリが削除済 ■ エントリがコンシューマに存在しない 存在する必要がないエントリが存在している場合は、以前に追加済であるか、最近識別名の操作変更があった可能性があります。
属性レベルの競合	属性レベルの競合は、2 つのディレクトリが、同じ属性を異なる値で異なる時間に更新している場合に発生します。属性が単一値の場合、レプリケーション・プロセスは、競合に含まれている変更のタイムスタンプを検証して、競合を解消します。

競合の一般的な原因

通常、競合は Wide Area Network 上で発生する場合がある通信速度の低下や送信エラーが原因で発生する変更の時間的なずれが原因です。また、過去に発生した不整合がタイムリに解消されていない場合、引き続き競合が発生する可能性があります。

競合の自動解消

ディレクトリ・レプリケーション・サーバーは、次の処理によって、発生した競合をすべて解消しようとします。

1. 変更が適用されたときに、競合が検出されます。
2. レプリケーション・プロセスは、特定の待機期間が過ぎると、特定回数分または反復による変更の再適用を、特定期間試行します。
3. レプリケーション・プロセスが変更の適用に成功しないまま再試行制限に達した場合、変更に競合のフラグを付けた後、解消を試みます。解消規則（次の項で説明）に従って競合を解消できない場合は、優先順位の低い管理者操作キューにその変更を移動します。変更は、レプリケーション承諾された `orclHIQSchedule` パラメータに指定した時間単位に従って適用されます。ディレクトリ・レプリケーション・サーバーは、変更を移動する前にシステム管理者用のログ・ファイルに競合を書き込みます。

注意： レプリケーション時に、スキーマ、カタログおよびグループ・エントリの競合の解消は行われません。これは、多数の複数値の属性の競合を解消しようとすると、パフォーマンスに重大な影響を及ぼす可能性があるためです。一度に複数のマスターからこのようなエントリの更新を行うことは、回避してください。

関連項目：

- スキーマについて不明点がある場合は、付録 B「Oracle Internet Directory のスキーマ要素」を参照してください。
- カタログについて不明点がある場合は、A-19 ページの「カタログ管理ツール（catalog.sh）構文」を参照してください。
- グループ・エントリについて不明点がある場合は、31-10 ページの「管理者のタスクの実行」を参照してください。

マルチマスター・レプリケーション・プロセス

この項では、自動レプリケーション・プロセスによるエントリの追加、削除、変更、および識別名と相対識別名の変更方法について紹介します。

マルチマスター・レプリケーション・プロセスがコンシューマに新規エントリを追加する動作

ディレクトリ・レプリケーション・サーバーは、コンシューマへの新規エントリの追加に成功すると、次の変更アプリケーション・プロセスを実行します。

1. ディレクトリ・レプリケーション・サーバーは、コンシューマ内でターゲット・エントリの親の識別名を探します。具体的には、その親の識別名に割り当てられている **Global Unique Identifier（GUID）**を探します。
2. 親エントリが存在している場合、ディレクトリ・レプリケーション・サーバーは新規エントリの識別名を作成し、コンシューマ内にあるその親の下に新規エントリを配置します。次に、変更エントリをパージ・キューに入れます。

1 回目の試行で変更エントリが正常に適用されなかった場合

ディレクトリ・レプリケーション・サーバーは新しい変更エントリをリトライ・キューに入れ、再試行回数を指定の最大値に設定して変更アプリケーション・プロセスを繰り返します。

2 回目から最終試行前までの試行で変更エントリが正常に適用されなかった場合

ディレクトリ・レプリケーション・サーバーは変更エントリをリトライ・キューに保持したまま、再試行回数を減らして変更アプリケーション・プロセスを繰り返します。

最終試行で変更エントリが正常に適用されなかった場合

ディレクトリ・レプリケーション・サーバーは、新規エントリが既存エントリと同一でないかどうかをチェックします。

変更エントリが同一エントリの場合

ディレクトリ・レプリケーション・サーバーは、次の競合解消規則を適用します。

* 作成タイムスタンプが古い方のエントリを使用します。
* 両方のエントリの作成タイムスタンプが同じ場合は、GUID の小さい方のエントリを使用します。

変更エントリを使用すると、ターゲット・エントリは削除されて変更が適用され、その変更エントリがパージ・キューに入ります。

ターゲット・エントリを使用すると、変更エントリがパージ・キューに入ります。

変更エントリが同一エントリではない場合

ディレクトリ・レプリケーション・サーバーは、変更エントリを管理者操作キューに入れ、orclHIQSchedule パラメータで指定した間隔で変更アプリケーション・プロセスを繰り返します。

変更エントリが管理者操作キューに入れられた後正常に適用されない場合

ディレクトリ・レプリケーション・サーバーは、このキューに変更を保持したまま、指定した間隔で変更アプリケーション・プロセスを繰り返すと同時に、管理者によるアクションを待ちます。管理者は、OID 調停ツールおよび管理者操作キュー操作ツールを使用して競合を解消できます。

マルチマスター・レプリケーション・プロセスがエントリを削除する動作

ディレクトリ・レプリケーション・サーバーは、コンシューマからエントリを削除すると、次の変更アプリケーション・プロセスを実行します。

1. ディレクトリ・レプリケーション・サーバーは、コンシューマ内で変更エントリの GUID と一致する GUID を持つエントリを探します。
2. 一致するエントリがコンシューマ内にある場合、ディレクトリ・レプリケーション・サーバーはそのエントリを削除します。次に、変更エントリをパージ・キューに入れます。

1 回目の試行で変更エントリが正常に適用されなかった場合

ディレクトリ・レプリケーション・サーバーは変更エントリをリトライ・キューに入れ、再試行回数を指定の最大値に設定して変更アプリケーション・プロセスを繰り返します。

2 回目から最終試行前までの試行で変更エントリが正常に適用されなかった場合

ディレクトリ・レプリケーション・サーバーは変更エントリをリトライ・キューに保持したまま、再試行回数を減らして変更アプリケーション・プロセスを繰り返します。

最終試行で変更エントリが正常に適用されなかった場合

ディレクトリ・レプリケーション・サーバーは、変更エントリを管理者操作キューに入れ、指定した間隔で変更アプリケーション・プロセスを繰り返します。

変更エントリが管理者操作キューに入れられた後正常に適用されない場合

ディレクトリ・レプリケーション・サーバーは、このキューに変更エントリを保持したまま、指定した間隔で変更アプリケーション・プロセスを繰り返すと同時に、管理者によるアクションを待ちます。管理者は、OID 調停ツールおよび管理者操作キュー操作ツールを使用して競合を解消できます。

マルチマスター・レプリケーション・プロセスがエントリを変更する動作

ディレクトリ・レプリケーション・サーバーは、コンシューマのエントリを変更すると、次の変更アプリケーション・プロセスを実行します。

1. ディレクトリ・レプリケーション・サーバーは、コンシューマ内で変更エントリの GUID と一致する GUID を持つエントリを探します。
2. 一致するエントリがコンシューマ内にある場合、ディレクトリ・レプリケーション・サーバーは、変更エントリ内の各属性と、ターゲット・エントリ内の各属性を比較します。
3. その後、ディレクトリ・レプリケーション・サーバーは、次の競合解消規則を適用します。
   a. 変更時間が最新の属性を使用します。
   b. 最新バージョンの属性を使用します（バージョン 1、2 または 3 など）。
   c. ホスト上の変更された属性のうち、アルファベットの A に最も近い名前のエントリを使用します。
4. ディレクトリ・レプリケーション・サーバーは、フィルタ処理済の変更を適用し、変更エントリをパージ・キューに入れます。

1 回目の試行で変更エントリが正常に適用されなかった場合

ディレクトリ・レプリケーション・サーバーは変更エントリをリトライ・キューに入れ、再試行回数を指定の最大値に設定して変更アプリケーション・プロセスを繰り返します。

2 回目から最終試行前までの試行で変更エントリが正常に適用されなかった場合

ディレクトリ・レプリケーション・サーバーは変更エントリをリトライ・キューに保持したまま、再試行回数を減らして変更アプリケーション・プロセスを繰り返します。

最終試行で変更エントリが正常に適用されなかった場合

ディレクトリ・レプリケーション・サーバーは、変更エントリを管理者操作キューに入れ、指定した間隔で変更アプリケーション・プロセスを繰り返します。

変更エントリが管理者操作キューに入れられた後正常に適用されない場合

ディレクトリ・レプリケーション・サーバーは、このキューに変更エントリを保持したまま、指定した間隔で変更アプリケーション・プロセスを繰り返すと同時に、管理者によるアクションを待ちます。管理者は、OID 調停ツールおよび管理者操作キュー操作ツールを使用して競合を解消できます。

マルチマスター・レプリケーション・プロセスが相対識別名を変更する動作

ディレクトリ・レプリケーション・サーバーは、コンシューマのエントリの相対識別名を変更すると、次の変更アプリケーション・プロセスを実行します。

1. ディレクトリ・レプリケーション・サーバーは、コンシューマ内で変更エントリの GUID と一致する GUID を持つ識別名を探します。
2. 一致するエントリがコンシューマ内にある場合、ディレクトリ・レプリケーション・サーバーはそのエントリの相対識別名を変更し、変更エントリをパージ・キューに入れます。

1 回目の試行で変更エントリが正常に適用されなかった場合

ディレクトリ・レプリケーション・サーバーは変更エントリをリトライ・キューに入れ、再試行回数を指定の最大値に設定して変更アプリケーション・プロセスを繰り返します。

2 回目から最終試行前までの試行で変更エントリが正常に適用されなかった場合

ディレクトリ・レプリケーション・サーバーは変更エントリをリトライ・キューに保持したまま、再試行回数を減らして変更アプリケーション・プロセスを繰り返します。

最終試行で変更エントリが正常に適用されなかった場合

ディレクトリ・レプリケーション・サーバーは、変更エントリを管理者操作キューに入れ、変更がそのターゲット・エントリと同一でないかどうかをチェックします。

変更エントリが同一エントリの場合

ディレクトリ・レプリケーション・サーバーは、次の競合解消規則を適用します。

* 作成タイムスタンプが古い方のエントリを使用します。
* 両方のエントリの作成タイムスタンプが同じ場合は、GUID の小さい方のエントリを使用します。

変更エントリを使用すると、ターゲット・エントリは削除されて、変更エントリが適用されパージ・キューに入ります。

ターゲット・エントリを使用すると、変更エントリがパージ・キューに入ります。

変更エントリが同一エントリではない場合

ディレクトリ・レプリケーション・サーバーは、変更エントリを管理者操作キューに入れ、指定した間隔で変更アプリケーション・プロセスを繰り返します。

変更エントリが管理者操作キューに入れられた後正常に適用されない場合

ディレクトリ・レプリケーション・サーバーは、このキューに変更エントリを保持したまま、指定した間隔で変更アプリケーション・プロセスを繰り返すと同時に、管理者によるアクションを待ちます。管理者は、OID 調停ツールおよび管理者操作キュー操作ツールを使用して競合を解消できます。

マルチマスター・レプリケーション・プロセスが識別名を変更する動作

ディレクトリ・レプリケーション・サーバーは、コンシューマのエントリの識別名を変更すると、次の変更アプリケーション・プロセスを実行します。

1. ディレクトリ・レプリケーション・サーバーは、コンシューマ内で変更エントリの GUID と一致する GUID を持つ識別名を探します。

   また、ディレクトリ・レプリケーション・サーバーは、コンシューマ内で変更エントリに指定されている新しい親の GUID と一致する GUID を持つ親の識別名も探します。

2. ターゲット・エントリの識別名と親の識別名の両方がコンシューマ内にある場合、ディレクトリ・レプリケーション・サーバーはそのエントリの識別名を変更し、変更エントリをパージ・キューに入れます。

1 回目の試行で変更エントリが正常に適用されなかった場合

ディレクトリ・レプリケーション・サーバーは変更エントリをリトライ・キューに入れ、再試行回数を指定の最大値に設定して変更アプリケーション・プロセスを繰り返します。

2 回目から最終試行前までの試行で変更エントリが正常に適用されなかった場合

ディレクトリ・レプリケーション・サーバーは変更エントリをリトライ・キューに保持したまま、再試行回数を減らして変更アプリケーション・プロセスを繰り返します。

最終試行で変更エントリが正常に適用されなかった場合

ディレクトリ・レプリケーション・サーバーは、変更エントリを管理者操作キューに入れ、変更がそのターゲット・エントリと同一でないかどうかをチェックします。

変更エントリが同一エントリの場合

ディレクトリ・レプリケーション・サーバーは、次の競合解消規則を適用します。

* 作成タイムスタンプが古い方のエントリを使用します。
* 両方のエントリの作成タイムスタンプが同じ場合は、GUID の小さい方のエントリを使用します。

変更エントリを使用すると、ターゲット・エントリは削除されて、変更エントリが適用されパージ・キューに入ります。

ターゲット・エントリを使用すると、変更エントリがパージ・キューに入ります。

変更エントリが同一エントリではない場合

ディレクトリ・レプリケーション・サーバーは、変更エントリを管理者操作キューに入れ、指定した間隔で変更アプリケーション・プロセスを繰り返します。

変更エントリが管理者操作キューに入れられた後正常に適用されない場合

ディレクトリ・レプリケーション・サーバーは、このキューに変更エントリを保持したまま、指定した間隔で変更アプリケーション・プロセスを繰り返すと同時に、管理者によるアクションを待ちます。管理者は、OID 調停ツールおよび管理者操作キュー操作ツールを使用して競合を解消できます。

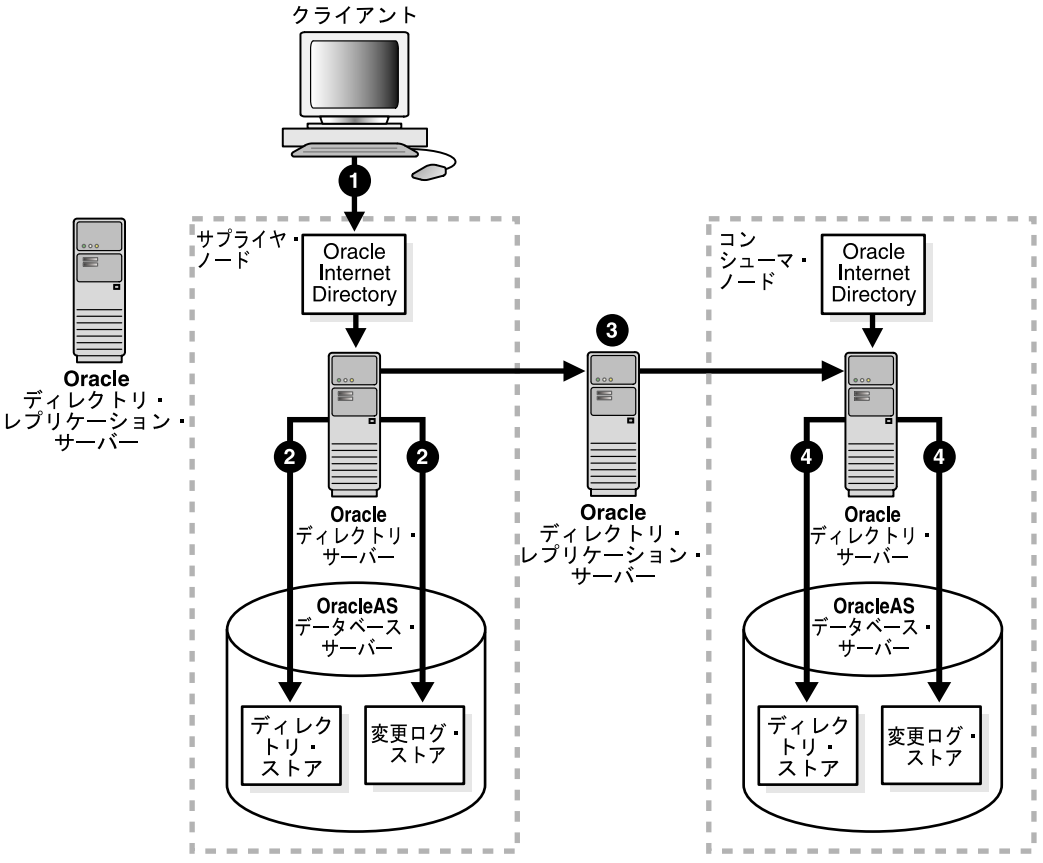
ファンアウトおよび部分レプリケーション

この項では、ファンアウトおよび部分レプリケーションの詳細を説明します。

ファンアウト・レプリケーションでは、コンシューマはサプライヤから直接データをレプリケートします。コンシューマとなるのは、サプライヤまたは 1 つ以上の別のコンシューマです。

図 24-12 およびその後に続く説明では、ファンアウト・レプリケーション・プロセスを示します。

図 24-12 ファンアウト・レプリケーション・プロセス



24-32 ページの図 24-12 に示す内容は、次のとおりです。

1. LDAP クライアントがディレクトリ変更要求をサプライヤ・ノード側のディレクトリに発行します。
2. サプライヤ・ノード側の Oracle ディレクトリ・サーバーは、ディレクトリ・ストアに必要な変更を行うと同時に変更ログ・ストアを更新します。

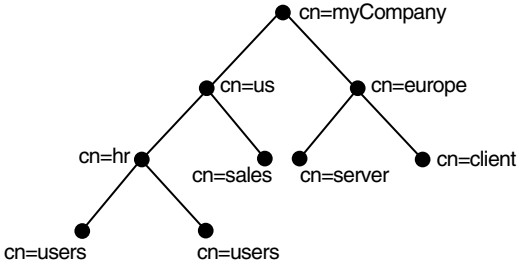
3. コンシューマ・ノード側のディレクトリ・レプリケーション・サーバーは、サプライヤ・ノード側のディレクトリ・サーバーから変更内容を取り出して、コンシューマ側のディレクトリ・サーバーに適用します。
4. コンシューマ側のディレクトリ・サーバーは、次のことを同時に行います。
   - 必要な変更を行い、ディレクトリ・ストア内の変更内容をレプリケートします。
   - 変更ログ・オブジェクト・ストアにシャドウ変更ログ・オブジェクトを生成します。この変更ログ・ストア内のオブジェクトは、他のファンアウト・コンシューマに伝播できます。
   - レプリケーション承諾エントリ内の `orcllastappliedchangenumber` 属性の値を更新し、ディレクトリ・サーバーがサプライヤ・ノードから最後に適用した変更の番号と一致させます。

     関連項目： `orcllastappliedchangenumber` 属性の詳細は、24-19 ページの「ディレクトリ・レプリケーションの変更ログ」を参照してください。

部分レプリケーションのフィルタ処理に関する規則

この項では、部分レプリケーションでネーミング・コンテキストを指定する場合の規則および推奨方法について説明します。図 24-13 に示すネーミング・コンテキストのサンプルに基づいて説明します。

図 24-13 ネーミング・コンテキストのサンプル



この項では、次の項目について説明します。

使用例 1: あるネーミング・コンテキスト・オブジェクトで、レプリケーションに含まれるネーミング・コンテキストが、別のネーミング・コンテキスト・オブジェクトで、レプリケーションに含まれるネーミング・コンテキストのサブツリーになっている

この部分レプリケーションの使用例では、ネーミング・コンテキスト・オブジェクト 2 で、レプリケーションに含まれるネーミング・コンテキスト自体が、ネーミング・コンテキスト・オブジェクト 1 で、レプリケーションに含まれるネーミング・コンテキストのサブツリーになっているとします。

ネーミング・コンテキスト・オブジェクト 1

```
cn=namectx001,
cn=replication namecontext,
orclagreementid=unique_identifier_of_the_replication_agreement,
orclreplicaid=unique_identifier_of_the_supplier,
cn=replication configuration,
    orclincludednamingcontexts: cn=mycompany
```

ネーミング・コンテキスト・オブジェクト 2

```
cn=namectx002,
cn=replication namecontext,
orclagreementid=unique_identifier_of_the_replication_agreement,
orclreplicaid=unique_identifier_of_the_supplier,
cn=replication configuration
    orclincludednamingcontexts: cn=hr,c=us,cn=mycompany
    orclexcludednamingcontexts: cn=users,cn=hr,c=us,cn=mycompany
    orclexcludedattributes: userpassword
```

この使用例では、レプリケートされるネーミング・コンテキストは、orclincludednamingcontexts 属性で最上位に指定されたネーミング・コンテキストです。除外対象ネーミング・コンテキストはレプリケートされません。この例を使用する場合、cn=users,cn=hr,c=us,cn=mycompany を除くサブツリー cn=mycompany の下のすべての変更がレプリケートされます。userpassword 属性は、cn=hr,c=us,cn=mycompany の下にレプリケートされたすべての変更から除外されます。

使用例 2: あるネーミング・コンテキスト・オブジェクトで、レプリケーションに含まれるネーミング・コンテキストが、別のネーミング・コンテキスト・オブジェクトで、レプリケーションから除外されたネーミング・コンテキストのサブツリーになっている

この部分レプリケーションの使用例では、ネーミング・コンテキスト・オブジェクト 4 で、レプリケーションから除外されたネーミング・コンテキストが、ネーミング・コンテキスト・オブジェクト 3 に定義する、レプリケーションから除外されたネーミング・コンテキストのサブツリーになっているとします。

ネーミング・コンテキスト・オブジェクト 3

```
cn=namectx001,cn=replication namecontext,
orclagreementid=identifier,orclreplicaid=supplier,cn=replication configuration
        orclincludednamingcontexts: cn=mycompany
        orclexcludednamingcontexts: cn=us,cn=mycompany
```

ネーミング・コンテキスト・オブジェクト 4

```
cn=namectx002,cn=replication
namecontext,orclagreementid=identifier,orclreplicaid=supplier,cn=replication
configuration
        orclincludednamingcontexts: cn=hr, c=us,cn=mycompany
        orclexcludednamingcontexts: cn=users,cn=hr,c=us,cn=mycompany
        orclexcludedattributes: userpassword
```

この使用例では、ネーミング・コンテキスト・オブジェクト 4 に指定した、レプリケーションに含まれるネーミング・コンテキストはレプリケートされません。このネーミング・コンテキストは、ネーミング・コンテキスト・オブジェクト 3 内に指定されたネーミング・コンテキストのサブツリーです。この場合、ネーミング・コンテキスト・オブジェクト 4 は無視され、cn=hr,c=us,cn=mycompany の下の変更はレプリケートされません。

ネーミング・コンテキストおよび属性の管理規則

予約済ネーミング・コンテキストおよび属性

次に示すネーミング・コンテキストはレプリケートできません。

```
orclagreementid=000001,cn=replication configuration
cn=subconfigsubentry
cn=Oracle Internet Directory
cn=subregistrysubentry
```

次に示すネーミング・コンテキストはレプリケーションから除外できません。

```
cn=catalogs
cn=subschemasubentry
cn=orclshemaversion
cn=replication configuration
```

次に示す属性は、必須またはオプションに関係なく、レプリケーションから除外できません。

```
orclguid
creatorsname
createtimestamp
cn
dn
attributetypes
objectclasses
objectclass
orclindexedattribute
orclproductversion
```

レプリケーションから除外できない他の属性

必須属性は、レプリケーションから除外できません。たとえば、my_object_class というオブジェクト・クラスがあるとします。これには、mandatory_attribute_1、optional_attribute_1 および optional_attribute_2 属性が含まれています。この場合、レプリケーションから mandatory_attribute_1 を除外できません。

レプリケーションからネーミング属性を除外するように設定しても、このネーミング属性は常にレプリケートされます。

パフォーマンスを向上させるための部分レプリケーションの最適化

慎重に計画しなかった場合、部分レプリケーションによってレプリケーション・プロセスのパフォーマンスが低下する可能性があります。たとえば、ネーミング・コンテキスト・オブジェクト 6 のネーミング・コンテキストの定義と比較すると、ネーミング・コンテキスト・オブジェクト 5 のネーミング・コンテキストの定義の方が、パフォーマンスが低下します。

ネーミング・コンテキスト・オブジェクト 5

このネーミング・コンテキスト・オブジェクトの場合、部分レプリケーションに 2 つのネーミング・コンテキスト・オブジェクトが存在します。

```
cn=namectx001,cn=replication
namecontext,orclagreementid=identifier,orclreplicaid=supplier,cn=replication
configuration
orclincludednamingcontexts: cn=mycompany
orclexcludednamingcontexts: c=europe,cn=mycompany
orclexcludedattributes: userpassword
```

ネーミング・コンテキスト・オブジェクト 6

```
cn=namectx002,cn=replication
namecontext,orclagreementid=<id>,orclreplicaid=<supplier>,cn=replication
configuration
orclincludednamingcontexts: cn=hr, c=us,cn=mycompany
orclexcludednamingcontexts: cn=users,cn=hr, c=us,cn=mycompany
orclexcludedattributes: userpassword
```

これら 2 つのネーミング・コンテキスト・オブジェクトを定義すると cn=mycompany の下の cn=europe,c=mycompany および cn=users,cn=hr,c=us,cn=mycompany を除くすべての変更がレプリケートされます。userpassword 属性は、フィルタ処理され除外されます。ただし、ネーミング・コンテキスト・オブジェクト 7 に示すとおり、同じ要件を満たし、部分レプリケーションでの不要なパフォーマンス低下を回避する単一ネーミング・コンテキスト・オブジェクトを作成できます。

ネーミング・コンテキスト・オブジェクト 7

```
cn=namectx001,cn=replication
namecontext,orclagreementid=identifier,orclreplicaid=supplier,cn=replication
configuration
orclincludednamingcontexts: cn=mycompany
orclexcludednamingcontexts: c=europe,cn=mycompany
orclexcludednamingcontexts: cn=users,cn=hr, c=us,cn=mycompany
orclexcludedattributes: userpassword
```

25

Oracle ディレクトリ・レプリケーションの管理

レプリケーションは、複数のノードで、指定したネーミング・コンテキストの完全な複製をメンテナンスする機能です。この章では、Oracle Internet Directory のレプリケーションのインストール、構成および管理方法を説明します。

この章では、次の項目について説明します。

- マルチマスター・レプリケーションのインストールと構成
- LDAP ベースのレプリケーションのインストールと構成
- レプリケーションの管理
- 例 : ファンアウトと組み合せたマルチマスター・レプリケーション・グループのインストールおよび構成

> **関連項目：** レプリケーションの概念の説明は、2-21 ページの「ディレクトリ・レプリケーション」を参照してください。

マルチマスター・レプリケーションのインストールと構成

この項では、マルチマスター・レプリケーション・グループのインストールと構成の方法、およびそのグループでの競合を手動で解決する方法について説明します。この項では、次の項目について説明します。

- マルチマスター・レプリケーション・グループのインストールと構成
- マルチマスター・レプリケーション・グループへのノードの追加
- マルチマスター・レプリケーション・グループからのノードの削除
- 手動でのマルチマスター・レプリケーション・グループ内の競合の解消

マルチマスター・レプリケーション・グループのインストールと構成

この項では、マルチマスター・レプリケーション・グループをインストールおよび構成する際に実行する一般的なタスクを説明します。次の項目について説明します。

マルチマスター・レプリケーション・グループをインストールし構成するための前提情報

タスク 1: マスター定義サイトへの Oracle Internet Directory のインストール

タスク 2: リモート・マスター・サイトへの Oracle Internet Directory のインストール

タスク 3: ディレクトリ・レプリケーション・グループ用の Oracle9i Advanced Replication の設定

タスク 4: ディレクトリへのデータのロード

タスク 5: 全ノードでの Oracle ディレクトリ・サーバー・インスタンスの起動

タスク 6: DRG の全ノードでのレプリケーション・サーバーの起動

タスク 7: ディレクトリ・レプリケーションのテスト

注意：

- この項の説明は、空のノードのグループ内におけるレプリケーションの設定に適用されます。DRG のすべてのノードにディレクトリ・データが存在していないと仮定しています。既存の DRG にノードを追加する方法は、25-13 ページの「マルチマスター・レプリケーション・グループへのノードの追加」を参照してください。
- Oracle Internet Directory10*g*（9.0.4）では、1 つのノードを複数のマルチマスター・レプリケーション・グループの一部にすることはできません。
- ディレクトリ・レプリケーション・サーバーでは、エントリのレプリケーション時に識別名の各相対識別名コンポーネント間の空白が必ずしも保持されるとはかぎりません。まれに、識別名の文字の大 / 小文字区別が保持されない場合があります。
- DSE ルート固有のデータ、サーバー構成データおよびレプリケーション承諾データは、ディレクトリ・レプリケーション・グループのサーバー間でレプリケートされるデータには含まれません。
- Oracle Internet Directory マルチマスター・レプリケーション・グループが構成されると、Oracle Application Server Single Sign-On データベース・スキーマは自動的にレプリケーションで構成されます。

マルチマスター・レプリケーション・グループをインストールし構成するための前提情報

この項では、マルチマスター・レプリケーション・グループの構成を実行するために必要なインストールのタイプを説明します。また、様々な構成タスクを実行できるレプリケーション環境管理ツールについても説明します。

Oracle9*i* Enterprise Edition Oracle Internet Directory 10*g*（9.0.4）では、マルチマスター・レプリケーションの実行に、Oracle9*i* Enterprise Edition の通常のインストールに含まれている **Oracle9i Advanced Replication** が必要になります。Oracle9*i* Standard Edition の通常のインストールには、Oracle9*i* Advanced Replication は含まれていません。

Oracle Application Server Infrastructure 任意のノードに Oracle Internet Directory を Oracle Application Server の一部としてインストールすると、製品を選択するように要求されます。この場合、「Oracle Application Server Infrastructure」を選択します。後のインストール・プロセスで、インストール・タイプの 1 つを選択するように要求されます。どのインストール・タイプを選択するかは、インストール先となるノードが果たす役割が**マスター定義サイト**か**リモート・マスター・サイト**によって決まります。

マスター定義サイトにインストールする場合

1. インストール・タイプとして「認証管理および OracleAS Metadata Repository」を選択します。「次へ」を選択します。「構成オプションの選択」画面が表示されます。
2. すべてのオプションが選択されていることを確認します。
3. 「次へ」を選択します。

リモート・マスター・サイトにインストールする場合

1. インストール・タイプとして「認証管理および OracleAS Metadata Repository」を選択します。「次へ」を選択します。「構成オプションの選択」画面が表示されます。
2. 「構成オプションの選択」画面で、すべての選択を解除します。
3. 「次へ」を選択します。

その後、Oracle Internet Directory のホストおよびポートを指定するように、Oracle Universal Installer から要求されます。MDS のホストおよびポート番号を指定します。サーバーがこのノードで稼働していることを確認します。

インストール後、次のように入力して、Wallet を作成します。

```
$Oracle_Home/bin/Oidpasswd connect=connect_string  create_wallet=TRUE
current_password=password_for_the_ODS_database_user
```

次のように入力して、Oracle Internet Directory プロセスを開始し、停止します。

```
$Oracle_Home/bin/oidmon connect=connect_string start

$Oracle_Home/bin/oidctl connect=connect_string server=oidldapd instance=1 start

$Oracle_Home/bin/oidmon connect=connect_string stop
```

レプリケーション環境管理ツール インストールおよび構成時、様々なタスクの実行にレプリケーション環境管理ツールを使用します。このツールは、次のタスクを支援します。

- レプリケーション・グループの構成
- レプリカの追加および削除
- ディレクトリ・レプリケーション・グループの管理
- レプリケーション・バインド BN パスワードの変更または再設定
- データベース・レプリケーション・ユーザー REPADMIN パスワードの変更
- 変更ログの伝播に関する様々なエラーおよびステータス情報の表示

注意： 部分レプリケーション（LDAP ベースのレプリケーション）の実行に、Oracle9*i* Advanced Replication は不要です。

ディレクトリ・レプリケーション・グループの場合、ノードにある Oracle Internet Directory のバージョンが同じであれば、バージョンの異なる Oracle9*i* データベース・サーバーのパッチ・セットがノードに存在してもかまいません。

ディレクトリ・レプリケーション・グループ内のノードで、異なるバージョンの Oracle Internet Directory が稼働している場合は、これらのノードのディレクトリ・サーバーに変更を加えることができます。ただし、新しいバージョンの Oracle Internet Directory で加えられた変更を、そのバージョンへのアップグレードが行われていないノードにレプリケートすることはできません。レプリケートすると、変更内容に、旧バージョンでは適正に解釈されない情報が含まれてしまいます。

関連項目： レプリケーション環境管理ツールの詳細は、A-62 ページの「レプリケーション環境管理ツール」を参照してください。

タスク 1: マスター定義サイトへの Oracle Internet Directory のインストール

Oracle Net Services を使用して、マスター定義サイトのデータベースおよび DRG 内の他のすべてのノードに接続できる必要があります。

注意： インストール時に、各 Oracle Internet Directory のデータベース・インスタンス名が各マシンで一意であることを確認してください。

関連項目：

- マスター定義サイトにインストールする方法は、25-3 ページの「Oracle Application Server Infrastructure」を参照してください。
- Oracle Internet Directory のインストール・ドキュメントを参照してください。

タスク 2: リモート・マスター・サイトへの Oracle Internet Directory のインストール

関連項目： リモート・マスター・サイトにインストールする方法は、25-3 ページの「Oracle Application Server Infrastructure」を参照してください。

タスク 3: ディレクトリ・レプリケーション・グループ用の Oracle9*i* Advanced Replication の設定

次の各項では、Oracle Internet Directory のインストール・スクリプトを使用して、Oracle9*i* Advanced Replication をインストールおよび構成する方法を説明します。Oracle9*i* Advanced Replication の上級ユーザーは、Oracle9*i* Replication Manager ツールを使用して Oracle9*i* Advanced Replication を構成することもできます。

> **関連項目：** Oracle9*i* Advanced Replication Manager を使用した Oracle9*i* Advanced Replication の構成方法は、『Oracle9*i* アドバンスト・レプリケーション』および Oracle9*i* Advanced Replication Manager のオンライン・ヘルプを参照してください。

ディレクトリ・レプリケーション・グループ（DRG）を設定するために Oracle9*i* Advanced Replication 環境を構成するには、次のタスクを実行します。

- 全ノードでのレプリケーション用の Oracle Net Services 環境の準備
- MDS でのディレクトリ・レプリケーション用の Oracle9i Advanced Replication の構成

全ノードでのレプリケーション用の Oracle Net Services 環境の準備 Oracle Net Services 環境を準備するには、ディレクトリ・レプリケーション・グループのすべてのノードで、次の各手順を実行します。詳細は、その後の説明を参照してください。

1. `sqlnet.ora` を構成します。
2. `tnsnames.ora` を構成します。
3. オプション : ロールバック表領域とロールバック・セグメントを作成します。
4. ロールバック表領域とロールバック・セグメントを作成した場合は、初期化パラメータ・ファイル内のパラメータを変更します。
5. リスナーを停止して、再起動します。
6. ロールバック表領域とロールバック・セグメントを作成した場合は、Oracle Internet Directory データベースを停止して、再起動します。
7. 重要 : DRG の各ノードで、全ノードに対して Oracle Net 接続をテストします。

Oracle Net Services 環境をレプリケーション用に準備する手順は、次のとおりです。

1. `sqlnet.ora` を構成します。

   `sqlnet.ora` ファイルには、少なくとも次のパラメータが記述されている必要があります。

   ```
   names.directory_path = (TNSNAMES)
   names.default_domain = domain
   ```

UNIX では、このファイルは *ORACLE_HOME*/network/admin にあります。

Windows NT では、このファイルは *%ORACLE_HOME%*¥network¥admin にあります。

2. tnsnames.ora を構成します。

DRG の全ノードで、DRG の Oracle Internet Directory データベース・インスタンスすべてを定義します。tnsnames.ora ファイルには、すべての Oracle Internet Directory データベースに対する**接続記述子**情報が、次の書式で記述されている必要があります。

```
connect_string =
    (DESCRIPTION =
      (ADDRESS =
         (PROTOCOL = TCP)
         (HOST = HOST_NAME_OR_IP_ADDRESS)
         (PORT = 1521))
      (CONNECT_DATA =
         (service_name = service_name)))
```

UNIX では、このファイルは *$ORACLE_HOME*/network/admin にあります。

Windows NT では、このファイルは *%ORACLE_HOME%*¥network¥admin にあります。

> **注意：** ネット・サービス名（例：sales.com）はドメイン修飾する必要があります。ただし、そのドメイン・コンポーネントが sqlnet.ora ファイル内の NAMES.DEFAULT_DOMAIN パラメータで指定されているドメイン・コンポーネントと一致していることを確認してください。

3. オプション：ロールバック表領域とロールバック・セグメントを作成します。

複数のロールバック・セグメントを作成することもできます。システム要件に合せて、表領域とセグメントのサイズを増やすことができます。

a. ロールバック・セグメント用の表領域を作成します。

次のコマンドを入力して、SQL*Plus を実行します。

```
sqlplus system/system_password@net_service_name
```

SQL*Plus プロンプトで、次のコマンドを入力します。

```
CREATE TABLESPACE table_space_name
datafile file_name_with_full_path SIZE 50M REUSE AUTOEXTEND ON NEXT 10M
MAXSIZE max_bulk_update transaction_size ex:500M;
```

b. ロールバック・セグメントを作成します。

SQL*Plus プロンプトで、各ロールバック・セグメントごとに次のコマンドを入力します。

```
CREATE ROLLBACK SEGMENT rollback_segment_name
tablespace table_space_name storage (INITIAL 1M NEXT 1M OPTIMAL 2M
MAXEXTENTS UNLIMITED);
```

初期化パラメータ・ファイルに入力されている各ロールバック・セグメントごとに CREATE ROLLBACK SEGMENT コマンドを繰り返します。

4. ロールバック表領域とロールバック・セグメントを作成した場合は、初期化パラメータ・ファイル内のパラメータを変更します。

初期化パラメータ・ファイルに次の行を入力します。

```
rollback_segments = (rollback_segment_name_1, rollback_segment_name_2 ...)
SHARED_POOL_SIZE = 20000000
```

システム・グローバル領域（SGA）の合計が、システムの物理メモリーの 50% を超えないようにしてください。

5. リスナーを停止して、再起動します。

Oracle Internet Directory データベースのリスナーを停止するには、リスナー制御ユーティリティ（lsnrctl）を使用します。LSNRCTL コマンド・プロンプトで、次のコマンドを入力します。

```
SET PASSWORD password
STOP [listener_name]
```

SET PASSWORD は、listener.ora ファイルにパスワードが設定されている場合のみ必要です。デフォルトのパスワードは ORACLE です。デフォルトのリスナー名は LISTENER です。

Oracle Internet Directory データベースのリスナーを再起動するには、LSNRCTL コマンド・プロンプトで次のコマンドを入力します。

```
START [listener_name]
```

6. ロールバック表領域とロールバック・セグメントを作成した場合は、Oracle Internet Directory データベースを停止して、再起動します。

Oracle Internet Directory データベースを停止して再起動するには、SQL*Plus を使用します。

関連項目：

- 『Oracle9*i* Net Services 管理者ガイド』
- データベースの停止と再起動の手順は、『Oracle9*i* データベース管理者ガイド』を参照してください。

7. **重要 :** DRG の各ノードで、全ノードに対して Oracle Net 接続をテストします。

   SQL*Plus を使用します。`internal@net_service_name` と `internal@net_service_name.domain` の両方をテストします。正しく動作しない場合、レプリケーションは動作しません。

MDS でのディレクトリ・レプリケーション用の Oracle9*i* Advanced Replication の構成 この手順は、次のとおりです。

1. システム・ユーザーとして MDS コンソールからすべてのノード（MDS を含む）に接続します。すべてのノードで、次のことを確認してください。
   - Oracle Internet Directory データベースが実行中であること
   - Oracle Internet Directory リスナーが実行中であること
   - 接続文字列が正しいこと
   - システム・パスワードが正しいこと
2. リモート・サイトで、次のことを確認してください。
   - Oracle Internet Directory に指定されたデータベースにパスワードを保存するための Wallet が存在すること。この Wallet は、`oidpwdl` という名前で、ディレクトリ *`ORACLE_HOME`*`/ldap/admin` にあります。
   - レプリケーション管理者のパスワードを保存するための Wallet が存在すること。この Wallet は、`oidpwdr` という名前で、ディレクトリ *`ORACLE_HOME`*`/ldap/admin` にあります。
3. MDS のコマンド・プロンプトで次のスクリプトを実行し、次の「注意」の前提条件を満たしていることを確認します。

   ```
   ORACLE_HOME/ldap/bin/remtool -asrsetup
   ```

   レプリケーション環境管理ツール（remtool）によって Oracle9*i* Advanced Replication が構成されます。

   注意： エラーが発生した場合は、レプリケーション環境管理ツールの `-asrcleanup` オプションを使用して、環境をクリーンアップします。その後、手順 3 を繰り返します。

関連項目：

- レプリケーション環境管理ツール（remtool）の -ASRSETUP オプションの使用方法および例は、A-68 ページの「-ASRSETUP オプション」を参照してください。
- データベースとリスナーが実行中であることを確認する方法は、『Oracle9*i* データベース管理者ガイド』を参照してください。
- 接続文字列が正しいことを確認する方法は、『Oracle9*i* Net Services 管理者ガイド』を参照してください。
- Oracle Wallet の作成方法は、『Oracle Advanced Security 管理者ガイド』の Oracle Wallet Manager についての章を参照してください。

タスク 4: ディレクトリへのデータのロード

DRG に追加するエントリが少数の場合は、DRG の構成が完了するまで待ち、ldapadd を使用してデータをいずれかのノードにロードできます。その後、エントリは指定した時間に他のノードにレプリケートされます。

DRG にロードするデータが大量の場合は、bulkload ユーティリティを使用します。この手順は、次のとおりです。

1. 任意のノードで、次のコマンドを入力します。

   ```
   bulkload.sh -connect connect_string -check -generate file_with_absolute_path_name
   ```

   注意： データを Oracle Internet Directory からロードした場合は、他のオプションに加え、`-restore` オプションを使用して、操作属性をリストアします。

2. 同じノードで、次のコマンドを入力します。

   ```
   bulkload.sh -connect connect_string_1 -load
   ```

3. *connect_string_1* を DRG の別のノードの接続文字列に置換して、データがすべてのノードにロードされるまで手順 2 を繰り返します。たとえば、次のコマンドを入力します。

   ```
   bulkload.sh -connect connect_string_2 -load
   ```

   その後、次のコマンドを入力します。

   ```
   bulkload.sh -connect connect_string_3 -load
   ```

DRG の各ノードへのデータのバルク・ロードが完了するまで、同様に繰り返します。

注意： Windows オペレーティング・システムでシェル・スクリプト・ツールを実行するには、次のいずれかの UNIX エミュレーション・ユーティリティが必要です。

- Cygwin 1.3.2.2-1 以上
  サイト : `http://sources.redhat.com`
- MKS Toolkit 6.1
  サイト : `http://www.datafocus.com/`

関連項目：

- 構文と使用方法は、A-45 ページの「bulkload の構文」を参照してください。

タスク 5: 全ノードでの Oracle ディレクトリ・サーバー・インスタンスの起動

全ノードで Oracle ディレクトリ・サーバー・インスタンスを起動するには、各ノードで次のコマンドを実行します。

```
oidmon [connect=connect_string] [sleep=seconds] start
oidctl connect=connect_string server=oidldapd instance=instance_number_of_directory_
server flags='-h host_name -p port' start
```

ディレクトリ・サーバーの変更ログ記録オプションは、必ずデフォルト（つまり、TRUE）に設定してください。

注意： `instance_number_of_directory_server` は、DRG 全体で一意である必要はありません。たとえば、ノード A とノード B の両方に `instance=1` を指定できます。

関連項目： Oracle ディレクトリ・サーバー・**インスタンス**の起動方法の詳細は、第 3 章「事前に実行するタスクと情報」を参照してください。

タスク 6: DRG の全ノードでのレプリケーション・サーバーの起動

すべてのノードでレプリケーション・サーバーを起動するには、各ノードで次のコマンドを入力します。

```
oidctl connect=connect_string server=oidrepld instance=1
   flags='-h host_on_which_the_directory_server_is_running -p port' start
```

インスタンス番号は、DRG 全体で一意である必要はありません。

> **関連項目：** レプリケーション・サーバーの起動方法は、第 5 章「Oracle ディレクトリ・サーバーの管理」を参照してください。

ディレクトリ・レプリケーション・サーバーで使用されるマルチマスター・フラグをオフにできます。オフにするには、-m フラグの値をデフォルトの TRUE から FALSE に変更して、Oracle ディレクトリ・レプリケーション・サーバーの OID 制御ユーティリティ・コマンドを実行します。このフラグをオフにすると、読取り専用のレプリカ・コンシューマを持つ単一のマスターを配置している場合、パフォーマンス・オーバーヘッドの低減に効果的です。マルチマスター・オプションは、競合の解消を制御しますが、単一のマスターを配置している場合は必要ありません。

> **関連項目：** 24-23 ページの「マルチマスター・レプリケーションにおける競合の解消」

注意： タスク 3 では、レプリケーション環境管理ツール（remtool）によって、レプリケーション・サーバーを簡単に起動できる通常のデフォルトが設定されます。これらのデフォルトを変更する場合は、25-35 ページの「レプリケーションの管理」を参照してください。

タスク 7: ディレクトリ・レプリケーションのテスト

Oracle Directory Manager を使用して、ディレクトリ・レプリケーション・サーバーが実行されていることを確認した後、次の手順を実行してディレクトリ・レプリケーションをテストします。

1. Oracle Directory Manager に orcladmin でログインします。
2. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**、「**エントリ管理**」の順に展開します。
3. MDS ノードに単一のエントリを作成します。

   同一のエントリが、RMS に約 1 ～ 10 分後に表示されます。このタイミングは、レプリケーション・サーバーの構成設定エントリで調整できます。エントリが DRG のいずれかのノードで変更されると、その変更はレプリケートされます。

注意： Oracle Application Server Single Sign-On のレプリケーションを構成するには、Oracle Application Server Single Sign-On 用のインストール後の手順を実行します。これらの手順は、『Oracle Application Server Single Sign-On 管理者ガイド』のレプリケーションのインストールに関する項を参照してください。

マルチマスター・レプリケーション・グループへのノードの追加

注意： 既存のマルチマスター・レプリケーション・グループに追加する新しいノードには、Oracle Application Server Infrastructure 製品がインストールされている必要があります。この製品のインストール時には、「Oracle Application Server Metadata Repository」がインストール・タイプとして選択されている必要があります。詳細は、25-5 ページの「タスク 2: リモート・マスター・サイトへの Oracle Internet Directory のインストール」を参照してください。

稼働中のレプリケーション・グループに新規ノードを追加する方法は、次の 2 通りがあります。

- ldifwrite および bulkload を使用する方法

  たとえば、ディレクトリのエントリが 100 万件以下の場合は、この方法を採用してください。

  この方法では、ldifwrite ユーティリティによって、保存されている操作属性を使用して LDAP データをバックアップする必要があります。この操作を実行した後は、bulkload ユーティリティを使用して、グループ内のすべてのレプリカにデータをロードします。

  bulkload は、`-check`、`-generate` および `-restore` 引数を付けて 1 回使用し、その後、`-load` 引数を付けてレプリカごとに 1 回ずつ使用します。各レプリカで `-load` 引数を使用する際、`-generate` 引数を使用して生成された同じ中間ファイルを使用して、操作属性を保存します。

  100 万件のエントリがあるディレクトリの場合、この方法でのバックアップに約 7 時間かかります。

- コールド・バックアップを使用する方法

  エントリが 100 万件を超えるディレクトリの場合、前述の方法よりも、この方法の方がバックアップにかかる時間が大幅に短くなります。

  関連項目： 付録 F「データベース・コピー・プロシージャを使用したディレクトリ・ノードの追加」

レプリケーション・ノードを追加する前に、25-6 ページの「全ノードでのレプリケーション用の Oracle Net Services 環境の準備」の説明に従って、Oracle Net Services 環境を準備します。

任意の有効サイズで稼働中の DRG にレプリケーション・ノードを追加するには、次の手順に従ってください。各手順の詳細は、この章で後述します。

タスク 1: 全ノードでのディレクトリ・レプリケーション・サーバーの停止

タスク 2: スポンサ・ノードの識別と読取り専用モードへの切替え

タスク 3: ldifwrite を使用したスポンサ・ノードのバックアップ

タスク 4: Oracle9i Advanced Replication 追加ノードの設定の実行

タスク 5: スポンサ・ノードの更新可能モードへの切替え

タスク 6: 新規ノード以外の全ノードでのディレクトリ・レプリケーション・サーバーの起動

タスク 7: bulkload を使用した新規ノードへのデータのロード

タスク 8: 新規ノードでのディレクトリ・サーバーの起動

タスク 9: 新規ノードでのディレクトリ・レプリケーション・サーバーの起動

注意： 以降の各タスクの中で示されているコマンドを実行するには、次のタイプのファイルが、対応するディレクトリに格納されている必要があります。

- バイナリ : `$ORACLE_HOME/bin`
- SQL スクリプト : `$ORACLE_HOME/ldap/admin`
- UNIX スクリプト : `$ORACLE_HOME/ldap/bin`

「タスク 1: マスター定義サイトへの Oracle Internet Directory のインストール」を開始する前に、これら 3 つのタイプのファイルがそれぞれのパスに存在することを確認してください。

タスク 1: 全ノードでのディレクトリ・レプリケーション・サーバーの停止

ディレクトリ・レプリケーション・サーバーを停止するには、LDAP レプリケーション・グループ内の各ノードで次のコマンドを実行します。

```
oidctl connect=db_connect_string server=oidrepld instance=1 stop
```

注意： インスタンス番号が 1 ではない場合があります。実行プロセスをチェックして、そこで使用されているインスタンス番号を検出してください。

タスク 2: スポンサ・ノードの識別と読取り専用モードへの切替え

スポンサ・ノードは、新規ノードにデータを供給するノードです。スポンサ・ノードを識別し、それを読取り専用モードへ切り替える手順は次のとおりです。

1. 次の記述を含んだ新規ファイル change_mode.ldif を作成します。

```
dn:
changetype: modify
replace: orclservermode
orclservermode: r
```

2. 識別されたスポンサ・ノードに対して、次のコマンドを実行します。

```
ldapmodify -D "cn=orcladmin" -w welcome -h host_name_of_sponsor_node
-p port -f change_mode.ldif
```

これにより、実行中の全 Oracle ディレクトリ・サーバーが読取り専用モードに切り替わります。

注意： スポンサ・ノードが読取り専用モードの間は、そのノードを更新できません。他のノードは更新できますが、その更新内容はすぐにはレプリケートされません。

また、スポンサ・ノードと **MDS** が同じノードの可能性もあります。

タスク 3: ldifwrite を使用したスポンサ・ノードのバックアップ

この処理には長時間かかる場合があるため、バックアップ処理中に「タスク 4: Oracle9i Advanced Replication 追加ノードの設定の実行」を開始してもかまいません。

次のコマンドを入力します。

```
ldifwrite -c connect string -b "orclAgreementID=000001,cn=replication configuration"
-f output_ldif_file
```

タスク 4: Oracle9*i* Advanced Replication 追加ノードの設定の実行

このタスクは、「タスク 3: ldifwrite を使用したスポンサ・ノードのバックアップ」の実行中にも実行できます。

スポンサ・ノードで、次のコマンドを入力します。

```
ORACLE_HOME/ldap/bin/remtool -addnode
```

レプリケーション環境管理ツールによって、ノードが DRG に追加されます。

> **注意：** エラーが発生した場合は、まず -asrverify オプションを使用します。このオプションでもエラーが発生した場合には、-asrrectify オプションを使用して、そのエラーを修正します。-asrverify および -asrrectify は、DRG 内のすべてのノードをリストします。新規ノードがリストにない場合は、-addnode オプションを使用してレプリケーション環境管理ツールを再度実行し、新規ノードを追加します。

> **関連項目：** -ADDNODE オプションの使用方法および例は、A-65 ページのレプリケーション環境管理ツールの「-ADDNODE オプション」を参照してください。

タスク 5: スポンサ・ノードの更新可能モードへの切替え

スポンサ・ノードを更新可能モードへ切り替える手順は、次のとおりです。

1. change_mode.ldif を次のように編集します。

   ```
   dn:
   changetype: modify
   replace: orclservermode
   orclservermode: rw
   ```

2. スポンサ・ノードで次のコマンドを実行します。

   ```
   ldapmodify -D "cn=orcladmin" -w welcome -h host_name_of_sponsor_node
   -p  port  -f change_mode.ldif
   ```

これにより、実行中の全 Oracle ディレクトリ・サーバーが読取り / 書込みモードに切り替わります。

注意： タスク 6 は、タスク 3 と類似しています。この手順では change_mode.ldif の orclservermode パラメータが、rw（すなわち読取り / 書込み）に設定される点のみが異なります

タスク 6: 新規ノード以外の全ノードでのディレクトリ・レプリケーション・サーバーの起動

ディレクトリ・レプリケーション・サーバーを起動するには、次のコマンドを入力します。

```
oidctl connect=db_connection_string server=oidrepld instance=1
flags='-h host -p port' start
```

新規ノードでディレクトリまたはレプリケーション処理が何も実行されていないことを検証します。

タスク 7: bulkload を使用した新規ノードへのデータのロード

データをロードするには、次のコマンドを入力します。

```
bulkload.sh -connect db_connect_string_of_new_node -check -generate -load
-restore absolute_path_to_the_ldif_file_generated_by_ldifwrite
```

注意： Windows オペレーティング・システムでシェル・スクリプト・ツールを実行するには、次のいずれかの UNIX エミュレーション・ユーティリティが必要です。

- Cygwin 1.3.2.2-1 以上
  サイト : `http://sources.redhat.com`
- MKS Toolkit 6.1
  サイト : `http://www.datafocus.com/`

タスク 8: 新規ノードでのディレクトリ・サーバーの起動

ディレクトリ・サーバーを起動するには、次のコマンドを入力します。

```
oidctl connect=db_connect_string_of_new_node server=oidldapd
instance=1 flags='-p port' start
```

タスク 9: 新規ノードでのディレクトリ・レプリケーション・サーバーの起動

注意： 構成パラメータまたは承諾パラメータの変更が必要な場合は、25-35 ページの「レプリケーションの管理」を参照してください。

ディレクトリ・レプリケーション・サーバーを起動するには、次のコマンドを入力します。

```
oidctl connect=db_connect_string_of_new_node server=oidrepld instance=1
flags='-h host_name_of_new_node -p port' start
```

注意： ディレクトリ・サーバー・インスタンスがレプリケーション承諾のメンバーとなった後は、データのノードへの追加に bulkload ツールを使用しないでください。かわりに、ldapadd を使用してください。

レプリケーションに Oracle Application Server Single Sign-On が必要な場合は、『Oracle Application Server Single Sign-On 管理者ガイド』のレプリケーションのインストールの項を参照して、Oracle Application Server Single Sign-On 用のインストール後の手順を実行してください。

マルチマスター・レプリケーション・グループからのノードの削除

たとえば、システム・エラーのために新規ノードの追加が完全に成功しなかった場合は、ノードを **DRG** から削除する必要があります。

DRG からレプリケーション・ノードを削除できるのは、DRG に 3 つ以上のノードがある場合のみです。

レプリケーション・ノードを削除するには、次の各タスクを実行してください。各タスクの詳細は、この項で説明します。

タスク 1: 全ノードでのディレクトリ・レプリケーション・サーバーの停止

タスク 2: 削除するノード内の全プロセスの停止

タスク 3: マスター定義サイトからのノードの削除

タスク 4: 全ノードでのディレクトリ・レプリケーション・サーバーの起動

タスク 1: 全ノードでのディレクトリ・レプリケーション・サーバーの停止

ディレクトリ・レプリケーション・サーバーを停止するには、DRG 内の各ノードで次のコマンドを実行します。

```
oidctl connect=connect_string server=oidrepld instance=1 stop
```

注意： インスタンス番号は違う場合があります。

タスク 2: 削除するノード内の全プロセスの停止

削除するノードで、**OID モニター**とすべてのディレクトリ・サーバー・インスタンスを停止します。

```
oidmon [connect=connect_string] [host=virtual/host_name] stop
oidctl connect=connect_string server=oidldapd instance=server_instance_number stop
```

関連項目：

- OID モニターの停止方法は、A-5 ページの「OID モニターの停止」を参照してください。
- OID 制御ユーティリティを使用してディレクトリ・サーバー・インスタンスを停止する方法は、A-9 ページの「Oracle ディレクトリ・サーバー・インスタンスの停止」を参照してください。

タスク 3: マスター定義サイトからのノードの削除

MDS から、次のスクリプトを実行します。

```
remtool -delnode
```

レプリケーション環境管理ツールによって、レプリケーション・グループからノードが削除されます。

関連項目： -DELNODE オプションの使用方法および例は、A-72 ページのレプリケーション環境管理ツールの「-DELNODE オプション」を参照してください。

この処理は、システム・リソースと DRG のサイズによって、長時間かかる場合があります。処理の経過は、継続的に通知されます。

注意： エラーが発生した場合は、まず `-asrverify` オプションを使用します。このオプションでもエラーが発生した場合には、`-asrrectify` オプションを使用して、そのエラーを修正します。`-asrverify` および `-asrrectify` は、DRG 内のすべてのノードをリストします。削除するノードがリストにない場合は、`-delnode` オプションを使用してレプリケーション環境管理ツールを再度実行し、削除するノードを追加します。

タスク 4: 全ノードでのディレクトリ・レプリケーション・サーバーの起動

ディレクトリ・レプリケーション・サーバーを起動するには、次のコマンドを入力します。

```
oidctl connect=connect_string server=oidrepld instance=1
flags='-h host -p port' start
```

関連項目： A-10 ページの「Oracle ディレクトリ・レプリケーション・サーバー・インスタンスの起動」

手動でのマルチマスター・レプリケーション・グループ内の競合の解消

この項では、次の項目について説明します。

レプリケーション変更の競合の監視

競合がログに書き込まれた場合、それは、システムに備わった解消手順では競合を解消できないということを意味します。以前に適用されなかった変更によって新しいレプリケーション変更の競合が発生することを防止するために、ログを定期的に監視することが重要です。

レプリケーション変更の競合を監視するには、レプリケーション・ログの内容を検証します。それぞれに付加されているタイムスタンプによって、各メッセージを識別できます。

競合解消メッセージの例

競合解消メッセージは、ファイル `oidrepld00.log` に記録されます。この項ではメッセージの例を示します。このファイルのパスは、*ORACLE_HOME*`/ldap/log` です。レプリケーション競合の解消を試みた結果は、各競合解消メッセージの最後に記述されています。

例 1: 存在しないエントリを変更しようとした場合

```
2000/08/03::10:59:05:  ************ Conflict Resolution Message ************
2000/08/03::10:59:05:  Conflict reason: Attempted to modify a non-existent entry.
2000/08/03::10:59:05:  Change number:1306.
2000/08/03::10:59:05:  Supplier:eastlab-sun.
2000/08/03::10:59:05:  Change type:Modify.
2000/08/03::10:59:05:  Target DN:cn=ccc,ou=Recruiting,ou=HR,ou=Americas,o=IMC,c=US.
2000/08/03::10:59:05:  Result: Change moved to low priority queue after failing on
10th retry.
```

例 2: 既存のエントリを追加しようとした場合

```
2000/08/03::10:59:05:  ************ Conflict Resolution Message ************
2000/08/03::10:59:05:  Conflict reason: Attempted to add an existing entry.
2000/08/03::10:59:05:  Change number:1209.
2000/08/03::10:59:05:  Supplier:eastlab-sun.
2000/08/03::10:59:05:  Change type:Add.
2000/08/03::10:59:05:  Target DN:cn=Lou Smith, ou=Recruiting, ou=HR, ou=Americas,
o=IMC, c=US.
2000/08/03::10:59:05:  Result: Deleted duplicated target entry which was created
later than the change entry. Apply the change entry again.
```

例 3: 存在しないエントリを削除しようとした場合

```
2000/08/03::10:59:06:  ************ Conflict Resolution Message ************
2000/08/03::10:59:06:  Conflict reason: Attempted to delete a non-existent entry.
2000/08/03::10:59:06:  Change number:1365.
2000/08/03::10:59:06:  Supplier:eastlab-sun.
2000/08/03::10:59:06:  Change type:Delete.
2000/08/03::10:59:06:  Target DN:cn=Lou
Smith,ou=recruiting,ou=hr,ou=americas,o=imc,c=us.
2000/08/03::10:59:06:  Result: Change moved to low priority queue after failing on
10th retry.
```

管理者操作キュー操作ツールの概要

管理者操作キュー操作ツールを使用すると、変更を管理者操作キューからリトライ・キューまたはパージ・キューへ移動できます。パージ・キューへの変更の移動は、ログ・エントリに対する変更の再適用を以降は試みないということを意味します。管理者操作キューの変更を処理するには、次の一般的な手順を実行してください。

1. ディレクトリ・レプリケーション・サーバーを停止します。
2. レプリケーション・ログを分析します。
3. 管理者操作キュー操作ツールを使用して、変更をリトライ・キューまたはパージ・キューへ移動します。詳細は、次項を参照してください。

> **関連項目：** 管理者操作キュー操作ツールの使用方法は、A-56 ページの「管理者操作キュー操作ツール」を参照してください。

OID 調停ツールの概要

ディレクトリ・レプリケーション・サーバーが一貫性のないデータを検出した場合、OID 調停ツールを使用して、コンシューマのエントリをサプライヤのエントリと同期化させることができます。その場合、次の一般的な手順を実行します。

1. サプライヤとコンシューマを、読取り専用モードに設定します。
2. サプライヤとコンシューマが安定した状態、つまり変更の供給も適用も行っていない状態にあることを確認します。安定した状態にない場合は、更新が完了するまで待ちます。
3. コンシューマ上の一貫性のないエントリまたはサブツリーを識別します。
4. OID 調停ツールを使用して、コンシューマ上の一貫性のないエントリまたはサブツリーを修正します。
5. サプライヤとコンシューマを、読取り / 書込みモードに戻します。

関連項目：

- ノードを読取り専用モードに設定する方法は、「タスク 2: スポンサ・ノードの識別と読取り専用モードへの切替え」を参照してください。
- OID 調停ツールの構文と動作の説明は、A-59 ページの「OID 調停ツール」を参照してください。

LDAP ベースのレプリケーションのインストールと構成

この項では、次の項目について説明します。

- LDAP ベースのレプリケーションの構成に関する規則
- LDAP ベースのレプリカのインストール
- LDAP ベースのレプリカの構成
- LDAP ベースのレプリカの削除
- LDAP ベースの部分レプリケーションでのレプリケート対象の決定

LDAP ベースのレプリケーションの構成に関する規則

次の規則は、完全および部分 LDAP ベース・レプリケーションの両方に適用されます。

- LDAP ベースのレプリカには、2 つのサプライヤは存在できない。
- LDAP ベースのレプリケーションでは、ルート DSE の `namingcontexts` 属性にリストされているネーミング・コンテキストのみ、コンシューマにレプリケートできる。
- LDAP ベースのレプリカのサプライヤは、スタンドアロン・ノードか、マルチマスター・レプリケーション・グループのメンバーのいずれかである。
- LDAP ベースのレプリカは、別の LDAP ベースのレプリカのコンシューマの場合もある。その場合、ファンアウト・レプリカと呼ばれる。

関連項目： スタンドアロン・ノードにインストールする方法は、25-4 ページの「マスター定義サイトにインストールする場合」を参照してください。

LDAP ベースのレプリカのインストール

任意のノードに Oracle Internet Directory をインストールする手順は、次のとおりです。

1. 製品を選択するように要求されたら、**Oracle Application Server Infrastructure** を選択します。
2. インストール・タイプに「**認証管理および OracleAS Metadata Repository**」を選択します。「**次へ**」を選択します。「構成オプションの選択」画面が表示されます。

3. 「構成オプションの選択」画面で、すべての選択を解除します。
4. 「**次へ**」を選択します。

その後、Oracle Internet Directory のホストおよびポートを指定するように、Oracle Universal Installer から要求されます。サプライヤのホストおよびポート番号を指定します。サーバーがこのノードで稼働していることを確認します。

インストール後、次のように入力して、Wallet を作成します。

```
$ORACLE_HOME/bin/Oidpasswd connect=connect_string  create_wallet=TRUE
current_password=password_for_the_ODS_database_user
```

次のように入力して、Oracle Internet Directory プロセスを開始し、停止します。

```
$ORACLE_HOME/bin/oidmon connect=connect_string start

$ORACLE_HOME/bin/oidctl connect=connect_string server=oidldapd instance=1 start

$ORACLE_HOME/bin/oidmon connect=connect_string stop
```

OPMNCTL ユーティリティを使用して、Oracle Internet Directory インスタンスを起動することもできます。この手順は、次のとおりです。

1. oidpasswd を実行して、Wallet を作成します。
2. opmn が実行中であることを確認します。次のように入力します。

   ```
   opmnctl ping
   ```

3. opmn が実行されていない場合は、起動します。この手順は、次のとおりです。
   a. 次のように入力します。

      ```
      opmnctl start
      ```

   b. 手順 2 を繰り返します。
4. $*ORACLE_HOME*/opmn/conf/opmn.xml の ias-component=OID のステータスを、disabled から enabled に変更します。
5. opmn.xml ファイルを再ロードします。

   ```
   opmnctl reload
   ```

6. Oracle Internet Directory を起動します。

   ```
   opmnctl startproc ias-component=OID
   ```

LDAP ベースのレプリカの構成

LDAP ベースのレプリカの構成方法は、ディレクトリのバックアップに、ldifwrite ツールを使用したか、または自動ブートストラップを使用したかによって異なります。表 25-1 に、これらの 2 つの方法の比較を示します。

表 25-1 バックアップおよび自動ブートストラップの比較

ldifwrite を使用したバックアップ	自動ブートストラップ
手動プロシージャ	自動プロシージャ
高速パフォーマンス	部分レプリケーションのフィルタ機能を使用
大量のデータに最適	エントリ数が少ない場合に最適

自動ブートストラップを使用した LDAP ベースのレプリカの構成

この項では、自動ブートストラップを使用して、LDAP ベースのレプリカを構成する場合に実行する一般的なタスクを説明します。この項では、次の項目について説明します。

- タスク 1: サプライヤ・ノードの特定
- タスク 2: レプリケーション環境管理ツールを使用した LDAP ベースのレプリカの追加
- タスク 3: 自動ブートストラップを行うためのレプリカの構成
- タスク 4: オプション : デフォルトのレプリケーション・パラメータの変更
- タスク 5: コンシューマ・レプリカでディレクトリ・レプリケーション・サーバーを起動

タスク 1: サプライヤ・ノードの特定 LDAP ベースのレプリカのサプライヤを特定します。次のいずれかがサプライヤとなります。

- スタンドアロン・ディレクトリ
- マルチマスター・レプリケーション・グループのノード
- 別の LDAP ベースのレプリカ

タスク 2: レプリケーション環境管理ツールを使用した LDAP ベースのレプリカの追加 レプリカを追加するには、次のように入力します。

```
remtool -paddnode [-v] [-bind supplier_host_name:port/replication_dn_password]
```

> **関連項目：** レプリケーション環境管理ツールの詳細は、A-62 ページの「レプリケーション環境管理ツール」を参照してください。

タスク 3: 自動ブートストラップを行うためのレプリカの構成 自動ブートストラップ機能を使用するには、次のように、レプリカ・サブエントリの orclReplicaState 属性を 0 に設定します。

1. サンプル・ファイル mod.ldif を、次のように編集します。

```
Dn: orclreplicaid=<unique replica identifier>, cn=replication configuration
Changetype:modify
add:orclReplicaState
OrclReplicaState: 0
```

2. ldapmodify を使用して、レプリカのサブエントリの orclreplicastate 属性を更新します。

```
Ldapmodify -D "cn=orcladmin" -w administrator_password -h my_host -p 389 -f
mod.ldif
```

関連項目： LDAP ベースのレプリケーションのブートストラップ機能の詳細は、25-35 ページの「レプリケーションの管理」を参照してください。

タスク 4: オプション : デフォルトのレプリケーション・パラメータの変更 レプリケーション承諾およびレプリカ・サブエントリのデフォルトのパラメータを変更できます。

関連項目：

- 25-35 ページの「ディレクトリ・レプリケーション・サーバーの構成パラメータの表示および変更」
- 25-38 ページの「特定のレプリカ・ノードについてのパラメータの表示および変更」
- 25-40 ページの「レプリケーション承諾のパラメータの変更」
- 24-13 ページの「ディレクトリ内のレプリケーション構成オブジェクト」
- 25-30 ページの「LDAP ベースの部分レプリケーションでのレプリケート対象の決定」

タスク 5: コンシューマ・レプリカでディレクトリ・レプリケーション・サーバーを起動

関連項目： A-10 ページの「Oracle ディレクトリ・レプリケーション・サーバー・インスタンスの起動」

ldifwrite ツールを使用した LDAP ベースのレプリカの構成

この項では、ldifwrite ツールを使用して、LDAP ベースのレプリカを構成する場合に実行する一般的なタスクを説明します。この項では、次の項目について説明します。

- タスク 1: サプライヤ・ノードとコンシューマ・ノードの両方でディレクトリ・サーバーを起動
- タスク 2: サプライヤ側のディレクトリ・サーバーの読取り専用モードへの切替え
- タスク 5: レプリケートするネーミング・コンテキストのバックアップ
- タスク 3: レプリケーション環境管理ツールを使用した LDAP ベースのレプリカの追加
- タスク 4: lastappliedchangenumber 属性の初期化
- タスク 6: サプライヤ側のディレクトリ・サーバーの読取り / 書込みモードへの切替え
- タスク 7: LDAP ベースのレプリカについてのデータのロード
- タスク 8: オプション : デフォルトのレプリケーション・パラメータの変更
- タスク 9: コンシューマ・レプリカでディレクトリ・レプリケーション・サーバーを起動

タスク 1: サプライヤ・ノードとコンシューマ・ノードの両方でディレクトリ・サーバーを起動 LDAP ベースのレプリカのサプライヤを特定し、ディレクトリ・サーバーがサプライヤとコンシューマの両方で稼働していることを確認します。次のいずれかがサプライヤとなります。

- スタンドアロン・ディレクトリ
- マルチマスター・レプリケーション・グループのノード
- 別の LDAP ベースのレプリカ

タスク 2: サプライヤ側のディレクトリ・サーバーの読取り専用モードへの切替え データ整合性を保証するために、サプライヤ・ノードのディレクトリ・サーバーを読取り専用モードに切り替えます。この手順は、次のとおりです。

1. LDIF ファイルを作成します。このファイルの内容は次のとおりです。

```
Dn:
Changetype: modify
Replace: orclservermode
Orclservermode: r
```

2. サプライヤ側で、次のコマンドを実行します。

```
ldapmodify -D "cn=orcladmin" -w administrator_password -h host_name_of_supplier_
node -p port -f name_of_LDIF_file.ldif
```

タスク 3: レプリケーション環境管理ツールを使用した LDAP ベースのレプリカの追加 レプリカを追加するには、次のように入力します。

```
remtool -paddnode [-v] [-bind supplier_host_name:port/replication_dn_password]
```

> **関連項目：** レプリケーション環境管理ツールの詳細は、A-62 ページの「レプリケーション環境管理ツール」を参照してください。

タスク 4: lastappliedchangenumber 属性の初期化 この手順は、次のとおりです。

1. サプライヤ・ノードで最後に適用された変更番号を検索します。

   ```
   ldapsearch -D bind_DN -w password -h host_name -p port_number -b "" -s base
   "objectclass=*" lastchangenumber
   ```

2. サプライヤ側で、検索の結果見つかった最後に適用された変更番号を使用して、対応する承諾を変更します。この手順は、次のとおりです。

   a. サプライヤ側で、検索の結果見つかった最後に適用された変更番号を使用して、LDIF ファイルを作成します。

      ```
      dn:orclagreementid=agreement_identifier,orclreplicaid=supplier_replica_
      identifier,cn=replication configuration
      changetype: modify
      replace: orclLastAppliedChangeNumber
      orclLastAppliedChangeNumber: last_change_number_retrieved_in_step_1.
      ```

   b. ldapmodify を使用して、承諾を変更します。

      ```
      ldapmodify -D bind_DN -w password -h host_name -p port_number -f LDIF_file
      ```

タスク 5: レプリケートするネーミング・コンテキストのバックアップ LDAP ベースのレプリカにレプリケートするエントリが、ネーミング・コンテキスト内に大量にある場合は、サプライヤ・ノードでこれらのネーミング・コンテキストをバックアップし、それを LDAP ベースのレプリカにロードすることをお薦めします。

ネーミング・コンテキストをバックアップする手順は、次のとおりです。

1. 25-27 ページの「タスク 3: レプリケーション環境管理ツールを使用した LDAP ベースのレプリカの追加」で作成したレプリケーション承諾識別名を指定します。

   ```
   ldapsearch -h supplier host -p port number -b "orclreplicaid=supplier replica
   ID, cn=replication configuration" -s sub "(orclreplicadn= orclreplicaid=consumer
   replica ID, cn=replication configuration)" dn
   ```

2. 次のコマンドを使用して、サプライヤからデータを取得します。ファイルにロードされたデータは、構成済の承諾に基づきます。

   ```
   ldifwrite -c connect string of sponsor node -b "replication agreement dn"
   -f name of output LDIF file.ldif
   ```

注意： 承諾で行った追加の変更がバックアップ時に反映されるには、25-29 ページの「タスク 8: オプション : デフォルトのレプリケーション・パラメータの変更」を実行してから、データをバックアップします。

関連項目：

25-30 ページの「LDAP ベースの部分レプリケーションでのレプリケート対象の決定」

ldifwrite を使用してネーミング・コンテキストの一部をバックアップする方法の詳細は、A-55 ページの「例 2: 指定したネーミング・コンテキストの一部のエントリを LDIF ファイルに変換する場合」を参照してください。

タスク 6: サプライヤ側のディレクトリ・サーバーの読取り / 書込みモードへの切替え 25-26 ページの「タスク 2: サプライヤ側のディレクトリ・サーバーの読取り専用モードへの切替え」を実行した場合は、サプライヤ側のディレクトリ・サーバーを読取り / 書込みモードに戻します。この手順は、次のとおりです。

1. LDIF ファイルを作成します。このファイルの内容は次のとおりです。

```
Dn:
Changetype: modify
Replace: orclservermode
Orclservermode: rw
```

2. サプライヤ側で、次のコマンドを実行します。

```
ldapmodify -D "cn=orcladmin" -w administrator_password -h host_name_of_supplier_
node -p port -f name_of_LDIF_file.ldif
```

タスク 7: LDAP ベースのレプリカについてのデータのロード この手順は、次のとおりです。

1. 複数のファイルがある場合は、たとえば、backup_data.ldif などの 1 つのファイルにまとめます。
2. LDAP ベースのコンシューマ・レプリカにネーミング・コンテキストがある場合は、bulkdelete を使用して削除します。次のように入力します。

```
Bulkdelete.sh -connect connect_string_of_replica  -b "naming_context"
```

25-27 ページの「タスク 5: レプリケートするネーミング・コンテキストのバックアップ」でバックアップした各ネーミング・コンテキストについて、この手順を実行します。

bulkload を使用して、追加モードでデータをレプリカにロードします。次のように入力します。

```
Bulkload.sh -connect connect_string_of_replica -append -check -generate -load
-restore backup_data.ldif
```

関連項目： デフォルトのモードまたは追加モードで bulkload を使用する方法は、A-45 ページの「bulkload の構文」を参照してください。

タスク 8: オプション : デフォルトのレプリケーション・パラメータの変更 レプリケーション承諾およびレプリカ・サブエントリのデフォルトのパラメータを変更できます。

関連項目：

- 25-35 ページの「ディレクトリ・レプリケーション・サーバーの構成パラメータの表示および変更」
- 25-38 ページの「特定のレプリカ・ノードについてのパラメータの表示および変更」
- 25-40 ページの「レプリケーション承諾のパラメータの変更」
- 24-13 ページの「ディレクトリ内のレプリケーション構成オブジェクト」
- 25-30 ページの「LDAP ベースの部分レプリケーションでのレプリケート対象の決定」

タスク 9: コンシューマ・レプリカでディレクトリ・レプリケーション・サーバーを起動

関連項目： A-10 ページの「Oracle ディレクトリ・レプリケーション・サーバー・インスタンスの起動」

LDAP ベースのレプリカの削除

この項では、LDAP ベースのレプリカの削除方法を説明します。この項では、次の項目について説明します。

- タスク 1: 削除するノードでのディレクトリ・レプリケーション・サーバーの停止
- タスク 2: 削除するノードでのディレクトリ・サーバーの停止
- タスク 3: レプリケーション・グループからのレプリカの削除

注意： 別のレプリカのサプライヤになっているレプリカは、削除できません。このようなレプリカを削除するには、先にそのすべてのコンシューマをレプリケーション・グループから削除する必要があります。

タスク 1: 削除するノードでのディレクトリ・レプリケーション・サーバーの停止

関連項目： A-11 ページの「Oracle ディレクトリ・レプリケーション・サーバー・インスタンスの停止」

タスク 2: 削除するノードでのディレクトリ・サーバーの停止

関連項目： A-9 ページの「Oracle ディレクトリ・サーバー・インスタンスの停止」

タスク 3: レプリケーション・グループからのレプリカの削除

このタスクは、レプリケーション環境管理ツールを使用して行います。次のように入力します。

```
remtool -pdelnode [-v] [-bind hostname:port_number/replication_dn_password]
```

LDAP ベースの部分レプリケーションでのレプリケート対象の決定

関連項目： A-62 ページの「レプリケーション環境管理ツール」

LDAP ベースの部分レプリケーションでは、レプリカのネーミング・コンテキスト・オブジェクトを定義することにより、レプリケートするものとしないものを決めることができます。これらのオブジェクトのパラメータは、次の識別名を持つエントリに格納されます。

```
cn=namingcontext_ID,cn=replication namecontext,
orclAgreementID=numeric_identifier_of_replication_agreement,
orclReplicaId=unique_identifier_of_replica, cn=replication configuration
```

注意： ディレクトリ・レプリケーション・サーバーは、レプリカのネーミング・コンテキスト・オブジェクトを、サプライヤ側にある承諾から読み込むため、すべての変更をサプライヤ側およびコンシューマ側（オプション）のネーミング・コンテキスト・オブジェクトに適用する必要があります。

Oracle Directory Manager を使用したレプリカのネーミング・コンテキスト・オブジェクトの表示と変更

レプリカのネーミング・コンテキスト・オブジェクトのパラメータを表示および変更する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**、「**レプリケーション管理**」、「**レプリカ・ノード : レプリカ識別子**」、「**レプリカ承諾 : レプリケーション承諾識別子**」の順に展開します。
2. 変更するレプリカのネーミング・コンテキストを選択します。「**レプリカのネーミング・コンテキスト**」タブ・ページが右側のペインに表示されます。このタブ・ページのフィールドの説明は、C-15 ページの表 C-18 を参照してください。
3. 適切な情報を入力した後、「**OK**」を選択します。

Oracle Directory Manager を使用したレプリカのネーミング・コンテキスト・オブジェクトの追加

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**、「**レプリケーション管理**」、「**レプリカ・ノード : レプリカ識別子**」、「**レプリカ承諾 : レプリケーション承諾識別子**」の順に展開します。
2. 「**ネーミング・コンテキスト : ネーミング・コンテキストの識別子**」を選択します。
3. ツールバーの「**作成**」ボタンを選択します。「新しいレプリカ承諾のネーミング・コンテキスト」ダイアログ・ボックスが表示されます。
4. 「新しいレプリカ承諾のネーミング・コンテキスト」ダイアログ・ボックスのフィールドに、適切な情報を入力します。このダイアログ・ボックスのフィールドの説明は、C-15 ページの表 C-18 を参照してください。
5. 「**OK**」を選択します。

Oracle Directory Manager を使用したレプリカのネーミング・コンテキスト・オブジェクトの削除

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**、「**レプリケーション管理**」、「**レプリカ・ノード : レプリカ識別子**」、「**レプリカ承諾 : レプリケーション承諾識別子**」の順に展開します。
2. 「**ネーミング・コンテキスト : ネーミング・コンテキストの識別子**」を右クリックします。
3. 「**削除**」を選択します。

ldapmodify を使用したレプリカのネーミング・コンテキスト・オブジェクト・パラメータの変更

レプリカのネーミング・コンテキスト・オブジェクト・パラメータの説明は、B-39 ページの表 B-33 を参照してください。

例 1: LDAP ベースのレプリカのネーミング・コンテキスト・オブジェクトの追加

この例では、次の処理を行うネーミング・コンテキスト・オブジェクトを作成します。

- ou=Americas,cn=mycompany ネーミング・コンテキストをレプリケート
- レプリケーションから cn=customer profile, ou=Americas, cn=mycompany ネーミング・コンテキストを除外
- レプリケーションから userpassword 属性を除外

手順は、次のとおりです。

1. サンプル・ファイル mod.ldif を、次のように編集します。

```
dn: cn=naming_context_identifier,cn=replication
namecontext,orclagreementid=replication_agreement_
identifier,orclreplicaid=consumer_replica_identifier,cn=replication
configuration
orclincludednamingcontexts: ou=Americas,cn=mycompany
orclexcludednamingcontexts: cn=customer profile, ou=Americas, cn=mycompany
orclexcludedattributes: userpassword
objectclass: top
objectclass: orclreplnamectxconfig
```

2. ldapadd を使用して、部分レプリケーションのネーミング・コンテキスト・オブジェクトをサプライヤとコンシューマの両方に追加します。

```
ldapadd -D "bind_DN" -w administrator_password -h host -p port_number -f
mod.ldif
```

例 2: LDAP ベースのレプリカのネーミング・コンテキスト・オブジェクトの削除

この例では、サプライヤとコンシューマから前述の例で作成したネーミング・コンテキスト・オブジェクトを削除します。

コマンドは次のとおりです。

```
ldapdelete -D "bind_DN" -w administrator_password
-h [supplier host | consumer host]
-p port_number
"cn=naming_context_identifier,
cn=replication namecontext,orclagreementid=replication_agreement_
identifier,orclreplicaid=consumer_replica_identifier,cn=replication configuration"
```

例 3: レプリカのネーミング・コンテキスト・オブジェクトの orclIncludedNamingcontexts 属性の変更

ディレクトリ・レプリケーション・サーバーは、レプリカのネーミング・コンテキスト・オブジェクトの orclIncludedNamingcontexts 属性の値を使用して、部分レプリケーションに含める最上位サブツリーを指定します。

この例では、含める対象ネーミング・コンテキストが c=us に設定されます。これは、cn=us が部分レプリケーションに含められることを意味しています。

1. サンプル・ファイル mod.ldif を、次のように編集します。

```
cn=naming_context_identifier,
cn=replication namecontext,
orclagreementid=replication_agreement_identifier,
orclreplicaid=consumer_replica_identifier,
cn=replication configuration
Changetype:modify
Replace: orclIncludedNamingcontexts
orclIncludedNamingcontexts: c=us
```

2. ldapmodify を使用して、レプリケーション承諾の orclupdateschedule 属性を更新します。

```
ldapmodify -D "cn=orcladmin" -w administrator_password -h my_host -p port -f
mod.ldif
```

3. ディレクトリ・レプリケーション・サーバーを再起動します。

例 4: レプリカのネーミング・コンテキスト・オブジェクトの orclExcludedNamingcontexts 属性の変更

ディレクトリ・レプリケーション・サーバーは、レプリカのネーミング・コンテキスト・オブジェクトの orclExcludedNamingcontexts 属性の値を使用して、部分レプリケーションから除外する最上位サブツリーを指定します。

この例では、除外対象ネーミング・コンテキストが ou=Europe,c=us および ou=Americas,c=us に設定されます。これは、この 2 つのネーミング・コンテキストが部分レプリケーションから除外されることを意味しています。

1. サンプル・ファイル mod.ldif を、次のように編集します。

```
cn=naming_context_identifier,
cn=replication namecontext,orclagreementid=replication_agreement_
identifier,orclreplicaid=consumer_replica_identifier,cn=replication
configuration
Changetype:modify
Replace: orclExcludedNamingcontexts
orclExcludedNamingcontexts: ou=Europe, c=us
orclExcludedNamingcontexts: ou=Americas, c=us
```

2. ldapmodify を使用して、レプリケーション承諾の orclupdateschedule 属性を更新します。

```
ldapmodify -D "cn=orcladmin" -w administrator_password -h my_host -p port -f
mod.ldif
```

3. ディレクトリ・レプリケーション・サーバーを再起動します。

注意： orclexcludednamingcontexts 属性に指定されたサブツリーは、同一レプリカのネーミング・コンテキスト・オブジェクトで指定される includednamingcontext のサブツリーである必要があります。

例 5: レプリカのネーミング・コンテキスト・オブジェクトの orclExcludedAttributes 属性の変更

含めるネーミング・コンテキストに加えられた特定の変更を、部分レプリケーションから除外するように指定できます。ディレクトリ・レプリケーション・サーバーは、レプリカのネーミング・コンテキスト・オブジェクトの orclExcludedAttributes 属性の値を使用して、除外する属性を判別します。

この例では、orclincludednamingcontexts 属性に指定された telephonenumber 属性および title 属性が、レプリケーションから除外されます。

1. サンプル・ファイル mod.ldif を、次のように編集します。

```
cn=naming_context_identifier,
cn=replication namecontext,orclagreementid=replication_agreement_
identifier,orclreplicaid=consumer_replica_identifier,cn=replication
configuration
Changetype:modify
Replace: orclExcludedAttributes
orclExcludedAttributes: telephonenumber
orclExcludedAttributes: title
```

2. ldapmodify を使用して、レプリケーション承諾の orclupdateschedule 属性を更新します。

```
ldapmodify -D "cn=orcladmin" -w administrator_password -h my_host -p port -f
mod.ldif
```

3. ディレクトリ・レプリケーション・サーバーを再起動します。

レプリケーションの管理

レプリケーションのインストールおよび構成後は、レプリケーションに関連するオブジェクトのデフォルト値を表示および変更できます。この項では、次の項目について説明します。

- ディレクトリ・レプリケーション・サーバーの構成パラメータの表示および変更
- 特定のレプリカ・ノードについてのパラメータの表示および変更
- レプリケーション承諾のパラメータの変更
- 全ノードでのレプリケーション管理者パスワードの変更
- 変更ログの管理
- ディレクトリ・レプリケーションの速度変更

関連項目：

- 24-12 ページの「レプリケーション承諾」
- 24-14 ページの「レプリカ・サブエントリ」

注意： レプリケーション・サーバーを再起動するまで、構成パラメータまたはレプリケーション承諾への変更は有効になりません。

ディレクトリ・レプリケーション・サーバーの構成パラメータの表示および変更

ディレクトリ・レプリケーション・サーバーの構成パラメータのリストおよび説明は B-36 ページの表 B-30 を参照してください。これらのパラメータは、`cn=configset0,cn=osdrepld,cn=subconfigsubentry` の識別名を持つレプリケーション・サーバー**構成設定エントリ**に格納されます。このエントリには、レプリケーション処理を制御するレプリケーション属性が含まれています。この属性の一部は変更できます。

Oracle Directory Manager を使用したディレクトリ・レプリケーション・サーバーの構成パラメータの表示

ディレクトリ・レプリケーション・サーバーの構成パラメータを表示する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**、「**サーバー管理**」の順に展開します。

2. 「**レプリケーション・サーバー**」を選択します。次のタブ・ページが、右側のペインに表示されます。
   - **アクティブ・レプリケーション・サーバー**: 現在実行中のディレクトリ・レプリケーション・サーバーを示します。
   - **レプリケーション・ステータス**: 各サプライヤから DRG 内の各コンシューマに適用された最終変更の番号を示します。
   - **変更ログ・サブスクライバ・ステータス**: 変更ログに対応するサブスクライバをリストし、このノードから適用された最終変更の番号を示します。

Oracle Directory Manager を使用したディレクトリ・レプリケーション・サーバーの構成パラメータの変更

ディレクトリ・レプリケーション・サーバーの構成パラメータを変更する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**、「**サーバー管理**」、「**レプリケーション・サーバー**」を展開します。
2. パラメータを変更するレプリケーションの構成設定を選択します。対応するタブ・ページが、右側のペインに表示されます。
3. 「**一般**」タブ・ページのフィールドを、必要に応じて変更します。このタブ・ページのフィールドの説明は、C-12 ページの表 C-14 を参照してください。
4. Oracle9*i* Advanced Replication ベースの承諾については、「**ASR 承諾**」タブ・ページのフィールドを必要に応じて変更します。このタブ・ページのフィールドの説明は、C-12 ページの表 C-15 を参照してください。
5. ディレクトリ・レプリケーション・サーバーを再起動して、変更内容を反映させます。

注意： DRG の全ノードのホスト名すべてを「レプリケーション・グループ・ノード」フィールドに必ず追加してください。DRG の全ノードに対して、この追加を実行してください。

コマンドライン・ツールを使用したディレクトリ・レプリケーション・サーバーの構成パラメータの変更

コマンドライン・ツールを使用してレプリケーションの構成パラメータを変更するには、A-32 ページの「ldapmodify の構文」で説明する構文を使用してください。

B-36 ページの表 B-30 は、レプリケーション・サーバーの構成パラメータのリストおよび説明です。表に示されているように、レプリケーションの変更可能な構成パラメータは、次のとおりです。

- orclChangeRetryCount
- orclThreadsPerSupplier

例 : ldapmodify を使用した、変更がパージ・キューに移動される前の再試行回数の変更 この例では、mod.ldif という名前の入力ファイルを使用して、再試行の回数をデフォルトの 10 回から 5 回に変更します。具体的には、更新を 5 回試行すると、その更新は削除され、レプリケーション・ログに記録されます。

1. サンプル・ファイル mod.ldif を、次のように編集します。

```
dn: cn=configset0,cn=osdrepld,cn=subconfigsubentry
changetype: modify
replace: orclChangeRetryCount
orclChangeRetryCount: 5
```

2. レプリケーション・サーバーの configset0 パラメータの値を更新するには、次のように ldapmodify を使用します。

```
ldapmodify -D "cn=orcladmin" -w administrator_password -h my_host -p 389 -f
mod.ldif
```

3. ディレクトリ・レプリケーション・サーバーを再起動します。

例 : ldapmodify を使用した変更ログの処理に使用されるワーカー・スレッド数の変更 この例では、mod.ldif という名前の入力ファイルを使用して、変更ログの処理で使用されるワーカー・スレッドの数を 7 に変更します。

1. サンプル・ファイル mod.ldif を、次のように編集します。

```
dn: cn=configset0,cn=osdrepld,cn=subconfigsubentry
changetype: modify
replace: orclthreadspersupplier
orclthreadspersupplier: 7
```

2. レプリケーション・サーバーの configset0 パラメータの値を更新するには、次のように ldapmodify を使用します。

```
ldapmodify -D "cn=orcladmin" -w administrator_password -h my_host -p 389 -f
mod.ldif
```

3. ディレクトリ・レプリケーション・サーバーを再起動します。

関連項目： ディレクトリ・レプリケーション・サーバーを再起動する方法は、A-16 ページの「Oracle Internet Directory サーバー・インスタンスの再起動」を参照してください。

特定のレプリカ・ノードについてのパラメータの表示および変更

特定のレプリカ・ノードを変更するには、レプリカ・サブエントリを変更します。レプリカ・サブエントリで変更できるパラメータのリストと説明は、B-36 ページの表 B-31 を参照してください。

注意： ディレクトリ・レプリケーション・サーバーは、レプリケーション・ノードのオブジェクトをコンシューマから読み込むため、すべての変更をコンシューマおよびサプライヤ（オプション）に適用する必要があります。

関連項目： レプリカ・サブエントリの詳細は、24-14 ページの「レプリカ・サブエントリ」を参照してください。

Oracle Directory Manager を使用した特定のレプリカ・ノードのパラメータの表示と変更

Oracle Directory Manager を使用して特定のレプリカ・ノードを表示および変更する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**、「**レプリケーション管理**」を展開します。
2. 表示または変更するレプリカ・ノードを選択します。対応するタブ・ページが、右側のペインに表示されます。
3. 「**一般**」タブ・ページでは、必要に応じてフィールドを変更してもかまいません。このタブ・ページのフィールドの説明は、C-13 ページの表 C-16 を参照してください。
4. 「**レプリカ承諾**」タブ・ページでは、指定ノードがメンバーとなっているレプリケーション承諾の詳細を参照できます。このタブ・ページの列の説明は、C-14 ページの表 C-17 を参照してください。
5. レプリカ・ノードを表示し、変更した後は、ディレクトリ・レプリケーション・サーバーを再起動します。

コマンドライン・ツールを使用した特定のレプリカ・ノードの変更

コマンドライン・ツールを使用してレプリケーションの構成パラメータを変更するには、A-32 ページの「ldapmodify の構文」で説明する構文を使用してください。

例 : 特定のレプリカ・ノードの orclReplicaURI 属性の変更 ディレクトリ・レプリケーション・サーバーは、レプリカ・サブエントリの orclReplciaURI 属性の値を使用して、そのレプリカのディレクトリ・サーバーを検索します。ディレクトリ・サーバーが稼働しているポートまたはホストが変更された場合は、この属性も変更する必要があります。

1. サンプル・ファイル mod.ldif を、次のように編集します。

```
Dn: orclreplicaid=unique_replica_identifier, cn=replication configuration
Changetype:modify
Replace:orclReplicaURI
OrclReplicaURI: ldap://host_name:port_number/
```

2. ldapmodify を使用して、レプリカ・サブエントリの orclreplicauri 属性を更新します。

```
ldapmodify -D "cn=orcladmin" -w administrator_password -h my_host -p 389 -f
mod.ldif
```

3. ディレクトリ・レプリケーション・サーバーを再起動します。

例 : 特定のレプリカの orclReplicaSecondaryURI 属性の変更 ディレクトリ・レプリケーション・サーバーは、orclReplicaSecondaryURI 属性の値を代替位置として使用して、特定のレプリカをディレクトリ・サーバーに問い合せます。ユーザーは、ldapURI を代替属性として追加でき、この属性は、ディレクトリ・サーバーにとって特定のレプリカについての問合せ先となります。ldapURI 属性を追加する手順は、次のとおりです。

1. サンプル・ファイル mod.ldif を、次のように編集します。

```
Dn: orclreplicaid=unique_replica_identifier, cn=replication configuration
Changetype:modify
add:orclReplicaSecondaryURI
OrclReplicaSecondaryURI: ldap://host_name:port_number/
```

2. ldapmodify を使用して、レプリカ・サブエントリの OrclReplicaSecondaryURI 属性を更新します。

```
Ldapmodify -D "cn=orcladmin" -w administrator_password -h my_host -p 389 -f
mod.ldif
```

3. ディレクトリ・レプリケーション・サーバーを再起動します。

例 : 特定のレプリカの orclReplicaState 属性の変更 OrclReplicaState は、特定のレプリカの状態を表します。レプリカをブートストラップ（再初期化）するには、次のようにこの属性を更新します。

1. サンプル・ファイル mod.ldif を、次のように編集します。

```
Dn: orclreplicaid=<unique replica identifier>, cn=replication configuration
Changetype:modify
replace:orclReplicaState
OrclReplicaState: 0
```

2. ldapmodify を使用して、レプリカのサブエントリの orclreplicastate 属性を更新します。

```
Ldapmodify -D "cn=orcladmin" -w administrator_password -h my_host -p 389 -f
mod.ldif
```

3. ディレクトリ・レプリケーション・サーバーを再起動します。

レプリケーション承諾のパラメータの変更

この項では、Oracle9*i* Advanced Replication ベースおよび LDAP ベースのレプリケーション承諾を変更する方法について説明します。

Oracle9*i* Advanced Replication ベースのレプリケーション承諾のパラメータの変更

Oracle9*i* Advanced Replication ベースのレプリケーション承諾のパラメータは、レプリケーション承諾エントリに格納されています。識別名は次のとおりです。

```
orclAgreementID=000001,cn=replication configuration
```

注意：

- Oracle9*i* Advanced Replication ベースのレプリケーション承諾では、パラメータ `DirectoryReplicationGroupDSAs` に、DRG 内のすべてのノードのホスト名を入力します。このリストは、すべてのノードで同一であることが必要です。
- Oracle Internet Directory 10*g*（9.0.4）の場合、使用できる Oracle9*i* Advanced Replication ベースのレプリケーション承諾は 1 つのみです。このレプリケーション承諾の識別名は、`orclagreementid=000001,cn=replication configuration` です。
- レプリケーション承諾のパラメータを変更する前に、すべてのノードで Oracle Internet Directory を起動していることを確認してください。

関連項目：

- 25-41 ページの「Oracle Directory Manager を使用した Oracle9i Advanced Replication ベースのレプリケーション承諾の表示と変更」
- 25-42 ページの「ldapmodify を使用した Oracle9i Advanced Replication ベースのレプリケーション承諾の管理」

Oracle Directory Manager を使用した Oracle9*i* Advanced Replication ベースのレプリケーション承諾の表示と変更 Oracle Directory Manager を使用してレプリケーション承諾のパラメータを表示および変更する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**、「**レプリケーション管理**」の順に展開します。次のタブ・ページが、右側のペインに表示されます。
   - **レプリケーション・ステータス**：各サプライヤから DRG 内の各コンシューマに適用された最終変更の番号を示します。
   - **レプリカ状態**：レプリカの状態（オンライン、オフライン、ブートストラップ中のいずれか）を示します。
   - **変更ログ・サブスクライバ・ステータス**：変更ログに対応するサブスクライバをリストし、このノードから適用された最終変更の番号を示します。
   - **ASR 承諾**：Oracle9*i* Advanced Replication ベースのレプリケーション承諾についての情報を表示および変更できます。このタブ・ページのフィールドの説明は、C-12 ページの表 C-15 を参照してください。

注意： DRG の全ノードのホスト名すべてを「レプリケーション・グループ・ノード」フィールドに必ず追加してください。DRG の全ノードに対して、この追加を実行してください。

2. このペインをオープンした時点で表示されていた値に戻す場合は、「**回復**」をクリックします。変更内容に問題がない場合は、「**適用**」をクリックします。

ldapmodify を使用した Oracle9*i* Advanced Replication ベースのレプリケーション承諾の管理 レプリケーション承諾パラメータのリストと説明、および変更できるパラメータの説明は、B-37 ページの表 B-32 を参照してください。

レプリケーション承諾エントリの値にノードを追加するには、LDIF フォーマットのファイルを参照して、コマンドラインで ldapmodify を実行します。

例 1: レプリケーション承諾へのノードの追加

この例では、`mod.ldif` という名前の入力ファイルを使用して、レプリケーション承諾に 2 つのノードを追加します。

1. `mod.ldif` を次のように編集します。

```
dn: orclagreementid=000001,cn=replication configuration
changetype: modify
add: orcldirreplgroupdsas
orcldirreplgroupdsas: hollis
orcldirreplgroupdsas: eastsun-11
```

2. レプリケーション・サーバーの `configset0` パラメータの値を更新するには、次のように ldapmodify を使用します。

```
ldapmodify -D "cn=orcladmin" -w administrator_password -h host -p port -f
mod.ldif
```

3. ディレクトリ・レプリケーション・サーバーを再起動します。

このプロシージャは、識別名が `orclagreementid=000001,cn=replication configuration` のレプリケーション承諾が含まれているエントリを変更します。入力ファイルを適用すると、`oraclagreementid=000001` で管理されているレプリケーション・グループに、`hollis` と `eastsun-11` の 2 つのノードが追加されます。

注意： レプリケーション・プロセスを起動する前に、レプリケート環境の各ノードの orclDirReplGroupDSAs パラメータに、新規ノード（例：前述の LDIF ファイルの例では hollis と eastsun-11）を組み込む必要があります。

25-13 ページの「マルチマスター・レプリケーション・グループへのノードの追加」で、レプリケーション環境に新規ノードを追加する処理について説明します。

Oracle Internet Directory 10*g*（9.0.4）でディレクトリ・レプリケーション・サーバーのためにサポートされている構成設定は 1 つのみのため、構成設定を指定する必要はありません。

例 2: Oracle9*i* Advanced Replication のレプリカ承諾の orclExcludedNamingcontexts 属性の変更

Oracle9*i* Advanced Replication ベースのレプリケーション承諾では、ディレクトリ・レプリケーション・サーバーは、レプリカ承諾エントリの orclExcludedNamingcontexts 属性の値を使用して、レプリケーションから除外する最上位サブツリーを指定します。

この例では、c=us と c=uk という 2 つの上位ネーミング・コンテキストが Oracle9*i* Advanced Replication から除外されます。

1. サンプル・ファイル mod.ldif を、次のように編集します。

```
dn: orclAgreementID=000001, cn=replication configuration
Changetype:modify
Replace: orclExcludedNamingcontexts
orclExcludedNamingcontexts: c=us
orclExcludedNamingcontexts: c=uk
```

2. ldapmodify を使用して、レプリケーション承諾の orclupdateschedule 属性を更新します。

```
ldapmodify -D "cn=orcladmin" -w administrator_password -h consumer_host -p port
-f mod.ldif
```

3. ディレクトリ・レプリケーション・サーバーを再起動します。

LDAP ベースのレプリケーション承諾のパラメータの変更

LDAP ベースのレプリケーション承諾のパラメータは、レプリケーション承諾エントリに格納されています。識別名は次のとおりです。

```
orclAgreementID=id number,orclReplicaId=replica id, cn=replication configuration
```

注意： 承諾がサプライヤ側およびコンシューマ側の両方で同一であることを確認します。最後に適用された変更番号とネーミング・コンテキストは、サプライヤ・ノード側の承諾から読み取られます。他の承諾属性は、コンシューマ側から読み取られます。

Oracle Directory Manager を使用した LDAP ベースのレプリケーション承諾のパラメータの表示と変更 Oracle Directory Manager を使用してレプリケーション承諾のパラメータを表示および変更する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「**ディレクトリ・サーバー・インスタンス**」、「**レプリケーション管理**」、「**レプリカ・ノード: レプリカ識別子**」の順に展開します。
2. 表示または変更するレプリカ承諾を選択します。次のタブ・ページが、右側のペインに表示されます。
   - **一般**: LDAP ベースのレプリケーション承諾についての情報を表示および変更できます。このタブ・ページのフィールドの説明は、C-14 ページの表 C-17 を参照してください。
   - **レプリカのネーミング・コンテキスト**: LDAP ネーミング・コンテキストのオブジェクトを表示、追加、削除および変更できます。このタブ・ページのフィールドの説明は、C-15 ページの表 C-18 を参照してください。

ldapmodify を使用した LDAP ベースのレプリケーション承諾のパラメータの変更 レプリケーション承諾パラメータのリストと説明、および変更できるパラメータの説明は、B-37 ページの表 B-32 を参照してください。

例 1: 特定のレプリカ承諾の orclUpdateSchedule 属性の変更

ディレクトリ・レプリケーション・サーバーは、レプリカ承諾エントリの `orclupdateschedule` 属性の値を使用して、レプリケーション・サーバーがサプライヤからの新しい変更ログを処理する間隔（分単位）を決めます。

次の例では、レプリケーション・サーバーがサプライヤからの新しい変更ログを 1 分ごとに処理します。

1. サンプル・ファイル mod.ldif を、次のように編集します。

```
dn: orclAgreementID=id_number,orclReplicaId=replica_identifier, cn=replication
configuration
Changetype:modify
Replace: orclupdateschedule
orclupdateschedule: 1
```

2. ldapmodify を使用して、レプリケーション承諾の orclupdateschedule 属性を更新します。

```
ldapmodify -D "cn=orcladmin" -w administrator_password -h consumer_host -p port
-f mod.ldif
```

3. ディレクトリ・レプリケーション・サーバーを再起動します。

例 2 特定のレプリカ承諾の orclLastAppliedChangeNumber 属性の変更

ディレクトリ・レプリケーション・サーバーは、orclLastAppliedChangeNumber 属性の値を使用して、コンシューマが処理した適用済最終変更ログの番号を判別します。

レプリケーション・サーバーは、サプライヤ側の同じ複製承諾から orclLastAppliedChangeNumber を読み込むため、orclLastAppliedChangeNumber 属性の変更をサプライヤ・ノードに適用する必要があります。

この例では、サプライヤ側の同じ複製承諾の orclLastAppliedChangeNumber 属性が 700 に設定されています。これは、700 より小さい変更ログ番号を持つすべての変更ログがレプリケーション・サーバーによって処理されていることを表しています。

注意： 部分レプリケーションのノード追加プロシージャ時に指示されている場合を除き、orclLastAppliedChangeNumber 属性は変更できません。

---

1. サンプル・ファイル mod.ldif を、次のように編集します。

```
dn: orclAgreementID=id_number,orclReplicaId=replica_id,cn=replication
configuration
Changetype:modify
Replace: orclLastAppliedChangeNumber
orclLastAppliedChangeNumber: 700
```

2. ldapmodify を使用して、サプライヤ側でレプリケーション承諾の orclupdateschedule 属性を更新します。

```
ldapmodify -D "cn=orcladmin" -w administrator_password -h supplier_host -p port
-f mod.ldif
```

3. ディレクトリ・レプリケーション・サーバーを再起動します。

全ノードでのレプリケーション管理者パスワードの変更

DRG のすべてのノードについてのレプリケーション管理者のデータベース・アカウントのパスワードは、レプリケーション環境管理ツールの -chgpwd ユーティリティを使用して変更できます。このユーティリティを起動するには、次のコマンドを入力します。

```
remtool -chgpwd
```

-chgpswd ユーティリティを実行すると、MDS グローバル名（つまり、マスター定義サイトの名前）、現行のパスワードおよび新規パスワードを要求するプロンプトが表示されます。さらに、新規パスワードの確認を要求されます。誤った現行のパスワードを入力した場合は、再びレプリケーション環境管理ツールを実行する必要があります。

レプリカのレプリケーション識別名のパスワードは、-pchgpwd ユーティリティを使用して変更します。このユーティリティを起動するには、次のコマンドを入力します。

```
remtool -pchgpwd
```

関連項目： このツールの使用方法の詳細は、A-62 ページの「レプリケーション環境管理ツール」を参照してください。

変更ログの管理

Oracle Directory Manager では、最近実行された 25 件の変更を表示し、これらの変更を変更ログ番号別、発生した操作の種類別（追加、変更、削除など）および各変更が加えられたエントリ別にリストすることができます。特定の変更を指定して、その詳細を表示することもできます。

変更ログを管理するには、ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開し、「**変更ログ管理**」を選択します。右側のペインに、直近の変更から順に最近の 25 件の変更が表示されます。変更番号、変更が発生した操作の種類および変更が行われたエントリも表示されます。

特定の変更の詳細を表示するには、右側のペインで該当する変更を選択し、「**プロパティの表示**」を選択します。「変更ログ」ウィンドウが表示されます。「変更ログ」ウィンドウの各フィールドの説明は、C-15 ページの表 C-19 を参照してください。

ディレクトリ・レプリケーションの速度変更

レプリケーションのデフォルトの構成では、orclupdateschedule 属性の値は 1（1 分を表す）に設定されています。orclupdateschedule 属性の値を 0（1 秒を表す）に変更すると、レプリケーションの処理時間を短縮できます。

Oracle9*i* Advanced Replication を使用している場合のディレクトリ・レプリケーションの速度変更

Oracle9*i* Advanced Replication ベースのディレクトリ・レプリケーションのデフォルト構成では、処理時間は約 2.5 分です。

- 1 分で、サプライヤがコンシューマに送信する変更を準備
- 30 秒で、Oracle9*i* Advanced Replication が変更をコンシューマに送信
- 1 分で、コンシューマが変更を適用

Oracle9*i* Advanced Replication の場合、`orclupdateschedule` 属性のデフォルト値を `0` に変更すると、レプリケーション時間は 32 秒になります。この手順は、次のとおりです。

1. `mod.ldif` を次のように編集します。

```
dn: orclagreementid=orclagreementid=000001, cn=replication configuration,
cn=replication configuration
changetype:modify
replace: orclupdateschedule
orclupdateschedule: 0
```

2. `mod.ldif` を次のようにアップロードします。

```
ldapmodify -h host name -p port number -v -f mod.ldif
```

3. ディレクトリ・レプリケーション・サーバーを再起動します。

```
oidctl connect=connect string server=oidrepld instance=instance number restart
```

LDAP ベースのレプリケーションを使用している場合のディレクトリ・レプリケーションの速度変更

LDAP ベースのディレクトリ・レプリケーションのデフォルト構成では、変更がサプライヤから取得され、コンシューマに適用されるまでの処理時間は約 1 分です。
`orclupdateschedule` 属性のデフォルト値を `0` に変更すると、レプリケーション時間は 1 秒になります。この手順は、次のとおりです。

1. `mod.ldif` を次のように編集します。

```
dn: orclagreementid=agreement ID,orclreplicaid=replica ID,
cn=replication configuration
changetype:modify
replace: orclupdateschedule
orclupdateschedule: 0
```

2. mod.ldif を次のようにアップロードします。

   ldapmodify -h *host name* -p *port number* -v -f mod.ldif

3. ディレクトリ・レプリケーション・サーバーを再起動します。

   oidctl connect=*connect string* server=oidrepld instance=*instance number* restart

例 : ファンアウトと組み合せたマルチマスター・レプリケーション・グループのインストールおよび構成

この項では、ファンアウトと組み合せたマルチマスター・レプリケーション・グループのインストールおよび構成を、表 25-2 に示す 3 つのシステムを使用した例で説明します。

表 25-2 部分レプリケーション配置例におけるノード

ノード	ホスト名	ポート
ノード 1	mycompany1.com	3000
ノード 2	mycompany2.com	4000
ノード 3	mycompany3.com	5000

この例のユーザー要件は、次のとおりです。

- いずれかのノードに加えられた変更が他のノードにレプリケートされるように、ノード 1 とノード 2 とを同期させる必要がありますが、ネーミング・コンテキスト cn=private users, cn=mycompany は、このレプリケーションから除外されます。
- ノード 2 の ou=Americas,cn=mycompany の下で行われた変更のみがノード 3 にレプリケートされるように、ノード 3 のネーミング・コンテキスト ou=Americas,cn=mycompany は、ノード 2 から部分的に同期させます。このレプリケーションから除外される変更を、次に示します。
  - cn=customer profile, ou=Americas, cn=mycompany の下で行われた変更
  - userpassword 属性に加えられた変更

この例の 1 つ目の要件を満たすために、マルチマスター・レプリケーション・グループをノード 1 およびノード 2 について設定します。この例の 2 つ目の要件を満たすために、部分レプリカをノード 2 およびノード 3 について設定します。

この項では、次の項目について説明します。

タスク 1: ノード 1 およびノード 2 を対象としたマルチマスター・レプリケーション・グループの設定

ノード 1 およびノード 2 に対してマルチマスター・レプリケーション・グループを設定するには、25-2 ページの「マルチマスター・レプリケーション・グループのインストールと構成」で説明したタスク 1 ～ 5 を実行します。

タスク 2: レプリケーション承諾の構成

ノード 1 とノード 2 間のレプリケーション承諾では、`orclExcludedNamingcontexts` 属性の値を、`cn=private users,cn=mycompany` として指定します。この手順は、次のとおりです。

1. サンプル・ファイル `mod.ldif` を、次のように編集します。

```
dn: orclAgreementID=000001,cn=replication configuration
Changetype:modify
Replace: orclExcludedNamingcontexts
orclExcludedNamingcontexts: cn=private users,cn=mycompany
```

2. ldapmodify を使用して、ノード 1 とノード 2 のレプリケーション承諾の `orclExcludedNamingcontexts` 属性を更新します。このためには、次のように入力します。

```
ldapmodify -D "cn=orcladmin" -w administrator_password -h mycompany1.com -p 3000
-f mod.ldif
ldapmodify -D "cn=orcladmin" -w administrator_password -h mycompany2.com -p 4000
-f mod.ldif
```

タスク 3: ノード 1 およびノード 2 でのレプリケーション・サーバーの起動

このタスクを実行するには、25-12 ページの「タスク 6: DRG の全ノードでのレプリケーション・サーバーの起動」にある指示に従ってください。

タスク 4: ディレクトリ・レプリケーションのテスト

このタスクを実行するには、25-12 ページの「タスク 7: ディレクトリ・レプリケーションのテスト」にある指示に従ってください。

タスク 5: ノード 3 をノード 2 の部分レプリカとしてインストール

部分レプリケーションのブートストラップ機能を使用する場合は、25-24 ページの「自動ブートストラップを使用した LDAP ベースのレプリカの構成」で説明したタスク 1 ～ 3 に従ってください。

ldifwrite ツールを使用してレプリカを構成する場合は、25-26 ページの「ldifwrite ツールを使用した LDAP ベースのレプリカの構成」で説明したタスク 1 ～ 7 に従ってください。

ノード 2 をサプライヤ、ノード 3 をコンシューマと識別します。

タスク 6: 部分レプリケーション承諾のカスタマイズ

この手順は、次のとおりです。

1. コンシューマ側、つまりノード 3 でディレクトリ・サーバーを起動します。
2. この例の 2 つ目の要件を満たすには、ノード 2 とノード 3 の間に、部分レプリカのデフォルトのレプリケーション・パラメータを構成する必要があります。部分レプリケーションでは、デフォルトでネーミング・コンテキスト `cn=oraclecontext` がレプリケートされます。サプライヤとコンシューマの両方でこのネーミング・コンテキストを削除することにより、レプリケートしないように選択できます。

```
ldapdelete -D "cn=orcladmin" -w administrator_password -h mycompany2.com -p 4000
"cn=includednamingcontext000001,cn=replication
namecontext,orclagreementid=000002,orclreplicaid==<node2_replica_
id>,cn=replication configuration"

ldapdelete -D "cn=orcladmin" -w administrator_password -h mycompany3.com -p 5000
"cn=includednamingcontext000001,cn=replication
namecontext,orclagreementid=000002,orclreplicaid==<node2_replica_
id>,cn=replication configuration"
```

ネーミング・コンテキスト ou=Americas,cn=mycompany をレプリケートし、ネーミング・コンテキスト cn=customer profile, ou=Americas, cn=mycompany および userpassword 属性をレプリケーションから除外するには、ネーミング・コンテキスト・オブジェクトを次のように作成します。

1. サンプル・ファイル mod.ldif を、次のように編集します。

```
dn: cn=includednamingcontext000002,cn=replication
namecontext,orclagreementid=000002,orclreplicaid=node2_replica_id,cn=replication
configuration
orclincludednamingcontexts: ou=Americas,cn=mycompany
orclexcludednamingcontexts: cn=customer profile, ou=Americas, cn=mycompany
orclexcludedattributes: userpassword
objectclass: top
objectclass: orclreplnamectxconfig
```

2. ldapadd を使用して、部分レプリケーションのネーミング・コンテキスト・オブジェクトをノード 2 とノード 3 の両方に追加します。

```
ldapadd -D "cn=orcladmin" -w administrator_password -h mycompany2.com -p 4000 -f
mod.ldif
ldapadd -D "cn=orcladmin" -w administrator_password -h mycompany3.com -p 5000 -f
mod.ldif
```

部分レプリケーションの自動ブートストラップ機能を使用する場合は、次の手順を実行してください。

1. サンプル・ファイル mod.ldif を、次のように編集します。

```
dn: orclreplicaid=<node2's replica id>,cn=replication configuration
changtype: modify
replace: orclreplicastate
orclreplicastate: 0
```

2. ldapmodify を使用して、ノード 2 とノード 3 で部分レプリカの orclreplicastate 属性を変更します。

```
ldapmodify -D "cn=orcladmin" -w administrator_password -h mycompany2.com -p 4000
-f mod.ldif
ldapmodify -D "cn=orcladmin" -w administrator_password -h mycompany3.com -p 5000
-f mod.ldif
```

タスク 7: DRG の全ノードでのレプリケーション・サーバーの起動

このタスクを実行するには、25-29 ページの「タスク 9: コンシューマ・レプリカでディレクトリ・レプリケーション・サーバーを起動」にある指示に従ってください。

26

高可用性とフェイルオーバーに関する考慮事項

この章では、Oracle Internet Directory のテクノロジ・スタックにおける様々なコンポーネントの可用性とフェイルオーバー機能について説明し、一般的なディレクトリ配置に関してこれらの製品を最適な状態で活用する方法を示します。次の項目について説明します。

- Oracle Internet Directory の高可用性とフェイルオーバーの概要
- Oracle Internet Directory および Oracle のテクノロジ・スタック
- クライアントにおけるフェイルオーバー・オプション
- パブリック・ネットワーク・インフラストラクチャのフェイルオーバー・オプション
- Oracle Internet Directory の高可用性とフェイルオーバー機能
- プライベート・ネットワーク・インフラストラクチャのフェイルオーバー・オプション
- 高可用性の配置例

> **関連項目：** クラスタ化された環境における高可用性とフェイルオーバーの詳細は、「ディレクトリ・レプリケーションおよび高可用性」を参照してください。

Oracle Internet Directory の高可用性とフェイルオーバーの概要

Oracle Internet Directory は、ミッション・クリティカルなアプリケーションに必要な高度なシステム可用性を提供するため、次のことを実現します。

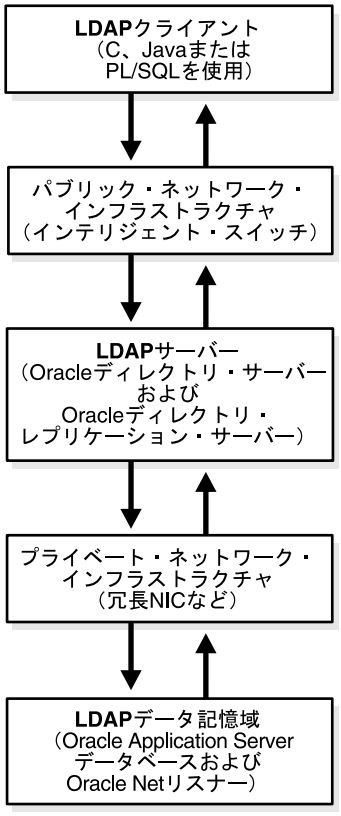
- システム内のすべてのコンポーネントで冗長構成を促進
- すべてのインタフェースで、**フェイルオーバー**と呼ばれる障害の認識とリカバリを促進
- 配置システム全体における、アプリケーションに依存しないネットワーク・フェイルオーバー機能の統合

Oracle 製品は通常、高可用性環境を目標として設計されており、必要な機能は Oracle テクノロジ・スタックのすべての層に組み込まれています。通常、すべてのコンポーネントでフェイルオーバー機能を使用する必要はありません。

Oracle Internet Directory および Oracle のテクノロジ・スタック

図 26-1 に、Oracle Internet Directory スタックの様々なコンポーネントの概要を示します。別々のコンピュータ間のスタック通信は、いくつかのコードのレイヤーを使用して、一方のノードから他方のノードへ情報を送ることによって発生します。情報はクライアント側でレイヤーを下降します。また、ネットワーク・メディアによるトランスポートのためにパッケージされます。情報はその後サーバー側のスタックを上昇し、対応するレイヤーによって変換および解釈されます。

図 26-1 Oracle Internet Directory および Oracle のテクノロジ・スタック



製品の可用性を最大限にするために、十分なフォルト・トレランス機能を各層に組み込むことができます。以降の項では、これらの各層で使用可能な高可用性オプションについて説明します。

クライアントにおけるフェイルオーバー・オプション

クライアントに十分なインテリジェント機能を取り込み、プライマリ Oracle ディレクトリ・サーバーで障害が発生した場合に、代替の Oracle ディレクトリ・サーバーにフェイルオーバーするオプションが有効な場合があります。このためには、クライアントに代替のサーバー情報をキャッシュし、接続障害の検出時にその情報を使用する必要があります。可用性を保証するこの方法は、ディレクトリにアクセスするクライアントのタイプを、完全に制御できる配置システムに対してのみ実行可能です。

この項では、次の項目について説明します。

ユーザー入力からの代替サーバー・リスト

クライアントは、プライマリ・サーバーで障害が発生した場合に自動的にフェイルオーバーできるように、代替の Oracle ディレクトリ・サーバーのリストをユーザーからの入力として受け取るように設計できます。ただし、このオプションは、クライアントの数が増加すると、クライアント・インストールの管理という面で負荷が高くなります。

Oracle Internet Directory サーバーからの代替サーバー・リスト

Oracle Internet Directory は、`AltServer` と呼ばれる DSE ルート属性をサポートしています。これは、LDAP バージョン 3 規格の属性で、ディレクトリ管理者がメンテナンスします。この属性は、ローカル・サーバーと同じネーミング・コンテキストのセットを持つ、システム内の他の Oracle ディレクトリ・サーバーを指し示します。ローカル・サーバーとの接続が失われた場合に、クライアントは、この属性にリストされているサーバーの 1 つにアクセスすることができます。このオプションを使用する場合は、この属性をメンテナンスする十分な管理活動が必要です。

クライアントは、プライマリ・サーバーで障害が発生した場合に使用できるように、代替サーバー・リスト内に情報をキャッシングする必要があります。

Oracle Directory Manager を使用した代替サーバー・リストの設定

代替サーバー・リストを設定する手順は、次のとおりです。

1. ナビゲータ・ペインで、「Oracle Internet Directory サーバー」を展開して、サーバーのインスタンスを選択します。右側のペインにシステム操作属性が表示されます。
2. 「代替サーバー」フィールドに、代替サーバーの名前を入力します。
3. 「OK」をクリックします。

関連項目：

- `altServer` 属性の使用方法の詳細は、`http://www.ietf.org` にある RFC 2251 を参照してください。
- `AltServer` 属性の設定手順は、6-17 ページの「コマンドライン・ツールを使用した属性の管理」を参照してください。

パブリック・ネットワーク・インフラストラクチャのフェイルオーバー・オプション

Oracle Internet Directory サービスへのアクセスに使用されるネットワークは、パブリック・ネットワーク・インフラストラクチャと呼ばれます。パブリック・ネットワーク・インフラストラクチャでネットワーク・レベルのロード・バランシングとフェイルオーバー対策（接続のリダイレクション）を準備することをお薦めします。これらの対策はアプリケーション・クライアントに対して、高度な柔軟性と透過性を提供します。

Oracle Internet Directory サービスが、インターネットからアクセスされる場合、このアクセスには、いくつかの高速リンク（T1 ～ T3）とインテリジェント TCP/IP レベルの接続リダイレクタが使用されます。Oracle Internet Directory サービスが、イントラネットからアクセスされる場合は、Oracle ディレクトリ・サーバーを実行しているサーバー・コンピュータへの高速 LAN 接続と、インテリジェント TCP/IP レベルの接続リダイレクタが使用されます。いずれの場合も、1 つの Oracle ディレクトリ・サーバー・コンピュータの障害が可用性に影響を与えないように、LDAP 要求を処理するコンピュータが複数存在しています。

図 26-2 に、ネットワーク・レベルのフェイルオーバーが使用可能な Oracle Internet Directory の一般的なインターネット配置を示します。

図 26-2 ネットワーク・レベルのフェイルオーバー

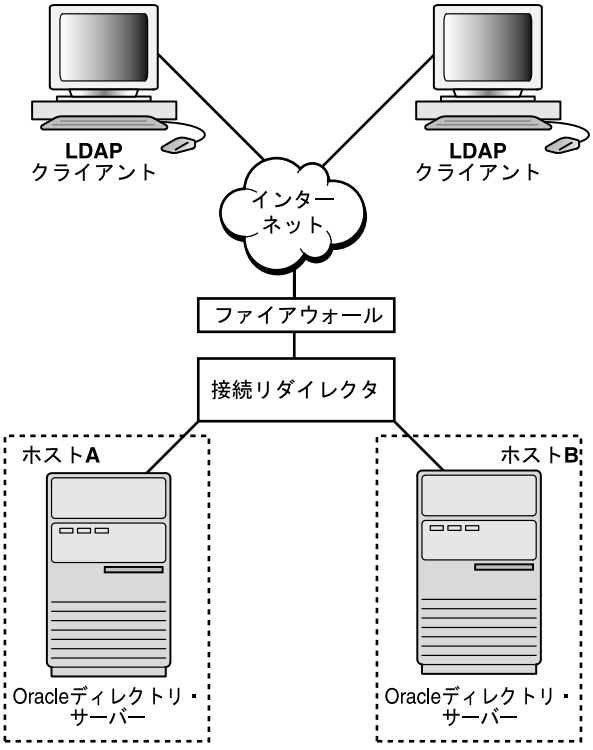


図 26-2 では、Oracle ディレクトリ・サーバー（LDAP サーバー）は、同じバックエンドのデータベースまたは異なるバックエンドのデータベースのいずれにも接続できます。この配置システムの場合、ネットワーク・レベルの接続リダイレクションは、ハードウェアとソフトウェア両方のソリューションによって実施できます。

この項では、次の項目について説明します。

- ハードウェア・ベースの接続リダイレクション
- ソフトウェア・ベースの接続リダイレクション

ハードウェア・ベースの接続リダイレクション

ハードウェア・ベースの接続リダイレクション技術は、複数のベンダーが提供しています。このリダイレクション・デバイスを使用すると、インターネットに直接接続し、複数のサーバー・コンピュータ間で要求の経路を指定できます。また、コンピュータ障害を検出し、障害が発生したコンピュータへの要求の送信を停止できます。この機能によって、クライアントからの新規接続が障害が発生したコンピュータに経路指定されないことが保証されます。コンピュータがリカバリすると、デバイスはそれを検出し、そのマシンへの新規要求の送信を開始します。また、このデバイスは、クライアント要求が均一に配布されるように、ある程度のロード・バランシングも実行します。

ハードウェア・ベースのリダイレクション技術を提供しているベンダーの例は、次のとおりです。

- Nortel Networks 社の Accelar Server Switches
- Cisco 社の Local Director
- F5 Labs Inc. 社の BIG/ip
- HydraWEB Technologies 社の Hydra
- Coyote Point Systems 社の Equalizer

ソフトウェア・ベースの接続リダイレクション

ソフトウェア・ベースのソリューションは、本質的に、対応するハードウェアと同様の方法で機能します。現在使用可能なソリューションの例に、Resonate 社の Dispatch および IBM 社の Network Dispatcher などがあります。

Oracle Internet Directory の高可用性とフェイルオーバー機能

マルチマスター・レプリケーション機能によって、ディレクトリ・システムは、そのシステム内のノードが少なくとも 1 つ使用可能であるかぎり、アクセスと更新のいずれにも常時使用できます。一定時間、非稼働状態のノードがオンラインに復旧すると、既存のノードからのレプリケーションが自動的に再開し、その内容は透過的に同期化されます。

高可用性が必要とされるディレクトリ・システムでは、常にマルチマスター構成でレプリケート・ノードのネットワークを使用する必要があります。レプリカ・ノードは、相対的に低速または帯域幅の狭いネットワーク・セグメントが原因になることがあるため、他の領域から分離されている各領域ごとに作成することをお薦めします。このような構成は、同一領域ではクライアントへのディレクトリ・アクセスを迅速に処理しながら、他の場所で領域障害が発生したとき、フェイルオーバー対策としても機能します。

プライベート・ネットワーク・インフラストラクチャのフェイルオーバー・オプション

プライベート・ネットワーク・インフラストラクチャは、Oracle Internet Directory とそのバックエンド・コンポーネントが相互通信に使用するネットワークです。Oracle Internet Directory がインターネット上に配置される場合、このネットワークとクライアント要求の処理に使用するネットワークを物理的に分離することをお薦めします。Oracle Internet Directory がイントラネットを介して配置される場合は、同一の LAN を使用できますが、ネットワーク・スイッチを利用して、Oracle Internet Directory のコンポーネント専用の帯域幅を確保してください。Oracle Internet Directory は、その通信に関してプライベート・ネットワーク・インフラストラクチャに依存するため、プライベート・ネットワークにおける障害発生時の可用性を保証するために、十分な予防措置を講じる必要があります。この領域で使用可能なオプションの例は、次のとおりです。

- IP アドレス・テイクオーバー（IPAT）
- 冗長リンク

IP アドレス・テイクオーバー（IPAT）

IP アドレス・テイクオーバー機能は、多数の商用クラスタで使用可能です。この機能は、ネットワーク・インタフェース・カード（NIC）の障害から装置を保護します。このメカニズムを使用するには、装置に 2 つの NIC があり、各 IP アドレスが 1 つのサーバーに割り当てられている必要があります。2 つの NIC は、いずれも同じ物理ネットワークに接続されている必要があります。一方の NIC は常にアクティブで、他方の NIC はスタンバイ・モードです。システムは、メイン・アダプタに問題を検出するとすぐに、スタンバイ NIC にフェイルオーバーします。継続中の TCP/IP 接続には影響しないため、クライアントが、そのサーバーの停止時間に気づくことはありません。

冗長リンク

すべてのネットワーク（ワイヤレス・ネットワークは除く）は、ある場所から別の場所まで配線されたケーブルで構成されているため、クライアント・コンピュータとサーバー・コンピュータを接続しているケーブルが誤って切断される可能性があります。これに対する予防措置を講じるには、リンク・レベルの障害時に冗長リンクを使用する機能を持つ、NIC とハブまたはスイッチを使用してください。

高可用性の配置例

図 26-3 では、データベースと Oracle ディレクトリ・サーバー（LDAP サーバー）は、同じコンピュータに共存しています。一方のディレクトリ・サーバー・インスタンスに加えられた変更は、マルチマスター・レプリケーション機能によってもう一方のディレクトリ・サーバー・インスタンスに反映されます。特定のノードでディレクトリ・サーバーまたはデータベース・サーバーに障害が発生すると、その障害はコンピュータ障害とみなされ、接続リダイレクタは、障害が発生したコンピュータへの接続の送信を停止します。

図 26-3 配置例（レプリケーションにおける Oracle Internet Directory の 2 つのノード）

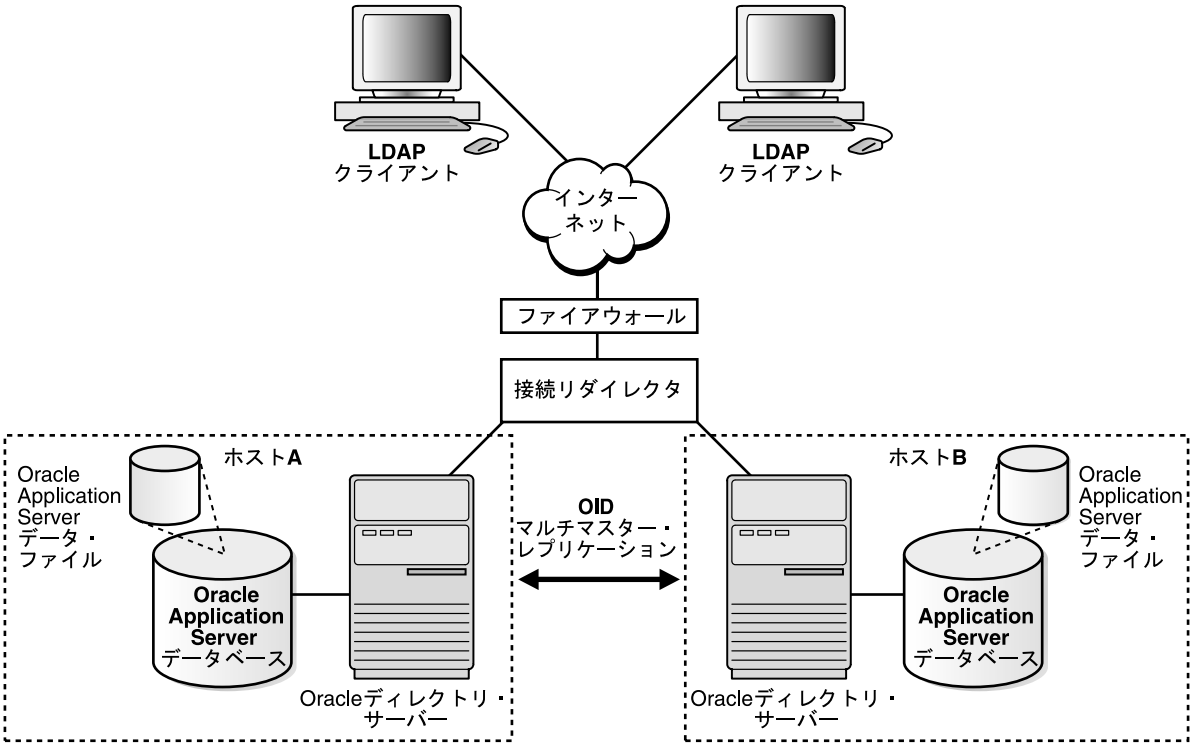
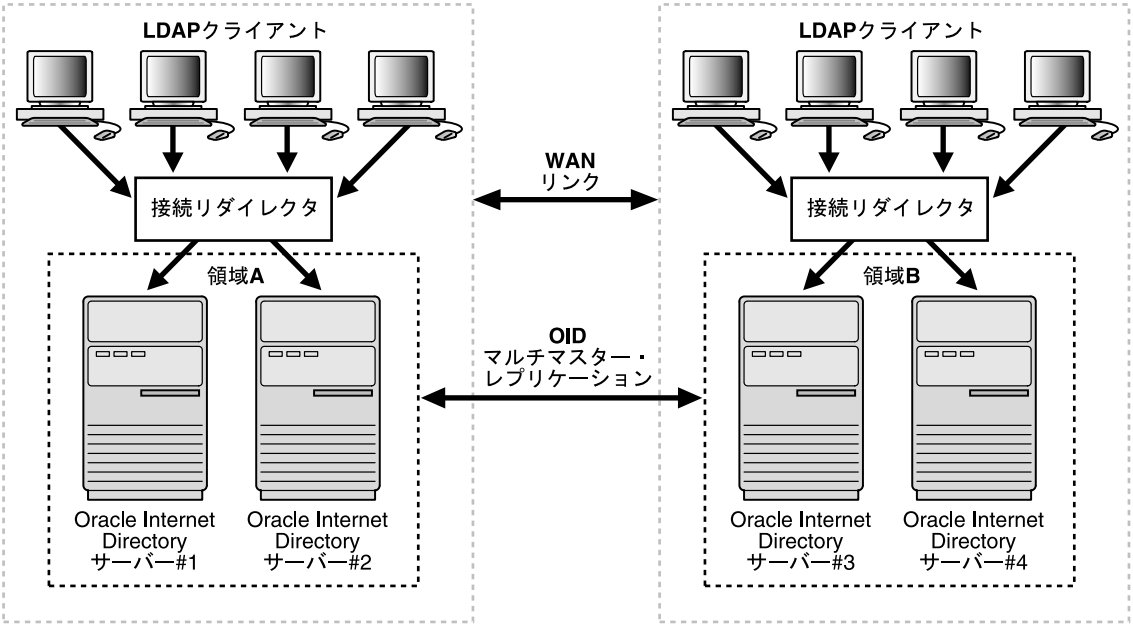


図 26-4 に示すように、相互にレプリケートする 2 つの Oracle Internet Directory ノードを各領域に設定できます。この構成は、大企業が配置しているグローバル・ディレクトリ・ネットワークの典型的な例で、前述の領域がそれぞれ、大陸または国に対応する場合などがあります。

図 26-4 配置例 2



27

ラックマウント型ディレクトリ・サーバー構成

この章では、ディレクトリ・サーバーに高可用性を提供するラックマウント型ディレクトリ・サーバー構成について説明します。この構成では、複数のディレクトリ・サーバーのインスタンスを異なるハードウェア・ノードで実行します。ディレクトリ・サーバーは、同一ディレクトリ・ストアに接続されます。このディレクトリ・ストアは、Oracle9*i* データベース・サーバーです。

この章では、次の項目について説明します。

注意： この章では、ディレクトリ・サーバーの高可用性構成について説明します。ディレクトリ・データが格納されるデータベース・サーバーの高可用性については説明していません。データベース・サーバーについては、Oracle Real Applications Clusters や Data Guard のようなデータベース・サーバーを対象とした標準の高可用性構成を使用してください。

関連項目： 第 29 章「Oracle9i Real Application Clusters 環境でのディレクトリ」

ラックマウント型ディレクトリ・サーバー構成の概要

ラックマウント型ディレクトリ・サーバー構成では、複数のディレクトリ・サーバー・インスタンスが異なるハードウェア・ノードで実行されます。ただし、これらのインスタンスは、同一ディレクトリ・ストア、すなわち Oracle9*i* データベース・サーバーに接続されます。

ラックマウント型構成の主要な利点は、次のとおりです。

- スケーラビリティおよびパフォーマンス

  ロード・バランシングは、LDAP クライアントを複数のディレクトリ・ノードにリダイレクトすることによって実現します。ディレクトリ・ノードに追加された各ハードウェア・ノードによって、サポートされる同時クライアント数と LDAP 操作のスループットの両方が増加します。

- ディレクトリ・サーバーの高可用性

  ディレクトリ・サーバーの高可用性は、あるディレクトリ・サーバー・ノードで障害が発生した場合、LDAP 要求の方向を、正常に動作している他のディレクトリ・サーバー・ノードへ切り替えるネットワーク・リダイレクタによって実現します。

- 所有コストの低減

  ラックマウント型ディレクトリ・サーバー構成では、低価格のハードウェアのみで、高パフォーマンス、高可用性、スケーラビリティのすべての利点が得られます。

ラックマウント型ディレクトリ・サーバー構成のアーキテクチャ

27-3 ページの図 27-1 に、ラックマウント型ディレクトリ・サーバー構成のアーキテクチャを示します。

図 27-1 ラックマウント型ディレクトリ・サーバー構成のアーキテクチャ

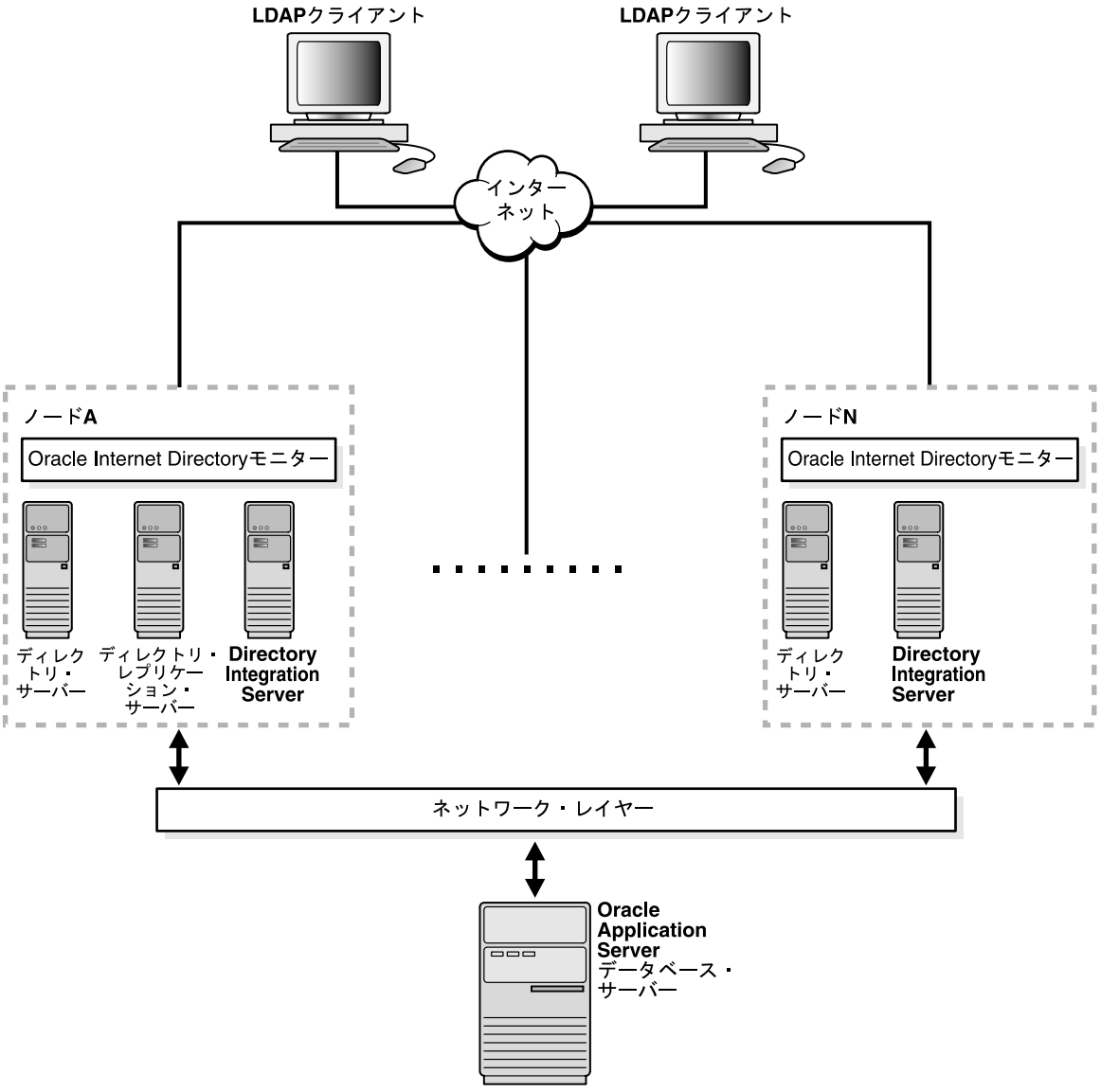


図 27-1 に示すとおり、ラックマウント環境では、レプリケーション・サーバーは 1 つのノードにのみ常駐します。1 つのノードの OID モニターが、10 回試行した後、Oracle ディレクトリ・レプリケーション・サーバーまたは Oracle Directory Integration and Provisioning Server の起動に失敗した場合、別のノードの OID モニターに起動要求が送信されます。

同一構成設定エントリを使用して、Oracle Directory Integration and Provisioning Server の複数のインスタンスを起動することはできません。

高可用性のためのロード・バランシング

ディレクトリ・サーバーの高可用性に必要なロード・バランシングは、あるディレクトリ・サーバー・ノードで障害が発生した場合、LDAP 要求の方向を正常に動作している他のディレクトリ・サーバー・ノードへ切り替えるネットワーク・リダイレクタによって実現します。

27-5 ページの図 27-2 に、ラックマウント型ディレクトリ・サーバー構成でのロード・バランシングを示します。

図 27-2 ラックマウント型ディレクトリ・サーバー構成でのロード・バランシング

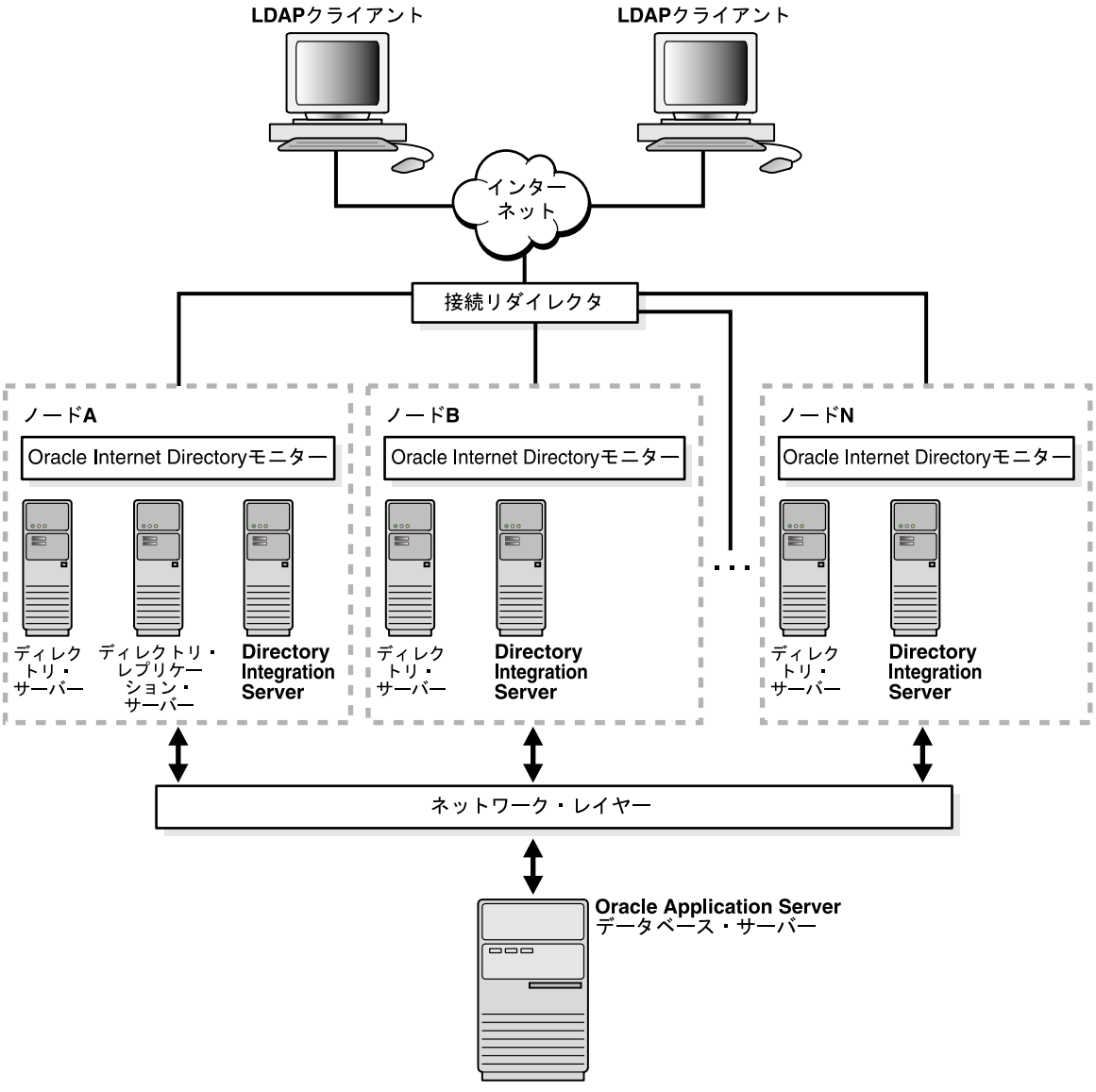


図 27-2 に示すとおり、LDAP クライアントがディレクトリへ接続しようとすると、接続リダイレクタがこの接続を処理します。1 つのディレクトリ・サーバー・ノードに障害が発生すると、このリダイレクタによってクライアントは正常に稼働しているノードに接続されます。

ラックマウント型ディレクトリ・サーバー環境でのメタデータの同期化

ラックマウント型ディレクトリ・サーバー環境では、すべてのディレクトリ・サーバー・ノードでメタデータ（オブジェクト・クラスの定義、属性、一致規則、ACP、パスワード・ポリシーなど）を同期させる必要があります。図 27-3 およびその後に続く説明では、ラックマウント環境内の 2 つのディレクトリ・サーバー・ノード（ホスト A とホスト B）の間でディレクトリ・サーバーのメタデータを同期させるプロセスを示します。

図 27-3 ラックマウント環境でのメタデータの同期化プロセス

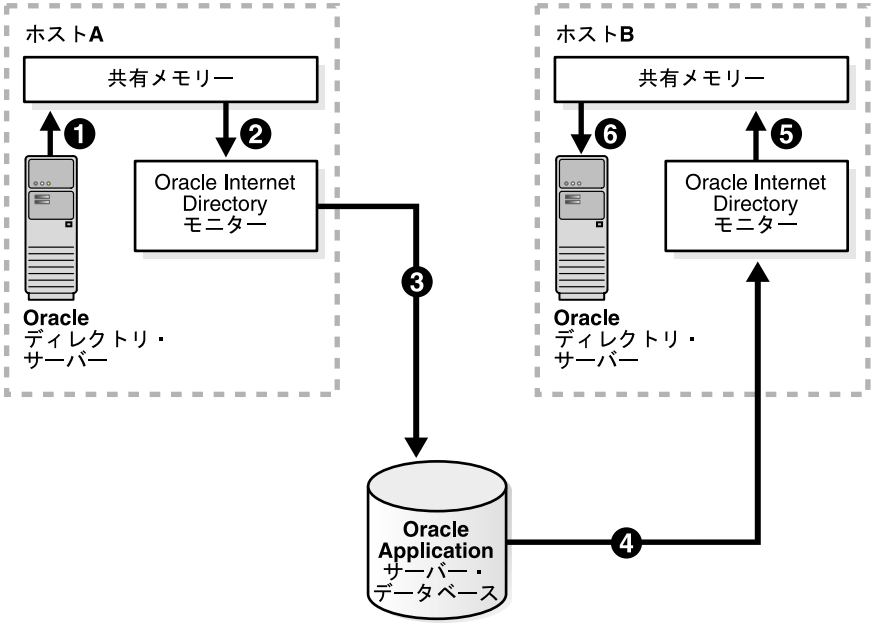


図 27-3 の例では、次のように、ラックマウント環境内でメタデータの同期化が行われます。

1. ホスト A では、ディレクトリ・サーバーが、メタデータの変更をこのホスト上の共有メモリーに書き込みます。
2. ホスト A の OID モニターが、このホスト上の共有メモリーをポーリングします。メタデータの変更が検出されると、この変更が取得されます。
3. OID モニターは、ラックマウント環境のディレクトリ・サーバーのメタデータのリポジトリである Oracle9*i* データベース・サーバーに変更を送信します。
4. ホスト B の OID モニターが、Oracle9*i* データベース・サーバーをポーリングし、ディレクトリ・サーバーのメタデータの変更を取得します。
5. ホスト B の OID モニターが、このホスト上の共有メモリーに変更を送信します。
6. ホスト B のディレクトリ・サーバーが、このホスト上の共有メモリーをポーリングし、メタデータの変更を調べます。その後、これらの変更を取得し、適用します。

ラックマウント型ディレクトリ・サーバー環境でのフェイルオーバーの動作

ラックマウント環境では、各ノードの OID モニターは、10 秒ごとに Oracle9*i* データベース・サーバーにメッセージを送信して、稼働中であることを他のノードに通知します。この処理を行う際、OID モニターは、他のすべてのディレクトリ・サーバー・ノードも実行中であることを確認するために、データベース・サーバーをポーリングします。250 秒後に、いずれかのノードの OID モニターからこの通知が行われなかった場合、他のディレクトリ・サーバー・ノードは、そのノードで障害が発生したものとみなします。この時点で、正常に稼働している他のノードのいずれかで、次の状況が発生します。

1. 稼働中のノードの OID モニターは、障害が発生したノードで実行されていたプロセスを自ノードに移します。
2. そのノードのディレクトリ・サーバーは、障害が発生したノードで進行していた操作の処理を継続します。
3. そのノードの OID モニターは、障害が発生したノードで実行されていたプロセスを移したことを記録します。

27-8 ページの図 27-4 およびその後に続く説明では、架空の 2 つノード A および B でのこのプロセスを示します。

図 27-4 ラックマウント環境でのフェイルオーバーの例

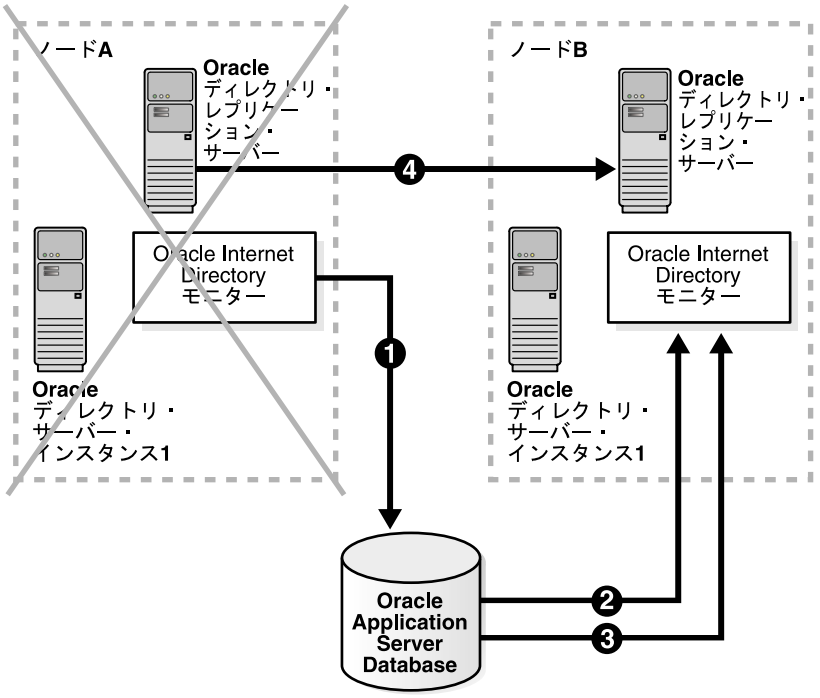


図 27-4 の例に示すとおり、ラックマウント環境内のフェイルオーバー・プロセスは、次のように進行されます。

1. ノード A の OID モニターは、10 秒ごとに、データベースへメッセージを送信して、稼働中であることを通知します。
2. ノード B の OID モニターは、他のノードに障害が発生していないか調べるために、データベースにポーリングします。
3. 250 秒経過してもノード A から応答がなかった場合、ノード B の OID モニターは、ノード A で障害が発生したものとみなします。次に、ノード A で稼働していた Oracle Internet Directory サーバーについての必要な情報をデータベースから取得します。この例では、ディレクトリ・レプリケーション・サーバーがノード A で稼働していたことが認識されます。

4. ディレクトリ・レプリケーション・サーバーはノード B では稼働していなかったため、ノード B の OID モニターは、ノード A で以前稼働していたディレクトリ・レプリケーション・サーバーに対応するディレクトリ・レプリケーション・サーバーを起動します。

関連項目： ディレクトリ・サーバー・ノード、ディレクトリ・サーバー・インスタンス、データベース内に格納されているディレクトリ・メタデータの種類については、2-13 ページの「Oracle Internet Directory のアーキテクチャ」を参照してください。

ラックマウント型ディレクトリ・サーバー環境の管理規則

ラックマウント型ディレクトリ・サーバー環境では、ディレクトリ・サーバーのポート番号は、すべてのノードで共通である必要があります。

ノード間の時間のずれを 250 秒以下にするために、グリニッジ標準時を使用して、すべてのノードの時間値を同期させる必要があります。

障害が発生したノードを再起動する場合は、そのノードで稼働していたすべてのサーバーを手動で起動する必要があります。

Oracle Internet Directory で指定されたデータベースのパスワードを変更する場合は、ラックマウント環境の他の各ノードを更新する必要があります。

関連項目：

- Oracle Internet Directory で指定されたデータベースのパスワードの変更方法は、A-129 ページの「OID データベース・パスワード・ユーティリティ（oidpasswd）構文」を参照してください。
- A-17 ページの「仮想ホストまたはラック・ノードでの Oracle Internet Directory サーバーの起動と停止」

ラックマウント型ディレクトリ・サーバーのインストール

ラックマウント型ディレクトリ・サーバーをインストールする手順は、次のとおりです。

1. データベース・ノードで、Oracle Internet Directory をインストールします。

   製品を選択するように要求された場合は、「Oracle Application Server Infrastructure」を選択します。

   インストールのタイプを選択するように要求された場合は、「Oracle Application Server Metadata Repository」を選択します。

2. 1 つ目のラックマウント・ノードで、OracleAS Portal Infrastructure、Identity Management の順にインストールします。

   構成オプションを選択するプロンプトでは、「Oracle Internet Directory」を選択します。

   リポジトリを指定するプロンプトでは、`sys dba username/password`、データベース・ノードの名前およびリスナーのポート番号を入力します。これによって、Oracle Internet Directory がインストールされ、リモート・データベースに対するベース・スキーマが構成されます。

3. 他の各ノードで、次のタスクを行います。

   a. OracleAS Portal Infrastructure、Identity Management の順にインストールします。

   b. 構成オプションを選択するプロンプトでは、すべての構成オプション（Oracle Internet Directory など）の選択を解除します。これによって、Oracle Internet Directory がインストールされますが、リモート・データベースに対するベース・スキーマの構成は行われません。

   c. `tnsnames.ora` を 1 つ目のラックマウント・ノードから *`ORACLE_HOME`*`/network/admin` ディレクトリにコピーします。

   d. OID データベース・パスワード・ユーティリティを実行して、Wallet を設定します。このためには、次のように入力します。

      ```
      oidpasswd connect=connect_string_for_the_database_node create_wallet=TRUE
      current_password=Oracle Application Server_admin_password.
      ```

      `connect_string_for_the_database_node` は、手順 c で 1 つ目のラックマウント・ノードからコピーした `tnsnames.ora` ファイルにあるものと同じです。

      `Oracle Application Server_admin_password` は、1 つ目のラックマウント・ノードへのインストールで使用したものと同じです。

   e. 次のように入力して、ディレクトリ・サーバーを起動します。

      ```
      oidmon [connect=connect_string_for_the_database_node] [host=virtual/host_
      name] [sleep=seconds] start

      oidctl connect=connect_string_for_the_database_node server=oidldapd
      instance=server_instance_number [configset=configset_number]
      [host=virtual/host_name] [flags=' -p port_number -work maximum_number_of_
      worker_threads_per_server -debug debug_level -l change_logging' -server
      number_of_server_processes] start
      ```

      関連項目：

      - A-4 ページの「OID モニターの起動」
      - A-7 ページの「Oracle ディレクトリ・サーバー・インスタンスの起動」

28

コールド・フェイルオーバー・クラスタ構成

この章では、Oracle Internet Directory の高可用性構成の 1 つであるコールド・フェイルオーバー・クラスタ構成について説明します。

この章では、次の項目について説明します。

- コールド・フェイルオーバー・クラスタ構成の概要
- 単純なコールド・フェイルオーバー構成
- 仮想ホスト上での Oracle Internet Directory の実行状態を確認する方法
- Oracle Internet Directory レプリケーションと組み合せたコールド・フェイルオーバー・クラスタ構成

コールド・フェイルオーバー・クラスタ構成の概要

クラスタは、相互接続された使用可能なコンピュータ全体の集合体で、単一コンピューティング・リソースとして使用されます。ハードウェア・クラスタによって、高可用性およびスケーラビリティが実現します。

フェイルオーバー中、1 つのクラスタ・ノードで稼働しているアプリケーションは透過的に別のクラスタ・ノードに移行します。この移行時に、クラスタ上のサービスにアクセスするクライアントは一時的に接続できず、フェイルオーバーが完了した後、場合によっては再接続する必要があります。

アプリケーションが常時稼働しているクラスタ・ノードは、**プライマリ・ノード**と呼ばれます。フェイルオーバー中、アプリケーションの移動先となるクラスタ・ノードは、セカンダリ・ノードと呼ばれます。

ハードウェア・クラスタでは、各物理ノードには独自の物理 IP アドレスと物理ホスト名が割り振られます。単一のシステムであるというイメージを外部に示すために、クラスタは、クラスタ内のどの物理ノードにも変更できる動的 IP アドレスを使用します。これは、**仮想 IP アドレス**と呼ばれます。この仮想 IP アドレスに対応するホスト名は、論理または**仮想ホスト名**と呼ばれます。コールド・フェイルオーバー構成のクラスタ上のサービスにアクセスするすべてのネットワーク・クライアントは、仮想ホスト名を使用します。

論理ホストは、1 つ以上のディスク・グループ、およびホスト名と IP アドレスのペアで構成されます。論理ホストは、クラスタ内の物理ホストにマップされます。この物理ホストは、論理ホストのホスト名と IP アドレスを使用することになります。

各ノードは、使用可能な完全なコンピュータですが、ほとんどの場合、すべてのノードがストレージ・サブシステムを共有します。コールド・フェイルオーバー・クラスタ構成では、共有ストレージ・サブシステムは、Oracle Internet Directory のインストール、すなわち *ORACLE_HOME* のホストになります。任意の時点で、このサブシステムにアクセスできるのは、アクティブな 1 つのノードです。

単純なコールド・フェイルオーバー構成

図 28-1 に、不特定多数の LDAP クライアントが物理ホスト A および物理ホスト B に接続する単純なコールド・フェイルオーバー構成を示します。

図 28-1 単純なコールド・フェイルオーバー構成

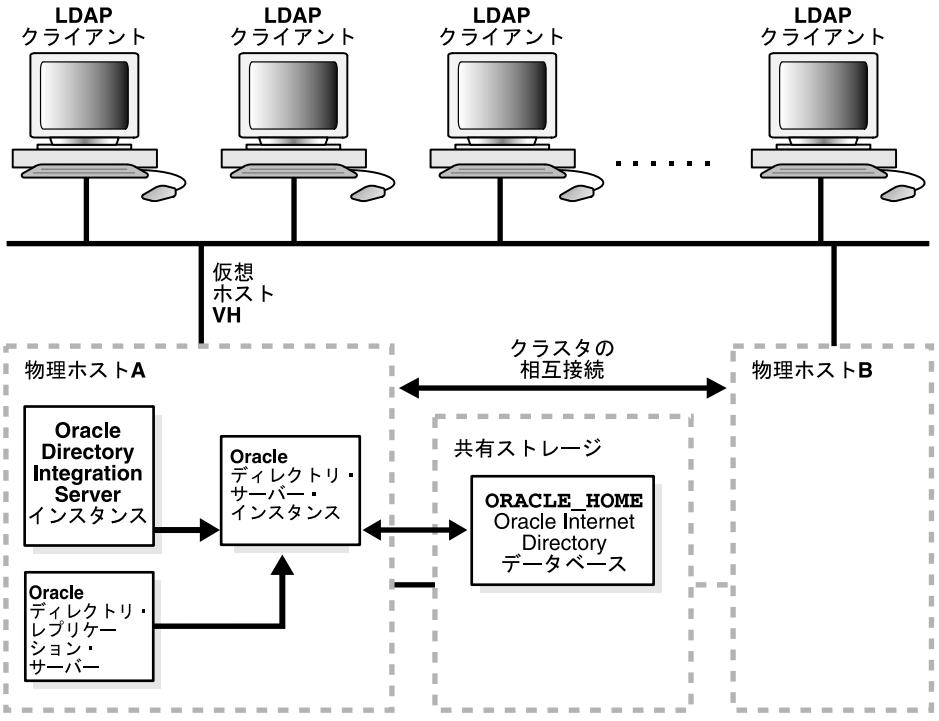


図 28-1 では、物理ホスト A がプライマリ・クラスタ・ノードで、物理ホスト B がセカンダリ・クラスタ・ノードです。インストールされているソフトウェアおよびデータベースは 1 つのみです。物理ホスト A および B は、Oracle Internet Directory ソフトウェアとデータベースが常駐する共有ディスクへのアクセス権を持ちます。

物理ホスト A は、仮想ホスト VH とこの仮想ホスト VH でのインストールのホストとなるように構成されています。Oracle Internet Directory プロセスは、仮想ホスト VH で起動されます。すべての LDAP クライアントは、仮想ホスト名 VH を使用して Oracle Internet Directory と通信します。

仮想ホスト上での Oracle Internet Directory の実行状態を確認する方法

Oracle Internet Directory サーバーは、OID モニター（oidmon）および OID 制御ユーティリティ（oidctl）を使用するか、または Oracle Directory Integration and Provisioning Server 登録ツール（`odisrvreg`）を使用して、仮想ホスト上で起動することができます。

Oracle Directory Integration and Provisioning Server 登録ツール（`odisrvreg`）を使用する場合は、仮想ホスト名を `lhost` パラメータで指定します。

関連項目：

- A-17 ページの「仮想ホストまたはラック・ノードでの Oracle Internet Directory サーバーの起動と停止」
- A-124 ページの「Oracle Directory Integration and Provisioning Server 登録ツール（odisrvreg）」

単純なコールド・フェイルオーバー・プロセス

コールド・フェイルオーバー・プロセスを説明するために、図 28-2 に、28-3 ページの図 28-1 と同じ環境で、物理ホスト A に障害が発生した状況を示します。

図 28-2 コールド・フェイルオーバー・プロセス

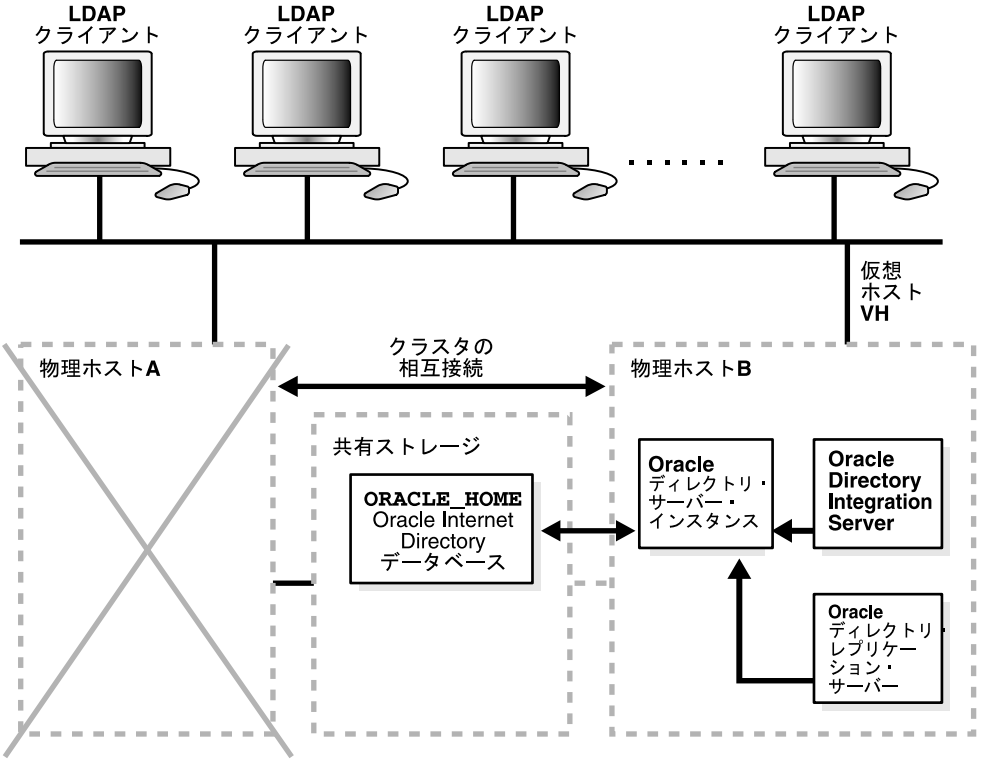


図 28-2 に示すとおり、物理ホスト A で障害が発生したか、またはメンテナンスのために停止した場合、仮想ホスト VH は仮想ホスト B に移行します。フェイルオーバー後は、Oracle9*i* データベース・サーバー、リスナーおよび Oracle Internet Directory を再起動する必要があります。

フェイルオーバーを自動化するために、必要なプロセスを起動するベンダー固有のスクリプトを作成できます。透過的なフェイルオーバーのセマンティックを反映するには、スクリプトを起動するようにクラスタ・ソフトウェアに指定します。

フェイルオーバー後も、LDAP クライアントは、同一ホスト、すなわち仮想ホスト VH との通信を継続します。そのため、これらのクライアントでのサービスの中断は最小限に抑えられます。フェイルオーバーが完了した時点で、クライアントは再接続する必要があります。

Oracle Internet Directory レプリケーションと組み合せたコールド・フェイルオーバー・クラスタ構成

可用性およびスケーラビリティをさらに高めるには、コールド・フェイルオーバー技術を Oracle Internet Directory レプリケーションと組み合せて使用します。28-6 ページの図 28-3 に、この構成を示します。

図 28-3 コールド・フェイルオーバー・クラスタ構成と組み合せたディレクトリ・レプリケーション

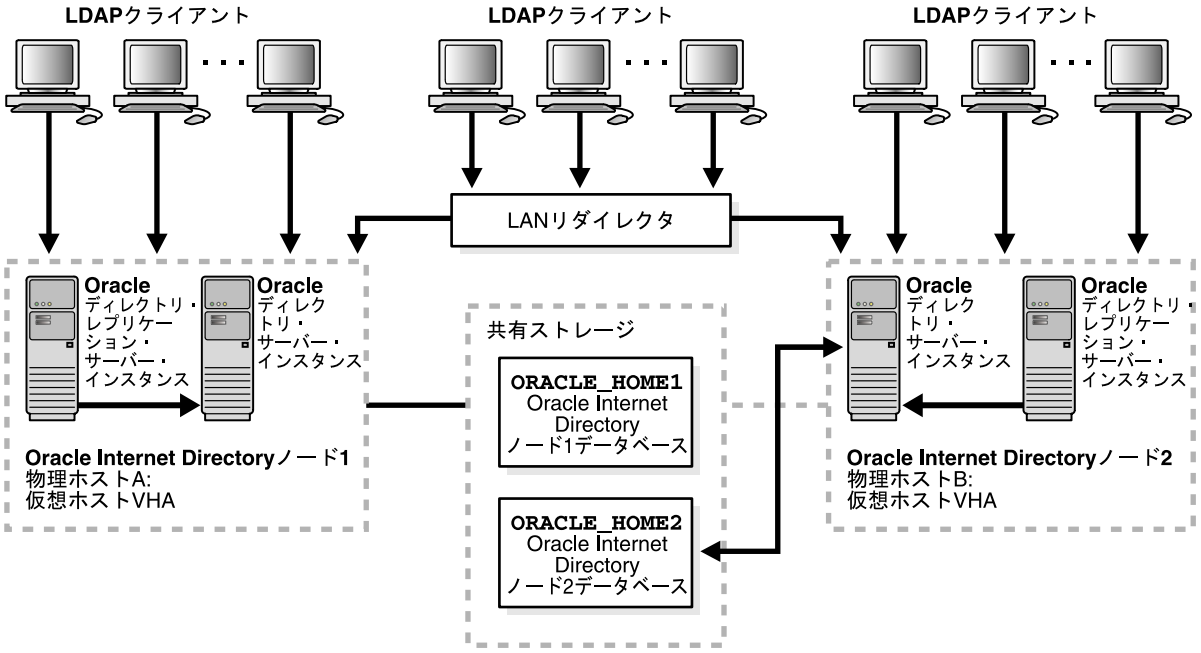


図 28-3 に示すとおり、2 ノード構成のクラスタでは、物理ホスト A が仮想ホスト VHA のホストとなり、物理ホスト B が仮想ホスト VHB のホストとなります。

Oracle Internet Directory のノード 1 は、仮想ホスト VHA にインストールされ、構成されています。

Oracle Internet Directory のノード 2 は、仮想ホスト VHB にインストールされ、構成されています。

Oracle Internet Directory の 2 つのノードは、マルチマスター・レプリケーションに対応するように構成されています。

LDAP アプリケーションでは、次のどちらかを行うことができます。

- LDAP ホストのそれぞれの仮想ホスト名を使用して、Oracle Internet Directory のいずれかのノードと直接通信します。
- Oracle Internet Directory のノードが構成されている 2 つのホストと接続する LAN リダイレクタまたはサード・パーティの別の解決方法を使用して、ロード・バランシングを行います。

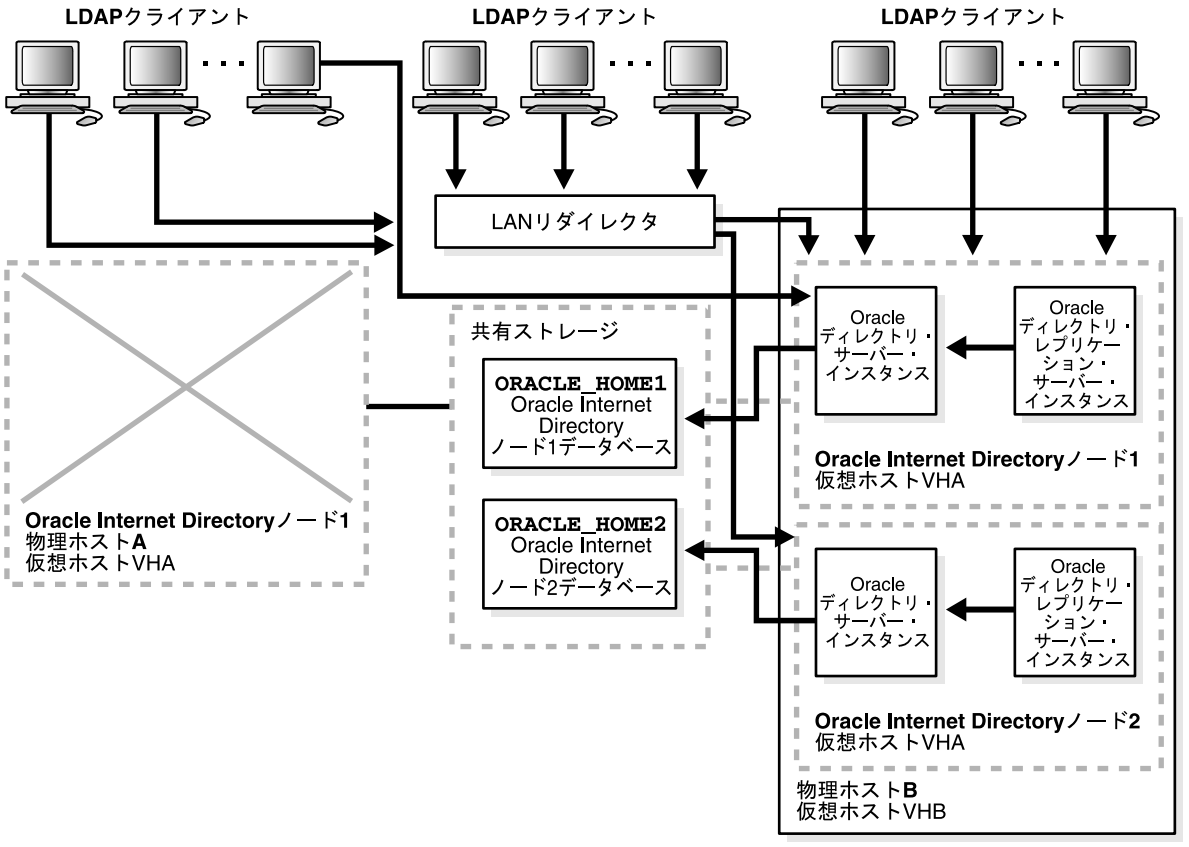
関連項目： 2-14 ページの「Oracle Internet Directory のノード」

この方法でコールド・フェイルオーバーを使用すると、単純なコールド・フェイルオーバー構成よりもパフォーマンスが向上します。Oracle Internet Directory のノードは 2 つあり、いずれもマルチマスター・レプリケーション環境です。Oracle Internet Directory は両方のクラスタ・ノードでアクティブになるため、アクティブ - アクティブ構成となります。アクティブ - パッシブ構成であるコールド・フェイルオーバー構成とは対照的に、Oracle Internet Directory サービスは、どの時点でも両方のクラスタ・ノードで使用可能です。

Oracle ディレクトリ・レプリケーションと組み合せたコールド・フェイルオーバー・プロセス

28-8 ページの図 28-4 に、Oracle ディレクトリ・レプリケーションと組み合せたコールド・フェイルオーバー・プロセスを示します。

図 28-4 Oracle ディレクトリ・レプリケーションと組み合せたコールド・フェイルオーバー・プロセス



28-8 ページの図 28-4 に示すとおり、物理ホスト A で障害が発生したか、またはメンテナンスによる停止時間のために使用できない場合、クラスタ・ソフトウェアは、仮想ホスト VHA を物理ホスト B にフェイルオーバーさせます。物理ホスト A で実行されていた Oracle Internet Directory のプロセスは、仮想ホスト VHA で再起動され、レプリケーションが再開します。

ホスト名 VHA を使用して、Oracle Internet Directory のノード 1 と直接通信している LDAP アプリケーションでは、一時的なサービス停止が発生します。フェイルオーバー完了後、これらのアプリケーションは同一ホスト名（VHA）を使用して再接続する必要があります。ロード・バランシングを行うために LAN リダイレクタが、Oracle Internet Directory の 2 つのノードのフロントエンドになっている場合は、一時的な LDAP の機能停止を完全に回避できます。

29

Oracle9*i* Real Application Clusters 環境でのディレクトリ

Oracle9*i* Real Application Clusters は、複数の、相互接続されたコンピュータの処理能力を活用するコンピューティング環境です。Oracle9*i* Real Application Clusters は、クラスタと呼ばれるハードウェアの集合とともに、各コンポーネントの処理能力を、単一の強力なコンピューティング環境にまとめます。クラスタは、ノードとも呼ばれる 2 つ以上のコンピュータで構成されます。

この章では、Oracle9*i* Real Application Clusters システムで Oracle Internet Directory を実行する方法について説明します。次の項目について説明します。

- 用語
- Oracle9i Real Application Clusters 環境での Oracle ディレクトリ・サーバー
- Real Application Clusters データベース・インスタンスを対象とした Oracle ディレクトリ・サーバーの接続モード
- Oracle Internet Directory の Real Application Clusters ノード間での Oracle ディレクトリ・レプリケーション
- Real Application Clusters ノードでの ODS パスワードの変更

用語

- ノード（Node）

  インスタンスが常駐するコンピュータを指します。ディスク記憶域を他のノードと共有する、大規模パラレル・コンピューティング・インフラストラクチャの一部である場合もあります。ほとんどの場合、ノードはオペレーティング・システムの独自のコピーを持ちます。

- クラスタ（Cluster）

  通常はそれぞれが異なるノード上で実行されるインスタンスの集合です。ディスク上の共有データベースへのアクセス時に相互に調整されます。

- Cluster Manager

  オペレーティング・システム固有のコンポーネントです。クラスタ上のクラスタ・メンバーシップに関する共通ビューを提供して、ノードのメンバーシップ状態を検出して追跡します。

- 透過的アプリケーション・フェイルオーバー（Transparent Application Failover: TAF）

  Oracle9*i* Real Application Clusters や Oracle Fail Safe など、可用性の高い環境を目的としたランタイム・フェイルオーバーです。これは、アプリケーションとサービス間接続のフェイルオーバーおよび再確立を参照します。これによって、接続に障害が発生した場合、クライアント・アプリケーションは自動的にデータベースに再接続され、処理中の SELECT 文を再開します。この再接続は、Oracle Call Interface（OCI）内から自動的に行われます。

  アプリケーションを処理するインスタンスが 1 つ残されていれば、クライアントが接続障害を感知することはありません。

- 接続時フェイルオーバー（Connect-time failover）

  最初のリスナーが応答しない場合に、クライアントの接続要求が他のリスナーに転送されるフェイルオーバー・メソッドです。接続時フェイルオーバーはサービス登録によって有効になります。これは、接続の試行前にインスタンスが起動されているかどうかをリスナーが認識できるためです。

Oracle9*i* Real Application Clusters 環境での Oracle ディレクトリ・サーバー

広範囲にわたる高可用性構成を実現するには、Real Application Clusters がアクティブ / アクティブ・モードで稼働するように Oracle Internet Directory を構成します。このためには、Oracle Internet Directory プロセスおよび Oracle Internet Directory で指定したデータベースを、Real Application Clusters のすべてのノードで実行する必要があります。

図 29-1 に、Oracle9*i* Real Application Clusters データベースが構成されている 2 ノード構成のクラスタを示します。

図 29-1 基本的な高可用性構成の Oracle Internet Directory

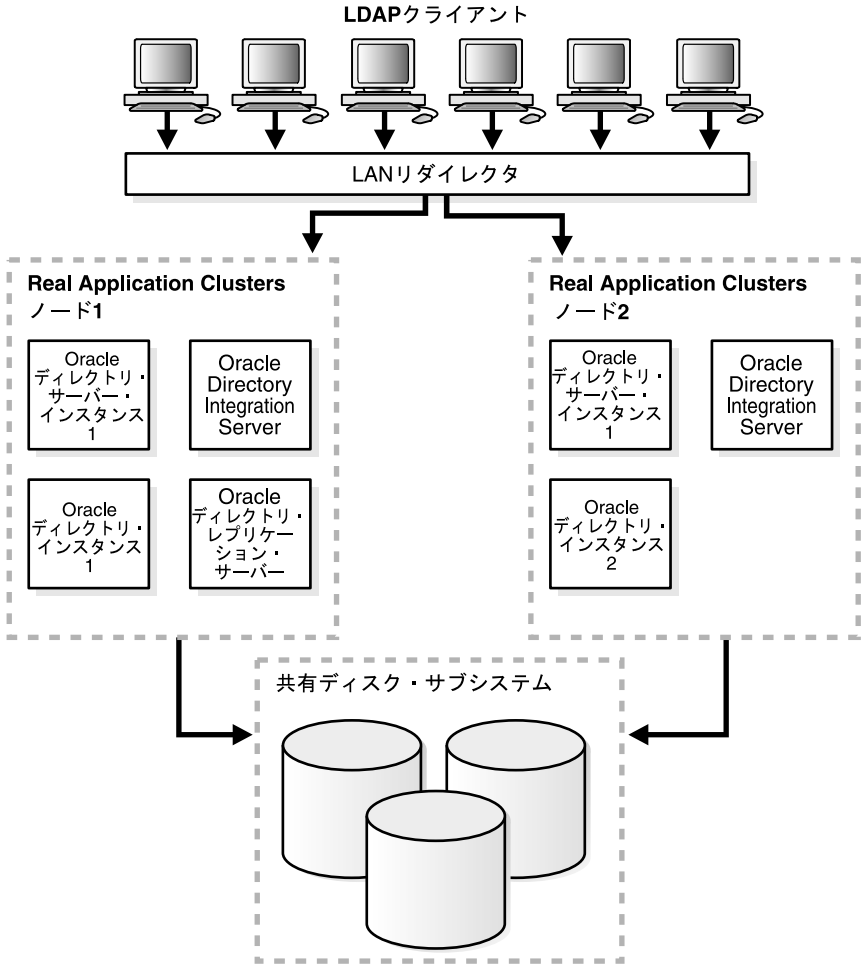


図 29-1 に示す内容は、次のとおりです。

- Oracle ディレクトリ・サーバー・インスタンス 1 は、Real Application Clusters のノード 1 でアクティブであり、Oracle ディレクトリ・サーバー・インスタンス 2 は、Real Application Clusters のノード 2 でアクティブです。各ノードで、複数の Oracle ディレクトリ・サーバー・インスタンスを起動できることに注意してください。
- Oracle Directory Integration and Provisioning Server のインスタンスは、両方のノードでアクティブです。
- Oracle ディレクトリ・レプリケーション・サーバー・インスタンスは、1 つのノードでのみアクティブです。ノードに障害が発生した場合、正常なノード側の OID モニターは、障害が発生したノードから Oracle ディレクトリ・レプリケーション・サーバー・インスタンスを正常なノード側に移します。
- LDAP クライアント・アプリケーションは、異なる Real Application Clusters ノード上の Oracle Internet Directory と直接通信するように構成できます。または、LAN リダイレクタを使用して Oracle Internet Directory サーバー・インスタンスをフロントエンドにして、Real Application Clusters ノードの単一システム・イメージを取り込むこともできます。
- 障害またはメンテナンスのために、1 つの Real Application Clusters ノードを使用できない場合は、もう 1 つの Real Applications Clusters ノード側の Oracle Internet Directory を使用できます。障害が発生した Real Application Clusters ノード上の Oracle Internet Directory と接続されている LDAP クライアントは、再接続する必要があります。

Real Application Clusters データベース・インスタンスを対象とした Oracle ディレクトリ・サーバーの接続モード

この項では、Oracle9*i* Real Application Clusters データベース・インスタンスと通信する Oracle ディレクトリ・サーバー・インスタンスで可能な様々な接続モードについて説明します。これらの接続モードは、Oracle Internet Directory クライアントには透過的で、Oracle Internet Directory とクライアントとの通信には影響を与えません。

この項では、次の項目について説明します。

- load_balance
- 接続時フェイルオーバー（CTF）
- 透過的アプリケーション・フェイルオーバー（TAF）
- フェイルオーバー用の tnsnames.ora ファイルの構成

load_balance

tnsnames.ora ファイル内の load_balance パラメータを on に設定すると、Oracle9*i* データベース・サーバーへの Oracle Internet Directory 接続が、Oracle9*i* データベース・サーバーの各ノードに分散されます。いずれかのノードでフェイルオーバーが発生している場合、使用可能な Oracle9*i* データベース・サーバーのノードへリダイレクトされるのは、障害が発生したノードへの接続のみです。

load_balance パラメータを off に設定すると、Oracle9*i* データベース・サーバーの 1 つのノードのみが、Oracle9*i* データベース・サーバーへのすべての Oracle Internet Directory 接続の対象になります。

フェイルオーバー中、すべての接続は、使用可能な Oracle9*i* データベース・サーバーのノードへリダイレクトされます。

接続時フェイルオーバー（CTF）

Oracle ディレクトリ・サーバーによって Oracle9*i* データベース・サーバーへの接続が行われる場合、Oracle9*i* データベース・サーバーのプライマリ・ノードが使用できないときは、Oracle Internet Directory サーバーはバックアップ（セカンダリ・データベース）へ接続します。

透過的アプリケーション・フェイルオーバー（TAF）

TAF を構成するには、tnsnames.ora ファイルで、type=select および method=preconnect を追加します。

LDAP 検索操作中、Oracle9*i* データベース・サーバーのプライマリ・ノードで障害が発生した場合、Oracle ディレクトリ・サーバーは、Oracle9*i* データベース・サーバーのバックアップ（セカンダリ・ノード）へ透過的に接続し、現行の LDAP 検索操作が継続されます。

フェイルオーバー用の tnsnames.ora ファイルの構成

この項では、2 つのノードでの tnsnames.ora ファイルの構成を示します。

ノード 1

```
db.us.acme.com=
 (description=
  (load_balance=off/on)  /* only connect time load balancing & connection load
balancing */
  (failover=on)          /* only connect time failover */
  (address=
       (protocol=tcp)
       (host=db1)
       (port=1521))
 (address=
```

```
        (protocol=tcp)
        (host=db2)
        (port=1521))
   (connect_data=
      (service_name=db.us.acme.com)
      (failover_mode=
        (backup=db2.acme.com)
        (type=select)
        (method=preconnect))))

db2.acme.com=
  (description=
   (address=
        (protocol=tcp)
        (host=db2)
        (port=1521))
   (connect_data=
      (service_name=db.us.acme.com)
      (instance_name=db2)
      (failover_mode=
      (backup=db2.acme.com)
      (type=select)
      (method=preconnect))
     ))
```

ノード 2

```
db.us.acme.com=
  (description=
   (load_balance=off/on)  /* only connect time load balancing & connection load
balancing */
   (failover=on)          /* only connect time failover */
   (address=
        (protocol=tcp)
        (host=db2)
        (port=1521))
  (address=
        (protocol=tcp)
        (host=db1)
        (port=1521))
   (connect_data=
      (service_name=db.us.acme.com)
      (failover_mode=
        (backup=db1.acme.com)
        (type=select)
        (method=preconnect))))
```

```
db1.acme.com=
 (description=
  (address=
       (protocol=tcp)
       (host=db1)
       (port=1521))
  (connect_data=
     (service_name=db.us.acme.com)
     (instance_name=db2)
     (failover_mode=
     (backup=db2.acme.com)
     (type=select)
     (method=preconnect))))
```

Oracle Internet Directory の Real Application Clusters ノード間での Oracle ディレクトリ・レプリケーション

ディレクトリ・レプリケーションは、Oracle Internet Directory の 2 つ以上の Real Application Clusters ノード間で構成できます。

- ディレクトリ・レプリケーション・グループ（DRG）内の各ノードは、Oracle Internet Directory の Real Application Clusters ノードです。
- ディレクトリ・レプリケーションによって、地理的可用性が得られ、DRG 内の Oracle Internet Directory の Real Application Clusters ノードによって、ローカルな可用性、管理性およびスケーラビリティが保証されます。

Real Application Clusters ノードでの ODS パスワードの変更

OID データベース・パスワード・ユーティリティを使用して、Real Application Clusters の 1 つのノードで ODS パスワードを変更する場合は、他の Real Application Clusters ノードで Wallet `$ORACLE_HOME/ldap/admin/oidpwdlldap1` を更新する必要があります。そのためには、変更した Wallet をすべてのノードにコピーするか、または他のすべてのノードで OID データベース・パスワード・ユーティリティを起動して、Wallet ファイルのみ更新します。この処理は、レプリケーション・パスワードの変更にも適用されます。この場合は、OID データベース・パスワード・ユーティリティではなく、レプリケーション環境管理ツールを使用します。

第 VI 部

Oracle Internet Directory での委任およびセルフ・サービス管理

第 VI 部は次の各章で構成されています。

30

Oracle Delegated Administration Services

この章では、Oracle Delegated Administration Services について説明します。Oracle Delegated Administration Services は、管理コンソールおよびセルフ・サービス・コンソールを構築するための事前定義済 Web ベース・ユニットで構成されるフレームワークです。委任管理者およびユーザーは、これらのコンソールを使用して、指定したディレクトリ操作を実行できます。

次の項目について説明します。

- Oracle Delegated Administration Services の概要
- Oracle Delegated Administration Services のインストールと構成
- Oracle Delegated Administration Services の起動および停止
- Oracle Delegated Administration Services を使用したアプリケーションの作成
- 既存の Oracle ホームでの Oracle Delegated Administration Services の構成
- 新しい Oracle ホームでの Oracle Delegated Administration Services の構成
- 別の DNS ドメインのロード・バランサを使用した Oracle Delegated Administration Services の構成

Oracle Delegated Administration Services の概要

Oracle Delegated Administration Services は、ユーザーのかわりにディレクトリ操作を実行するために事前定義された Web ベースのユニットのセットです。これにより、ディレクトリ管理者は他の管理者やエンド・ユーザーに対して特定の機能を委任でき、ディレクトリ管理の日常的な作業から解放されます。このサービスによって、ディレクトリ対応アプリケーションに必要な大部分の機能が提供されます。たとえば、ユーザー・エントリの作成、グループ・エントリの作成、エントリの検索、ユーザー・パスワードの変更などがあります。

Oracle Delegated Administration Services を使用して、ディレクトリ内のアプリケーション・データを管理するための独自のツールを開発できます。このツールではなく、Delegated Administration Services をベースとするツールである Oracle Internet Directory セルフ・サービス・コンソールを使用することもできます。このツールは、Oracle Internet Directory ですぐに使用できる状態で提供されています。

> **関連項目：** 第 31 章「Oracle Internet Directory セルフ・サービス・コンソール」

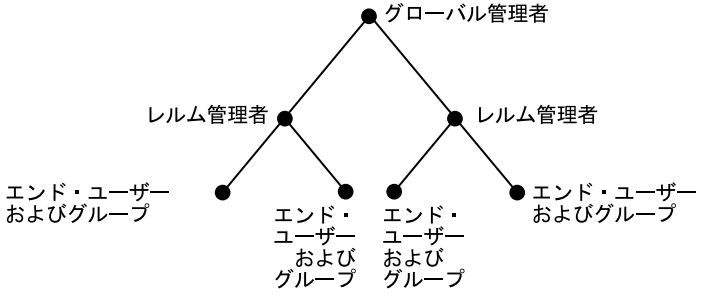
この項では、次の項目について説明します。

- ディレクトリ・データ管理の委任
- Oracle Delegated Administration Services の動作
- Oracle Delegated Administration Services によるディレクトリへの安全なアクセス方法

ディレクトリ・データ管理の委任

Oracle Delegated Administration Services を使用してアプリケーションを構築することにより、それぞれのタイプのユーザーに、特定のレベルのディレクトリ・アクセス権を付与することができます。図 30-1 に、ホスティングされた環境での様々な管理レベルの例を示します。

図 30-1 ホスティングされた環境での管理レベル



ディレクトリ全体の完全な権限を持つグローバル管理者は、ホスティングされた企業を対象としたレルムを作成し管理する権限をレルム管理者に委任できます。これらの管理者は、アプリケーション用パスワード、個人データおよび作業環境を変更する権限をエンド・ユーザーおよびグループに委任できます。このようにして、各タイプのユーザーに、適切なレベルの権限を与えることができます。

Oracle Delegated Administration Services の動作

Oracle Delegated Administration Services では、サーブレットと呼ばれる小さい Java プログラムで使用可能な Oracle Application Server Containers for J2EE（OC4J）を使用します。OC4J とサーブレットを組み合せて、次のタスクを実行します。

1. クライアントからの要求を受け取ります。
2. Oracle Internet Directory のデータを取り出すかまたは更新して、これらの要求を処理し、LDAP 結果を HTML ページにコンパイルします。
3. HTML ページをクライアントの Web ブラウザに戻します。

図 30-2 に、Oracle Delegated Administration Services 環境でのコンポーネント間の情報のフローを示します。

図 30-2 Oracle Delegated Administration Services 環境でのコンポーネント間の情報のフロー

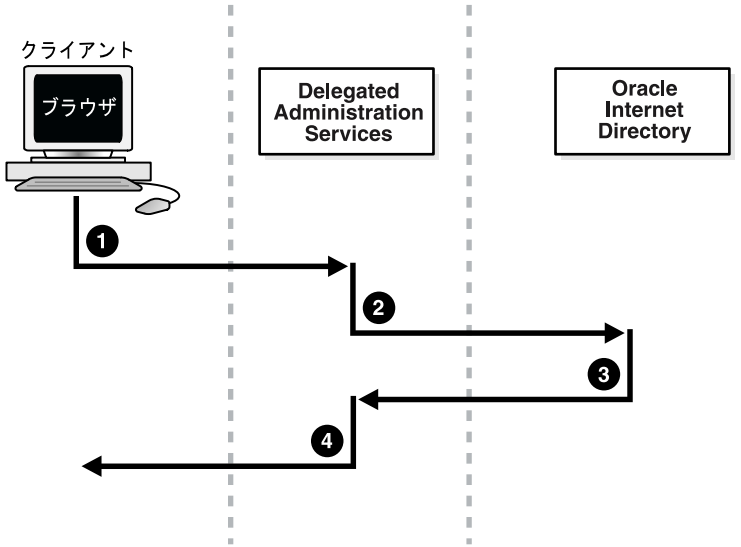


図 30-2 に示す内容は、次のとおりです。

1. ユーザーがブラウザから HTTP を使用して、ディレクトリ問合せが入っている要求を Oracle Delegated Administration Services に送信します。
2. Oracle Delegated Administration Services は、要求を受け取り、適切なサーブレットを起動します。このサーブレットは、要求を解釈し、LDAP を使用してこの要求を Oracle Internet Directory に送信します。
3. Oracle Internet Directory は、LDAP 結果を Oracle Delegated Administration Services サーブレットに送信します。
4. Oracle Delegated Administration Services サーブレットは、LDAP 結果を HTML ページにコンパイルし、それをクライアントの Web ブラウザに送信します。

Oracle Delegated Administration Services によるディレクトリへの安全なアクセス方法

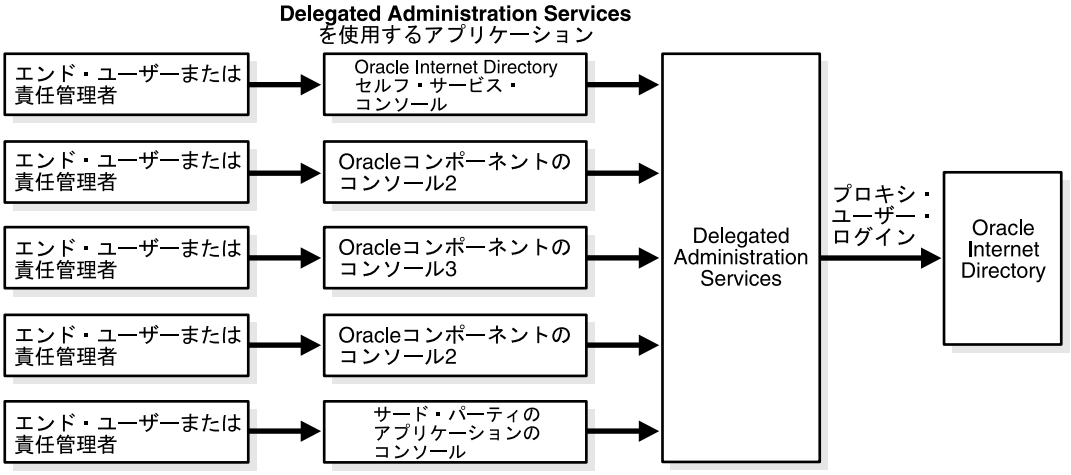
ユーザーが Oracle コンポーネントにログインするとき、このコンポーネントは、ユーザーの代理としてディレクトリから情報（パスワード・ベリファイアなど）を取得する必要がある場合があります。これを行う場合、通常、コンポーネントは**プロキシ・ユーザー**としてディレクトリにログインします。プロキシ・ユーザーとは、識別情報をエンド・ユーザーの識別情報に切り替えられるようにする機能です。

ただし、プロキシ・ユーザーとしてディレクトリにログインするコンポーネントの数が増えると、ユーザーがプロキシ・ユーザーとしてディレクトリへ不正にアクセスするリスクも増えるという問題があります。セキュリティ面のこの問題を回避するために、Oracle Delegated Administration Services ではプロキシ・ユーザーによるアクセスを一元化します。

Oracle Delegated Administration Services 環境では、各コンポーネントは、プロキシ・ユーザーとしてディレクトリにログインせず、中央の Oracle Delegated Administration Services にログインします。その後、Oracle Delegated Administration Services がプロキシ・ユーザーとしてディレクトリにログインし、自身の識別情報をエンド・ユーザーの識別情報に切り替え、ユーザーにかわって操作を実行します。プロキシ・ユーザーに、ディレクトリへアクセスするすべてのコンポーネントへのアクセス権を付与するという安全性の低い手法にかわり、この方法によるプロキシ・ユーザーのディレクトリ・アクセスの一元化が提供されます。

図 30-3 に、Oracle Delegated Administration Services 環境でのプロキシ・ユーザー機能を示します。エンド・ユーザーまたは委任管理者は、中央の Oracle Delegated Administration Services にログインします。このログインには、Oracle Internet Directory セルフ・サービス・コンソール、OracleAS Portal などの他の Oracle コンポーネントのコンソール、またはサード・パーティのアプリケーションのコンソールを使用します。この後、Oracle Delegated Administration Services は、プロキシ・ユーザーとして Oracle Internet Directory にログインします。

図 30-3 Oracle Delegated Administration Services でのプロキシ・ユーザー機能の一元化



Oracle Delegated Administration Services のインストールと構成

この項では、Oracle Delegated Administration Services のインストールおよび構成方法を説明します。次の項目について説明します。

- Oracle Delegated Administration Services 環境でのコンポーネント用ログ・ファイルの位置
- タスク 1: Oracle Delegated Administration Services のインストール
- タスク 2: Oracle Delegated Administration Services が稼働しているかどうかの確認
- タスク 3: デフォルト認証管理レルムの構成
- タスク 4: ユーザー・エントリの構成
- タスク 5: Oracle Delegated Administration Services のデバッグの有効化

Oracle Delegated Administration Services 環境でのコンポーネント用ログ・ファイルの位置

表 30-1 に、Oracle Delegated Administration Services 環境に格納されているコンポーネント用のログ・ファイルの位置を示します。

表 30-1 Oracle Delegated Administration Services 環境でのコンポーネント用ログ・ファイル

アプリケーション	ログ・ファイルの位置
Oracle HTTP Server	*$ORACLE_HOME*/Apache/Apache/logs
Oracle Application Server Containers for J2EE（OC4J）	$*ORACLE_HOME*/j2ee/OC4J_SECURITY/log
Oracle Delegated Administration Services	$*ORACLE_HOME*/ldap/log/das.log
Oracle Process Manager（OPMN）	$*ORACLE_HOME*/opmn/logs

タスク 1: Oracle Delegated Administration Services のインストール

Oracle Delegated Administration Services は、Oracle Internet Directory 10*g*（9.0.4）の一部としてインストールされます。

注意： インストール時、Oracle Delegated Administration Services は、OC4J_SECURITY インスタンスに配置されます。Oracle Delegated Administration Services のほとんどの設定は、このインスタンスに依存するため、このインスタンスの名前を変更しないように注意してください。

関連項目： ご使用のオペレーティング・システム用の Oracle Application Server のインストール・ドキュメント

タスク 2: Oracle Delegated Administration Services が稼働しているかどうかの確認

Oracle Delegated Administration Services が稼働しているかどうかを確認する手順は、次のとおりです。

手順 1: Oracle HTTP Server が稼働しているかどうかの確認

この確認を行うには、次のコマンドを使用します。

```
ps -ef | grep http
```

> **関連項目：** Oracle Delegated Administration Services 環境でのコンポーネント用ログ・ファイルの位置については、30-6 ページの表 30-1 を参照してください。

手順 2: Java（OC4J JVM）が稼働しているかどうかの確認

この確認を行うには、次のコマンドを使用します。

```
ps -ef | grep java
```

Java プロセスが実行されていることを確認します。実行されていない場合は、ログ・ファイルを調べてください。

> **関連項目：** ログ・ファイルの位置については、30-6 ページの表 30-1 を参照してください。

手順 3: Oracle Application Server Single Sign-On Server が稼働しているかどうかの確認

任意のブラウザを使用して、次のように入力します。

```
http://host_name:port_number/orasso/
```

host_name は、Oracle HTTP Server が稼働しているコンピュータの名前で、*port_number* は、対応するポート番号です。Oracle HTTP Server のデフォルトのポート番号は、7777 です。Oracle Application Server Single Sign-On のログイン・ウィンドウを使用して、ログインします。

手順 4: Oracle Delegated Administration Services が稼働しているかどうかの確認

任意のブラウザを使用して、次のように入力します。

```
http://host_name:port_number/oiddas/
```

host_name は、Oracle HTTP Server が稼働しているコンピュータの名前で、*port_number* は、対応するポート番号です。Oracle HTTP Server のデフォルトのポート番号は、7777 です。Oracle Delegated Administration Services のホームページが表示されます。

または、Enterprise Manager の Web サイトを使用して、Oracle Delegated Administration Services が稼働しているかどうかを確認します。この手順は、次のとおりです。

1. Enterprise Manager の Web サイトで、Instance のホームページに移動し、「システム・コンポーネント」までスクロールします。
2. 「名前」列で、「OC4J_SECURITY」を選択します。コンポーネントのホームページには、Oracle Delegated Administration Services のステータスが表示されます。

Oracle Delegated Administration Services が稼働していない場合は、30-9 ページの「Oracle Delegated Administration Services の起動および停止」の説明に従ってこのサービスを起動します。

タスク 3: デフォルト認証管理レルムの構成

このタスクを実行するには、31-11 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用した認証管理レルムの構成」の指示に従ってください。

タスク 4: ユーザー・エントリの構成

このタスクを実行するには、31-13 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用したユーザー・エントリの構成」の指示に従ってください。

タスク 5: Oracle Delegated Administration Services のデバッグの有効化

Oracle Delegated Administration Services のデバッグを有効または無効にするには、*$ORACLE_HOME*/ldap/das/das.properties ファイルを変更します。縦線（|）で値を区切ります。このファイルを変更した後、Oracle Delegated Administration Services インスタンスを再起動します。表 30-2 に、デバッグ引数のデフォルト値と可能な値を示します。

表 30-2　DAS.PROPERTIES ファイルのデバッグ引数

フラグ	デフォルト値	可能な値
DEBUG	FALSE	TRUE
		FALSE
DEBUG_LEVEL	なし	ERROR
		SCHEMA
		TRACING
		SESSION

DEBUG_LEVEL は、DEBUG フラグが TRUE に設定されている場合にのみ解釈されます。TRACING は、デバッグ目的でのみ使用します。

Oracle Delegated Administration Services の起動および停止

この項では、次の項目について説明します。

- コマンドラインを使用した Oracle Delegated Administration Services の起動および停止
- Oracle Enterprise Manager を使用した Oracle Delegated Administration Services の起動、停止および再起動

コマンドラインを使用した Oracle Delegated Administration Services の起動および停止

コマンドラインを使用して Oracle Delegated Administration Services を起動するには、次のように入力します。

```
ORACLE_HOME/dcm/bin/dcmctl start -co OC4J_SECURITY
```

コマンドラインを使用して Oracle Delegated Administration Services を停止するには、次のように入力します。

```
ORACLE_HOME/dcm/bin/dcmctl stop -co OC4J_SECURITY
```

Oracle Enterprise Manager を使用した Oracle Delegated Administration Services の起動、停止および再起動

Enterprise Manager の Web サイトからコンポーネントを起動、停止または再起動する手順は、次のとおりです。

1. Oracle Enterprise Manager の Web サイトで、Instance のホームページに移動し、「**システム・コンポーネント**」までスクロールします。
2. 「名前」列で、**OC4J_SECURITY** を選択します。コンポーネントのホームページが表示されます。
3. 「**システム・コンポーネント**」セクションで、「**起動**」、「**停止**」または「**再起動**」を選択します。

関連項目： 30-7 ページの「タスク 2: Oracle Delegated Administration Services が稼働しているかどうかの確認」

Oracle Delegated Administration Services を使用したアプリケーションの作成

Oracle Internet Directory を使用する Oracle アプリケーションとサード・パーティのセルフ・サービス・アプリケーションのいずれも、Oracle Delegated Administration Services に組み込むことができます。たとえば、Web ポータルを構築している場合、エンド・ユーザーがディレクトリに格納されているアプリケーションのパスワードを変更できるようにするために、Oracle Delegated Administration Services を追加できます。

各ユニットには、ディレクトリ内に格納された対応する URL があります。Oracle Delegated Administration Services のユニットを起動する場合、アプリケーションは、実行時にディレクトリに対応する URL を問い合せます。

> **関連項目：**『Oracle Internet Directory アプリケーション開発者ガイド』の Oracle Delegated Administration Services の URL API の章

ユーザー・エントリを対象とした Oracle Delegated Administration Services

Oracle Delegated Administration Services では、ユーザー・エントリに関する次の操作を実行できます。

- ユーザー・エントリを検索する。
- ユーザー・エントリを作成する。
- パスワードを自動編集する。
- ユーザー・エントリを選択し、編集する。
- ユーザー・エントリを選択し削除する。
- ユーザー・エントリを選択し、そのユーザーへ権限を割り当てる。
- ログインしたユーザーのプロファイルを表示する。
- 値リスト（LOV）（ユーザーを検索し、選択できるようにするポップアップ・ウィンドウ）を使用する。
- `orclguid` 属性を URL へ渡して、ユーザーを編集する。この後、エントリが表示されるため、ユーザーは検索を実行する必要がない。
- `orclguid` 属性を URL へ渡して、ユーザーを削除する。この後、エントリが表示されるため、ユーザーは検索を実行する必要がない。
- `orclguid` 属性を URL へ渡して、ユーザーに権限を割り当てる。この後、エントリが表示されるため、ユーザーは検索を実行する必要がない。

グループ・エントリを対象とした Oracle Delegated Administration Services

Oracle Delegated Administration Services では、グループ・エントリに関する次の操作を実行できます。

- グループ・エントリを検索する。
- グループ・エントリを作成する。
- グループ・エントリを選択し編集する。
- グループ・エントリを選択し削除する。
- グループ・エントリを選択し、そのグループへ権限を割り当てる。
- 値リスト（LOV）（グループを検索し、選択できるようにするポップアップ・ウィンドウ）をグループ化する。
- `orclguid` 属性を URL へ渡して、グループを編集する。この後、エントリが表示されるため、ユーザーは検索を実行する必要がない。
- `orclguid` 属性を URL へ渡して、グループを削除する。この後、エントリが表示されるため、ユーザーは検索を実行する必要がない。
- `orclguid` 属性を URL へ渡して、グループに権限を割り当てる。この後、エントリが表示されるため、ユーザーは検索を実行する必要がない。

既存の Oracle ホームでの Oracle Delegated Administration Services の構成

Oracle Enterprise Manager Application Server Control を使用して Oracle Identity Management の Oracle ホームで Oracle Delegated Administration Services を構成できます。このためには、Enterprise Manager で次の手順を実行します。

- Oracle Delegated Administration Services の URL の設定
- 適切な権限の設定
- OC4J_SECURITY インスタンスでの Oracle Delegated Administration Services の配置

注意： Oracle Delegated Administration Services を構成する前に、Oracle Application Server Single Sign-On が構成されていることを確認してください。Oracle Application Server Single Sign-On によって、Oracle Delegated Administration Services で必要な mod_osso が構成されます。mod_osso は、OracleAS Single Sign-On Server と通信する Oracle HTTP Server モジュールです。

Oracle Enterprise Manager Application Server Control を使用して Oracle Identity Management を構成する手順は、次のとおりです。

1. Enterprise Manager の「**スタンドアロン・インスタンス**」セクションで、Oracle Application Server インスタンスの名前を選択します。そのインスタンスに対応する画面が表示されます。
2. 「**コンポーネントの構成**」を選択します。「コンポーネントの選択」画面が表示されます。
3. 「**Oracle Delegated Administration Services**」を選択し、「**続行**」を選択します。「ログイン」画面が表示されます。
4. ディレクトリのスーパー・ユーザーのユーザー名とパスワードを入力します。デフォルトのユーザー名は `cn=orcladmin` です。
5. 「**終了**」をクリックして、構成を完了します。
6. Oracle Delegated Administration Services が配置される場所で OC4J_SECURITY インスタンスを起動します。この手順は、次のとおりです。
   a. 「**システム・コンポーネント**」セクションで、「**OC4J_SECURITY**」を選択します。
   b. 「**起動**」を選択します。

関連項目： 詳細は、Oracle Application Server 10*g* のインストレーション・ガイドを参照してください。

新しい Oracle ホームでの Oracle Delegated Administration Services の構成

Oracle Delegated Administration Services は、Identity Management および Metadata Repository のデフォルトのインストール（Oracle Internet Directory、Oracle Delegated Administration Services および OracleAS Single Sign-On が選択されている）の一環として自動的に構成されます。状況によっては、Infrastructure が構成されているコンピュータ以外のコンピュータにこのサービスを構成する必要があります。この構成は、Oracle Installer を使用してスタンドアロンの Oracle Delegated Administration Services のインストールを実行するか、または手動で行うことができます。

この項では、次の項目について説明します。

- スタンドアロンの Oracle Delegated Administration Services のインストールの実行
- 新しい Oracle ホームでの Oracle Delegated Administration Services の手動配置

スタンドアロンの Oracle Delegated Administration Services のインストールの実行

スタンドアロンの Oracle Delegated Administration Services のインストールを実行するには、Oracle Installer のプロンプトで求められた場合に「Identity Management」インストール・タイプを選択します。「構成オプション」画面で、「Delegated Administration Service」を選択します。

注意： 同じ Oracle Internet Directory に対して、Oracle Application Server Single Sign-On および Oracle Delegated Administration Services を個別のインストール環境に構成する場合は、最初に、OracleAS Single Sign-On を構成してください。これは、Oracle Delegated Administration Services が mod_osso に依存するためです。mod_osso は、指し示す Oracle Internet Directory に OracleAS Single Sign-On が構成されていないかぎり、インストール中には設定されません。

関連項目： 詳細は、Oracle Application Server 10*g* のインスレーション・ガイドを参照してください。

新しい Oracle ホームでの Oracle Delegated Administration Services の手動配置

新しい Oracle ホームで Oracle Delegated Administration Services を手動で配置する手順は、次のとおりです。

1. 少なくともコア・インストールがコンピュータにインストールされ、そのインストールが既存の Oracle Internet Directory/Oracle Application Server Single Sign-On を指し示していることを確認します。
2. *ORACLE_HOME*/dcm/bin ディレクトリにナビゲートします。
3. 次のコマンドを使用して、新しいコンポーネントを作成します。

   ```
   dcmctl createcomponent -verbose -debug -ct oc4j -co OC4J_SECURITY
   ```

4. 次のコマンドを使用して、コンポーネントを起動します。

   ```
   dcmctl start -verbose -debug -co OC4J_SECURITY
   ```

5. 次のコマンドを使用して、oiddas.ear ファイルを配置します。

   ```
   dcmctl deployApplication -debug -verbose -a oiddas -f
   ORACLE_HOME/ldap/das/oiddas.ear -co OC4J_SECURITY
   ```

6. 次の手順を実行して、環境変数 LD_LIBRARY_PATH および DISPLAY を opmn.xml ファイルに追加します。

   a. *ORACLE_HOME*/opmn/conf ディレクトリに移動し、テキスト・エディタで opmn.xml を開きます。

   b. opmn.xml ファイルの OC4J_SECURITY セクションに次の行を追加します。

      UNIX 環境の場合

      ```
      <environment>
      <prop name="DISPLAY" value="%hostname%:0.0"/>
      <prop name="LD_LIBRARY_PATH" value="%ORACLE_HOME%/lib"/>
      </environment>
      ```

      Windows 環境の場合

      ```
      <environment>
      <prop name="PATH" value="%ORACLE_HOME%/bin"/>
      </environment>
      ```

      ホスト名と ORACLE_HOME を適切な値に置き換えます。ホスト名は、X サーバーが稼働しているコンピュータを示す必要があります。

      次の例の <environment> セクションの配置に注目してください。

      ```
      <oc4j maxRetry="3" instanceName="OC4J_DAS" gid="OC4J_SECURITY"
      numProcs="1">
      <config-file path="/home/ias902/j2ee/OC4J_
      DAS/config/server.xml"/>
      <oc4j-option value="-properties"/>
      <port ajp="3001-3100" jms="3201-3300"
      rmi="3101-3200"/>
      <environment>
      <prop name="DISPLAY" value="sandal:0.0"/>
      <prop name="LD_LIBRARY_PATH" value="/home/ias902/lib"/>
      </environment>
      </oc4j>
      ```

   c. *ORACLE_HOME*/dcm/bin ディレクトリにナビゲートします。

   d. 次のコマンドを使用して、変更内容をリポジトリに保存します。

      ```
      dcmctl updateconfig -verbose -debug -ct opmn
      ```

   e. 次のコマンドを使用して、OPMN を再起動します。

      ```
      dcmctl restart -verbose -ct opmn
      ```

f. 次のコマンドを使用して、OC4J_SECURITY インスタンスを停止し、起動します。

```
dcmctl stop -verbose -debug -ct oc4j -co OC4J_SECURITY
dcmctl start -verbose -debug -ct oc4j -co OC4J_SECURITY
```

g. Oracle Delegated Administration Services に必要な権限を設定します。Oracle Directory Manager またはコマンドライン・ツールのいずれかを使用してグループを変更します。Oracle Delegated Administration Services が現在配置されている場所に、uniquemember として、新しく Oracle Application Server インスタンスの DN を追加します。

```
DN of the group to be modified:
cn=Associated
Mid-tiers,orclApplicationCommonName=DASApp,cn=DAS,cn=Products,cn=OracleConte
xt
```

Oracle Application Server インスタンスの DN は、次のとおりです。

```
orclApplicationCommonName=name of Oracle Application Server instance,cn=IAS
Instances, cn=IAS, cn=Products,
cn=OracleContext
```

name of Oracle Application Server instance は、$ORACLE_HOME/config/ias.properties から取得されます。

別の DNS ドメインのロード・バランサを使用した Oracle Delegated Administration Services の構成

Oracle Application Server Single Sign-On が個別の中間層ノードに構成される環境で Oracle Delegated Administration Services を構成する場合は、『Oracle Application Server Single Sign-On 管理者ガイド』の第 9 章に記載されている拡張構成に関する項の説明に従います。

31

Oracle Internet Directory セルフ・サービス・コンソール

この章では、Oracle Internet Directory セルフ・サービス・コンソールについて説明します。Oracle Internet Directory セルフ・サービス・コンソールは、Oracle Delegated Administration Services を使用して作成された既製のアプリケーションです。

次の項目について説明します。

Oracle Internet Directory セルフ・サービス・コンソールを使用した委任管理

この項では、次の項目について説明します。

委任管理の概要

委任管理は、Oracle Identity Management インフラストラクチャによって提供され、これによってユーザー、グループおよびサービスに関するすべてのデータを中央ディレクトリに保存し、そのデータの管理を複数の管理者とエンド・ユーザーに分散できます。この操作は、ユーザー環境における各種のセキュリティ要件に準拠した方法で実行します。

たとえば、企業において、ユーザー・データ用に 1 人の管理者、電子メール・サービス用にもう 1 人の管理者が必要であるとします。または、Oracle Financials などのコンポーネントの管理者がユーザー権限を完全に制御する必要があり、OracleAS Portal などの別のコンポーネントの管理者が特定のユーザーまたはグループに関する Web ページを完全に制御する必要があるとします。Oracle Identity Management インフラストラクチャが提供する委任管理によって、様々なセキュリティ要件を持つこれらのすべての管理者が、安全でスケーラブルな方法で集中データを管理できます。このような環境では、複数の管理者やエンド・ユーザーに管理を委任するために、Oracle Internet Directory セルフ・サービス・コンソールを使用すると便利です。

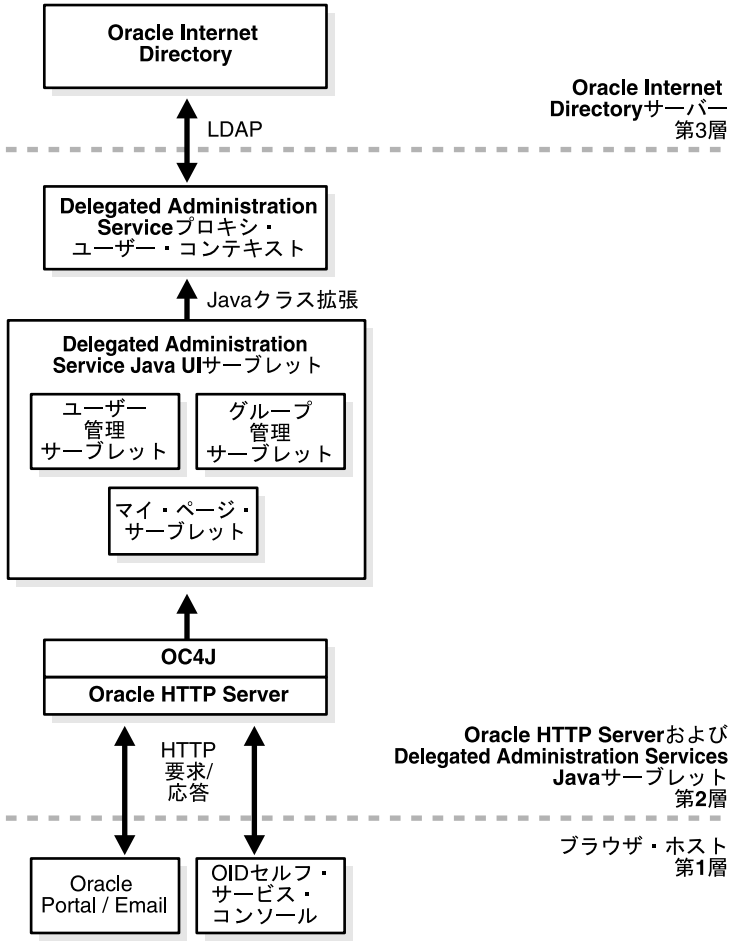
> **関連項目：** 委任管理の詳細は、第 17 章「Oracle テクノロジ配置のための権限の委任」を参照してください。

Oracle Internet Directory セルフ・サービス・コンソールの概要

Oracle Internet Directory セルフ・サービス・コンソールによって、管理者権限を複数の管理者およびエンド・ユーザーに委任することができます。Oracle Internet Directory セルフ・サービス・コンソールは、Oracle Delegated Administration Services を使用して作成された既製のアプリケーションです。ディレクトリ内のデータを管理するための単一のグラフィカル・インタフェースを委任管理者とエンド・ユーザーに提供します。

図 31-1 に、Oracle Internet Directory セルフ・サービス・コンソールと Oracle Delegated Administration Services の相互作用を示します。

図 31-1 Oracle Delegated Administration Services コンポーネントの相互作用



Oracle Internet Directory セルフ・サービス・コンソールの使用

Oracle Internet Directory セルフ・サービス・コンソールを使用すると、管理者もユーザーも各自の権限に応じて、各種のディレクトリ操作を実行できます。この項では、次の項目について説明します。

- Oracle Internet Directory セルフ・サービス・コンソールのスタート・ガイド
- Oracle Internet Directory セルフ・サービス・コンソールを使用したエントリの検索
- エンド・ユーザーのタスクの実行
- 管理者のタスクの実行

Oracle Internet Directory セルフ・サービス・コンソールのスタート・ガイド

この項では、Oracle Internet Directory セルフ・サービス・コンソールの起動、ログインおよび停止について説明します。

Oracle Internet Directory セルフ・サービス・コンソールの起動と停止

Oracle Delegated Administration Services を起動していない場合は、Oracle Internet Directory セルフ・サービス・コンソールを使用する前に起動する必要があります。

> **関連項目：** Oracle Delegated Administration Services の起動方法については、30-9 ページの「Oracle Delegated Administration Services の起動および停止」を参照してください。

Oracle Internet Directory セルフ・サービス・コンソールへのログイン

Oracle Internet Directory セルフ・サービス・コンソールにログインする手順は、次のとおりです。

1. Oracle Internet Directory セルフ・サービス・コンソールの URL にアクセスします。
2. 右上隅の「**ログイン**」を選択します。Oracle Application Server の「Single Sign-On」ウィンドウが表示されます。
3. 「Single Sign-On」ウィンドウの「**ユーザー名**」フィールドに、セルフ・サービス・コンソールのユーザー名（`jdoe` など）を入力します。
4. 「**パスワード**」フィールドには、自分のセルフ・サービス・コンソールのパスワードを入力します。
5. ホスティングされた複数の企業が存在するホスティングされた環境の場合は、「**企業**」フィールドが表示されます。それ以外の場合は、表示されません。「**企業**」フィールドが表示された場合は、企業名を入力します。
6. 「**ログイン**」を選択します。

Oracle Internet Directory セルフ・サービス・コンソールを使用したエントリの検索

Oracle Internet Directory セルフ・サービス・コンソールを使用すると、ユーザー・エントリとグループ・エントリの両方を検索できます。

Oracle Internet Directory セルフ・サービス・コンソールを使用したユーザー・エントリの検索

ユーザー・エントリを検索する手順は、次のとおりです。

1. Oracle Internet Directory セルフ・サービス・コンソールで、「**ディレクトリ**」タブを選択した後、「**ユーザー**」を選択します。
2. 「**ユーザーの検索**」フィールドに、次のいずれかの値の最初の数文字を入力します。
   - 名
   - 姓
   - ログイン名
   - 電子メール識別子
   - ユーザーの cn 属性

   たとえば、Anne Smith を探している場合は、`Ann` または `Smi` と入力します。

   ディレクトリ内の全ユーザーの一覧を出力するには、フィールドを空白のままにしておきます。
3. 「**実行**」を選択すると、検索結果が表示されます。

Oracle Internet Directory セルフ・サービス・コンソールを使用したグループ・エントリの検索

グループ・エントリを検索する手順は、次のとおりです。

1. 「**ディレクトリ**」タブを選択した後、「**グループ**」を選択します。
2. 検索するグループ名の最初の数文字を「**グループ名の検索**」テキスト・ボックスに入力します。

   ディレクトリ内の全グループの一覧を出力するには、フィールドを空白のままにしておきます。
3. 「**実行**」を選択すると、入力した条件に一致したエントリが表示されます。

エンド・ユーザーのタスクの実行

この項では、パスワード、写真、タイムゾーン、リソース・アクセス情報など、エンド・ユーザーの個人プロファイル内の要素を設定および変更する方法について説明します。表 31-1 に、管理タスクおよび対応する情報を示します。

表 31-1 エンド・ユーザーのタスク

タスク	参照先
プロファイルの編集	31-6 ページの「プロファイルの編集」
パスワードの変更	31-6 ページの「パスワードおよびパスワード・ヒントの変更」
パスワードの再設定	31-8 ページの「パスワードを忘れた場合の再設定」
組織図の表示	31-8 ページの「組織図の表示」
タイムゾーン設定の変更	31-8 ページの「タイムゾーン設定の変更」
リソース・アクセス情報の構成	31-9 ページの「リソース・アクセス情報の管理」

プロファイルの編集

プロファイルを編集する手順は、次のとおりです。

1. 「**マイ・プロファイル**」タブ・ページを選択した後、「**マイ・プロファイルの編集**」を選択します。「マイ・プロファイルの編集」ウィンドウが表示されます。
2. 変更を加えます。
3. 「**OK**」を選択します。

> **注意：** 「マイ・プロファイル」タブ・ページをサーバーの最新情報に更新するには、「ページの更新」を選択します。ブラウザの「更新」ボタンや「リロード」ボタンは使用しないでください。これらのボタンを使用すると、サーバーの情報ではなく、中間層キャッシュの情報のみで更新されます。

パスワードおよびパスワード・ヒントの変更

セルフ・サービス・コンソールを使用して、Oracle Application Server Single Sign-On およびその他の Oracle コンポーネント用のパスワードを変更できます。Oracle Application Server Single Sign-On 用のパスワードを変更すると、認証に Oracle Application Server Single Sign-On を使用しているすべてのアプリケーション用のパスワードも変更されます。

パスワードを変更するには、「**マイ・プロファイル**」タブを選択した後、「**マイ・パスワードの変更**」を選択します。「マイ・パスワードの変更」ウィンドウが表示されます。このウィンドウを使用して、Oracle Application Server Single Sign-On または別の Oracle コンポーネント用のパスワードを変更できます。

Oracle Application Server Single Sign-On 用のパスワードを変更する手順は、次のとおりです。

1. 「**Single Sign-On**」セクションで、「**旧パスワード**」フィールドに現在のパスワードを入力します。
2. 「**新規パスワード**」フィールドに新しいパスワードを入力した後、「**新規パスワードの確認**」フィールドに再度入力して確認します。
3. 「**パスワードのヒント**」フィールドには、母親の旧姓などの質問を入力します。後でパスワードを忘れた場合は、この質問に回答することになります。正しく回答すると、パスワードが伝えられます。
4. パスワードのヒントに回答するフィールドに、直前のフィールドに入力したヒントに対する回答を入力します。
5. 「**送信**」を選択します。

注意： パスワードのヒントに回答するフィールドへの入力内容は、入力したとおりに正確に覚えてください。ヒントの回答に、余分な空白、ハイフンまたは大文字の使用などのわずかな違いがあると、保存した回答とは一致しません。

Oracle Application Server Single Sign-On に対しては使用可能になっていない別の Oracle コンポーネント用のパスワードを変更する手順は、次のとおりです。

1. 「**アプリケーション・パスワード**」セクションで、新規パスワードを指定する Oracle コンポーネントを選択します。
2. 「**パスワードの更新**」を選択します。「**アプリケーション・パスワードの変更**」ウィンドウが表示されます。
3. 「**新規パスワード**」フィールドに新しいパスワードを入力した後、「**新規パスワードの確認**」フィールドに再度入力して確認します。
4. 「**送信**」を選択します。

パスワードを忘れた場合の再設定

パスワードを忘れた場合は、再設定できます。セキュリティ上の理由から、パスワードを再設定する場合は、最初にパスワードを設定したときに指定した質問に回答する必要があります。

1. Oracle Internet Directory セルフ・サービス・コンソールのホームページで「**パスワードを忘れた場合**」を選択します。「マイ Single Sign-On パスワードのリセット」ページが表示されます。
2. 「**識別情報の確認**」セクションのフィールドに値を入力します。これらのフィールドはユーザー環境に固有で、管理者によって構成されます。企業名も入力する必要があります。
3. 「**次へ**」を選択します。「追加の個人情報の確認」ウィンドウが表示されます。
4. 31-6 ページの「パスワードおよびパスワード・ヒントの変更」でパスワードのヒントを設定した場合、「追加の個人情報の確認」ウィンドウでは、そのヒントに基づいた質問が行われます。31-6 ページの「パスワードおよびパスワード・ヒントの変更」の手順で指定したパスワードのヒントに対する回答を入力します。

   パスワードのヒントを事前に設定していない場合、「追加の個人情報の確認」ウィンドウでは、管理者が設定したその他の個人データを入力するように要求されます。このデータは、ユーザーの識別情報の検証に使用されます。
5. 「**次へ**」を選択します。「SSO パスワードのリセット」ウィンドウが表示されます。
6. 「**新規パスワード**」フィールドに新しいパスワードを入力した後、「**新規パスワードの確認**」フィールドに再度入力して確認します。
7. 「**送信**」を選択します。

組織図の表示

組織階層内での自分の位置を確認する場合、組織図を表示できます。

組織図を表示するには、「**マイ・プロファイル**」タブを選択した後、「**マイ組織図の表示**」を選択します。

タイムゾーン設定の変更

タイムゾーン設定を変更する手順は、次のとおりです。

1. 「**マイ・プロファイル**」タブを選択した後、「**マイ・タイムゾーンの変更**」を選択します。「タイムゾーンの設定」ウィンドウが表示されます。
2. 「タイムゾーンの設定」ウィンドウで、新しいタイムゾーンを選択した後、「**送信**」を選択します。

リソース・アクセス情報の管理

Oracle Internet Directory セルフ・サービス・コンソールを使用して、リソース・アクセス情報を作成、変更および削除できます。

> **関連項目：** リソース・アクセス情報の詳細は、2-33 ページの「リソース情報」を参照してください。

> **注意：** 次の手順の「**設定**」リンクは、管理者がリソース・アクセス情報を作成した場合のみ表示されます。

リソース・アクセス情報の作成 リソース・アクセス情報を指定する手順は、次のとおりです。

1. 「**マイ・プロファイル**」タブ・ページを選択した後、「**設定**」を選択します。
2. 「**作成**」を選択します。「リソースの作成」ウィンドウが表示されます。
3. 「**リソース名**」フィールドで、リソース名、またはコンポーネントによってアクセスされるサービス名を指定します。
4. 「**リソース・タイプ**」リストで、アクセスされるリソースのタイプを選択します。デフォルトのオプションは次のとおりです。
   - **OracleDB**: Oracle9*i* データベース・サーバー
   - **ExpressPDS**: Oracle Express のトランスポータブル・データ・ソース
   - **JDBCPDS**: Java Database Connectivity のトランスポータブル・データ・ソース

   その他のリソース・タイプは、管理者が指定したとおりに、このリストに表示されます。
5. 「**次へ**」を選択します。リソース・アクセス情報ウィンドウが表示されます。
6. リソース・アクセス情報ウィンドウで、適切な情報を入力します。
7. 「**送信**」を選択します。

リソース・アクセス情報の変更 リソース・アクセス情報を変更する手順は、次のとおりです。

1. 「**マイ・プロファイル**」タブ・ページを選択した後、「**設定**」を選択します。
2. 情報を変更するリソースを選択し、「**編集**」を選択します。「リソースの編集」ウィンドウが表示されます。
3. 「リソースの編集」ウィンドウで、適切な情報を入力します。
4. 「**送信**」を選択します。

リソース・アクセス情報の削除 リソース・アクセス情報を削除する手順は、次のとおりです。

1. 「**マイ・プロファイル**」タブ・ページを選択した後、「**設定**」を選択します。
2. 情報を削除するリソースを選択します。
3. 「**削除**」を選択します。

> **関連項目：** リソース・アクセス情報の詳細は、2-33 ページの「リソース情報」を参照してください。

管理者のタスクの実行

管理者は、必要な管理権限を所有しているタスクおよび、エンド・ユーザーのすべてのタスクを実行できます。表 31-2 に、管理タスクを一覧し、該当する情報の参照先を示します。

表 31-2 管理者のタスク

タスク	参照先
認証管理レルムの管理	31-11 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用した認証管理レルムの構成」
	31-12 ページの「認証管理レルムの構成設定の表示」
	31-12 ページの「認証管理レルムの構成設定の変更」
	31-12 ページの「レルムでのエントリ用の親 DN の構成」
	31-13 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用した認証管理レルムの作成」
ユーザー・エントリの管理	31-13 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用したユーザー・エントリの構成」
	31-16 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用したユーザー・エントリの作成」
	31-17 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用したユーザー・エントリの変更」
	31-18 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用したユーザー・エントリの削除」
	31-18 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用したユーザーへの権限の割当て」
	31-19 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用したユーザー・パスワードの変更」

表 31-2 管理者のタスク（続き）

タスク	参照先
グループ・エントリの管理	31-19 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用したグループ・エントリの作成」
	31-21 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用したグループ・エントリの変更」
	31-21 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用したグループ・エントリの削除」
	31-21 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用したグループへの権限の割当て」
サービスの管理	31-22 ページの「サービス・プロパティの変更」
	31-22 ページの「サービス受信者に関するサブスクリプション情報の変更」
アカウントの管理	31-23 ページの「アカウントの管理」
リソース・アクセス情報の管理	31-24 ページの「リソース・タイプ情報の構成」
	31-16 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用したユーザー・エントリの作成」
	31-24 ページの「デフォルトのリソース・アクセス情報の構成」

Oracle Internet Directory セルフ・サービス・コンソールを使用した認証管理レルムの構成

適切な管理権限を所有している場合は、認証管理レルムに対して次の項目を指定できます。

- ログイン時にユーザーが自己識別に使用する属性
- ユーザー検索ベースおよびグループ検索ベースのルート・エントリ（ユーザーおよびグループ用のエントリを含むディレクトリ情報ツリー内の位置情報）
- ユーザー作成ベースおよびグループ作成ベース用のルート・エントリ（ユーザーおよびグループが作成された DIT 内の位置情報）。これは、ユーザー検索ベースと同じか、またはユーザー検索ベース下の位置情報の可能性があります。
- レルムと製品ロゴの表示

認証管理レルムを構成する手順は、次のとおりです。

1. 「**構成**」タブを選択します。
2. 「認証管理レルム」ウィンドウの各種フィールドに値を入力します。フィールドについては、C-45 ページの表 C-48 を参照してください。
3. 「**送信**」を選択して変更を保存します。

注意：「**ユーザー検索ベース**」フィールドには複数の値を入力できますが、パフォーマンスが低下することがあります。

認証管理レルムの構成設定の表示

認証管理レルムの構成設定を表示する手順は、次のとおりです。

1. Oracle Internet Directory セルフ・サービス・コンソールの右上にある「**レルムの管理**」アイコンを選択します。「認証管理レルム」ウィンドウが表示されます。
2. 「認証管理レルム」ウィンドウで、「**認証管理レルムの検索**」フィールドに、変更対象のエントリを含むレルムの名前のすべてまたは一部を入力し、「**実行**」を選択します。検索条件に一致したレルムが一覧表示されます。
3. 検索結果の一覧から、変更対象のレルムを選択した後、「**表示**」を選択します。「認証管理レルムの表示」ウィンドウが表示されます。このウィンドウのフィールドの説明は、C-45 ページの表 C-48 を参照してください。

認証管理レルムの構成設定の変更

管理者となっている認証管理レルムの設定は変更できます。この手順は、次のとおりです。

1. 「**構成**」タブを選択します。
2. 「認証管理レルム」ウィンドウの各種フィールドに値を入力します。フィールドについては、C-45 ページの表 C-48 を参照してください。
3. フィールドを変更した後、「**送信**」を選択します。

レルムでのエントリ用の親 DN の構成

エントリ用に 1 つ以上の親 DN をレルムに指定できます。複数指定した場合は、委任管理者が新規ユーザー・エントリの配置先の親 DN を選択できます。

親 DN を指定する方法は 2 通りあります。ユーザー作成ベースに値を指定する方法と組織単位（ou）属性に値を指定する方法です。それぞれに異なる値を指定した場合は、ou 属性が優先します。

「ユーザー作成ベース」の値によって親 DN を指定する手順は、次のとおりです。

1. 「**構成**」タブを選択した後、「**認証管理レルム**」を選択します。
2. 「**ユーザー作成ベース**」フィールドに 1 つ以上の DN を入力します（1 行に 1 つの DN を入力します）。
3. 「**送信**」を選択します。

また、組織単位（ou）属性に値を設定することによっても、親 DN を指定できます。この場合は、委任管理者がユーザー・エントリの配置先の組織単位を選択できます。この方法で親 DN を指定する手順は、次のとおりです。

1. 「**構成**」タブを選択し、「**ユーザー・エントリ**」を選択します。
2. 「**次へ**」を選択します。「ユーザー属性の構成」ウィンドウが表示されます。
3. 「**新規属性の追加**」を選択します。「新規属性の追加」ウィンドウが表示されます。
4. 「**ディレクトリ属性名**」リストで、ou 属性を選択します。
5. 「**UI タイプ**」リストから「**事前定義リスト**」を選択します。
6. 「**LOV 値**」フィールドに、親 DN の表示名を入力してセミコロン（;）を 3 つ続け、その後 DN を入力します。親 DN は、別の行に別の親 DN を指定して追加できます。

   次に例を示します。

   ```
   Sales;;;cn=users,dc=us,dc=my_company,dc=com
   HR;;;cn=groups,dc=us,dc=my_company,dc=com
   ```

この例に従って、ユーザー・エントリの配置先の組織単位を選択する場合、委任管理者は、`Sales` および `HR` を表示しているリストから選択します。

Oracle Internet Directory セルフ・サービス・コンソールを使用した認証管理レルムの作成

管理権限を所有している場合は、次のように認証管理レルム用にエントリを作成できます。

1. Oracle Internet Directory セルフ・サービス・コンソールの右上にある「**レルムの管理**」アイコンを選択します。「認証管理レルム」ウィンドウが表示されます。
2. 「認証管理レルム」ウィンドウで「**作成**」を選択します。「認証管理レルムの作成」ウィンドウが表示されます。
3. 「認証管理レルムの作成」ウィンドウのフィールドに該当する値を入力します。フィールドについては、C-44 ページの表 C-47 を参照してください。
4. 「**送信**」を選択します。

Oracle Internet Directory セルフ・サービス・コンソールを使用したユーザー・エントリの構成

ユーザー・エントリの作成または編集時、基本情報、パスワード、写真などの各種カテゴリが、それぞれの属性セットとともに Oracle Internet Directory セルフ・サービス・コンソールに表示されます。コンソールに表示するカテゴリ、表示方法および対応する属性を指定できます。

具体的には、Oracle Internet Directory セルフ・サービス・コンソールを使用して、次のことを実行できます。

- オブジェクト・クラスとユーザー・エントリを関連付けて、これらのオブジェクト・クラスを追加および変更する
- ユーザーが追加または変更できる属性のカテゴリを指定する
- Oracle Internet Directory セルフ・サービス・コンソールによるこれらのカテゴリおよび属性の表示方法をカスタマイズする

ユーザー・エントリを構成する手順は、次のとおりです。

1. 「**構成**」タブを選択し、「**ユーザー・エントリ**」を選択します。ユーザー・エントリに関連付けられている既存のオブジェクト・クラスを示す「ユーザー・オブジェクト・クラスの構成」ウィンドウが表示されます。
2. ユーザー・エントリ用にオブジェクト・クラスを追加する手順は、次のとおりです。
   a. 「ユーザー・オブジェクト・クラスの構成」ウィンドウで「**オブジェクト・クラスの追加**」を選択します。「すべてのオブジェクト・クラス」ウィンドウが表示されます。
   b. 情報を追加するオブジェクト・クラスを選択し、「**追加**」を選択します。「ユーザー・オブジェクト・クラスの構成」ウィンドウに戻ります。選択したオブジェクト・クラスがユーザー・エントリ用のオブジェクト・クラスとして表示されます。
   c. さらにオブジェクト・クラスを追加する場合は、前述の手順を繰り返します。次の手順に進む場合は、「**次へ**」を選択して「ユーザー属性の構成」ウィンドウを表示します。
3. 「ユーザー属性の構成」ウィンドウには、31-14 ページの手順 2 で指定したオブジェクト・クラスの属性のすべてではなく、一部が表示されます。これらのオブジェクト・クラスに属する属性は他にもあります。次の手順を実行して、必要に応じてその他の属性を追加できます。属性の表示方法の変更および属性の削除も実行できます。

   ユーザー・エントリに属性を追加する手順は、次のとおりです。

   a. 「ユーザー属性の構成」ウィンドウで「**新規属性の追加**」を選択します。「新規属性の追加」ウィンドウが表示されます。
   b. 「新規属性の追加」ウィンドウのフィールドに値を入力します。詳細は、C-41 ページの表 C-44 を参照してください。
   c. 「**完了**」を選択します。「ユーザー属性の構成」ウィンドウに戻ります。選択した属性が「属性構成」リストに示されます。
   d. さらに属性を追加する場合は、前述の手順を繰り返します。

属性の表示を変更する手順は、次のとおりです。

a. 「ユーザー属性の構成」ウィンドウの「**ディレクトリ属性名**」列で変更対象の属性を選択した後、「**編集**」を選択します。「属性の編集」ウィンドウが表示されます。

b. 「属性の編集」ウィンドウのフィールドに値を入力します。これらのフィールドの説明は、C-42 ページの表 C-45 を参照してください。

c. 「**完了**」を選択します。「ユーザー属性の構成」ウィンドウに戻ります。構成した属性が「ディレクトリ属性名」リストに反映されています。

d. さらに属性を構成または変更する場合は、前述の手順を繰り返します。

ユーザー・エントリの属性を削除する場合は、「ユーザー属性の構成」ウィンドウの「**ディレクトリ属性名**」リストから構成対象の属性を選択した後、「**削除**」を選択します。

4. カテゴリの表示をカスタマイズする場合は、「ユーザー属性の構成」ウィンドウで「**次へ**」を選択して「属性カテゴリの構成」ウィンドウを表示します。このウィンドウには、既存のカテゴリ、ユーザーに対して表示される名前および各カテゴリの表示順序を示す表が表示されます。

   a. 新しいカテゴリを追加する場合は、「**作成**」を選択します。「作成」ウィンドウが表示されます。「**UI ラベル**」フィールドに、インタフェースに表示するカテゴリの名前を入力します。

   b. カテゴリの表示名を変更する場合は、「**UI ラベル**」列で、変更対象の各属性のフィールドを編集します。

   c. カテゴリの表示順序を設定する場合は、「**順序**」を選択します。「順序」ウィンドウには、指定した各種カテゴリが表示されます。上下の矢印を使用して、目的とする順序になるようにカテゴリを移動します。

   d. カテゴリごとに属性の表示順序を設定する場合は、カテゴリを選択した後、「**編集**」を選択します。「順序」ウィンドウの矢印ボタンを使用して、属性の表示順序を設定するか、属性を削除して表示されないようにします。

   e. カテゴリを削除する場合は、カテゴリを選択した後、「**削除**」を選択します。

   属性カテゴリの構成が完了したら、「**次へ**」を選択して「検索表列の構成」ウィンドウを表示します。

5. ユーザーが検索を実行すると、結果が表に示されます。その表の列の数と見出しを指定できます。検索表の列を構成する手順は、次のとおりです。

   a. 「**すべての属性**」ボックスで、検索結果を表す 1 つ以上の属性を選択します。これらの属性は、検索結果表の列見出しになります。

   b. 左右の矢印を使用して、「**選択された属性**」ボックスに属性を移動します。

c. 「**選択された属性**」ボックスの右側の上下の矢印を使用して、属性を並べ替えます。リストの最初の属性は、検索結果表の左端の列を表します。

検索結果表の構成が完了したら、「**次へ**」を選択して「ロールの構成」ウィンドウを表示します。

6. ユーザーにロールの割当てを許可するには、「**ロールを使用可能にする**」カテゴリから「ユーザー管理インタフェースでのロール割当てを使用可能にします。」を選択します。

ユーザーが他のユーザーに割当て可能なロールを指定できます。

ユーザーが他のユーザーに割当て可能なロールを追加する手順は、次のとおりです。

a. 「**ロールの追加**」を選択して「検索と選択 : ロール」ウィンドウを表示します。

b. 追加する管理者グループの名前の最初の数文字を「**次の文字で始まるグループ名**」フィールドに入力します。

c. 検索結果から追加対象の管理者グループの名前を選択した後、「**選択**」を選択します。「ロールの構成」ウィンドウに戻ります。選択した管理者グループが「ロール」リストに示されます。

ロールを削除するには、表からロールを選択した後、「**削除**」を選択します。

7. ユーザー・エントリの構成が完了したら、「**終了**」を選択します。

Oracle Internet Directory セルフ・サービス・コンソールを使用したユーザー・エントリの作成

ユーザー・エントリを作成する手順は、次のとおりです。

1. 「**ディレクトリ**」タブを選択し、「**ユーザー・エントリ**」を選択します。
2. 「**作成**」を選択して「ユーザーの作成」ウィンドウを表示します。
3. 「ユーザーの作成」ウィンドウの一部のセクションはユーザー環境に固有で、その他のセクションは Oracle Internet Directory セルフ・サービス・コンソールに必須です。後者のセクションは、次のとおりです。

- **ロール割当て** : ユーザーに 1 つ以上のロールを割り当てることができます。
- **リソース・アクセス情報** : Oracle Forms と Oracle Reports 固有のリソースへのアクセス権をユーザーに付与できます。

ユーザーの環境に固有のフィールドに値を入力します。

Oracle Internet Directory セルフ・サービス・コンソールに必要なフィールドに値を入力する手順は、次のとおりです。

「**ロール割当て**」セクションの「**選択**」列で、ユーザーに割り当てるロールを選択します。

「**リソース・アクセス情報**」の「**選択**」列で、ユーザーにアクセス権を付与するリソースを選択します。リソース・アクセス情報が指定されていない場合は、作成できます。この手順は、次のとおりです。

a. 「**リソース・アクセス情報**」セクションで、「**作成**」を作成します。「リソースの作成」ウィンドウが表示されます。

b. 「**リソース名**」フィールドで、リソース名、またはコンポーネントによってアクセスされるサービス名を指定します。

c. 「**リソース・タイプ**」リストで、アクセスされるリソースのタイプを選択します。デフォルトのオプションは次のとおりです。

* **OracleDB**: Oracle9*i* データベース・サーバー
* **ExpressPDS**: Oracle Express のトランスポータブル・データ・ソース
* **JDBCPDS**: Java Database Connectivity のトランスポータブル・データ・ソース

その他のリソース・タイプは、管理者が指定したとおりに、このリストに表示されます。

d. 「**次へ**」を選択します。リソース・アクセス情報ウィンドウが表示されます。

e. リソース・アクセス情報ウィンドウで、適切な情報を入力します。

f. すべての情報を正しく入力したことを確認し、「**送信**」を選択します。

Oracle Internet Directory セルフ・サービス・コンソールを使用したユーザー・エントリの変更

ユーザー・エントリを変更する手順は、次のとおりです。

1. 「**ディレクトリ**」タブを選択し、エントリを変更するユーザーを検索します。

2. エントリを変更するユーザーを選択した後、「**編集**」を選択して「ユーザーの編集」ウィンドウを表示します。

3. 「ユーザーの編集」ウィンドウでは、一部のセクションは Oracle Internet Directory セルフ・サービス・コンソールに必須であり、他のセクションは、ご使用の環境に対して固有です。Oracle Internet Directory セルフ・サービス・コンソールに必須のセクションは、次のとおりです。

- **ロール割当て**: ユーザーに 1 つ以上のロールを割り当てることができます。
- **リソース・アクセス情報**: リソース・アクセス情報を作成、変更および削除できます。
- **既存のグループ・メンバーシップ**: このユーザーがすでにメンバーであるグループを表示します。

- **編集履歴**: ユーザー・エントリの作成者または変更者およびエントリの作成日また変更日を表示します。

Oracle Internet Directory セルフ・サービス・コンソールに必要なフィールドに値を入力する手順は、次のとおりです。

a. 「**ロール割当て**」セクションの「**選択**」列で、ユーザーに割り当てるロールを選択します。

b. 「**リソース・アクセス情報**」の「**選択**」列で、ユーザーにアクセス権を付与するリソースを選択します。

Oracle Internet Directory セルフ・サービス・コンソールに必須のフィールドに情報を入力した後、ご使用の環境に固有のフィールドにも情報を入力します。

4. 「**送信**」を選択します。

Oracle Internet Directory セルフ・サービス・コンソールを使用したユーザー・エントリの削除

ユーザー・エントリを削除する手順は、次のとおりです。

1. 「**ディレクトリ**」タブを選択し、エントリを削除するユーザーを検索します。
2. エントリを削除するユーザーを選択した後、「**削除**」を選択します。

Oracle Internet Directory セルフ・サービス・コンソールを使用したユーザーへの権限の割当て

ユーザーに次の権限を付与できます。

- ユーザーおよびグループの作成、編集および削除
- 他のユーザーおよびグループへの権限の付与

ユーザーの権限を取り消すこともできます。

ユーザーに権限を割り当てる手順は、次のとおりです。

1. 「**ディレクトリ**」タブを選択し、権限を割り当てるユーザーのエントリを検索します。
2. 検索結果リストから、権限を割り当てるユーザーを選択した後、「**権限の割当て**」を選択します。「ユーザーへの権限の割当て」ウィンドウに権限が一覧表示されます。
3. ユーザーに割り当てる権限を選択します。詳細は、C-43 ページの表 C-46 を参照してください。
4. 「**送信**」を選択するか、別のユーザーに権限を付与する場合は「**取消**」を選択して前述の手順を繰り返します。

Oracle Internet Directory セルフ・サービス・コンソールを使用したユーザー・パスワードの変更

必要なアクセス権を所有している場合は、他のユーザーのパスワードも変更できます。他のユーザーのパスワードを変更する手順は、次のとおりです。

1. 「**ディレクトリ**」タブを選択した後、「**ユーザー**」を選択します。
2. パスワードを変更するユーザーのエントリを検索します。
3. 検索結果からユーザー・エントリを選択した後、「**編集**」を選択して「ユーザーの編集」ウィンドウを表示します。
4. 「**基本情報**」セクションで、ユーザーに割り当てるパスワードを入力および確認します。
5. 「**送信**」を選択します。

注意： ユーザー・エントリを編集する権限がない場合、「編集」ボタンは表示されないため、この操作は実行できません。

Oracle Internet Directory セルフ・サービス・コンソールを使用したグループ・エントリの作成

グループ・エントリを作成する手順は、次のとおりです。

1. 「**ディレクトリ**」タブを選択した後、「**グループ**」を選択します。
2. 「**作成**」を選択します。「グループの作成」ウィンドウが表示されます。
3. 「グループの作成」ウィンドウの「**基本情報**」セクションにある「**名前**」フィールドにグループの名前を入力します。
4. 「**表示名**」フィールドにこのグループのわかりやすい名前を入力します。たとえば、**RDN** が `OracleDBCreators` の場合は、`Oracle Database Creators` などの表示名を入力します。
5. オプションとして、「**説明**」フィールドにこのグループについての簡単な説明を入力します。
6. このグループを所有者以外に表示しない場合は、「**グループの可視性**」フィールドで「**プライベート**」を選択します。所有者以外にも表示する場合は、デフォルトの「**PUBLIC**」を使用します。
7. このグループの所有者を構成します。グループの作成者は自動的にグループの所有者になります。

   このグループの所有者としてユーザーを追加する手順は、次のとおりです。

   a. 「**所有者**」セクションで「**ユーザーの追加**」を選択します。「検索と選択 : ユーザー」ウィンドウが表示されます。

b. このグループにメンバーとして追加するユーザーのエントリを検索します。

c. 「**選択**」を選択します。「グループの作成」ウィンドウに戻ります。指定したユーザーが「**所有者**」セクションに示されます。

このグループの所有者としてグループを追加する手順は、次のとおりです。

a. 「**所有者**」セクションで「**グループの追加**」を選択します。「検索と選択 : グループ」ウィンドウが表示されます。

b. グループの所有者として追加するグループのエントリを検索します。

c. 「**選択**」を選択します。「グループの作成」ウィンドウに戻ります。指定したグループが「**所有者**」セクションに示されます。

このグループの所有者からユーザーまたはグループを削除する場合は、ユーザーまたはグループを選択した後、「**削除**」を選択します。

8. このグループのメンバーを構成します。

このグループのメンバーとしてユーザーを追加する手順は、次のとおりです。

a. 「**メンバー**」セクションで「**ユーザーの追加**」を選択します。「検索と選択」ウィンドウが表示されます。

b. このグループのメンバーとして指定するユーザーのエントリを検索します。

c. 「**選択**」を選択します。「グループの作成」ウィンドウに戻ります。指定したユーザーが「**メンバー**」セクションに示されます。

このグループからユーザーを削除する場合は、「**メンバー**」セクションでユーザー名を選択した後、「**削除**」を選択します。

このグループのメンバーとしてグループを追加する手順は、次のとおりです。

a. 「**メンバー**」セクションで「**グループの追加**」を選択します。「検索と選択」ウィンドウが表示されます。

b. このグループのメンバーとして指定するグループのエントリを検索し、「**選択**」を選択します。「グループの作成」ウィンドウに戻ります。指定したグループが「**メンバー**」セクションに示されます。

9. このグループにはロールを割り当てることができます。

このグループに割り当てるロールを指定するには、「**ロール割当て**」セクションの「**選択**」列で、このグループに割り当てるロールを選択します。

このグループからロールを削除するには、「**ロール割当て**」セクションの「**選択**」列で、このグループから削除するロールを選択解除します。

Oracle Internet Directory セルフ・サービス・コンソールを使用したグループ・エントリの変更

グループ・エントリを変更する手順は、次のとおりです。

1. 「**ディレクトリ**」タブを選択し、エントリを変更するグループを検索します。
2. 検索結果から、変更するグループ・エントリを選択します。
3. 「**編集**」を選択します。「グループの編集」ウィンドウが表示されます。
4. 31-19 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用したグループ・エントリの作成」で説明したとおりにフィールドを変更します。
5. 「**送信**」を選択します。

Oracle Internet Directory セルフ・サービス・コンソールを使用したグループ・エントリの削除

グループ・エントリを削除する手順は、次のとおりです。

1. 「**ディレクトリ**」タブを選択し、エントリを削除するグループを検索します。
2. 検索結果から、エントリを削除するグループを選択します。
3. 「**削除**」を選択します。

Oracle Internet Directory セルフ・サービス・コンソールを使用したグループへの権限の割当て

次の 1 つ以上の権限をグループに付与できます。

- 新しいユーザーおよびグループの作成、編集および削除
- ユーザーおよびその他のグループへの権限の割当て

グループの権限を取り消すこともできます。

グループに権限を割り当てる手順は、次のとおりです。

1. 「**ディレクトリ**」タブを選択した後、「**グループ**」を選択します。
2. 権限を割り当てるグループのエントリを検索します。
3. 検索結果から権限を割り当てるグループを選択します。
4. 「**権限の割当て**」を選択します。「グループへの権限の割当て」ウィンドウに権限が一覧表示されます。
5. 「グループへの権限の割当て」ウィンドウで、グループに割り当てる権限を選択します。詳細は、C-43 ページの表 C-46 を参照してください。

6. 「**送信**」を選択するか、別のユーザーに権限を付与する場合は「**他のグループを指定してください。**」を選択して前述の手順を繰り返します。

サービス・プロパティの変更

サービスの表示名およびネットワーク・アドレスを変更できます。この手順は、次のとおりです。

1. 「**ディレクトリ**」タブを選択した後、「**サービス**」を選択します。使用可能なサービスを示す「サービス」ウィンドウが表示されます。
2. 「サービス」ウィンドウで、プロパティを変更するサービスを選択します。
3. 「**サービスの編集**」を選択します。「サービスの編集」ウィンドウが表示されます。
4. 「サービスの編集」ウィンドウの変更対象フィールドに値を入力します。
5. 「**送信**」を選択します。

サービス受信者に関するサブスクリプション情報の変更

サブスクリプション・リストに対しては、ユーザーの追加および削除を実行できます。また、受信の開始日または終了日も変更できます。

サブスクリプション情報を変更する手順は、次のとおりです。

1. 「**ディレクトリ**」タブを選択した後、「**サービス**」を選択します。使用可能なサービスを示す「サービス」ウィンドウが表示されます。
2. 「サービス」ウィンドウで、プロパティを変更するサービスを選択します。
3. 「**サブスクリプションの編集**」を選択します。「サブスクリプションの編集」ウィンドウが表示されます。
4. サブスクリプション情報を変更するサービス受信者を選択します。
5. 「**編集**」を選択します。「サービス受信者の編集」ウィンドウが表示されます。
6. 「サービス受信者の編集」ウィンドウで変更を行います。
   a. 「**サービス受信者**」フィールドには受信者の名前を指定します。
   b. 「**開始日**」フィールドには、受信者がサービスを使用開始できる日付を指定し、「**終了日**」フィールドには、使用を終了する日付を指定します。

   サブスクリプション・リストにユーザーを追加する手順は、次のとおりです。

   a. 「**ユーザーの追加**」を選択します。「検索と選択」ウィンドウが表示されます。
   b. 「検索と選択」ウィンドウでリストに追加するユーザーを検索します。
   c. 検索結果から、追加対象のユーザーを選択した後、「**選択**」を選択します。「新規サービス受信者の追加」ウィンドウに戻ります。追加したユーザーがリストに表示されます。

サブスクリプション・リストからユーザーを削除する場合は、ユーザーを選択した後、「**削除**」を選択します。

7. 「サービス受信者の編集」ウィンドウでの変更が完了したら、「**送信**」を選択します。「サブスクリプションの編集」ウィンドウに戻ります。
8. 「**送信**」を選択します。

アカウントの管理

ユーザー・アカウントは、ロック解除、有効化または無効化できます。

ユーザー・アカウントのロック解除 ユーザーのアカウントがロックされている場合（指定された期限内にパスワードを変更しなかった場合など）は、ユーザー・パスワードを再設定せずにロック解除できます。これによって、ユーザーに新規パスワードを明示的に知らせる必要がなくなります。かわりに、ユーザーは旧パスワードを使用してログインできます。

ユーザー・アカウントをロック解除する手順は、次のとおりです。

1. 「**ディレクトリ**」タブを選択した後、「**アカウントのロックを解除**」を選択します。ロックされているアカウントが一覧表示されます。
2. ロック解除するアカウントを選択します。
3. 「**ロック解除します**」を選択します。

ユーザー・アカウントの有効化 ユーザー・アカウントは、一時的に保留されている（無効になっている）場合、有効にできます。この手順は、次のとおりです。

1. 「**ディレクトリ**」タブを選択した後、「**アカウント**」を選択します。
2. 「**アカウントを有効化**」を選択します。無効になっているアカウントが一覧表示されます。
3. 有効にするアカウントを選択します。
4. 「**有効化**」を選択します。

ユーザー・アカウントの無効化 ユーザー・アカウントは、一時的に保留する（無効にする）ことができます。この手順は、次のとおりです。

1. 「**ディレクトリ**」タブを選択した後、「**アカウント**」を選択します。
2. 「**アカウントを無効化**」を選択します。有効になっているアカウントが一覧表示されます。
3. 無効にするアカウントを選択します。
4. 「**無効化**」を選択します。

リソース・タイプ情報の構成

Oracle Internet Directory セルフ・サービス・コンソールを使用して新しいリソース・タイプの情報を指定し、後でこの情報を変更または削除できます。

新しいリソース・タイプの指定 新しいリソース・タイプを指定するには、次の手順を実行します。

1. 「**構成**」タブを選択し、「**設定**」を選択します。
2. 「**リソース・タイプ情報の構成**」セクションで、「**作成**」を作成します。「リソース・タイプの作成」ウィンドウが表示されます。
3. 「リソース・タイプの作成」ウィンドウで、適切なフィールドに値を入力します。詳細は、C-47 ページの表 C-49 を参照してください。
4. 「リソース・タイプの作成」ウィンドウで適切な情報をすべて入力したら、「**送信**」を選択します。「設定」ウィンドウに戻ります。指定したリソース・タイプが、「**リソース・タイプ名**」列の下に表示されます。

> **関連項目：** リソース・タイプ情報の詳細は、2-33 ページの「リソース情報」を参照してください。

デフォルトのリソース・アクセス情報の構成

ユーザーが多数の場合、ユーザー・エントリごとにリソース・アクセス情報を指定するかわりに、すべてのユーザーが自動的に継承し、共通に使用されるリソースを定義できます。この手順は、次のとおりです。

1. 「**構成**」タブを選択し、「**設定**」を選択します。
2. 「**デフォルトのリソース・アクセス情報**」セクションで、「**作成**」を作成します。「リソースの作成」ウィンドウが表示されます。
3. 「**リソース名**」フィールドで、リソース名、またはコンポーネントによってアクセスされるサービス名を指定します。
4. 「**リソース・タイプ**」リストで、アクセスされるリソースのタイプを選択します。デフォルトのオプションは次のとおりです。
   - **OracleDB**: Oracle9*i* データベース・サーバー
   - **ExpressPDS**: Oracle Express のトランスポータブル・データ・ソース
   - **JDBCPDS**: Java Database Connectivity のトランスポータブル・データ・ソース

   その他のリソース・タイプは、管理者が指定したとおりに、このリストに表示されます。
5. 「**次へ**」を選択します。リソース・アクセス情報ウィンドウが表示されます。フィールドに適切な情報を入力します。

6. すべての情報を正しく入力したことを確認し、「**送信**」を選択します。「設定」ウィンドウに戻ります。指定したデフォルトのリソース・アクセス情報が、「**リソース名**」列に表示されます。

   関連項目： リソース・アクセス情報の詳細は、2-33 ページの「リソース情報」を参照してください。

第 VII 部

Oracle Directory Integration and Provisioning Platform

第 VII 部では、Oracle Directory Integration and Provisioning Platform の概念、コンポーネントおよびアーキテクチャについて説明し、複数ディレクトリを Oracle Internet Directory と同期化するための Oracle Directory Integration and Provisioning platform の構成方法および使用方法について説明します。第 VII 部は次の各章で構成されています。

32

Oracle Directory Integration and Provisioning Platform の概要とコンポーネント

この章では、Oracle Directory Integration and Provisioning Platform の概要とそのコンポーネント、構造および管理ツールについて説明します。

この章では、次の項目について説明します。

Oracle Directory Integration and Provisioning Platform の概要

サード・パーティの LDAP ディレクトリを含め、ディレクトリおよびアプリケーションを Oracle Internet Directory に統合することにより、管理作業に必要な時間とコストを削減できます。これは、Oracle Identity Management のコンポーネントである Oracle Directory Integration and Provisioning Platform によって実現します。たとえば、企業には次のようなニーズがあります。

- Oracle Human Resources と Oracle Internet Directory で従業員レコードの整合性を維持すること。Oracle Directory Integration and Provisioning Platform は Oracle Directory Synchronization Service によって、この同期化を行います。
- 変更が Oracle Internet Directory に適用されるたびに、OracleAS Portal などの LDAP 対応アプリケーションに通知されること。Oracle Directory Integration and Provisioning Platform は Oracle Directory Provisioning Integration Service によって、この通知を行います。

統合処理全体を通して、Oracle Directory Integration and Provisioning Platform は、アプリケーションとその他のディレクトリが確実な方法で必要な情報を受け取ったり提供することを保証します。

Oracle Directory Integration and Provisioning Platform は、Microsoft Active Directory や SunONE Directory Server など、様々なディレクトリに統合することができます。たとえば、Oracle Application Server 環境では、Oracle コンポーネントへのアクセスは、Oracle Internet Directory に格納されているデータに基づいて行います。この環境では、企業の中央ディレクトリとして Microsoft Active Directory も使用できます。これらのディレクトリのユーザーが Oracle コンポーネントにアクセスできるのは、Oracle Directory Integration and Provisioning Platform が、Microsoft Active Directory 内のデータを、Oracle Internet Directory 内のデータと同期化できるためです。

関連項目：

- 第 39 章「Oracle Human Resources との同期化」
- 第 42 章「SunONE（iPlanet）Directory Server との統合」
- 第 43 章「Microsoft Windows 環境との統合」

32-3 ページの図 32-1 に、Oracle Directory Integration and Provisioning Platform の配置例を示します。

図 32-1 Oracle Directory Integration and Provisioning Platform 環境の例

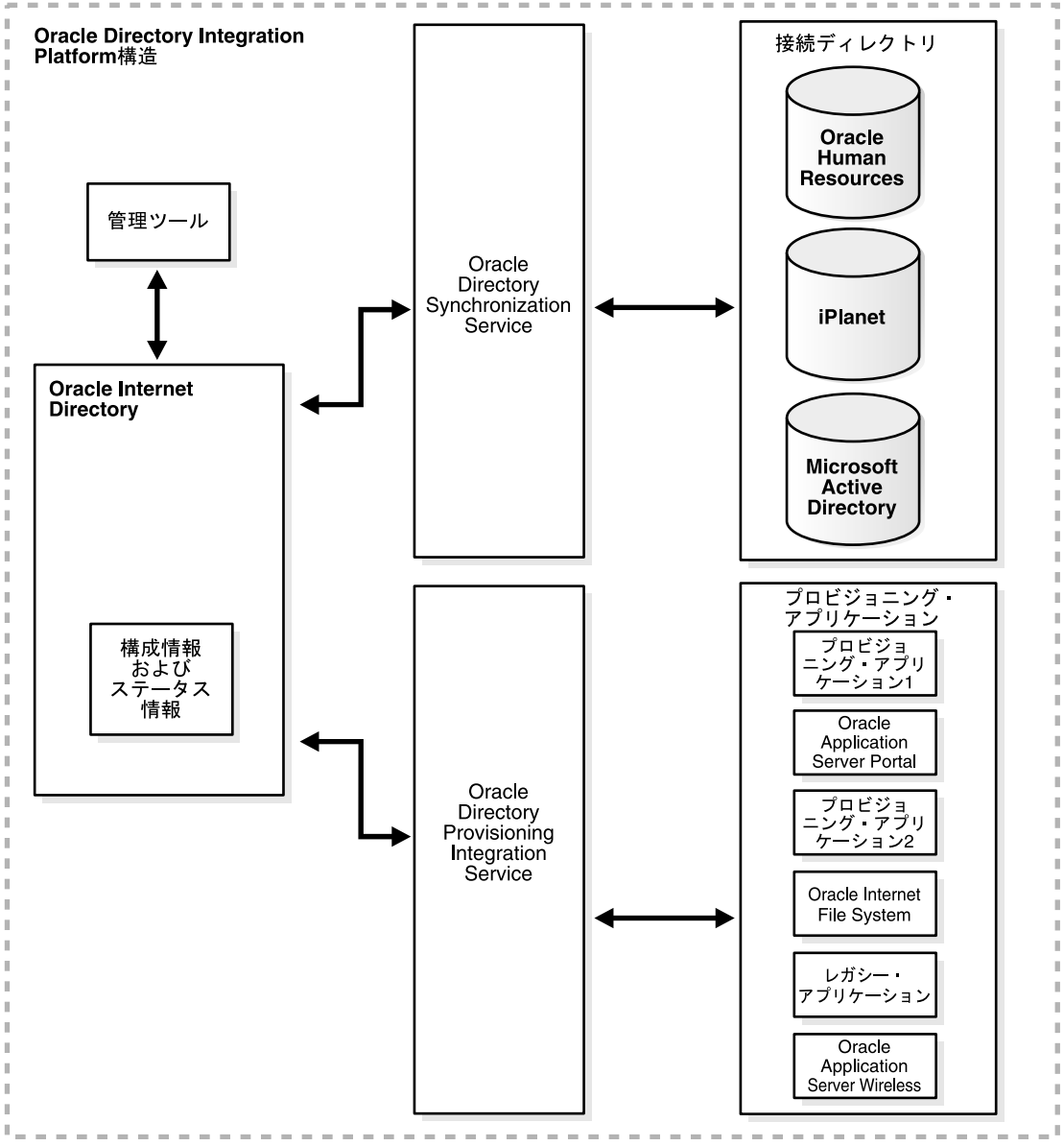


図 32-1 の例では、Oracle Internet Directory は Oracle Directory Synchronization Service によって接続ディレクトリと同期化されます。この例での接続ディレクトリは、Oracle Human Resources、SunONE Directory Server および Microsoft Active Directory です。同様に Oracle Internet Directory 内の変更は、Oracle Directory Provisioning Integration Service を使用して各種のアプリケーションに送信されます。この例では、プロビジョニング・アプリケーションとしては OracleAS Portal、Oracle Content Management Software Development Kit、Oracle Application Server Wireless、任意のプロビジョニング・アプリケーション、レガシー・アプリケーションなどがあります。

同期、プロビジョニングおよび両者の相違点

同期が扱うのは、アプリケーションではなくディレクトリです。同期では、Oracle Internet Directory と他の接続ディレクトリの両方に存在するエントリと属性の一貫性を確保します。

プロビジョニングが扱うのは、アプリケーションです。プロビジョニングは、アプリケーションで追跡が必要なユーザーやグループのエントリまたは属性への変更を、アプリケーションに通知します。

この項では、次の項目について説明します。

- 同期
- プロビジョニング
- 同期とプロビジョニングの相違点

同期

同期によって、Oracle Internet Directory と接続ディレクトリの間で変更を調整できます。すべてのディレクトリが最新のデータのみを使用し、提供するためには、その他の接続ディレクトリでの変更がすべて各ディレクトリに伝達される必要があります。同期は、プロビジョニングによって更新されたデータも含めて、ディレクトリ情報に対する変更の一貫性を確保します。

サード・パーティのディレクトリを Oracle Internet Directory に接続する場合は、特定のディレクトリ用に同期プロファイルを作成します。このプロファイルによって、Oracle Internet Directory と接続ディレクトリとの間で交換される通知の形式と内容が指定されます。

プロビジョニング

プロビジョニングによって、たとえば、ユーザーまたはグループに関する情報への変更をアプリケーションに確実に通知できます。このような変更は、プロセスに対するユーザー・アクセスをアプリケーションで許可するかどうかおよび使用できるリソースに影響を与えます。

プロビジョニングを使用するのは、次のアプリケーションを設計またはインストールする場合です。

- ディレクトリを維持しないアプリケーション
- LDAP 対応のアプリケーション
- リソースへのアクセスを認可ユーザーのみに限定するアプリケーション

プロビジョニング対象のアプリケーションをインストールする場合、プロビジョニング・サブスクリプション・ツールを使用して、そのためのプロビジョニング統合プロファイルを作成する必要があります。

関連項目： A-125 ページの「プロビジョニング・サブスクリプション・ツール （oidprovtool）の構文」

同期とプロビジョニングの相違点

同期とプロビジョニングには、表 32-1 のとおり、操作に重要な相違があります。

表 32-1 ディレクトリ同期とプロビジョニング統合の相違点

	ディレクトリ同期	プロビジョニング統合
アクションの時期	アプリケーションの配置時。ディレクトリ同期は、Oracle Internet Directory との同期を必要とする接続ディレクトリを対象としています。	アプリケーションの設計時。プロビジョニング統合は、LDAP 対応アプリケーションの開発を担当するアプリケーション設計者を対象としています。
通信方向	一方向または双方向（Oracle Internet Directory から接続ディレクトリへまたはその逆方向）、あるいは両方向	双方向（Oracle Internet Directory からプロビジョニング・アプリケーションへ、およびプロジェクト・アプリケーションから Oracle Internet Directory へ）
データの種類	ディレクトリ内のあらゆるデータ	プロビジョニング対象のユーザーとグループに制限
例	Oracle Human Resources SunONE Directory Server Microsoft Active Directory	OracleAS Portal

Oracle Directory Synchronization Service

Oracle Directory Integration and Provisioning Platform 環境における接続ディレクトリの内容は、Oracle Directory Synchronization Service を介して Oracle Internet Directory と同期されます。

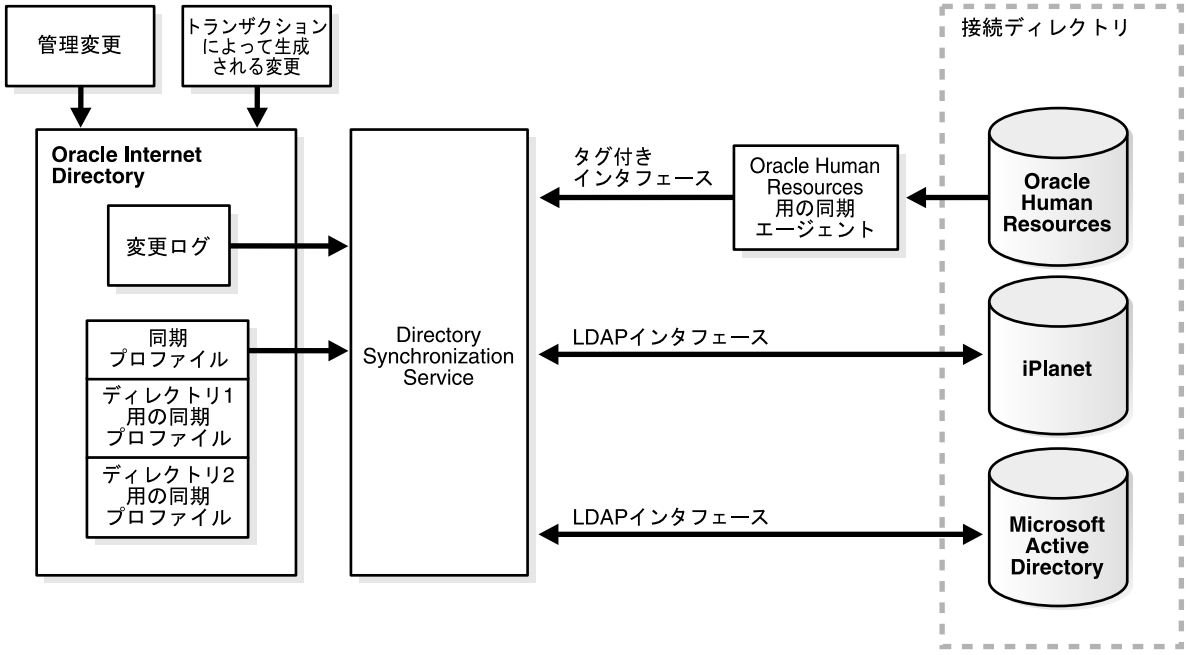
Oracle Application Server コンポーネントの場合、Oracle Internet Directory はすべての情報の中央ディレクトリであり、他のすべてのディレクトリと同期しています。この同期には、次の 2 つの方向があります。

- 一方向 : 一部の接続ディレクトリは、Oracle Internet Directory に変更を提供するのみで、変更を受け取ることがない場合があります。たとえば、Oracle Human Resources の場合、プライマリ・リポジトリと従業員情報の真のソースの場合がこれに該当します。
- 双方向 : Oracle Internet Directory での変更を接続ディレクトリにエクスポートでき、接続ディレクトリでの変更を Oracle Internet Directory にインポートできます。

同期サービスでは、特定の属性を対象とする（または無視する）ことができます。たとえば、Oracle Human Resources 内の従業員バッジ番号の属性は、Oracle Internet Directory、その接続ディレクトリまたはクライアント・アプリケーションには関係ありません。同期は不要です。ただし、従業員識別番号はこれらのコンポーネントとも関係があるため、同期が必要です。

図 32-2 に、配置例の Oracle Directory Synchronization Service 内のコンポーネント間の相互作用を示します。

図 32-2 Oracle Directory Synchronization Service の相互作用



このような同期アクティビティのすべてをトリガーする中心的なメカニズムが、Oracle Internet Directory の変更ログです。Oracle Internet Directory など、接続ディレクトリへの変更ごとに、変更ログに 1 つ以上のエントリが追加されます。Oracle Directory Synchronization Service の動作は次のとおりです。

- 変更ログを監視します。
- 変更が 1 つ以上の同期プロファイルに対応している場合は、常にアクションを実行します。
- 個別のプロファイルがログに記録された変更に対応している他の接続ディレクトリすべてに対し、適切な変更を実現します。接続ディレクトリには、リレーショナル・データベース、Oracle Human Resources、Microsoft Active Directory、SunONE Directory Server などが含まれます。接続ディレクトリが要求するインタフェースと形式を使用することで、これらの変更を実現します。Oracle Directory Integration and Provisioning Platform コネクタを介した同期によって、Oracle Internet Directory クライアントに必要なすべての情報について、Oracle Internet Directory が最新の状態に保持されます。

Oracle Directory Provisioning Integration Service

Oracle Directory Provisioning Integration Service は、ユーザーまたはグループ情報などの変更が各プロビジョニング・アプリケーションに通知されることを保証します。これは、プロビジョニング統合プロファイルに含まれている情報に基づいて行われます。各プロビジョニング・プロファイルの役割は、次のとおりです。

- そのプロファイルを適用するアプリケーションと組織を一意に識別します。
- アプリケーションに通知する必要があるユーザー、グループ、操作などを指定します。

プロファイルは、アプリケーションのインストール時に、プロビジョニング・サブスクリプション・ツールを使用して作成する必要があります。

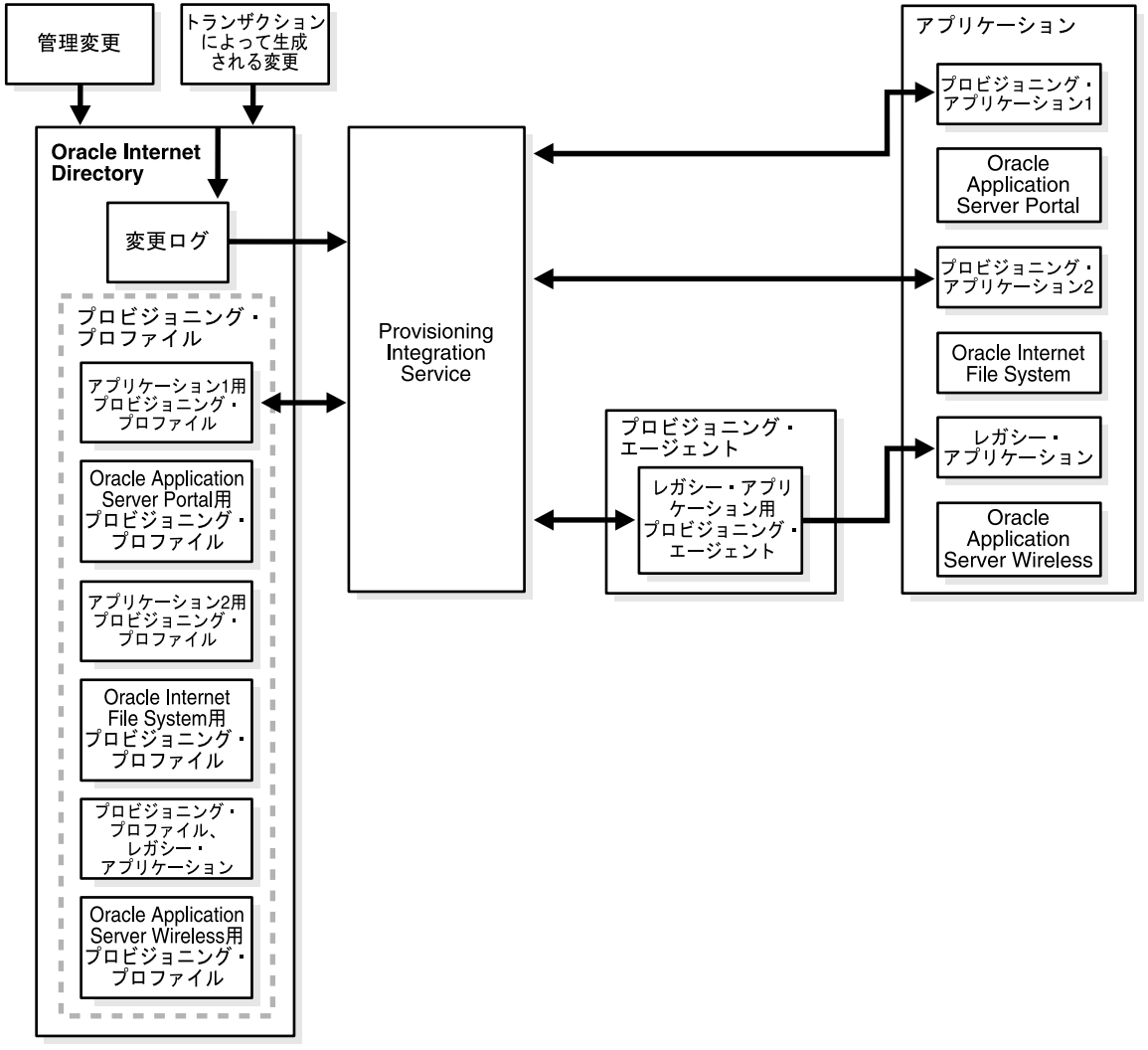
> **関連項目：** プロビジョニング・サブスクリプション・ツールの詳細は、A-125 ページの「プロビジョニング・サブスクリプション・ツール（oidprovtool）の構文」を参照してください。

Oracle Internet Directory での変更がアプリケーションのプロビジョニング・プロファイルに指定されているものと一致すると、Oracle Directory Provisioning Integration Service は、そのアプリケーションに関連データを送信します。

注意： レガシー・アプリケーション（Oracle Directory Provisioning Integration Service のインストール前に稼働状態であったアプリケーション）は、インストール時に通常の方法ではサブスクライブされません。レガシー・アプリケーションを使用してプロビジョニング情報を受信できるようにするには、プロビジョニング・プロファイルに加えて、**プロビジョニング・エージェント**を開発する必要があります。このエージェントは、Oracle Internet Directory からの関連データをレガシー・アプリケーションに必要な正確な形式に変換する必要があります。

図 32-3 に、Oracle Directory Provisioning Integration Service 環境でのコンポーネント間の相互作用を、レガシー・アプリケーションに使用するプロビジョニング・エージェントの特別なケースも含めて示します。

図 32-3 Oracle Directory Provisioning Integration Service の相互作用



Oracle Directory Integration and Provisioning Server

Oracle Directory Integration and Provisioning Server は、Oracle Directory Synchronization Service と Oracle Directory Provisioning Integration Service で構成される共有サーバー・プロセスです。次の機能が実行されます。

- Oracle Directory Synchronization Service の場合は、次のようになります。
  - スケジューリング ― 事前定義されたスケジュールに基づいて同期プロファイルを処理
  - マッピング ― 接続ディレクトリと Oracle Internet Directory の間のデータ変換ルールを実行
  - データ伝播 ― コネクタを使用して接続ディレクトリとデータを交換
  - エラー処理
- Oracle Directory Provisioning Integration Service の場合は、次のようになります。
  - スケジューリング ― 事前定義されたスケジュールに基づいてプロビジョニング・プロファイルを処理
  - イベント通知 ― Oracle Internet Directory に格納されているユーザー・データまたはグループ・データに関連した変更をアプリケーションに通知
  - エラー処理

関連項目： 第 35 章「Oracle Directory Integration and Provisioning Server の管理」

ディレクトリ統合ツールキット

ディレクトリ統合ツールキットによって、サード・パーティのベンダーと開発者は、そのソリューションを Oracle Directory Integration and Provisioning Platform 環境に統合できます。このようなベンダーには、メタディレクトリやプロビジョニング・ソリューションのプロバイダも含まれます。ツールキットによって、Oracle のテクノロジに基づいた（または使用した）製品のアプリケーション・ベンダーは、ユーザーやグループのプロビジョニングを Oracle Internet Directory に統合できます。

ツールキットには、次のインタフェース、ツールおよびプロシージャが組み込まれています。

- クライアントによる Oracle Internet Directory 変更にアクセスするためのインタフェース。
  - IETF 規格の変更ログ・インタフェース
  - Oracle 独自の変更ログ・インタフェース

  - スケジューリングまたはデータ・マッピング用に、Oracle Internet Directory でディレクトリ統合コネクタを登録または変更するためのインタフェース（LDIF ファイル構成を使用してデータを追加および変更するために、Oracle Directory Manager またはコマンドライン・ツールを使用）

- Oracle Directory Integration and Provisioning Platform 環境への接続ディレクトリのブートストラップのためのツールおよびプロシージャ。これらにより、次のことが可能になります。
  - LDIF ファイルから Oracle Internet Directory へのデータのバルク・インポート
  - Oracle Internet Directory から LDIF ファイルへのデータのバルク・エクスポート
- Oracle Internet Directory のユーザーおよびグループのプロビジョニング・イベント、つまり変更をサブスクライブするためのインタフェース。
- Oracle Directory Provisioning Integration Service によって送信された変更をコンシュームするためのインタフェース。

管理ツールと監視ツール

この項では、Oracle Directory Integration and Provisioning Platform の管理に使用できるツールについて説明します。次の項目について説明します。

- Oracle Directory Manager
- OID 制御と OID モニター
- Directory Integration and Provisioning Assistant
- Oracle Enterprise Manager

Oracle Directory Manager

Oracle Directory Manager は、Java ベースの Graphical User Interface（GUI）ツールで、次の方法で Oracle Directory Integration and Provisioning Platform を管理できます。

- 同期用のディレクトリ統合プロファイルの作成、変更および削除
- 同期用ディレクトリ統合プロファイルの同期の監視
- すべての Oracle Directory Integration and Provisioning Server インスタンスの状態の監視

関連項目：

- 第 4 章「ディレクトリ管理ツール」
- 第 35 章「Oracle Directory Integration and Provisioning Server の管理」

OID 制御と OID モニター

OID 制御と OID モニターは、Oracle Directory Integration and Provisioning Server の起動、停止および監視のために使用します。

Oracle Internet Directory では、OID 制御と OID モニターを使用して、Oracle ディレクトリ・サーバーまたは Oracle Directory Integration and Provisioning Server のいずれかがインストールされている *ORACLE_HOME* で、Directory Integration and Provisioning Server を制御できます。

Oracle Internet Directory をクライアントのみにインストールした場合は、OID 制御ユーティリティと OID モニターはインストールされません。この場合は、手動で Oracle Directory Integration and Provisioning Server を起動します。この構成でも、Oracle Directory Manager を使用して Oracle Directory Integration and Provisioning Server の状態を調べることはできます。

関連項目：

- A-6 ページの「OID 制御ユーティリティ（oidctl）の構文」
- A-4 ページの「OID モニター（oidmon）構文」
- 第 35 章「Oracle Directory Integration and Provisioning Server の管理」

Directory Integration and Provisioning Assistant

Directory Integration and Provisioning Assistant によって、Oracle Directory Integration and Provisioning Platform でのディレクトリ同期プロファイルとプロビジョニング統合プロファイルの作成、変更、削除が可能になります。また、Oracle Internet Directory を作成するためのブートストラップ・コマンドおよび情報交換以前のものと同じデータが入った接続ディレクトリも提供されます。

関連項目： A-106 ページの「Directory Integration and Provisioning Assistant」

Oracle Enterprise Manager

Oracle Enterprise Manager を使用すると、各種統合プロファイルのステータスを監視できます。この統合された包括的なシステム管理プラットフォームは、グラフィカル・コンソール、エージェント、共通サービスおよび異機種間環境をスケジューリング、監視および管理するためのツールを組み合せます。

関連項目：

- 10-17 ページの「Oracle Internet Directory サーバーの監視」（Oracle Internet Directory のプロセス監視のために Oracle Enterprise Manager を使用する方法について）
- Oracle Enterprise Manager オンライン・ヘルプ

例 : Oracle Directory Integration and Provisioning Platform の配置

この項では、MyCompany という企業内の様々なアプリケーションが Oracle Directory Integration and Provisioning Platform によって統合されている配置例を示します。

次の項目について説明します。

- 企業 MyCompany 内のコンポーネント
- 企業 MyCompany の要件
- 企業 MyCompany 内の全体的な配置
- 企業 MyCompany でのユーザーの作成とプロビジョニング
- 企業 MyCompany でのユーザー・プロパティの変更
- 企業 MyCompany でのユーザーの削除

企業 MyCompany 内のコンポーネント

この仮想の企業には、次のコンポーネントがあります。

- Oracle Human Resources システム。すべての従業員と契約社員が管理されています。
- SunONE Directory Server。特定のアプリケーションで使用されています。
- OracleAS Portal のインストール。全従業員のイントラネット・ポータルとして使用されています。
- Oracle Content Management Software Development Kit のインストール。社内の全文書の文書リポジトリとして使用されています。

企業 MyCompany の要件

企業 MyCompany の要件は次のとおりです。

- すべての従業員と契約社員を Oracle Human Resources で作成すること。作成後の情報は、企業内のすべてのアプリケーションが Oracle Internet Directory を介して共有する必要があります。
- シングル・サインオン・サービスなど、企業内のすべてのアプリケーションが、Oracle Human Resources で作成された従業員を認識できること。
- ユーザー・プロパティの変更時には、関連するすべてのアプリケーションにその変更が通知されること。
- Oracle Human Resources でユーザーが期限切れのときは、そのユーザーのすべてのアクセス権限が取り消されること。

企業 MyCompany 内の全体的な配置

図 32-4 に、様々なコンポーネントとそれらの相互関係を示します。

図 32-4 MyCompany での Oracle Directory Integration and Provisioning Platform の配置例

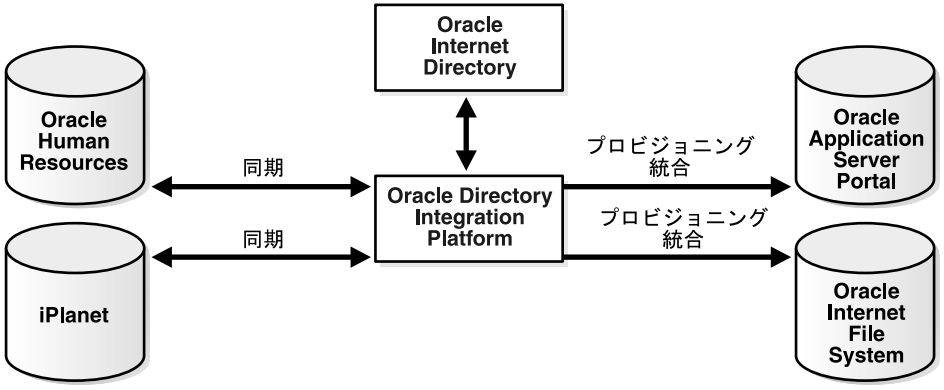


図 32-4 の例での要件は、次のとおりです。

- Oracle Internet Directory。企業の全アプリケーションの中央ユーザー・リポジトリです。
- Oracle Human Resources。すべてのユーザー関連情報に関する真のソースです。Oracle Directory Synchronization Service を使用して Oracle Internet Directory と同期しています。

- SunONE Directory Server。すでに企業内に配置されており、Oracle Directory Synchronization Service を使用して Oracle Internet Directory と同期しています。
- OracleAS Portal。Oracle Directory Provisioning Integration Service を使用して、Oracle Internet Directory 内の変更に関する通知を受け取ります。
- Oracle Content Management Software Development Kit。Oracle Directory Provisioning Integration Service を使用して、Oracle Internet Directory 内の変更に関する通知を受け取ります。

企業 MyCompany でのユーザーの作成とプロビジョニング

この例では、MyCompany という企業が、すべてのユーザーを Oracle Human Resources で作成する必要があるとします。Oracle Directory Integration and Provisioning Platform は、企業内のその他のすべてのリポジトリに新規ユーザー・レコードを伝播する必要があります。

図 32-5 に、Oracle Directory Integration and Provisioning Platform がタスクを実行する方法を示します。

図 32-5 ユーザーの作成とプロビジョニング

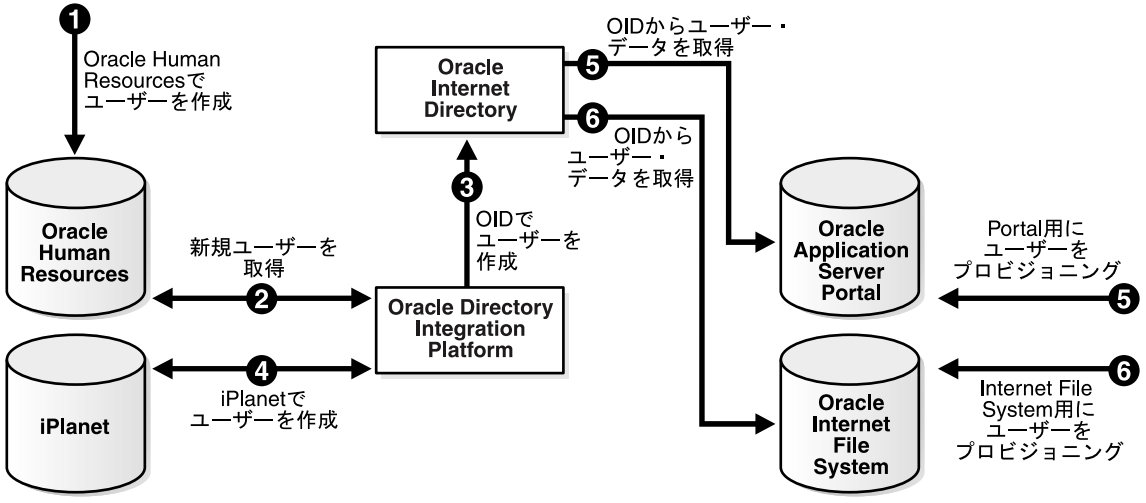


図 32-5 は、Oracle Human Resources での新規ユーザーの作成を示しています。この作成によって、そのユーザーに関するエントリが Oracle Internet Directory と SunONE Directory Server に作成されます。また、企業内に配置されている 2 つのアプリケーション、つまり OracleAS Portal および Oracle Content Management Software Development Kit にアクセスするユーザーのプロビジョニング・プロセスも示しています。ユーザーの作成とプロビジョニングは、次の方法で行われます。

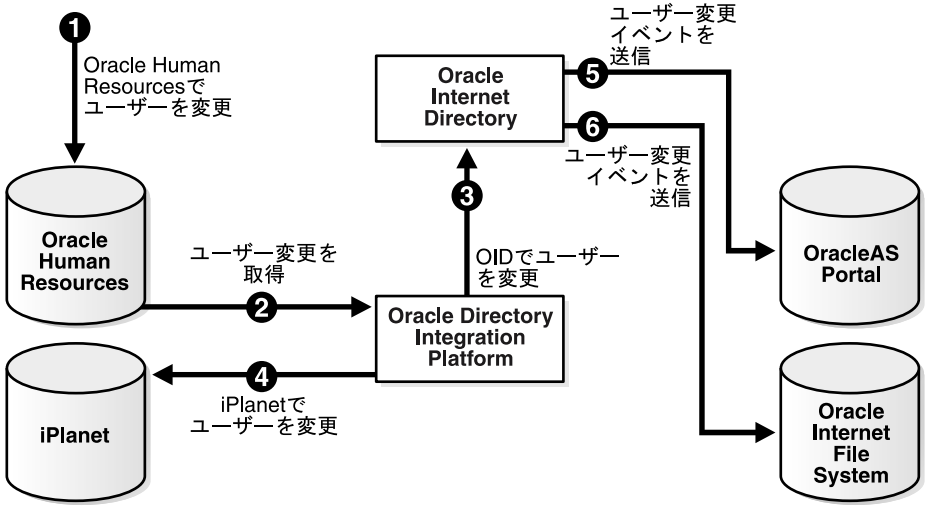
1. Oracle Human Resources 管理者は、ユーザーを Oracle Human Resources データベースに作成します。
2. Oracle Directory Integration and Provisioning Platform は Oracle Directory Synchronization Service を介して新規作成ユーザーを検出します。
3. Oracle Directory Integration and Provisioning Platform は、Oracle Directory Synchronization Service を介してユーザーのエントリを Oracle Internet Directory に作成します。
4. Oracle Directory Integration and Provisioning Platform は、Oracle Directory Synchronization Service を介して SunONE Directory Server にエントリを作成します。
5. このユーザー・エントリは Oracle Internet Directory で使用可能なため、OracleAS Portal の管理者は、OracleAS Portal のサービスを使用するユーザーをプロビジョニングできます。このタスクの実行時、OracleAS Portal ソフトウェアは、Oracle Internet Directory からユーザーの詳細を自動的に検索します。
6. Oracle Content Management Software Development Kit の管理者も、同様のプロセスを使用して、Oracle Content Management Software Development Kit サービスを使用するユーザーをプロビジョニングします。

Oracle Directory Integration and Provisioning Platform は、新規ユーザーについて OracleAS Portal または Oracle Content Management Software Development Kit に直接通知しないことに注意してください。これは、Oracle Human Resources で作成されたすべてのユーザーが、すべてのサービスへのアクセスを必要とするとはかぎらないためです。この場合の配置では、これらのサービスを使用するユーザーは、5 と 6 の手順に従って、明示的にプロビジョニングする必要があります。

企業 MyCompany でのユーザー・プロパティの変更

この例の企業 MyCompany では、ユーザー・プロパティに対するあらゆる変更が、その変更に関連するすべてのコンポーネントに伝達される必要があります。図 32-6 に、この要件を満たすために Oracle Directory Integration and Provisioning Platform が実行するアクションを示します。

図 32-6 ユーザー・プロパティの変更



このプロセスは、次のとおりです。

1. ユーザーは、最初に Oracle Human Resources で変更されます。
2. Oracle Directory Integration and Provisioning Platform は、Oracle Directory Synchronization Service を介してこれらの変更を取得します。
3. Oracle Directory Integration and Provisioning Platform は、Oracle Internet Directory 内の対応するユーザーを変更します。
4. Oracle Directory Synchronization Service は、SunONE Directory Server 内でユーザーを変更します。
5. Oracle Directory Integration and Provisioning Platform は、Oracle Directory Provisioning Integration Service を介してユーザー・プロパティの変更を OracleAS Portal に通知します。
6. Oracle Directory Integration and Provisioning Platform は、Oracle Directory Provisioning Integration Service を介してユーザー・プロパティの変更を Oracle Content Management Software Development Kit に通知します。

企業 MyCompany でのユーザーの削除

この例の企業 MyCompany では、Oracle Human Resources で削除または期限切れになったユーザーは、ディレクトリ・サービスに基づいた企業のすべてのリソースへのアクセスが自動的に拒否される必要があります。

図 32-7 に、ユーザーが削除されたときのイベントの流れを示します。

図 32-7 企業の Human Resources からのユーザーの削除

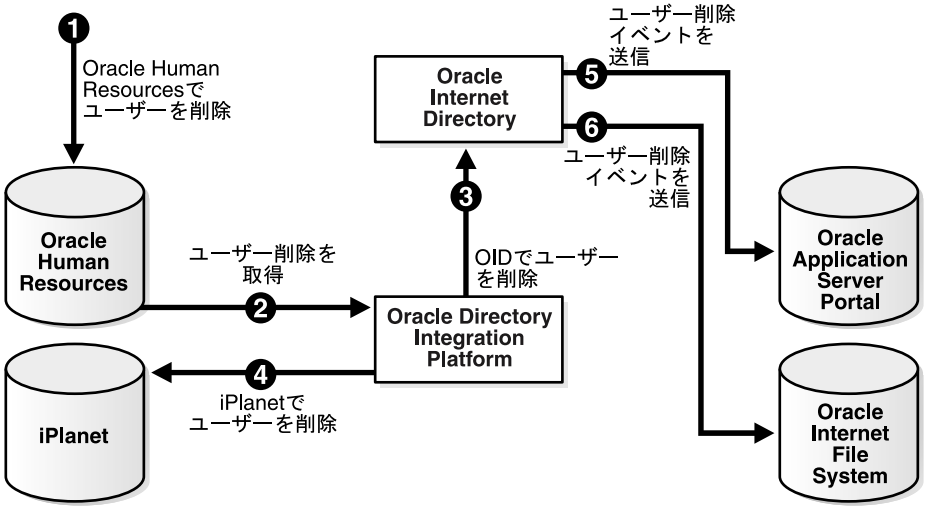


図 32-7 に、Oracle Directory Integration and Provisioning Platform がユーザーの削除を企業内のすべてのシステムに通信するプロセスを示します。このプロセスは、次のとおりです。

1. ユーザーは、最初に Oracle Human Resources で削除されます。
2. Oracle Directory Integration and Provisioning Platform は、Oracle Directory Synchronization Service を介してこれらの変更を取得します。
3. Oracle Directory Integration and Provisioning Platform は、Oracle Directory Synchronization Service を介して Oracle Internet Directory 内の対応するユーザーを削除します。
4. Oracle Directory Integration and Provisioning Platform は、Oracle Directory Synchronization Service を介して SunONE Directory Server 内でユーザーを削除します。
5. Oracle Directory Integration and Provisioning Platform は、Oracle Directory Provisioning Integration Service を介してユーザーの削除を OracleAS Portal に通知します。

6. Oracle Directory Integration and Provisioning Platform は、Oracle Directory Provisioning Integration Service を介してユーザーの削除を Oracle Content Management Software Development Kit に通知します。

前述のすべての手順が終了すると、Oracle Human Resources で削除されたユーザーは、OracleAS Portal や Oracle Content Management Software Development Kit にアクセスできなくなります。

33

Oracle Directory Synchronization Service

この章では、Oracle Internet Directory と接続ディレクトリをリンクする同期プロファイルとコネクタについて説明します。次の項目について説明します。

- コネクタとディレクトリ統合プロファイルの概要
- 同期プロファイルの管理
- Oracle Directory Integration and Provisioning Platform での同期に関するトラブルシューティング

関連項目：

- Oracle Directory Integration and Provisioning Platform の概念の説明は、第 32 章「Oracle Directory Integration and Provisioning Platform の概要とコンポーネント」を参照してください。
- 統合プロファイルのもう 1 つのタイプは、プロビジョニング統合プロファイルと呼ばれ、ユーザーまたはグループのデータ変更をアプリケーションに通知するために使用するデータおよび方法を識別します。詳細は、32-8 ページの「Oracle Directory Provisioning Integration Service」を参照してください。

コネクタとディレクトリ統合プロファイルの概要

この項では、次の項目について説明します。

ディレクトリ同期用のコネクタ

Oracle Internet Directory と接続ディレクトリを同期化するため、Oracle Directory Integration and Provisioning Platform はコネクタと呼ばれるあらかじめパッケージされた接続ソリューションを使用します。このコネクタは最小構成でも、同期に必要な全設定情報を含む**ディレクトリ統合プロファイル**で構成されます。

コネクタとサポート対象インタフェースの使用

Oracle Internet Directory と接続ディレクトリを同期化するとき、Oracle Directory Integration and Provisioning Platform は、DB、LDAP、タグ付きまたは LDIF インタフェースのいずれかを使用します。接続ディレクトリがこれらのインタフェースの 1 つを使用するときにコネクタに必要なものは、同期させるためのディレクトリ統合プロファイルのみです。たとえば、Oracle Internet Directory とともに提供される SunONE コネクタは LDAP インタフェースを使用して、SunONE Directory Server から変更を読み取ります。変更は SunONE Directory Server に固有な形式をとるため、SunONE Directory Server 内で ldap 検索を実行することで判断できます。

サポート対象インタフェースなしのコネクタの使用

接続ディレクトリで Oracle Directory Integration and Provisioning Platform によってサポートされているインタフェースの 1 つを使用できない場合は、ディレクトリ統合プロファイルに加えてエージェントが必要です。エージェントは、Oracle Directory Integration and Provisioning Platform がサポートする形式の 1 つから、接続ディレクトリがサポートする形式に、データを変換します。一例が、Oracle Human Resources コネクタです。このコネクタには、あらかじめパッケージされた統合プロファイルと Oracle Human Resources エージェントの両方があります。エージェントは、Oracle Internet Directory との通信に、Oracle Directory Integration and Provisioning Platform がサポートしているタグ付きファイル形式を使用します。Oracle Human Resources システムとの通信には、(OCI インタフェース経由で) SQL を使用します。

同期の使用例

変更が行われたかどうかによって、次の方向で同期がとられます。

- 接続ディレクトリから Oracle Internet Directory へ
- Oracle Internet Directory から接続ディレクトリへ
- 両方向

データが流れる方向に関係なく、次のことを前提としています。

- 同期時に、一方のディレクトリに対する増分変更が他方のディレクトリに伝播されます。
- 同期の完了後、両方のディレクトリには同じ情報が維持されています。

Oracle Internet Directory から接続ディレクトリへの同期

Oracle Internet Directory は、ディレクトリ・オブジェクトへの増分変更が保存される変更ログを保持します。変更ログ番号に基づいて、これらの変更が順に保存されます。

Oracle Internet Directory から接続ディレクトリへの同期は、この変更ログを活用します。したがって、Oracle Directory Integration and Provisioning Server の実行時は、変更ロギングが使用可能であるデフォルト設定で Oracle Internet Directory を起動する必要があります。変更ロギングが使用不可のときは、A-7 ページの「Oracle ディレクトリ・サーバー・インスタンスの起動」で説明するとおり、OID Control Utility （OIDCTL）内の `-l` フラグを使用して使用可能にできます。

Oracle Directory Synchronization Service は、同期プロファイルを処理するたびに、次のように動作します。

1. すべての変更が反映済である、最新の変更ログ番号を検索します。
2. その番号より新しい各変更ログ・エントリをチェックします。
3. プロファイル内のフィルタリング・ルールを使用して、接続ディレクトリと同期化する変更を選択します。
4. エントリに対してマッピング・ルールを適用し、接続ディレクトリ内で必要な変更を行います。

次に、その接続ディレクトリ内の適切なエントリまたは属性が更新されます。接続ディレクトリで、DB、LDAP、タグ付きまたは LDIF の各形式が直接使用されていない場合は、プロファイルに指定されているエージェントが起動されます。正常に使用された最終ログ番号がプロファイルに保存されます。

Oracle Internet Directory は、すべてのプロファイルが必要な変更ログを使用した後、その変更ログを定期的にパージして、後続の同期の開始位置を示します。

接続ディレクトリから Oracle Internet Directory への同期

接続ディレクトリで、DB、LDAP、タグ付きまたは LDIF の各形式が直接使用されている場合、そのエントリまたは属性への変更は、Oracle Directory Synchronization Service によって自動的に同期化されます。それ以外の場合、コネクタは同期プロファイル内にエージェントを持ち、エージェントが LDIF またはタグ付き形式でファイルへの変更を書き込みます。次に、Oracle Directory Synchronization Service は、この接続ディレクトリ・データのファイルを使用して、Oracle Internet Directory を更新します。

Oracle Internet Directory がサポートしていないインタフェースを持つディレクトリとの同期化

一部の接続ディレクトリは、Oracle Internet Directory でサポートされているどのインタフェースを使用してもデータを受信できません。このタイプのディレクトリに対するプロファイルには、同期用の個別のプログラムを識別する属性が含まれています。これはエージェントと呼ばれます。エージェントは接続ディレクトリの固有な形式と同期データが入っている DB、LDAP、タグ付きまたは LDIF ファイルとの間の変換を行います。プロファイル内で識別されているとおり、エージェントは Oracle Directory Synchronization Service によって起動されます。

Oracle Internet Directory からこのタイプの接続ディレクトリへデータをエクスポートする場合、Oracle Directory Synchronization Service は、必要なファイルをタグ付き形式または LDIF 形式で作成します。次にエージェントは、そのファイルを読み込んで、データを受信する接続ディレクトリに適した形式に変換し、そのディレクトリにデータを格納します。

このタイプの接続ディレクトリから Oracle Internet Directory へデータをインポートする場合、エージェントは必要なファイルをタグ付きまたは LDIF 形式で作成します。次に、Oracle Directory Synchronization Service は、このファイルのデータを使用して、Oracle Internet Directory を更新します。

ディレクトリ同期プロファイル

ディレクトリ同期プロファイルと呼ばれる同期用のディレクトリ統合プロファイルには、次のとおり同期化に必要なすべての設定情報が含まれます。

- 同期の方向

  一部の接続ディレクトリは、Oracle Internet Directory からのデータの受信のみを行います。つまり、エクスポート操作のみに関与します。その他の接続ディレクトリは、Oracle Internet Directory にデータを供給するのみです。つまり、インポート操作のみに関与します。インポート操作とエクスポート操作の両方に関与する接続ディレクトリもあります。

  プロファイルは、方向ごとに（つまり、接続ディレクトリから Oracle Internet Directory への情報用に 1 つ、および Oracle Internet Directory から接続ディレクトリへの情報用に 1 つ）個別に使用されます。

- インタフェース・タイプ

  一部の接続ディレクトリは、Oracle Directory Integration and Provisioning Platform に組み込まれているインタフェースのいずれかでデータを受け取ることができます。LDAP、タグ付き、DB（読取り専用）、LDIF などのインタフェースがあります。これらの接続ディレクトリについては、プロファイルに格納されている情報を使用して Oracle Directory Synchronization Service が同期そのものを直接実行します。

- マッピング・ルールとその形式

  ディレクトリ同期環境では、あるドメインの典型的なエントリ・セットを別のドメインに移動できます。同様に、ある属性のセットを別の属性のセットにマップすることができます。

  マッピング・ルールは、接続ディレクトリと Oracle Internet Directory の間の属性の変換を制御します。各コネクタでは、その同期プロファイルの `orclodipAttributeMappingRules` 属性に一連のマッピング・ルールが格納されています。Oracle Directory Integration and Provisioning Server はこれらの規則を使用し、ディレクトリからエクスポートする場合、および接続ディレクトリまたはファイルからインポートしたデータを変換する場合に、必要に応じて属性をマップします。Oracle Directory Integration and Provisioning Server では、変更を Oracle Internet Directory にインポートする場合、マッピング・ルールに従って接続ディレクトリの変更レコードを LDAP 変更レコードに変換します。同様に、エクスポート時は、コネクタが Oracle Internet Directory での変更内容を接続ディレクトリが理解できる形式に変換します。

- 接続ディレクトリの接続詳細

  この詳細には、ホスト、ポート、接続モード（SSL または非 SSL）など、接続ディレクトリについての情報および接続情報が含まれます。

- その他の情報

  コネクタによる Oracle Internet Directory と接続ディレクトリの同期に必要なほとんどの情報は、同期プロファイルに格納されますが、コネクタによっては、さらに多くの情報が必要な場合があります。これは、操作によっては、実行時に追加構成情報が必要な場合があるためです。

  このような追加のコネクタ構成情報は、いつでも、またどこにでも格納できます。ただし、Oracle Directory Integration and Provisioning Platform では、追加のコネクタ構成情報を同期プロファイルに `orclODIPAgentConfigInfo` と呼ばれる属性として格納できます。使用するかどうかは任意です。コネクタがこのような情報を必要としない場合は、この属性を空白のまま残しておきます。このような情報が必要な場合は、Directory Integration and Provisioning Assistant または `ldapuploadagentfile.sh` という名前のスクリプトを使用して、この属性にロードしておきます。追加構成情報属性に格納されるデータの型と形式は、各実行プログラムのニーズによって決定されます。

この構成情報は、コネクタまたは接続ディレクトリ（あるいはその両方）に関連付けることができます。Oracle Internet Directory および Oracle Directory Integration and Provisioning Server は、この情報を変更しません。コネクタの起動時に、Oracle Directory Integration and Provisioning Server は、この属性の情報を一時ファイルとしてコネクタに提供します。

関連項目：

- ディレクトリ統合プロファイル内の属性のリストおよび説明については、B-18 ページの表 B-20 を参照してください。
- Directory Integration and Provisioning Assistant の使用方法は、A-106 ページの「Directory Integration and Provisioning Assistant」を参照してください。
- `ldapuploadagentfile.sh` スクリプトの使用方法は、A-118 ページの「ldapUploadAgentFile.sh ツールの構文」を参照してください。

Oracle Directory Integration and Provisioning Platform へのコネクタの登録

コネクタは、Oracle Internet Directory に登録してから配置します。この登録には、ディレクトリにエントリとして格納されるディレクトリ同期プロファイルの作成作業が含まれます。このプロファイルの属性については、B-18 ページの表 B-20 を参照してください。

同期プロファイルの作成には、後続の各項で説明する Oracle Directory Manager または Directory Integration and Provisioning Assistant のいずれかを使用できます。Directory Integration and Provisioning Assistant を使用する場合は、マッピング・ファイルと構成ファイルをアップロードするための別の操作は不要です。

接続ディレクトリとのデータの同期に必要なほとんどの情報（アカウント名、パスワード、ホスト名、ポート番号など）は、同期プロファイルに格納されています。ただし、コネクタの実行に必要な追加情報は、33-4 ページの「ディレクトリ同期プロファイル」で説明したとおり、同期プロファイル・エントリの `orclOdipAgentConfigInfo` 属性に格納できます。

同期プロファイル・エントリの属性は、オブジェクト・クラス `orclodiProfile` に属します。ただし、`orclodiplastappliedchangenumber` 属性はオブジェクト・クラス `orclchangesubscriber` に属します。

プラットフォーム関連のクラスと属性には、オブジェクト ID 接頭辞 `2.16.840.1.113894.7` が割り当てられます。

ディレクトリ内の様々な同期プロファイル・エントリが、コンテナ `cn=subscriber profile,cn=changelog subscriber,cn=oracle internet directory` の下に作成されます。たとえば、`OracleHRAgent` と呼ばれるコネクタは、`orclodipagentname=OracleHRAgent,cn=subscriber profile,cn=changelog subscriber,cn=oracle internet directory` としてディレクトリに格納されます。

マッピング・ルール属性の形式

マッピング・ルール属性によって、1 つのディレクトリから別のディレクトリへエントリを変換する方法を指定できます。ドメイン・レベルのマッピングと属性レベルのマッピングを指定できます。この属性は、この項で説明するファイルの形式に基づいていることを前提としています。

マッピング・ルールは固定表形式で編成されます。この形式には慎重に従う必要があります。DomainRules という語のみが指定されている行と、### の文字のみが指定されている行の間に、マッピング・ルールの各セットが記述されます。各ルール内のフィールドは、コロン（:）で区切られます。

```
DomainRules
srcDomainName1: [dstDomainName1]: [DomainMappingRule1]
srcDomainName2: [dstDomainName2]: [DomainMappingRule2]
AttributeRules
srcAttrName1:[ReqAttrSeq]:[SrcAttrType]:[SrcObjectClass]:[dstAttrName1]:[DstAttrType
]:[DstObjectClass]:[AttrMappingRule1]
srcAttrName1,srcAttrName2:[ReqAttrSeq]:[SrcAttrType]:[SrcObjectClass]:[dstAttrName2]
:[DstAttrType]:[DstObjectClass]:[AttrMappingRule2]
###
```

srcAttrName1 と *srcAttrName2* を拡張する場合は、それぞれ改行なしで 1 行に記述します。

ドメイン・レベル・マッピング

ドメイン・ルールは、キーワード DomainRules のみが指定されている行の後に指定されます。各ドメイン・ルールは、表 33-1 で説明するコンポーネント（コロン区切り）で表現されます。

表 33-1 ドメイン・ルールのコンポーネント

コンポーネント名	説明
SrcDomainName	関係のあるドメインまたはコンテナの名前。LDAP および LDIF 以外のソースには、NONLDAP を指定します。
DstDomainName	宛先に関係のあるドメイン名。このエントリはオプションです。未指定の場合は、有効な状態にある SrcDomainName の値を採用します。LDAP および LDIF 以外の宛先には、NONLDAP を指定します。インポートとエクスポートは、常に Oracle Internet Directory に対して行われるため、NONLDAP:NONLDAP の組合せは許可されません。

表 33-1 ドメイン・ルールのコンポーネント（続き）

コンポーネント名	説明
DomainMappingRule	このフィールドは、Oracle Internet Directory へのインポート、または LDIF ファイルまたは他の外部 LDAP 準拠ディレクトリへのエクスポートの場合にのみ有効です。このルールは、ソース・ドメイン名または AttributeRules に指定されている属性（あるいはその両方）から、宛先ドメイン名を構成するために使用されます。このフィールドは、通常、cn=%,l=%,o=oracle,dc=com の形式です。これらの指定は、エントリをディレクトリ内の異なるドメインまたはコンテナに配置するために使用されます。LDAP 以外のソースの場合、このルールは、エントリのディレクトリへの配置に必要な、宛先ドメイン名の形式を整える方法を示します。 このコンポーネントは、LDAP から LDIF、LDAP から LDAP、または LDIF から LDAP の場合はオプションです。未指定の場合、ソース・ドメイン名と宛先ドメイン名は同じと考えられます。

属性レベル・マッピング

属性ルールは、キーワード AttributeRules のみが指定されている行の後に指定されます。各属性ルールは、表 33-2 で説明するコンポーネント（コロン区切り）で表現されます。属性ルールの指定は、### の文字のみが指定されている行で終わります。

表 33-2 属性ルールのコンポーネント

コンポーネント名	説明
SrcAttrName	LDAP 準拠ディレクトリのリポジトリの場合、このパラメータは変換する属性の名前を意味します。 Oracle9*i* データベース・サーバーのリポジトリの場合、このパラメータは、SrcClassName で指定された表の ColumnName を意味します。 他のリポジトリの場合、このパラメータは適切に解釈されます。
ReqAttrSeq	ソース属性を宛先に常に渡す必要があるかどうかを示します。エントリを Oracle Internet Directory と接続ディレクトリ間で同期化する場合は、一部の属性を同期キーとして使用する必要があります。このフィールドは、指定した属性がキーとして使用されているかどうかを示します。使用されている場合は、属性の変化には関係なく、その属性の値がソースから常に抽出されます。 属性を相手側に常に渡す必要がある場合は、このフィールドに 0（ゼロ）以外の整数値を指定します。

表 33-2 属性ルールのコンポーネント（続き）

コンポーネント名	説明
SrcAttrType	このパラメータは、整数、文字列、バイナリなど、属性の型を意味し、マッピング・ルールの妥当性をチェックします。
SrcObjectClass	共有している属性のソースが LDAP 準拠ディレクトリの場合は、このパラメータによって、その属性が所属しているオブジェクト・クラスの名前が指定されます。 共有属性のソースが Oracle9*i* データベース・サーバーのリポジトリの場合、このパラメータは表名を意味し、指定は必須です。他のリポジトリの場合、このパラメータは無視されます。
DstAttrName	オプションの属性。未指定の場合は、SrcAttrName が使用されます。 LDAP 準拠ディレクトリの場合、このパラメータは宛先の属性の名前を意味します。 Oracle9*i* データベース・サーバーのリポジトリの場合、このパラメータは、SrcClassName で指定された表の ColumnName を意味します。 他のリポジトリの場合、このパラメータは適切に解釈されます。
DstAttrType	このパラメータは、整数、文字列、バイナリなど、属性の型を意味します。ソースおよび宛先の属性型の互換性を保証する責任は管理者にあります。Oracle Directory Integration and Provisioning Platform はこの互換性を保証しません。
DstObjectClass	LDAP 準拠ディレクトリの場合、このパラメータは、属性が所属するオブジェクト・クラスを意味します。このパラメータはオプションです。 Oracle9*i* データベース・サーバーのリポジトリの場合、このパラメータは表名を意味し、指定は必須です。 他のリポジトリの場合、このパラメータは無視されます。
AttrMapping Rule	演算子 +、|、ファンクション toUpper (string)、toLower(String)、trunc (string,char) を使用するオプションの算術式。未指定の場合は、ソース属性値が宛先属性の値としてコピーされます。リテラルは一重引用符（'）または二重引用符（""）で指定できます。

新規に作成した同期プロファイルのマッピング・ルールは空になります。マッピング・ルールを入力するには、適切な形式に厳密に従ったファイルを編集します。

注意： マッピング・ファイルに属性およびオブジェクト・クラスが定義される際、スキーマに定義されているそれぞれの属性およびオブジェクト・クラスはソース・ディレクトリに入っているとみなされます。

同期用に親コンテナが選択されると、マッピング・ルールに一致するすべての子も同様に同期化されます。子コンテナを選択して同期から排除することはできません。

新規マッピング・ファイルの作成方法

新規マッピング・ファイルを作成する手順は、次のとおりです。

1. ソース・ディレクトリ内で同期に関係のあるコンテナ（1 つまたは複数）を識別します。
2. ソース・コンテナ内のオブジェクトのマッピング先である宛先コンテナ（1 つまたは複数）を識別します。指定されたコンテナがディレクトリ内に存在することを確認します。
3. 宛先ディレクトリ内に作成されるエントリの DN 作成ルールを決定します。LDAP から LDAP への場合、マッピングは通常 1 対 1 です。LDAP 以外から LDAP への場合は、ドメイン、DN 構成ルールが必要です。たとえば、タグ付きファイルまたは Human Resources エージェントからの同期の場合、マッピング・ルールは `uid=%,dc=mycompany,dc=com` の形式になることがあります。この場合、Oracle Human Resources から適用されるすべての変更に `uid` 属性が存在する必要があります。手順 6 で指定するとおり、必須属性として `uid` 属性が指定される必要があります。
4. ディレクトリ間で同期化するオブジェクト（ソースおよび宛先ディレクトリ内の関連オブジェクト・クラス）を識別します。通常、ディレクトリ間で同期化されるオブジェクトには、ユーザー、グループ、組織単位、組織およびその他のリソースがあります。これらのオブジェクトを識別するには、ディレクトリで使用されている実際のオブジェクト・クラスを識別します。
5. ディレクトリ間で同期化する各種オブジェクトのプロパティ（LDAP コンテキストの属性）を識別します。オブジェクトの属性すべてを同期化する必要はありません。同期化対象のユーザー・プロパティは、`cn`、`sn`、`uid`、`mail` などです。
6. マッピング・ルールを定義します。各マッピング・ルールの形式は次のとおりです。

   ```
   <srcAttrName>:<ReqdFlag>:<srcAttrType>:<SrcObjectClass>:
   <dstAttrName>:<dstAttrType>:<dstObjectClass>: <Mapping Rule>
   ```

   マッピング・ルールを定義するときは、必ず次のことを確認してください。

   - 必須属性にはそれぞれ順序番号が付いていること。たとえば、手順 3 で `uid` 属性が必須として識別された場合は、`<ReqdFlag>` のかわりに `1` の値を割り当てます。
   - 関連オブジェクト・クラスは、それぞれ宛先ディレクトリ上にスキーマ定義を持つこと。

- 宛先オブジェクト・クラス内の必須属性は、すべてソースから割り当てられた値を持つこと。様々な LDAP 実装は標準に完全に準拠していない可能性もありますが、これは標準オブジェクト・クラスにも有効です。

ソース・オブジェクト・クラスに属する属性のすべてを 1 つの宛先オブジェクト・クラスに割り当てる必要はありません。ソース・オブジェクト・クラスの各種の属性は、異なる宛先オブジェクト・クラスに属する様々な属性に割り当てることができます。

属性がバイナリ値をとる場合は、<attrtype> フィールドで binary として指定します。

サポートされている属性マッピング・ルールと例

サポートされている属性マッピング・ルールは次のとおりです。

- 連結（+）: 2 つの文字列属性の連結に使用します。

  次のようなマッピング・ルールについて考えてみます。

  ```
  Firstname,lastname: : : : givenname: : inetorgperson: firstname+lastname
  ```

  たとえば、ソースの Firstname が John、LastName が Doe の場合、このルールによって、宛先の givenname 属性は、JohnDoe という値になります。

- OR 演算子（|）: 2 つの文字列属性の 1 つを宛先に割り当てるときに使用します。

  次のようなマッピング・ルールについて考えてみます。

  ```
  Fistname,lastname : : : :givenname: :inetorgperson: firstname | lastname
  ```

  この例では、firstname の値が存在する場合は、それが givenname に割り当てられます。firstname 属性が存在しない場合、lastname の値が givenname に割り当てられます。両方の値が空である場合、値は割り当てられません。

- bin2b64 ( ): ソース・ディレクトリのバイナリ値を Base64 のエンコード値として宛先ディレクトリに保存するときに使用します。通常、次のように使用します。

  ```
  objectguid: : : :binary: :orclobjectguid: orcladuser:bin2b64(objectguid)
  ```

  (objectguid) の値を検索する必要がある場合、これは必須です。

- tolower(): 文字列属性値を小文字に変換します。

  ```
  firstname: : : :givenname: :inetorgperson: tolower(firstname)
  ```

- toupper(): 文字列属性値を大文字に変換します。

  ```
  firstname: : : :givenname: :inetorgperson: toupper(firstname)
  ```

- trunc(str, char): 指定した文字が最初に出現する箇所以降の文字列を切り捨てます。

  ```
  mail : : : : uid : : inetorgperson : trunc(mail,'@')
  ```

  たとえば、ソースの mail が John.Doe@acme.com の場合、このルールによって、宛先の uid 属性は、「John.Doe」という値になります。

- truncl(str, char): 指定した文字が最初に出現する箇所まで、文字列を切り捨てます。

  ```
  mail : : : : uid : : inetorgperson : trunc(mail,'@')
  ```

  たとえば、ソースの mail が John.Doe@acme.com の場合、このルールによって、宛先の uid 属性は、「acme.com」という値になります。

- trunc(str1, str2): 指定した文字列が最初に出現する箇所以降の文字列を切り捨てます。

  ```
  mail : : : : uid : : inetorgperson : trunc(mail, "@")
  ```

- dnconvert (str): ドメイン・マッピングが使用される場合に、DN タイプで使用されます。

  たとえば、次の場合を考えてみます。

  ```
  uniquemember : : : groupofuniquenames : uniquemember : :groupofuniquenames :
  dnconvert(uniquemember)
  ```

  この場合、ソースの uniquemember が cn=test user1,cn=srcdomain の場合、宛先の uniquemember は、cn=test user1,cn=dstdomain になります。

  ドメイン・マッピング・ルールは、次のような場合です。

  ```
  DomainRules
  cn=srcdomain:cn=dstdomain:
  ```

- リテラル:

  ```
  Userpassword: : :person: userpassword: :person: 'welcome1'
  ```

例: タグ付きファイル・インタフェース用のマッピング・ファイル

前述の説明に基づいて、ここではタグ付きファイル・インタフェースを使用して、Oracle Human Resources データベース表からユーザー・エントリをインポートするためのマッピング・ファイルの例を示します。このサンプル・ファイルはインストール時に提供され、*$ORACLE_HOME*/ldap/odi/conf/oraclehragent.map.master にあります。

```
DomainRules
NONLDAP:dc=myCompany,dc=com:uid=%dc=myCompany,dc=com
AttributeRules
```

```
firstname: : : :cn: :person
email : : : :cn: :person: trunc(email,'@')
email : 1 : :uid: :person:trunc(email,'@')
firstname,lastname: : : :cn: :person: firstname+","+lastname
lastname,firstname: : : :cn: :person: lastname+","+firstname
firstname,lastname: : : :sn: :person: lastname | firstname
EmployeeNumber: : : :employeenumber: :inetOrgperson
EMail: : : :mail: :inetOrgperson
TelephoneNumber1: : : :telephonenumber: :person
TelephoneNumber2: : : :telephonenumber: :person
TelephoneNumber3: : : :telephonenumber: :person
Address1: : : :postaladdress: :person
state: : : :st: :locality
street1: : : :street: :locality
zip: : : :postalcode: :locality
town_or_city: : : :l: :locality
Title: : : :title: :organizationalperson
#Sex: : : :sex: :person
###
```

前述のように、マッピング・ファイルは、キーワードおよびドメインと属性の一連のマッピング・ルール・エントリで構成されています。この例のマッピング・ファイルには、ドメイン・ルール NONLDAP:dc=myCompany,dc=com:cn=%,dc=myCompany,dc=com が含まれています。

- このルールは、ソース・ドメインが NONLDAP で、ソース・ドメインがないことを示しています。
- 宛先ドメイン（:dc=myCompany,dc=com）は、このプロファイルが処理するすべてのディレクトリ・エントリが、ドメイン dc=myCompany,dc=com にあることを示しています。同期化を開始する前に、ドメインが存在することを確認してください。
- ドメイン・マッピング・ルール（: uid=%,dc=myCompany,dc=com）は、ソースからのデータが、このドメイン・マッピング・ルールで構成した DN を持つディレクトリ内のエントリを参照する必要があることを示しています。この場合の uid は、常に NULL 以外の値を持つ宛先属性の 1 つである必要があります。同期化するエントリに対応するデータが NULL 値の場合、マッピング・エンジンは、そのエントリを無効と判断し、次のエントリに進みます。ディレクトリでエントリを正確に識別するには、uid が単一値であることも必要です。
- タグ付きファイルの場合、ソース・エントリは同期化対象のオブジェクトの型を示すオブジェクト・クラスを持ちません。SrcObjectClass フィールドは空白です。
- 宛先が Oracle Internet Directory のオブジェクトは、それぞれオブジェクト・クラスを持つ必要があります。各属性にオブジェクト・クラスを指定します。

- email は、マッピング・ファイル例では必須属性として指定されています。それは、uid 属性が email 属性から導出されているためです。同期化を成功させるには、タグ付きファイルに指定されているすべての変更に、次のとおり email 属性を指定する必要があります。

  ```
  Email : 1 : : :uid : : person : trunc(email,'@')
  ```

- 場合によっては、複数値属性の名前を使用して識別名の **RDN** を構成する必要があります。たとえば、cn=%,l=%,dc=myCompany,dc=com（cn は複数値属性）の DN でエントリを構成する場合、ドメイン・マッピング・ルールは、rdn,l=%,dc=myCompany,dc=com（rdn は、NULL 値以外の宛先属性の 1 つ）のような形式になります。これをサポートする典型的なマッピング・ファイルは、次のような形式です。

```
DomainRules
NONLDAP:dc=us,dc=myCompany,dc=com:rdn,l=%,dc=us,dc=myCompany,dc=com
AttributeRules
firstname: : :cn: :person
email : : : :cn: :person: trunc(email,'@')
email : 1: : :rdn: :person: 'cn='+trunc(email,'@')
firstname,lastname: : : :cn: :person: firstname+","+lastname
lastname,firstname: : : :cn: :person: lastname+","+firstname
firstname,lastname: : : :sn: :person: lastname | firstname
EmployeeNumber: : : :employeenumber: :inetOrgperson
EMail: : : :mail: :inetOrgperson
TelephoneNumber1: : : :telephonenumber: :person
TelephoneNumber2: : : :telephonenumber: :person
TelephoneNumber3: : : :telephonenumber: :person
Address1: : : :postaladdress: :person
Address1: : : :postaladdress: :person
Address1: : : :postaladdress: :person
state: : : :st: :locality
street1: : : :street: :locality
zip: : : :postalcode: :locality
town_or_city: 2 : : :1: :locality
Title: : : :title: :organizationalperson
#Sex: : : :sex: :person
###
```

マッピング・ルールには柔軟性があり、1 対多と多対 1 の両方のマッピングを組み込むことができます。

- 1 対多

  接続ディレクトリの 1 つの属性を、Oracle Internet Directory の多数の属性にマップできます。たとえば、接続ディレクトリのある属性が `Address:123 Main Street/MyTown, MyState 12345` であるとします。Oracle Internet Directory のこの属性は、LDAP 属性 `homeAddress` と LDAP 属性 `postalAddress` の両方にマップできます。

- 多対 1

  接続ディレクトリの複数の属性を、Oracle Internet Directory の 1 つの属性にマップできます。たとえば、Oracle Human Resources ディレクトリでは、`firstname=Anne` と `lastname=Smith` の 2 つの属性を使用して Anne Smith を表すとします。これらの 2 つの属性は、Oracle Internet Directory の 1 つの属性 `cn=Anne Smith` にマップできます。ただし、双方向同期では、逆方向のマッピングはできません。たとえば、*`cn=Anne Smith`* を複数の属性にマッピングすることはできません。

例 : LDIF インタフェース用のマッピング・ファイル

Directory Integration and Provisioning Assistant を使用したインストールの一部として、一連の統合プロファイル例が作成されます。プロファイル作成用に使用されるプロパティ・ファイルは、次のディレクトリにあります。

`$`*`ORACLE_HOME`*`/ldap/odi/samples`

インポート・マッピング・ファイル例

```
DomainRules
dc=mycompany.oid,dc=com:dc=mycompany.iplanet,dc=com
AttributeRules
# Mapping rules to map the domains and containers
o: : :organization: o: :organization
ou: : :organizationalUnit: ou: : organizationalUnit
dc: : :domain:dc: :domain
# Mapping Rules to map users
uid : : :person: uid: :inetOrgperson
sn: : :person:sn: :person
cn: : :person:cn: :person
mail: :inetorgperson: mail: :inetorgperson
employeenumber: :organizationalPerson: employeenumber: :organizationalperson
c: : :country:c: :country
l: : :locality: l: :locality
telephonenumber: :organizationalPerson: telephonenumber: :organizationalperson
userpassword: : :person: userpassword: :person
uid: : :person: orcldefaultProfileGroup: :orclUserV2
# Mapping Rules to map groups
```

```
cn: : :groupofuniquenames:cn: :groupofuniquenames
member: : :groupofuniquenames:member: :orclgroup
uniquemember: : :groupofuniquenames:uniquemember: :orclgroup
owner: : :groupofuniquenames:owner: :orclgroup
# userpassword: :base64:userpassword: :binary:
```

マッピング・ルールの更新

マッピング・ルールは、新規規則の追加、既存規則の変更または `orclodipAttributeMappingRules` 属性に指定されているマッピング・ルール・セットから一部の規則を削除することによって、カスタマイズできます。通常、これらの操作を実行するには、マッピング・ルールが指定されているファイルを特定するか、または A-39 ページの「ldapsearch の構文」に説明する ldapsearch コマンドを使用してファイルの属性値を格納します。

マッピング・ルールは、Oracle Directory Manager では編集できません。かわりに、マッピング・ルールをファイルに格納し、そのファイルを属性の値としてディレクトリにアップロードします。マッピング・ファイルをアップロードするには、Directory Integration and Provisioning Assistant または `ldapuploadagentfile.sh` ユーティリティを使用します。作成およびアップロードされたマッピング・ファイルのコピーは、*$ORACLE_HOME*`/ldap/odi/conf` ディレクトリに保持でき、将来更新した後に再度アップロードできます。

```
dipassistant mp -profile profile name odip.profile.mapfile=map file
```

関連項目：

A-106 ページの「Directory Integration and Provisioning Assistant」

A-118 ページの「ldapUploadAgentFile.sh ツールの構文」

エントリのマッピング・ルール・ファイルへの追加 新規エントリをマッピング・ルール・ファイルに追加するには、そのファイルを編集して、レコードをファイルに追加します。この手順は、次のとおりです。

1. Oracle Internet Directory にマップする必要がある接続ディレクトリの属性名とオブジェクト・クラスを識別します。
2. Oracle Internet Directory 内の対応する属性名およびマッピング先のオブジェクト・クラスを識別します。
3. 属性値に対して実行する必要がある変換を示すマッピング・ルール要素を生成します。
4. 属性マッピング・ルール・ファイルを同期プロファイルにロードします。

   たとえば、ソース・ディレクトリ内のあるエントリの電子メール属性を宛先の固有識別子にマッピングする必要がある場合は、次のようになります。

   ```
   Email:  :  : inetorgperson: uid: : person:
   ```

マッピング・ルール・ファイル内のエントリの変更 マッピング・ルール・ファイル内の変更するエントリを識別してから、属性値の変換に必要なマッピング・ルール要素を生成します。

エントリのマッピング・ルール・ファイルからの削除 マッピング・ルール・ファイル内の削除するエントリを識別した後は、エントリをファイルから削除したり、エントリの前にハッシュ符号（#）を付加してそのエントリをコメント化できます。

関連項目：

- Directory Integration and Provisioning Assistant の使用方法は、A-106 ページの「Directory Integration and Provisioning Assistant」を参照してください。
- `ldapuploadagentfile.sh` スクリプトの使用方法は、A-118 ページの「ldapUploadAgentFile.sh ツールの構文」を参照してください。
- これらのファイルの名前については、33-17 ページの「ファイルの位置とネーミング」を参照してください。

注意： Windows オペレーティング・システムでシェル・スクリプト・ツールを実行するには、次のいずれかの UNIX エミュレーション・ユーティリティが必要です。

- Cygwin 1.3.2.2-1 以上
  サイト：`http://sources.redhat.com`
- MKS Toolkit 6.1
  サイト：`http://www.datafocus.com/`

ファイルの位置とネーミング

表 33-3 に、ディレクトリ統合プロファイル内および同期時に使用される各種のファイルの位置を示します。

表 33-3 ファイルの位置と名前

ファイル	ファイル名
インポート・データ・ファイル	`$ORACLE_HOME/ldap/odi/data/import/`*`Profile_Name`*`.dat`
エクスポート・データ・ファイル	`$ORACLE_HOME/ldap/odi/data/export/`*`Profile_Name`*`.dat`
追加構成情報	`$ORACLE_HOME/ldap/odi/conf /`*`Profile_Name`*`.cfg`
マッピング・ルール	`$ORACLE_HOME/ldap/odi/conf /`*`Profile_Name`*`.map`

たとえば、Oracle Human Resources コネクタのデータ・ファイル名は `oraclehrprofile.dat` です。

同期プロファイルの管理

この項では、次の項目について説明します。

- Oracle Directory Manager を使用した同期の管理
- コマンドライン・ツールを使用した同期プロファイルの管理

Oracle Directory Manager を使用した同期の管理

この項では、Oracle Directory Manager を使用したプロファイルの登録と登録解除の方法を説明します。

Oracle Directory Manager を使用したプロファイルの登録

Oracle Directory Manager では、プロファイルを次の 2 つの方法で登録できます。

- 新規構成設定エントリを作成し、次にこのエントリにプロファイルを追加する方法
- 既存の構成設定エントリを選択し、次にこのエントリにプロファイルを追加する方法

ディレクトリ統合プロファイルを登録する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**、「**サーバー管理**」の順に展開します。
2. 「**統合サーバー**」を選択します。右側のペインに「アクティブ・プロセス」ボックスが表示されます。
3. ツールバーの「**作成**」ボタンを選択します。「構成設定」ダイアログ・ボックスが表示されます。
4. 「構成設定」ダイアログ・ボックスで、「**作成**」を選択します。「統合プロファイル」ダイアログ・ボックスが表示されます。次の 2 つのオプションがあります。
   - 既存のものをコピーして統合プロファイルを作成する

     この場合は、コピーする Oracle Directory Integration and Provisioning Platform プロファイルを選択し、「**類似項目の作成**」を選択します。「統合プロファイル」ダイアログ・ボックスに「**一般**」タブ・ページが表示されます。
   - 既存のものをコピーせずに統合プロファイルを作成する

     この場合は、「**新規作成**」を選択します。「統合プロファイル」ダイアログ・ボックスに「**一般**」タブ・ページが表示されます。
5. 「**一般**」タブ・ページを選択し、各フィールドに情報を入力します。詳細は、C-36 ページの表 C-40 を参照してください。

6. 「**実行**」タブを選択し、各フィールドに情報を入力します。詳細は、C-38 ページの表 C-41 を参照してください。
7. 「**マッピング**」タブを選択し、各フィールドに情報を入力します。詳細は、C-39 ページの表 C-42 を参照してください。
8. 「**ステータス**」タブを選択し、各フィールドに情報を入力します。詳細は、C-40 ページの表 C-43 を参照してください。このページにはコネクタの実行ステータスが表示されるため、ほとんどのフィールドは編集できません。
9. 情報を入力した後、「**OK**」を選択します。「構成設定」ダイアログ・ボックスに戻ります。このダイアログ・ボックスには、作成した統合プロファイルがリストされています。
10. 「**OK**」を選択して「構成設定」ダイアログ・ボックスを終了します。これで作成したプロファイルが Oracle Internet Directory に登録されます。

Oracle Directory Manager を使用したプロファイルの登録解除

プロファイルを登録解除する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「**ディレクトリ・サーバー・インスタンス**」、「**サーバー管理**」、「**統合サーバー**」の順に展開します。
2. プロファイルを削除する「構成設定」を選択します。「**統合プロファイル**」タブ・ページが右側のペインに表示されます。
3. 「**統合プロファイル**」タブ・ページで、登録解除するプロファイルを選択します。
4. 「**削除**」を選択します。

同期ステータス属性の変更

エクスポート操作で同期が行われている間、サーバーは同期ステータス属性の `orcllastappliedchangenumber` を常に更新します。Oracle Directory Manager では、このフィールドは**「OID 前回適用された変更番号」**と呼ばれます。

この属性を Oracle Directory Manager を使用して変更する手順は、次のとおりです。

1. Oracle Directory Integration and Provisioning Server がプロファイルに対する使用禁止フラグを認識することを確認します。

   デフォルト・モードでは、Directory Integration and Provisioning Server がこのフラグを認識するために、2 分間ほどかかる場合があります。このフラグを迅速に認識させるには、A-13 ページの表 A-5 で説明するとおり、更新間隔に低い値を設定します。
2. Oracle Directory Manager を使用して、エージェントを使用禁止にします。
3. 属性変更を行います。
4. 変更後、エージェントを再度使用可能にします。

コマンドライン・ツールを使用した同期プロファイルの管理

プロファイルは、Directory Integration and Provisioning Assistant またはその他のコマンドライン・ツールを使用して、登録または登録解除することができます。この項では、プロファイルの登録および登録解除の方法を説明します。

Directory Integration and Provisioning Assistant による同期プロファイルの登録および登録解除

Directory Integration and Provisioning Assistant を使用して同期プロファイルの作成および削除ができます。

関連項目： A-106 ページの「Directory Integration and Provisioning Assistant」

ldapcreateconn.sh を使用した同期プロファイルの登録

コマンドライン・ツール `ldapcreateconn.sh` を使用して同期プロファイルを作成できます。このツールは、ディレクトリ *`$ORACLE_HOME`*`/ldap/admin/` にあります。

関連項目： A-119 ページの「ldapCreateConn.sh ツール構文」

ldapdeleteconn.sh を使用した同期プロファイルの登録解除

コマンドライン・ツール `ldapdeleteconn.sh` を使用して同期プロファイルを登録解除できます。このツールは、ディレクトリ *`$ORACLE_HOME`*`/ldap/admin/` にあります。

関連項目： A-121 ページの「ldapDeleteConn.sh ツール構文」

注意： Windows オペレーティング・システムでシェル・スクリプト・ツールを実行するには、次のいずれかの UNIX エミュレーション・ユーティリティが必要です。

- Cygwin 1.3.2.2-1 以上
  サイト：`http://sources.redhat.com`
- MKS Toolkit 6.1
  サイト：`http://www.datafocus.com/`

Oracle Directory Integration and Provisioning Platform での同期に関するトラブルシューティング

実行中のプロファイル数が多い場合、または対象のプロファイル用のスケジューリング間隔が非常に短い場合、同期に関するトラブルシューティングが難しい場合があります。このような場合は、次の手順でコネクタの動作をテストできます。

1. 多数のプロファイルが実行中の場合は、Oracle Directory Manager を使用して、トラブルシューティングが必要なプロファイルを選択して無効にします。これに対し、1 つのプロファイルのみが実行中の場合は、Oracle Directory Integration and Provisioning Server を停止します。
2. $*ORACLE_HOME*/bin の oditest コマンドを次のように実行します。

   ```
   oditest sync profile_name host=host_of_Oracle_Internet_Directory port=port_for_
   Oracle_Internet_Directory binddn=bind_DN bindpass=password_for_the_bind_DN
   sslauth=0 debug=63
   ```

$*ORACLE_HOME*/ldap/odi/log ディレクトリに監査ファイルとログ・ファイルが作成されます。

同期の動作を確認する場合は、トレース・ファイルと監査ファイルを調べます。

デバッグの詳細を確認する場合は、ディレクトリ統合プロファイルでデバッグ・ロギング・レベルを設定します。

> **関連項目：** 適切なデバッグ・ロギング・レベルを判断する方法については、10-6 ページの「デバッグ・ロギング・レベルの設定」を参照してください。

34

Oracle Directory Provisioning Integration Service

Oracle Directory Provisioning Integration Service によって、アプリケーションは、プロビジョニング情報を Oracle Internet Directory から受信できます。

この章では、次の項目について説明します。

- Oracle Directory Provisioning Integration Service の概要
- Oracle Directory Provisioning Integration Service 環境の管理
- セキュリティと Oracle Directory Provisioning Integration Service
- Oracle Directory Provisioning Integration Service に関するトラブルシューティング

> **関連項目：**『Oracle Internet Directory アプリケーション開発者ガイド』にある「プロビジョニング統合アプリケーションの開発」の章を参照してください。

Oracle Directory Provisioning Integration Service の概要

この項では、Oracle Directory Provisioning Integration Service 環境のコンポーネントがプロビジョニング・プロセスを介して対話する方法について説明します。次の項目について説明します。

- プロビジョニングの概要
- Oracle Directory Provisioning Integration Service が、変更を Oracle Internet Directory から取得する方法
- アプリケーションを Oracle Directory Provisioning Integration Service に登録する方法
- アプリケーションが Oracle Internet Directory からプロビジョニング情報を受信する方法
- Oracle Internet Directory がアプリケーションからプロビジョニング情報を受信する方法
- Oracle Directory Provisioning Integration Service からのアプリケーション・サブスクライブを停止する方法

プロビジョニングの概要

プロビジョニングには次のものが含まれます。

- ディレクトリ内の特定のデータへの変更の受信をサブスクライブするアプリケーション
- これらの変更をサブスクライブ・アプリケーションに送信するディレクトリ

アプリケーション固有のディレクトリ内のすべてのエンティティを中央ディレクトリのエンティティと同期する場合がありますが、この場合、アプリケーションのプロビジョニングで受信するのは、そのエンティティの一部に関する通知のみです。たとえば、Oracle Human Resources のディレクトリには、通常、企業内の全従業員に関するデータが格納されているため、そのデータのすべてを中央ディレクトリと同期することがあります。ただし、メンバーが特定グループに加入した場合または脱退した場合のみ、指定したアプリケーションに通知するようにプロビジョニングすることもできます。

最初のインストール時に、ディレクトリにプロビジョニング・プロファイルを作成することによって、アプリケーションはプロビジョニングをサブスクライブします。各認証管理レルム内のアプリケーションごとに 1 つのプロファイルが必要です。

プロビジョニングの手順

ディレクトリ対応の環境では、プロビジョニングには次の作業が含まれます。

1. 中央ディレクトリでユーザーを作成します。
2. ユーザーのアプリケーションへの登録（アプリケーション固有のユーザー・アカウントとエンタイトルメントの作成）
3. アプリケーションのアカウントおよびエンタイトルメントと中央ディレクトリとの同期化

たとえば、電子メール・アプリケーションにアクセスするためにユーザーをプロビジョニングする場合は、次の手順が必要です。

1. 中央ディレクトリでユーザーを作成します。
2. ユーザーを電子メール・アプリケーションに登録します。この登録には、そのユーザーの電子メール・アカウントと割当て制限の設定、および必要なパブリック・フォルダの作成が含まれます。
3. 電子メール・アプリケーションのユーザー情報を中央ディレクトリの情報と同期化します。

ユーザー、グループおよびユーザー・サブスクリプションの情報は、次のいずれからでも変更できます。

- Oracle Delegated Administration Services
- Oracle Human Resources または Oracle Directory Integration and Provisioning Platform に統合されている他のアプリケーション
- Oracle Directory Manager
- Oracle Enterprise Manager のツール（Enterprise Security Manager など）

アプリケーションでのユーザーの登録

アプリケーションでのユーザー登録は、自動的にまたは手動で行うことができます。

自動登録 この方法は、「オンデマンド登録」と呼ばれることもあります。中央ディレクトリと継続して同期するかわりに、ユーザーが最初にアプリケーションにアクセスしたときに、アプリケーションでユーザーのフットプリントを作成します。Oracle Application Server Single Sign-On は、この方法でアプリケーションにアクセスするユーザーを登録します。

手動登録 この方法では、管理者がアプリケーション固有の管理ツールを使用して、アプリケーション固有の情報を準備します。

たとえば、登録前にマネージャからの承認を取得することを、ユーザーに要求することができます。この場合は、オンデマンド登録を使用しないで、必要な承認の取得後に、アプリケーション管理者がユーザーを手動で登録することができます。

プロビジョニング情報

通常、ユーザーのプロビジョニングには、2 種類の情報の作成が含まれます。

- Oracle Internet Directory の共有ユーザー・メタデータ

  このデータには、ユーザーの識別情報、資格証明、プロファイルおよび作業環境が含まれます。このデータは、標準のディレクトリ・ユーザー属性（住所や言語の設定項目など）によって表されます。

- アプリケーション内のアプリケーション固有のユーザー・データ

  このデータには、ユーザーの電子メール・メッセージ・フォルダ内のデータやカレンダ・アプリケーションでのユーザーのアポイントメント・データなどが含まれます。このデータは通常、ディレクトリまたはアプリケーション固有のリポジトリ内で、アプリケーション固有の表記規則を使用して表されます。

Oracle Directory Provisioning Integration Service が、変更を Oracle Internet Directory から取得する方法

Oracle Directory Provisioning Integration Service 環境では、次の方法で変更を取得します。

- Oracle Internet Directory は、ユーザー、グループおよびユーザー・サブスクリプションに関するすべての情報の中央リポジトリとして機能します。
- アプリケーションは、ディレクトリにプロビジョニング・プロファイルを作成することによって、プロビジョニング・イベントをサブスクライブして受信します。
- Oracle Directory Provisioning Integration Service は、関連する情報への変更について、Oracle Internet Directory を監視し、変更をプロビジョニング・イベントの形式でアプリケーションに伝達します。

Oracle Internet Directory から変更を受信するために、Oracle Directory Provisioning Integration Service は Oracle Internet Directory の変更ログをサブスクライブします。変更ログ内の変更はフィルタ処理され、必要な変更のみがアプリケーションに渡されます。アプリケーションに関係するのが特定サブツリーのイベントのみの場合、Oracle Directory Provisioning Integration Service は、それらの変更のみをアプリケーションに通知します。

図 34-1 に、Oracle Directory Provisioning Integration Service 環境でのコンポーネント間の関係を示します。

図 34-1 Oracle Directory Provisioning Integration Service 環境の典型的な配置

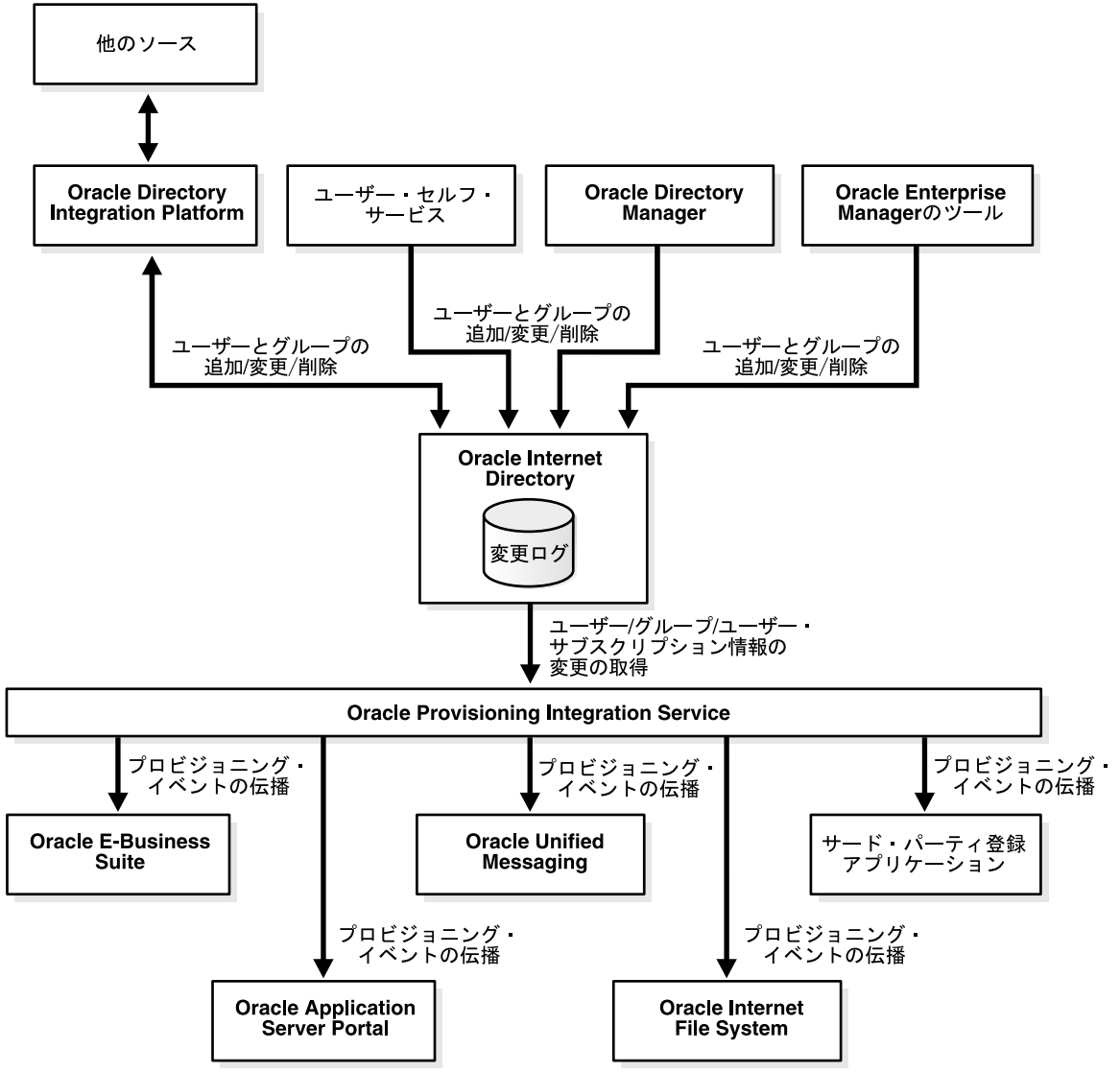


図 34-1 は、次のことを示しています。

- Oracle Internet Directory は、ユーザー、グループおよびユーザー・サブスクリプションに関するすべての情報の中央リポジトリとして機能します。
- 様々なコンポーネントが Oracle Internet Directory 内のユーザー、グループおよびユーザー・サブスクリプションのエントリを追加、変更または削除できます。これらのコンポーネントは、次のとおりです。
  - Oracle Human Resources や他のリポジトリなどと同期している Oracle Directory Integration and Provisioning Platform
  - Oracle Delegated Administration Services
  - Oracle Directory Manager
  - Oracle Enterprise Manager のツール（Enterprise Security Manager など）

  Oracle Internet Directory の変更ログには、これらの変更が記録されます。
- Oracle Directory Provisioning Integration Service は、ユーザー、グループおよびユーザー・サブスクリプションの情報への変更を Oracle Internet Directory から取得します。サブスクライブされたアプリケーションにこれらの変更を送信します。この図にあるアプリケーションは、OracleAS Portal、Oracle Unified Messaging、Oracle Content Management Software Development Kit およびサード・パーティ登録アプリケーションです。

アプリケーションを Oracle Directory Provisioning Integration Service に登録する方法

アプリケーションがインストールされ、Oracle Internet Directory 内にアプリケーションの識別情報が作成された後、次のいずれかの方法で、Oracle Directory Provisioning Integration Service によってアプリケーションを登録できます。

- アプリケーション自体がプロビジョニング・サブスクリプション・ツールを使用して、アプリケーションのインストール時に自動的に登録する。
- 管理者がプロビジョニング・サブスクリプション・ツールを使用して、手動で登録する。

これには次の登録情報が含まれます。

- Oracle ディレクトリ・サーバー・インスタンスのホスト名とポート番号
- Oracle Internet Directory ユーザーのユーザー名とパスワード
- Oracle Internet Directory にアプリケーションを登録するための情報
- Oracle Internet Directory にデータベース接続情報を登録するための情報
- Oracle Directory Provisioning Integration Service がアプリケーションにサービスを提供するための情報（必要な変更の種類やスケジューリング・プロパティなど）

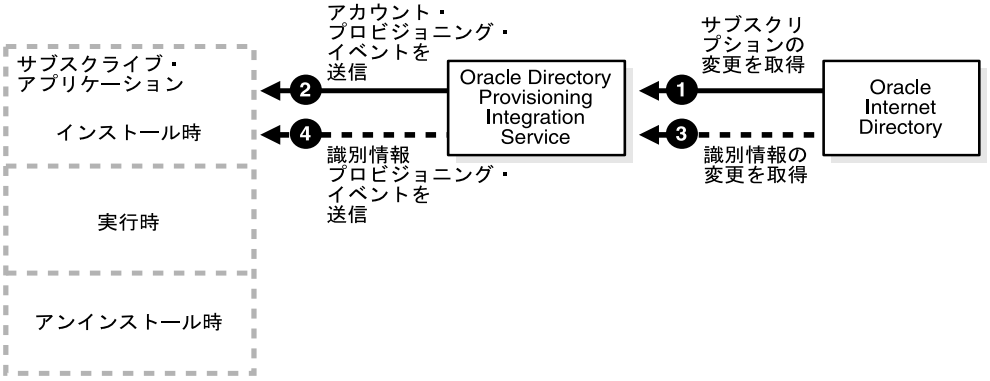
関連項目： プロビジョニング・サブスクリプション・ツールの使用方法は、付録 A「LDIF およびコマンドライン・ツールの構文」を参照してください。

アプリケーションが Oracle Internet Directory からプロビジョニング情報を受信する方法

Oracle Directory Provisioning Integration Service は、ユーザー、グループまたはユーザー・サブスクリプションの情報への変更について、Oracle Internet Directory を監視します。さらに、変更をプロビジョニング・イベントの形式でアプリケーションに伝達します。

図 34-3 に、アプリケーションが Oracle Internet Directory からプロビジョニング・イベントを受信する方法を示します。

図 34-2 アプリケーションが Oracle Directory Provisioning Integration Service を使用してプロビジョニング情報を受信する方法



プロビジョニング情報は、次のプロセスを使用して Oracle Internet Directory からアプリケーションへ送信されます。

1. Oracle Directory Provisioning Integration Service は、Oracle Internet Directory からそのアプリケーションに関するサブスクリプション情報への変更を取得します。
2. Oracle Directory Provisioning Integration Service は、サブスクリプション情報をアカウント・プロビジョニング・イベントに変換し、定期的にアプリケーションに送信します。この情報は、アプリケーション固有のデータベース接続情報に基づいています。
3. Oracle Directory Provisioning Integration Service は、識別情報についての情報への変更を Oracle Internet Directory から取得します。

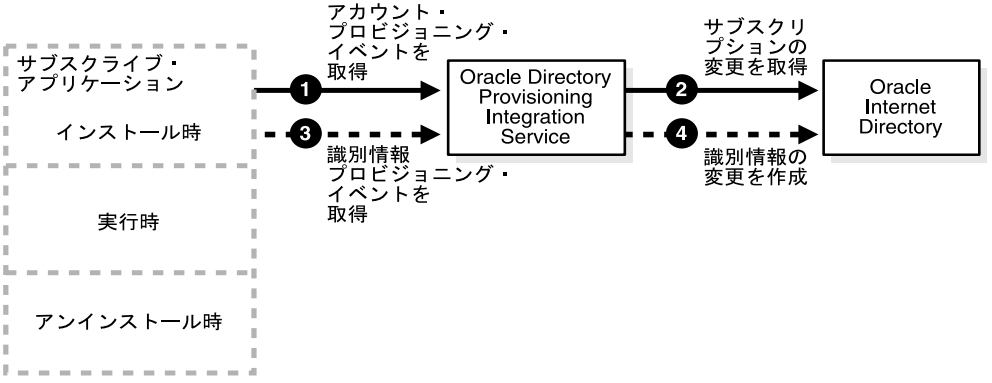
4. Oracle Directory Provisioning Integration Service は、識別情報に関する情報への変更を識別情報プロビジョニング・イベントに変換し、定期的にアプリケーションに送信します。

Oracle Internet Directory がアプリケーションからプロビジョニング情報を受信する方法

Oracle Internet Directory がアプリケーションからプロビジョニング情報を受信する方法は、アプリケーションが Oracle Internet Directory からプロビジョニング情報を受信する方法の逆です。プロセスについては、34-7 ページの「アプリケーションが Oracle Internet Directory からプロビジョニング情報を受信する方法」を参照してください。

図 34-3 に、アプリケーションが Oracle Internet Directory へプロビジョニング・イベントの通知を送信する方法を示します。

図34-3 Oracle Internet Directoryがアプリケーションからプロビジョニング情報を受信する方法



プロビジョニング情報は、次のプロセスを使用してアプリケーションから Oracle Internet Directory へ送信されます。

1. Oracle Directory Provisioning Integration Service は、アプリケーションからそのアプリケーションに関するアカウント・プロビジョニング・イベントを取得します。
2. Oracle Directory Provisioning Integration Service は、アカウント・プロビジョニング・イベントをサブスクリプション変更に変換し、定期的に Oracle Internet Directory に送信します。
3. Oracle Directory Provisioning Integration Service は、アプリケーションからそのアプリケーションに関する識別情報プロビジョニング・イベントを取得します。
4. Oracle Directory Provisioning Integration Service は、識別情報プロビジョニング・イベントを識別情報変更に変換し、定期的に Oracle Internet Directory に送信します。

Oracle Directory Provisioning Integration Service からのアプリケーション・サブスクライブを停止する方法

Oracle Directory Provisioning Integration Service からのアプリケーションのサブスクライブを次のいずれかの方法で停止することができます。

- アプリケーション自体が自動的にアンインストール
- プロビジョニング・サブスクリプション・ツールを使用して手動でサブスクライブを停止

関連項目： プロビジョニング・サブスクリプション・ツールの使用方法は、A-125 ページの「プロビジョニング・サブスクリプション・ツール（oidprovtool）の構文」を参照してください。

Oracle Directory Provisioning Integration Service 環境の管理

この項では、次の項目について説明します。

概要 : Oracle Directory Provisioning Integration Service の配置

Oracle Directory Provisioning Integration Service を配置するには、一般的に次の手順を実行します。

1. Oracle Internet Directory（Oracle Directory Integration and Provisioning Platform を含む）をインストールし、ユーザー情報をロードします。
2. Oracle Directory Integration and Provisioning Server（odisrv）が起動されていることを確認します。
3. アプリケーションをインストールし、プロビジョニング・サブスクリプション・ツールによるプロンプトに従って、アプリケーションによる Oracle Directory Provisioning Integration Service のサブスクライブに必要な情報を指定します。この情報によって、アプリケーションはプロビジョニング・イベントを受信できます。
4. 各アプリケーションについて、プロビジョニング・イベント伝播のステータスを定期的に監視します。これは、Oracle Enterprise Manager Application Server Control を使用して実行できます。

関連項目： 10-17 ページの「Oracle Internet Directory サーバーの監視」

Oracle Directory Provisioning Integration Service の管理

この項では、次の項目について説明します。

- Oracle Directory Integration and Provisioning Server の管理方法
- プロビジョニング・プロファイルの管理方法

Oracle Directory Integration and Provisioning Server の管理

Oracle Directory Integration and Provisioning Server は、Oracle Directory Provisioning Integration Service を実行して、プロビジョニング・イベントをサブスクライブ・アプリケーションに伝播します。

注意： Oracle Directory Integration and Provisioning Server をデフォルト・モードで起動すると、Oracle Directory Provisioning Integration Service のみがサポートされ、Oracle Directory Synchronization Service はサポートされません。

関連項目： Oracle Directory Integration and Provisioning Server の管理方法は、35-6 ページの「Oracle Directory Integration and Provisioning Server の管理」を参照してください。

プロビジョニング・プロファイルの管理

プロビジョニング・サブスクリプション・ツールを使用して、次の操作を実行します。

- 新規プロビジョニング・プロファイルの作成。作成された新規プロビジョニング・プロファイルは、Oracle Directory Integration and Provisioning Platform で処理できるように、使用可能な状態に設定されます。
- 既存のプロビジョニング・プロファイルの変更
- 既存のプロビジョニング・プロファイルの有効化または無効化
- 既存のプロビジョニング・プロファイルの削除。
- 指定したプロビジョニング・プロファイルの現行ステータスの取得。
- 既存のプロビジョニング・プロファイル内にあるすべてのエラーの消去。

プロビジョニング・プロファイルの監視には、Oracle Enterprise Manager Application Server Control の OID サーバー管理機能を使用します。

関連項目： 詳細は、次のドキュメントを参照してください。

- A-125 ページの「プロビジョニング・サブスクリプション・ツール（oidprovtool）の構文」
- Oracle Enterprise Manager オンライン・ヘルプ

セキュリティと Oracle Directory Provisioning Integration Service

この項では、プロビジョニング統合プロセスの主要なエンティティ、および様々な操作の実行に必要な権限について説明します。次の項目について説明します。

- プロビジョニング・プロファイルへのアクセス制御の必要性
- アクセス権限が必要なエンティティ
- エンティティに付与されるエントリ・レベルの権限
- エンティティに付与される属性レベルの権限

プロビジョニング・プロファイルへのアクセス制御の必要性

アプリケーションのプロビジョニング・プロファイルへのアクセスを制御することには、次の重要な理由があります。

- これらのプロファイルには、アプリケーションに関する機密情報（不正なディレクトリ・エントリに表示してはならない情報）が含まれています。
- プロビジョニング・イベントをアプリケーションに提供することによって、システム・リソースが消費されます。したがって、アプリケーションをプロビジョニングできる人数を制限する必要があります。

アクセス権限が必要なエンティティ

プロファイルの操作に関してエンティティに付与するアクセス権限は、そのアプリケーションの委任ニーズによって異なります。プロビジョニング・プロファイルに対する制御付きアクセス権限が必要なエンティティは、次のとおりです。

- Oracle Directory Integration and Provisioning Server グループ（つまり、`cn=odisgroup,cn=odi,cn=oracle internet directory`）
- プロビジョニング管理者（つまり、`cn=Provisioning Admins, cn=Provisioning Profiles...`）
- アプリケーション・エンティティ（つまり、`orclGUID` 属性の値が `orclODIPProvisioningAppGUID` のユーザー）

- プロビジョニング・プロファイル（つまり、プロビジョニング・プロファイルの識別名で識別されるユーザー）
- 他のすべてのユーザー

プロビジョニング・プロファイルの作成権限がアプリケーションで自動的に用意されることはありません。作成できるのは、プロビジョニング・プロファイルの管理権限を持つ LDAP ID のみです。

プロビジョニング管理者はグループとしてモデル化され、プロビジョニング・プロファイルに関する操作すべてを実行できます。他のすべての識別情報が持つ権限は、より小規模な内容です。

エンティティに付与されるエントリ・レベルの権限

表 34-1 に、各エンティティに付与されるエントリ・レベルの権限を示します。

表 34-1 エントリ・レベルの権限

ユーザー・カテゴリ	参照	追加	削除	説明
Oracle Directory Integration and Provisioning Server	はい	いいえ	はい	Oracle Directory Integration and Provisioning Server には、次の操作を行う権限が必要です。 ■ 全プロビジョニング・プロファイルの参照 ■ アプリケーションで削除しきれなかった半端なプロビジョニング・プロファイルの削除 ただし、Oracle Directory Integration and Provisioning Server には、新規プロビジョニング・プロファイルを追加する権限を指定しないでください。
プロビジョニング管理者	はい	はい	はい	プロビジョニング管理者グループには、すべての権限が必要です。
アプリケーション・エンティティ	はい	いいえ	はい	アプリケーション・エンティティ自体では、プロビジョニング・プロファイルの作成も、別のアプリケーションのプロファイルの参照もできません。ただし、プロファイルの作成後は、そのアプリケーション・エンティティ自体のプロファイルを参照、変更および削除することはできます。
プロビジョニング・プロファイル	はい	いいえ	いいえ	プロビジョニング・プロファイルにも、ディレクトリ内に識別情報があります。10*g*（9.0.4）の場合、この識別情報は使用されません。したがって、プロビジョニング・プロファイルには自己参照の実行権限のみがあります

表 34-1 エントリ・レベルの権限（続き）

ユーザー・カテゴリ	参照	追加	削除	説明
他のすべてのユーザー	いいえ	いいえ	いいえ	他のすべてのユーザーは、プロビジョニング・プロファイルの参照、追加または削除ができないようにしてください。

エンティティに付与される属性レベルの権限

プロビジョニング・プロファイルには、不正なアクセスからの保護を必要とする、セキュリティ上重要な属性が含まれています。表 34-2 にその属性を示します。

表 34-2 エンティティに付与される属性レベルの権限

属性	説明
`userpassword`	ディレクトリ・ユーザー・パスワードを格納します。
`orclPasswordAttribute`	クリア・テキスト・バージョンのディレクトリ・ユーザー・パスワードを格納します。
`orclODIPProfileInterfaceConnectInformation`	ターゲット・システムに対するパスワードも含め、ターゲット・アプリケーションへの接続情報の詳細を格納します。
`orclODIPProfileInterfaceAdditionalInformation`	インタフェース固有の情報を格納します。

表 34-3 に、保護属性のアクセス制御を示します。この制御は、プロビジョニング・プロファイルを操作する主なエンティティに対するものです。

表 34-3 保護属性のアクセス制御

ユーザー・カテゴリ	読取り	書込み	検索	比較	説明
Oracle Directory Integration and Provisioning Server	はい	いいえ	はい	はい	Oracle Directory Integration and Provisioning Server は、保護属性にアクセスして、処理サイクルを完了する必要があります。ただし、これらの属性の制御は、アプリケーション・エンティティおよびプロビジョニング管理者によってのみ行われるため、Oracle Directory Integration Server には書込みアクセス権は不要です。
プロビジョニング管理者	はい	はい	はい	はい	プロビジョニング管理者は統合上の問題を解決する必要があり、保護属性に対する完全なアクセス権限が必要です。

表 34-3 保護属性のアクセス制御（続き）

ユーザー・カテゴリ	読取り	書込み	検索	比較	説明
アプリケーション・エンティティ	はい	はい	はい	はい	アプリケーション・エンティティは保護属性の実際の所有者であるため、保護属性に対する完全なアクセス権限が必要です。
プロビジョニング・プロファイル	はい	いいえ	はい	いいえ	プロビジョニング・プロファイルは、これらの属性の書込みまたは比較を行う必要はありません。したがって、必要な権限は読取りと検索の権限のみです。
他のすべてのユーザー	いいえ	いいえ	いいえ	いいえ	他のすべてのユーザーには、権限が付与されません。

表 34-4 に、プロビジョニング・プロファイルのその他すべての属性に対するアクセス制御を示します。

表 34-4 他のすべての属性に対するアクセス制御

ユーザー・カテゴリ	読取り	書込み	検索	比較
Oracle Directory Integration and Provisioning Server	はい	はい	はい	はい
プロビジョニング管理者	はい	はい	はい	はい
アプリケーション・エンティティ	はい	はい	はい	はい
プロビジョニング・プロファイル	はい	はい	はい	はい
他のすべてのユーザー	いいえ	いいえ	いいえ	いいえ

保護属性とは異なり、その他の属性には比較的緩やかなアクセス制御が必要です。プロビジョニング・プロセスに関係するすべてのエンティティ（Oracle Directory Integration and Provisioning Server、プロビジョニング管理者、アプリケーション・エンティティおよびプロビジョニング・プロファイル）に完全なアクセス権が付与されます。他のすべてのユーザーには、これらの属性に対するアクセス権は付与されません。

Oracle Directory Provisioning Integration Service に関するトラブルシューティング

この項では、表示されるプロビジョニング・エラー・メッセージを示し、その解決策について説明します。これらのエラー・メッセージは、プロビジョニング・エラー・メッセージ属性に表示されます。

表 34-5 プロビジョニング・エラー・メッセージ

メッセージ	原因	対処方法
LDAP Connection Failure	Oracle Directory Integration and Provisioning Platform がディレクトリ・サーバーへの接続に失敗しました。	ディレクトリ・サーバーへの接続をチェックしてください。 **関連項目：**ディレクトリ・サーバーの接続については、5-13 ページの「アクティブ・サーバー・インスタンスの情報の表示」を参照してください。
LDAP Authentication Failure	管理者権限で、プロビジョニング・プロファイルを LDAP サーバーに接続できません。	ディレクトリの Oracle Directory Integration and Provisioning Server エントリを確認してください。`odisrvreg` を使用して Oracle Directory Integration and Provisioning Server を再登録します。 **関連項目：**35-13 ページの「Oracle Directory Integration and Provisioning Server の手動登録」を参照してください。
Initialization Failure	JNDI を使用してディレクトリ・サーバーに接続する際の問題です。	次の場所にあるトレース・ファイルまたは監査ファイルを調査してください。 `$ORACLE_HOME/ldap/odi/log/PROFILE_NAME.trc`
Database Connection Failure	指定のアカウント情報を使用してデータベースに接続する際の問題です。データベースが実行されていないか、または認証上問題があります。	次の場所にあるトレース・ファイルまたは監査ファイルを調査してください。 `$ORACLE_HOME/ldap/odi/log/PROFILE_NAME.trc`
Exception while calling SQL Operation	パッケージを実行する際の問題です。	パッケージの有用性を検査してください。 次の場所にあるトレース・ファイルまたは監査ファイルを調査してください。 `$ORACLE_HOME/ldap/odi/log/PROFILE_NAME.trc`

プロビジョニング統合プロファイル・ステータス情報の監視

Oracle Enterprise Manager Application Server Control から、特定のプロビジョニング統合プロファイル・ステータス情報を監視できます。

LDAP のメイン・ページから「Directory Integration Server」を選択します。必要なパッケージが正しくインストールされている場合、これは常に緑色になります。これは、Oracle Directory Integration and Provisioning Server が実行中かどうかを示すものではありません。サーバーのステータスをチェックする場合は、「統合」を選択します。

次のウィンドウでは、Oracle Enterprise Manager Application Server Control が、プロビジョニング用と同期用のものも含め、Directory Integration Platform Server の様々な実行中インスタンスを表示します。プロビジョニング統合プロファイルに関してこのウィンドウに表示される主なデータは次のとおりです。

- サブスクライブしたアプリケーションの名前
- サブスクリプションが行われた企業の名前
- プロファイルのステータス（ENABLED または DISABLED）
- このプロファイルのかわりにイベントがアプリケーションに伝播された Oracle Internet Directory 内の変更番号
- 最終実行時間
- プロファイルの最終成功実行時間
- エラー（存在する場合）

現在、このウィンドウにはこのプロファイルに関する様々なイベント・サブスクリプションは表示されません。

`status` 動作引数を指定して、`$ORACLE_HOME/bin/oidprovtool` コマンドラインを実行することで、プロビジョニング統合ステータスについての詳細出力を取得することもできます。

35

Oracle Directory Integration and Provisioning Server の管理

この章では、Oracle Directory Integration and Provisioning Server について説明し、その構成方法と管理方法を示します。この項では、次の項目について説明します。

Oracle Directory Integration and Provisioning Server の概要

Oracle Directory Integration and Provisioning Server は、Oracle Directory Integration and Provisioning Platform の中心的なコンポーネントです。次のことを行います。

- コネクタのスケジューリング

  Directory Integration and Provisioning Server は、Oracle Internet Directory と接続ディレクトリの間の同期用にコネクタをスケジューリングします。エージェントがある場合は、エージェントの実行時間もスケジューリングします。

- データのインポートとエクスポート

  Directory Integration and Provisioning Server は、Oracle Internet Directory との間で変更をインポートおよびエクスポートします。DB、LDAP、LDIF およびタグ付きの各インタフェースがサポートされます。

- マッピング

  Oracle Directory Integration and Provisioning Server には、接続ディレクトリとの間でデータをフィルタ処理し、マッピングする一般的な機能が組み込まれています。Directory Integration and Provisioning Server は、接続ディレクトリへのデータのエクスポート時、およびファイルまたはディレクトリから Oracle Internet Directory に入力するためにインポートしたデータの解析時に、属性をマップします。

Oracle Directory Integration and Provisioning Server は、同期化とプロビジョニングの両方の機能を実行します。複数の Directory Integration and Provisioning Server のインスタンスをホスト上で実行できます。

Oracle Directory Integration and Provisioning Server の操作情報

この項では、Directory Integration and Provisioning Server の構造および操作方法について説明します。次の項目について説明します。

- Oracle Directory Integration and Provisioning Server と構成設定エントリ
- Directory Integration and Provisioning Server イベントの標準の順序
- Oracle Directory Integration and Provisioning Server が使用する構成設定エントリの管理

Oracle Directory Integration and Provisioning Server と構成設定エントリ

各 Directory Integration and Provisioning Server は、次のいずれかの操作を行うためにコネクタ・セットを実行できます。

- Oracle Internet Directory と接続ディレクトリとの同期化。同期用のコネクタ・セットは、Oracle Directory Integration and Provisioning Server の起動時にコマンドラインに入力した構成設定番号で用意されます。
- Oracle コンポーネント用のユーザー、グループおよびレルムのプロビジョニング。プロビジョニング用のプロファイル・セットは、Oracle Directory Integration and Provisioning Server の起動時にコマンドラインに入力した `groupID` 引数で用意されます。

構成設定番号を指定しない場合、Directory Integration and Provisioning Server はプロビジョニング・プロファイル処理用のモードで起動します。構成設定番号を指定し、その構成設定番号用のディレクトリに統合プロファイルがない場合、Directory Integration and Provisioning Server は、その構成設定に統合プロファイルが追加されるまで無期限に待機します。この無期限待機は、構成設定に指定されている統合プロファイルが使用禁止になっている場合にも発生します。

コマンドラインで指定した構成設定がディレクトリ内に存在しない場合、Directory Integration and Provisioning Server は、この情報をログ・ファイルに記録して終了します。プロビジョニング・プロファイルの場合、コマンドラインで引数として渡される `groupID` 属性に関して同じ動作になります。

コネクタによる同期またはプロビジョニングがスケジューリングされている場合、常に、Directory Integration and Provisioning Server は別のスレッドを起動します。このスレッドは、Oracle Internet Directory からのエントリの読取りまたは書込みを実行するため、ディレクトリ・サーバーへの LDAP 接続をオープンし、終了前にこの接続をクローズします。

Directory Integration and Provisioning Server は、表 35-1 に示す 3 種類のスレッドをプロセス内で実行します。

表 35-1 Oracle Directory Integration and Provisioning Server のスレッド

スレッド	説明
メイン・スレッド	Oracle Directory Integration and Provisioning Server のデーモン・スレッド。このスレッドは、起動したスケジューラに更新シグナルを定期的に送信し、変更されたプロファイルを検索してスケジューラのキャッシュを更新します。このスレッドは、OID モニター（`oidmon`）による停止シグナルも検索します。この停止シグナルによって、スケジューラに停止シグナルを送信した後、スレッド自体が停止します。
スケジューラ・スレッド	指定されたスケジューリング間隔に基づいた同期用のコネクタのスケジューラ。このスレッドは、メイン・スレッドから更新シグナルを受信すると、同期プロファイルを最新の値に更新します。

表 35-1 Oracle Directory Integration and Provisioning Server のスレッド（続き）

スレッド	説明
コネクタ・スレッド	同期化において、プロファイル内で固有の名前を持つ実行可能なコネクタを起動し、属性をマッピングおよびフィルタ処理するスレッド。指定されたスケジュール間隔でスケジューラによって生成されます。ソース・ディレクトリからの変更がすべて宛先ディレクトリに伝播された後、このスレッドは終了します。

Directory Integration and Provisioning Server イベントの標準の順序

Oracle Directory Integration and Provisioning Server の各インスタンスによって、プロビジョニングまたは同期がサポートされます。Directory Integration and Provisioning Server は、同期とプロビジョニングのイベント伝播を処理するときに、共有サーバー・プロセスとして動作します。

35-3 ページの表 35-1 で説明した 3 つのスレッドは相互に機能して、次の一般的なプロセス・フローの順序を作成します。

- メイン・スレッド・プロセスの順序
- スケジューラ・スレッド・プロセスの順序
- 同期用のコネクタ・スレッド・プロセスの順序
- プロビジョニング用のコネクタ・スレッド・プロセスの順序

メイン・スレッド・プロセスの順序

起動時に、メイン・スレッドが起動されます。これはサーバーのデーモン・スレッドであり、スケジューラを起動します。ディレクトリ内のインスタンスの登録が検証されます。インスタンスが登録されていない場合、OID モニターからは起動されません。かわりに、構成設定番号とインスタンス番号の詳細を Oracle Internet Directory に自身で登録します。

メイン・スレッドは更新時期を定期的にチェックし、更新することをスケジューラに通知します。また、停止シグナルを定期的にチェックします。停止シグナルを受信すると、停止することをスケジューラ・スレッドに通知します。

スケジューラ・スレッドが停止すると、メイン・スレッドは登録を解除し、停止します。

スケジューラ・スレッド・プロセスの順序

スケジューラ・スレッドは、メイン・スレッドによって起動されると、構成設定を読み取り、スケジューリングを行う統合プロファイルを判断します。スケジューリング対象プロファイルのリストを作成し、指定されたスケジューリング間隔に基づいてスケジュールを設定します。プロファイルのリストを作成する間に、属性の妥当性をチェックします。プロファイル属性に無効な値がある場合、そのプロファイルは、同期またはプロビジョニングの対象となりません。

更新シグナルを受信したスケジューラ・スレッドは、統合プロファイルを更新します。スケジューラ・スレッドは停止シグナルを受信すると、すべてのコネクタが同期またはプロビジョニングのイベント伝播を完了するまで待機します。その後、メイン・スレッドに制御を戻します。

同期用のコネクタ・スレッド・プロセスの順序

同期スレッドは次のプロセスに従います。

1. 接続ディレクトリおよび Oracle Internet Directory との接続を確立します。
2. インポート操作では、コネクタに指定されているエージェント実行コマンドを実行します。
3. 必要に応じて、DB/LDAP/LDIF/ タグ付きファイルを開きます。
4. ソースから 1 つずつ変更を読み取ります。
5. 適用可能な場合、変更をフィルタ処理します。
6. マッピング・ルールの指定に従って変更をマップします。
7. 宛先変更レコードを作成します。
8. 変更を宛先に書き込みます。
9. すべての変更を適用した後、スレッドを閉じます。

プロビジョニング用のコネクタ・スレッド・プロセスの順序

プロビジョニング・スレッドは次のプロセスに従います。

1. 接続ディレクトリとの接続を確立します。
2. ソースから 1 つずつ変更を読み取ります。
3. 適用可能な場合、変更をフィルタ処理します。
4. 変更を次の特定のイベントとして識別します。
   - USER 追加 / 変更 / 削除
   - GROUP 追加 / 変更 / 削除
5. イベント通知レコードを作成します。
6. イベント通知をコンシュームする所定のパッケージを起動します。

Oracle Directory Integration and Provisioning Server の管理

この項では、次の項目について説明します。

- Oracle Directory Integration and Provisioning Server の情報の表示
- Oracle Directory Integration and Provisioning Server が使用する構成設定エントリの管理
- Oracle Internet Directory および接続ディレクトリの SSL 証明書の管理
- Oracle Directory Integration and Provisioning Server の起動、停止および再起動
- 高可用性を目的とした使用例での Oracle Directory Integration and Provisioning Server の起動と停止
- Oracle Directory Integration and Provisioning Server に対するデバッグ・レベルの設定
- レプリケート環境での Oracle Directory Integration and Provisioning Platform の管理
- ログ・ファイルの検索

注意： セキュリティ上の理由により、オラクル社はディレクトリ・サーバーと同じホスト上で Oracle Directory Integration and Provisioning Server を実行することをお薦めします。別のホスト上で実行する場合は、第 13 章「Secure Sockets Layer（SSL）とディレクトリ」で説明したとおり、SSL を使用して実行してください。

Oracle Directory Integration and Provisioning Server の情報の表示

Directory Integration and Provisioning Server は、起動時に固有の実行時情報を生成し、ディレクトリ内に格納します。これには次の情報が含まれます。

- Directory Integration and Provisioning Server のインスタンス番号
- 実行されているホスト
- Directory Integration and Provisioning Server の起動に使用された構成設定
- 実行中のプロビジョニング・プロファイル・グループのグループ識別子

Oracle Directory Manager または ldapsearch のいずれかを使用することで、この情報を表示できます。

Oracle Directory Manager を使用した Oracle Directory Integration and Provisioning Server の実行時情報の表示

Oracle Directory Manager を使用して Directory Integration and Provisioning Server インスタンスの実行時情報を表示する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**、「**サーバー管理**」の順に展開します。
2. 「**統合サーバー**」を選択します。右側のペインに「アクティブ・プロセス」ボックスが表示されます。
3. Directory Integration and Provisioning Server インスタンスを選択し、「**プロパティの表示**」を選択します。「サーバー・プロセス」ダイアログ・ボックスに情報が表示されます。

ldapsearch を使用した Oracle Directory Integration and Provisioning Server の実行時情報の表示

ldapsearch を使用して Directory Integration and Provisioning Server インスタンスの登録情報を表示するには、エントリでベース検索を実行します。次に例を示します。

```
ldapsearch -p 389 -h my_host -b cn=instance1,cn=odisrv,cn=subregistrysubentry -s
base -v "objectclass=*"
```

この例の検索では、次の情報が戻されます。

```
dn: cn=instance1,cn=odisrv,cn= subregistrysubentrycn: instance1orclodipconfigdns:
orclodipagentname=HRAgent,cn=subscriber profile,cn=changelog subscriber,cn=oracle
internet directory
orcldiaconfigrefreshflag: 0
orclhostname: my_host
orclconfigsetnumber: 1
objectclass: top
objectclass: orclODISInstance
```

Oracle Directory Integration and Provisioning Server が使用する構成設定エントリの管理

構成設定エントリを作成、変更および削除するには、Oracle Directory Manager または対応するコマンドライン・ツールを使用します。コネクタが登録されると、統合プロファイルが作成され、所定の構成設定に追加されます。構成設定エントリは、Directory Integration and Provisioning Server の動作を決定します。

Directory Integration and Provisioning Server の起動時に異なる構成設定エントリを使用することによって、Directory Integration and Provisioning Server の実行時動作を制御できます。たとえば、ホスト H1 の Directory Integration and Provisioning Server のインスタンス 1 を configset1 で起動し、ホスト H1 のインスタンス 2 を configset2 で起動することができます。インスタンス 1 の動作は configset1 に依存し、インスタンス 2 の動作は configset2 に依存します。ホスト H1 上のエージェントを 2 つの構成設定エントリに分割すると、2 つの Directory Integration and Provisioning Server インスタンスに負荷が分散されます。同様に、異なるホスト上で異なる構成設定とインスタンスを実行すると、サーバー間で負荷のバランスをとることができます。

Oracle Internet Directory および接続ディレクトリの SSL 証明書の管理

Oracle Internet Directory と接続ディレクトリの接続に使用される証明書は、Oracle Wallet Manager を使用して Wallet に保存されます。

> **関連項目：**『Oracle Advanced Security 管理者ガイド』の Oracle Wallet Manager についての章

Wallet の場所および Wallet を開くためのパスワードは、Oracle Directory Integration and Provisioning Platform が使用するプロパティ・ファイルに保存されます。これは、次のファイルです。

`$ORACLE_HOME/ldap/odi/conf/odi.properties`

典型的な `odi.properties` ファイルには、表 35-2 に示すエントリがあります。

表 35-2　odi.properties ファイルのエントリ

エントリ	説明
`RegWalletFile: odi/conf/srvWallet`	このエントリは、Oracle Internet Directory を使用して Oracle Directory Integration and Provisioning Platform の登録情報の場所を示します。ファイルの位置は、`$ORACLE_HOME/ldap` 関連のディレクトリです。
`CertWalletFile: location_of_certificate_wallet`	証明書 Wallet の位置。
`CertWalletPwdFile: location_of_certificate_wallet_password_file`	固有ファイルに暗号化形式で保存されている証明書 Wallet パスワード・ファイルの位置。 **関連項目：** 第 13 章「Secure Sockets Layer（SSL）とディレクトリ」 A-106 ページの「Directory Integration and Provisioning Assistant」

すべてのファイル位置は絶対パス名です。証明書 Wallet ファイルは、ewallet.p12 ファイルの位置です。

たとえば、odi.properties ファイルの内容は次のとおりです。

```
RegWalletFile:  /private/myhost/orahome/ldap/odi/conf
CertWalletFile:  /private/myhost/orahome/ldap/dipwallet
CertWalletPwdFile: /private/myhost/orahome/ldap/
```

この例では、Wallet ファイル ewallet.p12 は、ディレクトリ /private/myhost/orahome/ldap/dipwallet にあります。

Oracle Directory Integration and Provisioning Server の起動、停止および再起動

この項では、Oracle Directory Integration and Provisioning Server の起動、停止および再起動について説明します。

Oracle Directory Integration and Provisioning Server の起動

Oracle Directory Integration and Provisioning Server の起動方法は、インストールが一般的な Oracle Internet Directory 環境か Oracle Directory Integration and Provisioning Platform のみの環境かによって異なります。

関連項目： A-11 ページの「Oracle Directory Integration and Provisioning Server の起動」

Oracle Directory Integration and Provisioning Server の停止

Directory Integration and Provisioning Server の停止方法は、起動に使用したツールによって異なります。

関連項目： A-15 ページの「Oracle Directory Integration and Provisioning Server の停止」

Oracle Directory Integration and Provisioning Server の再起動

OID モニターと OID 制御ユーティリティを使用する場合は、Directory Integration and Provisioning Server の停止および再起動の両方を 1 つのコマンド RESTART で行うことができます。予定の更新時刻を待たず、サーバーのキャッシュを即時に更新する場合は、この方法が便利です。Directory Integration and Provisioning Server は、再起動時に停止前と同じパラメータを維持します。

関連項目： A-16 ページの「Oracle Internet Directory サーバー・インスタンスの再起動」

高可用性を目的とした使用例での Oracle Directory Integration and Provisioning Server の起動と停止

Oracle Directory Integration and Provisioning Server は、一定の制限付きで、高可用性を目的とした様々な使用例で実行できます。ここでは、Real Application Clusters 環境およびコールド・フェイルオーバー構成で運用する Oracle Directory Integration and Provisioning Server について説明します。

Real Application Clusters 環境での Oracle Directory Integration and Provisioning Server

Oracle Internet Directory インフラストラクチャは、Real Application Clusters モードで動作するように構成されます。Real Application Clusters では、Oracle Directory Integration and Provisioning Server は、すべてのディレクトリ・ノードに対して実行できます。

個々の構成設定は、Oracle Directory Integration and Provisioning Server の 1 つのインスタンスのみによって実行されます。このため、デフォルトのインストール中は、1 つのサーバー・インスタンス（つまりインスタンス 1）のみが、Real Application Clusters のマスター・ノードで起動されます。このサーバー・インスタンスは、構成設定 0 を実行します。そのサーバー・インスタンスはマスター・ノード上でのみ起動されますが、そのサーバーはすべてのノード上に登録されます。

マスター・ノードで障害が発生した場合は、2 次ノードの OID モニターによって、Oracle Directory Integration and Provisioning Server インスタンスが起動されます。複数の 2 次ノードが存在する場合は、1 番目の OID モニターによってサーバーが起動され、マスター・ノードに障害が発生したことが認識されます。

サーバーの起動時、OID モニターは、マスター・ノードで使用されていたものと同じインスタンス番号および構成設定を使用します。これは、エンド・ユーザーに対して透過的に行われ、一度、マスター・ノードと同じインスタンス番号および構成設定が使用されると、2 次ノードの Oracle Directory Integration and Provisioning Server がプライマリ・サーバーとして動作します。サーバーは、セカンダリ・ノードが使用可能であるかぎり、2 次ノード上での実行を継続します。

2 つのノードで実行されている別々の Oracle Directory Integration and Provisioning Server インスタンスは、同じ構成設定を同時に実行することはできません。OID モニターは、これをチェックしませんが、Oracle Directory Integration and Provisioning Server 自体が起動に失敗します。

OID 制御ユーティリティを使用すると、いつでも Oracle Directory Integration and Provisioning Server を停止できます。ただし、停止すると、他のノードでそのサーバーを自動的に起動することはできません。別のノードでサーバーを起動するには、OID 制御ユーティリティを使用して手動で起動してください。

コマンド `opmnctl stopall` を実行した後、`opmnctl startall` を実行すると、Oracle Directory Integration and Provisioning Server が起動します。

つまり、OID 制御コマンドによって Oracle Directory Integration and Provisioning Server を停止しないかぎり、OID モニターによって、常にサーバーが実行されていることになります。

コールド・フェイルオーバー構成での Oracle Directory Integration and Provisioning Server

Oracle Internet Directory インフラストラクチャは、コールド・フェイルオーバー構成モードで動作するように構成されます。Oracle Directory Integration and Provisioning Server は、アクティブ・ノードで実行します。

アクティブ・ノードに障害が発生した場合は、スタンバイ・ノードの OID モニターが、スタンバイ・ノードの Oracle Directory Integration and Provisioning Server インスタンスを起動します。この場合、以前アクティブ・ノードで使用されていたものと同じインスタンス番号および構成設定がスタンバイ・ノードで使用されます。これは、エンド・ユーザーに対して透過的です。アクティブ・ノードが使用可能であるかぎり、アクティブ・ノード上で実行を継続します。コールド・フェイルオーバー構成ではサーバーは、仮想ホスト名がアクティブ・ノードとスタンバイ・ノードの両方で同一であるため、サーバーは一度に両方に登録されます。

OID 制御ユーティリティを使用すると、いつでも Oracle Directory Integration and Provisioning Server を停止できます。ただし、停止すると、このノードでそのサーバーを再度起動することはできません。さらに、このノードがフェイルオーバーされると、スタンバイ・ノードの OID モニターは、Oracle Directory Integration and Provisioning Server を起動しません。サーバーを起動するには、OID 制御ユーティリティを使用する必要があります。

コマンド `opmnctl stopall` を実行した後、`opmnctl startall` を実行すると、Oracle Directory Integration and Provisioning Server が起動します。

つまり、OID 制御コマンドによって Oracle Directory Integration and Provisioning Server を停止しないかぎり、OID モニターによって、常にサーバーが実行されていることになります。

関連項目： 28-2 ページの「コールド・フェイルオーバー・クラスタ構成の概要」

Oracle Directory Integration and Provisioning Server に対するデバッグ・レベルの設定

Directory Integration and Provisioning Server の実行と各コネクタの実行は別々に制御できます。各種コネクタについても選択してデバッグを無効にすることができます。

サーバーの実行に関しては、サーバー・ログにトレースが保存されます。コネクタに関しては、各コネクタのトレース・ファイルにトレースが保存されます。

0（ゼロ）以外のデバッグ・レベルを指定すると、サーバー・ログ・ファイル内の各トレース文に次の種類のトレース文が含まれます。

- `Main`: コントローラ・スレッドからのメッセージ
- `Scheduler`: スケジューラ・スレッドからのメッセージ

表 35-3 サーバー・デバッグ用デバッグ・タイプ

デバッグ・イベント・タイプ	数値
異なるスレッドの起動と停止	1
詳細レベル : 更新の詳細の表示	2
コネクタの初期化、実行および終了の詳細	4
コネクタ実行時の詳細	8
コネクタの変更レコード	16
コネクタのマッピングの詳細	32
コネクタの実行時間の詳細	64

関連項目： スレッドを選択的にデバッグする方法については、33-18 ページの「同期プロファイルの管理」を参照してください。

デバッグ・フラグに値が設定されていない場合のデフォルト・レベルは `0`（ゼロ）で、35-12 ページの表 35-3 のいずれのデバッグ・イベントも記録されません。ただし、エラーと例外は常に記録されます。

コネクタをデバッグしない場合は、デバッグ値を `3` に設定します。

各コネクタのデバッグ・レベルは、プロファイル自身に設定することができます。

関連項目：

- 同期プロファイルのデバッグ属性の詳細は、B-18 ページの表 B-20 を参照してください。
- A-125 ページの「プロビジョニング・サブスクリプション・ツール（oidprovtool）の構文」

レプリケート環境での Oracle Directory Integration and Provisioning Platform の管理

プロビジョニングおよび同期化では、レプリケート・ディレクトリはマスター・ディレクトリと異なります。元のディレクトリで作成されたプロファイルを新しいディレクトリで再作成し、すべての構成を元のディレクトリと同様に実行する必要があります。

ログ・ファイルの検索

実行の詳細とデバッグ情報は、*$ORACLE_HOME*/ldap/log/odisrv*Instance_number*.log のログ・ファイルにあります。

たとえば、サーバーがサーバー・インスタンス番号 3 として起動された場合、ログ・ファイルのパス名は *$ORACLE_HOME*/ldap/log/odisrv03.log になります。

サーバー内のその他の例外は odisrv_jvm_*xxxx*.log ファイルにあります。この *xxxx* は、その表で Directory Integration and Provisioning Server を実行中のプロセスの識別子です。

プロファイル固有のデバッグ・イベントは、プロファイル固有のトレース・ファイル（*$ORACLE_HOME*/ldap/odi/log/*profile_name.trc*）に格納されます。

Oracle Directory Integration and Provisioning Server の手動登録

Oracle Directory Integration and Provisioning Platform のインストール時、Oracle Directory Integration and Provisioning Server は Oracle Internet Directory に登録されます。この登録により、指定されたホストが Oracle Directory Integration and Provisioning Platform の実行権限を持つことを示すフットプリントがディレクトリ内に作成されます。

クライアント側でこれを手動で登録する必要がある場合があります。たとえば、インストール中に障害が発生した場合などです。これは、Oracle Directory Integration and Provisioning Server 登録ツール（odisrvreg）または Oracle Enterprise Manager のいずれかを使用して実行できます。

Oracle Directory Integration and Provisioning Server 登録ツールの使用による Oracle Directory Integration and Provisioning Server の手動登録

各ホストにインストールされている各 Directory Integration and Provisioning Server は、そのホストで odisrvreg を実行して個別に登録する必要があります。このツールを実行するには、ディレクトリ・サーバーを管理する権限が必要になります。

関連項目：

- `oidsrvreg` の使用方法は、A-124 ページの「Oracle Directory Integration and Provisioning Server 登録ツール（odisrvreg）」を参照してください。
- 33-21 ページの「Oracle Directory Integration and Provisioning Platform での同期に関するトラブルシューティング」

Oracle Enterprise Manager Application Server Control の使用による Oracle Directory Integration and Provisioning Server の手動登録

Oracle Enterprise Manager Application Server Control を使用して Oracle Identity Management インフラストラクチャで Oracle Directory Integration and Provisioning Platform を構成できます。この場合、Application Server Control によって Oracle Directory Integration and Provisioning Server がこのインフラストラクチャに登録されます。

1. Application Server Control の Web サイトの「**スタンドアロン・インスタンス**」セクションで、Oracle Application Server インスタンスの名前を選択します。そのインスタンスに対応する画面が表示されます。
2. 「**コンポーネントの構成**」を選択します。「コンポーネントの選択」画面が表示されます。
3. 「**Oracle Directory Integration and Provisioning Platform**」を選択し、「**続行**」を選択します。「ログイン」画面が表示されます。
4. ディレクトリのスーパー・ユーザーのユーザー名とパスワードを入力します。デフォルトのユーザー名は `cn=orcladmin` です。
5. 「**終了**」を選択し、登録を完了します。

Oracle Directory Integration and Provisioning Server に関するトラブルシューティング

この項では、次の項目について説明します。

- インフラストラクチャのインストールでの Oracle Directory Integration and Provisioning Server に関するトラブルシューティング
- Oracle Directory Integration and Provisioning Platform のみのインストールでの Oracle Directory Integration and Provisioning Server に関するトラブルシューティング

インフラストラクチャのインストールでの Oracle Directory Integration and Provisioning Server に関するトラブルシューティング

Oracle Directory Integration and Provisioning Server の起動後、実行されているかどうかを確認する手順は、次のとおりです。

1. このプロセスが実行されていることを確認します。UNIX では、次のコマンドを使用して確認します。

   ```
   'ps -ef | grep odisrv'
   ```

   Windows では、このプロセスがタスク・バーに表示されているかどうかを確認します。

2. Oracle Directory Integration and Provisioning Server が実行されていない場合は、$*ORACLE_HOME*/ldap/log/oidmon.log を確認して起動されなかった原因を調べます。

3. ログ・ファイルにデータベース関連のエラーが表示されている場合は、次のように対処します。

   a. ORACLE_*SID* が設定されていることを確認します。ORACLE_*SID* が設定されていない場合は、値を設定します。

   b. ORACLE_*SID* に指定されている接続文字列が、$*ORACLE_HOME*/network/admin/tnsnames.ora ファイルに指定されていることを確認します。

   ログ・ファイルに、無効な構成設定番号またはサーバー・インスタンス番号などのエラーが表示された場合は、これらの引数に有効な値を指定します。

4. サーバー・インスタンス番号および構成設定番号が正しい場合は、ファイル $*ORACLE_HOME*/ldap/log/odisrv_xx.log（xx は、起動したインスタンスのインスタンス番号）を参照します。登録エラーが示されている場合は、odisrvreg を使用して Oracle Directory Integration and Provisioning Server を再登録します。

5. 手順 4 でエラーが発生していなかった場合は、ファイル $*ORACLE_HOME*/ldap/log/odisrv_jvm_yyy.log（yyy は、開始されている odisrv プロセスのプロセス識別子）を参照します。最新のタイムスタンプが含まれているファイルを検索します。

Oracle Directory Integration and Provisioning Platform のみのインストールでの Oracle Directory Integration and Provisioning Server に関するトラブルシューティング

Oracle Directory Integration and Provisioning Server の起動後、実行されているかどうかを確認する手順は、次のとおりです。

1. このプロセスが実行されていることを確認します。UNIX では、次のコマンドを使用して確認します。

   ```
   'ps -ef | grep odisrv'
   ```

   Windows では、このプロセスがタスク・バーに表示されているかどうかを確認します。

2. このプロセスが実行されていない場合は、ファイル *$ORACLE_HOME*/ldap/log/odisrv_xx.log（xx は、起動したインスタンスのインスタンス番号）を参照します。このログ・ファイルに登録エラーが示されている場合は、odisrvreg を使用して Oracle Directory Integration and Provisioning Server を再登録します。

3. 手順 2 でエラーが発生していなかった場合は、ファイル *$ORACLE_HOME*/ldap/log/odisrv_jvm_yyy.log（yyy は、開始されている odisrv プロセスのプロセス識別子）を参照します。最新のタイムスタンプが含まれているファイルを検索します。

36

Oracle Directory Integration and Provisioning Platform におけるセキュリティ

この章では、Oracle Directory Integration and Provisioning Platform のセキュリティにおける最も重要な事項について説明します。次の項目について説明します。

- Oracle Directory Integration and Provisioning Platform における認証
- アクセス制御、認可および Oracle Directory Integration and Provisioning Platform
- データの整合性と Oracle Directory Integration and Provisioning Platform
- データのプライバシと Oracle Directory Integration and Provisioning Platform
- ツール・セキュリティと Oracle Directory Integration and Provisioning Platform

Oracle Directory Integration and Provisioning Platform における認証

認証は、Oracle ディレクトリ・サーバーが、そのディレクトリに接続しているユーザーの正確な識別情報を取得するプロセスです。認証は、LDAP セッションが ldapbind 操作によって確立されたときに発生します。

Oracle Directory Integration and Provisioning Platform の各コンポーネントが、ディレクトリへのアクセスを許可される前に適切に認証されることは重要です。

この項では、次の項目について説明します。

Secure Sockets Layer（SSL）と Oracle Directory Integration and Provisioning Platform

Oracle Directory Integration and Provisioning Platform は、**Secure Sockets Layer（SSL）**を使用するかどうかにかかわらず配置できます。SSL の実装は、次のモードをサポートします。

- 認証なし－データの SSL 暗号化を提供しますが、認証には SSL を使用しません。
- SSL サーバー認証－データの SSL 暗号化とクライアントに対する SSL 認証の両方が含まれます。Oracle Directory Integration and Provisioning Platform では、サーバーはディレクトリ・サーバーであり、クライアントは Directory Integration and Provisioning Server です。

  サーバーは、信頼できる**認証局**が発行する**証明書**を送信することにより、クライアントに対する自己識別を行います。このモードには、公開鍵インフラストラクチャ（PKI）と証明書を保持するための SSL Wallet が必要です。

Oracle Directory Integration and Provisioning Platform で SSL を使用するには、Oracle ディレクトリ・サーバーと Oracle Directory Integration and Provisioning Server の両方を SSL モードで起動する必要があります。

> **関連項目：** SSL モードで Oracle ディレクトリ・サーバーを起動する方法は、第 3 章「事前に実行するタスクと情報」を参照してください。

Oracle Directory Integration and Provisioning Server の認証

Directory Integration and Provisioning Server は、複数のインスタンスを様々なホストにインストールし、実行できます。ただし、これを行う場合は、Directory Integration and Provisioning Server を装う不正なユーザーまたはその不正コピーを使用する不正なユーザーに注意する必要があります。

このようなセキュリティ問題を回避するには、次の点に注意します。

- 各 Directory Integration and Provisioning Server が正しく識別されていることを確認する。
- Directory Integration and Provisioning Server が Oracle Internet Directory へのアクセスを取得する前に正しく認証されていることを、Directory Integration and Provisioning Server の起動時に確認する。

非 SSL 認証

非 SSL 認証を使用するには、odisrvreg と呼ばれる登録ツールを使用して、各 Directory Integration and Provisioning Server を登録します。

この登録ツールでは、次のものを作成できます。

- ディレクトリ内の識別情報エントリ。Directory Integration and Provisioning Server は、ディレクトリにバインドするときにこのエントリを使用します。
- 暗号化されたパスワード。このパスワードは、Directory and Provisioning Integration Server エントリ内に格納されます。
- ローカル・ホストのプライベート Wallet。この Wallet には、暗号化されたパスワードを含むセキュリティ資格証明が含まれています。Wallet の名前は `odi.properties` ファイルに指定され、*`$ORACLE_HOME`*`/ldap/odi/conf` ディレクトリに格納されます。

Directory Integration and Provisioning Server は、ディレクトリにバインドするときにプライベート Wallet 内の暗号化されたパスワードを使用します。

注意： この Wallet は不正アクセスから保護するようにしてください。

関連項目： Directory Integration and Provisioning Server の登録方法は、35-13 ページの「Oracle Directory Integration and Provisioning Server の手動登録」を参照してください。

SSL モードでの認証

ディレクトリ・サーバーの識別情報を設定するには、Oracle Internet Directory と Directory Integration and Provisioning Server の両方を SSL サーバー認証モードで起動します。この場合、ディレクトリ・サーバーは自身の証明書を Directory Integration and Provisioning Server に提供し、Directory Integration and Provisioning Server は Oracle Internet Directory のクライアントとして機能します。

Directory Integration and Provisioning Server は、非 SSL モードと同じメカニズムを使用して認証されます。

サード・パーティのディレクトリに接続するときに SSL を使用するように Oracle Directory Integration and Provisioning Server を構成することもできます。この場合は、35-8 ページの「Oracle Internet Directory および接続ディレクトリの SSL 証明書の管理」で説明したとおり、接続ディレクトリ証明書を Wallet に保存します。

プロファイルの認証

Oracle Internet Directory の統合プロファイルは、識別名とパスワードを持つユーザーを表します。プロファイルにアクセスできるユーザーは次のとおりです。

- Oracle Directory Integration and Provisioning Platform の管理者（`DIPAdmin`）
- Oracle Directory Integration and Provisioning Platform 管理者グループのメンバー（`DIPAdminGroup`）

Directory Integration and Provisioning Server が統合プロファイルに基づいて Oracle Internet Directory にデータをインポートする場合、その統合プロファイルとしてディレクトリにプロキシ・バインドします。Oracle Directory Integration and Provisioning Platform は、このメカニズムを使用し、SSL モードと非 SSL モードの両方のモードでエージェントを認証します。

アクセス制御、認可および Oracle Directory Integration and Provisioning Platform

認可は、ユーザーが権限を持つ情報のみの読取りまたは更新を行うことを保証するプロセスです。ディレクトリ・セッション内でディレクトリ操作が行われようとすると、ディレクトリ・サーバーは、その操作の実行に必要な権限がユーザーに与えられていることを確認します（ユーザーの識別は、セッションに対応付けられた認可識別子によって行われます）。権限が与えられていない場合、操作は実行できません。この方法によって、ディレクトリ・サーバーは、ディレクトリ・ユーザーによる不正操作からディレクトリ・データを保護します。この方法はアクセス制御と呼ばれます。

アクセスを Oracle Internet Directory データの必要なサブセットのみに制限するには、Directory Integration and Provisioning Server とエージェントの両方に対する適切なアクセス・ポリシーをディレクトリに配置します。

この項では、このようなポリシーの詳細を説明します。次の項目について説明します。

- Oracle Directory Integration and Provisioning Server のアクセス制御
- エージェントに対するアクセス制御

Oracle Directory Integration and Provisioning Server のアクセス制御

Directory Integration and Provisioning Server は、ディレクトリへのバインドをそれ自身として行う場合と、エージェントのかわりに行う場合があります。

- それ自身としてバインドする場合、Directory Integration and Provisioning Server は様々な統合プロファイルに情報をキャッシュできます。これによって、Directory Integration and Provisioning Server は、様々なコネクタによって実行される同期アクションをスケジュールできます。
- エージェントのかわりに操作を行う場合、Directory Integration and Provisioning Server はエージェントのプロキシとして動作します。つまり、ディレクトリにバインドして様々な操作を実行するためにエージェントの資格証明を使用します。Directory Integration and Provisioning Server は、ディレクトリ内でエージェントに許可された操作のみを実行できます。

Directory Integration and Provisioning Server に付与されるアクセス権を設定し管理するために、Oracle Directory Integration and Provisioning Platform はインストール時に `odisgroup` と呼ばれるグループ・エントリを作成します。Directory Integration and Provisioning Server は、登録時にこのグループのメンバーになります。

Directory Integration and Provisioning Server に付与するアクセス権を制御するには、`odisgroup` エントリにアクセス制御ポリシーを設定します。デフォルトのポリシーでは、プロファイルにアクセスするための様々な権限が Directory Integration and Provisioning Server に付与されます。たとえば、デフォルトのポリシーでは、Directory Integration and Provisioning Server は、エージェントのかわりにバインドするとき、エージェントを認証するためのユーザー・パスワードを比較できます。デフォルトのポリシーによって、Directory Integration and Provisioning Server は、前回の同期日時や同期ステータスなど、プロファイルのステータス情報を変更することもできます。

エージェントに対するアクセス制御

統合プロファイルによる Oracle Internet Directory データへのアクセスを制御するには、Oracle Internet Directory 内に適切なアクセス制御ポリシーを設定します。このポリシーによって、あるエージェントが同期または処理したデータを他のエージェントの干渉から保護できます。また、ある属性の変更を、その属性の同期を所有する統合プロファイルにのみ許可することもできます。

> **関連項目：** グループ・エントリのアクセス制御ポリシーの設定方法は、14-3 ページの「セキュリティ・グループ」を参照してください。

たとえば、Oracle Internet Directory のインストール時に odipgroup と呼ばれるグループ・エントリを作成すると、様々なエージェントに付与したアクセス権を制御できます。権限は、適切なアクセス・ポリシーを odipgroup エントリに配置することによって制御されます。各エージェントはこのグループのメンバーです。メンバーシップは、エージェントがシステムに登録されるときに設定されます。製品とともに自動的にインストールされたデフォルトのアクセス・ポリシーでは、エージェントに対して、そのエージェントが所有する統合プロファイルへの標準的なアクセス権が付与されます。たとえば、統合プロファイル内の orclodipConDirLastAppliedChgTime パラメータなどのステータス情報を変更できる権限が付与されます。また、デフォルトのアクセス・ポリシーの場合、エージェントは Oracle Internet Directory の変更ログにアクセスできます（デフォルトのアクセス・ポリシー以外ではアクセスは制限されます）。

odisgroup グループ・エントリとそのデフォルトのポリシーは、Oracle Internet Directory のサーバー・インストール時に作成されます。Oracle Directory Integration and Provisioning Platform のみのインストールの場合は、これらのグループおよびポリシーは作成されません。

データの整合性と Oracle Directory Integration and Provisioning Platform

Oracle Directory Integration and Provisioning Platform は、SSL を使用して、送信時にデータの変更、削除または再現が行われないことを保証します。この SSL 機能は、暗号方式の保護メッセージ・ダイジェストを、MD5 アルゴリズムまたは Secure Hash Algorithm（SHA）を使用する暗号チェックサムを使用して生成し、ネットワークを介して送信する各パケットに組み込みます。

データのプライバシと Oracle Directory Integration and Provisioning Platform

Oracle Directory Integration and Provisioning Platform は、SSL で使用可能な公開鍵暗号を使用して、データが送信中に開示されないことを保証します。公開鍵暗号では、メッセージの送信側が受信側の公開鍵を使用して、メッセージを暗号化します。メッセージが送達されると、受信側は、受信側の秘密鍵を使用して、メッセージを復号化します。

Directory Integration and Provisioning Server と Oracle Internet Directory の間でデータを安全に交換するには、両方のコンポーネントを SSL モードで実行します。

ツール・セキュリティと Oracle Directory Integration and Provisioning Platform

一般的に使用されているツールは、すべて SSL モードで実行することにより Oracle Internet Directory にデータを安全に送信できます。たとえば、次のツールがあります。

- Oracle Directory Manager － ディレクトリ内のデータを管理するために使用します。
- Oracle Directory Integration and Provisioning Server 登録ツール（`odisrvreg`）－ Directory Integration and Provisioning Server をディレクトリに登録するために使用します。
- Directory Integration and Provisioning Assistant － SSL モードで実行する場合に使用します。
- プロビジョニング・サブスクリプション・ツール－ SSL モードで実行する場合に使用します。

37

Oracle Directory Integration and Provisioning Platform におけるディレクトリのブートストラップ

この章では、ディレクトリのブートストラップ（接続ディレクトリと Oracle Internet Directory の間のデータの移行）について説明します。

この章では、次の項目について説明します。

Oracle Directory Integration and Provisioning Platform でのディレクトリのブートストラップについて

Oracle Directory Integration and Provisioning Platform では、ブートストラップは、Directory Integration and Provisioning Assistant に `bootstrap` オプションを指定して処理されます。コマンドは次のとおりです。

```
dipassistant bootstrap
```

Directory Integration and Provisioning Assistant の使用方法を取得するには、次のように入力します。

```
dipassistant bootstrap -help
```

Directory Integration and Provisioning Assistant によって、パラメータ・ファイルまたは完全に構成された統合プロファイルのいずれかを使用して、ブートストラップができるようになります。後者の方法の場合は、たとえば、SunONE Directory Server からブートストラップするために、インストールの一部として作成されたデフォルトの統合プロファイルを構成します。具体的には、このプロファイルに適切な接続ディレクトリ情報とマッピング・ルールを入力します。

この章では、両方の方法について説明します。

関連項目： A-106 ページの「Directory Integration and Provisioning Assistant」

パラメータ・ファイルを使用したブートストラップ

このファイル内のパラメータは、ソース・データ型、宛先データ型、資格証明、および Oracle Internet Directory と接続ディレクトリの間でエントリをマッピングする方法を指定します。各種パラメータ、および Directory Integration and Provisioning Assistant がファイルの読取り時にそれらに対して想定するデフォルト値の詳細は、A-111 ページの表 A-30 を参照してください。

次のいずれかの方法で、LDIF ファイルを使用してブートストラップすることができます。

- Directory Integration and Provisioning Assistant を使用したソース・ディレクトリの読取り
- ディレクトリ依存ツールを使用したソース・ディレクトリの読取り
- Directory Integration and Provisioning Assistant を使用した Oracle Internet Directory へのデータのロード

インストール時に、サンプル・パラメータ・ファイルが $*ORACLE_HOME*/ldap/odi/samples/ ディレクトリにコピーされます。このファイルには、ブートストラップにおける各パラメータの機能が説明されています。

ブートストラップ用にツールを実行する場合は、*ORACLE_HOME* と NLS_LANG が正しく設定されていることを確認してください。

ブートストラップは、中間ファイルの有無にかかわらず、サービス間で実行できます。ただし、大きいディレクトリの場合は、中間 LDIF ファイルが必要です。

この項では、次の項目について説明します。

- LDIF ファイルを使用しないブートストラップ
- LDIF ファイルを使用したブートストラップ

LDIF ファイルを使用しないブートストラップ

この方法は、エントリが次の状態の小さいディレクトリに使用することをお薦めします。

- 比較的少数
- フラット構造
- 非相互依存（グループ・エントリの作成はユーザー・メンバー・エントリの存在に依存する場合などとは異なり、この場合、エントリの作成は別のエントリの存在には依存しない）

この方法を使用する手順は、次のとおりです。

1. 適切なマッピング・ルールを持つマッピング・ファイルを準備します。マッピング・ファイルは、ブートストラップ・ファイル内のプロパティの 1 つです。同期用に定義されたマッピング・ルールと一致していることを確認してください。
2. ソースを LDAP、宛先型を LDIF と指定した必須の詳細情報を持つパラメータ・ファイルを作成します。サンプル・パラメータ・ファイルは *ORACLE_HOME*/ldap/odi/samples/ldp2ldf.properties にあります。バイナリ属性が、「SrcAttrType」フィールドでバイナリとして指定されていることを確認します。
3. 次のとおり指定されている構成ファイルを使用して、Directory Integration and Provisioning Assistant の bootstrap コマンドを実行します。
   - ソースが LDAP ディレクトリと指定されている。
   - 宛先型が LDIF と指定されている。データを LDIF ファイルにダンプ。

   次のように入力して、Directory Integration and Provisioning Assistant を実行します。

   ```
   Dipassistant bootstrap -cfg parameter_file
   ```

4. エラーがないかどうか、bootstrap.log ファイルと bootstrap.trc ファイルをチェックします。
5. bulkload を使用して、Oracle Internet Directory にデータをアップロードします。
6. 同期を継続するには、最後の変更番号を更新します。

   ```
   dipassistant mp -profile profile_name -updcln
   ```

LDIF ファイルを使用したブートストラップ

この項では、LDIF ファイルを使用してディレクトリをブートストラップする 2 つの方法について説明します。

ディレクトリ依存ツールを使用してソース・ディレクトリを読み取ることによって LDIF ファイルからブートストラップする方法

大きいディレクトリに対してはこの方法を使用することをお薦めします。この方法を使用する手順は、次のとおりです。

1. ディレクトリから LDIF ファイルにデータをダウンロードします。使用するツールは、データのロード元のディレクトリによって異なります。Microsoft Active Directory からブートストラップしている場合は、「ldifde」を使用してデータをロードします。各エントリに必要なすべての属性をロードしてください。
2. 適切なマッピング・ルールを持つマッピング・ファイルを準備します。さらに同期を行う場合は、マッピング・ファイルが同期に使用されるものと同じであることを確認してください。
3. LDIF としてのソースと宛先、およびその他の詳細情報を持つ宛先パラメータ・ファイルを作成します。サンプル・パラメータ・ファイルは *ORACLE_HOME*/ldap/odi/samples/ldf2ldf.properties にあります。
4. ソースを LDIF、宛先型を LDIF と指定したパラメータ・ファイルとともに Directory Integration and Provisioning Assistant の bootstrap コマンドを使用します。これによって、ソース・データが変換され、Oracle Internet Directory で必要な新しい LDIF が作成されます。次のように入力して、Directory Integration and Provisioning Assistant を実行します。

   ```
   dipassistant bootstrap -cfg parameter_file
   ```

5. エラーがないかどうか、bootstrap.log ファイルと bootstrap.trc ファイルをチェックします。
6. Oracle Internet Directory のバルク・ロード・ツール（bulkload.sh）を使用して、データを Oracle Internet Directory にアップロードします。

7. さらに同期を行うために対応する同期プロファイルを作成する場合は、最後の変更番号を更新します。

   ```
   dipassistant mp -profile profile_name -updcln
   ```

Directory Integration and Provisioning Assistant を使用してデータを Oracle Internet Directory にロードすることによって LDIF ファイルからブートストラップする方法

この方法を使用する手順は、次のとおりです。

1. ディレクトリから LDIF ファイルにデータをダウンロードします。使用するツールは、データのロード元のディレクトリによって異なります。Microsoft Active Directory からブートストラップしている場合は、「ldifde」を使用してデータをロードします。各エントリに必要なすべての属性をロードしてください。
2. 適切なマッピング・ルールを持つマッピング・ファイルを準備します。さらに同期を行う場合は、マッピング・ファイルが同期に使用されるものと同じであることを確認してください。
3. ソースを LDIF、宛先を LDAP と指定して、プロパティ・ファイルを作成します。
4. ソースを LDIF ファイル、宛先型を LDAP、宛先を Oracle Internet Directory と指定したパラメータ・ファイルとともに Directory Integration and Provisioning Assistant の bootstrap コマンドを使用します。これによってソース・データが変換され、Oracle Internet Directory 内に必要なエントリが作成されます。サンプル・パラメータ・ファイル ldf2ldp.properties は、*$ORACLE_HOME*/ldap/odi/samples にあります。
5. エラーがないかどうか、bootstrap.log ファイルと bootstrap.trc ファイルをチェックします。
6. さらに同期を行うために対応する同期プロファイルを作成する場合は、最後の変更番号を更新します。

   ```
   dipassistant mp -profile profile_name -updcln
   ```

デフォルト統合プロファイルを使用した直接ブートストラップ

ブートストラップは、同期用に構成された既存の統合プロファイルに依存します。この構成の詳細は、サード・パーティ・ディレクトリへの接続に使用されます。

この方法を使用する場合は、ソース・ディレクトリを読取り専用モードに設定します。

プロファイルが IMPORT プロファイルの場合は、接続ディレクトリ内の必須オブジェクトのフットプリントが Oracle Internet Directory に作成されます。プロファイルが EXPORT プロファイルの場合は、Oracle Internet Directory からの必須オブジェクトのフットプリントが接続ディレクトリ内に作成されます。

これらのエントリの作成中、統合プロファイルに指定されているとおり、ドメイン・レベルおよびオブジェクト・レベルのマッピングが使用されます。エントリのアップロードに失敗した場合は、*$ORACLE_HOME*/ldap/odi/log/bootstrap.log に情報が記録されます。トレース情報は、*$ORACLE_HOME*/ldap/odi/log/bootstrap.trc ファイルに書き込まれます。

たとえば、SunONE Directory Server から Oracle Internet Directory にブートストラップする場合は、次の手順を実行します。

1. デフォルトの統合プロファイル IplanetImport をカスタマイズします。このプロファイルは、42-5 ページの「タスク 1: SunONE コネクタ用の統合プロファイルの構成」に従ってインストールの一部として作成されます。
2. 次のコマンドを入力します。

   ```
   dipassistant bootstrap -profile IplanetImport -dn  'cn=orcladmin' -passwd
   'welcome'
   ```

3. bootstrap.log ファイルと bootstrap.trc ファイルをチェックし、ブートストラップが正常に終了したことを確認してください。

Directory Integration and Provisioning Assistant を使用してブートストラップしている場合は、ブートストラップ処理の最後に Directory Integration and Provisioning Assistant によって、以降の同期化のために lastchangenumber 属性が初期化されます。

関連項目： A-117 ページの「Oracle Internet Directory 10g（9.0.4）での Directory Integration and Provisioning Assistant の制限」

38

リレーショナル・データベースの表との同期

この章では、リレーショナル・データベース内の表のデータを Oracle Internet Directory と同期させる方法について説明します。同期は、増分（たとえば、データベース表の行単位）またはすべてのデータベース表を一括で実行できます。

注意： この章を読む前に、Oracle Directory Integration and Provisioning Platform の概要についての次の章をよく理解しておく必要があります。

- 第 32 章「Oracle Directory Integration and Provisioning Platform の概要とコンポーネント」
- 第 33 章「Oracle Directory Synchronization Service」

また、Oracle Internet Directory 10*g*（9.0.4）の場合は、Oracle Internet Directory からリレーショナル・データベースにデータをエクスポートできないことに注意してください。

この章では、次の項目について説明します。

- 概要 : Oracle Internet Directory とリレーショナル・データベース表との同期
- Oracle Internet Directory とリレーショナル・データベースの間の同期の管理

概要 : Oracle Internet Directory とリレーショナル・データベース表との同期

データベース・サーバーとの同期プロセスでは、ディレクトリ統合プロファイルを実行する必要があります。このプロセスには 2 つの手順があります。

1. データベースからのデータの取得。これには、指定したデータ・レコードをデータベースから取得する SQL の SELECT 文を実行する必要があります。
2. ディレクトリへのデータの書込み。これには、取得したデータ・レコードを LDAP 属性値に変換し、ディレクトリに対して LDAP 操作を実行する必要があります。

Oracle Internet Directory とリレーショナル・データベースの間の同期の管理

この項では、Oracle Internet Directory をリレーショナル・データベースに同期させるために実行するタスクについて説明します。また、適切な詳細情報を持つ統合プロファイルの作成例も示します。

この項では、次の項目について説明します。

タスク 1: 追加構成情報ファイルの準備

リレーショナル・データベースから Oracle Internet Directory への同期中、データベースからのデータの取得は、追加構成情報ファイルによって制御されます。追加構成情報ファイルは、Oracle Directory Integration and Provisioning Server に次の情報を提供します。

- 実行対象の SELECT 文
- 増分同期に使用される属性またはデータベース列のいずれか。通常、タイムスタンプを含む属性、または次の SQL 文で増分データの取得に使用する必要がある変更順序番号のいずれかです。

このファイルを構成するには、*ORACLE_HOME*/ldap/odi/samples/ にあるサンプル・ファイル DBReader.cfg.master をユーザーの仕様に従って編集してください。

追加構成情報ファイルの形式

このファイルの構成では、正しい形式に従うことが非常に重要です。TAG 名を使用して、各種セクションに分割します。各 TAG セクションには、パラメータのリストとそれぞれの値を示します。通常のレイアウトは次のとおりです。

```
[TAG]
PARAMETER1: value
PARAMETER2: value

[TAG]
PARAMETER1: value
PARAMETER2: value¥
VALUE continuation¥
value continuation¥
end of value continuation

[TAG]
PARAMETER1: value
PARAMETER2: value¥
end of value continuation
```

この形式に従うと、たとえば、DBReader.cfg.master ファイルは次のようになります。

```
[DBQUERY]
SELECT: SELECT¥
    EMPNO EmpNum,¥
    ENAME,¥
    REPLACE(EMAIL),'@ACME.COM','') UID,¥
    EMAIL,¥
    TELEPHONE,¥
    TO_CHAR(LAST_UPDATE_DATE,'YYYYMMDDHH24MISS') Modified_Date¥
FROM¥
    EMPLOYEE¥
WHERE¥
    LAST_UPDATE_DATE>TO_DATE (:Modified_Date,'YYYYMMDDHH24MISS')¥
ORDER BY¥
LAST_UPDATE_DATE

[SYNC-PARAMS]
CHANGEKEY: Modified_Date
```

SELECT 文全体がパラメータ SELECT の値として、TAG DBQUERY で表されているセクションに入力されています。値が冗長なため、SELECT 文の終わりまですべての行で値継続文字が最後の文字として入力されています。

CHANGEKEY パラメータ値は、増分同期中に使用される列の名前です。これらの列の値は、常に、プロファイルの orclOdipLastAppliedChgNum 属性に格納されます。SELECT 文が実行されるたびに、それに応じてこの属性の現在の値が SQL 文に入力されます。これによって、データは常に増分取得されます。

たとえば、column1:column2 のように複数の列名が CHANGEKEY にある場合は、プロファイルの orclOdipLastAppliedChgNum 属性の値が value1~value2 として格納されます。ここで value1 は column1 に、value2 は column2 に対応しています。

列名は、属性値ペアとして Oracle Directory Integration and Provisioning Platform に取得された後、設定されたマッピング・ルールに従って LDAP 属性値にマッピングされます。このため、SELECT 文で取得されたすべての列名は、式ではなく単純名である必要があります。たとえば、式 REPLACE(EMAIL),'@ACME.COM','') を使用することはできますが、この式の値は、UID として取得されます。

この例では、Modified_Date が増分同期のキーです。これは日付であるため、文字列書式で表す必要があります。

プロファイルを作成する場合は、orclOdipLastAppliedChgNum 属性に値を設定する必要があります。この日付以降のすべての変更（この値より大きい LAST_UPDATE_DATE を持つ表内の行）が取得されます。たとえば、orclOdipLastAppliedChgNum 属性を 20000101000000 に設定すると、2000 年 1 月 1 日以降のすべての従業員の変更が取得されます。

ORDER BY 句を使用しているため、戻されるすべてのデータベース行は LAST_UPDATE_DATE の順序です。変更は、行われた順に取得されディレクトリに適用されます。最後の変更が取得されて適用された後、次の処理が行われます。

1. orclOdipLastAppliedChgNum 属性値が、取得された最後の行から Modified_Date に設定されます。
2. プロファイルが更新されます。

Oracle Directory Integration and Provisioning Platform は、プロファイルを再実行する場合、常に、以前格納された値を使用します。

タスク 2: マッピング・ファイルの準備

マッピング・ルールを構成するには、33-5 ページの「マッピング・ルールとその形式」の指示に従います。

タスク 3: ディレクトリ統合プロファイルの準備

Oracle Directory Manager または Directory Integration and Provisioning Assistant を使用して、ディレクトリ統合プロファイルを作成できます。Oracle Directory Manager を使用する場合は、Directory Integration and Provisioning Assistant または `ldapUploadAgentFile.sh` スクリプトを使用して、追加構成情報ファイルとマッピング・ファイルをアップロードする必要があります。

ディレクトリ統合プロファイルを構成するには、33-6 ページの「Oracle Directory Integration and Provisioning Platform へのコネクタの登録」の指示に従います。ただし、次の注意事項があります。

- エージェント実行コマンド（`orclodipAgentExeCommand`）属性に値を設定しないでください。
- インタフェース・タイプ（`orclodipDataInterfaceType`）属性を `DB` に設定します。

関連項目：

- A-106 ページの「Directory Integration and Provisioning Assistant」
- ldapUploadAgentFile.sh スクリプトの使用方法は、A-118 ページの「ldapUploadAgentFile.sh ツールの構文」を参照してください。

例：リレーショナル・データベース表と Oracle Internet Directory の同期化

この例では、従業員データを含む次のリレーショナル・データベース表が Oracle Internet Directory と同期化されます。

表 38-1 Employee 表

EMPNO	ENAME	LAST_UPDATE_DATE	EMAIL	TELEPHONE
98357	JOHN DOE	2-JAN-2000	JOHN.DOE@ACME.COM	435-324-3455
98360	ROGER BECK	3-JUL-2001	ROGER.BECK@ACME.COM	435-324-3600
98365	JIMMY WONG	4-MAR-2001	JIMMY.WONG@ACME.COM	435-324-2390
98370	GEORGE MICHAEL	6-FEB-2002	GEORGE.MICHAEL@ACME.COM	435-324-9232

この例のサンプル・プロファイルは、*ORACLE_HOME*`/ldap/odi/samples` ディレクトリにあります。また、サンプル構成ファイルとサンプル・マッピング・ファイルも同じディレクトリにあります。この例では、次のように仮定します。

- 表の名前は、`Employee` です。
- プロファイル名は `TESTDBIMPORT` です。

- データベース・レコードをディレクトリ・エントリと結合するには、従業員番号（EMPNO）が使用されます。この番号は、B-18 ページの表 B-20 に示す OID 照合フィルタ（orclOdipOIDMatchingFilter）属性に指定されています。
- この表は、データベース内の testsync/testsyncpwd スキーマにあります。データベースはホスト machine.acme.com に存在し、データベース・リスナー・ポートは 1526、SID は iasdb です。データベース URL は、machine.acme.com:1526:iasdb です。
- 適切な読取り / 書込み権限、orclodipagentname=testdbimport が明示的にこのプロファイルに付与されています。
  cn=subscriber profile,
  cn=changelog subscriber,
  cn=oracle internet directory
- プロファイルは、構成設定 1 内に作成されます。

タスク 1: 追加構成情報ファイルの構成

この例では、38-2 ページの「タスク 1: 追加構成情報ファイルの準備」で説明した追加構成情報ファイルと同じファイルを使用します。

タスク 2: マッピング・ファイルの構成

この例のマッピング・ファイルの内容は次のとおりです。

```
DomainRules
NONLDAP:dc=testdbsync,dc=com:uid=%,dc=testdbsync,dc=com
AttributeRules
ename: : : :cn: :person
ename : : : :sn: :person
uid : : : :uid: :inetOrgperson:
EMail: : : :mail: :inetOrgperson
Telephone: : : :telephonenumber: :inetOrgperson
empnum: : : :employeenumber: :inetOrgperson
```

このマッピング・ファイルは次のことを指定しています。

- ディレクトリ・エントリは uid=%,dc=testdbsync,dc=com として作成されています。% は、uid の実際の値のプレースホルダです。マッピング後 uid に値を含めるには、uid がマッピング・ファイル内に存在している必要があります。存在しない場合、識別名の構成は失敗します。
- cn および sn の両方の属性は ename と同じ値を持ちます。
- uid 要素は、EMail 接頭辞の値（電子メール・アドレス内の @ 文字より前の部分）を持つ必要があります。

- empnum は、ディレクトリ・エントリ内の employeenumber になります。
- telephone は、ディレクトリ・エントリ内の telephone number になります。

タスク 3: ディレクトリ統合プロファイルの構成

この例のディレクトリ統合プロファイルには、38-7 ページの表 38-2 に示す属性値が含まれます。これらの値を持つサンプル統合プロファイルおよびそれに対応するマッピング・ファイルと構成ファイルが *$ORACLE_HOME*/ldap/odi/samples ディレクトリに用意されています。createprofile モードで Directory Integration and Provisioning Assistant を実行し、引数としてファイルを指定してプロファイルを作成できます。また、Oracle Directory Manager を使用してプロファイルを作成することもできます。

関連項目：

- A-106 ページの「Directory Integration and Provisioning Assistant」
- Oracle Directory Manager を使用してプロファイルを作成する方法は、33-18 ページの「Oracle Directory Manager を使用したプロファイルの登録」を参照してください。

表 38-2 TESTDBIMPORT 用のディレクトリ統合プロファイル

属性	値
プロファイル名 (orclOdipAgentName)	TESTDBIMPORT
同期モード (orclOdipSynchronizationMode)	IMPORT
プロファイル・ステータス (orclOdipAgentControl)	ENABLE
エージェント実行コマンド (orclodipAgentExeCommad)	NULL
追加構成情報 (orclOdipAgentConfigInfo)	前述のファイルに示したとおり。アップロードの必要あり。
接続ディレクトリ・アカウント (orclOdipConDirAccessAccount)	testdbsync
接続ディレクトリ・アカウント・パスワード (orclOdipConDirAccessPassword)	testdbsyncpwd
接続ディレクトリ URL (orclOdipConDirURL)	machine.acme.com:1526:iasdb

表 38-2 TESTDBIMPORT 用のディレクトリ統合プロファイル（続き）

属性	値
インタフェース・タイプ (orclodipDataInterfaceType)	DB
マッピング・ファイル：	ファイルからアップロード
OID 照合フィルタ (orclOdipOIDMatchingFilter)	employeenumber これは、一致を検索中、ディレクトリの検索に employeenumber が使用されることを意味します。一致が検証されると、ディレクトリ・エントリが修正されます。それ以外の場合は、新しいエントリが作成されます。これは、orclOdipOIDMatchingFilter 属性がデータベース内で一意なことを保証するためにも必要です。 データベース行が取得されると、Oracle Directory Integration and Provisioning Server は、ドメイン・ルールに従って、employeenumber を検出されるためにドメイン dc=testdbsync,dc=com 内のディレクトリを検索します。一致が検出された場合は、検索された行内の列の最新の値でそのエントリが更新されます。一致が検出されなかった場合は、列値のすべての属性を持つ新しいエントリがディレクトリ内に作成されます。
前回適用された変更番号 (orclodipConDirLastAppliedChgNum)	20000101000000 これは、プロファイルの最初の実行時に、4 つすべての行を取得し同期することを意味します。その後は、表内の LAST_UPDATE_DATE 列が最終更新時刻に更新した場合にのみ、行が取得されます。

タスク 4: 追加構成情報ファイルのアップロード

プロファイルの作成に Oracle Directory Manager を使用した場合は、次のコマンドを入力します。

```
ORACLE_HOME/ldap/odi/admin/ldapuploadagentfile.sh -name "TESTDBIMPORT" -config 1 ¥
-bindpass password -binddn "cn=orcladmin" -attrtype "ATTR" ¥
-filename full_path_name_of_the_file
```

タスク 5: マッピング・ファイルのアップロード

プロファイルの作成に Oracle Directory Manager を使用した場合は、次のコマンドを入力します。

```
ORACLE_HOME/ldap/odi/admin/ldapuploadagentfile.sh -name "TESTDBIMPORT" -config 1 ¥
-bindpass password -binddn "cn=orcladmin" -attrtype "MAP" ¥
-filename full_path_name_of_the_file
```

同期化プロセス

この例では、同期化プロセスの手順は、次のとおりです。

1. スケジューリング間隔（orclOdipSchedulingInterval）属性に指定された値が期限切れになるたびに、Oracle Directory Integration and Provisioning Server は、TESTDBIMPORT プロファイル用に新しいプロファイル・スレッドを開始します。
2. プロファイル・スレッドは、追加構成情報を読み取って、SQL の実行を準備した後、SQL を実行します。
3. データベースから取得された行ごとに、マッピング・ルールがレコードに適用され、LDAP 属性が作成されます。
4. OID 照合フィルタ（orclOdipOIDMatchingFilter）属性によって、Oracle Internet Directory 内に一致するエントリがあるかどうかを Directory Integration and Provisioning Server が判断します。一致するエントリがある場合は更新されます。ない場合は新しいエントリが作成されます。ディレクトリ操作の後、最後に適用された変更番号（orclodipConDirLastAppliedChgNum）属性が更新されます。

例に関する注意事項

行は、次の形式でデータベースから取得されます。

```
EmpNum: 98357
EName: JOHN DOE
UID: JOHN.DOE
EMAIL: JOHN.DOE@ACME.COM
TELEPHONE: 435-324-3455
Modified_Date: 20000102000000
```

このレコード上で行われたマッピングは、次の形式で出力されます。

```
dn: uid=john.doe,dc=testdbsync,dc=com
uid: JOHN.DOE
cn: JOHN DOE
sn: JOHN DOE
mail: JOHN.DOE@ACME.COM
employeenumber: 98357
telephonenumber: 435-324-3455
objectclass: person
objectclass: inetorgperson
```

ドメイン dc=testdbsync,dc=com 下のフィルタ employeenumber=98357 を使用して、ディレクトリ内でサブツリー検索が行われます。検索結果が既存のエントリの場合は、そのエントリが更新されます。それ以外の場合は、新しいエントリが作成されます。OID 照合フィルタ（orclOdipOIDMatchingFilter）属性が employeenumber に設定されているため、取得されるすべてのデータベース・レコードがその列を持つ必要があります。この場合は、employeenumber にマッピングされているとおりの EmpNum です。

マッピング・ファイル内のその他の属性で、SQL によって取得されるデータに含まれないもの（birthday 属性など）は無視されます。

プロファイル・スレッドは、SQL からのすべての変更レコードを処理した後、これらの属性の正しい値でディレクトリを更新します。

- 前回適用された変更番号（orclodipConDirLastAppliedChgNum）
- 最終実行時刻（orclOdipLastExecutionTime）
- 前回成功実行日時（orclOdipLastSuccessfulExecutionTime）

39

Oracle Human Resources との同期化

企業内の従業員用の真のソースとして Oracle Human Resources を使用している場合は、Oracle Human Resources と Oracle Internet Directory を同期化する必要があります。同期化には、Oracle Human Resources コネクタを使用します。

この章では、Oracle Human Resources コネクタを紹介し、その配置方法を説明します。次の項目について説明します。

- Oracle Human Resources との同期化の概要
- Oracle Human Resources からインポートできるデータ
- Oracle Human Resources と Oracle Internet Directory の間の同期の管理
- Oracle Human Resources からの Oracle Internet Directory のブートストラップ

> **関連項目：** このリリースの Oracle Internet Directory と同期化できる Oracle Human Resources のリリースを確認する場合は、Oracle Internet Directory リリース・ノートを参照してください。

Oracle Human Resources との同期化の概要

Oracle Human Resources コネクタによって、従業員データのサブセットを、Oracle Human Resources から Oracle Internet Directory にインポートできます。Oracle Internet Directory とともにデフォルトの構成でインストールされます。パラメータを構成して配置の要件を満たした後、実行できます。

Oracle Human Resources コネクタは、Oracle Human Resources システムから増分変更を抽出するように構成することによって、いつでも実行できるようにスケジュールできます。また、Oracle Human Resources の列名と Oracle Internet Directory の属性の間のマッピングを設定および変更できます。

Oracle Human Resources の実行可能エージェントは `odihragent` という名前で、`$ORACLE_HOME/ldap/odi/bin` ディレクトリにあります。Directory Integration and Provisioning Assistant または Oracle Directory Manager を使用して、プロファイルを管理できます。

Oracle Human Resources からインポートできるデータ

表 39-1 に、Oracle Human Resources スキーマの表を示します。選択した場合は、これらの属性のほとんどを Oracle Internet Directory にインポートできます。

表 39-1　Oracle Human Resources スキーマの表

表名	コネクタ構成情報フィールドで使用される別名
PER_PEOPLE_F	PER
PER_ADDRESSES	PA
PER_PERIOD_OF_ SERVICE	PPS
PER_PERSON_TYPE	PPT

Oracle Human Resources データベースに apps アカウントでログインした場合は、これらの表はすべて参照できます。

属性は実行時に構成ファイルから追加または削除できるので、Oracle Human Resources コネクタは、必要な属性のみを選択して取り出す SQL 文を動的に作成します。

表 39-2 に、Oracle Human Resources のユーザー・インタフェースのフィールドの一部を示します。これらのフィールドは、従業員データを追加または変更するときに表示されます。

表 39-2　Oracle Human Resources のユーザー・インタフェースのフィールド

属性名	説明	フォーム / キャンバス / フィールド名
LAST_NAME	個人の姓	個人情報 / 氏名 / 姓
FIRST_NAME	個人の名	個人情報 / 氏名 / 名

表 39-2 Oracle Human Resources のユーザー・インタフェースのフィールド（続き）

属性名	説明	フォーム / キャンバス / フィールド名
TITLE	個人のタイトル	個人情報 / 氏名 / タイトル
SUFFIX	サフィックス（Jr、Sr、Ph.D など）	個人情報 / 氏名 / サフィックス
MIDDLE_NAME	ミドルネーム	個人情報 / 氏名 / サフィックス
SEX	性別	「性別リスト」ボックス
START_DATE	入社日	個人情報 / 入社日
DATE_OF_BIRTH	生年月日	個人情報 / 個人情報 / 生年月日
MARITAL_STATUS	婚姻区分	個人情報 / 個人情報 / ステータス
NATIONAL_ INDENTIFIER	米国居住者用社会保障番号	個人情報 /ID/ 社会保障
EMPLOYEE_NUMBER	従業員番号	個人情報 /ID/ 従業員
REGISTERD_ DISABLED_FLAG	障害の有無のインジケータ	個人情報 / 個人情報 / 障害の有無
EMAIL_ADDRESS	電子メール・アドレス	個人情報 / 個人情報 / 電子メール
OFFICE_NUMBER	オフィス所在地	個人情報 / オフィス所在地情報 / オフィス
MAILSTOP	郵便物配達先	個人情報 / オフィス所在地情報 / 郵便宛先
INTERNAL_ LOCATION	事務所	個人情報 / オフィス所在地情報 / 事業所
ADDRESS_LINE1		個人住所情報 / 住所 1
ADDRESS_LINE2		個人住所情報 / 住所 2
ADDRESS_LINE3		個人住所情報 / 住所 3
TOWN_OR_CITY		個人住所情報 / 市区町村
REGION_1		個人住所情報 / 都
REGION_2		個人住所情報 / 都道府県
POSTAL_CODE		個人住所情報 / 郵便番号
COUNTRY		個人住所情報 / 国
TELEPHONE_ NUMBER_1		個人住所情報 / 電話番号
TELEPHONE_ NUMBER_2		個人住所情報 / 電話番号 2

Oracle Human Resources と Oracle Internet Directory の間の同期の管理

この項では、次の項目について説明します。

タスク 1: Oracle Human Resources コネクタのディレクトリ統合プロファイルの構成

Oracle Human Resources コネクタを配置するには、そのためのディレクトリ統合プロファイルを Oracle Internet Directory 内に作成する必要があります。インストール時に、デフォルトの統合プロファイルが作成されます。デフォルト統合プロファイルのパラメータのリストと説明は、B-18 ページの表 B-20 を参照してください。これらのパラメータの一部に対しては、Human Resources コネクタとの統合に固有の値を指定する必要があります。39-4 ページの表 39-3 に、Human Resources コネクタに固有のパラメータを示します。

表 39-3 Oracle Human Resources コネクタ統合プロファイルに固有の属性

属性	説明
一般情報	
プロファイル名（orclODIPAgentName）	システム内でコネクタを識別するための一意名。統合プロファイルを識別する識別名の相対識別名コンポーネントとして使用されます。この名前には英数字のみを使用できます。この属性は必須で、変更不可です。デフォルトの名前は OracleHRAgent です。
同期モード（ModeorclODIPSynchronizationMode）	Oracle Internet Directory と接続ディレクトリの間での同期の方向。 ■ IMPORT は接続ディレクトリから Oracle Internet Directory への変更のインポートを示します。 ■ EXPORT は Oracle Internet Directory から接続ディレクトリへの変更のエクスポートを示します。 デフォルトは IMPORT です。 この属性は必須で、変更可能です。 **注意：** Oracle Internet Directory 10*g*（9.0.4）は、Oracle Human Resources に対してのみインポート操作をサポートします。

表 39-3 Oracle Human Resources コネクタ統合プロファイルに固有の属性（続き）

属性	説明
実行情報	

エージェント実行コマンド（orclODIPAgentExeCommand）	Directory Integration and Provisioning Server がコネクタの実行に使用する、コネクタ実行可能ファイルの名前と引数のリスト。
	この属性は必須で、変更可能です。
	デフォルトは次の値です。
	`odihragent OracleHRAgent connect=hrdb ¥`
	`login=%orclodipConDirAccessAccount ¥`
	`pass=%orclodipConDirAccessPassword ¥`
	`date=%orclODIPLastSuccessfulExecutionTime ¥`
	引数 connect=hrdb の値は、Oracle Human Resources システム・データベースの接続文字列に設定する必要があります。

接続ディレクトリ・アカウント（orclodipConDirAccessAccount）	コネクタが同期で使用する、接続ディレクトリ内の有効なユーザー・アカウント。Human Resources Agent の場合のユーザー・アカウントは、Oracle Human Resources データベース内の有効なユーザー識別子です。 **関連項目：**コマンドラインで引数を渡す一般的な使用方法は、第 39 章「Oracle Human Resources との同期化」を参照してください。
追加構成情報（orclODIPAgentConfigInfo）	コネクタが Oracle Internet Directory に格納する構成情報。この構成情報は、コネクタの起動時に、Directory Integration and Provisioning Server によってコネクタに渡されます。この情報は属性として格納され、Directory Integration and Provisioning Server はその内容を認識しません。 この属性に格納される値は、Oracle Human Resources からの同期が必要な（Oracle Human Resources コネクタについて）すべての属性を表します。 **関連項目：**39-7 ページの「タスク 2: Oracle Internet Directory と同期化される属性のリストの構成」を参照してください。 Oracle Human Resources コネクタの場合、この属性は必須です。構成ファイルを編集してからプロファイルに再度アップロードすることによって変更できます。この属性は、Oracle Directory Manager では修正できません。
接続ディレクトリの URL	接続ディレクトリのホストとポートの詳細情報です。*host*:*port*:*sid* の形式で入力する必要があります。

表 39-3 Oracle Human Resources コネクタ統合プロファイルに固有の属性（続き）

属性	説明
インタフェース・タイプ (orclODIPInterfaceType)	データ転送に使用するインタフェース。このインタフェースはタグ付きファイルの形式であるため、TAGGED に設定されます。 **注意：** Oracle Human Resources プロファイルの場合、この属性は変更しないでください。
マッピング情報	
マッピング・ルール (orclODIPAttributeMappingRules)	マッピング・ルールを格納するための属性。マッピング・ルールは、Directory Integration and Provisioning Assistant または ldapuploadagentfile.sh ツールを使用してファイルに格納します。 Oracle Human Resources の場合、この属性は必須で、変更可能です。 **関連項目：** ■ 33-5 ページの「マッピング・ルールとその形式」 ■ 33-7 ページの「マッピング・ルール属性の形式」 ■ A-106 ページの「Directory Integration and Provisioning Assistant」
接続ディレクトリの照合フィルタ (orclODIPConDirMatchingFilter)	Oracle Human Resources 接続には使用されません。
OID の照合フィルタ (orclODIPOIDMatchingFilter)	この属性は、Oracle Internet Directory でのターゲット・エントリの検索に使用される LDAP フィルタを指定します。Oracle Directory Integration and Provisioning Server はこのフィルタを使用して、同期に必要な LDAP 操作の種類を検出します。 employeenumber=% の形式で指定します。 この属性はオプションで、変更可能です。
ステータス情報	
OID の前回適用された変更番号 (orcllastappliedChangenumber)	この属性は、すべての EXPORT プロファイルの基準で、Oracle Human Resources の同期には適用されません。
前回適用された変更番号 (orclODIPConDirLastAppliedChgNum)	この属性は、すべてのプロファイルの基準で、Oracle Human Resources の同期には適用されません。

タスク 2: Oracle Internet Directory と同期化される属性のリストの構成

デフォルトの Oracle Human Resources プロファイルは、Oracle Human Resources から Oracle Internet Directory に同期化される属性のデフォルト・リストを提供します。このリストはカスタマイズ可能で、属性を追加または削除できます。

デフォルトの属性リストは、統合プロファイルの一部として orclodipAgentConfigInfo 属性に格納されます。構成情報も、$*ORACLE_HOME*/ldap/odi/conf ディレクトリにある oraclehragent.cfg.master ファイルに用意されています。

注意： oraclehragent.cfg.master ファイルはバックアップとして機能するため、変更できません。

Oracle Human Resources の属性のデフォルトのリストには、次の列があります。

列	説明
ATTRNAME	出力データ・ファイルに生成される出力タグ。
COLUMN_NAME	この値の取得元になるデータベース列名。
TABLE_NAME	この値の取得元になるデータベース表名。
FORMAT	この属性の列データ型。（ASCII、NUMBER、DATE）
MAP	この属性を Oracle Human Resources から抽出するかどうかのインジケータ。値 Y は抽出されることを示し、値 N は抽出されないことを示します。

oraclehragent.cfg.master ファイルの内容は、次のとおりです。

```
ATTRNAME:COLUMN_NAME:TABLE_NAME:FORMAT:MAP
PersonId:person_id:PER:NUMBER:Y
PersonType:person_type_id:PER:NUMBER:Y
PersonTypeName:system_person_type:PPT:ASCII:Y
LastName:last_name:PER:ASCII:Y
StartDate:start_date:PER:DATE:Y
BirthDate:date_of_birth:PER:DATE:Y
EMail:email_address:PER:ASCII:Y
EmployeeNumber:employee_number:PER:NUMBER:Y
FirstName:first_name:PER:ASCII:Y
FullName:full_name:PER:ASCII:Y
knownas:known_as:PER:ASCII:Y
MaritalStatus:marital_status:PER:ASCII:Y
middleName:middle_names:PER:ASCII:Y
country:country:PA:ASCII:Y
socialsecurity:national_identifier:PER:ASCII:Y
```

```
Sex:sex:PER:ASCII:Y
Title:title:PER:ASCII:Y
suffix:suffix:PER:ASCII:Y
street1:address_line1:PA:ASCII:Y
zip:postal_code:PA:ASCII:Y
Address1:address_line1:PA:ASCII:Y
Address2:address_line2:PA:ASCII:Y
Address3:address_line3:PA:ASCII:Y
TelephoneNumber1:telephone_number_1:PA:ASCII:Y
TelephoneNumber2:telephone_number_2:PA:ASCII:Y
TelephoneNumber3:telephone_number_3:PA:ASCII:Y
town_or_city:town_or_city:PA:ASCII:Y
state:region_2:PA:ASCII:Y
Start_date:effective_start_date:PER:DATE:Y
End_date:effective_end_date:PER:DATE:Y
per_updateTime:last_update_date:PER:DATE:Y
pa_updateTime:last_update_date:PA:DATE:Y
```

同期化される Oracle Human Resources の追加属性の変更

同期化される Oracle Human Resources の属性を追加する手順は、次のとおりです。

1. `oraclehragent.cfg.master` ファイルをコピーし、*`Agent_Name`*`.cfg` 以外の名前を付けます。これは、Directory Integration and Provisioning Server がこの名前の構成ファイルを生成し、Oracle Human Resources エージェントの実行時に構成情報を渡すのに使用するためです。

2. このファイルにレコードを追加することにより、Oracle Human Resources の同期化される属性を追加します。これには、次の情報が必要です。

   - 属性値の抽出元になるデータベース内の表名。これらの表は、39-2 ページの表 39-1 にリストされています。このファイルでは、同期に使用される 4 つの表に、省略された名前が使用されます。
   - 表の列名。
   - 列のデータ型。有効な値は ASCII、NUMBER、DATE です。

   また、列名に属性名を割り当てる必要もあります。これは、出力ファイル内でこの属性を識別するための出力タグとして動作します。このタグは、マッピング・ルール内で Oracle Human Resources の属性と Oracle Internet Directory の属性の間の規則を確立するために使用されます。

   `map` 列（レコード内の最後の列）が値 `Y` に設定されていることを確認する必要もあります。

注意： 属性リストに新規属性を追加する場合は、orclodipAttributeMappingRules 属性内に対応するルールを定義する必要があります。定義しない場合、Oracle Human Resources の属性は、Oracle Human Resources コネクタに抽出されても Oracle Internet Directory と同期化されません。

Oracle Human Resources の同期化される属性の除外

現在 Oracle Internet Directory と同期化されている Oracle Human Resources の属性を除外する手順は、次のとおりです。

1. oraclehragent.cfg.master ファイルをコピーし、*Agent_Name*.cfg 以外の名前を付けます。これは、Directory Integration and Provisioning Server がこの名前の構成ファイルを生成し、Oracle Human Resources コネクタの実行時に構成情報を渡すのに使用するためです。
2. 次のいずれか 1 つを行います。
   - 属性リスト内の対応するレコードの前にハッシュ符号（#）を付けてコメント化する。
   - 列 map の値を N に設定する。

構成ファイルでの SQL SELECT 文の構成による複雑な選択基準のサポート

前述のサポートされている属性の構成が、Oracle Human Resources データベースからデータを抽出するには不十分な場合、Oracle Human Resources エージェントは、構成ファイル内にある事前構成済の SQL SELECT 文の実行もサポートします。構成ファイルには、このサポートを示すタグ（構成ファイル内の [SELECT] ）があります。

次の例は、Oracle Human Resources データベースから情報の一部を取得するサンプルの SELECT 文を示しています。SQL 文を配置できるのは、[SELECT] タグの下のみです。BINDVAR バインド変数は、増分変更を取得するために必要です。代入値によって、この変数の値（タイムスタンプ）が Oracle Human Resources コネクタに渡されます。

SELECT 文で取得される列の式にはすべて列名を指定する必要があります。たとえば、REPLACE(ppx.email_address),'@ORACLE.COM','') は、EMAILADDRESS として取得されます。Oracle Human Resources コネクタは、REPLACE(ppx.email_address),'@ORACLE.COM''' 式の結果の属性値とともに、EMAILADDRESS を属性名として出力ファイルに書き出します。

次に構成ファイル内の SELECT 文の例を示します。

```
[SELECT]

SELECT
     REPLACE(ppx.email_address),'@ORACLE.COM',''), EMAILADDRESS ,
     UPPER(ppx.attribute26) GUID,
```

```
    UPPER(ppx.last_name) LASTNAME,
    UPPER(ppx.first_name) FIRSTNAME,
    UPPER(ppx.middle_names) MIDDLENAME,
    UPPER(ppx.known_as) NICKNAME,
    UPPER(SUBSTR(ppx.date_of_birth,1,6)) BIRTHDAY,
    UPPER(ppx.employee_number) EMPLOYEEID,
    UPPER(ppos.date_start)  HIREDATE,
FROM
   hr_organization_units hou,
   per_people_x ppx,
   per_people_x mppx,
   per_periods_of_service ppos
  WHERE
      pax.supervisor_id  = mppx.person_id(+)
  AND pax.organization_id = hou.organization_id(+)
  AND ppx.person_id = ppos.person_id
  AND ppx.person_id = pax.person_id
  AND ppos.actual_termination_date IS NULL
  AND UPPER(ppx.current_employee_flag) = 'Y'
  AND ppx.last_update_date >= (:BINDVAR,'YYYYMMDDHH24MISS')
```

タスク 3: Oracle Human Resources コネクタに関するマッピング・ルールの設定

属性マッピング・ルールは、Directory Integration and Provisioning Server が Oracle Human Resources と Oracle Internet Directory の間で属性を変換する方法を制御します。Directory Integration and Provisioning Server が使用するマッピング・ルールはカスタマイズできます。

Oracle Human Resources エージェント・プロファイルには、デフォルトのマッピング・ファイルがあります。一連のマッピング・ルールはこのマッピング・ファイルの `orclodipAttributeMappingRules` 属性に格納されています。この情報は、`oraclehragent.map.master` というファイルにも格納されています。このファイルは、`$ORACLE_HOME/ldap/odi/conf` ディレクトリの下にあります。

注意： `oraclehragent.map.master` ファイルは変更できません。バックアップとして機能しているためです。

関連項目： `oraclehragent.map.master` の内容およびマッピング・ルール・レコードの形式の説明は、33-5 ページの「マッピング・ルールとその形式」を参照してください。

タスク 4: Oracle Human Resources から Oracle Internet Directory への同期の準備

この項では、Oracle Human Resources から Oracle Internet Directory への同期の設定方法を説明します。

同期の準備

Oracle Human Resources と Oracle Internet Directory の間の同期を準備するには、次の手順に従います。

1. Oracle Human Resources コネクタと Directory Integration and Provisioning Server が、Oracle Human Resources コネクタの実行元であるホストにインストールされていることを確認します。

   関連項目： 詳細は、Oracle Internet Directory 10*g*（9.0.4）のファイル `install.txt` およびリリース・ノートを参照してください。

2. Oracle Human Resources システムにアクセスするための情報を持っていることを確認します。これには次の情報があります。
   - Oracle Human Resources システムのデータベースへの接続文字列
   - アクセス・アカウント
   - パスワード
3. 39-4 ページの「タスク 1: Oracle Human Resources コネクタのディレクトリ統合プロファイルの構成」の説明に従って、Oracle Human Resources コネクタの統合プロファイルを構成します。統合プロファイルのすべての値が適切に設定されていることを確認します。これには次の値があります。
   - Oracle Human Resources の属性リスト
   - Oracle Human Resources の属性マッピング・ルール
   - スケジューリング間隔
4. すべてを適切に設定した後、プロファイル・ステータス（`orclodipagentcontrol`）属性を `ENABLE` に設定します。この設定によって、Oracle Human Resources コネクタを実行する準備が完了していることを示します。
5. それぞれのホストで Oracle ディレクトリ・サーバーと Oracle Human Resources が実行されていない場合、これらを起動します。
6. 準備が完了した後、まだこのホストで Directory Integration and Provisioning Server が実行されていない場合は、これを起動します。

   関連項目： Directory Integration and Provisioning Server を起動および停止する方法は、35-9 ページの「Oracle Directory Integration and Provisioning Server の起動、停止および再起動」を参照してください。

同期のプロセス

Oracle Human Resources システム、Oracle Internet Directory および Directory Integration and Provisioning Server が実行され、Oracle Human Resources コネクタが使用可能になると、Directory Integration and Provisioning Server は、Oracle Human Resources システムから Oracle Internet Directory への変更の同期を自動的に開始します。そのプロセスは、次のとおりです。

1. 前回実行日時（orclodipLastExecutionTime）およびスケジューリングの間隔（orclodipschedulinginterval）に指定されている値に従って、Directory Integration and Provisioning Server は、Oracle Human Resources コネクタを起動します。
2. Human Resources エージェントは次のものを抽出します。
   - 統合プロファイル内の orclodipLastSuccessfulExecutionTime 属性に指定されている日時に基づいた Oracle Human Resources System からのすべての変更
   - プロファイル内の orclodipAgentConfigInfo 属性に指定されている属性のみ

   変更は、Oracle Human Resources のインポート・ファイルである *$ORACLE_HOME*/ldap/odi/import/HR_Agent_Name.dat に書き込まれます。
3. エージェントは、実行を完了した後、次のようなデータ・ファイルを作成します。

```
FirstName: John
LastName: Liu
EmployeeNumber: 12345
Title: Mr.
Sex: M
MaritalStatus: Married
TelephoneNumber: 123-456-7891
Mail: Jliu@my_company.com
Address: 100 Jones Parkway
City: MyTown
```

4. Oracle Directory Integration and Provisioning Server は、次の操作を実行して変更を Oracle Internet Directory へインポートします。
   - インポート・ファイルからの各変更レコードの読取り。
   - 統合プロファイルのマッピング・ルール（orclodipAttributeMappingRules）に指定されている規則に基づいた、各変更レコードの LDAP 変更エントリへの変換。

5. すべての変更内容が Oracle Internet Directory に正常にインポートされると、Oracle Human Resources コネクタは、インポート・ファイルをアーカイブ・ディレクトリ（$*ORACLE_HOME*/ldap/odi/import/archive）に移動します。ステータスの属性である前回実行日時（orclodipLastExecutionTime）と前回成功実行日時（orclodipLastSuccessfulExecutionTime）を現行の日時に更新します。

   インポート操作に失敗した場合は、前回実行日時（orclodipLastExecutionTime）属性のみが更新され、コネクタは前回成功実行日時（orclodipLastSuccessfulExecutionTime）属性に基づいて Human Resources システムからの変更の抽出を再試行します。失敗の理由は、$*ORACLE_HOME*/ldap/odi/HR_Agent_Name.trc のトレース・ファイルに記録されます。

Oracle Human Resources からの Oracle Internet Directory のブートストラップ

Oracle Human Resources から Oracle Internet Directory をブートストラップする方法は 2 つあります。

- Oracle Human Resources コネクタを使用する。統合プロファイルで、orclodipLastSuccessfulExecutionTime を Oracle Human Resources がインストールされた時間よりも前に設定する。
- 外部ツールを使用して、Oracle Human Resources から Oracle Internet Directory にデータを移行する。

40

Oracle E-Business Suite へのデータ・プロビジョニングの統合

Oracle Internet Directory 10*g*（9.0.4）では、Oracle Directory Provisioning Integration Service を使用して、ユーザー・アカウントと Oracle E-Business Suite からの他のユーザー情報を同期させることができます。

関連項目： この統合の詳細および管理方法は、Oracle E-Business Suite のドキュメントを参照してください。

41

サード・パーティ・ディレクトリとの統合に関する考慮事項

この章では、サード・パーティ・ディレクトリとの統合を行う前に決定が必要な事項について説明します。これらの事項を決定した後、ディレクトリ間でブートストラップおよび同期を構成できます。この章を読む前に、次の章の内容を理解しておく必要があります。

- 第 19 章「Oracle Identity Management レルムの配置」
- 第 30 章「Oracle Delegated Administration Services」
- 第 31 章「Oracle Internet Directory セルフ・サービス・コンソール」

この章では、次の項目について説明します。

サード・パーティ・ディレクトリとの統合に関する一般的考慮事項

LDAP ディレクトリ・サーバーをすでに所有している企業に Oracle Internet Directory を配置する場合は、両方のディレクトリが同じ環境に共存するように構成する必要があります。ご使用の環境でデータベース・サーバー側からのエンタープライズ・ユーザーがサポートされている場合は、ディレクトリ間での単純な同期を構成します。ただし、サード・パーティ・ディレクトリがエンタープライズ・ディレクトリとして使用されていて、アプリケーションの Oracle Application Server Suite が配置されている場合は、同期を構成する前に、認証管理レルムを構成する必要があります。したがって、ディレクトリの共存には、次のいずれかの配置が必要です。

- エンタープライズ・ユーザー・セキュリティをサポートするための Oracle Internet Directory との単純な同期
- Oracle Application Server Suite の様々なアプリケーションに対してすべてのエンタープライズ・ユーザーを有効にするための Oracle Application Server Infrastructure との完全な統合

この項では、次の項目について説明します。

サード・パーティ・ディレクトリとの単純な同期の構成

SunONE Directory Server との単純な同期の構成については、第 42 章「SunONE（iPlanet）Directory Server との統合」を参照してください。

Microsoft Active Directory との単純な同期の構成については、第 43 章「Microsoft Windows 環境との統合」を参照してください。

Oracle Application Server Infrastructure との完全な統合の構成

すべての Oracle Application Server コンポーネントが認証管理レルムに依存するため、Oracle Application Server との完全な統合には、そのレルムのコンテナに関する基本的な決定を行う必要があります。これらの事項を決定した後、ディレクトリ間でブートストラップおよび同期を構成できます。

企業の中央ディレクトリとなるディレクトリの選択

企業の中央ディレクトリは、企業内のすべてのユーザー、グループおよびレルムに関する情報の事実上のソースです。Oracle Internet Directory またはサード・パーティ・ディレクトリのいずれかを指定できます。

この項では、次の項目について説明します。

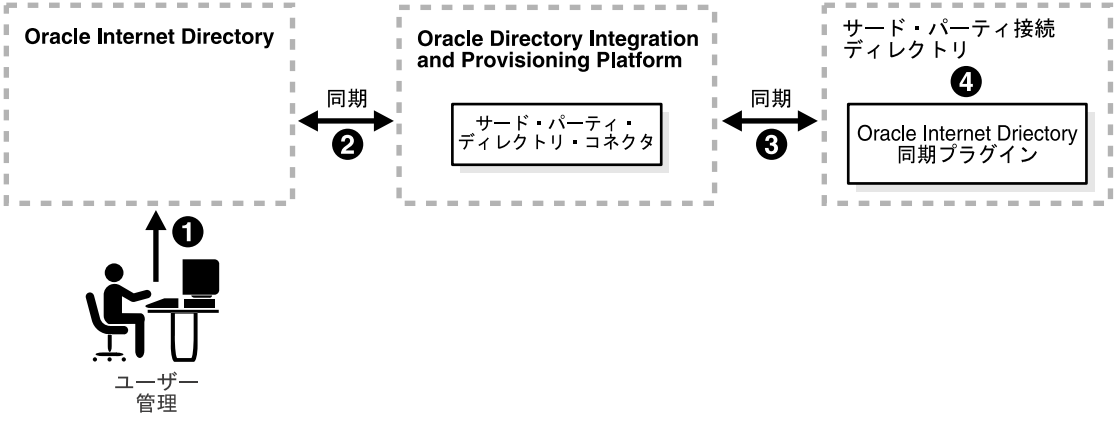
- 企業の中央ディレクトリとしての Oracle Internet Directory
- 中央ディレクトリとしてのサード・パーティ・ディレクトリ

企業の中央ディレクトリとしての Oracle Internet Directory

Oracle Internet Directory が中央ディレクトリの場合、ユーザー・オブジェクト、グループ・オブジェクトおよびレルム・オブジェクトを作成すると、Oracle Internet Directory はすべての Oracle コンポーネントおよびサード・パーティ・ディレクトリに関するプロビジョニング情報のソースになります。その後、企業全体のユーザー・オブジェクトとグループ・オブジェクトが、各種 Oracle コンポーネントおよびサード・パーティ・ディレクトリ内に Oracle Internet Directory からプロビジョニングされます。

図 41-1 に、Oracle Internet Directory が企業の中央ディレクトリとなっている場合の通常の配置を示します。

図 41-1 Oracle Internet Directory を中央ディレクトリとして使用するコンポーネント間の相互作用



41-3 ページの図 41-1 に示すとおり、Oracle Internet Directory が企業の中央ディレクトリの場合、ユーザーまたはグループの通常のプロビジョニングは次のプロセスに従います。

1. ユーザー・エントリまたはグループ・エントリは、Oracle Internet Directory セルフ・サービス・コンソール、Oracle Directory Manager またはコマンドライン・ツールを使用して Oracle Internet Directory に作成されます。
2. 次にスケジュールされた時刻に、エントリ作成イベントが、Oracle Directory Integration and Provisioning Platform 内のサード・パーティ・ディレクトリ・コネクタによって読み取られます。
3. 統合プロファイル内のマッピング情報に従って、Oracle Internet Directory 内のユーザー属性またはグループ属性が、サード・パーティ・ディレクトリのスキーマで必要な、対応するユーザー属性またはグループ属性に適切にマッピングされます。
4. ユーザー・エントリおよびグループ・エントリがサード・パーティ・ディレクトリ内に作成されます。

次の場合、Oracle Internet Directory 内でユーザー・エントリが変更されます。

- 新しい属性がエントリに追加される場合
- 既存の属性の値が変更される場合
- 既存の属性が削除される場合

Oracle Internet Directory が企業の中央ディレクトリの場合、ユーザー・エントリまたはグループ・エントリの変更時に実行されるイベントの順序は次のとおりです。

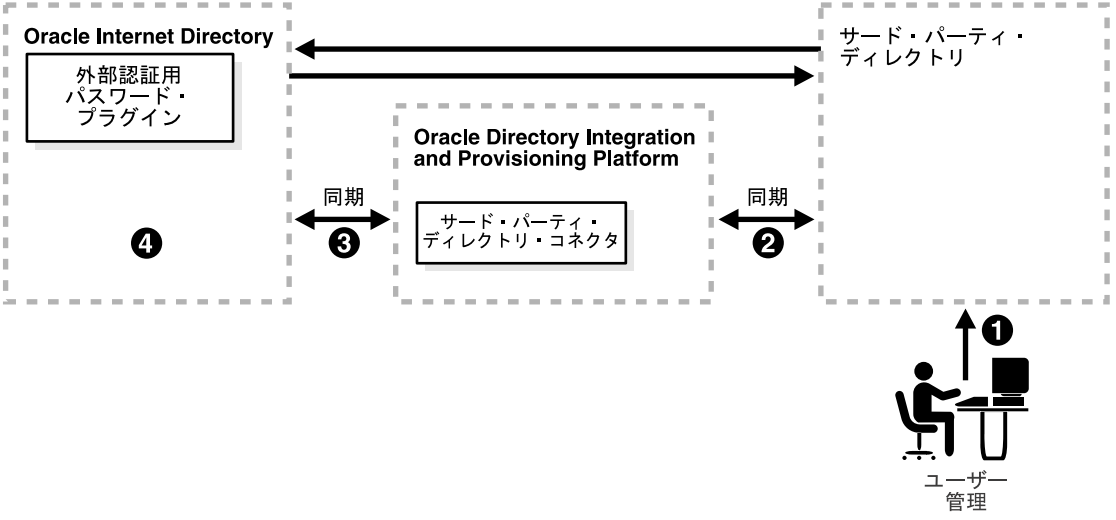
1. Oracle Internet Directory セルフ・サービス・コンソール、Oracle Directory Manager またはコマンドライン・ツールを使用して、エントリが変更されます。
2. 次にスケジュールされた時刻に、エントリ変更イベントが、Oracle Directory Integration and Provisioning Platform 内のサード・パーティ・ディレクトリ・コネクタによって読み取られます。
3. 統合プロファイル内のマッピング情報に従って、Oracle Internet Directory 内の属性が、接続ディレクトリ内の対応する属性に適切にマッピングされます。
4. サード・パーティ・ディレクトリ内でユーザー・エントリが変更されます。

中央ディレクトリとしてのサード・パーティ・ディレクトリ

サード・パーティ・ディレクトリが中央ディレクトリの場合、ユーザー・オブジェクト、グループ・オブジェクトおよびレルム・オブジェクトを作成すると、サード・パーティ・ディレクトリはすべての Oracle コンポーネントおよびその他の・ディレクトリに関するプロビジョニング情報のソースになります。この場合、Oracle Internet Directory は Oracle コンポーネントのサポート用に配置されます。このサポートを提供するために、Oracle Internet Directory には、サード・パーティ・ディレクトリ内のエントリの識別を可能にするフットプリントが格納されています。

図 41-2 に、サード・パーティ・ディレクトリが企業の中央ディレクトリとなっている場合の通常の配置を示します。

図 41-2 サード・パーティ・ディレクトリを使用する中央ディレクトリとして使用するコンポーネント間の相互作用



ユーザーまたはグループのプロビジョニング・プロセス

図 41-2 に示すとおり、サード・パーティ・ディレクトリが企業の中央ディレクトリの場合、ユーザーまたはグループの通常のプロビジョニングは次のプロセスに従います。

1. ユーザー・エントリまたはグループ・エントリがサード・パーティ・ディレクトリ内に作成されます。
2. 次にスケジュールされた時刻に、エントリ作成イベントが、Oracle Directory Integration and Provisioning Platform 内のサード・パーティ・ディレクトリ・コネクタによって読み取られます。
3. 統合プロファイル内のマッピング情報に従って、サード・パーティ・ディレクトリのユーザー属性またはグループ属性が Oracle Internet Directory 内の対応する属性にマッピングされます。
4. ユーザー・エントリまたはグループ・エントリが Oracle Internet Directory 内に作成されます。

ユーザー・エントリまたはグループ・エントリの変更プロセス

次の場合、サード・パーティ・ディレクトリ内でエントリが変更されます。

- 新しい属性がエントリに追加される場合
- 既存の属性の値が変更される場合
- 既存の属性が削除される場合

サード・パーティ・ディレクトリが企業の中央ディレクトリの場合、ユーザー・エントリまたはグループ・エントリの変更は次のプロセスに従います。

1. サード・パーティ・ディレクトリ内でエントリが変更されます。
2. 次にスケジュールされた時刻に、エントリ変更イベントが、Oracle Directory Integration and Provisioning Platform 内のサード・パーティ・ディレクトリ・コネクタによって読み取られます。
3. 統合プロファイル内のマッピング情報に従って、サード・パーティ・ディレクトリ内の属性が Oracle Internet Directory 内の対応する属性に適切にマッピングされます。
4. Oracle Internet Directory 内でユーザー・エントリまたはグループ・エントリが変更されます。

図 41-2 に示すとおり、サード・パーティ・ディレクトリが企業の中央ディレクトリの場合、パスワード・リポジトリとして動作しているディレクトリ内でパスワードの変更が非同期に発生します。これは、プラグインを使用することによって発生します。

パスワードの格納場所の選択

企業の中央ディレクトリとなるディレクトリに関係なく、パスワードは、一方または両方のディレクトリに格納できます。いずれのオプションにも利点と欠点があります。この項では、次の項目について説明します。

- 1 つのディレクトリにのみパスワードを格納する場合の利点と欠点
- 両方のディレクトリにパスワードを格納する場合の利点と欠点

1 つのディレクトリにのみパスワードを格納する場合の利点と欠点

攻撃される箇所を 1 つに減らすことによって、1 つのディレクトリにのみパスワードを格納すると、パスワードのセキュリティがより強力になります。また、パスワードが変更された場合の同期の問題もなくなります。

ただし、1 つのディレクトリにのみパスワードを格納すると、ネットワーク全体に対するシングル・ポイント障害の原因となります。障害が発生したディレクトリがサード・パーティ・ディレクトリの場合、ユーザーは、Oracle Internet Directory 内でユーザー・フットプリントが使用可能な場合でも Oracle コンポーネントにアクセスできません。

また、中央ディレクトリにのみパスワードを格納すると同期の問題はなくなりますが、そのディレクトリに対してユーザーを認証するアプリケーションを有効にする必要があります。これには、適切なプラグインを使用する必要があります。たとえば、企業の中央ディレクトリおよび中央パスワード・ストアの両方として Microsoft Active Directory を使用している場合は、Microsoft Active Directory に対してユーザーを認証するアプリケーションを有効にする必要があります。これには、外部認証プラグインを使用します。SunONE Directory Server に対する認証にも、同様のメカニズムがサポートされています。

注意： Oracle コンポーネントは、パスワード・ベリファイアを使用してユーザーを認証します。パスワードがサード・パーティ・ディレクトリに格納される場合、それらのベリファイアは Oracle Internet Directory に格納されません。ただし、Oracle コンポーネントを使用してパスワードが変更された場合は、Oracle Internet Directory 内でベリファイアが生成および格納されます。

両方のディレクトリにパスワードを格納する場合の利点と欠点

両方のディレクトリにパスワードを格納する場合、理想的には、リアルタイムでパスワードを同期化する必要があります。

Oracle Internet Directory 10*g*（9.0.4）の場合、パスワードはリアルタイムではなく、スケジュールに従って同期化されます。これは、中央ディレクトリ内でパスワードが変更された時刻とその変更がもう 1 つのディレクトリに記録される時刻の間に、明確な差があることを意味します。中央ディレクトリとして Oracle Internet Directory を配置した場合、パスワード値は、Oracle Internet Directory から接続ディレクトリへ定期的に同期化されます。この同期化を行うには、レルムのパスワード・ポリシーと可逆暗号化の両方を有効にする必要があります。

関連項目：

- パスワード・ポリシーの設定方法は、第 15 章「Oracle Internet Directory のパスワード・ポリシー」を参照してください。
- 可逆暗号化の詳細は、第 16 章「パスワード・ベリファイアのディレクトリ格納」を参照してください。

通常、パスワード値はハッシュされます。両方のディレクトリが同一のハッシング・アルゴリズムを使用する場合は、そのままの状態でハッシュ値を同期化できます。たとえば、SunONE Directory Server と Oracle Internet Directory が統合されている環境があるとします。これらのディレクトリは両方とも共通のハッシング・アルゴリズムに対応しています。Oracle Internet Directory でサポートされているハッシング方法を使用して、パスワードをハッシュし、SunONE Directory Server に格納する場合、SunONE Directory Server から Oracle Internet Directory へのパスワードの同期化は、その他の属性の場合と同様です。

ただし、両方のディレクトリで同一のハッシング・アルゴリズムがサポートされていない場合は、クリアテキスト形式でのみパスワードを同期化する必要があります。セキュリティ上の理由から、Oracle Internet Directory とのパスワードの同期は、SSL モードでのみ可能（サーバー専用認証）です。

Oracle Internet Directory が事実上のソースの場合および Oracle Internet Directory でサポートされているハッシング・アルゴリズムがその他のディレクトリによってサポートされていない場合でも、パスワードの可逆暗号化が有効なときには SSL モード 2（`sslmode=2`）経由で同期化が可能です。

Microsoft Active Directory が事実上のソースの場合に Microsoft Active Directory 内でパスワードを変更すると、プラグインがパスワード変更を妨害し、変更したパスワードを（可能な場合、暗号化形式で）新しい属性に格納します。その属性は、Oracle Internet Directory と同期化できます。Oracle Internet Directory が企業の中央ディレクトリおよび中央パスワード・ストアの場合も、同様のプロセスが必要です。

注意： 両方のディレクトリが同一のハッシング・アルゴリズムを使用しない場合、Oracle Internet Directory のデフォルトのインストール環境ではパスワードの同期化は実行できません。構成する必要があります。

Oracle Internet Directory が中央ディレクトリではない配置では、サード・パーティ・ディレクトリによってパスワード・ポリシーが施行されます。サード・パーティ・ディレクトリに対する認証要求がある場合、このディレクトリによって認証が成功したか失敗したかが応答されます。ただし、サード・パーティ・ディレクトリからのパスワード・ポリシーの詳細なエラーは、Oracle Internet Directory に配信されないため、クライアント・アプリケーションにも配信されません。

関連項目： パスワードの同期の詳細は、次の章を参照してください。

- 第 42 章「SunONE（iPlanet）Directory Server との統合」
- 第 43 章「Microsoft Windows 環境との統合」

プラグインの詳細は、次の章を参照してください。

- 第 45 章「Oracle Internet Directory プラグイン・フレームワーク」
- 第 47 章「カスタマイズされた外部認証プラグインの設定」

ディレクトリ情報ツリーの構造の選択

インストール時に、各ディレクトリ・サーバーがデフォルトのドメインとデフォルトの**ディレクトリ情報ツリー**構造を作成します。サード・パーティ・ディレクトリとの同期化の場合は、両方のディレクトリ上に同様のディレクトリ情報ツリー構造を作成することもできます。それ以外の場合は、ドメイン・レベルのマッピングが必要です。ドメイン・レベルのマッピングを選択する場合は、属性に識別名を持つエントリとグループとの同期化に制限があります。

この項では、次の項目について説明します。

- 両方のディレクトリ上での同一ディレクトリ情報ツリー構造の作成
- ドメイン・レベルのマッピングと制約

両方のディレクトリ上での同一ディレクトリ情報ツリー構造の作成

両方のディレクトリ上で同一のディレクトリ情報ツリーを構成することをお薦めします。これによって、すべてのユーザー・オブジェクトとグループ・オブジェクトをそのままの状態で同期化できるため、一方のディレクトリ内の識別名を持つエントリを別のディレクトリの URL にマッピングする必要がなくなります。また、このようなマッピングで発生する可能性があるパフォーマンスの問題も回避できます。

同一のディレクトリ情報ツリーを作成するには、まず、企業の中央ディレクトリとなるディレクトリを決定し、その後、それに合わせてもう一方のディレクトリ情報ツリーを変更します。ディレクトリ統合プロファイルとプロビジョニング・プロファイルを更新して、確実にドメイン・レベルのルールを反映してください。

ユーザーが Oracle Application Server Single Sign-On を介して Oracle アプリケーションにアクセスできるようにするには、ディレクトリ情報ツリーを、独自の認証および認可ドメインを持つ個別の認証管理レルムとして識別することをお薦めします。

> **関連項目：** 認証管理レルムの詳細は、第 19 章「Oracle Identity Management レルムの配置」を参照してください。

ドメイン・レベルのマッピングと制約

両方のディレクトリ上に同一のディレクトリ情報ツリーを持つことが不可能な場合は、Oracle Internet Directory と接続ディレクトリの間でドメインをマッピングする必要があります。たとえば、コンテナ `dc=mydir,dc=com` の下にあるエントリはすべて、Oracle Internet Directory 内の `dc=myoid,dc=com` の下で同期化する必要があります。これを実行するには、ドメイン・レベルのマッピング・ルールに指定します。

すべてのユーザーおよびグループの同期が目的の場合は、適切なドメイン・レベルのマッピングですべてのユーザー・エントリを同期化できます。ただし、グループ・エントリを同期化する場合は、時間がかかり、制限が追加される場合があります。この項では、ドメイン・レベルでマッピングされている場合のユーザーおよびグループの両方の同期の例を示します。

例 : ユーザー・エントリ・マッピング

マッピング・ファイルでは、SunONE Directory Server 内のエントリは uid=name,ou=people,o=iplanet.org という形式をとるとします。また、Oracle Internet Directory 内のエントリは、cn=name,cn=users,dc=iplanet,dc=com という形式をとるとします。SunONE Directory Server 上のネーミング属性は uid ですが Oracle Internet Directory 上では cn です。

マッピング・ファイルには次のようなルールがあります。

```
DomainRules
ou=people,o=iplanet.org: cn=users,dc=iplanet,dc=com: cn=%, cn=users,
dc=iplanet,dc=com
AttributeRules
Uid:1: :person:cn: :inetorgperson:
```

最後の行の 2 番目の列の 1 という値は、各変更が SunONE Directory Server から Oracle Internet Directory へ伝播される場合に uid 属性が必要であることを示しています。これは、Oracle Internet Directory 内のエントリの識別名を構成するには、常に uid を使用可能にする必要があるためです。

例 : グループ・エントリ・マッピング

ドメイン・レベルでマッピングされている場合、グループ・エントリの同期化は複雑になります。グループ・メンバーシップ（識別名）には、同期後、有効な識別名の値が必要です。これは、ユーザー識別名に対して行われたドメイン・レベルのマッピングをグループ・メンバーシップの値に適用する必要があることを意味します。

たとえば、ユーザー識別名の値を次のようにマッピングするとします。

```
ou=people,o=iplanet.org: cn=users,dc=iplanet,dc=com:
```

これは、ou=people,o=iplanet.org 下のすべてのユーザー・エントリが cn=users,dc=iplanet,dc=com に移動されることを示します。

グループ・メンバーシップは、次のようにマッピングする必要があります。

```
uniquemember: : : groupofuniquenames: uniquemember: :groupofuniquenames:
dnconvert(uniquemember)
```

たとえば、uniquemember の値が cn=testuser1,ou=people,o=iplanet.org の場合、その値は cn=testuser1,cn=users,dc=iplanet,dc=com になります。

また、uniquemember の値が cn=testuser1,dc=subdomain,ou=people,o=iplanet.org の場合、その値は cn=testuser1,dc=subdomain,cn=users,dc=iplanet,dc=com になります。

これは、ネーミング属性または RDN 属性が両方のディレクトリで同じ場合に適した解決方法です。ネーミング属性が ou=people,o=iplanet.org:cn=users,dc=iplanet,dc=com:cn=%,cn=users,dc=iplanet,dc=com などのようにそれぞれのディレクトリで異なる場合、グループ・メンバーシップの実際の識別名は、指定したマッピング・ルールでは導出できません。現在、このような場合に、uniquemember またはその他の識別名タイプの属性に対してドメイン・レベルのマッピングを行うことはできません。

グループ・メンバーシップを同期化する場合は、ソース・ディレクトリと宛先ディレクトリに同じネーミング属性を指定してください。

関連項目： マッピング・ルールの指定方法については、33-7 ページの「マッピング・ルール属性の形式」を参照してください。

loginID 属性の選択

loginID 属性には、Oracle コンポーネントにログインする際のエンド・ユーザーの識別情報が含まれます。この属性は、Oracle Internet Directory のコンテナ cn=common,cn=products,cn=oracleContext,*identity_management_realm* の下に、属性 orclcommonnicknameattribute の値として格納されます。

デフォルトでは、orclcommonnicknameattribute の値は uid です。これは、ログインに使用される識別情報がユーザー・エントリの uid 属性に格納されることを意味します。

接続ディレクトリにログイン用の特定の属性が存在する場合は、Oracle Internet Directory 内の正しい orclcommonnicknameattribute にその属性をマッピングする必要があります。これは、サード・パーティ・ディレクトリとの同期に関連付けられているコネクタ用のマッピング・ファイル内のマッピング・ルールの 1 つである必要があります。

たとえば、Oracle Internet Directory を Microsoft Active Directory と同期させると想定します。また、後者では、ログイン識別子がユーザー・エントリの userPrincipalName 属性に含まれているとします。userPrincipalName 属性の値を Oracle Internet Directory に同期させ、orclcommonnicknameattribute 属性の値である uid 属性に格納します。このマッピングは、ディレクトリ統合プロファイル内のマッピング・ルールに反映する必要があります。

ログイン用のその他の属性も使用できます。たとえば、ログインに employeeID を使用する場合は、それに応じてマッピング・ルールを設定できます。この設定は、構成には影響しません。

関連項目： ログイン名用の属性の設定方法は、31-11 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用した認証管理レルムの構成」を参照してください。

ユーザー検索ベースの選択

ユーザー検索コンテキストは、ユーザーが存在するすべてのコンテナをリストする複数値属性によって表されます。配置に応じて、ユーザー集団全体にわたるユーザー検索コンテキスト値を設定するか、Oracle Internet Directory セルフ・サービス・コンソールを使用してユーザー検索コンテキスト属性にコンテナを追加します。

> **関連項目：** ユーザー検索コンテキストの設定方法は、31-11 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用した認証管理レルムの構成」を参照してください。

グループ検索ベースの選択

グループ検索コンテキストは、グループが存在するすべてのコンテナをリストする複数値属性によって表されます。配置に応じて、すべてのグループ・エントリにわたるグループ検索コンテキスト値を設定するか、Oracle Internet Directory セルフ・サービス・コンソールを使用してグループ検索コンテキスト属性にコンテナを追加します。

> **関連項目：** グループ検索コンテキストの設定方法は、31-11 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用した認証管理レルムの構成」を参照してください。

セキュリティ問題に対処する方法の決定

セキュリティ上の 3 つの主要な問題を考慮する必要があります。

- アクセス・ポリシー : ユーザー検索ベースとグループ検索ベースを不正なユーザーによるアクセスから適切に保護する必要があります。
- 同期 : Oracle Internet Directory およびサード・パーティ・ディレクトリへの接続時に SSL を使用するように Oracle Directory Integration and Provisioning Server を構成できます。これを実行すると、ディレクトリ・サーバー間で交換されるすべての情報が保護されます。
- パスワードの同期化 : 構成に応じて、パスワードを同期化できます。たとえば、Oracle Internet Directory が企業の中央ディレクトリの場合は、パスワードの変更を接続ディレクトリに通信できます。

  パスワードを同期化する場合は、SSL でのディレクトリ間の通信をサーバー専用認証で構成することをお薦めします。SSL での接続ディレクトリ間の通信を構成する手順は次のとおりです。

  1. 統合プロファイルで、通信モードが SSL であることを示すには、`connectedDirectoryURL` 属性を `host:port:1` の形式で構成します。ポート番号が SSL ポートであることを確認します。デフォルトの SSL ポート番号は 636 です。

2. 接続ディレクトリから証明書を生成します。サーバーからのトラスト・ポイント証明書が必要です。外部の証明書サーバーを使用する不要はありません。
3. 証明書を BASE64 エンコード形式にしてエクスポートします。
4. Oracle Wallet Manager を使用して、Oracle Wallet 内のトラスト・ポイントとして証明書をインポートします。
5. `$ORACLE_HOME/ldap/odi/conf` 内の `odi.properties` ファイルに Wallet の位置を指定します。
6. wp オプションを指定して Directory Integration and Provisioning Assistant を使用し、Wallet パスワードを格納します。
7. Oracle Directory Integration and Provisioning Server を SSL モードで起動します。

サード・パーティ・ディレクトリとの同期の構成 : 手順の説明

この項では、配置例を構成する手順を示します。「手順 4: 新しい認証管理レルムを作成するかどうかの判断」から「手順 6: ログイン識別子の選択」では、新しい認証管理レルムの構成およびそのパラメータの設定を行います。これらの手順を実行すると、すでに環境にインストールされている Oracle Application Server Single Sign-On およびその他の中間層アプリケーションの動作に影響する場合があります。したがって、各手順は慎重に実行し、アプリケーションの動作を確認してください。

> **関連項目：** 認証管理レルムおよび Oracle Application Server でのその役割の詳細は、第 19 章「Oracle Identity Management レルムの配置」を参照してください。

この項では、次の項目について説明します。

手順 1: Oracle Internet Directory 内のデフォルト認証管理レルムの識別

Oracle Internet Directory 内のデフォルト認証管理レルムを識別するには、次のコマンドを実行します。

```
ldapsearch -p port -h host -D distinguished_name -w password
-b "cn=common, cn=products,cn=oraclecontext" -s base "objectclass=*"
orcldefaultsubscriber
```

この配置例では、Oracle Internet Directory 内のデフォルト認証管理レルムは、`dc=us,dc=mycompany,dc=com` です。

手順 2: Oracle Internet Directory 内のユーザーおよびグループ検索ベースの識別

Oracle Internet Directory 内のユーザー検索コンテキストおよびグループ検索コンテキストを識別するには、次のコマンドを実行します。

```
ldapsearch -p <port> -h <host> -D distinguished_name -w <passwd>
b “cn=common, cn=products,cn=oraclecontext, <Identity Management Realm>” -s base
"objectclass=*"
```

`orclcommonusersearchbase` 属性と `orclcommongroupsearchbase` 属性の値を書き留めてください。これらは、ユーザー検索コンテキストおよびグループ検索コンテキストとして Oracle Internet Directory セルフ・サービス・コンソールに示される値です。

この配置例では、Oracle Internet Directory 内のユーザー検索コンテキストおよびグループ検索コンテキストは次のとおりです。

```
orclcommonusersearchbase is : cn=users,  dc=us,dc=mycompany,dc=com
orclcommongroupsearchbase is : cn=groups,  dc=us,dc=mycompany,dc=com
```

手順 3: リモート・ディレクトリのネーミング・コンテキストの識別

デフォルトのネーミング・コンテキストは、ユーザーが格納されているネーミング・コンテキストのルートです。各ディレクトリは独自の方法でデフォルトのネーミング・コンテキストを作成します。

Microsoft Active Directory を使用している場合は、そのディレクトリに対して次の ldapsearch を実行して、デフォルトのネーミング・コンテキストを識別します。

```
ldapsearch -p port -h host -D distinguished_name -w password -b "" -s base
"objectclass=*" defaultnamingcontext
```

通常、Microsoft Active Directory 内のユーザーの識別名は次の形式です。
`cn=user name, cn=users, defaultnamingcontext.`

ユーザーは *username@domain* などの名前にもバインドすることができます。

たとえば、ドメイン名が `newcompany.com` の場合、デフォルトのネーミング・コンテキストは `dc=newcompany,dc=com` になります。ユーザーの通常のログイン識別子は `user@newcompany.com` です。

SunONE Directory Server を使用する場合は、SunONE Directory Server に対して次の ldapsearch を実行して、SunONE Directory Server 内のネーミング・コンテキストを識別します。

```
ldapsearch -p port -h host -D distinguished_name -w password -b "" -s base
"objectclass=*" namingcontexts
```

異なるサブツリーには、それぞれ異なるユーザー・エントリのセットが存在します。同期化の対象のオブジェクトが含まれているネーミング・コンテキストを選択します。

手順 4: 新しい認証管理レルムを作成するかどうかの判断

Oracle Internet Directory のディレクトリ情報ツリーとサード・パーティ・ディレクトリのディレクトリ情報ツリーが異なる場合は、新しい認証管理レルムを作成することをお薦めします。これは、Oracle Internet Directory セルフ・サービス・コンソールを使用して行います。ただし、デフォルトのネーミング・コンテキストが `mycompany.com` である Microsoft Active Directory がサード・パーティ・ディレクトリの場合は、新しい認証管理レルムを作成する必要がないこともあります。

手順 5: ユーザー検索ベースとグループ検索ベースの選択

この方法は、前述の手順で説明したように新しい認証管理レルムを作成したかどうかによって異なります。

新しい認証管理レルムを作成した場合は、次の指示に従います。

1. ユーザー検索ベースとユーザー作成コンテキストを選択します。これは、Oracle Internet Directory セルフ・サービス・コンソールを使用して行います。サード・パーティ・ディレクトリ内のユーザーが格納されているコンテナを反映するようにユーザー検索コンテキストを設定します。詳細は、31-11 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用した認証管理レルムの構成」を参照してください。

   ユーザー作成コンテキストの設定と同じ方法に従います。

2. グループ検索ベースとグループ作成コンテキストを選択します。これは、Oracle Internet Directory セルフ・サービス・コンソールを使用して行います。サード・パーティ・ディレクトリ内のグループが格納されているコンテナを反映するようにグループ検索コンテキストを設定します。詳細は、31-11 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用した認証管理レルムの構成」を参照してください。

   グループ作成コンテキストの設定と同じ方法に従います。

新しい認証管理レルムを作成していない場合、すべての Oracle コンポーネントがユーザーおよびグループ・エントリにアクセスできるようにするには、Oracle Internet Directory セルフ・サービス・コンソールのデフォルトのパラメータを変更する必要があります。これは、次の手順に従って行います。

1. ユーザー検索コンテキストにサード・パーティ・ディレクトリ内のユーザー・コンテナの識別名を入力するか、検索コンテキストに指定されているコンテナのサブツリーを入力します。たとえば、次のいずれかを入力します。

   ```
   cn=users,dc=myCompany,dc=com
   ```

   ```
   dc=myCompany,dc=com.
   ```

2. グループ検索コンテキストにサード・パーティ・ディレクトリ内のグループ・コンテナの識別名を入力するか、検索コンテキストに指定されているコンテナのサブツリーを入力します。たとえば、次のいずれかを入力します。

   ```
   cn=groups,dc=myCompany,dc=com
   ```

   ```
   dc=myCompany,dc=com
   ```

   関連項目： 31-13 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用したユーザー・エントリの構成」

手順 6: ログイン識別子の選択

ログインに使用する属性は、`orclcommonnicknameattribute` です。Oracle Internet Directory セルフ・サービス・コンソールでは、このフィールドは「ログイン名の属性」という名前です。デフォルト値は `UID` です。デフォルト値を保持することをお薦めします。この属性を変更した場合（`mail` に変更した場合など）は、作業中のコンテナ内のすべてのエントリに `mail` 属性値が移入されていることを確認してください。移入されていない場合、ユーザーは Oracle Application Server Single Sign-On を介してログインできなくなります。

手順 7: 追加した変更を反映させるためのマッピング・ファイルの変更

属性を変更した場合は、デフォルトのマッピング・ファイルを変更する必要があります。各種マッピング・ルールを確認し、要件に応じて変更します。異なるコンテナにユーザーおよびグループがある場合は、同一のマッピング・ファイル内に複数のドメイン・ルールのセットを指定する必要がある場合があります。

SunONE Directory Server と Microsoft Active Directory との統合に関するデフォルトのマッピング・ルールは、*`$ORACLE_HOME`*`/ldap/odi/conf` ディレクトリにあります。

変更対象の重要なパラメータは次のとおりです。

- loginid 属性に関するマッピング・ルール
  - Microsoft Active Directory 用のデフォルト・プロファイルでは、サンプル・マッピング・ファイルの loginid 属性に関するデフォルトのマッピング・ルールは次のとおりです。

    ```
    Userprincipalname: : :user: uid: : :inetorgperson
    ```

  - SunONE Directory Server 用のデフォルト・プロファイルでは、UID が直接 UID 属性にマッピングされます。

    これは、ログインに使用される属性に応じて変更できます。たとえば、loginid として employeenumber を使用するには、マッピング・ファイルを次のように変更します。

    ```
    Employeenumber: : :user: uid: : :inetorgperson
    ```

- Kerberos ログイン用のマッピング・ルール

  Windows のネイティブ認証をサポートするため、Oracle Application Server Single Sign-On は、Windows 環境用に Kerberos ログインを使用します。この場合は、Windows ログイン用のマッピング・ルールが必要です。Kerberos ログイン用の属性は、cn=common,cn=public,cn=oraclecontext,*identity_management_realm* エントリ内の orclcommonkrbprincipalattribute です。デフォルトでは、krbPrincipalName に設定されます。

  Microsoft Active Directory との統合に関するデフォルトのマッピング・ルールは次のとおりです。

  ```
  Userprincipalname: : :user: krbPrincipalName: : :orclUserV2.
  ```

  このルールは、Microsoft Active Directory 内のユーザー・プリンシパル名を Kerberos プリンシパル名にマッピングします。Kerberos ログイン用に別の値をサポートする場合は、このルールを変更します。

  > **関連項目：** Oracle Application Server Single Sign-On での Windows のネイティブ認証に対するサポートについては、『Oracle Application Server Single Sign-On 管理者ガイド』を参照してください。

手順 8: 新しいマッピング・ルールのセットでの同期プロファイルの作成または変更

この手順を実行するには、Directory Integration and Provisioning Assistant を使用します。

```
dipassistant mp -profile profile_name odip.profile.mapfile=relative_path_name_of_
mapping_file
```

手順 9: アクセス制御の構成

次のいずれかにある各種コンテナへのアクセス制御を構成します。

- プロファイル `orclodipagentname=`*`profile_name`*`,cn=subscriber profile,cn=changelog subscriber,cn=oracle internet directory`'
- グループ `cn=odipgroup,cn=odi,cn=oracle internet directory`

サンプル ACI は *`ORACLE_HOME`*`/ldap/odi/samples/commonaci.ldif` に用意されています。このサンプルには次の属性が含まれていますが、すべての属性が同じ値です。

- `UserSearchBase`
- `GroupSearchBase`
- `UserCreateBase`
- `GroupCreateBase`

Oracle Directory Manager を使用して ACI をこれらのコンテナに設定できます。

手順 10: Directory Integration and Provisioning Assistant を使用したディレクトリのブートストラップ

ディレクトリをブートストラップするには、Directory Integration and Provisioning Assistant の `bootstrap` コマンドを使用します。

関連項目：

- 第 37 章「Oracle Directory Integration and Provisioning Platform におけるディレクトリのブートストラップ」
- Directory Integration and Provisioning Assistant の `bootstrap` コマンドの使用方法は、A-106 ページの「Directory Integration and Provisioning Assistant」を参照してください。

手順 11: 同期用の最終変更番号の更新

この手順を実行するには、次のように入力します。

```
dipassistant mp –profile profile_name -updlcn
```

Directory Integration and Provisioning Assistant によってディレクトリ統合プロファイルが読み取られて、接続ディレクトリが判断されます。

手順 12: Either Oracle Directory Manager または Directory Integration and Provisioning Assistant を使用したプロファイルの有効化

この手順を実行するには、Oracle Directory Manager または Directory Integration and Provisioning Assistant のいずれかを使用します。

関連項目：

- Oracle Directory Manager を使用してこの手順を実行する方法は、33-18 ページの「Oracle Directory Manager を使用したプロファイルの登録」を参照してください。
- Directory Integration and Provisioning Assistant を使用してこの手順を実行する方法は、33-20 ページの「Directory Integration and Provisioning Assistant による同期プロファイルの登録および登録解除」を参照してください。

手順 13（オプション）：パスワードを同期化するための外部認証プラグインの有効化

Oracle Internet Directory からサード・パーティ・ディレクトリにパスワード変更を同期化する必要がある場合は、次の指示に従って、外部認証プラグインを有効にします。

- 認証管理レルム内でパスワード・ポリシーを有効にします。これは、Oracle Internet Directory セルフ・サービス・コンソールまたは Oracle Directory Manager のいずれかを使用して実行できます。
- `orclpwdencryptionenable` 属性を `TRUE` に設定して可逆パスワード暗号化を有効にします。

Oracle Internet Directory で使用されているハッシング技術をサポートしないディレクトリにパスワードが同期される場合は、SSL モード 2（`sslmode=2`）の使用によってのみ同期が可能です。

関連項目：

- 15-10 ページの「セルフ・サービス・コンソールを使用したパスワード・ポリシーの管理」
- 15-6 ページの「Oracle Directory Manager を使用したパスワード・ポリシーの管理」
- 可逆暗号化の有効化の詳細は、16-2 ページの「Oracle Internet Directory に対する認証用パスワード・ベリファイアの格納および管理」を参照してください。

手順 14: Oracle Directory Integration and Provisioning Server の起動

この手順は、A-11 ページの「Oracle Directory Integration and Provisioning Server の起動」の指示に従って行います。

注意： パスワードを同期させるには、`sslmode=2`（サーバー専用認証）で Oracle Directory Integration and Provisioning Platform を起動します。

Oracle Internet Directory 10*g*（9.0.4）でのサード・パーティ統合の制限事項

Oracle Internet Directory 10*g*（9.0.4）では、スキーマおよび ACL の同期はサポートされません。スキーマまたは ACL を変更する場合は、手動で変更を適用する必要があります。そのために、schemasync ツールが用意されています。

関連項目： SchemaSync ツールの詳細は、A-123 ページの「schemasync ツールの構文」を参照してください。

42

SunONE（iPlanet）Directory Server との統合

この章では、Oracle Directory Integration and Provisioning Platform の SunONE コネクタを使用して、Oracle Application Server Infrastructure を SunONE Directory Server（Netscape Directory Server および iPlanet Directory Server）と統合する方法を説明します。

> **注意：** この章を読む前に、第 41 章「サード・パーティ・ディレクトリとの統合に関する考慮事項」を読み、配置に関する必要事項の決定および基本的な構成を行っておく必要があります。

この章では、次の項目について説明します。

- SunONE コネクタについて
- SunONE コネクタの構成
- 同期のプロセス
- SunONE Directory Server との同期に関するトラブルシューティング

SunONE コネクタについて

SunONE コネクタには、Oracle Directory Integration and Provisioning Server によって起動される同期コンポーネントが含まれています。このコンポーネントは、次の方法でディレクトリ間の一貫性を維持します。

- SunONE Directory Server からのデータと増分変更のインポート
- Oracle Internet Directory から SunONE Directory Server へのデータと増分変更のエクスポート

SunONE Directory Server および Oracle Internet Directory では、パスワードの格納に同様のハッシング技術がサポートされています。同じハッシング・アルゴリズムが使用されるように両方のディレクトリを構成し、マッピング・ルールを適切に構成すると、他の属性に対して行う場合と同様に SunONE コネクタでパスワードを同期化できます。SunONE Directory Server にパスワードを格納するには、この章で説明する SunONE Directory Server の外部認証プラグインを使用します。

注意： Oracle Internet Directory 10*g*（9.0.4）は、Netscape Directory Server リリース 4.13 および SunONE（iPlanet）Directory Server リリース 5.0、5.1 および 5.2 と同期させることができます。

関連項目：

- Oracle Internet Directory でサポートされているハッシング・アルゴリズムの詳細は、16-3 ページの「パスワード・ベリファイアを作成するためのハッシング・スキーム」を参照してください。
- SunONE（iPlanet）Directory Server の外部認証プラグインの構成については、42-11 ページの「タスク 4:（オプション）SunONE Directory Server 外部認証プラグインの構成」を参照してください。

SunONE Directory Server 統合の概念

この項では、次の項目について説明します。

- Oracle Internet Directory と SunONE Directory Server 間の同期
- SunONE Directory Server 外部認証プラグイン

Oracle Internet Directory と SunONE Directory Server 間の同期

SunONE Directory Server との同期は、ソース・ディレクトリから宛先ディレクトリへの増分変更の読取りに基づきます。両方のディレクトリで変更が行われる場合は、両方のディレクトリで変更ロギングを有効にしておく必要があります。完全な同期化のためには、変更ログおよび削除済とマークされたエントリが、異なるリリースで正確に構成されている必要があります。削除時間は、すべての変更の同期がとれるだけの十分な長さに設定する必要があります。

関連項目：

- 変更ロギングを有効にして Oracle ディレクトリ・サーバーを起動する方法は、A-7 ページの「Oracle ディレクトリ・サーバー・インスタンスの起動」を参照してください。
- 変更ロギングを有効にして SunONE Directory Server を起動する方法は、SunONE Directory Server のドキュメントを参照してください。

パスワードを同期させる場合は、Oracle Internet Directory で使用されるハッシング技術が SunONE Directory Server でもサポートされていることを確認してください。Oracle Internet Directory で現在使用可能なハッシング技術は、Oracle Internet Directory で、次のとおりベース検索を行って入手できます。

```
ldapsearch  -h host -p port_number -b '' -s base 'objectclass=*'   orclcryptoscheme
```

SunONE Directory Server 外部認証プラグイン

Oracle コンポーネントは Oracle Internet Directory のクライアントです。ただし、統合環境では、これらのコンポーネント用のセキュリティ資格証明を外部リポジトリに格納するオプションがあります。この場合は、Oracle Internet Directory ではなく SunONE Directory Server に格納します。セキュリティ資格証明を外部リポジトリに格納すると、Oracle コンポーネントに対するユーザー認証は、Oracle Internet Directory ではなく外部リポジトリで行われます。

外部リポジトリと通信する場合、Oracle コンポーネントは Oracle ディレクトリ・サーバーに依存します。Oracle ディレクトリ・サーバーでは、外部リポジトリにアクセスできるプラグインが使用されます。この認証プロセス全体は Oracle コンポーネントには透過的です。Oracle コンポーネントでは、すべての LDAP 要求が Oracle ディレクトリ・サーバーによって処理されていると認識されます。

外部認証の種類

ユーザーのセキュリティ資格証明を確認するために、Oracle コンポーネントによって、Oracle ディレクトリ・サーバー経由で、次のいずれかに対する要求を伴う単純なバインドを外部リポジトリに送信できます。

- 非 SSL ldapbind
- SSL ldapbind
- ldapcompare

外部リポジトリに対する認証方法

Oracle ディレクトリ・サーバーでプラグインが構成され使用可能な場合、Oracle コンポーネントに対してユーザーを認証するために次の処理が行われます。

1. ユーザーが Oracle コンポーネントへのアクセス権を要求します。
2. Oracle Internet Directory のクライアントである Oracle コンポーネントが、認証要求を受信し、ldapbind または ldapcompare 要求のいずれかを Oracle ディレクトリ・サーバーに渡します。
3. Oracle ディレクトリ・サーバーが制御をプラグインに渡します。
4. プラグインが要求を外部リポジトリに発行します。
5. プラグインがその要求の結果を取得し、その結果を Oracle ディレクトリ・サーバーに戻します。
6. Oracle ディレクトリ・サーバーが、その結果をクライアント・アプリケーションに戻します。その後、クライアント・アプリケーションがユーザーへのアクセス権を付与または否認します。

SunONE コネクタの構成

この項では、SunONE コネクタを構成するためのタスクについて説明します。次の項目について説明します。

- タスク 1: SunONE コネクタ用の統合プロファイルの構成
- タスク 2: アクセス制御リストの構成
- タスク 3: 同期用の両方のディレクトリの準備
- タスク 4: （オプション）SunONE Directory Server 外部認証プラグインの構成
- タスク 5: 同期の開始

タスク 1: SunONE コネクタ用の統合プロファイルの構成

SunONE Directory Server との同期化に使用する統合プロファイル・テンプレートは、インストール・プロセスの一部として Oracle ディレクトリ・サーバーに作成されます。

デフォルトの統合プロファイルは 2 つあります。

- `iPlanetImport`: ディレクトリ同期方法を使用して SunONE Directory Server からエントリと変更をインポートするためのプロファイル
- `iPlanetExport`: Oracle Internet Directory から SunONE Directory Server に変更をエクスポートするためのプロファイル

これらは、配置要件を満たすためにカスタマイズする単純なテンプレートです。

デフォルトの統合プロファイルのカスタマイズ

デフォルトの統合プロファイルをカスタマイズするには、シェル・スクリプト、Directory Integration and Provisioning Assistant または Oracle Directory Manager を使用できます。インポート操作用とエクスポート操作用に別々のプロファイルを構成します。

スクリプト iplanetconfig.sh を使用したデフォルトの統合プロファイルの構成 次の場合にこの方法を使用します。

- SunONE Directory Server で、同期化するオブジェクトに対してカスタム・スキーマ変更が行われていない場合（ユーザーおよびグループのオブジェクト属性とオブジェクト・クラスがデフォルトの属性とクラスの場合）
- カスタム・スキーマ要素がユーザーまたはグループのオブジェクト属性とオブジェクト・クラスに追加されていない場合

同期化が終了すると、SunONE Directory Server から同期化されたユーザー・オブジェクトおよびグループ・オブジェクトは、Oracle Application Server Infrastructure と統合された Oracle コンポーネントで参照できます。

スクリプト `iplanetconfig.sh` は、`$ORACLE_HOME/ldap/odi/admin` にあります。次のように入力して、このスクリプトを実行します。

```
iplanetconfig.sh -oidport port -oidhost host
```

このスクリプトによって、次の項目の入力を求めるプロンプトが表示されます。

- Oracle Internet Directory のスーパー・ユーザーの識別名およびパスワード
- SunONE Directory Server の URL（*host*:*port*）
- SunONE コネクタで使用される SunONE Directory Server のユーザー・アカウントおよびパスワード
- 同期化する SunONE Directory Server ドメイン

これらのパラメータ値を入力すると、`iplanetconfig.sh` によって Directory Integration and Provisioning Assistant が起動され、デフォルトの SunONE Directory Server 統合プロファイル内の SunONE Directory Server コネクタ情報およびマッピング・ルール情報が設定されます。

Directory Integration and Provisioning Assistant または Oracle Directory Manager を使用したデフォルトの統合プロファイルの構成 次の場合にこの方法を使用します。

- SunONE Directory Server のデフォルトが、配置要件に従ってカスタマイズされている場合（ユーザー・オブジェクトまたはグループ・オブジェクトにカスタム・スキーマ要素が含まれている場合）
- Oracle Internet Directory のオブジェクトにカスタム・スキーマ要素が含まれている場合
- 2 つのディレクトリ間で同期化するオブジェクトおよび属性がデフォルトのものではない場合

この方法を使用してディレクトリ統合プロファイルを構成する手順は、次のとおりです。

1. 42-7 ページの「マッピング・ルールの構成」で説明したとおりにマッピング・ルールを構成します。
2. 42-8 ページの「デフォルト・パラメータの更新」で説明したとおりにデフォルトのパラメータを更新します。
3. 42-10 ページの「タスク 3: 同期用の両方のディレクトリの準備」で説明したとおりにディレクトリをブートストラップします。ブートストラップを行うためのデフォルトのマッピング・ファイルは、`iplanetimp.map.master` ファイルに類似しています。変更を行う場合は、このファイルをサンプルとして使用します。
4. パスワードの同期を構成します。デフォルトのマッピング・ルールは、SunONE Directory Server と Oracle Internet Directory 間でのパスワードの同期には適していません。

   Oracle Internet Directory および SunONE Directory Server で同じパスワード・ハッシング技術が使用されている場合は、次のマッピング・ルールをマッピング・ファイルに挿入し、そのマッピング・ファイルをプロファイルにアップロードします。

   ```
   Userpassword: : :person:userpassword: :person
   ```

   2 つのディレクトリで同じハッシング技術が使用されていない場合は、Oracle Directory Integration and Provisioning Server およびディレクトリ統合ファイルを SSL モードで構成（サーバー専用認証）すると、同じマッピング・ルールが適用されます。

双方向同期化用のデフォルトの統合プロファイルの構成 ディレクトリ間で相互に同じ変更を同期化しないように、Oracle Directory Manager または Directory Integration and Provisioning Assistant を使用して、接続ディレクトリおよび Oracle Internet Directory に対してフィルタ属性を設定します。

インポート・プロファイルでは、接続ディレクトリ・フィルタを次のように設定します。

```
modifiersname != DN of the user account with which changes are made by the export
profile in SunONE
```

エクスポート・プロファイルでは、Oracle Internet Directory フィルタを次のように設定します。

```
modifiersname != orclodipagentname=import profile name,cn=subscriber
profile,cn=changelog subscriber,cn=oracle internet directory
```

マッピング・ルールの構成

デフォルトのプロファイルには、SunONE Directory Server 内のユーザー属性、グループ属性およびオブジェクト・クラスを Oracle Internet Directory にマッピングするためのデフォルトのマッピング・ルールがあります。これらのマッピング・ルールは、インストール後、いずれのディレクトリにもユーザー固有およびグループ固有のスキーマ変更が加えられていないことを想定しています。そのような変更がある場合は、マッピング・ファイル内にそれらの変更が適切に反映されている必要があります。

マッピング・ルールを確認および変更する手順は、次のとおりです。

1. 同期させるドメインまたはコンテナを決定します。SunONE Directory Server の場合、同期用に指定されるコンテナはディレクトリ内の任意のネーミング・コンテキストです。
2. 同期させるオブジェクト（エントリの型）を決定します。認証管理環境では、通常、これらはユーザー・エントリとグループ・エントリです。
3. 属性、およびそれらの属性を同期中にディレクトリ間でマッピングする方法を識別します。
4. 適切なマッピング・ルールでマッピング・ファイルを生成します。

> **関連項目：** マッピング・ファイルの作成方法およびサンプル・マッピング・ファイルの詳細は、33-7 ページの「マッピング・ルール属性の形式」を参照してください。

デフォルト・パラメータの更新

マッピング・ファイルの生成後は、Oracle Directory Manager または Directory Integration and Provisioning Assistant を使用して、デフォルトの統合プロファイル内のパラメータを更新できます。B-18 ページの表 B-20 に、サード・パーティ・ディレクトリ用のデフォルト統合プロファイル内の属性を示します。これらの属性の一部には、SunONE Directory Server との統合に固有の値が含まれています（表 42-1 を参照）。

表 42-1 SunONE Directory Server 統合プロファイルのデフォルト属性値

属性	値
プロファイル名（orclodipAgentName）	インポート・プロファイルのデフォルト値は、iPlanetImport です。 エクスポート・プロファイルのデフォルト値は、iPlanetExport です。 この属性は必須です。
接続ディレクトリ URL（orclOdipConDirURL）	接続ディレクトリへの接続に必要な接続詳細。このパラメータは、ホスト名とポート番号を *host*:*port*:*sslmode* の形式で示します。 SSL を使用して接続するには、*host*:*port*:1 を入力します。 ディレクトリに接続するための証明書が Wallet に格納され、その場所がファイル odi.properties に指定されていることを確認します。 **注意：**SSL を使用して SunONE Directory Server に接続するには、サーバー証明書を Wallet にロードする必要があります。 **関連項目：**『Oracle Advanced Security 管理者ガイド』の Oracle Wallet Manager についての章を参照してください。
マッピング・ルール（orclOdipAttributeMappingRules）	マッピング・ルールを格納するための属性。マッピング・ルールは、Directory Integration and Provisioning Assistant または ldapuploadagentfile.sh ツールを使用してファイルに格納します。 **関連項目：** ■ 33-5 ページの「マッピング・ルールとその形式」 ■ 33-7 ページの「マッピング・ルール属性の形式」 ■ A-106 ページの「Directory Integration and Provisioning Assistant」
接続ディレクトリ・アカウント（orclodipConDirAccessPassword）	接続ディレクトリへの接続に対して、orclOdipConDirAccessAccount 属性で指定されたユーザーが使用するパスワード。SunONE 同期コネクタの場合のパスワードは、SunONE ディレクトリ・サーバー内の有効なバインド・パスワードです。

表 42-1 SunONE Directory Server 統合プロファイルのデフォルト属性値（続き）

属性	値
接続ディレクトリ・アカウント (orclodipConDirAccessAccount)	変更が SunONE Directory Server から Oracle Internet Directory にインポートされる場合、このユーザー・アカウントには、SunONE Directory Server 変更ログ・コンテナの読取り権限が必要です。 Oracle Internet Directory での変更が SunONE Directory Server にエクスポートされる場合、ユーザーには同期ドメインに対する追加権限および変更権限が必要です。 **注意：**同期化を行うためには、SunONE コネクタ専用の SunONE Directory Server のユーザー・アカウントを作成します。
エージェント実行コマンド (orclodipAgentExeCommad)	このフィールドは空にしておく必要があります。

関連項目：

- 必須手順および設定が必要な各属性の一般的な説明は、33-6 ページの「Oracle Directory Integration and Provisioning Platform へのコネクタの登録」を参照してください。
- A-106 ページの「Directory Integration and Provisioning Assistant」

タスク 2: アクセス制御リストの構成

サブスクライブ・ドメインで読取り、追加または変更を行うためのアクセス権を許可する適切な ACL を設定します。

インポート操作時に、Oracle Internet Directory ユーザー `orclodipagentname=iPlanetImport,cn=subscriber profile,cn=changelog subscriber,cn=oracle internet directory` に権限を付与して、Oracle Internet Directory のサブスクライブ・ドメインを更新します。

たとえば、対象のドメインに対して ACL が適用されていない場合は、次の LDIF サンプルを使用できます。このファイルでは、対象のドメインは *`Synchronization_domain_in_OID`* です。

```
ACL in OID:
    dn: Synchronization_domain_in_OID
    changetype: modify
    add: orclaci
    orclaci: access to entry by "orclodipagentname=iPlanetImport,cn=subscriber
    profile,cn=changelog subscriber,cn=oracle internet directory"
    (browse,add,delete)
    orclaci: access to attr=(*) by "orclodipagentname=iPlanetImport,cn=subscriber
    profile,cn=changelog subscriber,cn=oracle internet directory"
    (read,search,write,compare)"
```

また、プロファイルがメンバーである cn=odipgroup,cn=odi,cn=oracle internet directory グループにも権限を付与できます。ただし、権限がグループに付与されると、そのグループのすべてのメンバーに、意図的であるかどうかに関係なく権限が付与されることに注意してください。

インポート操作中、統合プロファイル内の接続ディレクトリ・アカウントの属性で指定されるユーザーには、次の権限が必要です。

- Oracle Internet Directory 内のターゲット・コンテナに対する書込みアクセス権
- SunONE Directory Server 内の変更ログおよびソース・コンテナに対する読取りアクセス権

エクスポート操作中、統合プロファイル内の接続ディレクトリ・アカウントの属性で指定されるユーザーには、次の権限が必要です。

- SunONE Directory Server 内のターゲット・コンテナに対する書込みアクセス権
- SunONE Directory Server 内の変更ログおよびソース・コンテナに対する読取りアクセス権

> **関連項目：** SunONE Directory Server 変更ログ・コンテナおよび SunONE Directory Server サブスクライブ・ドメインに ACL を適用する方法は、SunONE Directory Server のドキュメントを参照してください。

タスク 3: 同期用の両方のディレクトリの準備

次の手順で行ってください。

1. 同期化を開始する前に、対象の両ドメインにあるデータを同等にします。これは、ブートストラップ・オプションを指定した Directory Integration and Provisioning Assistant を使用して実行できます。ブートストラップの詳細は、第 37 章「Oracle Directory Integration and Provisioning Platform におけるディレクトリのブートストラップ」を参照してください。
2. LDIF ファイル・ベースのブートストラップを使用している場合は、lastchangenumber 値を初期化する必要があります。これは、Directory Integration and Provisioning Assistant を使用して実行できます。

   ```
   dipassistant mp -profile profile_name -updlcn
   ```

3. ブートストラップの終了時に、Oracle ディレクトリ・サーバーの変更ロギング・オプションがデフォルト（TRUE）に設定されていることを確認してください。FALSE に設定されている場合は、Oracle Internet Directory サーバーを停止し、**OID 制御ユーティリティ**を使用して変更ログを使用可能にして再起動します。

   同様に、SunONE Directory Server で変更ログが使用可能になっていることを確認します。

関連項目：

- A-106 ページの「Directory Integration and Provisioning Assistant」
- OID 制御ユーティリティの詳細は、A-7 ページの「Oracle ディレクトリ・サーバー・インスタンスの起動と停止」を参照してください。

タスク 4:（オプション）SunONE Directory Server 外部認証プラグインの構成

SunONE Directory Server のみにパスワードを格納し、これらのパスワードを Oracle Internet Directory と同期化しない場合は、SunONE Directory Server 外部認証プラグインを使用して、Oracle Internet Directory から SunONE Directory Server ユーザーを認証する必要があります。

この項では、コマンドラインを使用して SunONE Directory Server 外部認証プラグインをインストール、削除、有効化および無効化する方法について説明します。インストール以外のこれらの操作は、Oracle Directory Manager を使用して実行できます（45-5 ページの「Oracle Directory Manager を使用したプラグインの登録と管理」を参照）。

注意： SunONE Directory Server 外部認証プラグインは、単一の SunONE Directory Server に対してのみ認証を行うように構成できます。

SunONE Directory Server 外部認証プラグインのインストール

プラグインをインストールする手順は、次のとおりです。

1. *$ORACLE_HOME*/ldap/admin/oidspipi.sh を実行します。

注意： Windows オペレーティング・システムでシェル・スクリプト・ツールを実行するには、次のいずれかの UNIX エミュレーション・ユーティリティが必要です。

- Cygwin 1.3.2.2-1 以上
  サイト：http://sources.redhat.com
- MKS Toolkit 6.1
  サイト：http://www.datafocus.com/

---

oidspipi.sh を実行するには、次のとおり入力します。

```
cd $ORACLE_HOME/ldap/admin
oidspipi.sh
```

Windows オペレーティング・システムを使用している場合は、UNIX エミュレーション・ユーティリティのインストール後、次のとおり入力して oidspipi.sh を実行します。

```
sh oidspipi.sh
```

2. SunONE Directory Server のホスト名を入力します。これは、同期させる SunONE Directory Server です。この値は必須です。
3. SSL 接続を使用するかどうかを選択します。

   Microsoft Windows オペレーティング・システムで Wallet の位置を指定する場合は、円記号（¥）を追加します。たとえば、Wallet の位置が `D:storage¥wallet` の場合は、`D:¥¥storage¥¥wallet` と入力します。
4. SunONE Directory Server のポート番号を入力します。
5. データベース接続文字列を入力します。
6. ODS パスワードを入力します。デフォルトの ODS パスワードは、Oracle Application Server 管理者用にインストール時に設定されたものと同じです。
7. Oracle ディレクトリ・サーバーのホスト名を入力します。この値は必須です。
8. Oracle ディレクトリ・サーバーのポート番号を入力します。デフォルトのポートは 389 です。
9. Oracle 管理者のパスワード（`orcladmin`）を入力します。この値は必須です。
10. プラグインを適用する必要があるコンテナの識別名を入力します。このコンテナのすべてのエントリが SunONE Directory Server に対して認証されます。この入力値は、Oracle Internet Directory セルフ・サービス・コンソールに用意されているユーザー検索ベースである必要はありません。この検索ベースに基づくすべてのユーザーが SunONE Directory Server に対して外部認証されます。複数の値を指定する場合は、セミコロン（;）を使用して区切ります。
11. プラグイン要求グループ識別名を入力します。セキュリティ上の理由から、プラグインは、このグループに属するユーザーによってのみ起動できます。たとえば、Oracle Application Server Single Sign-On 管理者がグループ `cn=OracleUserSecurityAdmins,cn=Groups,cn=OracleContext` に属しているとします。プラグイン要求グループ識別名にこの値を入力すると、Oracle Application Server Single Sign-On 管理者からの要求のみが外部認証プラグインをトリガーできます。複数の識別名値を入力できます。セミコロン（;）を使用して区切ります。この値は必須ではありませんが、セキュリティのため、指定することをお薦めします。
12. SunONE Directory Server に対する認証から除外するエントリの値を入力します。この値は、42-12 ページの項目 10 に対する例外です。値は標準 ldapsearch フィルタの書式で入力する必要があります。たとえば、値 `(&(objectclass=inetorgperson)(cn=orcladmin))` を指定すると、項目 10 に指定されたユーザー・コンテナの下にある `cn=orcladmin` および `objectclass=inetorgperson` 属性値を持つエントリは、SunONE Directory Server に対して認証されません。

13. フェイルオーバーに備えて SunONE Directory Server をバックアップするかどうかを指定します。

SunONE Directory Server 外部認証プラグインの削除

Oracle Directory Manager を使用して SunONE Directory Server 外部認証プラグインを削除するには、45-6 ページの「Oracle Directory Manager によるプラグインの削除」の指示に従います。

コマンドライン・ツールを使用して SunONE Directory Server プラグインを削除するには、次のコマンドを実行します。

```
ldapdelete -h host -p port -D cn=orcladmin -w password
"cn=ipwhencompare,cn=plugin,cn=subconfigsubentry"

ldapdelete -h host -p port -D cn=orcladmin -w password
"cn=ipwhenbind,cn=plugin,cn=subconfigsubentry"
```

SunONE Directory 外部認証プラグインの有効化

Oracle Directory Manager を使用して SunONE Directory 外部認証プラグインを有効にするには、45-5 ページの「Oracle Directory Manager によるプラグインの編集」の指示に従って、「プラグイン使用可能」フィールドを 1 に設定します。

コマンドライン・ツールを使用して SunONE Directory Server 外部認証プラグインを有効にするには、次のコマンドを実行します。

```
ldapmodify -h host_name -p port_number -D cn=orcladmin -w password <<EOF
dn: cn=ipwhencompare,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclpluginenable
orclpluginenable: 1
EOF


ldapmodify -h host_name -p port_number -D cn=orcladmin -w password <<EOF
dn: cn=ipwhenbind,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclpluginenable
orclpluginenable: 1
EOF
```

SunONE Directory Server 外部認証プラグインの無効化

Oracle Directory Manager を使用して SunONE Directory Server 外部認証プラグインを無効にするには、45-5 ページの「Oracle Directory Manager によるプラグインの編集」の指示に従って、「プラグイン使用可能」フィールドを 0 に設定します。

コマンドライン・ツールを使用して SunONE Directory Server 外部認証プラグインを無効にするには、次のコマンドを実行します。

```
ldapmodify -h host_name -p port_number -D cn=orcladmin -w password <<EOF
dn: cn=ipwhencompare,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclpluginenable
orclpluginenable: 0
EOF


ldapmodify -h <host> -p <port> -D cn=orcladmin -w <password> <<EOF
dn: cn=ipwhenbind,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclpluginenable
orclpluginenable: 0
EOF
```

SunONE Directory 外部認証プラグイン・デバッグの有効化と無効化

不明エラーが発生した場合は、プラグイン・デバッグを有効にできます。このためには、次のように入力します。

```
sqlplus ods/odspassword @$ORACLE_HOME/ldap/admin/oidspdon.pls
```

プラグイン・デバッグのログをチェックするには、次のように入力します。

```
sqlplus ods/ods
select * from plg_debug_log order by id;
```

プラグイン・デバッグのログを削除するには、次のように入力します。

```
sqlplus ods/ods
truncate table plg_debug_log
```

プラグイン・デバッグを無効にするには、次のように入力します。

```
sqlplus ods/ods @$ORACLE_HOME/ldap/admin/oidspdof.pls
```

注意： プラグイン設定（インストール時に入力した情報）を変更する必要がある場合は、インストール・スクリプトを再実行できます。スクリプトを再実行する前に、42-13 ページの「SunONE Directory Server 外部認証プラグインの削除」の指示に従って、SunONE Directory 外部認証プラグインを削除します。

関連項目：

- パスワードを保護するために Oracle Internet Directory でサポートされるハッシング・アルゴリズムのリストは、12-8 ページの「ディレクトリ認証用ユーザー・パスワードの保護」を参照してください。
- SunONE Directory Server のパスワードに適切なハッシング・アルゴリズムを設定する方法は、SunONE Directory Server のドキュメントを参照してください。

タスク 5: 同期の開始

同期を開始する手順は、次のとおりです。

1. Oracle Directory Manager または Directory Integration and Provisioning Assistant のいずれかで、`profileStatus` 属性を `ENABLE` に設定してプロファイルを有効にします。
2. プロファイルが格納されている適切な構成設定エントリを含む OID 制御ユーティリティ（oidctl）を使用して Oracle Directory Integration and Provisioning Server を起動します。

同期のプロセス

同期のプロセスは、次のとおりです。

1. インポート操作では、`orclodipConDirLastAppliedChgNum` 属性に指定された値に基づいて、SunONE コネクタがすべての変更を SunONE Directory Server から抽出します。その後、SunONE コネクタは、抽出した変更を Oracle Internet Directory に適用します。

   エクスポート操作では、`orclodipLastAppliedChangeNumber` に基づいて、SunONE コネクタがすべての変更を Oracle Internet Directory から抽出し、SunONE Directory Server に適用します。
2. すべての変更が読み取られて適用されると、適切な属性（`orclodipConDirLastAppliedChgNum` または `orclodipLastAppliedChangeNumber`）が更新されます。
3. 実行が完了した後、Directory Integration and Provisioning Server は実行ステータス属性を更新します。

SunONE Directory Server との同期に関するトラブルシューティング

この項では、次の項目について説明します。

エラー・メッセージ・ファイルの位置

Oracle Directory Integration and Provisioning Server は、35-12 ページの表 35-3 に示した適切なファイルにエラー・メッセージを格納します。

SunONE コネクタのデバッグ方法

oditest ユーティリティを使用して SunONE コネクタをデバッグできます。

- SunONE インポート・コネクタに関するトラブルシューティングを行うには、`AgentName` を `IplanetImport` と指定して oditest ユーティリティを実行し、`iPlanetImport.trc` および `iPlanetImport.aud` ファイルを参照します。
- デフォルトの SunONE エクスポート・コネクタに関するトラブルシューティングを行うには、`AgentName` を `IplanetExport` として指定して oditest ユーティリティを実行し、`iPlanetExport.trc` および `iPlanetExport.aud` ファイルを参照します。

関連項目： oditest ユーティリティの使用方法は、33-21 ページの「Oracle Directory Integration and Provisioning Platform での同期に関するトラブルシューティング」を参照してください。

SunONE Directory Server との統合でサポートされる構成

Oracle Internet Directory を中央ディレクトリとして配置した場合は、次の構成がサポートされます。

- 両方のディレクトリで同一の DIT
- ドメイン・マッピングを使用した同期
- パスワードの同期。この環境では、同期化によって、SunONE Directory Server でのフットプリントの作成のみが保証されます。ユーザー・エントリまたはグループ・エントリへのアクセスに必要なその他の構成変更は、配置によって特別に処理される必要があります。

SunONE Directory Server を中央ディレクトリとして配置した場合は、次の構成がサポートされます。

- 両方のディレクトリで同一の DIT
- ドメイン・マッピングを使用した同期
- パスワードの同期
- Oracle Internet Directory からのプラグイン・ベースの認証

43

Microsoft Windows 環境との統合

すべての Oracle コンポーネントは、Oracle Identity Management と統合することによって、セキュリティが集中管理されます。同様に、Windows 2000 および Microsoft Windows NT では、すべての Microsoft アプリケーションを Microsoft Active Directory と統合することによって、セキュリティが集中管理されます。

この章では、Oracle と Microsoft の両方のテクノロジ・スタックが使用された環境で、Oracle Identity Management を Microsoft Windows 環境と統合する方法について説明します。次の項目について説明します。

関連項目： OTN-J（`http://otn.oracle.co.jp`）の Oracle Internet Directory のセクションを参照してください。

Microsoft Windows 環境との統合の概要

この項では、関連する Oracle コンポーネントとツール、および Windows 統合環境の様々な要素について説明します。次の項目について説明します。

- Microsoft Windows 環境との統合用コンポーネント
- Microsoft Active Directory での変更の追跡方法
- Active Directory コネクタのインストール時に設定される構成情報
- 設定時に必要な情報
- 複数ドメイン Microsoft Active Directory 環境に必要な情報
- Microsoft Active Directory との統合用に設定されたディレクトリ情報ツリー
- Active Directory コネクタ構成用のツール

Microsoft Windows 環境との統合用コンポーネント

43-2 ページの表 43-1 に、Oracle Internet Directory を Microsoft Active Directory と統合する場合に使用する各 Oracle コンポーネントを示します。

表 43-1 Microsoft Active Directory との統合用コンポーネント

コンポーネント	説明
Oracle Internet Directory	Oracle コンポーネントおよびサード・パーティのアプリケーションによってユーザー ID および資格証明が格納およびアクセスされるリポジトリ。Oracle ディレクトリ・サーバーを使用して、格納された資格証明に対してユーザーを認証します。資格証明がサード・パーティのディレクトリに格納されていて、Oracle Internet Directory に格納されていない場合でも、ユーザーを認証することはできます。この場合は、Oracle Internet Directory で、サード・パーティのディレクトリに移動して認証を行う外部認証プラグインが使用されます。

表 43-1 Microsoft Active Directory との統合用コンポーネント（続き）

コンポーネント	説明
Oracle Directory Integration and Provisioning Platform	このプラットフォームでは、次のことを実行できます。 ■ Oracle Internet Directory と他のディレクトリおよびユーザー・リポジトリ間の同期 ■ Oracle コンポーネント用の自動プロビジョニング・サービス Oracle Application Server Infrastructure の一部としてインストールされますが、個別にインストールすることもできます。 このプラットフォームには、Oracle Internet Directory と他の LDAP ディレクトリ間の同期に使用されるコネクタが含まれています。そのコネクタの 1 つである Active Directory コネクタは、Oracle Internet Directory と Microsoft Active Directory 間の双方向同期用に設計されています。 Active Directory コネクタを使用して、次のことを実行できます。 ■ 一方向または双方向のいずれかの同期の構成。 ■ 同期の属性の特定のサブセットの指定。これは、適切なマッピング・ルールを構成することによって行います。マッピング・ルールは、実行時に変更できます。 ■ 複数の Microsoft Active Directory Server に対する同期化。変更は、個々のサーバーに対して直接同期化できます。また、Microsoft Global Catalog を使用して、Microsoft Active Directory 環境からも同期化できます。 Oracle Directory Integration and Provisioning Platform を使用して、Oracle Internet Directory と Microsoft Windows NT 間でユーザー・データを同期化することはできません。ただし、この同期化は、まず、Oracle Internet Directory と Microsoft Active Directory 間で同期化し、次に、Microsoft Active Directory と Microsoft Windows NT 間で同期化することによって間接的に実行できます。

表 43-1 Microsoft Active Directory との統合用コンポーネント（続き）

コンポーネント	説明
Directory Integration and Provisioning Assistant	このツールを使用すると、Oracle Internet Directory とサード・パーティのディレクトリ間でデータを移行できます。具体的には、次のことを実行できます。 ■ いずれかの方向でのデータの移行 ■ LDIF ファイルを使用した大量データの移行または直接 LDAP コマンドを使用した小量データの移行 ■ 各エントリ内の属性のすべてまたはサブセットの移行。このツールでは、Oracle Directory Integration and Provisioning Server と同じマッピング・ルールが使用されます。 Directory Integration and Provisioning Assistant を使用して、Oracle Internet Directory から Microsoft Windows NT にユーザー・データを直接ロードすることはできません。ただし、このロードは、まず、Microsoft Active Directory にデータをロードし、次に、Microsoft ツールを使用して Microsoft Active Directory から Microsoft Windows NT にデータをロードすることによって、間接的に実行できます。
Oracle Application Server Single Sign-On	Oracle Application Server Single Sign-On を使用すると、1 回のみのログインで、Web ベースの Oracle コンポーネントにアクセスできます。 Oracle コンポーネントは、ログイン機能を OracleAS Single Sign-On Server に委任します。初めて Oracle コンポーネントにログインする場合は、そのコンポーネントによって OracleAS Single Sign-On Server へのログインにリダイレクトされます。OracleAS Single Sign-On Server では、Oracle Internet Directory に格納されている資格証明に対して、ユーザーが入力した資格証明を検証することによってユーザーが認証されます。ユーザーは、認証されると、残りのセッション中、使用を要求し認可されたすべてのコンポーネントに対する権限を OracleAS Single Sign-On Server によって付与されます。 Oracle Application Server Single Sign-On を使用すると、Microsoft Windows 環境でネイティブ認証（自動ログイン）が有効になります。ユーザーは、Windows デスクトップにログインすると、自動的に Oracle コンポーネントにアクセスできるようになります。OracleAS Single Sign-On が、ユーザーの Kerberos 資格証明を使用してユーザーを Oracle 環境に自動的にログインさせます。

表 43-1 Microsoft Active Directory との統合用コンポーネント（続き）

コンポーネント	説明
Active Directory 外部認証プラグイン	Oracle ディレクトリ・サーバーの一部であるこのプラグインを使用すると、Microsoft Windows ユーザーは、Microsoft Windows 資格証明を使用して Oracle 環境にログインできます。Microsoft Windows ユーザーがこの方法でログインしようとすると、ユーザーが入力した資格証明と、Oracle Internet Directory に格納された資格証明の検証が OracleAS Single Sign-On Server によって試行されます。ユーザーの資格証明が Oracle Internet Directory に格納されていない場合は、Oracle ディレクトリ・サーバーによって Active Directory の外部認証プラグインが起動されます。このプラグインによって、Microsoft Windows 内のユーザー資格証明が検証されます。検証が正常に実行された場合は、それに応じて Oracle ディレクトリ・サーバーから OracleAS Single Sign-On に通知されます。 このプラグインは、Microsoft Windows での外部認証を有効にするのみでなく、Microsoft Windows ユーザーを Oracle Identity Management システムに自動的にプロビジョニングします。
Oracle Internet Directory セルフ・サービス・コンソール	Oracle Internet Directory セルフ・サービス・コンソールは、Oracle Internet Directory でユーザー、グループおよびそれらの資格証明を管理するための Web ベースのツールです。このツールは、Oracle Delegated Administration Services のサービス・ユニットで構築されているため、ユーザー・パスワードおよびパスワード・ポリシーの管理に使用できます。 **参照：**このツールを使用して、レルム、ユーザー検索ベースおよびグループ検索ベースを管理する方法の詳細は、第 31 章「Oracle Internet Directory セルフ・サービス・コンソール」を参照してください。
Oracle Directory Manager	Oracle Directory Manager は、Oracle Internet Directory を管理するための Java ベースのツールです。Oracle Directory Manager を使用すると、ディレクトリ管理者は、Oracle Directory Integration and Provisioning Server で使用されるユーザー情報、構成情報などのすべてのディレクトリ・データを管理できます。

Microsoft Active Directory での変更の追跡方法

Microsoft Active Directory は、ディレクトリの内容に加えられた変更を追跡する様々な方法を提供しています。次に、これらの方法のうちの 2 つを示します。

- DirSync 制御ベースの方法
- USNChanged ベースの方法

各方法では、変更の導出元のディレクトリが、Active Directory コネクタによってスケジュールされた間隔でポーリングされます。

各方法には、利点と欠点があります。表 43-2 に、これらの 2 つの方法の相違点を示します。

表 43-2 DirSync 方法と USNChanged 方法の比較

考慮事項	DirSync 方法	USNChanged 方法
キーの変更	エントリの一意の識別子である ObjectGUID に変更を渡します。	識別名に変更を渡します。ObjectGUID は相対識別名の変更の追跡に使用されます。
複数値の属性の変更	複数値の属性に加えられた増分変更を、属性値の完全置換として反映します。ネットワークに不要なトラフィックを発生させる可能性があります。	複数値の属性に加えられた増分変更を、属性値の完全置換として反映します。ネットワークに不要なトラフィックを大量に発生させる可能性があります。
エラー処理	同期が中断された場合に、現在の場所から次のサイクルを開始します。同期操作中に適用された変更件数を記録しておく必要があります。そうしないと、一部の変更が再度適用されます。	同期が原子性を持つ必要はありません。特定のエントリの同期が失敗した場合は、現在または次のエントリから次の同期サイクルを開始できます。
検索結果の情報	変更された属性と新しい値のみで構成される検索結果を提供します。これらの値は、Oracle Internet Directory に非常に簡単に適用できます。	完全な変更エントリで構成される検索結果を提供します。すべての属性値が Oracle Internet Directory に格納されている古い値と比較され、変更されている場合のみ適用されます。これには時間がかかります。
適用された変更の監視	ディレクトリ内の変更を問い合せたときに、ディレクトリの状態を識別する Cookie 値に基づく増分変更が渡されます。Cookie はバイナリ値をとるため、ある期間にわたる変更を選択して無視することはできません。	ディレクトリ内の変更は、整数値をとる USNChanged 属性に基づいて問い合されます。値は必要に応じて簡単に変更できます。
同期ユーザーに必要な権限	ユーザーには SE_SYNC_AGENT_NAME 権限が必要です。この権限があれば、オブジェクトおよび属性に対するアクセス保護に関係なく Microsoft Active Directory 内のすべてのオブジェクトおよび属性を読み取ることができます。	特別な権限は不要です。ユーザーには特定のコンテナでの読取り / 書込み権限が必要です。

表 43-2 DirSync 方法と USNChanged 方法の比較（続き）

考慮事項	DirSync 方法	USNChanged 方法
複数ドメインのサポート	異なるドメイン内のエントリに加えられた変更を読み取るには、異なるドメイン・コントローラへの個々の接続が必要です。	Global Catalog Server に接続することで、複数のドメインに加えられた変更を読み取ることをユーザーに許可します。
フェイルオーバー時のレプリケート・ディレクトリからの同期	そのまま継続できます。レプリケートされた環境に接続するときも同期キーは同じです。	フェイルオーバー・ディレクトリとの同期を開始する前に、変更番号を更新する必要があります。
同期の有効範囲	ディレクトリに加えられたすべての変更を読み取り、必須エントリへの変更以外を Oracle Internet Directory に伝播します。	特定のサブツリー内の変更を検索できます。
双方向の同期	双方向同期の場合、ドメイン・コントローラごとにインポート・プロファイルとエクスポート・プロファイルの構成が必要です。	双方向同期の場合、すべてのドメイン・コントローラから変更をインポートするためのプロファイル、および各ドメイン・コントローラに変更をエクスポートするための個々のプロファイルが必要です。
ロード・バランサの背後に複数の Microsoft Active Directory Server を配置した環境の可用性	特定の Microsoft Active Directory ノード（可能であれば Global Catalog Server）に接続します。	特定の Microsoft Active Directory ノードに接続します。

Active Directory コネクタのインストール時に設定される構成情報

インストール時に、デフォルトの同期プロファイル、マッピング・ルールおよびアクセス制御が事前構成されます。この構成は、配置要件を満たすようにカスタマイズできます。

同期プロファイル

同期を有効にするほぼすべての情報は、インストール時に Oracle Internet Directory に事前構成され、`Synchronization Profile` というディレクトリ・エントリに格納されます。この情報は、同期時に Oracle Directory Integration and Provisioning Server、ブートストラップ時に Directory Integration and Provisioning Assistant で使用されます。

この情報は、要件に合わせて、実行時に変更できます。Directory Integration and Provisioning Server では、構成情報の変更後、そのプロファイルが同期に使用されると、変更された情報でキャッシュが自動的に更新されます。このため、構成情報を変更するたびにこのサーバーを再起動する必要はありません。

インストール時に、3 つのデフォルトの Active Directory 同期プロファイルが Oracle Internet Directory に作成されます。これらが要件を満たしている場合は、Active Directory コネクタの実行に使用できます。要件を満たしていない場合は、配置要件を満たすようにカスタマイズして、テンプレートとして使用します。これらの同期プロファイルには、次のようなものがあります。

- `ActiveImport`: DirSync 方法を使用して、Microsoft Active Directory から Oracle Internet Directory へ変更をインポートするためのプロファイルです。
- `ActiveChgImp`: USNChanged 方法を使用して、Microsoft Active Directory から Oracle Internet Directory へ変更をインポートするためのプロファイルです。
- `ActiveExport`: Oracle Internet Directory から Microsoft Active Directory へ変更をエクスポートするためのプロファイルです。

マッピング・ルール

同期プロファイルの重要な要素であるマッピング・ルールは、ディレクトリ間で同期化されるディレクトリ情報の内容、およびディレクトリ情報の同期化方法を決定します。マッピング・ルールは、要件に合わせて、実行時に変更できます。

デフォルトのユーザー属性およびグループ属性が指定されたデフォルトのマッピング・ルール デフォルトの Active Directory 同期プロファイルには、それぞれデフォルトのマッピング・ルールが含まれています。これらのルールには、デフォルトで、同期用に構成された最小限のデフォルトのユーザー属性およびグループ属性が含まれています。これらのデフォルトの属性については、表 43-3 を参照してください。この表では、属性が、Microsoft Active Directory および Oracle Internet Directory でのそれぞれの名前で示されています。

表 43-3 デフォルトのユーザー属性およびグループ属性

Microsoft Active Directory での名前	Oracle Internet Directory での名前	説明
デフォルトのユーザー属性		
`cn`	`cn`	ユーザー名
`SAMAccountName`	`user:orclADSAMAccountName`	Microsoft Active Directory のログイン ID が含まれています。Oracle Single Sign-On Service で Windows のネイティブ認証用に使用されます。
`UserprinicipalName`	`uid`	Oracle Single Sign-On Service でシングル・サインオン用に使用されます。
`UserprinicipalName`	`orclADUserprinicipalName`	uid が使用できない場合に、Oracle Single Sign-On Service でシングル・サインオン用に使用されます。

表 43-3 デフォルトのユーザー属性およびグループ属性（続き）

Microsoft Active Directory での名前	Oracle Internet Directory での名前	説明
ObjectGUID	orclADObjectGUID	Active Directory コネクタで同期キーとして使用されます。
ObjectSID	orclsADObjectSID	現在は使用されていません。
デフォルトのグループ属性		
cn	cn	ユーザー名
SAMAccountName	user:orclADSAMAccountName	Microsoft Active Directory のログイン ID が含まれています。
Managedby	Owner	グループ・エントリの所有者を表します。
Member	uniquememeber	グループのメンバー・ユーザーの識別名を表します。

表 43-3 のデフォルトの属性のみでなく、ou（組織単位）属性も同期用に事前構成されます。Microsoft Active Directory と Oracle Internet Directory の両方で ou と表されます。

アクセス制御

使用を認可されたデータのみにユーザーがアクセスできるようにするには、Oracle Internet Directory に適切なアクセス制御が必要です。具体的には、アクセス制御で次のことを実行する必要があります。

- Microsoft Active Directory から同期化されている場合、認可されたアカウントのみが Oracle Internet Directory にデータを作成できるようにします。
- ユーザー・オブジェクトおよびグループ・オブジェクトのみを適切なコンテナに作成できるようにします。

インストール時に、デフォルトの 2 つのアクセス制御ポリシーが事前構成されます。これらのポリシーによって、認可されたユーザーのみが Oracle Internet Directory にエントリを作成できるようになります。最初のポリシーによって、users サブツリー（同期化されるすべてのユーザー用のデフォルトのコンテナ）下のユーザー以外のオブジェクトは作成できなくなります。2 番目のポリシーによって、groups サブツリー（同期化されるすべてのグループ用のデフォルトのコンテナ）下のグループ以外のオブジェクトは作成できなくなります。

関連項目： ユーザー属性およびグループ属性の詳細は、43-11 ページの「Microsoft Active Directory との統合用に設定されたディレクトリ情報ツリー」を参照してください。

設定時に必要な情報

Oracle Internet Directory のインストール後、2 つのディレクトリ間の同期を有効にするには、同期プロファイル内の最小限の追加情報のみを構成する必要があります。単純な配置では、この情報は、スクリプト `adprofilecfg.sh` を使用して簡単に構成できます。情報を構成するツールには、他にも次のものがあります。

- Oracle Internet Directory セルフ・サービス・コンソール : 第 31 章「Oracle Internet Directory セルフ・サービス・コンソール」を参照してください。
- Directory Integration and Provisioning Assistant: 43-2 ページの「Directory Integration and Provisioning Assistant」を参照してください。
- Oracle Directory Manager: 4-2 ページの「Oracle Directory Manager の使用方法」を参照してください。

> **関連項目：** 同期を有効にするために構成する必要がある情報の詳細は、43-21 ページの「Active Directory コネクタの構成」を参照してください。

複数ドメイン Microsoft Active Directory 環境に必要な情報

Microsoft Active Directory から Oracle Internet Directory への同期化に必要な情報

Microsoft Directory を Oracle Internet Directory に同期させるために複数ドメイン Microsoft Active Directory 環境に必要な構成情報は、Global Catalog が構成されているかどうかによって異なります。Global Catalog を使用できる場合は、Active Directory コネクタによって Global Catalog から同期化できます。この場合、構成する必要があるのは 1 つのみの同期プロファイルです。Global Catalog を使用できない場合は、Active Directory コネクタを各 Microsoft Active Directory Server に接続して Microsoft Active Directory から同期化します。この場合、Microsoft Active Directory ドメインの数と同数のエクスポート・プロファイルを構成する必要があります。

Oracle Internet Directory から Microsoft Active Directory への同期に必要な情報

Oracle Internet Directory を Microsoft Directory に同期させるために複数ドメイン Microsoft Active Directory 環境に必要な構成情報は、Global Catalog に依存しません。常に、Active Directory コネクタを各 Active Directory に接続して、Oracle Internet Directory を Microsoft Active Directory に同期させます。Microsoft Active Directory ドメインの数と同数のエクスポート・プロファイルを構成する必要があります。

> **関連項目：** 複数の Microsoft Active Directory ドメインが存在する環境で同期を構成する方法については、43-21 ページの「Active Directory コネクタの構成」および 43-42 ページの「Active Directory コネクタのカスタマイズ」を参照してください。

Microsoft Active Directory との統合用に設定されたディレクトリ情報ツリー

LDAP ディレクトリの情報は、ディレクトリ情報ツリー（DIT）に編成されます。このツリーでは、各ノードは、識別名（DN）という一意の値で識別されるディレクトリ・エントリと呼ばれます。

他のエントリ用のコンテナとして機能するツリーの一部は、サブツリーと呼ばれます。他のエントリが含まれていないツリーのノードは、リーフと呼ばれます。

ユーザーおよびグループは、エントリとして表され、リーフまたはリーフ以外のノードのいずれかになります。

ディレクトリで情報を適切かつ簡単に編成し、アクセス制御を適切に適用するために、インストール時に、最上位レベルの DIT 構造がディレクトリに構成されます。たとえば、Oracle Internet Directory のドメインは `us.MyCompany.com` で、インストール時に、事前に構成されたデフォルトのレルム値が構成されます。インストール後、Oracle Internet Directory Configuration Assistant によってデフォルトの DIT が構成されます。このデフォルトの DIT（43-12 ページの図 43-1 を参照）には、`users` と `groups` の 2 つの特別なエントリが含まれています。これらの 2 つのエントリは、ユーザーおよびグループを含む 2 つのサブツリーのルートです。

ディレクトリ情報ツリーの計画

同期化を行う前に決定する必要がある重要な事項は、次のとおりです。

- 同期化する情報

  DIT の全体または一部のいずれかを同期化できます。

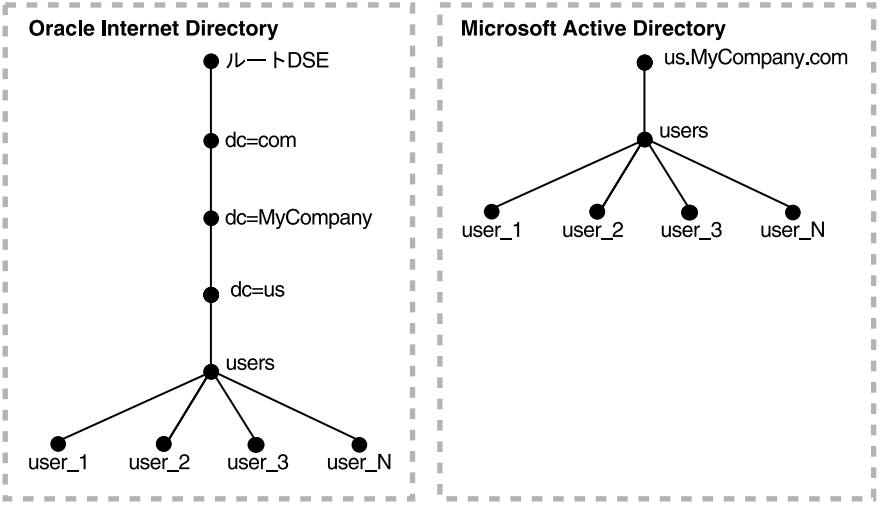
- 同期化する位置

  Active Directory コネクタを使用して、次の 2 つの構成から選択できます。

  - DIT の各エントリの相対的な位置が、ソース・ディレクトリと宛先ディレクトリの両方で同じになるように同期化。この構成は、1 対 1 ドメイン・マッピングと呼ばれ、最も一般的に使用されている構成です。また、推奨構成でもあります。
  - DIT の各エントリの相対的な位置が、ソース・ディレクトリと宛先ディレクトリで異なるように同期化。この構成では、情報が同期化されるたびに、マップされたすべてのエントリ（グループ・エントリ内の参照を含む）の識別名値を変更する必要があります。これを実行すると、非常に費用がかかる場合があります。

図 43-1 に、2 つのディレクトリの DIT 間での 1 対 1 のマッピングの例を示します。

図 43-1　両方のディレクトリ・ホストがドメイン us.MyCompany.com 下に存在する場合の Oracle Internet Directory および Microsoft Active Directory でのデフォルトの DIT 構造



次に、図 43-1 に示す配置について説明します。

- Microsoft Active Directory と Oracle Internet Directory の両方のホストが同じドメイン（`us.MyCompany.com`）に存在します。
- ユーザーは、Microsoft Active Directory から Oracle Internet Directory へのみ同期化されます。同期化されるすべてのユーザーが、Microsoft Active Directory 内の 1 つのコンテナ（`users.us.MyCompany.com`）に格納されます。
- 同じ DIT 構造が Microsoft Active Directory と Oracle Internet Directory の両方で保持されます。すべてのユーザーが、値 `users.us.MyCompany.com` で識別される同じ users サブツリーに表示されます。

このような配置では、1 対 1 のドメイン・マッピングを使用して、`users` サブツリーのみを Microsoft Active Directory から Oracle Internet Directory に同期化する必要があります。

ディレクトリ情報ツリーの構成

DIT を構成する手順は、次のとおりです。

1. インポート操作に使用される Active Directory 同期プロファイルにマッピング・ルールを設定します。この例でのマッピング・ルールは、次のとおりです。

   ```
   Domain Rule
   Cn=users, dc=us, cd=MyCompany, dc=comusers.us.MyCompany.com:
   users.us.MyCompany.com
   ```

   このマッピング・ルールは、1 対 1 のドメイン・マッピングを使用して users コンテナのみを同期化する必要があることを示します。

   Microsoft Active Directory と Oracle Internet Directory の両方のユーザー・エントリの識別名は同一です。

   複数のサブツリーを同期化する場合は、複数のドメイン・ルールを構成する必要があります。

2. Oracle Internet Directory に、デフォルトのレルム usersearchbase および groupsearchbase 値を設定します。これらの値によって、Oracle Internet Directory 内のユーザーおよびグループを検索する位置が、各種 Oracle コンポーネントに指定されます。インストール時に、これらの値を正しく設定してください。正しく設定しないと、同期が適切に機能している場合でも、コンポーネントから Oracle Internet Directory 内のユーザーおよびグループにアクセスできない場合があります。

   デフォルトのレルムはインストール時に設定されます。ただし、デフォルトのレルム値がインストール時に正しく指定されなかった場合は、次のことを実行します。

   - Oracle Application Server をインストールした後、配置していない場合は、正しいデフォルトのレルム値ですべてを再インストールする方法が簡単です。
   - Oracle Application Server をすでに配置している場合は、デフォルトのレルムを変更する必要があります。

   usersearchbase および groupsearchbase 値は、Oracle コンポーネントによってユーザーおよびグループが検索される Oracle Internet Directory のサブツリーのルートを指します。これらの値は、インストール時にデフォルトの値に設定されます。ただし、Microsoft Active Directory との統合が必要な配置では、Active Directory の DIT 構造に応じて、これらの値を適切な値に再設定する必要があります。

   たとえば、前述の例の usersearchbase の値は、cn=users,dc=us,dc=MyCompany,dc=com、またはその親のいずれかに設定する必要があります。同様に、groupsearchbase は、DIT に groups というサブツリーが存在する場合、cn=groups,dc=us, dc=MyCompany,dc=com に設定できます。

   usersearchbase および groupsearchbase 値は、Windows の統合設定（43-21 ページの「Active Directory コネクタの構成」を参照）の一部として設定されます。

複数ドメイン Active Directory 環境でのディレクトリ情報ツリー

複数ドメインが存在する Microsoft Active Directory の配置には、1 つのシングル DIT または複数のツリーで構成されるフォレスト（一群）を含めることができます。通常、Microsoft Active Directory には複数のドメイン・コントローラがあります。複数ドメイン・コントローラを持つ配置には、1 つのシングル DIT または複数のツリーで構成されるフォレスト（一群）を含めることができます。43-14 ページの図 43-2 と 43-15 ページの図 43-3 に、シングル・ツリーの場合とフォレスト構成の場合の Oracle Internet Directory の DIT と Microsoft Active Directory の DIT 間のマッピングを示します。

図 43-2 に、Microsoft Active Directory の複数のドメインがどのように Oracle Internet Directory の DIT にマッピングされるかを示します。

図 43-2 Oracle Internet Directory と Microsoft Active Directory 内の複数ドメインとの統合

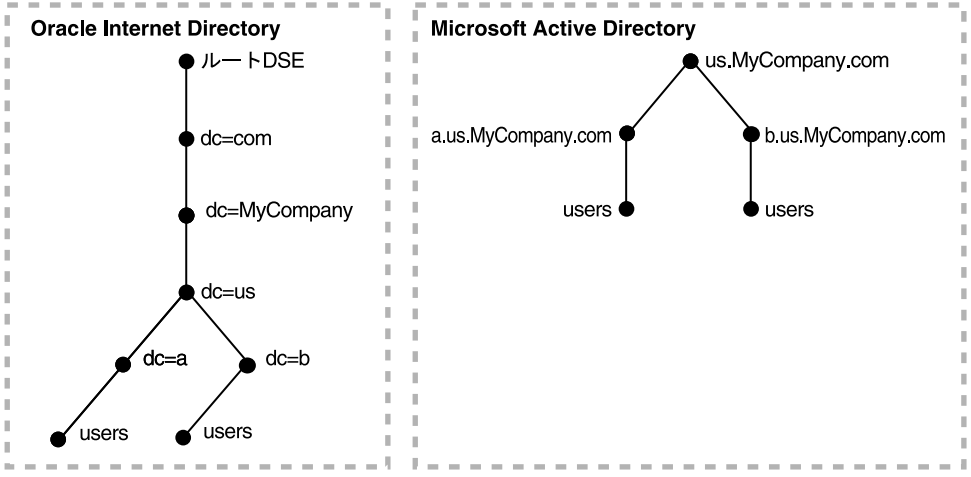


図 43-2 では、Microsoft Active Directory 環境には 1 つの親ドメインと 2 つの子ドメインがあります。各ドメインにはドメイン・コントローラが関連付けられています。`us.mycompany.com` ノードをサポートしている Microsoft Active Directory は、Global Catalog Server です。

最初の子ドメイン `a.us.MyCompany.com` は、Oracle Internet Directory の `dc=a,dc=us,dc=MyCompany,dc=com` にマップされます。2 番目の子ドメイン `b.us.MyCompany.com` は、Oracle Internet Directory の `dc=b,dc=us,dc=MyCompany,dc=com` にマップされます。Microsoft Active Directory 環境の共通ドメイン・コンポーネント `us.MyCompany.com` は、Oracle Internet Directory のデフォルト認証管理レルム `dc=us,MyCompany,dc=com` にマップされます。

図 43-3 に、Microsoft Active Directory のフォレストが Oracle Internet Directory にどのように反映されるかを示します。

図 43-3 Oracle Internet Directory と Microsoft Active Directory 内のフォレストとのマッピング

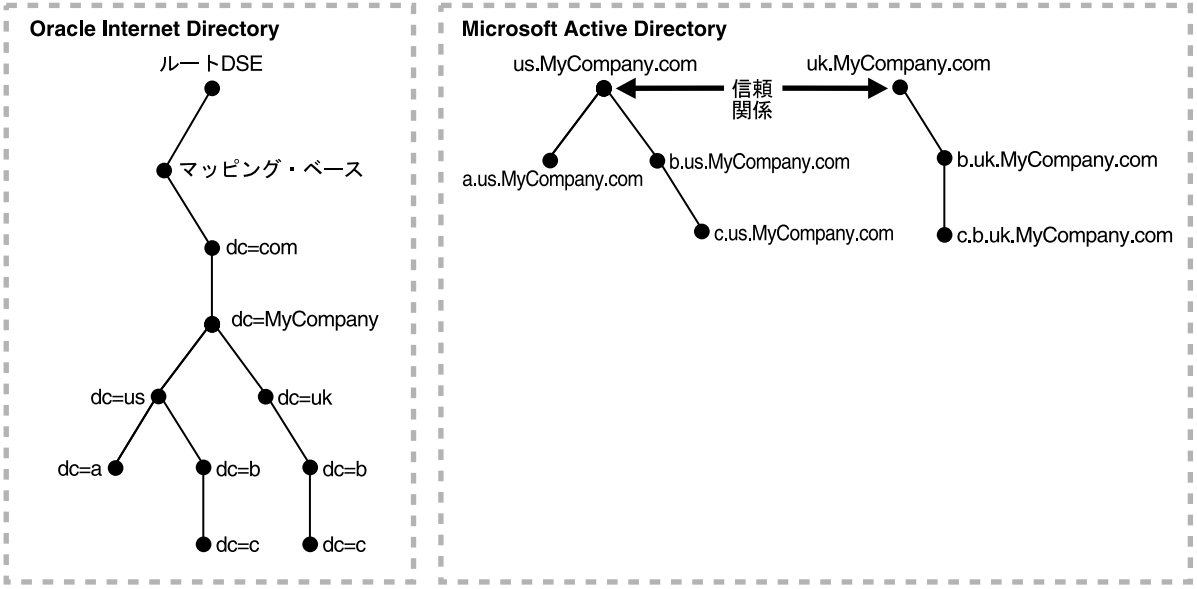


図 43-3 では、Microsoft Active Directory は企業ディレクトリです。このディレクトリでは、2 つのドメイン・ツリーがフォレストを構成しています。このフォレストは Oracle Internet Directory 内の同一構造のサブツリーにマップされます。

Active Directory コネクタ構成用のツール

表 43-4 に、Microsoft Active Directory との統合の設定および管理に使用するツールを示します。

表 43-4 Microsoft Active Directory との統合の設定および管理用ツール

ツール	説明
`adprofilecfg.sh`	Windows 環境に関連する構成情報（Microsoft Active Directory のホスト情報、ポート情報など）を簡単に設定する方法を提供するシェル・スクリプト。このツールは、単純な使用例でのみ有効で、デフォルト・プロファイルの情報構成のみに使用できます。このツールによって、3 つのデフォルト・プロファイルすべての情報が設定されます。このツールを実行すると、マスターのデフォルト・プロファイルから、前述の 3 つのデフォルト・プロファイルが作成され、ユーザーが入力する情報で更新されます。次の項で説明する様々な設定タスクで、このツールを使用します。このツールは、`$ORACLE_HOME/ldap/odi/admin` にあります。
Directory Integration and Provisioning Assistant	主にデータの初期移行用のコマンドライン・ツール。同期プロファイルの管理もできます。このツールを使用して、新しいデフォルトのプロファイルを作成し、それらのプロファイルに様々な属性を設定できます。次の項で説明する様々な設定タスクで、このツールを使用します。 **参照：** Assistant の使用方法の詳細は、A-106 ページの「Directory Integration and Provisioning Assistant」を参照してください。
Oracle Internet Directory セルフ・サービス・コンソール	管理者およびエンド・ユーザーが使用する Web ベースの GUI ツール。Windows 統合設定では、主に、レルムおよびユーザー・グループ検索ベースを管理するための情報の構成に使用されます。ユーザーおよびグループの作成および管理にも使用されます。 **参照：** このツールを使用して、レルム、ユーザー検索ベースおよびグループ検索ベースを管理する方法については、第 31 章「Oracle Internet Directory セルフ・サービス・コンソール」を参照してください。
Oracle Directory Manager	Oracle Internet Directory のすべてのデータを管理するためのスタンドアロンの Java ベースの GUI ツール。Oracle Directory Manager を使用すると、次の操作を行うことができます。 ■ 様々な同期プロファイルの作成および管理 ■ デフォルトのプロファイルのカスタマイズ ■ 同期プロファイルおよび同期ステータスの監視 ■ 同期に関するトラブルシューティング **関連項目：** 詳細は、4-2 ページの「Oracle Directory Manager の使用方法」を参照してください。

表 43-4 Microsoft Active Directory との統合の設定および管理用ツール（続き）

ツール	説明
コマンドライン・ツール	同期プロファイルの管理およびトラブルシューティング用のツール（ldapmodify、ldapsearch など）。次の項で説明する様々な設定タスクで、このツールを使用します。Windows 統合の様々な設定要件を理解した後で、カスタマイズを迅速に行うには、これらのツールが有効です。 **関連項目：**A-18 ページの「エントリおよび属性の管理コマンドライン・ツール構文」を参照してください。

高水準の構成要件

Microsoft Windows 環境との統合を配置するには、2 つの一般的な方法があります。最初の方法では、Oracle Internet Directory が、Microsoft Windows 2000 および Windows NT 環境のユーザー・データおよびグループ・データに対する企業の中央ディレクトリおよび真のソースです。2 番目の方法では、Microsoft Active Directory が、Oracle コンポーネントのユーザー・データおよびグループ・データに対する企業の中央ディレクトリおよび真のソースです。

この項では、次の項目について説明します。

- 中央ディレクトリとしての Oracle Internet Directory の配置
- 中央ディレクトリとしての Microsoft Active Directory の配置

中央ディレクトリとしての Oracle Internet Directory の配置

表 43-5 に、この配置の一般的な要件を示します。

表 43-5 中央ディレクトリとしての Oracle Internet Directory の一般的な要件

要件	中央ディレクトリとしての Oracle Internet Directory
初期ブートストラップ	Directory Integration and Provisioning Assistant によって、Oracle Internet Directory に格納されているユーザーおよびグループが Microsoft Active Directory に移入されます。 複数の Microsoft Active Directory Server が存在する場合は、Microsoft Active Directory Server の数と同じ回数 Directory Integration and Provisioning Assistant を実行する必要があります。これを実行するたびに、ターゲットの Microsoft Active Directory Server で必要な特定のデータ・セットを選択します。
同期	ユーザーおよびグループ情報は、Oracle Internet Directory で管理されます。この情報に対する変更は、Oracle Directory Integration and Provisioning Server によって Microsoft Active Directory に反映されます。 Microsoft Active Directory から Oracle Internet Directory への同期は、インポート・プロファイルを構成することによってでは実現できない場合があります。

表 43-5 中央ディレクトリとしての Oracle Internet Directory の一般的な要件（続き）

要件	中央ディレクトリとしての Oracle Internet Directory
パスワードおよびパスワード・ベリファイア	パスワードは、Oracle Internet Directory セルフ・サービス・コンソールなどの Oracle ツール製品を使用して Oracle Internet Directory で管理されます。パスワードの変更は、Oracle Directory Integration and Provisioning Server によって Microsoft Active Directory に反映されます。ただし、このサーバーでパスワードの変更を同期化する前に、マッピング・ルールにパスワードの同期を構成する必要があります。Oracle 環境にパスワード・ベリファイアが必要な場合は、ユーザー・エントリを作成するか、またはパスワードを変更すると、パスワード・ベリファイアが自動的に生成されます。
Oracle Application Server Single Sign-On	OracleAS Single Sign-On Server を構成した後、ユーザーは、このサーバーを介して Oracle 環境にログインします。 Oracle ディレクトリ・サーバーは、ユーザーの認証のために OracleAS Single Sign-On Server からコールされると、ローカルで使用可能な資格証明を使用します。外部認証は起動しません。 ユーザーが Oracle 環境内の各種アプリケーションにアクセスするためにログインするのは 1 回のみです。
Windows のネイティブ認証（自動ログイン）	これは、OracleAS Single Sign-On Server を自動ログイン・モードで構成することによって、Windows ベースのユーザーに対して有効にできます。 Windows ネイティブ認証が構成されると、Windows ユーザーは、Windows デスクトップにログインした後、再度 Oracle 環境にログインする必要はありません。
Active Directory 外部認証プラグイン	Oracle Internet Directory ではユーザーの資格証明がローカルで管理されるため、Active Directory 外部認証プラグインは必要ありません。

Oracle Internet Directory に作成された新しいユーザーまたはグループは、Oracle Directory Integration and Provisioning Server によって Microsoft Windows 環境に自動的にプロビジョニングされます。このプロビジョニングが実行される前に、Oracle Internet Directory と Microsoft Active Directory 間の一方向同期を構成する必要があります。

複数の Microsoft Active Directory Server が含まれている場合は、Oracle Directory Integration and Provisioning Server によって、それぞれの Microsoft Active Directory Server 内のユーザーおよびグループがプロビジョニングされます。このプロビジョニングが実行される前に、Oracle Internet Directory と Microsoft Active Directory 間の一方向同期を構成する必要があります。

中央ディレクトリとしての Microsoft Active Directory の配置

表 43-6 に、この配置の一般的な要件を示します。

表 43-6 中央ディレクトリとしての Microsoft Active Directory の一般的な要件

要件	中央ディレクトリとしての Microsoft Active Directory
初期ブートストラップ	Directory Integration and Provisioning Assistant によって、Microsoft Active Directory に格納されているユーザーおよびグループが Oracle Internet Directory に移入されます。 複数の Microsoft Active Directory Server が存在する場合は、Microsoft Active Directory Server の数と同じ回数 Directory Integration and Provisioning Assistant を実行する必要があります。 Microsoft Active Directory でのみ、パスワード資格証明などのユーザー情報の管理を選択できます。この配置では、Oracle 環境でシングル・サインオンを有効にするために、Oracle Directory Integration and Provisioning Server によって、ユーザー・エントリの属性の最小セットを Oracle Internet Directory に同期させることができます。 パスワードは移行されません。
同期	ユーザーおよびグループ情報の真のソースは Microsoft Active Directory です。この情報は Microsoft Active Directory で管理されます。ユーザーおよびグループ情報に対する変更も、Oracle Directory Integration and Provisioning Server によって、Microsoft Active Directory から Oracle Internet Directory に同期化されます。 Oracle Internet Directory から Microsoft Active Directory への同期は、エクスポート・プロファイルを構成することによってでは実現できない場合があります。
パスワードおよびパスワード・ベリファイア	パスワードは、Microsoft Windows のツールを使用して Microsoft Active Directory で管理することが前提とされています。パスワードの変更は、Oracle Directory Integration and Provisioning Server によっては Oracle Internet Directory に反映されません この配置では、Oracle 環境で必要な場合があるパスワード・ベリファイアは生成できません。ユーザーは、パスワード・ベリファイアを Oracle 環境で使用可能にするために、Oracle 環境にパスワードを設定してパスワード・ベリファイアを生成することができます。ただし、この場合は、パスワードの変更時に、Oracle ディレクトリ・サーバーによってパスワード・ベリファイアが生成されます。このパスワードは `userpassword` 属性には格納されません。この属性は空のままになります。
Oracle Application Server Single Sign-On	OracleAS Single Sign-On Server を構成した後、ユーザーは、このサーバーを介して Oracle 環境にログインします。Oracle 環境内の各種コンポーネントにアクセスするためにログインするのは 1 回のみです。 Microsoft Active Directory でのみ資格証明を持つユーザーは、外部認証プラグインを起動する Oracle ディレクトリ・サーバーによって認証されます。 Oracle Internet Directory で資格証明を持つユーザーは、Oracle ディレクトリ・サーバーによってローカルで認証されます。

表 43-6 中央ディレクトリとしての Microsoft Active Directory の一般的な要件（続き）

要件	中央ディレクトリとしての Microsoft Active Directory
Windows のネイティブ認証（自動ログイン）	Oracle Internet Directory を中央ディレクトリとする配置と同様です。ただし、自動ログインを使用するユーザーは、Microsoft Active Directory に存在する必要があります。 Oracle Internet Directory にローカル・ユーザーが含まれ、Windows のネイティブ認証が有効な場合、シングル・サインオンはそれらに対して機能しません。このようなユーザーでは、シングル・サインオンが機能する前に、属性 `orclsamaccountname` および `krbprincipalname` をユーザー・エントリに移入する必要があります。
Active Directory 外部認証プラグイン	Microsoft Active Directory では、ユーザーの資格証明がローカルで管理されるため、このプラグインが必要です。 Oracle ディレクトリ・サーバーは、ユーザーの認証のために OracleAS Single Sign-On Server からコールされると、その資格証明が Oracle Internet Directory では使用できないことを検出します。その後、外部認証プラグインを起動します。 このプラグインによって、Microsoft Active Directory に格納されているユーザーの資格証明に対するユーザーの認証が実行されます。

Microsoft Active Directory に作成された新しいユーザーまたはグループは、Oracle Directory Integration and Provisioning Server によって、Oracle Internet Directory に自動的にプロビジョニングされます。このプロビジョニングが実行される前に、Microsoft Active Directory と Oracle Internet Directory 間の一方向同期を確立する必要があります。

複数の Microsoft Active Directory Server が含まれている場合は、Oracle Directory Integration and Provisioning Server によって、それぞれの Microsoft Active Directory Server から Oracle Internet Directory にユーザーおよびグループがプロビジョニングされます。このプロビジョニングが実行される前に、Oracle Internet Directory と各 Microsoft Active Directory Server 間の一方向同期を確立する必要があります。

パスワードは移行されません。

Microsoft Active Directory との統合の計画

Oracle Identity Management と Microsoft Active Directory との統合を正常に設定するには、次のことを実行します。

- 必要な同期の種類を決定します。この決定は、次の考慮事項に基づいて行います。
  - Oracle Internet Directory または Microsoft Active Directory をユーザーおよびグループ情報の真のソースにする必要があるかどうか
  - 一方向または双方向の同期が必要かどうか
  - 単一または複数の Microsoft Active Directory ドメインを統合する必要があるかどうか

  - Microsoft Active Directory 環境に Global Catalog が構成されているかどうか（複数ドメインの場合）

- Active Directory 外部認証プラグインが必要かどうかを決定します。必要な場合は、43-40 ページの「Active Directory 外部認証プラグインの構成」の手順を実行します。
- Microsoft Active Directory から Oracle Internet Directory に同期化し、Microsoft Active Directory で変更を追跡する必要がある場合は、43-6 ページの表 43-2 を使用して追跡方法を決定します。43-21 ページの「Active Directory コネクタの構成」で説明する同期の使用例は、USNChanged 方法に基づいています。DirSync 方法を使用するには、同期の使用例に対して、その使用例に記載されているわずかな変更を行う必要があります。
- 43-21 ページの「Active Directory コネクタの構成」で説明する同期の使用例が要件を満たしていない場合は、43-42 ページの「Active Directory コネクタのカスタマイズ」を参照してください。

同期の準備が完了した後、同期を開始する前に、Microsoft Active Directory から Oracle Internet Directory、または Oracle Internet Directory から Microsoft Active Directory にデータの初期移行が必要かどうかを判断します。必要な場合は、43-49 ページの「ディレクトリ間でのデータの移行」の手順を実行します。

> **関連項目：** 様々な同期の使用例の設定方法については、43-21 ページの「Active Directory コネクタの構成」を参照してください。

Active Directory コネクタの構成

この項では、様々な使用例で、Microsoft Active Directory との統合を構成する方法について説明します。

次の項目について説明します。

- Active Directory コネクタ構成の使用例の概要
- 使用例の概要
- Directory コネクタに追加する必要がある情報の概要
- adprofilecfg.sh ツールの概要
- 様々な使用例に共通のタスク
- シングル・ドメイン Microsoft Active Directory と Oracle Internet Directory 間の同期
- 複数ドメイン Microsoft Active Directory と Oracle Internet Directory 間の同期

Active Directory コネクタ構成の使用例の概要

この項で説明する使用例では、次のことが前提とされています。

- 同期化を行うための十分なデフォルトの属性セットが Oracle Internet Directory とともにインストールされています。
- ユーザーおよびグループ・オブジェクトのみを同期化する必要があります。
- Microsoft Active Directory からのユーザーおよびグループの移行は不要です。

シングル・ドメインを持つ Microsoft Active Directory 環境での同期の使用例

表 43-7 シングル・ドメインを持つ Microsoft Active Directory 環境での使用例

使用例番号	同期構成
使用例 1	Microsoft Active Directory から Oracle Internet Directory へのユーザーおよびグループの同期化
使用例 2	Oracle Internet Directory から Microsoft Active Directory へのユーザーおよびグループの同期化
使用例 3	Oracle Internet Directory と Microsoft Active Directory 間でのユーザーおよびグループの双方向の同期化

複数ドメインを持つ Microsoft Active Directory 環境での同期の使用例

表 43-8 複数ドメインを持つ Microsoft Active Directory 環境での使用例

使用例番号	同期構成
使用例 4	Global Catalog Server から Oracle Internet Directory へのユーザーおよびグループの同期化
使用例 5	Global Catalog Server を使用しない、Microsoft Active Directory から Oracle Internet Directory へのユーザーおよびグループの同期化
使用例 6	Oracle Internet Directory から Microsoft Active Directory へのユーザーおよびグループの同期化

使用例の概要

各使用例では、1 つの例が使用されています。これらの例では、次のことが前提とされています。

- Oracle Internet Directory と Microsoft Active Directory 間のユーザーおよびグループの同期化には、常に、1 対 1 のドメイン・マッピングが使用されます。つまり、ユーザー・エントリおよびグループ・エントリの識別名は両方のディレクトリで同じになります。
- Oracle Internet Directory は、ホスト `iasdemo.us.mycompany.com` にインストールされます。これは、Oracle Internet Directory のデフォルトのレルムが `dc=us,dc=mycompany,dc=com` であることを意味します。
- Oracle ディレクトリ・サーバーはポート 389 で稼働しています。
- ディレクトリ管理者のパスワードは、Oracle Internet Directory のインストール時に選択されたとおり、`welcome1` です。
- 他のツール（Directory Integration and Provisioning Assistant および adprofilecfg.sh）によって、パスワードの入力を求めるプロンプトが表示されます。入力するパスワードは `welcome1` です。
- adprofilecfg.sh によって、スーパー・ユーザーの識別名の入力を求めるプロンプトが表示されます。入力する値は `dn=orcladmin` です。
- シングル・ドメイン Microsoft Active Directory 環境では、ホスト名は `addemo.us.mycompany.com` です。これは、Microsoft Active Directory ホストのドメインが、インストール時に設定した Oracle Internet Directory のデフォルトのレルム（`dc=us,dc=mycompany,dc=com`）と同様であることを意味します。

  そうでない場合は、Oracle Internet Directory のインストール時に、デフォルトのレルム値を、Microsoft Active Directory ドメインに対応して設定する必要があります。この例では、そのドメインは `dc=us,dc=mycompany,dc=com` です。

  Oracle Internet Directory をすでにインストールしていて、デフォルトのレルムが Microsoft Active Directory ホストのドメインに対応していない場合は、Oracle Identity Management を再インストールすることをお薦めします。再インストールする場合は、適切な値のデフォルトのレルムを設定してください。適切な値を設定しないと、この項で説明する設定の使用例は正常に実行されません。
- この項では、複数ドメイン Microsoft Active Directory 環境の例で、ホスト名 `ad1demo.a.us.mycompany.com` および `ad2demo.b.us.mycompany.com` の 2 つのドメインを使用します。これは、Microsoft Active Directory ホストのドメインがそれぞれ `dc=a,dc=us,dc=mycompany,dc=com` と `dc=b,dc=us,dc=mycompany,dc=com` であることを意味します。

また、Oracle Internet Directory のインストール時に、デフォルトのレルム値を Microsoft Active Directory Server のドメインの親に設定する必要があります。この例では、デフォルトのレルム値は dc=us,dc=mycompany,dc=com です。そうでない場合は、Oracle Identity Management を再インストールすることをお薦めします。再インストールする場合は、適切な値のデフォルトのレルムを設定してください。適切な値を設定しないと、この項で説明する設定の使用例は正常に実行されません。

- 後半の使用例では、Active Directory で変更を追跡するために USNChanged 方法を使用します。ただし、DirSync 方法を使用する必要がある場合は、プロファイル ActiveChgImp を、この手順で必要なプロファイル activeImport に置き換えます。
- Oracle Internet Directory から作成されたすべてのユーザーは、オブジェクト・クラス orclADUser にエントリ（orclSAMAccountName という必須属性を含む）を追加する必要があります。orclSAMAccountName には、特殊文字を指定できないことに注意してください。Oracle Internet Directory セルフ・サービス・コンソールからユーザーを作成する場合は、Oracle Internet Directory セルフ・サービス・コンソールを介して、orclADUser オブジェクト・クラスおよび orclSAMAccountName が含まれるようにユーザー作成プロパティを変更します。また、属性 orclSAMAccountName の値は、ActiveDirectorydomain$userid と指定できます。

Directory コネクタに追加する必要がある情報の概要

インストール時に、同期の有効化に必要なほぼすべての構成情報が Oracle Internet Directory に事前構成されます。その事前構成された情報以外に、最小限の情報を Active Directory コネクタに追加する必要があります。

Active Directory コネクタに追加する必要がある情報は、Microsoft Active Directory 環境に関係します。これには次の情報が含まれます。

- Microsoft Active Directory の URL（host:port）
- Active Directory コネクタで使用される Microsoft Active Directory のユーザー・アカウントおよびパスワード
- 同期化されるユーザーおよびグループを含む Microsoft Active Directory ドメイン

この情報の追加には、コマンドライン・ツールまたは Oracle Directory Manager のいずれかを使用できます。

また、デフォルトのレルムが変更された場合は、各種同期プロファイルの所有者のみが user および group コンテナの下にエントリを作成、変更および削除できるように、ACL を再作成する必要があります。デフォルトの ACL は、インストール時に作成されますが、配置のセキュリティ要件を満たすように変更する必要がある場合があります。ACL を変更する必要がある場合については、43-27 ページの「使用例 1: Microsoft Active Directory から Oracle Internet Directory への一方向同期」を参照してください。

関連項目： デフォルトのアクセス制御構成をカスタマイズする方法の詳細は、3-3 ページの「タスク 3: デフォルトのセキュリティ構成の再設定」を参照してください。

adprofilecfg.sh ツールの概要

次の項で説明する使用例では、adprofilecfg.sh ツールを使用して Microsoft Active Directory 関連情報をデフォルトのプロファイルに構成します。このツールを実行すると、マスターのデフォルトのプロファイルから、3 つのデフォルトのプロファイルが作成され、ユーザーが入力する情報で更新されます。デフォルトのプロファイルのいずれかをすでにカスタマイズしている場合は、adprofilecfg.sh ツールによって上書きされます。この場合は、次の「様々な使用例に共通のタスク」で説明するとおり、デフォルトのプロファイルの名前を変更します。

様々な使用例に共通のタスク

この項では、ほぼすべての使用例で、それぞれのインストールに対して 1 回のみ実行する必要があるタスクについて説明します。たとえば、この章の後半で説明する使用例 1 と 2 の両方を実行するとします。これらのタスクを実行して使用例 1 を設定した場合は、使用例 2 の設定時にこれらのタスクを再度実行する必要はありません。

タスク 1: Active Directory 同期プロファイルに構成される Microsoft Active Directory 情報の確認

これを行うには、Microsoft Active Directory Server に対して次のコマンドを入力します。

```
ldapsearch -p port -h host -D user account -w password -b "" -s base "objectclass=*"
defaultnamingcontext
```

たとえば、次のようにします。

```
ldapsearch -p 389 -h adtest.us.MyCompany.com -D Administrator@us.MyCompany.com -w
welcome1 -b "" -s base "objectclass=*" defaultnamingcontext
```

これによって、Microsoft Active Directory Server のドメイン名が戻されます。

この例では、正確な出力は `defaultNamingContext=DC=us,DC=MyCompany,dc=com` です。

タスク 2: Microsoft Active Directory 環境に関連する情報の構成

このタスクには、43-10 ページの「設定時に必要な情報」で説明した情報の同期化に使用する同期プロファイルへの追加も含まれます。

デフォルトの同期プロファイルを使用する場合は、スクリプト $ORACLE_HOME/ldap/odi/admin/adprofilecfg.sh を使用して情報を設定します。このスクリプトによって、次の値を入力するプロンプトが表示されます。

- Oracle Internet Directory のスーパー・ユーザーの識別名およびパスワード
- Microsoft Active Directory の URL（host:port）
- Active Directory コネクタで使用される Microsoft Active Directory のユーザー・アカウントおよびパスワード
- 同期化される Microsoft Active Directory ドメイン : たとえば、cn=users,dc=us,dc=com

パラメータ値を入力すると、adprofilecfg.sh によって Directory Integration and Provisioning Assistant が起動されます。この Assistant によって、デフォルトの Active Directory 同期プロファイルに Microsoft Active Directory 接続情報およびマッピング・ルール情報が設定されます。

注意 : この手順は、デフォルトのプロファイルが使用されるすべての同期の使用例に対して 1 回のみ実行する必要があります。

タスク 3: 同期化に使用する Oracle Directory Integration and Provisioning Server の起動

注意 :

- この手順は、同期化に使用する Directory Integration and Provisioning Server を起動するために、1 回のみ実行する必要があります。ただし、同期化は、同期プロファイルが有効になるまで開始されません。
- インストール後、Directory Integration and Provisioning Server は、デフォルトで、常に、instance=1 として稼働しています。この Directory Integration and Provisioning Server は、同期化に必要な Directory Integration and Provisioning Server とは無関係です。同期化に使用される Directory Integration and Provisioning Server は、1 以上のインスタンスとして実行する必要があります。

同期化に使用する Directory Integration and Provisioning Server を起動するには、次のコマンドを入力します。

```
oidctl connect=iasdb server=odisrv instance=2 configset=1 flags="port=3060" start
```

シングル・ドメイン Microsoft Active Directory と Oracle Internet Directory 間の同期

この項では、シングル・ドメイン Microsoft Active Directory と Oracle Internet Directory 間のユーザーおよびグループの一方向同期を設定する様々な使用例について説明します。

使用例 1: Microsoft Active Directory から Oracle Internet Directory への一方向同期

この使用例では、次のことが前提とされています。

- デフォルトの属性セットのみが Microsoft Active Directory から Oracle Internet Directory に同期化される必要があります。
- デモおよびテスト・システムで一般的であるように、データの初期移行は必要ありません。

通常、この使用例を設定するには、次の手順を実行します。

1. 43-25 ページの「様々な使用例に共通のタスク」で説明したタスク 1 ～ 3 を実行します。
2. グループを同期化する場合は、この項で説明するタスク 4 ～ 6 を実行します。

タスク 4: グループを同期化するための ACL の構成（グループを同期化する場合にのみ必要）

> **注意：** この手順は、グループが同期化されている場合にのみ実行する必要があります。

このタスクによって、users コンテナの下にグループを作成できるように適切なアクセス制御が設定されます。適切なアクセス制御を設定するには、次の手順を実行します。

1. grantrole.ldif という LDIF ファイルを作成します。このサンプル・ファイルについては、この章の終わりを参照してください。デフォルトのレルムが dc=us,dc=mycompany,dc=com でない場合は、ファイル grantrole.ldif を編集し、すべての dc=us,dc=mycompany,dc=com 文字列を実際のデフォルトのレルム（dc=us,dc=YourCompany,dc=com）に置き換えます。このファイルを保存します。
2. 次のコマンドを入力します。

   ```
   ldapmodify -h host  -p port -D DN of orcladmin -p password -f grantrole.ldif
   ```

   たとえば、次のように入力します。

   ```
   ldapmodify -c -h iasdemo -p 3060 -D cn=orcladmin -w welcome1 -f grantrole.ldif
   ```

   これによって、Oracle Internet Directory でグループを作成および変更するために必要な ACL ポリシーが Oracle Internet Directory に構成されます。

タスク 5: Microsoft Active Directory から Oracle Internet Directory への同期の開始

このタスクでは、profileStatus 属性を ENABLE に設定してそれぞれのプロファイルを有効にする必要があります。このタスクを実行するには、次のコマンドを入力します。

```
Dipassistant mp -profile ActiveChgImp odip.profile.status = ENABLE
```

タスク 6: 同期が開始されていることの確認

次のコマンドを入力します。

```
ldapsearch -h oid_host -p oid_port -D cn=dipadmin -w orcladmin_password -b
"orclodipagentname=activechgimp,cn=subscriber profile,cn=changelog
subscriber,cn=oracle internet directory' -s base "objectclass=*"
orclodipsynchronizationstatus orclodiplastsuccessfulexecutiontime
```

表 43-9 に、同期が正常に開始された場合のステータス属性の値を示します。

表 43-9 正常な同期を示す属性値

属性	正常な同期を示す値
同期ステータス	`Synchronization successful`
最終正常実行時間	*Date and time* (**注意 :** この値は、現在の日時に近い値である必要があります。)

次に、正常な同期を示す結果の例を示します。

```
Synchronization successful November 04, 2003 15:56:03
```

注意 :

- 日時は、現在の日時に近い値である必要があります。
- ldapsearch コマンドを実行する場合は、インストール時に指定された、orcladmin パスワードと同一の dipadmin パスワードが必要です。

使用例 2: Oracle Internet Directory から Microsoft Active Directory への一方向同期

この使用例では、43-27 ページの「使用例 1: Microsoft Active Directory から Oracle Internet Directory への一方向同期」と同様のことが前提とされていますが、同期の方向は、Oracle Internet Directory から Microsoft Active Directory です。この使用例では、追加情報およびアクセス制御を設定する必要はありません。

通常、この使用例を設定するには、次の手順を実行します。

1. 43-25 ページの「様々な使用例に共通のタスク」で説明したタスク 1 ～ 3 を実行します。
2. この項で説明するタスク 4 および 5 を実行します。

タスク 4: Microsoft Active Directory から Oracle Internet Directory への同期の開始

このタスクでは、profileStatus 属性を ENABLE に設定してそれぞれのプロファイルを有効にする必要があります。このタスクを実行するには、次のコマンドを入力します。

```
Dipassistant mp -profile ActiveChgImp odip.profile.status = ENABLE
```

タスク 5: 同期が開始されていることの確認

次のコマンドを入力します。

```
ldapsearch -h oid_host -p oid_port -D cn=dipadmin -w orcladmin_password -b
"orclodipagentname=activechgimp,cn=subscriber profile,cn=changelog
subscriber,cn=oracle internet directory' -s base "objectclass=*"
orclodipsynchronizationstatus orclodiplastsuccessfulexecutiontime
```

表 43-9 に、同期が正常に開始された場合のステータス属性の値を示します。

表 43-10 正常な同期を示す属性値

属性	正常な同期を示す値
同期ステータス	Synchronization successful
最終正常実行時間	*Date and time* (**注意 :** この値は、現在の日時に近い値である必要があります。)

次に、正常な同期を示す結果の例を示します。

```
Synchronization successful November 04, 2003 15:56:03
```

注意 :

- 日時は、現在の日時に近い値である必要があります。
- ldapsearch コマンドを実行する場合は、インストール時に指定された、orcladmin パスワードと同一の dipadmin パスワードが必要です。

使用例 3: Oracle Internet Directory と Microsoft Active Directory 間の双方向同期

双方向同期を設定するには、前述したとおり、使用例 1 および 2 の両方を実行します。

複数ドメイン Microsoft Active Directory と Oracle Internet Directory 間の同期

この項では、2 つのドメインが存在する Microsoft Active Directory 環境での設定タスクについて説明します。3 つ以上のドメインが存在する Microsoft Active Directory 環境では、追加ドメインの同期を設定するタスクは、この項で説明するタスクに類似しています。

使用例 4: Microsoft Active Directory 環境に Global Catalog が構成されている場合の Microsoft Active Directory から Oracle Internet Directory への一方向同期

注意： Global Catalog は、変更を Microsoft Active Directory から Oracle Internet Directory に同期化する場合にのみ使用できます。また、Microsoft Active Directory での変更の追跡に USNChanged 方法が使用されている場合にのみ使用できます。

この使用例の説明には、次の 2 つの Microsoft Active Directory ドメイン・サーバーを持つ配置例を使用します。

- `a.us.MyCompany.com`
- `b.us.MyCompany.com`

3 つ以上のドメインが存在する場合の設定手順は、使用例 1 と同様（LDIF ファイルを実際の複数ドメイン環境に応じてカスタマイズするタスク 4 を除く）となります。

通常、この使用例を設定するには、次の手順を実行します。

1. 43-25 ページの「様々な使用例に共通のタスク」で説明したタスク 1 ～ 3 を実行します。
2. この項で説明するタスク 4 ～ 6 を実行します。

タスク 1 ～ 3 を実行する場合は、次の考慮事項に注意してください。

- タスク 1 および 2 では、Microsoft Active Directory のホストおよびポートの情報が、Global Catalog が稼働しているホストおよびポートの情報であることを確認してください。Global Catalog が稼働しているデフォルトのポート番号は 3268 です。
- タスク 2 では、Microsoft Active Directory ドメインの値を適切に入力する必要があります。通常、すべての Microsoft Active Directory ドメインの親であるエントリの識別名にする必要があります。この例では、この値は、`dc=us,dc=MyCompany,dc=com` です。

タスク 4: 適切な DIT 構造の作成およびグループの同期化に必要な ACL の構成

Oracle Internet Directory には、複数ドメイン Microsoft Active Directory の使用例で使用するための完全な DIT 構造は準備されていません。そのため、次のことを実行する必要があります。

- Oracle Internet Directory にエントリを作成します。この例では、最初のドメインに users コンテナを作成するために、次の識別名を持つエントリを作成する必要があります。

  ```
  dc=a,dc=us,dc=mycompany,dc=com
  dc=b,dc=us,dc=mycompany,dc=com
  cn=users,dc=a,dc=us,dc=mycompany,dc=com
  ```

  2 番目のドメインに `users` コンテナを作成するには、次の識別名を持つエントリを作成する必要があります。

  ```
  cn=users,dc=b,dc=us,dc=mycompany,dc=com
  ```

- ACL を `users` コンテナに割り当てて、それらのコンテナの下にユーザーおよびグループを作成できるようにします。

  値 `dc=us,dc=mycompany,dc=com` を指すように、ユーザー検索ベースおよびグループ検索ベースを再設定します。これによって、すべての Oracle アプリケーションで、2 つの *users* コンテナ内のユーザーおよびグループを検索できるようになります。

- `multidomaindit.ldif` という LDIF ファイルを作成します。このファイルによって、適切な DIT 構造およびこの例で必要な ACL が作成されます。

- このファイルの例は、43-58 ページの「multidomaindit.ldif」を参照してください。このファイルは、この使用例の Microsoft Active Directory サンプル・ドメインを、ご使用の環境の Microsoft Active Directory ドメインに置き換えることによって編集できます。

  このファイルをロードするには、次のコマンドを入力します。

  ```
  ldapmodify -h host  -p port -D DN of orcladmin -p password -f
  multidomaindit.ldif
  ```

  たとえば、次のように入力します。

  ```
  ldapmodify -h iasdemo  -p 3060 -D cn=orcladmin -p welcome1
  -f multidomaindit.ldif
  ```

タスク 5: Microsoft Active Directory から Oracle Internet Directory への同期の開始

このタスクでは、profileStatus 属性を ENABLE に設定してそれぞれのプロファイルを有効にする必要があります。このタスクを実行するには、次のコマンドを入力します。

```
Dipassistant mp –profile ActiveChgImp odip.profile.status = ENABLE
```

タスク 6: 同期が開始されていることの確認

次のコマンドを入力します。

```
ldapsearch -h oid_host -p oid_port -D cn=dipadmin -w orcladmin_password -b
"orclodipagentname=activechgimp,cn=subscriber profile,cn=changelog
subscriber,cn=oracle internet directory' -s base "objectclass=*"
orclodipsynchronizationstatus orclodiplastsuccessfulexecutiontime
```

表 43-11 に、同期が正常に開始された場合のステータス属性の値を示します。

表 43-11 正常な同期を示す属性値

属性	正常な同期を示す値
同期ステータス	Synchronization successful
最終正常実行時間	*Date and time* (**注意 :** この値は、現在の日時に近い値である必要があります。)

次に、正常な同期を示す結果の例を示します。

```
Synchronization successful November 04, 2003 15:56:03
```

注意 :

- 日時は、現在の日時に近い値である必要があります。
- ldapsearch コマンドを実行する場合は、インストール時に指定された、orcladmin パスワードと同一の dipadmin パスワードが必要です。

使用例 5: Microsoft Active Directory 環境に Global Catalog が構成されていない場合の Microsoft Active Directory から Oracle Internet Directory への一方向同期

注意：

- 3 つ以上のドメインが存在する場合、この項で説明する設定手順は、LDIF ファイルを実際の複数ドメイン環境に応じて変更するタスク 4 を除いて同様です。
- この設定では、Microsoft Active Directory ドメインの数と同数のプロファイルを作成する必要があります。この例では、設定に 2 つのプロファイルが必要です。この使用例では、1 つのデフォルトのプロファイル（`ActiveChgImp`）を使用し、このプロファイルの名前を `ActiveChgImp1` に変更した後、`ActiveChgImp` という別のプロファイルを作成します。

通常、この使用例を設定するには、次の手順を実行します。

1. 最初の Microsoft Active Directory ドメインで、43-25 ページの「様々な使用例に共通のタスク」で説明したタスク 1 ～ 3 を実行します。このドメインは、`a.MyOracle.com` などにすることができます。
2. この項で説明するタスク 4 ～ 9 を実行します。

タスク 1 ～ 3 を実行する場合は、次の考慮事項に注意してください。

- タスク 1 および 2 では、Microsoft Active Directory のホストおよびポートの情報が、最初のドメイン・サーバーのホストおよびポートの情報であることを確認してください。この例では、`a.MyOracle.com` です。
- タスク 2 では、Microsoft Active Directory ドメインの値を適切に入力する必要があります。通常、この値は、Microsoft Active Directory ドメイン・エントリの識別名です。この例では、この値は `dc=a,dc=us,dc=MyCompany,dc=com` です。

タスク 4: 適切な DIT 構造の作成およびグループの同期化に必要な ACL の構成

Oracle Internet Directory には、複数ドメイン Microsoft Active Directory の使用例で使用するための完全な DIT 構造は準備されていません。そのため、次のことを実行する必要があります。

- Oracle Internet Directory にエントリを作成します。この例では、最初のドメインに users コンテナを作成するために、次の識別名を持つエントリを作成する必要があります。

```
dc=a,dc=us,dc=mycompany,dc=com
dc=b,dc=us,dc=mycompany,dc=com
cn=users,dc=a,dc=us,dc=mycompany,dc=com
```

2 番目のドメインに users コンテナを作成するには、次の識別名を持つエントリを作成する必要があります。

```
cn=users,dc=b,dc=us,dc=mycompany,dc=com
```

- ACL を *users* コンテナに割り当てて、それらのコンテナの下にユーザーおよびグループを作成できるようにします。

  値 dc=us,dc=mycompany,dc=com を指すように、ユーザー検索ベースおよびグループ検索ベースを再設定します。これによって、すべての Oracle アプリケーションで、2 つの users コンテナ内のユーザーおよびグループを検索できるようになります。

- multidomainditimp.ldif という LDIF ファイルを作成します。このファイルによって、適切な DIT 構造およびこの例で必要な ACL が作成されます。

  このファイルの例は、43-58 ページの「multidomaindit.ldif」を参照してください。

  このファイルをロードするには、次のコマンドを入力します。

  ```
  ldapmodify -h host  -p port -D DN of orcladmin -p password -f
  multidomaindit.ldif
  ```

  たとえば、次のようにします。

  ```
  ldapmodify -h iasdemo  -p 3060 -D cn=orcladmin -p welcome1
  -f multidomaindit.ldif
  ```

タスク 5: プロファイル名の変更

プロファイル名を変更するには、次のことを実行します。

- ディレクトリにプロファイルに対するアクセス権を追加します。このアクセス権によって、名前を変更したプロファイルを使用するコネクタのかわりに Directory Integration and Provisioning Server を使用して、ユーザーおよびグループを追加、変更および削除できます。
- 古いプロファイルに対するアクセス権を削除します。

たとえば、43-60 ページの「renameprofile.ldif」のサンプル・ファイルを使用して、renameprofile.ldif という名前のプロファイルを作成します。このサンプル・プロファイルでは、デフォルトのインポート・プロファイルの名前を ActiveChgImp から ActiveChgImp1 に変更することが前提とされています。次の手順を実行します。

1. LDIF ファイルを変更して、名前 ActiveChgImp および ActiveChgImp1 をご使用のプロファイル名と置き換えます。

2. 次のコマンドを入力します。

```
ldapmodify -h host  -p port -D DN of orcladmin -p password -f renameprofile.ldif
```

たとえば、次のように入力します。

```
ldapmodify -h iasdemo  -p 3060 -D cn=orcladmin -p welcome1 -f renameprofile.ldif
```

タスク 6: 2 番目の Microsoft Active Directory ドメイン・サーバー（b.MyCompany.com）用の別のプロファイルの作成

このタスクを実行するには、次のコマンドを入力します。

```
Dipassistant cp $ORACLE_HOME/ldap/odi/conf/activechgimp.properties
```

これによって、ActiveChgImp という別のプロファイルが作成されます。

タスク 7: 新しいプロファイルに対するタスク 1 および 2 の実行

2 番目のディレクトリ・ドメイン（b.MyOracle.com）で、43-25 ページの「様々な使用例に共通のタスク」で説明したタスク 1 および 2 を実行します。次の考慮事項に注意してください。

- タスク 1 および 2 では、Microsoft Active Directory のホストおよびポートの情報が、2 番目のドメイン・サーバーのホストおよびポートの情報であることを確認してください。この例では、b.MyOracle.com です。
- タスク 2 では、Microsoft Active Directory ドメインの値を適切に入力する必要があります。通常は、Microsoft Active Directory ドメイン・エントリの識別名です。前述のとおり、この例では、dc=b,dc=us,dc=MyCompany,dc=com です。

タスク 8: Microsoft Active Directory から Oracle Internet Directory への同期の開始

このタスクでは、profileStatus 属性を ENABLE に設定してそれぞれのプロファイルを有効にする必要があります。

同期を開始するには、次のコマンドを入力します。

```
Dipassistant mp -profile ActiveChgImp odip.profile.status = ENABLE
Dipassistant mp -profile ActiveChgImp1 odip.profile.status = ENABLE
```

これによって、両方の Microsoft Active Directory から Oracle Internet Directory への同期が開始されます。

タスク 9: 同期が開始されていることの確認

次のコマンドを入力します。

```
ldapsearch -h oid_host -p oid_port -D cn=dipadmin -w orcladmin_password -b
"orclodipagentname=activechgimp,cn=subscriber profile,cn=changelog
subscriber,cn=oracle internet directory' -s base "objectclass=*"
orclodipsynchronizationstatus orclodiplastsuccessfulexecutiontime
```

表 43-12 に、同期が正常に開始された場合のステータス属性の値を示します。

表 43-12 正常な同期を示す属性値

属性	正常な同期を示す値
同期ステータス	`Synchronization successful`
最終正常実行時間	*Date and time* （**注意：**この値は、現在の日時に近い値である必要があります。）

次に、正常な同期を示す結果の例を示します。

```
Synchronization successful November 04, 2003 15:56:03
```

注意：

- 日時は、現在の日時に近い値である必要があります。
- ldapsearch コマンドを実行する場合は、インストール時に指定された、orcladmin パスワードと同一の dipadmin パスワードが必要です。

使用例 6: Oracle Internet Directory から Microsoft Active Directory への一方向同期

注意：

- 3 つ以上のドメインが存在する場合、この項で説明する設定手順は、LDIF ファイルを実際の複数ドメイン環境に応じて変更するタスク 4 を除いて同様です。
- この設定では、Microsoft Active Directory ドメインの数と同数のプロファイルを作成する必要があります。この例では、設定に 2 つのプロファイルが必要です。この使用例では、1 つのデフォルトのプロファイル（`ActiveExport`）を使用し、このプロファイルの名前を `ActiveExport1` に変更した後、`ActiveExport` という別のプロファイルを作成します。

通常、この使用例を設定するには、次の手順を実行します。

1. 最初の Microsoft Active Directory ドメインで、43-25 ページの「様々な使用例に共通のタスク」で説明したタスク 1 ～ 3 を実行します。このドメインは、`a.MyOracle.com` などの名前にすることができます。
2. この項で説明するタスク 4 ～ 9 を実行します。

タスク 1 ～ 3 を実行する場合は、次の考慮事項に注意してください。

- タスク 1 および 2 では、Microsoft Active Directory のホストおよびポートの情報が、最初のドメイン・サーバーのホストおよびポートの情報であることを確認してください。この例では、`a.MyOracle.com` です。
- タスク 2 では、Microsoft Active Directory ドメインの値を適切に入力する必要があります。通常、この値は、Microsoft Active Directory ドメイン・エントリの識別名です。この例では、この値は `dc=a,dc=us,dc=MyCompany,dc=com` です。

タスク 4: 適切な DIT 構造の作成およびグループの同期化に必要な ACL の構成

Oracle Internet Directory には、複数ドメイン Microsoft Active Directory の使用例で使用するための完全な DIT 構造は準備されていません。そのため、次のことを実行する必要があります。

- Oracle Internet Directory にエントリを作成します。この例では、最初のドメインに users コンテナを作成するために、次の識別名を持つエントリを作成する必要があります。

  ```
  dc=a,dc=us,dc=mycompany,dc=com
  dc=b,dc=us,dc=mycompany,dc=com
  cn=users,dc=a,dc=us,dc=mycompany,dc=com
  ```

  2 番目のドメインに `users` コンテナを作成するには、次の識別名を持つエントリを作成する必要があります。

  ```
  cn=users,dc=b,dc=us,dc=mycompany,dc=com
  ```

- ACL を *users* コンテナに割り当てて、それらのコンテナの下にユーザーおよびグループを作成できるようにします。

  値 `dc=us,dc=mycompany,dc=com` を指すように、ユーザー検索ベースおよびグループ検索ベースを再設定します。これによって、すべての Oracle アプリケーションで、2 つの `users` コンテナ内のユーザーおよびグループを検索できるようになります。

- `multidomainditimp.ldif` という LDIF ファイルを作成します。このファイルによって、適切な DIT 構造およびこの例で必要な ACL が作成されます。

  このファイルの例は、43-58 ページの「multidomaindit.ldif」を参照してください。

このファイルをロードするには、次のコマンドを入力します。

```
ldapmodify -h host  -p port -D DN of orcladmin -p password -f
multidomaindit.ldif
```

たとえば、次のようにします。

```
ldapmodify -h iasdemo  -p 3060 -D cn=orcladmin -p welcome1
-f multidomaindit.ldif
```

タスク 5: プロファイル名の変更

プロファイル名を変更するには、次のことを実行します。

- ディレクトリにプロファイルに対するアクセス権を追加します。このアクセス権によって、名前を変更したプロファイルを使用するコネクタのかわりに Directory Integration and Provisioning Server を使用して、ユーザーおよびグループを追加、変更および削除できます。
- 古いプロファイルに対するアクセス権を削除します。

たとえば、43-60 ページの「renameprofile.ldif」のサンプル・ファイルを使用して、`renameprofile.ldif` という名前のプロファイルを作成します。このサンプル・プロファイルでは、デフォルトのエクスポート・プロファイルの名前を `ActiveExport` から `ActiveExport1` に変更することが前提とされています。次の手順を実行します。

1. LDIF ファイルを変更して、名前 `ActiveChgImp` を `ActiveExport` と、`ActiveChgImp1` を `ActiveExport1` と置き換えます。
2. 次のコマンドを入力します。

   ```
   ldapmodify -h host  -p port -D DN of orcladmin -p password -f renameprofile.ldif
   ```

   たとえば、次のように入力します。

   ```
   ldapmodify -h iasdemo  -p 3060 -D cn=orcladmin -p welcome1 -f renameprofile.ldif
   ```

タスク 6: 2 番目の Microsoft Active Directory ドメイン・サーバー（b.MyCompany.com）用の別のプロファイルの作成

このタスクを実行するには、次のコマンドを入力します。

```
Dipassistant cp $ORACLE_HOME/ldap/odi/conf/activeexport.properties
```

これによって、`ActiveExport` という別のプロファイルが作成されます。

タスク 7: 新しいプロファイルに対するタスク 1 および 2 の実行

2 番目のディレクトリ・ドメイン（b.MyOracle.com）で、43-25 ページの「様々な使用例に共通のタスク」で説明したタスク 1 および 2 を実行します。次の考慮事項に注意してください。

- タスク 1 および 2 では、Microsoft Active Directory のホストおよびポートの情報が、2 番目のドメイン・サーバーのホストおよびポートの情報であることを確認してください。この例では、b.MyOracle.com です。
- タスク 2 では、Microsoft Active Directory ドメインの値を適切に入力する必要があります。通常は、Microsoft Active Directory ドメイン・エントリの識別名です。前述のとおり、この例では、dc=b,dc=us,dc=MyCompany,dc=com です。

タスク 8: Microsoft Active Directory から Oracle Internet Directory への同期の開始

このタスクでは、profileStatus 属性を ENABLE に設定してそれぞれのプロファイルを有効にする必要があります。

同期を開始するには、次のコマンドを入力します。

```
Dipassistant mp -profile ActiveExport odip.profile.status = ENABLE
Dipassistant mp -profile ActiveExport1 odip.profile.status = ENABLE
```

これによって、両方の Microsoft Active Directory から Oracle Internet Directory への同期が開始されます。

タスク 9: 同期が開始されていることの確認

次のコマンドを入力します。

```
ldapsearch -h oid_host -p oid_port -D cn=dipadmin -w orcladmin_password -b
"orclodipagentname=ActiveExport,cn=subscriber profile,cn=changelog
subscriber,cn=oracle internet directory' -s base "objectclass=*"
orclodipsynchronizationstatus orclodiplastsuccessfulexecutiontime
```

表 43-12 に、同期が正常に開始された場合のステータス属性の値を示します。

表 43-13 正常な同期を示す属性値

属性	正常な同期を示す値
同期ステータス	Synchronization successful
最終正常実行時間	*Date and time* （**注意：**この値は、現在の日時に近い値である必要があります。）

次に、正常な同期を示す結果の例を示します。

```
Synchronization successful November 04, 2003 15:56:03
```

注意：

- 日時は、現在の日時に近い値である必要があります。
- ldapsearch コマンドを実行する場合は、インストール時に指定された、orcladmin パスワードと同一の dipadmin パスワードが必要です。

Active Directory 外部認証プラグインの構成

Microsoft Active Directory にパスワードを格納している場合は、Active Directory 外部認証プラグインを使用して、Oracle Internet Directory から Microsoft Active Directory ユーザーを認証する必要があります。

この項では、Active Directory 外部認証プラグインをインストールおよび有効化する方法を説明します。

通常、これらの手順は、シングル・ドメインおよび複数ドメインの両方の Microsoft Active Directory 環境にプラグインを設定する場合と同様です。ただし、複数ドメイン環境では、外部認証プラグインに Microsoft Active Directory Global Catalog Server が必要であるという点が異なります。

この項では、次の項目について説明します。

- Active Directory 外部認証プラグインのインストール
- Active Directory 外部認証プラグインの有効化

Active Directory 外部認証プラグインのインストール

プラグインをインストールする手順は、次のとおりです。

1. `$ORACLE_HOME/ldap/admin/oidspadi.sh` を実行します。

注意： Windows オペレーティング・システムでシェル・スクリプト・ツールを実行するには、次のいずれかの UNIX エミュレーション・ユーティリティが必要です。

- Cygwin 1.3.2.2-1 以上
  サイト：`http://sources.redhat.com`
- MKS Toolkit 6.1
  サイト：`http://www.datafocus.com/`

oidspadi.sh を実行するには、次のとおり入力します。

```
cd $ORACLE_HOME/ldap/admin
sh oidspadi.sh
```

Windows オペレーティング・システムを使用している場合は、UNIX エミュレーション・ユーティリティのインストール後、次のとおり入力して oidspadi.sh を実行します。

```
sh oidspadi.sh.
```

2. Microsoft Active Directory のホスト名を入力します。これは、同期させる Microsoft Active Directory です。この値は必須です。
3. Microsoft Active Directory のポート名を入力します。複数ドメイン環境では、デフォルトのポートは Global Catalog Server のデフォルト・ポート（3268）です。
4. ディレクトリ・サーバーのホスト名を入力します。この値は必須です。
5. ディレクトリ・サーバーのポート番号を入力します。デフォルトのポートは 389 です。
6. Oracle 管理者のパスワード（orcladmin）を入力します。この値は必須です。
7. プラグインを適用する必要があるコンテナの識別名を入力します。このコンテナのすべてのエントリが Microsoft Active Directory に対して認証されます。この入力値は、Oracle Internet Directory セルフ・サービス・コンソールに用意されているユーザー検索ベースである必要はありません。この検索ベースに基づくすべてのユーザーは、Microsoft Active Directory に対して外部から認証されます。複数のコンテナを指定する場合は、セミコロン（;）を使用して識別名を区切ります。
8. Microsoft Active Directory に対する認証から除外するエントリの値を入力します。この値は、手順 7 に対する例外です。値は標準 ldapsearch フィルタの書式で入力する必要があります。たとえば、値 (&(objectclass=inetorgperson)(cn=orcladmin)) を指定すると、手順 7 で指定したユーザー・コンテナの下にあるエントリで cn=orcladmin および objectclass=inetorgperson 属性値を持つものは Microsoft Active Directory に対して認証されません。
9. プラグイン要求グループ識別名を入力します。セキュリティ上の理由から、プラグインは、このグループに属するユーザーによってのみ起動できます。たとえば、Oracle Application Server Single Sign-On 管理者がグループ cn=OracleUserSecurityAdmins,cn=Groups,cn=OracleContext に属しているとします。プラグイン要求グループ識別名にこの識別名を値として入力すると、Oracle Application Server Single Sign-On 管理者のメンバーからの要求でのみ外部認証プラグインをトリガーできます。複数の識別名値を入力できます。セミコロン（;）を使用して区切ります。この値は必須ではありませんが、セキュリティのため、指定することをお薦めします。

10. Active Directory との SSL 接続を使用するかどうかを選択します。SSL の使用を選択した場合は、次の事項を入力する必要があります。

    a. Active Directory SSL 接続ポート番号。

    b. Oracle Wallet の位置。この Wallet には、接続しようとしている Active Directory からの有効な証明書が必要です。

    c. Oracle Wallet パスワード。

    Microsoft Windows オペレーティング・システムで Wallet の位置を指定する場合は、円記号（¥）を追加します。たとえば、Wallet の位置が `D:¥storage¥wallet` の場合は、`D:¥¥storage¥¥wallet` と入力します。

11. Microsoft Active Directory のバックアップ・ドメイン・コントローラの詳細を指定します（オプション）。

Active Directory 外部認証プラグインの有効化

Active Directory 外部認証プラグインを有効にするには、次の 2 つのコマンドを使用します。

```
ldapmodify -h host  -p port  -D cn=orcladmin -w password  <<EOF
dn: cn=adwhencompare,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclpluginenable
orclpluginenable: 1
EOF

ldapmodify -h host  -p port  -D cn=orcladmin -w password  <<EOF
dn: cn=adwhenbind,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclpluginenable
orclpluginenable: 1
EOF
```

関連項目： 43-50 ページの「Active Directory 外部認証プラグインの管理」

Active Directory コネクタのカスタマイズ

デフォルト以外に必要な構成が最小限である単純な配置に Active Directory コネクタを構成する方法については、43-21 ページの「Active Directory コネクタの構成」を参照してください。ただし、配置が複雑な場合は、コネクタ構成をカスタマイズする必要がある場合があります。

注意： *ORACLE_HOME* が正しい値に設定されていることを確認してください。正しい値に設定されていない場合は、様々な使用例で指定するコマンドが適切に機能しません。

この項では、配置で必要な場合がある様々なカスタマイズについて説明します。次の項目について説明します。

- 同期プロファイルの作成およびカスタマイズ
- マッピング・ルールのカスタマイズ
- Microsoft Active Directory から情報を取得する検索フィルタのカスタマイズ
- SSL モードでの Active Directory コネクタの実行
- パスワードの同期化
- ACL のカスタマイズ
- LDAP スキーマのカスタマイズ

同期プロファイルの作成およびカスタマイズ

配置では、デフォルトのプロファイルを使用するかわりに、新しいプロファイルを作成する必要がある場合があります。また、これらのプロファイルの構成を変更する必要がある場合もあります。新しいプロファイルを作成する場合、3 つの使用可能なツールがあります。これらのツールは、次のとおりです。

- Directory Integration and Provisioning Assistant: プロファイルの作成、およびプロファイルの様々な構成パラメータ（属性）の設定に使用するコマンドライン・ツール。
- adprofilecfg.sh: デフォルトのプロファイルを作成し、Microsoft Active Directory 環境に必要な最小限の情報をすべてのデフォルトのプロファイルに設定するスクリプト。たとえば、この最小限の情報には、Microsoft Active Directory のホストおよびポート情報が含まれます。
- Oracle Directory Manager: プロファイルの作成、変更および削除に使用可能なスタンドアロンの Java ベースの GUI ツール。配置で広範囲のカスタマイズが必要な場合に有効です。

関連項目：

- 43-2 ページの「Directory Integration and Provisioning Assistant」
- 43-25 ページの「adprofilecfg.sh ツールの概要」
- 4-2 ページの「Oracle Directory Manager の使用方法」

マッピング・ルールのカスタマイズ

次のことを行う必要がある場合は、マッピング・ルールをカスタマイズする必要があります。

- ドメイン・レベル・マッピングの変更。ドメイン・レベル・マッピングによって、Microsoft Active Directory の DIT を Oracle Internet Directory の DIT にマップする方法が確立されます。
- 同期化する必要がある属性の変更。
- ソース・ディレクトリからターゲット・ディレクトリに同期化されている間に実行する必要がある変換（マッピング・ルール）の変更。

ドメイン・レベル・マッピング

次に、ドメイン・レベル・マッピングの例を示します。

```
DomainRules
%USERBASE%:%USERBASE%:
```

USERBASE は、Microsoft Active Directory のユーザーおよびグループのマップ元のコンテナを指します。通常、これは、Microsoft Active Directory ドメインのルートの下にある users コンテナです。

たとえば、Microsoft Active Directory ホストがドメイン us.mycompany.com に存在する場合、Microsoft Active Directory ドメインのルートは us.mycompany.com で、このドメインの下にある user コンテナに、識別名値 cn=users, dc=us,dc=mycompany,dc=com が含まれます。

Microsoft Active Directory と Oracle Internet Directory 間の 1 対 1 のドメイン・マッピングの場合、Oracle Internet Directory は、デフォルトのレルム値 dc=us,dc=mycompany,dc=com を使用してインストールする必要があります。このデフォルトのレルム値には、識別名値 cn=users,dc=us,dc=mycompany,dc=com を持つデフォルトのレルムの下にある users コンテナが自動的に含まれます。これによって、Microsoft Active Directory と Oracle Internet Directory 間の 1 対 1 のドメイン・マッピングが有効になります。

次に、us.mycmpany.com の下の users のみを同期化する場合のドメイン・マッピング・ルールを示します。

```
DomainRules
cn=users, dc=us, dc=mycompany, dc=com :cn=users, dc=us, dc=mycompany, dc=com
```

このルールによって、users コンテナのみを同期化できます。users コンテナ外の他のエントリに対する変更は同期化されません。

後で、ドメイン内の他のオブジェクトを同期化する必要がある場合は、次のようにルールを変更できます。

```
DomainRules
dc=us, dc=mycompany, dc=com :dc=us, dc=mycompany, dc=com
```

このルールによって、dc=us,dc=mycompany,dc=com の下のすべてのエントリを同期化できます。

属性レベル・マッピング

次に、属性レベル・マッピングの例を示します。

```
SAMAccountName:1: :user:orclADSAMAccountName: :orclADUser
userPrincipalName: : :user:orclADUserPrincipalName:
:orclADUser:name|userPrincipalName
```

ここで、Microsoft Active Directory の SAMAccountName および userPrincipalName は、それぞれ orclADSAMAccountName および orclADUserPrincipalName にマップされます。

同期化する別の属性を追加するには、前述したとおり、別のルールを追加する必要があります。同様に、属性を同期化する必要がなくなった場合は、対応するルールを削除またはコメント化する必要があります。

マッピング・ルールのカスタマイズ方法

マッピング・ルールをカスタマイズするには、次のことを実行する必要があります。

- "" の下に格納されているマッピング・ルール・ファイルを編集し、前述した必要な変更を行います。
- 変更の完了後、次のコマンドを実行します。

  dipassistant mp -profile *profile name* -host *oidhost* -port *oidport* -dn *DN* -passwd *password* odip.profile.mapfile=*pathname*

  たとえば、次のように入力します。

  ```
  dipassistant mp -profile ActiveChgImp -host iasdemo.us.oracle.com -port 3060 -dn
  cn=orcladmin -passwd welcome1 odip.profile.mapfile= activechgimp.map
  ```

サンプル・マップ・ファイルは、ディレクトリ $*ORACLE_HOME*/ldap/odi/conf にあります。各種プロファイルの拡張子は map.master です。

Microsoft Active Directory から情報を取得する検索フィルタのカスタマイズ

デフォルトでは、Active Directory コネクタによって、同期用に構成されたコンテナからすべてのタイプのオブジェクトの変更が取得されます。ただし、特定のタイプの変更のみ（ユーザーとグループのみなど）が配置に必要な場合は、検索フィルタを構成することによって、特定の変更のみを簡単に取得できます。フィルタは、変更に対して Active Directory をポーリングする際に不要な変更をフィルタ処理するために、Active Directory コネクタで使用されます。フィルタを格納する同期プロファイルには、`searchfilter` という属性があります。

たとえば、Computers オブジェクトではなく、ユーザーおよびグループに対する変更を同期化する場合は、searchfilter 属性の値を `searchfilter=(|(objectclass=group)(&(objectclass=user)(!(objectclass=computer)))` にする必要があります。

この属性を更新するには、Oracle Directory Manager または Directory Integration and Provisioning Assistant を使用できます。

SSL モードでの Active Directory コネクタの実行

Active Directory コネクタでは、2 つのサーバー間で SSL を使用することによって、Oracle Internet Directory と Microsoft Active Directory 間の同期が保護されます。SSL モードで同期化するかどうかは、配置要件によって決まります。たとえば、パブリック・データに SSL は必要ありません。ただし、パスワードなどの重要な情報の同期化には SSL が必要です。セキュリティ設定（ハード設定）では、サーバー専用認証が指定されている SSL モード（SSL モード 2）でのみ Oracle Internet Directory から Microsoft Active Directory にパスワードの変更を同期化できます。

チャネルを保護するには、次のものが必要です。

- Oracle Internet Directory と Oracle Directory Integration and Provisioning Server 間の SSL
- Oracle Directory Integration and Provisioning Server と Microsoft Active Directory 間の SSL

Oracle Internet Directory と Oracle Directory Integration and Provisioning Server 間の SSL または Oracle Directory Integration and Provisioning Server と Oracle Internet Directory 間の SSL を有効にできますが、重要な情報を同期化する前に、完全にチャネルを保護することをお薦めします。パスワードの同期化などの場合は、SSL を介してのみ同期化を行うことができます。

SSL を構成するには、次のことを実行する必要があります。

- SSL モードで Oracle ディレクトリ・サーバーを実行します（第 13 章「Secure Sockets Layer（SSL）とディレクトリ」を参照）。

- SSL モードで Oracle Directory Integration and Provisioning Server を実行します（第 36 章「Oracle Directory Integration and Provisioning Platform におけるセキュリティ」を参照）。この SSL モードは、Oracle Internet Directory Server が起動されたモードと同じである必要があります。Oracle Directory Integration and Provisioning Server の起動時に指定する `sslauth` パラメータは、SSL 通信が認証に基づいていないか、またはサーバー専用認証に基づいているかによって、1 または 2 にします。
- SSL モードで Microsoft Active Directory Server を実行します。SSL を介した Microsoft Active Directory との通信には SSL モード 2（サーバー専用認証）が必要です。また、Oracle Internet Directory および Oracle Directory Integration and Provisioning Server も SSL モード 2 で実行する必要があります。
- Oracle Internet Directory と Microsoft Active Directory の両方の証明書およびそれらを格納する Wallet を取得します。詳細は、第 13 章「Secure Sockets Layer（SSL）とディレクトリ」を参照してください。

注意： Oracle Application Server 10*g* では、クライアント / サーバー認証モードでの SSL はサポートされていません。

パスワードの同期化

Oracle Internet Directory から Microsoft Active Directory（またはその逆）にパスワードを同期化できます。

Oracle Internet Directory から Microsoft Active Directory へのパスワードの同期化

Active Directory コネクタでこの方向にパスワードを同期化する前に、次のことを行う必要があります。

- マッピング・ファイルへのパスワードの同期を有効にするマッピング・ルールの追加。次に、このマッピング・ルールの例を示します。

  ```
  Userpassword: : :person:unicodepwd: :user
  ```

- Oracle ディレクトリ・サーバーでのパスワード・ポリシーおよびパスワードの可逆暗号化の有効化。これを実行するには、エントリ `cn=PwdPolicyEntry,cn=common,cn=products,`*`DN of realm`* 内の `orclPwdPolicyEnable` および `orclpwdEncryptionEnable` 属性を値 `1` に設定する必要があります。これは、Oracle Directory Manager を使用するか、または ldapmodify コマンドを実行して行うことができます。

- SSL モード 2（サーバー専用認証）での次のサーバーの起動 :
  - Oracle ディレクトリ・サーバー
  - Oracle Directory Integration and Provisioning Server
  - Microsoft Active Directory Server

Microsoft Active Directory から Oracle Internet Directory へのパスワードの同期化

LDAP クライアントからは Microsoft Active Directory のパスワードにアクセスできないため、Oracle Application Server 10*g* では、Microsoft Active Directory から Oracle Internet Directory へのパスワードの同期化はできません。ただし、Oracle Internet Directory で使用可能なパスワードが配置に必要な場合は、次の 2 つの方法をお薦めします。

- パスワードの変更を取得し、そのパスワードを Oracle Internet Directory と同期化する Microsoft Active Directory 用プラグインを作成する。
- Oracle 環境から Active Directory パスワードを管理する。このように管理を行うと、Active Directory コネクタを使用して Oracle Internet Directory から Microsoft Active Directory にパスワードを同期化できるため、Oracle Internet Directory と Microsoft Active Directory の両方でパスワードを使用可能にできます。

ACL のカスタマイズ

デフォルトの ACL では、ユーザーおよびグループのみ作成、変更および削除できます。また、デフォルトのレルムの下にある `users` および `groups` コンテナにのみユーザーおよびグループを作成できます。

次の場合、アクセス制御リスト（ACL）をカスタマイズする必要があります。

- ユーザーおよびグループ以外のオブジェクトを同期化する必要がある場合。
- ユーザーおよびグループが同期化されるコンテナが指定したコンテナと異なる場合。これは、優先コンテナが users および groups コンテナでないか、またはデフォルトのレルムの下にない場合です。

> **関連項目：** ACL をカスタマイズする方法は、第 14 章「ディレクトリ・アクセス制御」を参照してください。

LDAP スキーマのカスタマイズ

次の場合、LDAP スキーマをカスタマイズする必要があります。

- ディレクトリ配置に、カスタム・オブジェクト・クラス、カスタム属性などのスキーマ拡張が含まれている場合。
- カスタム属性は、ディレクトリ・サーバー間で同期化する必要があります。

LDAP スキーマをカスタマイズするには、次のことを実行する必要があります。

- ソース・ディレクトリでスキーマ拡張を識別します。
- データの移行および同期を開始する前に、ターゲット・ディレクトリでスキーマ拡張を作成します。

注意： スキーマ拡張に加えて、同期化に必要な属性もマッピング・ルールに追加する必要があります。

ディレクトリ間でのデータの移行

Active Directory コネクタおよびプラグインの構成完了後、次の手順を実行します。

1. 移行するデータを識別します。ディレクトリ内のデータ全体またはサブセットのみの移行を選択できます。
2. 同期が有効にされていないことを確認します。
3. `bootstrap` オプションを指定した Directory Integration and Provisioning Assistant を使用して、ディレクトリ間でデータを移行します。ブートストラップの詳細は、第 37 章「Oracle Directory Integration and Provisioning Platform におけるディレクトリのブートストラップ」を参照してください。

   ブートストラップが完了すると、Directory Integration and Provisioning Assistant によって同期プロファイルのプロファイル・ステータス属性が適切に更新されます。
4. LDIF ファイル・ベースのブートストラップを使用した場合は、`lastchangenumber` 値を初期化する必要があります。これは、Directory Integration and Provisioning Assistant を使用して実行できます。次のように入力します。

   ```
   Dipassistant mp -updlcn
   ```

   この `lastchangenumber` 属性は、ブートストラップを開始する前に、ソース・ディレクトリの最終変更番号の値に設定する必要があります。
5. 双方向同期が必要な場合は、エクスポート・プロファイルを有効にし、Oracle ディレクトリ・サーバーで変更ロギング・オプションが有効になっていることを確認します。変更ロギングは、Oracle Internet Directory の起動時に `-l` オプションによって制御されます。デフォルトでは、変更ロギングが有効なことを意味する `TRUE` に設定されます。`FALSE` に設定されている場合は、Oracle ディレクトリ・サーバーを停止し、OID 制御ユーティリティを使用して変更ログを有効にして再起動します。

Microsoft Windows との統合の管理

この項では、次の項目について説明します。

- 一般的な管理タスク
- Active Directory 外部認証プラグインの管理

一般的な管理タスク

実行されている一般的な管理タスクは、次のとおりです。

- 同期プロファイルおよびマッピング・ファイルの管理。次のサービスが含まれます。
  - 新しいプロファイルの作成
  - プロファイルの構成（属性）の変更
  - プロファイルによるメンテナンス許可の無効化およびその再有効化。プロファイルを無効にすると、そのプロファイルに関連する同期が停止されます。
- マッピング・ルールの管理。次のサービスが含まれます。
  - 追加の属性を同期化する必要がある場合の新しいルールの作成
  - 属性を同期化する方法を変更する必要がある場合の既存のルールの変更
  - 特定の属性を同期化する必要がない場合の不要なルールの削除またはコメント化
- アクセス制御の管理
- Oracle ディレクトリ・サーバーおよび Oracle Directory Integration and Provisioning Server の起動および停止

関連項目：

- プロファイル、マッピング・ルールおよびアクセス制御の管理方法については、43-42 ページの「Active Directory コネクタのカスタマイズ」を参照してください。
- サーバーの起動方法および停止方法については、A-4 ページの「Oracle Internet Directory サーバーの起動、停止、再起動および監視」を参照してください。

Active Directory 外部認証プラグインの管理

この項では、Active Directory 外部認証プラグインを削除、無効化および再有効化する方法について説明します。

Active Directory 外部認証プラグインの削除

Active Directory 外部認証プラグインを削除するには、次のコマンドを使用します。

```
ldapdelete -h host -p port -D cn=orcladmin -w password
"cn=adwhencompare,cn=plugin,cn=subconfigsubentry"

ldapdelete -h host -p port -D cn=orcladmin -w password
"cn=adwhenbind,cn=plugin,cn=subconfigsubentry"
```

Active Directory 外部認証プラグインの無効化

Microsoft Active Directory 外部認証プラグインを無効にするには、次の 2 つのコマンドを使用します。

```
ldapmodify -h host -p port -D cn=orcladmin -w password <<EOF
dn: cn=adwhencompare,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclpluginenable
orclpluginenable: 0
EOF

ldapmodify -h host -p port -D cn=orcladmin -w password <<EOF
dn: cn=adwhenbind,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclpluginenable
orclpluginenable: 0
EOF
```

Active Directory 外部認証プラグインの再有効化

Active Directory 外部認証プラグインを再度有効にするには、次の 2 つのコマンドを使用します。

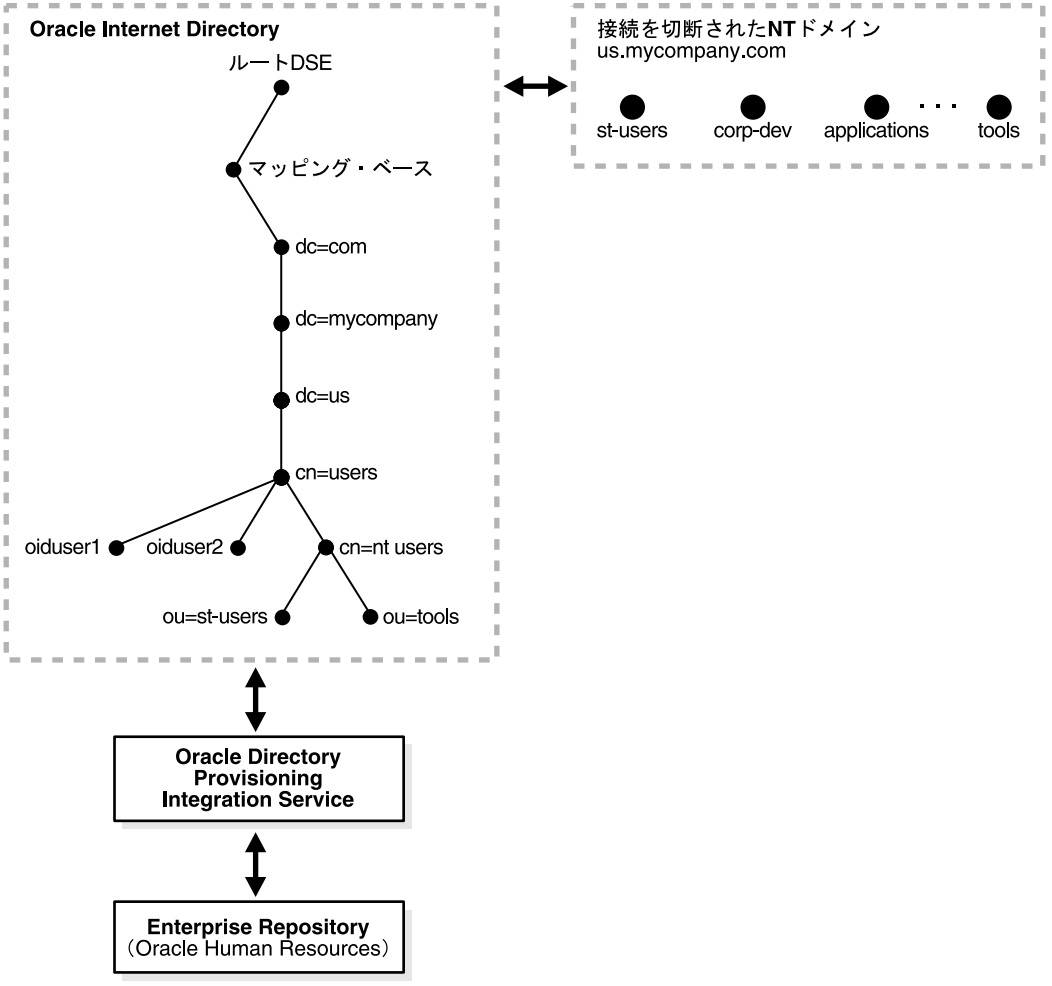
```
ldapmodify -h host  -p port  -D cn=orcladmin -w password  <<EOF
dn: cn=adwhencompare,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclpluginenable
orclpluginenable: 1
EOF

ldapmodify -h host  -p port  -D cn=orcladmin -w password  <<EOF
dn: cn=adwhenbind,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclpluginenable
orclpluginenable: 1
EOF
```

関連項目： 43-40 ページの「Active Directory 外部認証プラグインの構成」

Microsoft Windows NT 4.0 との統合

Microsoft Windows NT ドメイン・ユーザーは環境にも統合できます。Microsoft Windows NT グループは Oracle Internet Directory とは同期されません。またそのグループのメンバーの情報も同期されません。この場合、Microsoft Windows NT の各ドメインは、ドメイン・オブジェクトまたは Oracle Internet Directory 内の組織単位オブジェクトにマップできます。43-52 ページの図 43-4 に、Oracle Internet Directory ディレクトリ情報ツリー内のドメイン・コンテナへの Microsoft Windows NT ドメインの一般的なマッピングを示します。

図 43-4 Oracle Internet Directory DIT と Microsoft Windows NT ドメインとの統合



最小のユーザー・フットプリントが Oracle Internet Directory に自動的に作成されるように、Microsoft Windows NT ドメインは Oracle Internet Directory に統合されます。

ユーザー・エントリが Microsoft Windows NT 内にあるが、Oracle Internet Directory にない場合、Oracle Application Server コンポーネントを使用するためにユーザーがログインを試行すると、自動登録プラグインが最小フットプリント情報で Oracle Internet Directory 内にシャドウ・エントリを作成します。このエントリは、同じユーザーが次回ログインを試行するときのために、Oracle Internet Directory 内に残ります。

外部リポジトリとして Microsoft Windows NT を使用し、プラグインを使用することで外部認証がサポートされます。Microsoft Windows NT 環境との継続同期はサポートされません。

Windows NT 外部認証および自動プロビジョニング・プラグインのインストールと構成

SQL スクリプト `oidspnti.sql` は、Oracle Internet Directory が Microsoft Windows プライマリ・ドメイン・コントローラと自動プロビジョニングに対して外部認証を使用できるようにするプラグインをインストールします。

スクリプトをインストールする手順は、次のとおりです。

1. Oracle Internet Directory Server が実行中かどうかを確認します。
2. 次のコマンドを入力して、スクリプトを実行します。

   ```
   cd $ORACLE_HOME/ldap/admin
   sh oidpnti.sh
   ```

3. Oracle Internet Directory のホスト名とポート番号を入力します。デフォルトのポート番号は 389 です。
4. Oracle 管理者（`orcladmin`）、つまりディレクトリ・スーパーユーザーのパスワードを入力します。
5. プラグインを適用する必要があるコンテナの識別名を入力します。このコンテナのすべてのエントリが Microsoft Windows NT ドメインに対して認証されます。Oracle Internet Directory セルフ・サービス・コンソールに用意されているユーザー検索ベースでなくてもかまいません。この検索ベースに基づくすべてのユーザーは、Microsoft Windows NT ドメインに対して外部から認証されます。複数の値を指定する場合は、セミコロン（;）を使用して区切ります。

6. プラグイン要求グループ識別名を入力します。セキュリティ上の理由から、プラグインは、このグループに属するユーザーによってのみ起動できます。たとえば、Oracle Application Server Single Sign-On 管理者がグループ `cn=OracleUserSecurityAdmins,cn=Groups,cn=OracleContext` に属しているとします。プラグイン要求グループ識別名にこの値を入力すると、Oracle Application Server Single Sign-On 管理者からの要求のみが外部認証プラグインをトリガーできます。複数の識別名値を入力できます。セミコロン（;）を使用して区切ります。この値は必須ではありませんが、セキュリティのため指定することをお薦めします。
7. 自動登録を選択します。デフォルトは Yes です。登録時、各エントリはオブジェクト・クラス `orclNTUser` に割り当てられます。

これらの手順が完了すると、プラグインがインストールされ使用可能になります。

Windows NT 外部認証プラグインの有効化

外部認証を有効にするには、次の 2 つのコマンドを入力します。

```
ldapmodify -h host -p port -D cn=orcladmin -w password <<EOF
dn: cn=ntwhencompare,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclpluginenable
orclpluginenable: 1
EOF

ldapmodify -h host -p port -D cn=orcladmin -w password <<EOF
dn: cn=ntwhenbind,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclpluginenable
orclpluginenable: 1
EOF
```

Windows NT 外部認証プラグインの無効化

外部認証プラグインを無効にするには、前述の各コマンドの `orclpluginenable` 属性を 0 に設定します。

自動プロビジョニングの有効化

自動プロビジョニングを有効にするには、次のコマンドを入力します。

```
ldapmodify -h host -p port -D cn=orcladmin -w password <<EOF
dn: cn=ntpostsearch,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclpluginenable
orclpluginenable: 1
EOF
```

自動プロビジョニングの無効化

自動プロビジョニングを無効にするには、前述のコマンドで orclpluginenable 属性の値を 0 に設定します。

Active Directory 外部認証および自動プロビジョニング・プラグインの削除

外部認証と自動登録を削除するには、Oracle Internet Directory から 2 つのプラグイン・エントリを削除します。

```
ldapdelete -h host -p port D cn=orcladmin -w password
"cn=ntwhencompare,cn=plugin,cn=subconfigsubentry"

ldapdelete -h host -p port -D cn=orcladmin -w password
"cn=ntwhenbind,cn=plugin,cn=subconfigsubentry"

ldapdelete -h host -p port -D cn=orcladmin -w password
"cn=ntpostsearch,cn=plugin,cn=subconfigsubentry"
```

Active Directory 外部認証プラグインのデバッグ

不明なエラーが発生した場合は、プラグイン・デバッグを有効にできます。次のように入力します。

```
sqlplus ods/odspassword @$ORACLE_HOME/ldap/admin/oidspdon.pls
```

プラグイン・デバッグのログを調べるには、次のように入力します。

```
sqlplus ods/ods
select * from plg_debug_log order by id;
```

プラグイン・デバッグのログを削除するには、次のように入力します。

```
sqlplus ods/ods
truncate table plg_debug_log
```

プラグイン・デバッグを無効にするには、次のように入力します。

```
sqlplus ods/ods @$ORACLE_HOME/ldap/admin/oidspdof.pls
```

注意： Active Directory 外部認証プラグインの設定（インストール時に入力した情報）に変更を加える必要がある場合は、インストール・スクリプトを再実行します。スクリプトを再実行する前に、前述の指示に従って、Active Directory 外部認証プラグインを削除してください。

Microsoft Windows との統合に関するトラブルシューティング

この項では、次の項目について説明します。

- Active Directory コネクタとの同期に関するトラブルシューティング
- Microsoft Active Directory 外部認証プラグインのデバッグ

Active Directory コネクタとの同期に関するトラブルシューティング

oditest ユーティリティを使用して Active Directory コネクタをデバッグできます。

Active Directory コネクタに関するトラブルシューティングを行うには、次のことを実行します。

- AgentName を ProfileName と指定して oditest を実行します。
- ファイル ProfileName.trc および ProfileName.aud を参照します。

複数のプロファイルが有効な場合は、このツールを各プロファイルに対して実行できます。

> **関連項目：** oditest ユーティリティの使用方法は、「Oracle Directory Integration and Provisioning Platform での同期に関するトラブルシューティング」を参照してください。

Microsoft Active Directory 外部認証プラグインのデバッグ

不明なエラーが発生した場合は、プラグイン・デバッグを有効にできます。このためには、次のように入力します。

```
sqlplus ods/odspassword @$ORACLE_HOME/ldap/admin/oidspdon.pls
```

プラグイン・デバッグのログをチェックするには、次のように入力します。

```
sqlplus ods/ods
select * from plg_debug_log order by id;
```

プラグイン・デバッグのログを削除するには、次のように入力します。

```
sqlplus ods/ods
truncate table plg_debug_log
```

プラグイン・デバッグを無効にするには、次のように入力します。

```
sqlplus ods/ods @$ORACLE_HOME/ldap/admin/oidspdof.pls
```

Microsoft Windows との統合に必要な LDIF ファイルのサンプル

この項では、次の LDIF ファイルのサンプルについて説明します。

- grantrole.ldif
- multidomaindit.ldif
- renameprofile.ldif

grantrole.ldif

```
# This ACL policy grants access to privilaged users to create groups under the
container
# cn=users,dc=us,dc=mycompany,dc=com which is the container for creating users
dn: cn=Users,dc=us,dc=mycompany,dc=com
changetype: modify
add: orclaci
orclaci: access to entry by group="cn=IASAdmins,
cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" added_object_
constraint=(objectclass=orclcontainer) (browse,add)
orclaci: access to entry by group="cn=oracledascreategroup,
cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" added_object_
constraint=(objectclass=orclgroup*) (browse,add) by group="cn=Common Group
Attributes, cn=Groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" (browse)
orclaci: access to entry filter=(&(objectclass=orclgroup)(orclisvisible=false)) by
groupattr=(owner) (browse, add, delete) by dnattr=(owner) (browse, add, delete) by
group="cn=Common Group Attributes,
cn=Groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" (browse) by * (none)
orclaci: access to entry filter=(&(objectclass=orclgroup)(!(orclisvisible=false)))
by group="cn=oracledascreategroup,
cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" added_object_
constraint=(objectclass=orclgroup) (browse,add) by group="cn=oracledasdeletegroup,
cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" (browse,delete) by
group="cn=oracledaseditgroup, cn=Groups,cn=OracleContext,dc=us,dc=mycompany,dc=com"
(browse) by groupattr=(owner) (browse, add, delete) by dnattr=(owner) (browse, add,
delete) by group="cn=Common Group Attributes,
cn=Groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" (browse)
orclaci: access to attr=(*) filter=(&(objectclass=orclgroup)(orclisvisible=false))
by groupattr=(owner) (read,search,write,compare) by dnattr=(owner)
(read,search,write,compare) by * (none) by group="cn=Common Group Attributes,
cn=Groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" (read, search, compare)
orclaci: access to attr=(*)
filter=(&(objectclass=orclgroup)(!(orclisvisible=false))) by groupattr=(owner)
(read,search,write,compare) by dnattr=(owner) (read,search,write,compare)  by
group="cn=oracledaseditgroup, cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com"
(read,search,write,compare) by group="cn=Common Group Attributes,
cn=Groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" (read, search, compare)
```

```
dn: cn=Users,dc=us,dc=mycompany,dc=com
changetype: modify
add: orclentrylevelaci
orclentrylevelaci: access to entry by group="cn=oracledascreategroup,
cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" added_object_
constraint=(objectclass=orclgroup) (browse, add) by group="cn=IASAdmins,
cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" added_object_
constraint=(objectclass=orclcontainer) (browse,add) by * (browse)
```

multidomaindit.ldif

```
#Add the users container
_dn: dc=a,dc=us,dc=mycompany,dc=com
_changetype: add
_dc: a
_objectclass: domain

_
_dn: cn=users,dc=a,dc=us,dc=mycompany,dc=com
_changetype: add
_cn: users
_objectclass: orclcontainer

dn: dc=b,dc=us,dc=mycompany,dc=com
changetype: add
dc: b
objectclass: domain

dn: cn=users,dc=b,dc=us,dc=mycompany,dc=com
changetype: add
cn: users
objectclass: orclcontainer

# ACLS for Users
#Add the acls to create/delete/modify user entries in the users container
dn: cn=users,dc=a,dc=us,dc=mycompany,dc=com
changetype: modify
add: orclaci
#ACL to add user objects
orclaci: access to entry by group =
"cn=oracledascreateuser,cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" added_
object_constraint=(objectclass=orcluser*) (browse,add)
#ACL to delete user objects
orclaci: access to entry by group="cn=oracledasdeleteuser,
cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" added_object_
constraint=(objectclass=orcluser*) (browse,delete)
#ACL to modify user objects
```

```
orclaci: access to attr = (*) by group="cn=orcldasedituser,
cn=Groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" (read, write, search, compare)
by self (read,search,write,compare) by * (noread, nowrite, nocompare)

#Add the acls to create/delete/modify user entries in the users container
dn: cn=users,dc=b,dc=us,dc=mycompany,dc=com
changetype: modify
add: orclaci
#ACL to add user objects
orclaci: access to entry by group =
"cn=oracledascreateuser,cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" added_
object_constraint=(objectclass=orcluser*) (browse,add)
#ACL to delete user objects
orclaci: access to entry by group="cn=oracledasdeleteuser,
cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" added_object_
constraint=(objectclass=orcluser*) (browse,delete)
#ACL to modify user objects
orclaci: access to attr = (*) by group="cn=orcldasedituser,
cn=Groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" (read, write, search, compare)
by self (read,search,write,compare) by * (noread, nowrite, nocompare)


#Change the usersearchbase to point to dc=us,dc=mycompany,dc=com
dn: cn=common, cn=products,cn=oraclecontext,dc=us,d=mycompany,dc=com
changetype: modify
replace: orclCommonUserSearchBase
orclCommonUserSearchBase: dc=us,dc=mycompany,dc=com

#ACLS for Groups
#Add the acls to create/delete/modify group entries in the users container
dn: cn=users,dc=a,dc=us,dc=mycompany,dc=com
changetype: modify
add: orclaci
#ACL to add group objects
orclaci: access to entry by group =
"cn=oracledascreategroup,cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com"
added_object_constraint=(objectclass=orclgroup*) (browse,add)
#ACL to delete group objects
orclaci: access to entry by group="cn=oracledasdeletegroup,
cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" added_object_
constraint=(objectclass=orclgroup*) (browse,delete)
#ACL to modify group objects
orclaci: access to attr = (*) by group="cn=orcldaseditgroup,
cn=Groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" (read, write, search, compare)
by self (read,search,write,compare) by * (noread, nowrite, nocompare)

#Add the acls to create/delete/modify group entries in the users container
```

```
dn: cn=users,dc=b,dc=us,dc=mycompany,dc=com
changetype: modify
add: orclaci
#ACL to add group objects
orclaci: access to entry by group =
"cn=oracledascreategroup,cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com"
added_object_constraint=(objectclass=orclgroup*) (browse,add)
#ACL to delete group objects
orclaci: access to entry by group="cn=oracledasdeletegroup,
cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" added_object_
constraint=(objectclass=orclgroup*) (browse,delete)
#ACL to modify group objects
orclaci: access to attr = (*) by group="cn=orcldaseditgroup,
cn=Groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" (read, write, search, compare)
by self (read,search,write,compare) by * (noread, nowrite, nocompare)

#Change the GroupSearchBase to point to dc=us,dc=mycompany,dc=com
dn: cn=common, cn=products,cn=oraclecontext,dc=us,d=mycompany,dc=com
changetype: modify
replace: orclCommonGroupSearchBase
orclCommonGroupSearchBase: dc=us,dc=mycompany,dc=com
```

renameprofile.ldif

```
#Modify the name of the profile
dn: orclodipagentname=activechgimp,cn=subscriber profile,cn=changelog
subscriber,cn=oracle internet directory
changetype: modrdn
newrdn: activechgimp1
deleteoldrdn: 1

#Remove the privileges given to the old profile and add the privileges to the new
profile
dn: cn=odipgroup,cn=odi,cn=oracle internet directory
changetype: modify
delete: uniquemember
uniquemember: orclodipagentname=activechgimp,cn=subscriber profile,cn=changelog
subscriber,cn=oracle internet directory
-
add: uniquemember
uniquemember: orclodipagentname=activechgimp1,cn=subscriber profile,cn=changelog
subscriber,cn=oracle internet directory
```

44

サード・パーティのメタディレクトリ・ソリューションとの同期

Oracle Directory Integration and Provisioning Server には、サード・パーティのメタディレクトリ・ソリューション用のマッピングやスケジューリングは用意されていません。かわりに、Oracle Internet Directory は、サポートするサード・パーティのメタディレクトリ・ソリューションとの同期を可能にするために変更ログを使用します。この章では、変更ログ情報の生成方法と、サポートするソリューションでの変更ログ情報の使用方法について説明します。また、Oracle Internet Directory と同期できるように、サード・パーティのメタディレクトリ・ソリューションを使用可能にする方法を示します。

この章では、次の項目について説明します。

変更ログ

Oracle Internet Directory は、各変更をエントリとして変更ログ・コンテナに記録します。サード・パーティのメタディレクトリ・ソリューションは、変更ログ・コンテナから変更を取得し、サード・パーティ・ディレクトリに適用します。これらの変更を取得するために、サード・パーティのメタディレクトリ・ソリューションは Oracle Internet Directory の変更ログをサブスクライブする必要があります。

変更ログ・ストアの各エントリには変更番号があります。サード・パーティのメタディレクトリ・ソリューションは、最後に適用した変更番号を記録しておき、その番号よりも大きい変更番号の変更のみを Oracle Internet Directory から取得します。たとえば、サード・パーティのメタディレクトリ・ソリューションが取得した最後の変更の番号が 250 だった場合、それ以降は番号が 251 以上の変更を取得します。

注意： サード・パーティのメタディレクトリ・ソリューションが Oracle Internet Directory の変更ログでサブスクライブされず、ソリューションが最初に取得した変更番号が最後に適用した変更番号よりも 2 以上大きい場合、Oracle Internet Directory 変更ログ内の変更の一部は、すでにパージされています。この場合、サード・パーティのメタディレクトリ・ソリューションは、Oracle Internet Directory 全体を読み取り、ソリューションが保持するコピーと Oracle Internet Directory の情報とを同期化する必要があります。

関連項目： ディレクトリ統合プロファイルの概念は、33-2 ページの「コネクタとディレクトリ統合プロファイルの概要」を参照してください。

Oracle Internet Directory と同期化するためのサード・パーティのメタディレクトリ・ソリューションの有効化

サード・パーティのメタディレクトリ・ソリューションが Oracle Internet Directory から変更を取得するには、この項で説明する次の各タスクを実行します。

- タスク 1: 初期ブートストラップの実行
- タスク 2: Oracle Internet Directory でのサード・パーティのメタディレクトリ・ソリューション用変更サブスクリプション・オブジェクトの作成

タスク 1: 初期ブートストラップの実行

ローカル・ディレクトリと Oracle Internet Directory 間のデータを同期化するためにディレクトリをブートストラップする手順は、次のとおりです。

1. Oracle Internet Directory に記録されている最後の変更番号を検索します。この番号は、DSE ルート属性の `lastChangeNumber` にあります。

   Oracle Internet Directory に記録されている最後の変更番号を検索するには、ldapsearch を使用します。次のコマンドを入力します。

   ```
   ldapsearch -h host_name -p port_number -s base -b "" 'objectclass=*'
   lastchangenumber
   ```

   変更ログがすでにパージされているために変更エントリがない場合、取得される変更番号は `0`（ゼロ）になります。

2. ldifwrite を使用して、データを Oracle Internet Directory から LDIF ファイルにエクスポートします。

3. この LDIF ファイルをクライアント・ディレクトリに適した形式に変換し、クライアント・ディレクトリにロードします。

注意： Oracle Internet Directory の新規インストールでは、初期ブートストラップは不要です。この場合、新規にインストールした Oracle Internet Directory の現行の変更番号は `0`（ゼロ）です。

関連項目： ldifwrite の使用方法は、A-54 ページの「ldifwrite の構文」を参照してください。

タスク 2: Oracle Internet Directory でのサード・パーティのメタディレクトリ・ソリューション用変更サブスクリプション・オブジェクトの作成

サード・パーティのメタディレクトリ・ソリューションが Oracle Internet Directory と同期するには、Oracle Internet Directory にそのソリューション用の変更サブスクリプション・オブジェクトを作成する必要があります。この変更サブスクリプション・オブジェクトによって、Oracle Internet Directory に格納されている変更ログ・オブジェクトへのアクセス権限がサード・パーティのメタディレクトリ・ソリューションに付与されます。

変更サブスクリプション・オブジェクトの概要

変更サブスクリプション・オブジェクトは、Oracle Internet Directory の次のコンテナの下に位置するエントリです。

```
cn=Subscriber Profile,cn=ChangeLog Subscriber,cn=Oracle Internet Directory
```

この変更サブスクリプション・オブジェクトは、サード・パーティのメタディレクトリ・ソリューションが Oracle Internet Directory とバインドして変更を取得するための一意の資格証明を提供します。管理者は、この変更サブスクリプション・オブジェクトを補助型オブジェクト・クラスの `orclChangeSubscriber` に関連付けます。このオブジェクト・クラスにはいくつかの属性があります。次の属性は必須です。

- `userPassword`

  Oracle Internet Directory の変更ログ・オブジェクトにアクセスするときに、ディレクトリが使用するパスワード。

- `orclLastAppliedChangeNumber`

  前回の同期で適用された変更番号。この属性によって、ディレクトリは、Oracle Internet Directory での変更から未適用の変更のみを取得できます。

変更サブスクリプション・オブジェクトの作成

変更サブスクリプション・オブジェクトの作成には、ldapadd を使用します。次の例では、入力ファイル `add.ldif` を使用して、コンテナ `cn=Subscriber Profile,cn=ChangeLog Subscriber,cn=Oracle Internet Directory` の下に変更サブスクリプション・オブジェクト `my_change_subscription_object` を作成し、このオブジェクトを使用可能にします。
`orclLastAppliedChangeNumber` は、初期ブートストラップ前のディレクトリにある現行の変更番号で、この例では 250 です。

- `add.ldif` ファイルの編集:

  ```
  dn: cn=my_change_subscription_object,cn=Subscriber Profile,cn=ChangeLog
  Subscriber,cn=Oracle Internet Directory
  userpassword: my_password
  orclLastAppliedChangeNumber: 250
  orclSubscriberDisable: 0
  objectclass: orclChangeSubscriber
  objectclass: top
  ```

- エントリの追加:

  ```
  ldapadd -h my_host -p 389 -f add.ldif
  ```

  関連項目： 変更サブスクリプション・オブジェクトを一時的に使用禁止にする方法またはすべて削除する方法については、44-6 ページの「変更サブスクリプション・オブジェクトの無効化と削除」を参照してください。

同期のプロセス

この項では、次の項目について説明します。

- 接続ディレクトリによって、最初に Oracle Internet Directory から変更を取得する方法
- 接続ディレクトリによって、Oracle Internet Directory 内の orclLastAppliedChangeNumber 属性を更新する方法

接続ディレクトリによって、最初に Oracle Internet Directory から変更を取得する方法

次の例では、my_change_subscription_object という名前の変更サブスクリプション・オブジェクトを持つ接続ディレクトリが Oracle Internet Directory から変更を取得します。

```
ldapsearch -h my_host -p 389 -b "cn=changeLog" -s one
(&(objectclass=changeLogEntry)
(changeNumber >= orclLastAppliedChangeNumber )
( ! (modifiersname =cn=my_change_subscription_object,cn=Subscriber Profile,
     cn=ChangeLog Subscriber,cn=Oracle Internet Directory ) ) )
```

最初にディレクトリが変更を取得する場合、orclLastAppliedChangeNumber の値は、44-3 ページの「タスク 2: Oracle Internet Directory でのサード・パーティのメタディレクトリ・ソリューション用変更サブスクリプション・オブジェクトの作成」で設定した値です。

フィルタ内の引数（(modifiersname=*client_bind_dn*)）によって、Oracle Internet Directory は、接続ディレクトリ自体が行った変更を戻しません。

接続ディレクトリによって、Oracle Internet Directory 内の orclLastAppliedChangeNumber 属性を更新する方法

Oracle Internet Directory から変更を取得した後、接続ディレクトリは、Oracle Internet Directory 内の対応する変更サブスクリプション・オブジェクトの orclLastAppliedChangeNumber 属性を更新します。この更新によって、Oracle Internet Directory は、接続ディレクトリがすでに適用した変更をパージできます。また、この更新によって、接続ディレクトリは、適用済の変更を無視して最新の変更のみを取得できます。

次の例は、接続ディレクトリに my_change_subscription_object という名前の変更サブスクリプション・オブジェクトがあり、前回適用した変更番号が 121 の入力ファイル mod.ldif を使用します。この接続ディレクトリは、Oracle Internet Directory 内の対応する変更サブスクリプション・オブジェクトの orclLastAppliedChangeNumber を更新します。

1. mod.ldif ファイルの編集:

```
dn: cn=my_change_subscription_object,cn=Subscriber Profile,
    cn=ChangeLog Subscriber,cn=Oracle Internet Directory
changetype:modify
replace: orclLastAppliedChangeNumber
orclLastAppliedChangeNumber: 121
```

2. ldapmodify を使用した編集済 mod.ldif ファイルのロード:

```
ldapmodify -h host -p port -f mod.ldif
```

関連項目: 変更番号に従って変更をパージする方法は、22-7 ページの「マルチマスター・レプリケーションの変更ログの削除」を参照してください。

変更サブスクリプション・オブジェクトの無効化と削除

既存の変更サブスクリプション・オブジェクトは、一時的に使用禁止にしたり、すべて削除することができます。この項では、次の項目について説明します。

- 変更サブスクリプション・オブジェクトの無効化
- 変更サブスクリプション・オブジェクトの削除

変更サブスクリプション・オブジェクトの無効化

サード・パーティのメタディレクトリ・ソリューションにある既存の変更サブスクリプション・オブジェクトを一時的に使用禁止にする場合は、orclSubscriberDisable 属性を 1 に設定します。次の例では、入力ファイル mod.ldif を使用して、変更サブスクリプション・オブジェクトを使用禁止にします。

- mod.ldif ファイルの編集:

```
dn: cn=my_change_subscription_object,cn=Subscriber Profile,
    cn=ChangeLog Subscriber,cn=Oracle Internet Directory
changetype: modify
replace: orclSubscriberDisable
orclSubscriberDisable: 1
```

- エントリの変更:

```
ldapmodify -h my_ldap_host -p 389 -v -f mod.ldif
```

変更サブスクリプション・オブジェクトの削除

変更サブスクリプション・オブジェクトの削除には、ldapdelete を使用します。次のコマンドを入力します。

```
ldapdelete -h ldap_host -p ldap_port
           "cn=my_change_subscription_object,cn=Subscriber Profile,
            cn=ChangeLog Subscriber,cn=Oracle Internet Directory"
```

第 VIII 部

ディレクトリ・プラグイン

第 VIII 部は次の章で構成されています。

45

Oracle Internet Directory プラグイン・フレームワーク

この章では、オラクル社またはサード・パーティ・ベンダーが開発したプラグインを使用して、Oracle ディレクトリ・サーバーの機能を拡張する方法について説明します。

この章では、次の項目について説明します。

> **関連項目：**『Oracle Internet Directory アプリケーション開発者ガイド』の Oracle Internet Directory サーバーのプラグイン・フレームワークに関する章を参照してください。

ディレクトリ・サーバー・プラグインの概要

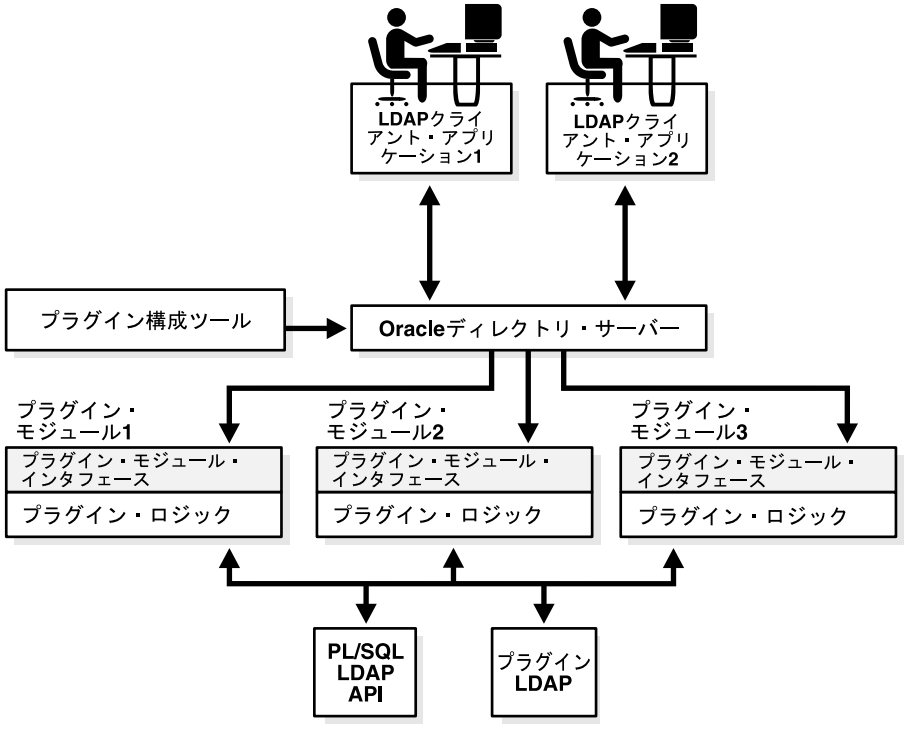
ディレクトリ・サーバーのプラグインは、次のような機能をディレクトリ・サーバーに追加します。

- ディレクトリ・サーバーによる操作実行前のデータの妥当性チェック
- サーバーによる操作実行後の指定処理の実行
- パスワード・ポリシーの定義
- 外部に格納された資格証明によるユーザーの認証

起動時に、ディレクトリ・サーバーはプラグイン構成およびライブラリをロードします。その後、要求を処理するときに、指定されたイベントが発生した場合は常に、プラグイン・ファンクションをコールします。

45-3 ページの図 45-1 に、LDAP クライアントが個々のアプリケーションを使用して行う、Oracle ディレクトリ・サーバーとの間の情報の送受信について示します。同様に、プラグイン構成ツールもディレクトリ・サーバーに情報を送信します。ディレクトリ・サーバーはデータをプラグイン・モジュール 1、プラグイン・モジュール 2 およびプラグイン・モジュール 3 に送信します。各プラグイン・モジュールはプラグイン・モジュール・インタフェースとプラグイン・ロジックを備えています。各プラグイン・モジュールは、PL/SQL LDAP API およびプラグイン LDAP との間の情報の送受信を行います。

図 45-1 Oracle Internet Directory のプラグイン・フレームワーク



プラグインの動作は、通常のディレクトリ・サーバー操作の前後に実行するか、または追加として実行するかによって異なります。表 45-1 に、操作ベースの様々なプラグインについて説明します。

表 45-1 操作ベースのプラグインのタイプ

プラグインのタイプ	説明
操作前	ディレクトリ・サーバーが LDAP 操作を実行する前にコールするプラグイン。一般的にこれらのプラグインは、LDAP 操作でデータを使用する前に、そのデータの妥当性をチェックします。妥当性チェックに失敗した場合、ディレクトリ・サーバーはプラグインから戻されるエラーまたは警告に従って、LDAP 操作を続行するかどうかを判断します。ただし、関連付けられている LDAP 要求が後で失敗した場合、Oracle Internet Directory は、プラグインによってコミット済の内容をロールバックしません。

表 45-1 操作ベースのプラグインのタイプ（続き）

プラグインのタイプ	説明
操作後	ディレクトリ・サーバーが LDAP 操作を実行した後にコールするプラグイン。一般的にこれらのプラグインは、ディレクトリ・サーバーが特定の操作を実行した場合に、ロギングまたは通知などのファンクションを起動します。プラグインの実行が失敗した場合、ディレクトリ・サーバーは関連付けられている LDAP 操作をロールバックしません。プラグインは、関連付けられている LDAP 操作が失敗したかどうかに関係なく実行されます。
操作時	標準的な処理に加えてディレクトリ・サーバーがコールするプラグイン。一般的に、これらのプラグインは既存の機能を補強するもので、対応する LDAP 操作と同じトランザクション内で付加的な操作を実行します。LDAP 操作またはプラグインが失敗すると、ディレクトリ・サーバーは変更をロールバックします。 操作時プラグインには、アドオンと置換の 2 種類があります。 アドオン・プラグインは、ldapadd、ldapdelete および ldapmodify 操作を実行できます。 置換プラグインは、ldapcompare、ldapbind および ldapmodify 操作を実行できます。 たとえば、ldapcompare 操作の場合は操作時アドオン・タイプのプラグインを使用できます。Oracle Internet Directory サーバーはサーバー比較コードを実行し、プラグイン開発者が定義したプラグイン・モジュールを実行します。置換タイプのプラグインの場合、Oracle Internet Directory は独自の比較コードを実行しません。かわりに、プラグイン・モジュールに基づいて比較を実行し、比較結果を戻します。サーバー比較プロシージャは、プラグイン・モジュールによって置き換えられます。

プラグインの登録と管理

ディレクトリ・サーバーが適時にプラグインをコールできるように、プラグインをディレクトリ・サーバーに登録する必要があります。登録するには、プラグインの構成エントリを `cn=plugin,cn=subconfigsubentry` に作成します。このプラグインには、そのオブジェクト・クラスの 1 つとして `orclPluginConfig` が必要です。

> **関連項目：** `orclPluginConfig` オブジェクト・クラスの属性の詳細は、B-31 ページの「プラグインのスキーマ要素」を参照してください。

この項では、次の項目について説明します。

- Oracle Directory Manager を使用したプラグインの登録と管理
- コマンドライン・ツールを使用したプラグインの登録と管理

Oracle Directory Manager を使用したプラグインの登録と管理

この項では、Oracle Directory Manager を使用してプラグイン構成エントリを作成、変更および削除する例を示します。

Oracle Directory Manager によるプラグイン構成エントリの追加

プラグインを登録する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開します。
2. 「**プラグイン管理**」を選択します。右側のペインに「プラグイン管理」ウィンドウが表示されます。
3. 「**作成**」を選択します。「新規プラグイン」ダイアログ・ボックスが表示されます。
4. 「新規プラグイン」ダイアログ・ボックスのフィールドに値を入力します。これらのフィールドの説明は、C-9 ページの表 C-13 を参照してください。
5. 値を入力した後、「**OK**」を選択します。「プラグイン管理」ウィンドウに戻ります。作成したプラグインが「プラグイン・エントリ名」列に表示さます。
6. 「**OK**」を選択します。

Oracle Directory Manager によるプラグインの編集

プラグイン・エントリを編集する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開します。
2. 「**プラグイン管理**」を選択します。右側のペインに「プラグイン管理」ウィンドウが表示されます。
3. 右側のペインで、編集するプラグイン・エントリの名前を選択し、「**編集**」を選択します。「プラグイン :」ダイアログ・ボックスが表示されます。
4. 「プラグイン :」ダイアログ・ボックスで、適切なフィールドの値を編集します。これらのフィールドの説明は、C-9 ページの表 C-13 を参照してください。
5. 「**OK**」を選択します。

Oracle Directory Manager によるプラグインの削除

プラグインを削除する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、**ディレクトリ・サーバー・インスタンス**の順に展開します。
2. 「**プラグイン管理**」を選択します。右側のペインに「プラグイン管理」ウィンドウが表示されます。
3. 右側のペインで、削除するプラグイン・エントリの名前を選択し、「**編集**」を選択します。「プラグイン :」ダイアログ・ボックスが表示されます。
4. 「プラグイン」ダイアログ・ボックスで、「**削除**」を選択します。プロンプトに従って削除を確認します。「プラグイン管理」ウィンドウに戻ります。削除したプラグイン・エントリは、リストに表示されなくなります。

コマンドライン・ツールを使用したプラグインの登録と管理

この項では、コマンドライン・ツールを使用してプラグイン構成エントリを作成、変更および削除する例を示します。

> **関連項目：** orclPluginConfig オブジェクト・クラスの属性の詳細は、「プラグインのスキーマ要素」を参照してください。

例 : コマンドライン・ツールによるプラグイン構成エントリの追加

次の例では、`my_plugin1` と呼ばれる操作ベースのプラグインのエントリが作成されます。LDIF ファイルの名前は、`my_ldif_file.ldif` です。

例 1: 比較操作用の操作ベースのプラグイン・エントリの作成 次に、オブジェクトを作成する LDIF ファイルの例を示します。

```
cn=when_comp,cn=plugin,cn=subconfigsubentry
objectclass=orclPluginConfig
objectclass=top
orclPluginName=my_plugin1
orclPluginType=operational
orclPluginTiming=when
orclPluginLDAPOperation=ldapcompare
orclPluginEnable=1
orclPluginVersion=1.0.1
orclPluginIsReplace=1
cn=when_comp
orclPluginKind=PLSQL
orclPluginSubscriberDNList=dc=COM,c=us;dc=us,dc=oracle,dc=com;dc=org,dc=us;
o=IMC,c=US
```

例 2: 変更操作用の操作ベースのプラグイン・エントリの作成 次に、オブジェクトを作成する LDIF ファイルの例を示します。

```
cn=post_mod_plugin,cn=plugin,cn=subconfigsubentry
objectclass=orclPluginConfig
objectclass=top
orclPluginName=my_plugin1
orclPluginType=operational
orclPluginTiming=post
orclPluginLDAPOperation=ldapmodify
orclPluginEnable=1
orclPluginVersion=1.0.1
cn=post_mod_plugin
orclPluginKind=PLSQL
```

次のコマンドを使用して、このファイルをディレクトリに追加します。

```
ldapadd -p 389 -h myhost -D binddn -w password -f my_ldif_file.ldif
```

このエントリをディレクトリに追加すると、ディレクトリ・サーバーはただちにその内容を実行し、コンパイルまたはアクセス権限のエラーをチェックして、そのプラグインを検証します。次に、プラグインに関係する LDAP 操作のタイミングやタイプなど、このプラグインに関する詳細な情報を収集します。

注意： プラグイン構成エントリ（cn=plugin,cn=subconfigsubentry などのメタデータ）は、一貫性のない状態になるのを回避するために、レプリケーション環境ではレプリケートされません。

例 : コマンドライン・ツールによるプラグイン構成エントリの変更

次に、プラグインを無効にする例を示します。

```
ldapmodify -h  host_name -p  port_number -D cn=orcladmin -w orcladminpwd <<EOF
dn: cn=post_mod_plugin,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclPluginEnable
orclPluginEnable: 0
EOF
```

例 : コマンドライン・ツールによるプラグイン構成エントリの削除

次に、プラグインを削除する例を示します。

```
ldapdelete -h  host_name -p port_number -D cn=orcladmin -w orcladminpwd
"cn=post_mod_plugin,cn=plugin,cn=subconfigsubentry"
```

46

Oracle Internet Directory のパスワード・ポリシー・プラグイン

Oracle Internet Directory は、プラグインを使用して、パスワード値のチェックを他のパスワード・ポリシー管理機能に追加します。このプラグインを使用すると、追加または変更されたパスワードが、指定された最小文字数以上であるかどうかなどを確認できます。個別の要件に合わせて、パスワード値チェックをカスタマイズできます。

この章では、次の項目について説明します。

パスワード・ポリシー・プラグインの動作

パスワードを追加または変更する場合、カスタマイズされたパスワード値チェックが次のように処理されます。

1. クライアントが、ldapadd 要求または ldapmodify 要求をディレクトリ・サーバーに送信します。
2. ディレクトリ・サーバーは、追加または変更を行う前にパスワード値をプラグインに渡します。
3. プラグインは次のように動作します。
   a. エントリを解析
   b. クリア・テキストの userpassword 属性値を取得
   c. 指定したパスワード値チェックを実施
4. パスワードが指定と一致する場合は、そのことがプラグインによってディレクトリ・サーバーに通知され、ディレクトリ・サーバーによって追加または変更が行われます。一致しない場合は、次のいずれかのエラー・メッセージがプラグインによってディレクトリ・サーバーに送信され、その後、ディレクトリ・サーバーからクライアントに渡されます。

   ```
   ldap_add: UnKnown Error Encountered
   ldap_add: additional info: PASSWORD POLICY VIOLATION:0000X, less than 8 chars

   ldap_add: UnKnown Error Encountered
   ldap_add: additional info: PASSWORD POLICY VIOLATION:0000X, contains dictionary
   word
   ```

   同じロジックが PRE ldapmodify プラグインにも適用されます。

パスワード・ポリシー・プラグインが実行できる値チェックには、次のような種類があります。

- アルファベットの最大および最小文字数
- 数字の最大文字数
- 記号の最大および最小文字数
- 連続した文字の最大文字数
- 任意の文字の最大インスタンス数

例 : カスタマイズされたパスワード・ポリシー・プラグインのインストール、構成および有効化

この例は、PL/SQL プログラム pluginpkg.sql（46-5 ページの「サンプル PL/SQL パッケージ pluginpkg.sql の内容」を参照）を使用しています。通常、このパッケージには次のものが含まれます。

- プラグイン・モジュール pre_add および pre_modify
- パスワードが最小文字数要件の 8 文字を満たしていることを確認する値チェック・ファンクション isGoodPwd

この例では、ユーザーが 8 文字未満の userpassword 値を入力すると、要求は拒否されます。同様に、ユーザー・パスワードを変更する際に、新しいパスワード値が 8 文字未満の場合は要求が拒否されます。

この項では、次の項目について説明します。

- PL/SQL プログラムのロードおよび登録
- パスワード・ポリシー・プラグインのコード化
- パスワード・ポリシー・プラグインのデバッグ
- サンプル PL/SQL パッケージ pluginpkg.sql の内容

PL/SQL プログラムのロードおよび登録

スタンドアロンの値チェック PL/SQL プログラムを実装した場合は、次の手順を実行します。

1. プラグイン・パッケージをデータベースにロードします。この例では、次のように入力します。

   ```
   sqlplus ods/odspwd @pluginpkg.sql
   ```

2. プラグインを登録します。この例では、次の内容のファイル pluginreg.dat を使用します。

   ```
   ### add plugin ###
   dn: cn=pre_add_plugin,cn=plugin,cn=subconfigsubentry
   objectclass:orclPluginConfig
   objectclass:top
   orclpluginname:pwd_plugin
   orclplugintype:operational
   orclplugintiming:pre
   orclpluginldapoperation:ldapadd
   orclpluginenable:1
   orclpluginversion:1.0.1
   cn:pre_add_plugin
   ```

```
orclpluginsubscriberdnlist:dc=com;o=IMC ,c=US
orclpluginattributelist:userpassword

### modify plugin ###
dn: cn=pre_mod_plugin,cn=plugin,cn=subconfigsubentry
objectclass:orclPluginConfig
objectclass:top
orclpluginname:pwd_plugin
orclplugintype:operational
orclplugintiming:pre
orclpluginldapoperation:ldapmodify
orclpluginenable:1
orclpluginversion:1.0.1
cn:pre_mod_plugin
orclpluginsubscriberdnlist:dc=com;o=IMC ,c=US
orclpluginattributelist:userpassword
```

このプラグインでは、ldapadd 要求または ldapmodify 要求を受け取った際に起動する 2 つのプラグイン・モジュールをディレクトリ・サーバーに認識させています。ターゲット・エントリが dc=com または o=IMC、c=US 下の場合のみプラグインが起動するように、orclpluginsubscriberdnlist:dc=com;o=IMC,c=US を使用しています。

このファイルをディレクトリに追加するには、次のとおり入力します。

```
ldapadd -p portnum -h hostname -D cn=orcladmin -w orcladminpwd -v -f
pluginreg.dat
```

パスワード・ポリシー・プラグインのコード化

標準 PL/SQL 文字ファンクションを使用して、パスワード値を処理できます。正規表現を行う PL/SQL プログラムをダウンロードします。値チェック・ファンクションとプラグイン・モジュールを統合することが重要です。

パスワード・ポリシー・プラグインのデバッグ

ディレクトリ・サーバー・プラグインを設定すると、プラグインのプロセスと内容を調べることができます。

ディレクトリ・サーバー・プラグインのデバッグを設定するには、次のコマンドを実行します。

```
sqlplus ods/password @$ORACLE/ldap/admin/oidspdsu.pls
```

ディレクトリ・サーバー・プラグインのデバッグを有効にするには、次のコマンドを実行します。

```
sqlplus ods/password @$ORACLE/ldap/admin/oidspdon.pls
```

ディレクトリ・サーバー・プラグインのデバッグを無効にするには、次のコマンドを実行します。

```
sqlplus ods/password @$ORACLE/ldap/admin/oidspdof.pls
```

ディレクトリ・サーバー・プラグインのデバッグ・メッセージを表示するには、次のコマンドを実行します。

```
sqlplus ods/password @$ORACLE/ldap/admin/oidspdsh.pls
```

ディレクトリ・サーバー・プラグインのデバッグ・メッセージを削除するには、次のコマンドを実行します。

```
sqlplus ods/password @$ORACLE/ldap/admin/oidspdde.pls
```

サンプル PL/SQL パッケージ pluginpkg.sql の内容

この例で使用するスクリプト `pluginpkg.sql` の内容は次のとおりです。

```
CREATE OR REPLACE PACKAGE pwd_plugin AS

PROCEDURE pre_add (ldapplugincontext IN  ODS.plugincontext,
   dn       IN  VARCHAR2,
   entry    IN  ODS.entryobj,
   rc       OUT INTEGER,
   errormsg OUT VARCHAR2
   );

PROCEDURE pre_modify (ldapplugincontext IN  ODS.plugincontext,
      dn       IN  VARCHAR2,
      mods     IN  ODS.modlist,
      rc       OUT INTEGER,
      errormsg OUT VARCHAR2
      );

-- Function: isGoodPwd
-- Parameter: inpwd
-- Purpose: simple password validation function
--          if the password is less than 8 chars
--          this function will return 0, indicating that
--          it is not a good password
```

```
FUNCTION isGoodPwd(inpwd IN VARCHAR2)
  RETURN INTEGER;


END pwd_plugin;
/

show error

CREATE OR REPLACE PACKAGE BODY pwd_plugin AS

FUNCTION isGoodPwd(inpwd IN VARCHAR2)
  RETURN INTEGER
  IS
     i NUMBER;
     ret NUMBER DEFAULT 1;
     minpwdlen NUMBER DEFAULT 8;
     len       NUMBER DEFAULT 0;
BEGIN
   plg_debug( '=== begin of ISGOODPWD ===');
   plg_debug( 'password = ' || inpwd);
   len := LENGTH(inpwd);
   plg_debug( 'password length = ' || len);

   IF len < minpwdlen THEN
      RETURN 0;
    ELSE
      RETURN ret;
   END IF;

   plg_debug( '=== end of ISGOODPWD ===');

EXCEPTION
   WHEN OTHERS THEN
      plg_debug( 'Exception in isGoodPwd(). Error code is ' || TO_CHAR(SQLCODE));
      plg_debug( '   ' || Sqlerrm);
      RETURN 0;
END;


PROCEDURE pre_add (ldapplugincontext IN  ODS.plugincontext,
   dn       IN  VARCHAR2,
   entry    IN  ODS.entryobj,
   rc       OUT INTEGER,
   errormsg OUT VARCHAR2
   )
```

```
  IS
     inpwd VARCHAR2(256) DEFAULT NULL;
     ret   NUMBER        DEFAULT 1;
BEGIN
   plg_debug( '=== begin of PRE_ADD_PLUGIN ===');
   plg_debug( 'dn = ' || dn);

   plg_debug( 'entry obj ' || ':entryname = ' || entry.entryname);

   FOR l_counter1 IN 1..entry.attr.COUNT LOOP
      plg_debug( 'attrname[' || l_counter1 || '] = ' ||
 entry.attr(l_counter1).attrname);
      FOR l_counter2 IN 1..entry.attr(l_counter1).attrval.COUNT LOOP
 plg_debug( entry.attr(l_counter1).attrname ||
    '[' || l_counter1 || ']' ||
    '.val[' || l_counter2 || '] = ' ||
    entry.attr(l_counter1).attrval(l_counter2));
      END LOOP;

      IF entry.attr(l_counter1).attrname = 'userpassword' THEN
 inpwd := entry.attr(l_counter1).attrval(1);
 -- assuming only one attr val for userpassword
      END IF;

   END LOOP;

   IF (inpwd IS NOT NULL) THEN
      ret := isGoodPwd(inpwd);
   END IF;

   IF (inpwd IS NULL OR ret = 0) THEN
      rc := 1;
      errormsg := 'PASSWORD POLICY VIOLATION:0000X, less than 8 chars';
      plg_debug( ' we got an invalid password ');
    ELSE
      plg_debug( ' we got a good password ');
      rc := 0;
      errormsg := 'no pre_mod plguin error msg';
   END IF;

   plg_debug( '=== end of PRE_ADD_PLUGIN ===');

EXCEPTION
   WHEN OTHERS THEN
      plg_debug( 'Exception in PRE_ADD plugin. Error code is ' || TO_CHAR(SQLCODE));
      plg_debug( '   ' || Sqlerrm);
      rc := 1;
```

```
      errormsg := 'exception: pre_add plguin';
END;

PROCEDURE pre_modify (ldapplugincontext IN  ODS.plugincontext,
      dn       IN  VARCHAR2,
      mods     IN  ODS.modlist,
      rc       OUT INTEGER,
      errormsg OUT VARCHAR2
      )
  IS
     old_passwd VARCHAR2(256) DEFAULT NULL;
     new_passwd VARCHAR2(256) DEFAULT NULL;
     ret        NUMBER        DEFAULT 1;

BEGIN
   plg_debug( '=== begin of PRE_MOD_PLUGIN ===');
   plg_debug( dn);

   FOR l_counter1 IN 1..mods.COUNT LOOP
      IF (mods(l_counter1).operation = 2) AND(mods(l_counter1).type  'userpassword')
THEN

 FOR l_counter2 IN 1..mods(l_counter1).vals.COUNT LOOP
    new_passwd := mods(l_counter1).vals(l_counter2).val;
 END LOOP;
      END IF;

      IF (mods(l_counter1).operation = 0) AND
(mods(l_counter1).type = 'userpassword') THEN

 FOR l_counter2 IN 1..mods(l_counter1).vals.COUNT LOOP
    new_passwd := mods(l_counter1).vals(l_counter2).val;
 END LOOP;
      END IF;

      IF (mods(l_counter1).operation = 1) AND
(mods(l_counter1).type = 'userpassword') THEN

 FOR l_counter2 IN 1..mods(l_counter1).vals.COUNT LOOP
    old_passwd := mods(l_counter1).vals(l_counter2).val;
 END LOOP;
      END IF;
   END LOOP;

   plg_debug(' new password: ' || new_passwd);
   plg_debug(' old password: ' || old_passwd);
```

```
   IF (new_passwd IS NOT NULL) THEN
      ret := isGoodPwd(new_passwd);
   END IF;

   IF (new_passwd IS NULL OR ret = 0) THEN
      rc := 1;
      errormsg := 'PASSWORD POLICY VIOLATION:0000X, less than 8 chars';
      plg_debug( ' we got an invalid password ');
    ELSE
      plg_debug( ' we got a good password ');
      rc := 0;
      errormsg := 'no pre_mod plguin error msg';
   END IF;

   plg_debug( '=== end of PRE_MOD_PLUGIN ===');

EXCEPTION
   WHEN OTHERS THEN
      plg_debug( 'Exception in PRE_MODIFY plugin. Error code is ' || TO_
CHAR(SQLCODE));
      plg_debug( '   ' || Sqlerrm);
      rc := 1;
      errormsg := 'exception: pre_mod plguin';
END;

END pwd_plugin;
/
show error

GRANT EXECUTE ON pwd_plugin TO ods_server;

EXIT;
```

47

カスタマイズされた外部認証プラグインの設定

ユーザー・セキュリティ資格証明を Oracle Internet Directory 以外のリポジトリ（データベースや他の LDAP ディレクトリなど）に格納し、Oracle コンポーネントに対するユーザー認証に使用できます。資格証明を Oracle Internet Directory に格納し、同期させておく必要はありません。外部リポジトリに格納された資格証明によるユーザー認証を、外部認証と呼びます。

この章では、次の項目について説明します。

- ネイティブ認証と外部認証との対比
- 例 : 外部認証プラグインのインストール、構成および有効化

ネイティブ認証と外部認証との対比

Oracle Internet Directory に格納されたセキュリティ資格証明に基づく認証を、ネイティブ認証と呼びます。ユーザーがセキュリティ資格証明を入力すると、ディレクトリ・サーバーは Oracle Internet Directory に格納されている資格証明とそれを比較します。資格証明が一致すると、ディレクトリ・サーバーはユーザーを認証します。

Oracle Internet Directory 以外のディレクトリに格納されたセキュリティ資格証明に基づく認証を、外部認証と呼びます。ユーザーがセキュリティ資格証明を入力すると、ディレクトリ・サーバーは他のディレクトリに格納されている資格証明とそれを比較します。この比較は次のものを使用して行われます。

- 外部認証作業を行う PL/SQL プログラム
- この PL/SQL プログラムを起動する外部認証プラグイン

例 : 外部認証プラグインのインストール、構成および有効化

この項では、次の項目について説明します。

サンプル PL/SQL パッケージ oidexaup.sql

この例は、PL/SQL プログラム `oidexaup.sql`（47-5 ページの「PL/SQL パッケージ oidexaup.sql の内容」を参照）を使用しています。このパッケージは、外部認証プラグイン PL/SQL パッケージをインストールするために使用します。このパッケージには、2 つのプラグイン `when_compare_replace`、`when_modify_replace` およびユーティリティ・ファンクション `get_nickname` が含まれています。統合パッケージは、プラグイン・パッケージ `OIDEXTAUTH` です。このパッケージは、配置環境に合わせて変更できるテンプレートとしても使用できます。

外部認証プラグインをインストールおよび構成し、有効にする手順は、次のとおりです。

1. スタンドアロンの外部認証 PL/SQL プログラムを実装します。たとえば、ユーザー名とパスワードで認証する場合は、この 2 つのパラメータを取る PL/SQL プログラムを使用する必要があります。

   サンプル・コードでは、`oidexaup.sql`、`auth_external` はプログラム・パッケージ名で、`authenticate_user` は認証を行うファンクションです。スタンドアロンのプログラムが適切に動作していることを確認してから、次の手順に進んでください。

2. スタンドアロンのプログラムをプラグイン・モジュールに登録します。

3. プラグイン・パッケージをデータベースにロードします。この例では、次のように入力します。

```
sqlplus ods/odspwd @oidexaup.sql
```

4. プラグインを登録します。プラグインの起動に必要な情報をディレクトリ・サーバーに提供する LDIF ファイルを作成し、アップロードすることにより登録します。

5. この例では、次の内容のファイル oidexauth.ldif を使用します。

```
dn: cn=whencompare,cn=plugin,cn=subconfigsubentry
objectclass:orclPluginConfig
objectclass:top
orclpluginname:oidextauth
orclplugintype:operational
orclplugintiming:when
orclpluginldapoperation:ldapcompare
orclpluginenable:1
orclpluginversion:1.0.1
orclPluginIsReplace:1
cn:whencompare
orclpluginsubscriberdnlist:dc=com;o=IMC,c=US
orclpluginattributelist:userpassword
orclpluginrequestgroup:$prgdn

dn: cn=whenmodify,cn=plugin,cn=subconfigsubentry
objectclass:orclPluginConfig
objectclass:top
orclpluginname:oidextauth
orclplugintype:operational
orclplugintiming:when
orclpluginldapoperation:ldapmodify
orclpluginenable:1
orclpluginversion:1.0.1
orclPluginIsReplace:1
cn:whenmodify
orclpluginsubscriberdnlist:dc=com;o=IMC,c=US
orclpluginattributelist:userpassword
orclpluginrequestgroup:$prgdn
```

このファイルでは、ldapcompare 要求または ldapmodify 要求があった際に 2 つのプラグインが起動することをディレクトリ・サーバーに通知します。

ターゲット・エントリが dc=com または o=IMC、c=US 下の場合のみプラグインが起動するように、orclpluginsubscriberdnlist:dc=com;o=IMC,c=US を使用しています。

$prgdn を、プラグイン要求グループ識別名に置換します。これはオプションの推奨セキュリティ機能です。Oracle Application Server Single Sign-On との統合には、この値が必須フィールドです。入力されたグループのメンバーのみがプラグインを起動できます。複数のグループの入力が可能です。エントリを区切るには、セミコロンを使用します。

推奨デフォルトは、cn=OracleUserSecurityAdmins,cn=Groups,cn=OracleContext および cn=OracleDASAdminGroup,cn=Groups,cn=OracleContext, o=default_subscriber,dc=com です。Oracle Application Server Single Sign-On Server は、最初のグループのメンバーです。また、配置環境に合わせて o=default_subscriber を正しい値に置換してください。

このファイルをディレクトリに追加するには、次のとおり入力します。

```
ldapadd -p portnum -h hostname -D cn=orcladmin -w orcladminpwd -v -f
oidexauth.ldif
```

これで、すべての準備が完了しました。ldapcompare コマンドライン・ツールを使用すると、Oracle Application Server Single Sign-On からユーザーを認証する前にプラグインおよび認証プログラムが適切に動作していることを確認できます。

この例では、ユーザー・パスワードを外部変更するためのプラグイン・コードも提供されています。

外部認証プラグインのデバッグ

ディレクトリ・サーバー・プラグインを設定すると、プラグインのプロセスと内容を調べることができます。

ディレクトリ・サーバー・プラグインのデバッグを設定するには、次のコマンドを実行します。

```
sqlplus ods/password @$ORACLE/ldap/admin/oidspdsu.sql
```

ディレクトリ・サーバー・プラグインのデバッグを有効にするには、次のコマンドを実行します。

```
sqlplus ods/password @$ORACLE/ldap/admin/oidspdon.sql
```

ディレクトリ・サーバー・プラグインのデバッグを無効にするには、次のコマンドを実行します。

```
sqlplus ods/password @$ORACLE/ldap/admin/oidspdof.sql
```

ディレクトリ・サーバー・プラグインのデバッグ・メッセージを表示するには、次のコマンドを実行します。

```
sqlplus ods/password @$ORACLE/ldap/admin/oidspdsh.sql
```

ディレクトリ・サーバー・プラグインのデバッグ・メッセージを削除するには、次のコマンドを実行します。

```
sqlplus ods/password @$ORACLE/ldap/admin/oidspdde.sql
```

PL/SQL パッケージ oidexaup.sql の内容

この例で使用するスクリプト oidexaup.sql の内容は次のとおりです。

```
CREATE OR REPLACE PACKAGE OIDEXTAUTH AS

  PROCEDURE when_compare_replace (ldapplugincontext IN  ODS.plugincontext,
                                  result             OUT INTEGER,
                                  dn                 IN  VARCHAR2,
                                  attrname           IN  VARCHAR2,
                                  attrval            IN  VARCHAR2,
                                  rc                 OUT INTEGER,
                                  errormsg           OUT VARCHAR2
                                  );

  PROCEDURE when_modify_replace (ldapplugincontext IN  ODS.plugincontext,
                                 dn                IN  VARCHAR2,
                                 mods              IN  ODS.modlist,
                                 rc                OUT INTEGER,
                                 errormsg          OUT VARCHAR2
                                 );

  FUNCTION get_nickname (dn         IN  VARCHAR2,
                         my_session IN  DBMS_LDAP.session)
    RETURN VARCHAR2;

END OIDEXTAUTH;
/

SHOW ERROR

CREATE OR REPLACE PACKAGE BODY OIDEXTAUTH AS

  -- We use this function to convert the dn to nickname.
  -- When OID server receives the ldapcompare request, it
  -- only has the dn information. We need to use DBMS_LDAP_UTL
  -- package to find out the nickname attribute value of
  -- the entry.
```

```
FUNCTION get_nickname (dn         IN VARCHAR2,
                       my_session IN DBMS_LDAP.session)
  RETURN VARCHAR2
  IS
     my_pset_coll        DBMS_LDAP_UTL.PROPERTY_SET_COLLECTION;
     my_property_names   DBMS_LDAP.STRING_COLLECTION;
     my_property_values  DBMS_LDAP.STRING_COLLECTION;

     user_handle         DBMS_LDAP_UTL.HANDLE;
     user_id             VARCHAR2(2000);
     user_type           PLS_INTEGER;
     user_nickname       VARCHAR2(256) DEFAULT NULL;

     my_attrs            DBMS_LDAP.STRING_COLLECTION;
     retval              PLS_INTEGER;

BEGIN
   plg_debug( '=== Beginning of get_nickname() === ');
   user_type     := DBMS_LDAP_UTL.TYPE_DN;
   user_id       := dn;

   retval := DBMS_LDAP_UTL.create_user_handle(user_handle, user_type, user_id);

   plg_debug( 'create_user_handle() Returns ' || To_char(retval));

   retval := DBMS_LDAP_UTL.get_user_properties(my_session,
                                               user_handle,
                                               my_attrs,
                                               DBMS_LDAP_UTL.NICKNAME_PROPERTY,
                                               my_pset_coll);

   plg_debug( 'get_user_properties() Returns ' || To_char(retval));

   IF my_pset_coll.COUNT > 0 THEN
      FOR i IN my_pset_coll.first .. my_pset_coll.last LOOP
         retval := DBMS_LDAP_UTL.get_property_names(my_pset_coll(i),
                                                    my_property_names);
         IF my_property_names.COUNT > 0 THEN
            FOR j IN my_property_names.first .. my_property_names.last LOOP
               retval := DBMS_LDAP_UTL.get_property_values(my_pset_coll(i),
                                                           my_property_names(j),
                                                           my_property_values);
               IF my_property_values.COUNT > 0 THEN
                  FOR k IN my_property_values.FIRST..my_property_values.LAST LOOP
                     user_nickname := my_property_values(k);
                     plg_debug( 'user nickname = ' || user_nickname);
```

```
                END LOOP;
              END IF;
            END LOOP;
          END IF; -- IF my_property_names.count > 0
        END LOOP;
    END IF; -- If my_pset_coll.count > 0

    plg_debug( 'got user_nickname: ' || user_nickname);

    -- Free my_properties
    IF my_pset_coll.count > 0 then
       DBMS_LDAP_UTL.free_propertyset_collection(my_pset_coll);
    END IF;

    DBMS_LDAP_UTL.free_handle(user_handle);

    RETURN user_nickname;

EXCEPTION
    WHEN OTHERS THEN
       plg_debug('Exception in get_nickname. Error code is ' || to_char(sqlcode));
       plg_debug('   ' || Sqlerrm);
       RETURN NULL;
END;


PROCEDURE when_compare_replace (ldapplugincontext IN  ODS.plugincontext,
                                result            OUT INTEGER,
                                dn                IN  VARCHAR2,
                                attrname          IN  VARCHAR2,
                                attrval           IN  VARCHAR2,
                                rc                OUT INTEGER,
                                errormsg          OUT VARCHAR2
                                )
  IS
     retval pls_integer;
     lresult BOOLEAN;

     my_session          DBMS_LDAP.session;
     my_property_names   DBMS_LDAP.STRING_COLLECTION;
     my_property_values  DBMS_LDAP.STRING_COLLECTION;
     my_attrs            DBMS_LDAP.STRING_COLLECTION;
     my_pset_coll        DBMS_LDAP_UTL.PROPERTY_SET_COLLECTION;
     user_handle         DBMS_LDAP_UTL.HANDLE;

     user_id             VARCHAR2(2000);
     user_type           PLS_INTEGER;
```

```
    user_nickname       VARCHAR2(60);
    remote_dn           VARCHAR2(256);

    i                   PLS_INTEGER;
    j                   PLS_INTEGER;
    k                   PLS_INTEGER;

BEGIN
   plg_debug( '=== Begin of WHEN-COMPARE-REPLACE plug-in');
   plg_debug( 'DN = ' || dn);
   plg_debug( 'Attr = ' || attrname);
   --plg_debug( 'Attrval = ' || attrval);

   DBMS_LDAP.USE_EXCEPTION := FALSE;
   errormsg := 'No error msg';
   rc := 0;

   -- converting dn to nickname
   my_session := LDAP_PLUGIN.init(ldapplugincontext);
   plg_debug( 'ldap_session =' || RAWTOHEX(SUBSTR(my_session,1,8)));

   retval := LDAP_PLUGIN.simple_bind_s(ldapplugincontext, my_session);
   plg_debug( 'simple_bind_res =' || TO_CHAR(retval));

   user_nickname := get_nickname(dn, my_session);
   plg_debug( 'user_nickname =' || user_nickname);

   -- unbind from the directory
   retval := DBMS_LDAP.unbind_s(my_session);
   plg_debug( 'unbind_res Returns ' || To_char(retval));

   IF (user_nickname IS NULL) THEN
      result := 32;
      errormsg := 'Can''t find the nickname';
      plg_debug( 'Can''t find the nickname');
      RETURN;
   END IF;

   plg_debug( '=== Now go to extauth ');

   BEGIN
      retval := auth_external.authenticate_user(user_nickname, attrval);
      plg_debug( 'auth_external.authenticate_user() returns = ' || 'True');
      result := 6; -- compare result is TRUE
   EXCEPTION
      WHEN OTHERS THEN
         result := 5; -- compare result is FALSE
```

```
        plg_debug( 'auth_external.authenticate_user() returns = ' || 'False');
        RETURN;
   END;

   plg_debug( '=== End of WHEN-COMPARE-REPLACE plug-in');
EXCEPTION
   WHEN OTHERS THEN
      rc := 1;
      errormsg := 'Exception: when_compare_replace plugin';
      plg_debug( 'EXCEPTION: ' || retval);
      plg_debug('Exception in when_compare. Error code is ' || to_char(sqlcode));
      plg_debug('   ' || Sqlerrm);
END;


PROCEDURE when_modify_replace (ldapplugincontext IN  ODS.plugincontext,
                               dn                IN  VARCHAR2,
                               mods              IN  ODS.modlist,
                               rc                OUT INTEGER,
                               errormsg          OUT VARCHAR2
                               )
  IS
     retval pls_integer;
     lresult BOOLEAN;

     my_session          DBMS_LDAP.SESSION;
     my_property_names   DBMS_LDAP.STRING_COLLECTION;
     my_property_values  DBMS_LDAP.STRING_COLLECTION;
     my_attrs            DBMS_LDAP.STRING_COLLECTION;
     my_modval           DBMS_LDAP.BERVAL_COLLECTION;
     my_pset_coll        DBMS_LDAP_UTL.PROPERTY_SET_COLLECTION;
     user_handle         DBMS_LDAP_UTL.HANDLE;

     l_mod_array         RAW(32);
     user_id             VARCHAR2(2000);
     user_type           PLS_INTEGER;
     user_nickname       VARCHAR2(2000);
     old_passwd          VARCHAR2(60) DEFAULT NULL;
     new_passwd          VARCHAR2(60) DEFAULT NULL;
     remote_dn           VARCHAR2(256);

     i                   PLS_INTEGER;
     j                   PLS_INTEGER;
     k                   PLS_INTEGER;

BEGIN
   plg_debug( '=== Begin of WHEN-MODIFY-REPLACE plug-in');
```

```
DBMS_LDAP.USE_EXCEPTION := FALSE;
user_type     := DBMS_LDAP_UTL.TYPE_DN;
user_id       := dn;

-- converting dn to nickname
my_session := LDAP_PLUGIN.init(ldapplugincontext);
plg_debug( 'ldap_session =' || RAWTOHEX(SUBSTR(my_session,1,8)));

retval := LDAP_PLUGIN.simple_bind_s(ldapplugincontext, my_session);
plg_debug( 'simple_bind_res =' || TO_CHAR(retval));

user_nickname := get_nickname(dn, my_session);
plg_debug( 'user_nickname =' || user_nickname);

-- unbind from the directory
retval := DBMS_LDAP.unbind_s(my_session);

FOR l_counter1 IN 1..mods.COUNT LOOP
   IF (mods(l_counter1).operation = 2) AND
     (mods(l_counter1).type = 'userpassword') THEN

      FOR l_counter2 IN 1..mods(l_counter1).vals.COUNT LOOP
         new_passwd := mods(l_counter1).vals(l_counter2).val;
      END LOOP;
   END IF;

   IF (mods(l_counter1).operation = 0) AND
     (mods(l_counter1).type = 'userpassword') THEN

      FOR l_counter2 IN 1..mods(l_counter1).vals.COUNT LOOP
         new_passwd := mods(l_counter1).vals(l_counter2).val;
      END LOOP;
   END IF;

   IF (mods(l_counter1).operation = 1) AND
     (mods(l_counter1).type = 'userpassword') THEN

      FOR l_counter2 IN 1..mods(l_counter1).vals.COUNT LOOP
         old_passwd := mods(l_counter1).vals(l_counter2).val;
      END LOOP;
   END IF;
END LOOP;

IF new_passwd IS NOT NULL AND old_passwd IS NOT NULL THEN
  BEGIN
     auth_external.change_passwd(user_nickname, old_passwd, new_passwd);
  EXCEPTION
```

```
            WHEN OTHERS THEN
               rc := 1;
               plg_debug( 'auth_external.change_passwd() raised exception.');
               errormsg := 'auth_external.change_passwd() raised exception.';
               RETURN;
         END;
        ELSIF new_passwd IS NOT NULL AND old_passwd IS NULL THEN
         BEGIN
            auth_external.reset_passwd(user_nickname, new_passwd);
         EXCEPTION
            WHEN OTHERS THEN
               plg_debug( 'auth_external.reset_passwd() raised exception.');
               rc := 1;
               errormsg := 'auth_external.reset_passwd() raised exception.';
               RETURN;
         END;
        ELSE
               rc := 1;
               errormsg := 'PLG_Exception. Not enough info to change passwd.';
       END IF;

       plg_debug( 'external change password succeed');
       rc := 0;
       errormsg := 'No when_mod_replace plguin error msg';

       retval := DBMS_LDAP.unbind_s(my_session);

       plg_debug( 'End of WHEN-MODIFY-REPLACE');
       --COMMIT;
    EXCEPTION
       WHEN others THEN
          rc := 1;
          errormsg := 'PLG_Exception: when_modify_replace plguin';
          plg_debug('Exception in when_modify. Error code is ' || to_char(sqlcode));
          plg_debug('   ' || Sqlerrm);
    END;

END OIDEXTAUTH;
/
SHOW ERRORS
--list


GRANT EXECUTE ON OIDEXTAUTH TO ods_server;

EXIT;
```

第 IX 部

付録

第 IX 部は次の各付録で構成されています。

- 付録 A「LDIF およびコマンドライン・ツールの構文」
- 付録 B「Oracle Internet Directory のスキーマ要素」
- 付録 C「Oracle Internet Directory Graphical User Interface（GUI）の要素」
- 付録 D「LDAP フィルタ定義」
- 付録 E「アクセス制御ディレクティブ書式」
- 付録 F「データベース・コピー・プロシージャを使用したディレクトリ・ノードの追加」
- 付録 G「ディレクトリにおけるグローバリゼーション・サポート」
- 付録 I「トラブルシューティング」

A

LDIF およびコマンドライン・ツールの構文

この付録では、**LDAP Data Interchange Format（LDIF）**と LDAP コマンドライン・ツールに関する構文、使用方法および例を紹介します。次の項目について説明します。

- LDAP Data Interchange Format（LDIF）の構文
- Oracle Internet Directory サーバーの起動、停止、再起動および監視
- エントリおよび属性の管理コマンドライン・ツール構文
- バルク操作コマンドライン・ツールの構文
- レプリケーション管理コマンドライン・ツールの構文
- Oracle Directory Integration and Provisioning Platform コマンドライン・ツールの構文
- OID データベース・パスワード・ユーティリティ（oidpasswd）構文
- OID データベース統計収集ツール（oidstats.sh）の構文
- OID 移行ツール（ldifmigrator）の構文

LDAP Data Interchange Format（LDIF）の構文

ディレクトリ・エントリの標準ファイル形式は、次のとおりです。

```
dn: distinguished_name
attribute_type: attribute_value
.
.
.
objectClass: object_class_value
.
.
.
```

プロパティ	値	説明
dn:	*RDN,RDN,RDN, ...*	相対識別名をカンマで区切ります。
attribute_ type:	*attribute_value*	この行は、エントリの各属性、および複数値属性の各属性値ごとに繰り返します。
objectClass:	*object_class_ value*	この行は、各オブジェクト・クラスごとに繰り返します。

次の例は、ある従業員のファイル・エントリを示しています。1 行目は識別名です。識別名に続く各行は、属性のニーモニックで始まり、その属性の値が続きます。各エントリが、そのエントリのオブジェクト・クラスを定義する行で終了していることに注意してください。

```
dn: cn=Suzie Smith,ou=Server Technology,o=Acme, c=US
cn: Suzie Smith
cn: SuzieS
sn: Smith
mail: ssmith@us.Acme.com
telephoneNumber: 69332
photo: /ORACLE_HOME/empdir/photog/ssmith.jpg
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

次の例は、ある組織のファイル・エントリを示しています。

```
dn: o=Acme,c=US
o: Acme
ou: Financial Applications
objectClass: organization
objectClass: top
```

LDIF 形式化の注意事項

次に示すのは、形式化規則のリストです。このリストは、全規則ではありません。

- 追加対象のエントリに属しているすべての必須属性は、非 NULL 値で LDIF ファイルに記述する必要があります。

  ヒント： オブジェクト・クラスの必須属性とオプション属性のタイプを調べるには、Oracle Directory Manager を使用します。6-7 ページの「Oracle Directory Manager を使用したオブジェクト・クラスのプロパティの表示」を参照してください。

- 非表示文字やタブは、BASE64 エンコーディングによる属性値で記述します。
- ファイル内のエントリの間は、空白行で区切る必要があります。
- ファイルには、少なくとも 1 つのエントリが含まれている必要があります。
- 次の行に継続する場合は、継続行を空白またはタブで開始します。
- 個々のエントリの間に空白行を追加してください。
- 写真などのバイナリ・ファイルは、スラッシュ（/）で始まるファイルの絶対アドレスで参照を付けます。
- 識別名には、オブジェクトに対する一意の完全なディレクトリ・アドレスが含まれます。
- 識別名の後にリストされる行には、属性とその値が含まれます。入力ファイルで使用される識別名と属性は、ディレクトリ情報ツリーの既存の構造と一致している必要があります。ディレクトリ情報ツリー内で実装していない属性は、入力ファイルで使用しないでください。
- LDIF ファイル内のエントリは、ディレクトリ情報ツリーが上位から下位へ作成されるように順に記述します。エントリがその識別名の上位のエントリに依存している場合は、その子エントリの前に上位エントリを必ず追加してください。
- LDIF ファイル内にスキーマを定義するときは、左カッコと最初のテキストの間、および最後のテキストと右カッコの間に空白を挿入してください。

関連項目：

- LDIF 形式化規則の全リストは、xlviii ページ の「関連ドキュメント」の各種資料を参照してください。
- G-3 ページの「LDIF ファイルでのグローバリゼーション・サポートの使用方法」

Oracle Internet Directory サーバーの起動、停止、再起動および監視

この項では、コマンドライン・ツールを使用して Oracle Internet Directory サーバーを起動、停止、再起動および監視する方法について説明します。次の項目について説明します。

- OID モニター（oidmon）構文
- OID 制御ユーティリティ（oidctl）の構文

OID モニター（oidmon）構文

OID モニターを使用して、ディレクトリ・サーバー・プロセスを開始、監視および終了します。レプリケーション・サーバーをインストールするように選択した場合、レプリケーション・サーバーは OID モニターによって制御されます。ディレクトリ・サーバー・インスタンスを起動または停止するために OID 制御ユーティリティ（OIDCTL）を介してコマンドを発行すると、そのコマンドはこのプロセスによって解析されます。

OID モニターの起動

OID モニターを起動すると、以前停止したすべての Oracle Internet Directory プロセスが再起動されます。

OID モニターを起動する手順は、次のとおりです。

1. 次の環境変数を設定します。
   - *ORACLE_HOME*
   - ORACLE_*SID* または適切な TNS CONNECT 文字列
   - NLS_LANG（*APPROPRIATE_LANGUAGE*.AL32UTF8）。インストール時のデフォルトの言語設定は、AMERICAN_AMERICA です。
   - PATH。環境変数 PATH では、UNIX バイナリ・ディレクトリの前に Oracle LDAP バイナリ（*ORACLE_HOME*/bin）を指定します。
2. コマンド・プロンプトで、次のコマンドを入力します。

```
oidmon [connect=connect_string] [host=virtual/host_name][sleep=seconds] start
```

表 A-1 OID モニターを起動するための引数

引数	説明
connect=*connect_string*	接続先データベースの接続文字列を指定します。tnsnames.ora ファイルに設定されているネットワーク・サービス名です。この引数はオプションです。
host=*virtual/host_name*	OID モニターを起動する仮想ホストまたはラック・ノードを指定します。
sleep=*seconds*	OID モニターが、OID 制御ユーティリティからの新規要求、および停止している可能性があるサーバーの再起動要求をチェックするまでの秒数を指定します。デフォルトのスリープ・タイムは 10 秒です。この引数はオプションです。
start	OID モニター・プロセスを開始します。

次に例を示します。

```
oidmon connect=dbs1 sleep=15 start
```

仮想ホスト上で OID モニターを起動する手順は、次のとおりです。

```
oidmon connect=dbsl host=virtual_host start
```

OID モニターの停止

OID モニターを停止すると、他のすべての Oracle Internet Directory プロセスも停止されます。

OID モニター・デーモンを停止するには、コマンド・プロンプトで次のコマンドを入力します。

```
oidmon [connect=connect_string] [host=virtual/host_name] stop
```

表 A-2 OID モニターを停止するための引数

引数	説明
connect=*connect_string*	接続先データベースの接続文字列を指定します。これは、tnsnames.ora ファイルに設定されている接続文字列のセットです。
host=*virtual/host name*	OID モニターを起動する仮想ホストまたはラック・ノードを指定します。
stop	OID モニターのプロセスを停止します。

次に例を示します。

```
oidmon connect=dbs1 stop
```

コールド・フェイルオーバー・クラスタ構成での OID モニターの起動と停止

OID モニターを起動および停止する場合は、host パラメータを使用して仮想ホスト名を指定します。構文は次のとおりです。

```
oidmon [connect=connect_string] host=virtual_host start|stop
```

> **注意：** OIDMON および OIDCTL の両方を使用して、仮想ホストで Oracle Internet Directory サーバーを起動する場合は、仮想ホストとして必ず host 引数を指定してください。
>
> host=*host name* 引数を指定して OID モニターを起動すると、ホスト名が物理ホストの名前と一致しない場合は、OID モニターによって、対象ホストが論理ホストであるとみなされます。OIDCTL を使用してサーバーを停止または起動する場合は、同じホスト名を使用する必要があります。同じホスト名を使用しない場合、OID モニターはサーバーを起動または停止しません。
>
> 物理ホスト名を判断するには、uname コマンドを実行します。

OID 制御ユーティリティ（oidctl）の構文

OID 制御ユーティリティは、ディレクトリ・サーバーの起動と停止に使用するコマンドライン・ツールです。コマンドは、OID モニター・プロセスによって解析され、実行されます。

次の項目について説明します。

- Oracle ディレクトリ・サーバー・インスタンスの起動と停止
- ディレクトリ・サーバー・インスタンスの起動に関するトラブルシューティング
- Oracle ディレクトリ・レプリケーション・サーバー・インスタンスの起動と停止
- Oracle Directory Integration and Provisioning Server の起動
- Oracle Directory Integration and Provisioning Server の停止
- Oracle Internet Directory サーバー・インスタンスの再起動
- 仮想ホストまたはラック・ノードでの Oracle Internet Directory サーバーの起動と停止

Oracle ディレクトリ・サーバー・インスタンスの起動と停止

OID 制御ユーティリティを使用して、Oracle ディレクトリ・サーバー・インスタンスの起動と停止を行います。

Oracle ディレクトリ・サーバー・インスタンスの起動 Oracle ディレクトリ・サーバー・インスタンスを起動する構文は、次のとおりです。

```
oidctl connect=connect_string server=oidldapd instance=server_instance_number
[configset=configset_number] [host=virtual/host_name][flags=' -p port_number -work
maximum_number_of_worker_threads_per_server -debug debug_level -l change_logging'
-server number_of_server_processes] start
```

表 A-3 OIDCTL を使用してディレクトリ・サーバーを起動するための引数

引数	説明
-debug *debug_level*	Oracle ディレクトリ・サーバー・インスタンス起動中のデバッグ・レベルを指定します。
-l *change_logging*	レプリケーションの変更ログを記録するかどうかを設定します。設定をオフにする場合は、-l false を入力します。設定をオンにするには、次のいずれかを実行します。 ■ -l フラグを省略します。 ■ -l を入力します。 ■ -l true を入力します。 -l false で、指定したノードに対する変更ログの記録をオフにすると、2 つの問題が発生します。指定したノードから DRG のその他のノードへの更新のレプリケーションが阻止され、アプリケーション・プロビジョニングおよび接続ディレクトリの同期が阻止されます。これは、この 2 つのサービスには、アクティブな変更ログが必要なためです。デフォルトは TRUE で、レプリケーション、プロビジョニングおよび同期を許可します。
-p *port_number*	サーバー・インスタンス起動中のポート番号を指定します。デフォルトのポート番号は 389 です。
-server *number_of_server_processes*	このポートで起動するサーバー・プロセスの数を指定します。

表 A-3 OIDCTL を使用してディレクトリ・サーバーを起動するための引数（続き）

引数	説明
`-sport`	サーバー・インスタンス起動中に SSL ポート番号を指定します。未設定の場合、デフォルトのポート番号は 636 です。 **関連項目：** ■ `orclsslenable` 属性の詳細は、B-5 ページの「構成設定エントリのスキーマ要素」を参照してください。 ■ 13-3 ページの「SSL パラメータの構成」
`-work` *`maximum_number_of_worker_threads_per_server`*	このサーバーのワーカー・スレッドの最大数を指定します。
`configset=`*`configset_number`*	サーバーの起動に使用される configset の番号。未設定の場合は、デフォルトで `configset0` に設定されます。0 ～ 1000 の間の数値を設定してください。
`connect=`*`connect_string`*	すでに `tnsnames.ora` ファイルを構成している場合は、*`ORACLE_HOME`*`/network/admin` にある、そのファイルに指定されているネット・サービス名です。
`host=`*`virtual/host_name`*	ディレクトリ・サーバーを起動する仮想ホストまたはラック・ノードを指定します。
`instance=`*`server_instance_number`*	起動するサーバーのインスタンス番号。1 ～ 1000 の間の数値を設定してください。
`server=oidldapd`	起動するサーバーの種類（有効な値は OIDLDAPD と OIDREPLD です）。大文字と小文字は区別されません。
`start`	`server` 引数で指定したサーバーを起動します。

たとえば、ネット・サービス名が dbs1 で、`configset5` を使用し、ポート 12000、デバッグ・レベル 1024、インスタンス番号 3、変更ログ記録なしでディレクトリ・サーバー・インスタンスを起動するには、コマンド・プロンプトで次のように入力します。

```
oidctl connect=dbs1 server=oidldapd instance=3 configset=5 flags='-p 12000
-debug 1024 -l ' start
```

Oracle ディレクトリ・サーバー・インスタンスの起動と停止では、コマンド `start` または `stop` 同様に、サーバー名とインスタンス番号が必須です。その他の引数はすべてオプションです。

フラグ引数内のペアのキーワード値はすべて、その間を 1 つの空白で区切る必要があります。

フラグは引用符で囲む必要があります。

configset 識別子が未設定の場合は、デフォルトで 0（configset0）に設定されます。

注意： デフォルト・ポート（無保護使用の場合は 389、保護使用の場合は 636）以外のポートを使用する場合は、Oracle Internet Directory の配置に使用するポートをクライアントに通知する必要があります。デフォルト・ポートを使用する場合、クライアントは、接続要求でポートを参照せずに Oracle Internet Directory に接続できます。

Oracle ディレクトリ・サーバー・インスタンスの停止 コマンド・プロンプトで、次のコマンドを入力します。

```
oidctl connect=connect_string server=oidldapd instance=server_instance_number stop
```

次に例を示します。

```
oidctl connect=dbs1 server=oidldapd instance=3 stop
```

ディレクトリ・サーバー・インスタンスの起動に関するトラブルシューティング

ディレクトリ・サーバーが起動に失敗した場合は、ディレクトリ・サーバーを起動するためにユーザーが指定した構成パラメータをすべてオーバーライドし、サーバー起動後に ldapmodify 操作で、構成設定を使用可能な状態に戻すことができます。

ディレクトリに格納されている構成パラメータのかわりに、ハードコードされたデフォルト・パラメータを使用してディレクトリ・サーバーを起動するには、コマンド・プロンプトで次のコマンドを入力します。

```
oidctl connect=connect_string flags='-p port_number -f'
```

フラグ内に -f オプションを指定すると、定義済の構成設定が configset0 内の値を除いてすべてオーバーライドされ、ハードコードされた構成値でサーバーが起動されます。

OID 制御ユーティリティによって生成されたデバッグ・ログ・ファイルを見るには、$*ORACLE_HOME*/ldap/log にナビゲートします。

Oracle ディレクトリ・レプリケーション・サーバー・インスタンスの起動と停止

OID 制御ユーティリティを使用して、Oracle ディレクトリ・レプリケーション・サーバー・インスタンスの起動と停止を行います。

Oracle ディレクトリ・レプリケーション・サーバー・インスタンスの起動 Oracle ディレクトリ・レプリケーション・サーバーを起動する構文は、次のとおりです。

```
oidctl connect=connect_string server=oidrepld instance=server_instance_number
[configset=configset_number] flags=' -p directory_server_port_number -d debug_level
-h directory_server_host_name -m [true | false]-z transaction_size ' start
```

表 A-4 OIDCTL を使用してディレクトリ・レプリケーション・サーバーを起動するための引数

引数	説明
connect=*connect_string*	すでに tnsnames.ora ファイルを構成している場合は、ORACLE_HOME/network/admin にある、そのファイルに指定されている名前です。
server=oidrepld	起動するサーバーの種類（有効な値は OIDLDAPD と OIDREPLD です）。大文字と小文字は区別されません。
instance=*server_instance_number*	起動するサーバーのインスタンス番号。1 ～ 1000 の間の数値を設定してください。
configset=*configset_number*	サーバーの起動に使用される configset の番号。デフォルトの設定は、configset0 です。0 ～ 1000 の間の数値を設定してください。
-p *directory_server_port_number*	TCP ポート *directory_server_port_number* 上のディレクトリへの接続でレプリケーション・サーバーが使用するポート番号。このオプションを指定しない場合は、デフォルト・ポート（389）に接続されます。
-d *debug_level*	レプリケーション・サーバー・インスタンス起動中のデバッグ・レベルを指定します。
-h *directory_server_host_name*	レプリケーション・サーバーを、デフォルトのホスト以外のホスト（つまり、ローカル・コンピュータ）に接続する場合、*directory_server_host_name* で指定します。*directory_server_host_name* には、コンピュータ名または IP アドレスを指定します。（レプリケーション・サーバーのみ）
-m [*true*|*false*]	競合解消を行うかどうかを設定します。TRUE および FALSE が有効な値です。デフォルトは TRUE です。（レプリケーション・サーバーのみ）
-z *transaction_size*	各レプリケーション更新サイクルで適用される変更の数を指定します。指定しない場合は、Oracle ディレクトリ・サーバーの sizelimit パラメータの値で決まります。sizelimit パラメータのデフォルト設定は 1024 です。この設定は変更できます。
start	*server* 引数で指定したサーバーを起動します。

たとえば、インスタンスが 1、ポート 12000、デバッグ・レベル 1024 でレプリケーション・サーバーを起動するには、コマンド・プロンプトで次のように入力します。

```
oidctl connect=dbs1 server=oidrepld instance=1 flags='-p 12000 -h eastsun11 -d 1024'
start
```

Oracle ディレクトリ・レプリケーション・サーバーの起動と停止では、-h フラグ（ホスト名を指定する引数）が必須です。その他のフラグはすべてオプションです。

フラグ引数内のペアのキーワード値はすべて、その間を 1 つの空白で区切る必要があります。

フラグは引用符で囲む必要があります。

configset 識別子が未設定の場合は、デフォルトで 0（configset0）に設定されます。

> **注意：** デフォルト・ポート（無保護使用の場合は 389、保護使用の場合は 636）以外のポートを使用する場合は、Oracle Internet Directory の配置に使用するポートをクライアントに通知する必要があります。デフォルト・ポートを使用する場合、クライアントは、接続要求でポートを参照せずに Oracle Internet Directory に接続できます。

Oracle ディレクトリ・レプリケーション・サーバー・インスタンスの停止 コマンド・プロンプトで、次のコマンドを入力します。

```
oidctl connect=connect_string server=OIDREPLD instance=server_instance_number stop
```

次に例を示します。

```
oidctl connect=dbs1 server=oidrepld instance=1 stop
```

Oracle Directory Integration and Provisioning Server の起動

Oracle Directory Integration and Provisioning Server の実行可能ファイル odisrv は、$*ORACLE_HOME*/bin ディレクトリに存在します。

Directory Integration and Provisioning Server の起動方法は、インストール環境によって異なります。

- 一般的な Oracle Internet Directory のインストール

  この場合、インストール環境には、サーバーおよびクライアント・コンポーネントのうち、特に OID モニターと OID 制御ユーティリティが含まれます。この場合は、これらのツールを使用して Directory Integration and Provisioning Server を起動および停止します。

> **注意：** Directory Integration and Provisioning Server は OID モニターと OID 制御ユーティリティを使用せずに起動することもできますが、これらを使用して起動することをお薦めします。これによって、Directory Integration and Provisioning Server が予期せずに終了した場合、OID モニターを使用して再起動できます。

- Oracle Directory Integration and Provisioning Platform のみのインストール

  この場合、Directory Integration and Provisioning Server の起動方法は、高可用性を目的として Oracle Directory Integration and Provisioning Platform を使用しているかどうかによって異なります。

  - 高可用性を目的として Oracle Directory Integration and Provisioning Platform を使用している場合は、OID モニターと OID 制御ユーティリティを使用して Directory Integration and Provisioning Server を起動することをお薦めします。この場合は、正しいホストおよび OID モニターの接続先の SID で、`tnsnames.ora` ファイルを構成する必要があります。
  - 高可用性を目的として Oracle Directory Integration and Provisioning Platform を使用していない場合は、OID モニターを使用せずに Directory Integration and Provisioning Server を起動することをお薦めします。

Directory Integration and Provisioning Server は、SSL モード（厳しいセキュリティ）または非 SSL モードのいずれでも起動することができます。データベースへの接続には、接続文字列を使用する必要があります。

> **注意：** Oracle Directory Integration and Provisioning Server をデフォルト・モードで起動すると、Oracle Directory Provisioning Integration Service のみがサポートされ、Oracle Directory Synchronization Service はサポートされません。

OID モニターと OID 制御ユーティリティを使用した Oracle Directory Integration and Provisioning Server の起動 Directory Integration and Provisioning Server を非 SSL モードで起動する手順は、次のとおりです。

1. OID モニターが実行されていることを確認します。このことを UNIX で確認するには、コマンドラインで次のように入力します。

   ```
   ps -ef | grep oidmon
   ```

   OID モニターが実行されていない場合は、A-4 ページの「OID モニター（oidmon）構文」の説明に従って OID モニターを起動します。

2. OID 制御ユーティリティを使用して Directory Integration and Provisioning Server を起動します。起動するには、次のように入力します。

```
oidctl [connect=connect_string] server=odisrv [instance=instance_number]
[config=configuration_set_number] [flags="[host=hostname] [port=port_number]
[debug=debug_level] [refresh=interval_between_refresh]
[grpID=group_identifier_of_provisioning_profile]
[maxprofiles=number_of_profiles]
[ sslauth=ssl_mode ]"] start
```

表 A-5 に、このコマンドの引数を示します。

表 A-5 Oracle Directory Integration and Provisioning Server を起動するための引数の説明

引数	説明
connect=*connect_string*	すでに tnsnames.ora ファイルを構成している場合は、$*ORACLE_HOME*/network/admin にある、そのファイルに指定されているネット・サービス名です。
server=odisrv	起動するサーバーの型。このケースでは、起動されるサーバーは odisrv です。大文字と小文字は区別されません。この引数は必須です。
instance=*instance_number*	Directory Integration and Provisioning Server に割り当てるインスタンス番号を指定します。このインスタンス番号は一意である必要があります。OID モニターは、インスタンス番号が、このサーバーの現在実行中のインスタンスに対応付けられていないことを検証します。インスタンス番号が現在実行中のインスタンスに対応付けられている場合、OID モニターはエラー・メッセージを戻します。
config=*configuration_set_number*	Directory Integration and Provisioning Server が実行する構成設定の番号を指定します。この引数は必須です。
host=*hostname*	Oracle ディレクトリ・サーバーのホスト名。
port=*port_number*	Oracle ディレクトリ・サーバーのポート番号。
debug=*debug_level*	Directory Integration and Provisioning Server に必要なデバッグ・レベル。 **関連項目：**様々なデバッグ・レベルの詳細は、10-7 ページの表 10-2 を参照してください。
refresh=*interval_between_refreshes*	サーバーが統合プロファイルの変更を更新する間隔を分単位で指定します。デフォルトは 2 分（Refresh=2）です。
maxprofiles=*number_of_profiles*	このサーバー・インスタンスに対して同時に実行できるプロファイルの最大数を指定します。

表 A-5 Oracle Directory Integration and Provisioning Server を起動するための引数の説明（続き）

引数	説明

sslauth=*ssl_mode*	SSL モード。
	■ 0: SSL が使用されない非 SSL モード。
	■ 1: 暗号化用にのみ使用される SSL モード（PKI 認証なし）。この場合、Wallet は使用されません。
	■ 2: サーバー認証でのみ使用される SSL モード。このモードでは、Wallet のロケーションのみを必要とする他の Oracle Internet Directory ツールとは異なり、Oracle Wallet の完全なパス名（ファイル名自体を含む）を指定する必要があります。たとえば、サーバーのみのインストールまたは完全インストールの場合は、次のように入力します。
	`oidctl server=odisrv [instance=instance_number] [configset=configset_number] [grpID=group_identifier_of_provisioning_profile] flags="host=myhost port=myport sslauth=2`
	
	クライアントのみのインストールの場合は、次のように入力します。
	`odisrv [host=host_name] [port=port_number] config=configuration_set_number [instance=instance_number] [debug=debug_level] [refresh=interval_between_refresh] [maxprofiles=number_of_profiles] [refresh=interval_between_refresh] [maxprofiles=number_of_profiles] [sslauth=ssl_mode]`

OID モニターと OID 制御ユーティリティを使用しない Oracle Directory Integration and Provisioning Server の起動 OID モニターおよび OID 制御ツールを使用できないクライアントのみのインストール環境では、OID モニターまたは OID 制御ユーティリティを使用せずに、Oracle Directory Integration and Provisioning Server を非 SSL モードまたは SSL モード（高セキュリティ用）のいずれかで起動できます。各タイプで起動するためのパラメータについては、A-13 ページの表 A-5 を参照してください。

Directory Integration and Provisioning Server を起動するには、コマンドラインで次のように入力します。

```
odisrv [host=host_name] [port=port_number]
config=configuration_set_number [instance=instance_number] [debug=debug_level]
[refresh=interval_between_refresh] [maxprofiles=number_of_profiles] [sslauth=ssl_
mode]
```

Oracle Directory Integration and Provisioning Server の停止

Directory Integration and Provisioning Server の停止方法は、起動に使用したツールによって異なります。

OID モニターと OID 制御ユーティリティを使用した Oracle Directory Integration and Provisioning Server の停止 OID モニターと OID 制御ユーティリティを使用して Directory Integration and Provisioning Server を起動した場合は、これらを使用して停止する必要があります。

1. Directory Integration and Provisioning Server を停止する前に、OID モニターが実行されていることを確認します。このことを確認するには、コマンドラインで次のように入力します。

   ```
   ps -ef | grep oidmon
   ```

   OID モニターが実行されていない場合は、A-4 ページの「OID モニター（oidmon）構文」の説明に従って OID モニターを起動します。

2. 次のように入力して、Directory Integration and Provisioning Server を停止します。

   ```
   oidctl [connect=connect_string] server=odisrv instance=instance stop
   ```

OID モニターと OID 制御ユーティリティを使用しない Oracle Directory Integration and Provisioning Server の停止 OID モニターと OID 制御ツールを使用できないクライアントのみのインストール環境では、OID 制御ツールを使用せずに Oracle Directory Integration and Provisioning Server を起動できます。これらのツールを使用せずにサーバーを停止するには、*$ORACLE_HOME*/ldap/admin ディレクトリに格納されている stopodiserver.sh ツールを使用します。

注意： Windows オペレーティング・システムでシェル・スクリプト・ツールを実行するには、次のいずれかの UNIX エミュレーション・ユーティリティが必要です。

- Cygwin 1.3.2.2-1 以上
  サイト：http://sources.redhat.com
- MKS Toolkit 6.1
  サイト：http://www.datafocus.com/

関連項目： stopodiserver.sh ツールの使用方法は、A-122 ページの「StopOdiServer.sh ツールの構文」を参照してください。

注意： 前述以外の方法で Oracle Directory Integration and Provisioning Server が停止した場合、そのサーバーは同じホストから起動できません。この場合は、次のコマンドを使用して、ディレクトリ内にある前回実行した際のフットプリントを削除する必要があります。

```
$ORACLE_HOME/ldap/admin/stopodiserver.sh [-host
directory_server_host] [-port directory_server_port]
[-binddn super_user_dN (default is cn=orcladmin)]
[-bindpass super_user_password (default is welcome)]
-instance number_of_the_instance_to_stop -clean
```

Oracle Internet Directory サーバー・インスタンスの再起動

予定の更新時刻を待たず、サーバーのキャッシュを即時に更新する場合は、RESTART コマンドを使用します。再起動した Oracle Internet Directory サーバーは、停止前と同じパラメータを保持しています。

Oracle Internet Directory サーバー・インスタンスを再起動するには、コマンド・プロンプトで次のコマンドを入力します。

```
oidctl connect=connect_string server={oidldapd|oidrepld|odisrv}
instance=server_instance_number  restart
```

ディレクトリ・サーバー・インスタンスを再起動する場合は、常に OID モニターが実行中であることが必要です。

ダウンしているサーバーに接続しようとすると、SDK からエラー・メッセージ「81:LDAP サーバーと通信できません。」を受け取ります。

アクティブなサーバー・インスタンスが参照している構成設定エントリを変更する場合、構成設定エントリの変更値をそのサーバー・インスタンスで有効にするには、そのインスタンスを停止してから再起動してください。STOP コマンドの後に START コマンドを発行するか、RESTART コマンドを使用します。RESTART は、サーバー・インスタンスを停止してから再起動します。

たとえば、Oracle ディレクトリ・サーバーの instance1 が、configset3 を使用してネット・サービス名 dbs1 で起動されたとします。その後、instance1 の稼働中に、configset3 内の属性の 1 つを変更したとします。configset3 の変更内容を instance1 で有効にするには、次のコマンドを入力します。

```
oidctl connect=dbs1 server=oidldapd instance=1 restart
```

configset3 を使用する複数の Oracle ディレクトリ・サーバーのインスタンスが、そのノードで実行中の場合は、次のコマンド構文を使用して、すべてのインスタンスを一度に再起動できます。

```
oidctl connect=dbs1 server=oidldapd restart
```

このコマンドは、configset3 を使用しているかどうかに関係なく、そのノードで実行中のインスタンスをすべて再起動することに注意してください。

重要： 再起動を実行中、クライアントは Oracle ディレクトリ・サーバー・インスタンスにアクセスできません。ただし、再起動にかかる時間は数秒です。

仮想ホストまたはラック・ノードでの Oracle Internet Directory サーバーの起動と停止

ディレクトリ・サーバー、ディレクトリ・レプリケーション・サーバーまたは Directory Integration and Provisioning Server を起動する場合は、host パラメータを使用して、仮想ホスト名を指定します。

仮想ホストまたはラック・ノードでのディレクトリ・サーバーの起動と停止

仮想ホスト上でディレクトリ・サーバーを起動するには、次のように入力します。

```
oidctl [connect=connect_string] host=virtual_host_name server=oidldapd
instance=instance_number configset=configset_number flags= "..." start
```

仮想ホスト上でディレクトリ・サーバーを停止するには、次のように入力します。

```
oidctl host=virtual_host_name server=oidldapd instance=instance_number stop
```

仮想ホストまたはラック・ノードでのディレクトリ・レプリケーション・サーバーの起動と停止

仮想ホスト上でディレクトリ・レプリケーション・サーバーを起動するには、次のように入力します。

```
oidctl [connect=connect_string] host=virtual_host_name server=oidrepld
instance=instance_number flags= "..." start
```

仮想ホスト上でディレクトリ・レプリケーション・サーバーを停止するには、次のように入力します。

```
oidctl host=virtual_host_name server=oidrepld instance=instance_number stop
```

仮想ホストまたはラック・ノードでの Oracle Directory Integration and Provisioning Server の起動と停止

仮想ホスト上で Directory Integration and Provisioning Server を起動するには、次のように入力します。

```
oidctl [connect=connect_string] host=virtual_host_name server=odisrv
instance=instance_number configset=configset_number flags= "..." start
```

仮想ホスト上で Directory Integration and Provisioning Server を停止するには、次のように入力します。

```
oidctl host=virtual/host_name server=odisrv instance=instance_number stop
```

ディレクトリ・サーバーは、仮想ホスト上での実行のために起動された場合、その仮想ホストのみに対応する IP アドレスに指定された LDAP ポートで要求をバインドおよびリスニングします。

ディレクトリ・サーバーとの通信時、ディレクトリ・レプリケーション・サーバーでは仮想ホスト名が使用されます。また、Oracle Internet Directory ノードに対する一意のレプリケーション識別子を表す `replicaID` 属性が 1 回生成されます。この属性は、ホスト名に依存しないため、コールド・フェイルオーバー構成での特別な処理は必要ありません。

ディレクトリ・サーバーとの通信時、Directory Integration and Provisioning Server では仮想ホスト名が使用されます。

エントリおよび属性の管理コマンドライン・ツール構文

この項では、次のツールの使用方法を説明します。

注意： UNIX シェルでは、アスタリスク（*）などの一部の文字が特殊文字として解釈される場合があります。使用しているシェルに応じて、これらの文字をエスケープする必要があります。

カタログ管理ツール（catalog.sh）構文

Oracle Internet Directory では、索引を使用して属性を検索できます。Oracle Internet Directory のインストール時に、エントリ `cn=catalogs` に、検索で使用できる属性がリストされます。次の条件を満たす属性のみ索引を付けることができます。

- 等価の一致規則
- Oracle Internet Directory でサポートする一致規則

その他の属性を検索フィルタで使用する場合は、使用する属性をカタログ・エントリに追加する必要があります。この操作は、Oracle Directory Manager を使用して属性を作成するときに実行できます。ただし、すでに存在している属性への索引付けに使用できるのは、カタログ管理ツールのみです。

catalog.sh を実行する前に、ディレクトリ・サーバーが停止または読取り専用モードのいずれかの状態にあることを確認してください。これらの状態でない場合は、データの一貫性が維持されなくなります。

注意： Oracle Internet Directory ベースのスキーマで作成された索引に対して、catalog.sh `-delete` オプションは使用しないでください。ベース・スキーマ属性から索引を削除すると、Oracle Internet Directory の操作に悪影響を及ぼす場合があります。

注意： Windows オペレーティング・システムでシェル・スクリプト・ツールを実行するには、次のいずれかの UNIX エミュレーション・ユーティリティが必要です。

- Cygwin 1.3.2.2-1 以上
  サイト：`http://sources.redhat.com`
- MKS Toolkit 6.1
  サイト：`http://www.datafocus.com/`

カタログ管理ツールは次の構文を使用します。

```
catalog.sh -connect connect_string {-add|-delete} {-attr attr_name|-file file_name}
```

表 A-6　カタログ管理ツール（catalog.sh）の引数

引数	説明
`-connect connect_string`	ディレクトリ・データベースに接続するための接続文字列を指定します。この引数は必須です。 **関連項目：**『Oracle9*i* Net Services 管理者ガイド』を参照してください。
`-add -attr attr_name`	指定した属性を索引付けします。
`-delete -attr attr_name`	指定した属性から索引を削除します。
`-add -file file_name`	指定したファイル内の属性（1 行に 1 つずつ）を索引付けします。
`-delete -file file_name`	指定したファイル内の属性から索引を削除します。

`catalog.sh` コマンドを入力すると、次のメッセージが表示されます。

```
This tool can only be executed if you know the OiD user password.
Enter OiD password:
```

正しいパスワードを入力すると、コマンドが実行されます。パスワードに誤りがあると、次のメッセージが表示されます。

```
Cannot execute this tool
```

カタログ管理ツールの実行後にその変更内容を有効にするには、Oracle ディレクトリ・サーバーを停止して再起動してください。

関連項目：

- ディレクトリ・サーバーの起動と再起動の方法は、A-6 ページの「OID 制御ユーティリティ（oidctl）の構文」を参照してください。ディレクトリ・サーバーを起動する場合は、あらかじめ OID モニターが実行されている必要があります。
- OID モニターの開始については、A-4 ページの「OID モニター（oidmon）構文」を参照してください。
- Oracle Internet Directory でサポートする一致規則については、B-46 ページの「一致規則」を参照してください。

ldapadd の構文

ldapadd コマンドライン・ツールを使用すると、エントリ、そのオブジェクト・クラス、属性および値をディレクトリに追加できます。既存のエントリに属性を追加するには、ldapmodify コマンドを使用します。このコマンドについては、A-32 ページの「ldapmodify の構文」を参照してください。

> **関連項目：** 入力ファイルを使用してサーバーを構成するために ldapadd を使用する方法は、5-7 ページの「ldapadd を使用した構成設定エントリの追加」を参照してください。

ldapadd は次の構文を使用します。

```
ldapadd [arguments] -f file_name
```

file_name は、A-2 ページの「LDAP Data Interchange Format（LDIF）の構文」で説明した仕様に従って作成された LDIF ファイルの名前です。

次の例は、LDIF ファイル `my_ldif_file.ldi` に指定されているエントリを追加します。

```
ldapadd -p 389 -h myhost -f my_ldif_file.ldi
```

表 A-7 ldapadd の引数

オプションの引数	説明
`-b`	ファイルにバイナリ・ファイル名が含まれていることを指定します。バイナリ・ファイル名はスラッシュで始まります。ツールは、参照先のファイルから実際の値を取り出します。
`-c`	エラーが発生しても処理を継続する場合に指定します。エラーはレポートされます。（このオプションを使用しない場合、エラーが発生すると ldapadd は停止します。）
`-D "binddn"`	ディレクトリに対して認証を行う場合に、*binddn* に指定されているエントリ（認証を必要とするユーザーの識別名）として認証することを指定します。この引数は、`-w` *password* オプションとともに使用します。
`-E "character_set"`	ネイティブ・キャラクタ・セット・エンコーディングを指定します。詳細は、付録 G「ディレクトリにおけるグローバリゼーション・サポート」を参照してください。
`-f file_name`	LDIF 形式のインポート・データ・ファイルの入力名を指定します。LDIF ファイルの形式化の詳細は、A-2 ページの「LDAP Data Interchange Format（LDIF）の構文」を参照してください。
`-h ldaphost`	デフォルトのホスト（ローカル・コンピュータ）ではなく、*ldaphost* に接続します。*ldaphost* には、コンピュータ名または IP アドレスを指定します。

表 A-7 ldapadd の引数（続き）

オプションの引数	説明
-K	-k と同様ですが、Kerberos バインドの最初の手順のみ実行します。
-k	簡易認証のかわりに、Kerberos 認証を使用して認証します。このオプションを使用可能にするには、定義済の Kerberos でコンパイルする必要があります。証明書を付与する有効なチケットをすでに所有している必要があります。
-M	ManageDSAIT 制御をサーバーに送信するようにツールに指示します。ManageDSAIT 制御は、参照をクライアントに送信しないようにサーバーに指示します。この指示がない場合、参照エントリが通常のエントリとして戻されます。
-n	操作を実際には実行せずに、予測結果を示します。
-O *ref_hop_limit*	クライアントが処理する参照ホップの数を指定します。デフォルト値は 5 です。
-p *directory_server_port_number*	TCP ポート *directory_server_port_number* のディレクトリに接続します。このオプションを指定しない場合は、デフォルト・ポート（389）に接続されます。
-P *wallet_password*	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet のパスワードを指定します。
-U *SSLAuth*	SSL 認証モードを指定します。 ■ 1: SSL 認証なし ■ 2: サーバー認証 ■ 3: クライアントとサーバーの認証
-v	冗長モードを指定します。
-V *ldap_version*	使用する LDAP プロトコルのバージョンを指定します。デフォルト値は 3 で、この場合ツールは LDAP バージョン 3 のプロトコルを使用します。値が 2 の場合、ツールは LDAP バージョン 2 のプロトコルを使用します。
-w *password*	接続に必要なパスワードを指定します。
-W *wallet_location*	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet の位置を指定します。 たとえば、このパラメータは、UNIX では -W "file:/home/my_dir/my_wallet" と設定します。 また、Windows NT では -W "file:C:¥my_dir¥my_wallet" と設定します。

表 A-7 ldapadd の引数（続き）

オプションの引数	説明
`-X dsml_file`	DSML 形式のインポート・データ・ファイルの入力名を指定します。

ldapaddmt の構文

ldapaddmt は ldapadd に類似しています。これを使用すると、エントリ、そのオブジェクト・クラス、属性および値をディレクトリに追加できます。ldapadd と異なるのは、複数のエントリを同時に追加するために複数のスレッドをサポートしている点です。

LDIF エントリの処理中に、ldapaddmt は、現行のディレクトリ内の `add.log` ファイルにエラー・ログを記録します。

ldapaddmt は次の構文を使用します。

```
ldapaddmt -T number_of_threads -h host -p port -f file_name
```

file_name は、A-2 ページの「LDAP Data Interchange Format（LDIF）の構文」で説明した仕様に従って作成された LDIF ファイルの名前です。

次の例は、5 つの同時スレッドを使用して、ファイル `myentries.ldif` 内のエントリを処理しています。

```
ldapaddmt -T 5 -h node1 -p 3000 -f myentries.ldif
```

注意： 同時スレッドの数が増加すると、LDIF エントリの作成は速くなりますが、システム・リソースはより多く消費されます。

表 A-8 ldapadd の引数

オプションの引数	説明
`-b`	データ・ファイルにバイナリ・ファイル名が含まれていることを指定します。バイナリ・ファイル名はスラッシュで始まります。ツールは、参照先のファイルから実際の値を取り出します。
`-c`	エラーが発生しても処理を継続する場合に指定します。エラーはレポートされます。（このオプションを使用しない場合、エラーが発生するとツールは停止します。）
`-D "binddn"`	ディレクトリに対して認証を行う場合に、*binddn* に指定されているエントリ（認証を必要とするユーザーの識別名）として認証することを指定します。この引数は、`-w password` オプションとともに使用します。

表 A-8 ldapadd の引数（続き）

オプションの引数	説明
`-E "character_set"`	ネイティブ・キャラクタ・セット・エンコーディングを指定します。詳細は、付録 G「ディレクトリにおけるグローバリゼーション・サポート」を参照してください。
`-h ldap_host`	デフォルトのホスト（ローカル・コンピュータ）ではなく、*ldaphost* に接続します。*ldaphost* には、コンピュータ名または IP アドレスを指定します。
`-K`	-k と同様ですが、Kerberos バインドの最初の手順のみ実行します。
`-k`	簡易認証のかわりに、Kerberos 認証を使用して認証します。このオプションを使用可能にするには、定義済の Kerberos でコンパイルする必要があります。証明書を付与する有効なチケットをすでに所有している必要があります。
`-M`	`ManageDSAIT` 制御をサーバーに送信するようにツールに指示します。`ManageDSAIT` 制御は、参照をクライアントに送信しないようにサーバーに指示します。この指示がない場合、参照エントリが通常のエントリとして戻されます。
`-n`	操作を実際には実行せずに、予測結果を示します。
`-O ref_hop_limit`	クライアントが処理する参照ホップの数を指定します。デフォルト値は 5 です。
`-p ldapport`	TCP ポート *ldapport* 上のディレクトリに接続します。このオプションを指定しない場合は、デフォルト・ポート（389）に接続されます。
`-P wallet_password`	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet のパスワードを指定します。
`-T`	エントリを同時に処理するスレッドの数を設定します。
`-U SSLAuth`	SSL 認証モードを指定します。 ■ 1: SSL 認証なし ■ 2: サーバー認証 ■ 3: クライアントとサーバーの認証
`-v`	冗長モードを指定します。
`-V ldap_version`	使用する LDAP プロトコルのバージョンを指定します。デフォルト値は 3 で、この場合ツールは LDAP バージョン 3 のプロトコルを使用します。値が 2 の場合、ツールは LDAP バージョン 2 のプロトコルを使用します。

表 A-8 ldapadd の引数（続き）

オプションの引数	説明
`-w password`	接続に必要なパスワードを指定します。
`-W wallet_location`	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet の位置を指定します。たとえば、このパラメータは、UNIX では -W "file:/home/my_dir/my_wallet" と設定し、Windows NT では -W "file:C:¥my_dir¥my_wallet" と設定します。
`-X dsml_file`	DSML 形式のインポート・データ・ファイルの入力名を指定します。

ldapbind の構文

ldapbind コマンドライン・ツールを使用すると、サーバーに対してクライアントを認証できるかどうかを調べることができます。

ldapbind は次の構文を使用します。

```
ldapbind [arguments]
```

表 A-9 ldapbind の引数

引数	説明
-D "*binddn*"	ディレクトリに対して認証を行う場合に、*binddn* に指定されているエントリ（認証を必要とするユーザーの識別名）として認証することを指定します。この引数は、`-w` *password* オプションとともに使用します。
-E "*.character_set*"	ネイティブ・キャラクタ・セット・エンコーディングを指定します。詳細は、付録 G「ディレクトリにおけるグローバリゼーション・サポート」を参照してください。
-h *ldaphost*	デフォルトのホスト（ローカル・コンピュータ）ではなく、*ldaphost* に接続します。*ldaphost* には、コンピュータ名または IP アドレスを指定します。
-n	操作を実際には実行せずに、予測結果を示します。
-p *ldapport*	TCP ポート *ldapport* 上のディレクトリに接続します。このオプションを指定しない場合は、デフォルト・ポート（389）に接続されます。
-P *wallet_password*	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet のパスワードを指定します。

表 A-9 ldapbind の引数（続き）

引数	説明
-U *SSLAuth*	SSL 認証モードを指定します。 1: SSL 認証なし 2: サーバー認証 3: クライアントとサーバーの認証
-V *ldap_version*	使用する LDAP プロトコルのバージョンを指定します。デフォルト値は 3 で、この場合ツールは LDAP バージョン 3 のプロトコルを使用します。値が 2 の場合、ツールは LDAP バージョン 2 のプロトコルを使用します。
-w *password*	接続に必要なパスワードを指定します。
-W *wallet_location*	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet の位置を指定します。たとえば、このパラメータは、UNIX では -W "file:/home/my_dir/my_wallet" と設定し、Windows NT では -W "file:C:¥my_dir¥my_wallet" と設定します。
-O *sasl_security_properties*	SASL セキュリティ・プロパティを指定します。サポートされるセキュリティ・プロパティは、-O "auth" です。このセキュリティ・プロパティは、DIGEST-MD5 SASL メカニズム用です。データ整合性またはデータ・プライバシのない認証を実行できます。
-Y *sasl_mechanism*	SASL メカニズムを指定します。次のメカニズムがサポートされます。 ■ Y "DIGEST-MD5" ■ Y "EXTERNAL": このメカニズムでの SASL 認証は、クライアントとサーバーの SSL 認証とともに実行されます。この場合、SSL Wallet に格納されているユーザーの識別情報が SASL 認証に使用されます。
-R *sasl_realm*	SASL レルムを指定します。

ldapcompare の構文

ldapcompare コマンドライン・ツールを使用すると、コマンドラインで指定した属性値と、ディレクトリ・エントリの属性値を比較できます。

ldapcompare は次の構文を使用します。

```
ldapcompare [arguments]
```

次の例は、Person Nine の title が associate であるかどうかを通知します。

```
ldapcompare -p 389 -h myhost -b "cn=Person Nine,ou=EuroSInet Suite,o=IMC,c=US" -a
title -v associate
```

表 A-10 ldapcompare の引数

オプションの引数	説明
-a *attribute name*	比較を実行する属性を指定します。この引数は必須です。
-b "*basedn*"	比較を実行するエントリの識別名を指定します。この引数は必須です。
-v *attribute value*	比較する属性値を指定します。この引数は必須です。
-D *binddn*	ディレクトリに対して認証を行う場合に、*binddn* に指定されているエントリ（認証を必要とするユーザーの識別名）として認証することを指定します。この引数は、-w *password* オプションとともに使用します。
-d *debug-level*	デバッグ・レベルを設定します。詳細は、10-6 ページの「OID 制御ユーティリティを使用したデバッグ・ロギング・レベルの設定」を参照してください。
-E "*character_set*"	ネイティブ・キャラクタ・セット・エンコーディングを指定します。詳細は、付録 G「ディレクトリにおけるグローバリゼーション・サポート」を参照してください。
-f *file_name*	入力ファイル名を指定します。
-h *ldaphost*	デフォルトのホスト（ローカル・コンピュータ）ではなく、*ldaphost* に接続します。*ldaphost* には、コンピュータ名または IP アドレスを指定します。
-M	ManageDSAIT 制御をサーバーに送信するようにツールに指示します。ManageDSAIT 制御は、参照をクライアントに送信しないようにサーバーに指示します。この指示がない場合、参照エントリが通常のエントリとして戻されます。
-O *ref_hop_limit*	クライアントが処理する参照ホップの数を指定します。デフォルト値は 5 です。
-p *ldapport*	TCP ポート *ldapport* 上のディレクトリに接続します。このオプションを指定しない場合は、デフォルト・ポート（389）に接続されます。
-P *wallet_password*	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet のパスワードを指定します。

表 A-10 ldapcompare の引数（続き）

オプションの引数	説明
-U *SSLAuth*	SSL 認証モードを指定します。 ■ 1: SSL 認証なし ■ 2: サーバー認証 ■ 3: クライアントとサーバーの認証
-V *ldap_version*	使用する LDAP プロトコルのバージョンを指定します。デフォルト値は 3 で、この場合ツールは LDAP バージョン 3 のプロトコルを使用します。値が 2 の場合、ツールは LDAP バージョン 2 のプロトコルを使用します。
-w *password*	接続に必要なパスワードを指定します。
-W *wallet_location*	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet の位置を指定します。たとえば、このパラメータは、UNIX では `-W "file:/home/my_dir/my_wallet"` と設定します。 また、Windows NT では `-W "file:C:¥my_dir¥my_wallet"` と設定します。

ldapdelete の構文

ldapdelete コマンドライン・ツールを使用すると、コマンドラインに指定したディレクトリからエントリ全体を削除できます。

ldapdelete は次の構文を使用します。

```
ldapdelete [arguments] ["entry_DN" | -f input_file_name]
```

注意： エントリ識別名を指定する場合は、`-f` オプションは使用できません。

次の例では、myhost という名前のホストでポート 389 を使用しています。

```
ldapdelete -p 389 -h myhost "ou=EuroSInet Suite, o=IMC, c=US"
```

表 A-11 ldapdelete の引数

オプションの引数	説明
-D "*binddn*"	ディレクトリに対して認証を行う場合に、*binddn* パラメータに完全識別名（認証を必要とするユーザーの識別名）を使用します。通常、`-w` *password* オプションとともに使用します。

表 A-11 ldapdelete の引数（続き）

オプションの引数	説明
-d *debug-level*	デバッグ・レベルを設定します。詳細は、10-6 ページの「OID 制御ユーティリティを使用したデバッグ・ロギング・レベルの設定」を参照してください。
-E "*character_set*"	ネイティブ・キャラクタ・セット・エンコーディングを指定します。詳細は、付録 G「ディレクトリにおけるグローバリゼーション・サポート」を参照してください。
-f *input_file_name*	入力ファイル名を指定します。
-h *ldaphost*	デフォルトのホスト（ローカル・コンピュータ）ではなく、*ldaphost* に接続します。*ldaphost* には、コンピュータ名または IP アドレスを指定します。
-k	簡易認証のかわりに、Kerberos 認証を使用して認証します。このオプションを使用可能にするには、定義済の Kerberos でコンパイルする必要があります。証明書を付与する有効なチケットをすでに所有している必要があります。
`-M`	`ManageDSAIT` 制御をサーバーに送信するようにツールに指示します。`ManageDSAIT` 制御は、参照をクライアントに送信しないようにサーバーに指示します。この指示がない場合、参照エントリが通常のエントリとして戻されます。
-n	削除を実際には実行せずに、予測結果を示します。
-O *ref_hop_limit*	クライアントが処理する参照ホップの数を指定します。デフォルト値は 5 です。
-p *ldapport*	TCP ポート *ldapport* 上のディレクトリに接続します。このオプションを指定しない場合は、デフォルト・ポート（389）に接続されます。
-P *wallet_password*	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet のパスワードを指定します。
-U *SSLAuth*	SSL 認証モードを指定します。 ■ 1: SSL 認証なし ■ 2: サーバー認証 ■ 3: クライアントとサーバーの認証
-v	冗長モードを指定します。
-V *ldap_version*	使用する LDAP プロトコルのバージョンを指定します。デフォルト値は 3 で、この場合ツールは LDAP バージョン 3 のプロトコルを使用します。値が 2 の場合、ツールは LDAP バージョン 2 のプロトコルを使用します。

表 A-11 ldapdelete の引数（続き）

オプションの引数	説明
-w *password*	接続に必要なパスワードを指定します。
-W *wallet_location*	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet の位置を指定します。たとえば、このパラメータは、UNIX では -W "file:/home/my_dir/my_wallet" と設定し、Windows NT では -W "file:C:¥my_dir¥my_wallet" と設定します。

ldapmoddn の構文

ldapmoddn コマンドライン・ツールを使用すると、エントリの識別名または相対識別名を変更できます。

ldapmoddn は次の構文を使用します。

```
ldapmoddn [arguments]
```

次の例では、ldapmoddn を使用して、識別名の相対識別名コンポーネントを cn=mary smith から cn=mary jones に変更しています。ポートは 389、myhost という名前のホストを使用しています。

```
ldapmoddn -p 389 -h myhost -b "cn=mary smith,dc=Americas,dc=imc,dc=com" -R "cn=mary jones"
```

表 A-12 ldapmoddn の引数

引数	説明
-b "*basedn*"	変更されるエントリの識別名を指定します。この引数は必須です。
-D "*binddn*"	ディレクトリに対して認証を行う場合に、*binddn* に指定されているエントリ（認証を必要とするユーザーの識別名）として認証します。この引数は、-w *password* オプションとともに使用します。
-E "*character_set*"	ネイティブ・キャラクタ・セット・エンコーディングを指定します。詳細は、付録 G「ディレクトリにおけるグローバリゼーション・サポート」を参照してください。
-f *file_name*	入力ファイル名を指定します。
-h *ldaphost*	デフォルトのホスト（ローカル・コンピュータ）ではなく、*ldaphost* に接続します。*ldaphost* には、コンピュータ名または IP アドレスを指定します。
-M	ManageDSAIT 制御をサーバーに送信するようにツールに指示します。ManageDSAIT 制御は、参照をクライアントに送信しないようにサーバーに指示します。この指示がない場合、参照エントリが通常のエントリとして戻されます。

表 A-12 ldapmoddn の引数（続き）

引数	説明
-N *newparent*	相対識別名の新しい親を指定します。この引数または引数 -R を指定する必要があります。
-O *ref_hop_limit*	クライアントが処理する参照ホップの数を指定します。デフォルト値は 5 です。
-p *ldapport*	TCP ポート *ldapport* 上のディレクトリに接続します。このオプションを指定しない場合は、デフォルト・ポート（389）に接続されます。
-P *wallet_password*	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet のパスワードを指定します。
-r	旧相対識別名を変更エントリ内に値として保持しないことを指定します。この引数が指定されない場合、旧相対識別名は変更エントリ内に属性として保持されます。
-R *newrdn*	新規相対識別名を指定します。この引数または引数 -N を指定する必要があります。
-U *SSLAuth*	SSL 認証モードを指定します。 1: SSL 認証なし 2: サーバー認証 3: クライアントとサーバーの認証
-V *ldap_version*	使用する LDAP プロトコルのバージョンを指定します。デフォルト値は 3 で、この場合ツールは LDAP バージョン 3 のプロトコルを使用します。値が 2 の場合、ツールは LDAP バージョン 2 のプロトコルを使用します。
-w *password*	接続に必要なパスワードを指定します。
-W *wallet_location*	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet の位置を指定します。たとえば、このパラメータは、UNIX では `-W "file:/home/my_dir/my_wallet"` と設定します。 また、Windows NT では `-W "file:C:¥my_dir¥my_wallet"` と設定します。

ldapmodify の構文

ldapmodify ツールは、属性で作用します。

ldapmodify は次の構文を使用します。

```
ldapmodify [arguments] -f file_name
```

file_name は、A-2 ページの「LDAP Data Interchange Format（LDIF）の構文」で説明した仕様に従って作成された LDIF ファイルの名前です。

次の表の引数リストは、すべての引数ではありません。これらの引数はすべてオプションです。

表 A-13 ldapmodify の引数

引数	説明
-a	エントリが追加対象で、入力ファイルが LDIF 形式であることを示します。
-b	データ・ファイルにバイナリ・ファイル名が含まれていることを指定します。バイナリ・ファイル名はスラッシュで始まります。
-c	エラーが発生しても処理を継続する場合に指定します。エラーはレポートされます。（このオプションを使用しない場合、エラーが発生すると ldapmodify は停止します。）
-D "*binddn*"	ディレクトリに対して認証を行う場合に、*binddn* に指定されているエントリ（認証を必要とするユーザーの識別名）として認証することを指定します。この引数は、-w *password* オプションとともに使用します。
-E "*character_set*"	ネイティブ・キャラクタ・セット・エンコーディングを指定します。詳細は、付録 G「ディレクトリにおけるグローバリゼーション・サポート」を参照してください。
-h *ldaphost*	デフォルトのホスト（ローカル・コンピュータ）ではなく、*ldaphost* に接続します。*ldaphost* には、コンピュータ名または IP アドレスを指定します。
-M	ManageDSAIT 制御をサーバーに送信するようにツールに指示します。ManageDSAIT 制御は、参照をクライアントに送信しないようにサーバーに指示します。この指示がない場合、参照エントリが通常のエントリとして戻されます。
-n	操作を実際には実行せずに、予測結果を示します。
-o *log_file_name*	-c オプションとともに、ログ・ファイル内の誤った LDIF エントリの書込みに使用できます。ログ・ファイル名には絶対パスを指定する必要があります。

表 A-13 ldapmodify の引数（続き）

引数	説明
-O *ref_hop_limit*	クライアントが処理する参照ホップの数を指定します。デフォルト値は 5 です。
-p *ldapport*	TCP ポート *ldapport* 上のディレクトリに接続します。このオプションを指定しない場合は、デフォルト・ポート（389）に接続されます。
-P *wallet_password*	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet のパスワードを指定します。
-U *SSLAuth*	SSL 認証モードを指定します。 ■ 1: SSL 認証なし ■ 2: サーバー認証 ■ 3: クライアントとサーバーの認証
-v	冗長モードを指定します。
-V *ldap_version*	使用する LDAP プロトコルのバージョンを指定します。デフォルト値は 3 で、この場合ツールは LDAP バージョン 3 のプロトコルを使用します。値が 2 の場合、ツールは LDAP バージョン 2 のプロトコルを使用します。
-w *password*	デフォルトの非認証の NULL バインドをオーバーライドします。認証を強制するには、このオプションを `-D` オプションとともに使用します。
-W *wallet_location*	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet の位置を指定します。たとえば、このパラメータは、UNIX では `-W "file:/home/my_dir/my_wallet"` と設定します。 また、Windows NT では `-W "file:C:¥my_dir¥my_wallet"` と設定します。

`-f` フラグを使用して `modify`、`delete` および `modifyrdn` 操作を実行するには、入力ファイル形式に LDIF を使用します（A-2 ページの「LDAP Data Interchange Format（LDIF）の構文」を参照）。仕様は、この項に示すとおりです。

いくつかの変更を行う場合は、入力する各変更の間に、ハイフン（-）のみを含む行を追加します。次に例を示します。

```
dn: cn=Barbara Fritchy,ou=Sales,o=Oracle,c=US
changetype: modify
add: work-phone
work-phone: 510/506-7000
work-phone: 510/506-7001
-
delete: home-fax
```

属性値の後の空白など、LDIF 入力ファイルにおける不要な空白は、LDAP 操作が失敗する原因となります。

第 1 行 : 変更レコードの場合は、その 1 行目にリテラル `dn:`、その後にエントリの識別名値を記述します。次に例を示します。

```
dn:cn=Barbara Fritchy,ou=Sales,o=Oracle,c=US
```

第 2 行 : 変更レコードの場合は、その 2 行目にリテラル `changetype:`、その後に変更の種類（`add`、`delete`、`modify`、`modrdn` など）を記述します。次に例を示します。

```
changetype: modify
```

または

```
changetype: modrdn
```

変更の種類に応じて、次の要件に従って各レコードの残りの部分を形式化します。

- `changetype: add`

  LDIF 形式を使用します（A-2 ページの「LDAP Data Interchange Format（LDIF）の構文」を参照）。

- `changetype: modify`

  この changetype に続く行には、前述の第 1 行で指定したエントリに属する属性に対する変更内容を記述します。属性を変更する場合は、3 種類の変更タイプ（add、delete および replace）を指定できます。変更タイプについて次に説明します。

  – **属性値の追加。**changetype modify のこのオプションは、既存の複数値の属性にさらに値を追加します。属性が存在しない場合は、指定した値で新規属性を追加します。

  ```
  add: attribute name
  attribute name: value1
  attribute name: value2...
  ```

次に例を示します。

```
dn:cn=Barbara Fritchy,ou=Sales,o=Oracle,c=US
changetype: modify
add: work-phone
work-phone: 510/506-7000
work-phone: 510/506-7001
```

– **値の削除。***delete* 行のみ記述すると、指定した属性のすべての値が削除されます。属性行を指定した場合は、その属性から特定の値を削除できます。

```
delete: attribute name
[attribute name: value1]
```

次に例を示します。

```
dn: cn=Barbara Fritchy,ou=Sales,o=Oracle,c=US
changetype: modify
delete: home-fax
```

– **値の置換。**このオプションを使用すると、新しく指定した設定で、属性の値をすべて置換できます。

```
replace: attribute name
[attribute name: value1 ...]
```

replace に属性を指定しない場合、ディレクトリは空のセットを追加します。次に、ディレクトリはその空のセットを削除要求と解釈し、エントリから属性を削除することによって対応します。この方法は、存在するかどうかわからない属性を削除する場合に便利です。

次に例を示します。

```
dn: cn=Barbara Fritchy,ou=Sales,o=Oracle,c=US
changetype: modify
replace: work-phone
work-phone: 510/506-7002
```

* changetype: delete

この変更タイプは、エントリを削除するときに使用します。第 1 行でエントリを指定し、第 2 行で changetype に delete を指定しているため、それ以上の入力は必要ありません。

次に例を示します。

```
dn: cn=Barbara Fritchy,ou=Sales,o=Oracle,c=US
changetype: delete
```

* `changetype: modrdn`

  変更タイプに続く行に、次の形式で新規の相対識別名を指定します。

  `newrdn: RDN`

  次に例を示します。

```
dn: cn=Barbara Fritchy,ou=Sales,o=Oracle,c=US
changetype: modrdn
newrdn: cn=Barbara Fritchy-Blomberg
```

属性を単一値として指定するには、LDIF ファイルの属性定義エントリに、空白で囲んだキーワード SINGLE-VALUE を含めます。

例 : ldapmodify を使用した属性の追加

この例では、myAttr と呼ばれる新規属性を追加します。この操作の LDIF ファイルは次のようになります。

```
dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: (1.2.3.4.5.6.7 NAME 'myAttr' DESC 'New attribute definition'
EQUALITY caseIgnoreMatch SYNTAX
'1.3.6.1.4.1.1466.115.121.1.15' )
```

1 行目では、この新規属性の位置を指定する識別名を入力します。すべての属性およびオブジェクト・クラスが cn=subschemasubentry に格納されます。

2 行目と 3 行目は、新規属性を追加するための正しい形式を示します。

最後の行は属性定義です。この最初の部分は、オブジェクト識別子番号 1.2.3.4.5.6.7 です。これは、他のすべてのオブジェクト・クラスおよび属性の中で一意であることが必要です。次の部分は属性の NAME です。このケースでは、属性の NAME は myAttr です。これは引用符で囲む必要があります。次の部分は属性の説明です。引用符の間に任意の説明を入力します。この例の属性定義の最後の部分は、属性に対するオプションの形式化規則です。このケースでは、EQUALITY caseIgnoreMatch の一致規則と Directory String の SYNTAX を追加します。この例では、SYNTAXES の名前 Directory String のかわりにオブジェクト ID 番号 1.3.6.1.4.1.1466.115.121.1.15 が使用されています。

属性情報は、この例のような形式のファイルに格納します。次に、次のコマンドを実行して、Oracle ディレクトリ・サーバーのスキーマに属性を追加します。

```
ldapmodify -h yourhostname -p 389 -D "orcladmin" -w "welcome" -v -f
/tmp/newattr.ldif
```

この ldapmodify コマンドでは、Oracle ディレクトリ・サーバーがポート 389 で実行されており、スーパー・ユーザーのアカウント名が orcladmin で、スーパー・ユーザーのパスワードが welcome です。また、LDIF ファイルが newattr.ldif であることが仮定されています。*yourhostname* と表示されるコンピュータのホスト名を置換します。

LDIF ファイルがあるディレクトリを現在使用中でない場合は、コマンドの最後でファイルにフル・ディレクトリ・パスを入力する必要があります。この例では、LDIF ファイルが /tmp ディレクトリにあることが仮定されています。

ldapmodifymt の構文

ldapmodifymt コマンドライン・ツールを使用すると、複数のエントリを同時に変更できます。

ldapmodifymt は次の構文を使用します。

```
ldapmodifymt -T number_of_threads [arguments] -f file_name
```

file_name は、A-2 ページの「LDAP Data Interchange Format（LDIF）の構文」で説明した仕様に従って作成された LDIF ファイルの名前です。

> **関連項目：** ldapmodifymt で使用されるその他の形式化仕様については、A-32 ページの「ldapmodify の構文」を参照してください。

次の例は、5 つの同時スレッドを使用して、ファイル myentries.ldif 内のエントリを変更しています。

```
ldapmodifymt -T 5 -h node1 -p 3000 -f myentries.ldif
```

> **注意：** ldapmodifymt ツールは、エラー・メッセージを、このコマンドを実行しているディレクトリにあるファイル add.log にログします。

次の表の引数はすべてオプションです。

表 A-14 ldapmodifymt の引数

引数	説明
-a	エントリが追加対象で、入力ファイルが LDIF 形式であることを示します。（ldapadd を実行している場合、このフラグは必要ありません。）
-b	データ・ファイルにバイナリ・ファイル名が含まれていることを指定します。バイナリ・ファイル名はスラッシュで始まります。

表 A-14 ldapmodifymt の引数（続き）

引数	説明
`-c`	エラーが発生しても処理を継続する場合に指定します。エラーはレポートされます。（このオプションを使用しない場合、エラーが発生すると ldapmodify は停止します。）
`-D "binddn"`	ディレクトリに対して認証を行う場合に、*binddn* に指定されているエントリ（認証を必要とするユーザーの識別名）として認証することを指定します。この引数は、`-w` *password* オプションとともに使用します。
`-E "character_set"`	ネイティブ・キャラクタ・セット・エンコーディングを指定します。詳細は、付録 G「ディレクトリにおけるグローバリゼーション・サポート」を参照してください。
`-h ldaphost`	デフォルトのホスト（ローカル・コンピュータ）ではなく、*ldaphost* に接続します。*ldaphost* には、コンピュータ名または IP アドレスを指定します。
`-M`	`ManageDSAIT` 制御をサーバーに送信するようにツールに指示します。`ManageDSAIT` 制御は、参照をクライアントに送信しないようにサーバーに指示します。この指示がない場合、参照エントリが通常のエントリとして戻されます。
`-n`	操作を実際には実行せずに、予測結果を示します。
`-O ref_hop_limit`	クライアントが処理する参照ホップの数を指定します。デフォルト値は 5 です。
`-p ldapport`	TCP ポート *ldapport* 上のディレクトリに接続します。このオプションを指定しない場合は、デフォルト・ポート（389）に接続されます。
`-P wallet_password`	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet のパスワードを指定します。
`-T`	エントリを同時に処理するスレッドの数を設定します。
`-U SSLAuth`	SSL 認証モードを指定します。 ■ 1: SSL 認証なし ■ 2: サーバー認証 ■ 3: クライアントとサーバーの認証
`-v`	冗長モードを指定します。

表 A-14 ldapmodifymt の引数（続き）

引数	説明
`-V ldap_version`	使用する LDAP プロトコルのバージョンを指定します。デフォルト値は 3 で、この場合ツールは LDAP バージョン 3 のプロトコルを使用します。値が 2 の場合、ツールは LDAP バージョン 2 のプロトコルを使用します。
`-w password`	デフォルトの非認証の NULL バインドをオーバーライドします。認証を強制するには、このオプションを -D オプションとともに使用します。
`-W wallet_location`	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet の位置を指定します。たとえば、このパラメータは、UNIX では -W "file:/home/my_dir/my_wallet" と設定します。 また、Windows NT では `-W "file:C:¥my_dir¥my_wallet"` と設定します。

ldapsearch の構文

ldapsearch コマンドライン・ツールを使用すると、ディレクトリ内の特定のエントリを検索および取得できます。

ldapsearch ツールは次の構文を使用します。

```
ldapsearch [arguments] filter [attributes]
```

filter の形式は RFC-2254 に準拠している必要があります。

> **関連項目：** フィルタの形式の標準の詳細は、`http://www.ietf.org` で RFC-2254 を参照してください。

属性は空白で区切ります。属性を何も入力しないと、すべての属性が取り出されます。

注意：

- ldapsearch ツールは、デフォルトでは LDIF 出力を生成しません。ldapsearch コマンドライン・ツールから LDIF 出力を生成するには、`-L` フラグを使用します。
- UNIX シェルでは、アスタリスク（*）などの一部の文字が特殊文字として解釈される場合があります。使用しているシェルに応じて、これらの文字をエスケープする必要があります。

表 A-15 ldapsearch の引数

引数	説明
-b "*basedn*"	検索のためのベース識別名を指定します。この引数は必須です。
-s *scope*	検索有効範囲（base、one-level または sub-tree）を指定します。 ベース : 特定のディレクトリ・エントリを取り出します。この検索範囲の指定とともに、検索基準バーを使用して、属性 `objectClass` とフィルタ `Present` を選択します。 1 レベル : 検索のルートの 1 レベル下のすべてのエントリに検索を制限します。 サブツリー : 検索のルートを含め、サブツリー全体のエントリを検索します。 有効範囲を指定しない場合は、ldapsearch はサブツリーの検索を行います。
-A	属性名のみ取り出します（値は取り出しません）。
-a *deref*	別名参照解除（never、always、search または find）を指定します。
-B	非 ASCII 値を出力します。
-D "*binddn*"	ディレクトリに対して認証を行う場合に、*binddn* に指定されているエントリ（認証を必要とするユーザーの識別名）として認証することを指定します。この引数は、`-w` *password* オプションとともに使用します。
-d *debug level*	指定したレベルにデバッグ・レベルを設定します（10-7 ページの表 10-2 を参照）。
-E "*character_set*"	ネイティブ・キャラクタ・セット・エンコーディングを指定します。詳細は、付録 G「ディレクトリにおけるグローバリゼーション・サポート」を参照してください。
-f *file*	*file* にリストされている検索順を実行します。
-F sep	属性名と値の間に、「=」ではなく「`sep`」を印刷します。
-h *ldaphost*	デフォルトのホスト（ローカル・コンピュータ）ではなく、*ldaphost* に接続します。*ldaphost* には、コンピュータ名または IP アドレスを指定します。
-L	エントリを LDIF 形式で出力します（引数 `-B` の内容も含まれます）。
-l *timelimit*	ldapsearch コマンドが完了するまでの最大待機時間（秒）を指定します。

表 A-15 ldapsearch の引数（続き）

引数	説明
-M	ManageDSAIT 制御をサーバーに送信するようにツールに指示します。ManageDSAIT 制御は、参照をクライアントに送信しないようにサーバーに指示します。この指示がない場合、参照エントリが通常のエントリとして戻されます。
-n	検索を実際には実行せずに、予測結果を示します。
-O *ref_hop_limit*	クライアントが処理する参照ホップの数を指定します。デフォルト値は 5 です。
-p *ldapport*	TCP ポート *ldapport* 上のディレクトリに接続します。このオプションを指定しない場合は、デフォルト・ポート（389）に接続されます。
-P *wallet_password*	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet のパスワードを指定します。
-S *attr*	検索結果を属性 *attr* でソートします。
-t	/tmp のファイルに書き込みます。
-u	わかりやすいエントリ名で出力します。
-U *SSLAuth*	SSL 認証モードを指定します。 ■ 1: SSL 認証なし ■ 2: サーバー認証 ■ 3: クライアントとサーバーの認証
-v	冗長モードを指定します。
-w *passwd*	簡易認証の場合にバインド・パスワードを指定します。
-W *wallet_location*	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet の位置を指定します。たとえば、このパラメータは、UNIX では -W "file:/home/my_dir/*my_wallet*" と設定します。 また、Windows NT では -W "file:C:¥my_dir¥*my_wallet*" と設定します。
-z *sizelimit*	エントリの最大検索数を指定します。
-X	エントリを DSML バージョン 1 の形式で出力します。

ldapsearch フィルタの例

検索コマンドの作成方法を理解するには、次の例を参考にしてください。

例 1: ベース・オブジェクト検索 次の例は、ディレクトリ上でルートからベース・レベルの検索を実行します。

```
ldapsearch -p 389 -h myhost -b "" -s base -v "objectclass=*"
```

- -b で、検索のためのベース識別名（この場合はルート）を指定します。
- -s で、ベース検索（base）、1 レベルの検索（one）またはサブツリー検索（sub）のうちの、いずれの検索かを指定します。
- "objectclass=*" で、検索のフィルタを指定します。

例 2: 1 レベルの検索 次の例は、"ou=HR, ou=Americas, o=IMC, c=US" で開始される 1 レベルの検索を実行します。

```
ldapsearch -p 389 -h myhost -b "ou=HR, ou=Americas, o=IMC, c=US" -s one -v
"objectclass=*"
```

例 3: サブツリー検索 次の例は、サブツリー検索を実行して、"cn=us" で始まる識別名を持つすべてのエントリを戻します。

```
ldapsearch -p 389 -h myhost -b "c=US" -s sub -v "cn=Person*"
```

例 4: サイズ制限を使用する検索 次の例では、一致するエントリが 3 つ以上あっても、実際に取り出すエントリは 2 つのみです。

```
ldapsearch -h myhost -p 389 -z 2 -b "ou=Benefits,ou=HR,ou=Americas,o=IMC,c=US" -s
one "objectclass=*"
```

例 5: 必須の属性での検索 次の例は、一致したエントリの DN 属性値のみを戻します。

```
ldapsearch -p 389 -h myhost -b "c=US" -s sub -v "objectclass=*" dn
```

次の例は、姓（sn）および説明（description）属性値を使用して、識別名のみを取り出します。

```
ldapsearch -p 389 -h myhost -b "c=US" -s sub -v "cn=Person*" dn sn description
```

例 6: 属性オプションでのエントリの検索 次の例では、言語コード属性オプションを指定するオプションのある一般名（cn）属性を使用して、エントリを取り出します。この例の場合には、一般名がフランス語で、R で始まるエントリを取り出します。

```
ldapsearch -p 389 -h myhost -b "c=US" -s sub "cn;lang-fr=R*"
```

John のエントリで、cn;lang-it 言語コード属性オプションに値が設定されていないと想定します。この場合、次の例では John のエントリは戻されません。

```
ldapsearch -p 389 -h myhost -b "c=us" -s sub "cn;lang-it=Giovanni"
```

例 7: 全ユーザー属性および指定した操作属性の検索 次の例は、全ユーザー属性と、createtimestamp および orclguid 操作属性を取り出します。

```
ldapsearch -p 389 -h myhost -b "ou=Benefits,ou=HR,ou=Americas,o=IMC,c=US" -s sub
"cn=Person*" * createtimestamp orclguid
```

次の例は、Anne Smith によって変更されたエントリを取り出します。

```
ldapsearch -h sun1 -b "" "(&(objectclass=*)(modifiersname=cn=Anne
Smith))"
```

次の例は、2001 年 4 月 1 日から 2001 年 4 月 6 日までの間に変更されたエントリを取り出します。

```
ldapsearch -h sun1 -b "" "(&(objectclass=*)(modifytimestamp >= 20000401000000)
(modifytimestamp <= 20000406235959))"
```

注意： modifiersname と modifytimestamp は索引付き属性ではないので、catalog.sh を使用してこれら 2 つの属性に索引を付けてください。前述の 2 つの ldapsearch コマンドを発行する前に、Oracle ディレクトリ・サーバーを再起動してください。

その他の例 : 次の各例は、ホスト sun1 のポート 389 で、識別名 "ou=hr,o=acme,c=us" から開始してサブツリー全体を検索します。

次の例は、objectclass 属性の値を持つすべてのエントリを検索します。

```
ldapsearch -p 389 -h sun1 -b "ou=hr, o=acme, c=us" -s subtree "objectclass=*"
```

次の例は、objectclass 属性の値が orcl で始まるエントリをすべて検索します。

```
ldapsearch -p 389 -h sun1 -b "ou=hr, o=acme, c=us" -s subtree "objectclass=orcl*"
```

次の例は、objectclass 属性が orcl で始まり、cn が foo で始まるエントリを検索します。

```
ldapsearch -p 389 -h sun1 -b "ou=hr, o=acme, c=us" -s subtree
"(&(objectclass=orcl*)(cn=foo*))"
```

次の例は、一般名（cn）が foo ではないエントリを検索します。

```
ldapsearch -p 389 -h sun1 -b "ou=hr, o=acme, c=us" -s subtree "(!(cn=foo))"
```

次の例は、cn が foo で始まるか、あるいは sn が bar で始まるエントリを検索します。

```
ldapsearch -p 389 -h sun1 -b "ou=hr, o=acme, c=us" -s subtree
"(|(cn=foo*)(sn=bar*))"
```

次の例は、employeenumber が 10000 より小か等しいエントリを検索します。

```
ldapsearch -p 389 -h sun1 -b "ou=hr, o=acme, c=us" -s subtree
"employeenumber<=10000"
```

バルク操作コマンドライン・ツールの構文

この項では、次の項目について説明します。

- bulkdelete の構文
- bulkload の構文
- bulkmodify の構文
- ldifwrite の構文

注意： Windows オペレーティング・システムでシェル・スクリプト・ツールを実行するには、次のいずれかの UNIX エミュレーション・ユーティリティが必要です。

- Cygwin 1.3.2.2-1 以上
  サイト：http://sources.redhat.com
- MKS Toolkit 6.1
  サイト：http://www.datafocus.com/

注意： すべてのバルク・ツールでは、ods データベースにアクセスするために、正しいパスワードの入力が要求されます。

bulkdelete の構文

bulkdelete コマンドライン・ツールを使用すると、サブツリーを効率的に削除できます。このツールは、Oracle ディレクトリ・サーバーと Oracle ディレクトリ・レプリケーション・サーバーがともに稼働しているときに使用できます。また、パフォーマンス向上のために、SQL インタフェースを使用します。このリリースでは、bulkdelete ツールは一度に 1 つのノードでのみ動作します。

注意： bulkmodify の起動時にサーバー側エントリ・キャッシュが無効になっていることを確認してください。

このツールは、フィルタベースの削除はサポートしていません。つまり、サブツリーのルート下にあるサブツリー全体が削除されます。ベース識別名が、ディレクトリのインストール時に作成された識別名ではなく、ユーザーが追加した識別名の場合でも削除の対象となります。削除中はサブツリーに対する LDAP アクティビティを制限する必要があります。

bulkdelete ツールは次の構文を使用します。

```
bulkdelete.sh -connect connect_string -base "base_dn" -size number_of_entries
-encode "character_set"
```

表 A-16 bulkdelete の引数

必須の引数	説明
`-connect` *connect_string*	ディレクトリ・データベースに接続するための接続文字列を指定します。この引数は必須です。 **関連項目：**『Oracle9*i* Net Services 管理者ガイド』を参照してください。
`- base "`*base_dn*`"`	削除するサブツリーのベース識別名を指定します。この引数は必須です。
`-size` *number_of_entries*	1 トランザクションとしてコミットされるエントリの数を指定します。
`-encode "`*character_set*`"`	ネイティブ・キャラクタ・セット・エンコーディングを指定します。 **関連項目：**付録 G「ディレクトリにおけるグローバリゼーション・サポート」を参照してください。

bulkload の構文

bulkload コマンドライン・ツールは、多数のエントリをディレクトリ・サーバーにロードする場合に有効です。Oracle SQL*Loader を使用してディレクトリ・エントリをロードします。bulkload ツールは、入力ファイルが LDIF であることを想定しています。

関連項目：

- A-2 ページの「LDAP Data Interchange Format（LDIF）の構文」
- Oracle Internet Directory の旧バージョンから LDIF ファイルをバルク・ロードする場合の orclguids のアップグレードの詳細は、Oracle Application Server 10*g* のアップグレード・ガイドを参照してください。

bulkload ツールは、次のフェーズで操作を実行します。

1. チェック

   チェック・フェーズでは、LDIF ファイルのすべてのエントリが、LDAP スキーマおよび重複するエントリに対して検証されます。バルク・ローダーによってエラーがレポートされた場合、ユーザーは、そのエラーを修正し、bulkload を再試行する必要があります。

2. 生成

   生成フェーズでは、LDIF 入力ファイルが中間ファイルに変換されます。この中間ファイルは、SQL*Loader によって、Oracle Internet Directory ディレクトリ・ストアへのデータのロードに使用されます。

3. ロード

   生成フェーズで生成された中間ファイルが、Oracle Internet Directory ディレクトリ・ストアである Oracle9*i* データベース・サーバーにロードされます。バルク・ローダーは、次の 2 つのタイプのデータのロードをサポートします。

   - 増分モードのロード

     増分モードでは、既存のディレクトリ・データにデータを追加できます。この増分モードは、少量のデータを追加する場合に使用する必要があります。このモードを使用すると、処理速度が他の「追加」メソッドよりも速くなりますが、バルク・モード・ロードほどは速くなりません。このモードでは、バルク・ローダーはカタログ索引の削除および再構築を行いません。かわりに、SQL*Loader を挿入モードで使用して、データをデータベースに追加し、その挿入データによって索引を更新します。

     ここでの少量とは相対的な数で、ディレクトリ内の既存データ、ロードされるデータの量およびロードを処理するハードウェアの機能によって異なります。

     増分モードを起動するには、-append を他のオプションとともに指定する必要があります。

     bulkload を増分モードで使用する場合には、ディレクトリ・サーバーを読取り / 変更モードに切り替える必要があります。読取り / 変更モードでは、検索と変更の操作は可能ですが、識別名の追加、削除および変更操作は禁止されています。

     関連項目： Oracle Directory Manager を使用してアクセス権を設定する方法については、14-21 ページの「タスク 2: 構造型アクセス項目の構成」を参照してください。

- バルク・モードのロード

  バルク・モードでは、大量のエントリをディレクトリに追加可能である必要があります。デフォルトでは、バルク・ローダーはバルク・モードで稼働します。バルク・モードの方が増分モードよりも処理速度が速くなります。

  バルク・モードでは、すべての Oracle Internet Directory サーバー・インスタンスを停止する必要があります。このモードでは、バルク・ローダーは既存の索引を削除し、データのロード後再作成します。データのロードでは、Oracle SQL*Loader のダイレクト・パス・モードが使用されます。

  関連項目： A-9 ページの「Oracle ディレクトリ・サーバー・インスタンスの停止」

4. 索引の作成

   バルク・モードで行われたロードが完了すると、索引が作成されます。また、バルク・ローダー・ツールによって、すべての索引を再作成するオプションも提供されます。このオプションは、前回の索引作成が正常に実行されなかった場合に有効です。

5. ディレクトリ・データ・リカバリ

   bulkload 操作のロード・フェーズで障害が発生すると、ディレクトリ・データが一貫性のない状態のままになっている可能性があります。バルク・ローダーを使用すると、bulkload 起動前の元の状態に戻すことができます。bulkload 実行中に障害が発生した場合は、-recover オプションを使用してディレクトリ・データをリカバリします。

bulkload ツールの使用手順

bulkload ツールは、単一ノード環境および複数ノード環境で使用可能です。

単一ノード環境

バルク・モードでのロード 一般的な使用手順では、Oracle Internet Directory のインストール後、ディレクトリ・データをロードします。LDIF ファイルのスキーマ・エラーをチェックし、中間ファイルを生成して、そのデータを Oracle Internet Directory ディレクトリ・ストアにロードします。通常、parallel オプションを使用すると、ロードと索引作成がパラレルで実行されるため、より速く処理されます。bulkload を起動するには、次の構文を使用します。

```
bulkload.sh -connect <conn_str> -check -generate -load -parallel <LDIF>
```

前述の操作のチェック、生成、ロードは、個別に実行できます。LDIF データが別の Oracle Internet Directory ディレクトリ・ノードのデータの場合は、チェックを省略することもできます。

増分モードまたは付加モードでのロード　すでに LDIF ユーザー・データが格納されている Oracle Internet Directory ディレクトリ・ストアにディレクトリ・エントリを追加する必要がある場合は、増分モードまたは付加モードでロードを行います。通常、このモードを使用すると、他の追加メソッドでエントリをディレクトリに追加するよりも速くロードできます。ただし、bulkload でデータの追加を開始する前に、Oracle Internet Directory LDAP インスタンスを読取り / 変更モードにしておく必要があります。通常、bulkload を起動するには、次の構文を使用します。

```
bulkload.sh -connect <conn_str> -check -generate -load -append <LDIF>
```

索引の作成　bulkload 操作によって、索引の更新または索引の作成が行われます。ただし、サイズ設定が適切でないなどの問題のため、索引が更新または適切に作成されない場合があります。バルク・ローダーには、すべての索引を再作成するオプションが用意されています。bulkload を起動するには、次の構文を使用します。

```
bulkload.sh -connect <conn_str> -index
```

エラーが発生した場合のデータ・リカバリ　ディスクのサイズ設定が適切でないなどの問題のため、bulkload の load フェーズが失敗する場合があります。このようなエラーが発生すると、ディレクトリ・データの一貫性がなくなる可能性があります。このため、バルク・ローダーには、bulkload 起動前の状態にディレクトリ・データをリカバリするオプションが用意されています。

```
bulkload.sh -connect <conn_str> -recover
```

複数ノード環境

バルク・モードのロード　関連するすべての Oracle Internet Directory ノードの接続文字列を指定する必要があります。bulkload を起動するには、次の構文を使用します。

```
bulkload.sh -connect "<conn_str1> <conn_str2> <conn_str3>" -check -generate -load
-parallel <LDIF>
```

バルク・ローダーは、この構文を次のように処理します。

1. すべてのノードのすべての Oracle Internet Directory LDAP サーバーを読取り / 変更モードに切り替えるようにユーザーに求めます。
2. <conn_str1> に対応するノードの Oracle Internet Directory サーバーを停止するようにユーザーに求めます。
3. <cons_str1> に対応するノードで、チェックと生成が実行されます。
4. <conns_str1> に対応するノードで、ロードが実行されます。

5. <conn_str1> に対応するノードの Oracle Internet Directory サーバーを起動するようにユーザーに求めます。
6. すべてのノードに対して手順 2、4、5 が繰り返し実行されます。
7. すべての Oracle Internet Directory LDAP サーバーが読取り / 書込みモードに変更可能になります。

増分モードのロード このモードでのロード方法は、Oracle Internet Directory LDAP サーバーを停止する必要はなく、すべてのサーバーを読取り専用モードにする必要があることを除いて、バルク・モードのロードと同じです。

Oracle Internet Directory 10*g*（9.0.4）でのバルク・ローダーの制限事項

複数ノード環境では、ディレクトリ管理者が、バルク・ローダーの実行前にすべてのノードに同じスキーマが含まれていることを確認する必要があります。

ユーザーが badentry.ldif に不良エントリが記録されているのを確認して、そのエントリを修正しなかった場合は、このデータの一貫性がなくなる可能性があります。

バルク・ローダーのチェック・モードでは、エントリ間の親子関係の欠如はチェックおよびレポートされません。

増分または付加モードは、新規のエントリの追加にのみ使用され、既存のエントリへの新しい属性値の追加には使用されません。

複数ノード環境では、指定された最初の接続文字列がローカル・ノードを指している必要があります。

> **関連項目：** A-2 ページの「LDAP Data Interchange Format（LDIF）の構文」

bulkload ツールの構文

bulkload ツールは次の構文を使用します。

```
bulkload.sh -connect connect_string <[-check] [-generate] [-restore] [-numThread]
[-parallel] [-encode] [-append] [-load] | [-index] | [-recover] absolute_path_to_
LDIF_data_file
```

表 A-17 に、このコマンドの引数を示します。

表 A-17 bulkload.sh の引数

引数	説明	必須
-connect	tnsnames.ora ファイルに定義されているネット・サービス名を指定します。単一ノードでデータをロードする場合は、接続文字列（orcl など）を指定します。複数ノードでデータをロードする場合は、すべてのノードの接続文字列（orcl1 orcl2 orcl3 など）を指定します。 **関連項目：**『Oracle9*i* Net Services 管理者ガイド』を参照してください。	はい
-check	ファイル内の不整合と重複している識別名の存在に関して LDAP スキーマをチェックします。	いいえ
-generate	SQL*Loader を使用した Oracle Internet Directory へのロードに適切な中間ファイルを作成します。	いいえ
-restore	orclguid、creatorsname、createtimestamp などの操作属性が、すでに LDIF ファイルに存在するとします。-generate を指定して bulkload.sh を使用すると、SQL*Loader の出力ファイルに操作属性値が重複して作成されなくなります。-check を指定して bulkload.sh を使用すると、LDIF ファイル内の既存の操作属性値の検出に関連したエラーが発生しなくなります。	いいえ
-numThread n	作成されるスレッドの数を指定します。- numThread は、-generate モードでのみ有効です。デフォルト値はマシンの CPU の数 + 1 です。	いいえ
-parallel	ロードをパラレルで実行するように指定します。-load オプションとともに使用すると有効です。	いいえ
-encode	ネイティブ・キャラクタ・セット・エンコーディングを指定します。 **関連項目：**付録 G「ディレクトリにおけるグローバリゼーション・サポート」を参照してください。	いいえ
-append	付加 / 増分モードを指定します（デフォルトはバルク・モード / 付加）。	いいえ
-load	generate で作成されたファイルを、指定したデータベースにロードします。	いいえ
-index	すべてのカタログ表で索引を再作成します。	いいえ
-recover	bulkload.sh が失敗した場合、元のデータのディレクトリをリカバリします。	いいえ
-file_name	LDIF ファイルの絶対パス。	いいえ

LDIF データ・ファイルのパスは、check または generate 操作時にはフルパスを指定する必要があります。

bulkload をコールする場合、-check、-generate、-load、-recover、-index アクションの 1 つ以上を指定する必要があります。

バルク・ロードを効果的に行うには、特定の組合せのオプションを同時にコールする必要があります。

- -restore フラグは、LDIF ファイルに orclguid、creatorsname などの操作属性が含まれている場合にのみ使用します。
- LDIF データ・ファイルへのパス名を完全に指定し、データ・ファイルを -check または -generate アクションに対して指定する必要があります。
- -numThread は、-generate オプションとともに使用される場合にのみ有効です。
- -parallel は、-load とともにのみコールする必要があります。
- -recover または -index は、他のオプションとともには指定できません。

関連項目： レプリケート環境での複数ノードのバルク・ロードの詳細は、「ディレクトリ・レプリケーション」を参照してください。

レプリケート環境における複数ノードのバルク・ロード

generate オプションでファイルを生成した後、その同じ SQL*Loader ファイルを、load オプションを使用して複数のコンピュータにロードできます。この処理は、新規のレプリカ・ノードを作成するときのみ実行してください。

関連項目： 25-1 ページの「Oracle ディレクトリ・レプリケーションの管理」

レプリケート・ネットワークにおいて、同一データを複数ノードにロードするときは、orclGUID パラメータ（グローバル ID）がノード全体で一貫していることを確認してください。これは、bulkload のデータ・ファイルを 1 回のみ生成（-generate オプションを使用）し、生成した同じデータ・ファイルを他のノードにロード（-load オプションを使用）することによって処理できます。

bulkmodify の構文

bulkmodify コマンドライン・ツールを使用すると、多数の既存エントリを効率的に変更できます。bulkmodify ツールは、次の機能をサポートしています。

- サブツリー・ベースの変更。
- 単一属性フィルタ。たとえば、`objectclass=*`、`objectclass=oneclass` または `telephonenumber=*` などのフィルタを設定できます。
- 属性値の追加と置換。一致するエントリを一括変更します。

bulkmodify ツールは、指定した属性名と値に対して、初期化時にスキーマ・チェックを実行します。次の基準を満たすすべてのエントリが変更されます。

- 指定したサブツリーの下にあること
- 単一のフィルタ条件を満たしていること
- 変更対象の属性を、必須またはオプションとして含んでいること

一括変更処理時に、Oracle ディレクトリ・サーバーと Oracle ディレクトリ・レプリケーション・サーバーが同時に稼働している可能性がありますが、一括変更はレプリケーション・サーバーには影響しません。一括変更は、すべてのレプリカに対して実行する必要があります。

注意： LDIF ファイル・ベースの変更は、bulkmodify ではサポートされていません。このタイプの変更では、エントリごとにスキーマ・チェックを行う必要があるため、既存の ldapmodify ツールを上回るパフォーマンスの向上はありません。

bulkmodify の起動時にサーバー側エントリ・キャッシュが無効になっていることを確認してください。

一括変更中はサブツリーへのユーザー・アクセスを制限する必要があります。必要に応じて、bulkmodify の更新対象のサブツリーに、アクセス制御情報アイテム（**ACI**）制限を適用できます。

bulkmodify は、すでに値が 1 つ存在する単一値の属性に値を追加するためには使用できません。2 つ目の値を追加する場合は、ディレクトリ・スキーマを変更して、その属性を複数値の属性にする必要があります。

bulkmodify ツールは次の構文を使用します。

```
bulkmodify -c connect_string -b "base_dn" {-a|-r} attr_name -v att_value [-f filter]
[-s size]
```

表 A-18 bulkmodify の引数

引数	説明
`-c connect_string`	ディレクトリ・データベースのための接続文字列を指定します。この引数は必須です。 **関連項目：**『Oracle9*i* Net Services 管理者ガイド』を参照してください。
`-b "base_dn"`	変更するサブツリーのベース識別名を指定します。この引数は必須です。
`-a attr_name`	追加する場合に属性名を指定します。この引数は必須です。
`-r attr_name`	置換する場合に属性名を指定します。この引数は必須です。
`-v attr_value`	追加または置換する場合に属性値を指定します。この引数は必須です。
`-f filter`	使用するフィルタを指定します。
`-s number_of_entries`	1 トランザクションとしてコミットされるエントリの数を指定します。指定しない場合、デフォルトは 100 です。
`-E "character_set"`	ネイティブ・キャラクタ・セット・エンコーディングを指定します。詳細は、付録 G「ディレクトリにおけるグローバリゼーション・サポート」を参照してください。

`-f` オプションで指定したフィルタには単一の属性が含まれている必要があります。

フィルタを指定しないと、デフォルトのフィルタ `objectclass=*` が使用されます。

各実行時に、`-a` または `-r` オプションに指定できる属性名は 1 つのみです。

各実行時に、`-v` オプションに指定できる値は 1 つのみです。たとえば、次の bulkmodify コマンドは、マネージャが Anne Smith の全従業員のエントリに、電話番号 408-123-4567 を追加します。

```
bulkmodify -c my_database -b "c=US" -a telephoneNumber -v "408-123-4567" -f
"manager=Anne Smith"
```

bulkmodify プロシージャの完了後、変更されたエントリが確実に読み込まれるように、Oracle Internet Directory サーバーを再起動してください。

ldifwrite の構文

ldifwrite コマンドライン・ツールを使用すると、Oracle Internet Directory に常駐している情報の一部またはすべてを LDIF に変換できます。変換した情報は、レプリケート・ディレクトリの新規ノード、またはバックアップ保管用の別のノードへのロードに使用できます。

注意： ldifwrite ツールの出力には、cn=subschemasubentry、cn=catalogs および cn=changelog entries など、ディレクトリ自体の操作データは含まれません。これらのエントリを LDIF 形式にエクスポートするには、ldapsearch を -L フラグとともに使用します。

---

ldifwrite ツールは、指定した識別名を含めその下の全エントリを処理対象とするサブツリー検索を実行します。

ldifwrite ツールは次の構文を使用します。

```
ldifwrite -c connect_string -b "base_DN" -f file_name
```

表 A-19 ldifwrite の引数

必須の引数	説明
-c *connect_string*	データの取得元であるディレクトリのネット・サービス名を指定します。ネット・サービス名は、tnsnames.ora ファイルに定義されています。この引数は必須です。 **関連項目：**『Oracle9*i* Net Services 管理者ガイド』を参照してください。
-b "*base_dn*"	LDIF 形式で書き出すサブツリーのベース識別名を指定します。この引数は必須です。 ベース識別名がレプリケーション承諾エントリの場合は、LDAP ネーミング・コンテキストの構成に基づいてネーミング・コンテキストの一部をバックアップできます。この場合、構文は次のようになります。 `ldifwrite -c connect string -b "replication agreement DN" -f file name` **関連項目：** 24-33 ページの「部分レプリケーションのフィルタ処理に関する規則」
-f *file_name*	作成する LDIF ファイルの名前を指定します。この引数は必須です。
-E "*character_set*"	ネイティブ・キャラクタ・セット・エンコーディングを指定します。 **関連項目：** G-9 ページの「ldifwrite でのグローバリゼーション・サポートの使用方法」を参照してください。

例 1: 指定したネーミング・コンテキストのすべてのエントリを LDIF ファイルに変換する場合

次の例は、ou=Europe, o=imc, c=us の下の全エントリを output1.ldi ファイルに書き出します。

```
ldifwrite -c nldap -b "ou=Europe, o=imc, c=us" -f output1.ldi
```

引数はすべて必須です。

LDIF ファイルと中間ファイルは、常に現行のディレクトリに書き込まれます。

ldifwrite ツールには、createtimestamp、creatorsname および orclguid など、ディレクトリ内の各エントリの操作属性が含まれます。

Oracle Internet Directory パスワードを要求された場合は、基礎となる ODS ユーザーのパスワードを入力します。デフォルトのパスワードは ods です。

例 2: 指定したネーミング・コンテキストの一部のエントリを LDIF ファイルに変換する場合

この例では、部分レプリケーションに定義された次のネーミング・コンテキスト・オブジェクトを使用します。

```
dn: cn=includednamingcontext000001,
cn=replication namecontext,
orclagreementid=000001,
orclreplicaid=node replica identifier,
cn=replication configuration
orclincludednamingcontexts: c=us
orclexcludednamingcontexts: ou=Americas, c=us
orclexcludedattributes: userpassword
objectclass: top
objectclass: orclreplnamectxconfig
```

この例では、ou=Americas,c=us を除いて、c=us 下のすべてのエントリがバックアップされます。userpassword 属性も除外されます。コマンドは次のようになります。

```
ldifwrite -c connect string -b "cn=includednamingcontext000001,cn=replication
namecontext,orclagreementid=000001,orclreplicaid=node replica
identifier,cn=replication configuration" -f file name
```

レプリケーション管理コマンドライン・ツールの構文

この項では、次の項目について説明します。

レプリケーション競合解消コマンドライン・ツール

レプリケーションの競合が発生すると、Oracle ディレクトリ・レプリケーション・サーバーは変更をリトライ・キューに入れ、そこからの変更の適用を指定された回数だけ再試行します。指定された失敗回数に達した後、レプリケーション・サーバーは変更を管理者操作キューに入れます。レプリケーション・サーバーはそこから長い間隔で変更適用プロセスを繰り返すと同時に、管理者によるアクションを待ちます。

この時点で、次の操作を行う必要があります。

1. 管理者操作キューにある変更を検証します。
2. 競合している変更を調停します。
3. 変更をリトライ・キューに戻すか、パージ・キューに入れます。

このプロセスを支援するツールが 2 つあります。OID 調停ツールを使用すると、競合している変更を同期化できます。管理者操作キュー操作ツールを使用すると、変更を管理者操作キューからリトライ・キューまたはパージ・キューに移動できます。

管理者操作キュー操作ツール

管理者操作キュー操作ツールを使用すると、変更を管理者操作キューからリトライ・キューまたはパージ・キューへ移動できます。パージ・キューへの変更の移動は、変更ログ・エントリの再適用を以降は試みないということを意味します。次の一般的な手順を実行して、管理者操作キューの変更を移動してください。

1. Oracle ディレクトリ・レプリケーション・サーバーを停止します。
2. レプリケーション・ログを分析します。
3. 管理者操作キュー操作ツールを使用して、変更をリトライ・キューまたはパージ・キューへ移動します。詳細は、次項を参照してください。

注意： Windows オペレーティング・システムでシェル・スクリプト・ツールを実行するには、次のいずれかの UNIX エミュレーション・ユーティリティが必要です。

- Cygwin 1.3.2.2-1 以上
  サイト : `http://sources.redhat.com`
- MKS Toolkit 6.1
  サイト : `http://www.datafocus.com/`

管理者操作キューからリトライ・キューへの変更の移動 変更をリトライ・キューへ戻すには、次の構文を使用します。

```
hiqretry.sh -connect connect_string [-start change_number]
[-end change_number] [-equal change_number] -supplier supplier_node
```

引数は、次のとおりです。

表 A-20 管理者操作キューからリトライ・キューへの変更の移動用引数

引数	説明
`-connect` *connect_string*	`tnsnames.ora` ファイルに定義されているネット・サービス名を使用してデータベースに接続します。
`-start` *change_number*	再試行操作の開始変更番号を指定します。このオプションをスキップすると、コマンドは、指定した終了変更番号より小か等しいすべての変更をリトライ・キューに戻します。
`-end` *change_number*	再試行操作の終了変更番号を指定します。このオプションをスキップすると、コマンドは、指定した開始変更番号より大か等しいすべての変更をリトライ・キューに戻します。
`-equal` *change_number*	変更番号を指定します。コマンドは、その変更の競合のみをリトライ・キューに戻します。このオプションは、`-start` または `-end` を使用している場合は指定できません。
`-supplier` *supplier_node*	変更が発生したサプライヤのノードを指定します。

管理者操作キューからパージ・キューへの変更の移動 変更をパージ・キューへ戻すには、次の構文を使用します。

```
hiqpurge.sh -connect connect_string [-start change_number] [-end change_number]
[-equal change_number] -supplier supplier_node
```

引数は、次のとおりです。

表 A-21 管理者操作キューからパージ・キューへの変更の移動用引数

引数	説明
`-connect` *connect_string*	tnsnames.ora ファイルに定義されているネット・サービス名を使用してデータベースに接続します。
`-start` *change_number*	削除操作の開始変更番号を指定します。このオプションをスキップすると、コマンドは、指定した終了変更番号より小か等しいすべての変更をパージ・キューに戻します。
`-end` *change_number*	削除操作の終了変更番号を指定します。このオプションをスキップすると、コマンドは、指定した開始変更番号より大か等しいすべての変更をパージ・キューに戻します。
`-equal` *change_number*	変更番号を指定します。コマンドは、その変更の競合のみをパージ・キューに戻します。このオプションは、`-start` または `-end` を使用している場合は指定できません。
`-supplier` *supplier_node*	変更が発生したサプライヤのノードを指定します。

注意： hiqretry.sh または hiqpurge.sh を使用する場合、変更のすべてを移動しないときには、`-equal` フラグ、または `-start` フラグと `-end` フラグの組合せを指定する必要があります。

例 : 管理者操作キュー操作ツールの使用 次の例は、管理者操作キュー操作ツールの使用方法を示しています。

例 : 変更の再試行と廃棄 レプリケーション・ログを分析した結果、次のように決定したとします。

- サプライヤ・ノード ldap_rep1 からの変更のうち、変更番号 10324 ～ 10579 のものを再試行する
- 変更番号 10581 ～ 10623 の変更を廃棄する

これらを行うために、次の 2 つのコマンドを発行します。

```
hiqretry.sh -connect oiddb1 -start 10324 -end 10579 -supplier ldap_rep1
hiqpurge.sh -connect oiddb1 -start 10581 -end 10623 -supplier ldap_repl
```

最初のコマンドは、ldap_rep1 で発生した変更番号 10324 ～ 10579 の変更をリトライ・キューに戻します。2 番目のコマンドは、サプライヤ ldap_repl で発生した変更番号 10581 ～ 10623 の変更を削除します。

例 : 管理者操作キューからリトライ・キューへの単一の変更の移動　次のコマンドは、変更番号 10519 の変更をリトライ・キューに戻します。

```
hiqretry.sh -connect oiddb1 -equal 10519 -supplier ldap_repl
```

例 : 管理者操作キューからリトライ・キューへの複数の変更の移動　次のコマンドは、変更番号が 10324 より大か等しいすべての変更をリトライ・キューに戻します。

```
hiqretry.sh -connect oiddb1 -start 10324 -supplier ldap_repl
```

次のコマンドは、変更番号が 10579 より小か等しいすべての変更をリトライ・キューに戻します。

```
hiqretry.sh -connect oiddb1 -end 10579 -supplier ldap_repl
```

例 : 管理者操作キューからリトライ・キューへのすべての変更の移動　次のコマンドにはオプションがありません。このコマンドは、サプライヤ ldap_repl で発生したすべての変更を管理者操作キューからリトライ・キューへ移動します。

```
hiqretry.sh -connect oiddb1 -supplier ldap_repl
```

OID 調停ツール

Oracle ディレクトリ・レプリケーション・サーバーが一貫性のないデータを検出した場合、OID 調停ツールを使用して、コンシューマのエントリをサプライヤのエントリと同期化させることができます。その場合、次の一般的な手順を実行します。

1. サプライヤとコンシューマを、読取り専用モードに設定します。
2. サプライヤとコンシューマが安定した状態にあることを確認します。安定した状態にない場合は、更新が完了するまで待ちます。
3. コンシューマ上の一貫性のないエントリまたはサブツリーを識別します。
4. OID 調停ツールを使用して、コンシューマ上の一貫性のないエントリまたはサブツリーを修正します。
5. サプライヤとコンシューマを、読取り / 書込みモードに戻します。

注意 :　Windows オペレーティング・システムでシェル・スクリプト・ツールを実行するには、次のいずれかの UNIX エミュレーション・ユーティリティが必要です。

- Cygwin 1.3.2.2-1 以上
  サイト : `http://sources.redhat.com`
- MKS Toolkit 6.1
  サイト : `http://www.datafocus.com/`

OID 調停ツールは、次の構文を使用します。

```
oidreconcile -h supplier_host -c consumer_host [-P supplier_port] [-p consumer_port]
[-s scope] -b "basedn" -W supplier_password -w consumer_password [-T thread]
```

表 A-22 OID 調停ツールを使用した一貫性のないデータの調停用引数

引数	説明
-h *supplier_host*	サプライヤ・ホスト。コンピュータ名または IP アドレスです。
-c *consumer_host*	コンシューマ・ホスト。コンピュータ名または IP アドレスです。
-P *supplier_port*	サプライヤの TCP ポート。このオプションを指定しない場合は、デフォルト・ポート（389）に接続されます。
-p *consumer_port*	コンシューマの TCP ポート。このオプションを指定しない場合は、デフォルト・ポート（389）に接続されます。
-s *scope*	調停の適用範囲 : サブツリー **注意 :** この引数に base または one-level を指定することはできません。
-b "*basedn*"	調停を実行するエントリの識別名を指定します。
-W *supplier_password*	サプライヤ・ノードのレプリケーション識別名のパスワード。
-w *consumer_password*	コンシューマ・ノードのレプリケーション識別名のパスワード。
-T *thread*	ワーカー・スレッドの数。

OID 調停ツールは指定された識別名を受け取ると、サプライヤとコンシューマ両方の親の識別名の orclGuid を比較します。

両方の親のグローバル識別子（orclGuid）が一致し、オプション -s *subtree* が設定されている場合、OID 調停ツールは次のことを行います。

1. コンシューマ・ノードのサブツリー内のエントリをすべて削除します。
2. サプライヤ・ノードからのエントリでそれらを置換します。

たとえば、次のコマンドは、コンシューマの "ou=hr,o=acme,c=us" から始まるサブツリー全体を対応するサプライヤのサブツリーと置換します。

```
oidreconcile -h supplier_host -P 389 -c consumer_host -p 389
-b "ou=hr,o=acme,c=us" -s subtree -W supplier_password -w consumer_password
```

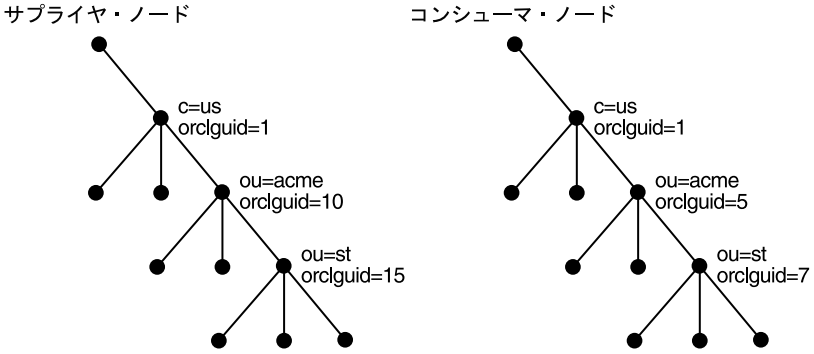
両方の親（"o=acme,c=us"）のグローバル識別子（orclGuid）が一致し、-s subtree が設定されていない場合、OID 調停ツールはコンシューマ・ノードのエントリ自身のみをサプライヤ・ノードからの指定されたエントリと置換します。

たとえば、オプション "-s subtree" が設定されていない次のコマンドは、指定されたエントリ "ou=hr,o=acme,c=us" のみを置換します。

```
oidreconcile -h supplier -P 389 -c consumer -p 389 -b "ou=hr, o=acme, c=us"
-W supplier_password -w consumer_password
```

次の図では、この処理の動作を説明します。

図 A-1 例 : OID 調停ツールの処理



この図は 2 つのディレクトリ情報ツリーを表しています。一方はサプライヤ・ノード、もう一方はコンシューマ・ノードです。サプライヤ・ノードのディレクトリ情報ツリーでは、c=us の orclGuid は 1、o=acme の orclGuid は 10、ou=st の orclGuid は 15 です。コンシューマ・ノードでは、o=acme の orclGuid は 5、ou=st の orclGuid は 7 です。

o=acme,c=us の親の orclGuid、つまり c=us は、サプライヤとコンシューマで一致します。したがって、次のコマンドは、コンシューマの o=acme、c=us の下のすべてのエントリを、サプライヤの対応するエントリと置換します。

```
oidreconcile -h supplier -c consumer -b "o=acme, c=us" -s subtree -W supplier_
password -w consumer_password
```

両方の親の orclGuid が一致しない場合、OID 調停ツールは調停を実行しません。かわりに、orclGuid がサプライヤの同じ祖先クラスのものと一致する、コンシューマの最初の祖先クラスを表示します。

たとえば、前述の例で、次のコマンドを実行するとします。

```
oidreconcile -h supplier -c consumer -b "ou=st, o=acme, c=us" -s subtree
-W supplier_password -w consumer_password
```

このコマンドを実行すると、orclGuid が一致する ou=st の最初の祖先クラスが o=acme,c=us である場合に、メッセージが戻されます。このメッセージは、oidreconcile の basedn 引数として o=acme、c=us を使用する必要があるということを意味します。

レプリケーション環境管理ツール

レプリケーション環境管理ツールを使用して、Oracle Internet Directory レプリケーション構成アクティビティを管理します。

レプリケーション環境管理ツールの機能の詳細は次のとおりです。

- Oracle9*i* Advanced Replication ベースのマルチマスター・レプリケーションを構成します。
- レプリケーション環境をスキャンし、Oracle9*i* Advanced Replication ベースのディレクトリ・レプリケーション・グループのレプリケーション設定の妥当性を検証します。
- Oracle9*i* Advanced Replication ベースのディレクトリ・レプリケーション・グループで発生した問題を修正します。問題を修正できない場合は、管理者が手動で操作できるように障害の発生箇所をレポートします。
- Oracle9*i* Advanced Replication ベースのディレクトリ・レプリケーション・グループのキュー統計、遅延トランザクション・エラー、管理リクエスト・エラーをレポートします。
- Oracle9*i* Advanced Replication ベースのディレクトリ・レプリケーション・グループを再構成します。
- LDAP ベースのレプリケーションを構成します。
- LDAP ベースのディレクトリ・レプリケーション・グループを再構成します。

レプリケーション環境管理ツールの構文は次のとおりです。

```
remtool [ -asrsetup | -addnode | -delnode |-asrverify  |-asrrectify | -chgpwd |
-asrcleanup | -suspendasr | -resumeasr  | -dispqstat  |  -dispasrerr | -paddnode |
-pdelnode  | -pchgpwd  | -presetpwd  | -pchgwalpwd | -pcleanup  ]
[-v] [-connect repadmin_name/password@net_service_name  |
-bind host:port/replication_dn_password]
```

表 A-23 レプリケーション環境管理ツール（remtool）の引数

引数	説明
-connect	Oracle9*i* Advanced Replication 専用。 マスター定義サイト（MDS）またはリモート・マスター・サイト（RMS）のみの接続文字列。-connect オプションが指定されていない場合は、接続の詳細情報の入力を求めるプロンプトが表示されます。 この引数には、次の 3 つの要素が必要です。 ■ レプリケーション管理者の名前 ■ レプリケーション管理者のパスワード ■ マスター定義サイトまたはリモート・マスター・サイトのネット・サービス名
-bind	LDAP ベースのレプリケーション専用。 ディレクトリ・サーバーの詳細情報をバインドします。 この引数には、次の 3 つの要素が必要です。 ■ ディレクトリ・サーバーが実行されているホスト名 ■ ディレクトリ・サーバーがリスニングを行うポート ■ レプリケーション識別名のパスワード
-v	冗長モード。 -v オプションを指定すると、remtool の経過が示されるのみでなく、$ORACLEHOME/ldap/log フォルダに作成された remtool.log に、remtool のすべてのアクションが記録されます。-v オプションを指定しない場合は、remtool の限定されたアクションのみが記録されます。

表 A-24 Oracle9*i* Advanced Replication ベースのディレクトリ・レプリケーション・グループ（remtool）の構成および管理用オプション

引数	説明
-asrsetup	Oracle9*i* Advanced Replication を構成してディレクトリ・レプリケーション・グループ（DRG）を作成します
-addnode	既存の DRG に新規ノードを追加します。
-delnode	Oracle9*i* Advanced Replication を再編成して、既存の DRG からノードを削除します。
-asrverify	DRG の Oracle9*i* Advanced Replication の構成の妥当性を検証します。このオプションは、問題をレポートしますが、修正は行いません。

表 A-24 Oracle9*i* Advanced Replication ベースのディレクトリ・レプリケーション・グループ（remtool）の構成および管理用オプション（続き）

引数	説明
-asrrectify	DRG の Oracle9*i* Advanced Replication の設定の妥当性を検証し、問題がある場合は修正します。
-chgpwd	DRG のすべてのノードに対するレプリケーション管理者データベース・アカウント・パスワードを変更します。
-asrcleanup	DRG の Oracle9*i* Advanced Replication の設定をクリーンアップします。
-suspendasr	DRG のレプリケーション・アクティビティを静止 / 一時停止します。
-resumeasr	DRG のレプリケーション・アクティビティを再開します。
-dispqstat	すべてのノードのキュー統計を表示します。
-dispasrerr	DRG の遅延トランザクション・エラーおよび管理リクエスト・エラーを表示します。

表 A-25 LDAP ベースのディレクトリ・レプリケーション・グループ（remtool）の構成および管理用オプション

引数	説明
-paddnode	DRG に部分レプリカを追加します。
-pdelnode	DRG から部分レプリカを削除します。
-pchgpwd	レプリカのレプリケーション識別名のパスワードを変更します。
-presetpwd	レプリカのレプリケーション識別名のパスワードを再設定します。
-pchgwalpwd	レプリカのレプリケーション識別名のパスワードを Wallet 内のみで変更します。
-pcleanup	DRG の部分レプリケーション設定をクリーンアップします。

例 1: Oracle9*i* Advanced Replication 構成の検証（冗長モード）

この例で、レプリケーション環境管理ツールは次のように動作します。

- DRG の Oracle9*i* Advanced Replication の構成の妥当性を検証します。
- 検証の経過をレポートします。
- 問題は修正しません。

コマンドは次のとおりです。

```
remtool -asrverify -v
```

例 2: Oracle9*i* Advanced Replication 構成の検証（非冗長モード）

この例で、レプリケーション環境管理ツールは次のように動作します。

- DRG の Oracle9*i* Advanced Replication の構成の妥当性を検証します。
- 検証の経過はレポートしません。
- 問題は修正しません。

コマンドは次のとおりです。

```
remtool -asrverify
```

例 3: Oracle9*i* Advanced Replication 構成の検証および問題の修正

この例で、レプリケーション環境管理ツールは次のように動作します。

- DRG の Oracle9*i* Advanced Replication 構成の妥当性を検証します。
- 検証の経過をレポートします。
- 問題を修正します。

コマンドは次のとおりです。

```
remtool -asrrectify -v -connect repadmin/repadmin@node_1.my_company.com
```

-ADDNODE オプション

構文は次のとおりです。

```
remtool -addnode [-v] [-conn[ect] rep_admin_name/rep_admin_password@connectid_of_
mds_or_rms]
```

-ADDNODE オプションの使用方法

1. addnode オプションを使用して、新規ノードを ASRSETUP オプションによって作成された既存の DRG に追加します。
2. 追加対象のノードは空にしておく必要があります。
3. マスター定義サイト（MDS）および他のリモート・マスター・サイト（RMS）上の Oracle Internet Directory プロセスを停止しておく必要があります。
4. addnode プロシージャの完了後、Oracle Internet Directory プロセスを起動できます。
5. このオプションは、新規ノードの SYSTEM ユーザーパスワードが必要です。

例 : -ADDNODE オプション

この例では、MY_HOST1.MY_COMPANY.COM および MY_HOST2.MY_COMPANY.COM で構成される DRG に MY_HOST3.MY_COMPANY.COM が追加されます。これを実行するには、次のコマンドを発行します。

```
remtool -addnode -v -conn repadmin/repadmin@MY_HOST1.MY_COMPANY.COM
```

結果は次のとおりです。

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :

-------- ------------ ---------------------- ------------ ------------ ----
Instance Host Name     Global Name            Version      Replicaid    Site
Name                                                                    Type
-------- ------------ ---------------------- ------------ ------------ ----
rid2      my_host      MY_HOST1.MY_COMPANY.COM  OID 9.0.4.0.0 my_host_rid1  MDS
rid2      my_host      MY_HOST2.MY_COMPANY.COM  OID 9.0.4.0.0 my_host_rid2  RMS
-------- ------------ ---------------------- ------------ ------------ ----
Do you want to continue? [y/n] : y

-------------------------------------------------------------------------------
WARNING:
Make sure that the replication administrator database
account does not exist already in the new node to be
added to the DRG. If the account exists, that
account will be dropped and will be created newly.
-------------------------------------------------------------------------------
Enter global name of new node to be added          : MY_HOST3.MY_COMPANY.COM

Enter SYSTEM user password of new node to be added :
-------------------------------------------------------------------------------
Adding a new node...

MY_HOST3.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST3.MY_COMPANY.COM : Dropping replication administrator repadmin...
MY_HOST3.MY_COMPANY.COM : Creating replication administrator repadmin...
MY_HOST3.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST3.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST3.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST3.MY_COMPANY.COM : Dropping replication group LDAP_REP...
MY_HOST3.MY_COMPANY.COM : Creating purge job...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to MY_HOST1.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to MY_HOST1.MY_COMPANY.COM...
```

```
MY_HOST3.MY_COMPANY.COM : Creating database link to MY_HOST1.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Scheduling push job to MY_HOST1.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to MY_HOST2.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to MY_HOST2.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Creating database link to MY_HOST2.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Scheduling push job to MY_HOST2.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to MY_HOST3.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to MY_HOST3.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Creating database link to MY_HOST3.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Scheduling push job to MY_HOST3.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to MY_HOST3.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to MY_HOST3.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Creating database link to MY_HOST3.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Scheduling push job to MY_HOST3.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Quiescing replication activity...
MY_HOST1.MY_COMPANY.COM : Adding replication site MY_HOST3.MY_COMPANY.COM to
replication group LDAP_REP...
MY_HOST1.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST3.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST1.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST1.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST3.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST1.MY_COMPANY.COM : Resuming replication activity...
MY_HOST1.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST3.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid3...
CORRECTED:
MY_HOST1.MY_COMPANY.COM : "my_host_rid3" hostname has been added to replication
agreement entry.
MY_HOST2.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid3...
CORRECTED:
MY_HOST2.MY_COMPANY.COM : "my_host_rid3" hostname has been added to replication
agreement entry.
MY_HOST3.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST3.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid...
CORRECTED:
MY_HOST3.MY_COMPANY.COM : "my_host_rid" hostname has been added to replication
agreement entry.
MY_HOST3.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid2...
CORRECTED:
MY_HOST3.MY_COMPANY.COM : "my_host_rid2" hostname has been added to replication
agreement entry.
MY_HOST3.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid3...
CORRECTED:
```

```
MY_HOST3.MY_COMPANY.COM : "my_host_rid3" hostname has been added to replication
agreement entry.
MY_HOST1.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST2.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST3.MY_COMPANY.COM : Verifying initialization parameter...
------------------------------------------------------------------------------
Node MY_HOST3.MY_COMPANY.COM has been added to this DRG.
------------------------------------------------------------------------------
Directory Replication Group (DRG) details :

-------- ------------ ---------------------- ------------ ------------ ----
Instance Host Name     Global Name            Version      Replicaid    Site
Name                                                                    Type
-------- ------------ ---------------------- ------------ ------------ ----
rid1     my_host      MY_HOST1.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid1 MDS
rid2     my_host      MY_HOST2.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid2 RMS
rid3     my_host      MY_HOST3.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid3 RMS
-------- ------------ ---------------------- ------------ ------------ ----
```

-ASRSETUP オプション

構文は次のとおりです。

```
remtool -asrsetup [-v]
```

-ASRSETUP オプションの使用方法

1. `-asrsetup` オプションを使用した場合、`-conn[ect]` オプションは無視されます。
2. ユーザーは次の詳細情報の入力を求められます。

   ```
   MDS Globalname
   MDS Password
   globalname of all RMSs
   password of all RMSs
   ```

3. MDS とすべての RMS で、Oracle Internet Directory プロセスを停止しておく必要があります。`ASRSETUP` オプションの完了後、すべての Oracle Internet Directory プロセスとレプリケーション・サーバー・プロセスを起動できます。

例 : -ASRSETUP オプション

この例では、`MY_HOST1.MY_COMPANY.COM` および `MY_HOST2.MY_COMPANY.COM` で構成される DRG が作成されます。これを実行するには、次のコマンドを発行します。

```
remtool -asrsetup -v
```

結果は次のとおりです。

```
-------------------------------------------------------------------------------
ASR Setup for OID Replication
WARNING:
Make sure that the replication administrator that you
enter below does not exist already in any of the nodes
that will be part of the DRG to be created now. If the
user exists, that user will be dropped and will be
created newly.
-------------------------------------------------------------------------------
Enter replication administrator's name       : repadmin

Enter replication administrator's password   :
Reenter replication administrator's password :
Enter Master Definition Site (MDS) details   :
Enter global name of MDS                     : MY_HOST1.MY_COMPANY.COM

Enter SYSTEM user password of MDS            :
Enter Remote Master Site (RMS) details       :
Enter global name of RMS #  1                : MY_HOST2.MY_COMPANY.COM

Enter SYSTEM user password of MDS            :
Are there more Remote Master Sites in the group? [y/n/q] : n

Verify the details you had entered.
-------------------------------------------------------------------------------
Replication administrator's name   : repadmin
Master Definition Site             : MY_HOST1.MY_COMPANY.COM
Remote Master Site #  1            : MY_HOST2.MY_COMPANY.COM
Are these details correct? [y/n/q] : y

-------------------------------------------------------------------------------
ASR setup in progress...

MY_HOST1.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Dropping replication administrator repadmin...
MY_HOST1.MY_COMPANY.COM : Creating replication administrator repadmin...
MY_HOST1.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST1.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST1.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST1.MY_COMPANY.COM : Creating purge job...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to MY_HOST2.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to MY_HOST2.MY_COMPANY.COM...
```

```
MY_HOST1.MY_COMPANY.COM : Creating database link to MY_HOST2.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Scheduling push job to MY_HOST2.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Dropping replication administrator repadmin...
MY_HOST2.MY_COMPANY.COM : Creating replication administrator repadmin...
MY_HOST2.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST2.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST2.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST2.MY_COMPANY.COM : Creating purge job...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to MY_HOST1.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to MY_HOST1.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Creating database link to MY_HOST1.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Scheduling push job to MY_HOST1.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping replication group LDAP_REP...
MY_HOST1.MY_COMPANY.COM : Creating replication group LDAP_REP...
MY_HOST1.MY_COMPANY.COM : Adding object TABLE ODS.ASR_CHG_LOG to replication group
LDAP_REP...
MY_HOST1.MY_COMPANY.COM : Generating replication support for TABLE ODS.ASR_CHG_
LOG...
MY_HOST1.MY_COMPANY.COM : Adding object TABLE ODS.ODS_CHG_STAT to replication group
LDAP_REP...
MY_HOST1.MY_COMPANY.COM : Generating replication support for TABLE ODS.ODS_CHG_
STAT...
MY_HOST2.MY_COMPANY.COM : Dropping replication group LDAP_REP...
MY_HOST1.MY_COMPANY.COM : Adding replication site MY_HOST2.MY_COMPANY.COM to
replication group LDAP_REP...
MY_HOST1.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST2.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST1.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST1.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST2.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST1.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST2.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST1.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST2.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST1.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST2.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST1.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Inserting replication agreement entry my_host_...
CORRECTED:
MY_HOST1.MY_COMPANY.COM : "my_host_rid" hostname has been added to replication
agreement entry.
```

```
MY_HOST1.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid2...
CORRECTED:
MY_HOST1.MY_COMPANY.COM : "my_host_rid2" hostname has been added to replication
agreement entry.
MY_HOST2.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid...
CORRECTED:
MY_HOST2.MY_COMPANY.COM : "my_host_rid1" hostname has been added to replication
agreement entry.
MY_HOST2.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid2...
CORRECTED:
MY_HOST2.MY_COMPANY.COM : "my_host_rid2" hostname has been added to replication
agreement entry.
MY_HOST1.MY_COMPANY.COM : Resuming replication activity...
------------------------------------------------------------------------------
ASR setup has been configured successfully.
------------------------------------------------------------------------------
Directory Replication Group (DRG) details :

-------- ------------ ---------------------- ------------ ------------ ----
Instance Host Name     Global Name            Version      Replicaid    Site
Name                                                                    Type
-------- ------------ ---------------------- ------------ ------------ ----
rid1      my_host      MY_HOST1.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid1  MDS
rid2      my_host      MY_HOST2.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid2  RMS
-------- ------------ ---------------------- ------------ ------------ ----
```

-CHGPWD オプション

構文は次のとおりです。

```
remtool -chgpwd [-v] [-conn[ect] rep_admin_name/rep_admin_password@connectid_of_mds_
or_rms]
```

1. ASRSETUP プロシージャによって作成された DRG のレプリケーション管理者のパスワードを変更する場合に使用します。

   ```
   created by ASRSETUP procedure.
   ```

2. ASR ベースのレプリケーションでは、すべてのノードで repadmin パスワードは同じです。このオプションによって、すべてのノードでレプリケーション管理者データベース・アカウントのパスワードが変更されます。

例 : -CHGPWD オプション

この例では、MY_HOST1.MY_COMPANY.COM および MY_HOST2.MY_COMPANY.COM で構成される DRG のレプリケーション管理者のパスワードが変更されます。これを実行するには、次のコマンドを発行します。

```
remtool -chgpwd -v -conn repadmin/repadmin@MY_HOST1.MY_COMPANY.COM
```

結果は次のとおりです。

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :

-------- ------------ ---------------------- ------------ ------------ ----
Instance Host Name     Global Name            Version      Replicaid    Site
Name                                                                    Type
-------- ------------ ---------------------- ------------ ------------ ----
rid1       my_host     MY_HOST1.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid1  MDS
rid2       my_host     MY_HOST2.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid2  RMS
-------- ------------ ---------------------- ------------ ------------ ----
Enter new password of the replication administrator   :
Reenter new password of the replication administrator :
------------------------------------------------------------------------------
Changing the password of all nodes...

MY_HOST1.MY_COMPANY.COM : Changing password of replication administrator repadmin...
MY_HOST2.MY_COMPANY.COM : Changing password of replication administrator repadmin...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to MY_HOST2.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to MY_HOST2.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Creating database link to MY_HOST2.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to MY_HOST1.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to MY_HOST1.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Creating database link to MY_HOST1.MY_COMPANY.COM...
------------------------------------------------------------------------------
Password has been changed.
------------------------------------------------------------------------------
```

-DELNODE オプション

構文は次のとおりです。

```
remtool -delnode [-v] [-conn[ect] rep_admin_name/rep_admin_password@connectid_ of_
mds_or_rms]
```

-DELNODE オプションの使用方法

1. -DELNODE オプションを使用して、ASRSETUP オプションによって作成された DRG からノードを削除します。
2. 削除対象のノードのグローバル名を指定する必要があります。
3. DRG のすべてのノードで、Oracle Internet Directory プロセスを停止しておく必要があります。
4. -DELNODE オプションを使用して、DRG から RMS のみを削除できます。
5. -DELNODE オプションを使用して、DRG から MDS は削除できません。
6. -DELNODE オプションを使用して、2 つのノード（MDS と RMS を 1 つずつ）のみが含まれる DRG から RMS を削除することもできます。削除すると、DRG には MDS のみが含まれます。ユーザーは、後で、この DRG にマルチマスター・ノードを追加できます。
7. remtool は、-DELNODE オプションを指定して起動した場合、DRG のいずれかのノードが稼働していないことを検出すると、そのノードを削除対象として選択します。

例 1: -DELNODE オプション

この例では、MY_HOST1.MY_COMPANY.COM、MY_HOST2.MY_COMPANY.COM、MY_HOST3.MY_COMPANY.COM で構成される DRG から MY_HOST3.MY_COMPANY.COM が削除されます。これを実行するには、次のコマンドを発行します。

```
remtool -delnode -v -conn repadmin/repadmin@MY_HOST1.MY_COMPANY.COM
```

結果は次のとおりです。

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
MY_HOST3.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :

-------- ------------ ---------------------- ------------ ------------ ----
Instance Host Name     Global Name            Version      Replicaid    Site
Name                                                                    Type
-------- ------------ ---------------------- ------------ ------------ ----
rid1      my_host      MY_HOST1.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid1  MDS
rid2      my_host      MY_HOST2.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid2  RMS
rid3      my_host      MY_HOST3.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid3  RMS
-------- ------------ ---------------------- ------------ ------------ ----
Do you want to continue? [y/n] : y

Enter globalname of node to be deleted : MY_HOST3.MY_COMPANY.COM

------------------------------------------------------------------------------
Deleting an existing node...
```

```
MY_HOST1.MY_COMPANY.COM : Dropping replication site MY_HOST3.MY_COMPANY.COM from
replication group LDAP_REP...
MY_HOST3.MY_COMPANY.COM : Dropping replication group LDAP_REP...
MY_HOST3.MY_COMPANY.COM : Unscheduling push job to MY_HOST1.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Unscheduling push job to MY_HOST2.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to MY_HOST1.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to MY_HOST2.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to MY_HOST1.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to MY_HOST2.MY_COMPANY.COM...
Enter "SYSTEM" user password for "MY_HOST3.MY_COMPANY.COM" database at "my_host"
host :
MY_HOST3.MY_COMPANY.COM : Dropping replication administrator repadmin...
MY_HOST1.MY_COMPANY.COM : Unscheduling push job to MY_HOST3.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to MY_HOST3.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to MY_HOST3.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Unscheduling push job to MY_HOST3.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to MY_HOST3.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to MY_HOST3.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Deleting replication agreement entry my_host_rid3...
CORRECTED:
MY_HOST1.MY_COMPANY.COM : "my_host_rid3" hostname has been removed from replication
agreement entry as it is not part of DRG or was repeated.
MY_HOST2.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Deleting replication agreement entry my_host_rid3...
CORRECTED:
MY_HOST2.MY_COMPANY.COM : "my_host_rid3" hostname has been removed from replication
agreement entry as it is not part of DRG or was repeated.
--------------------------------------------------------------------------------
Node MY_HOST3.MY_COMPANY.COM has been deleted from this DRG.
--------------------------------------------------------------------------------
Directory Replication Group (DRG) details :

-------- ------------- ---------------------- ------------- ------------- ----
Instance Host Name     Global Name            Version       Replicaid     Site
Name                                                                      Type
-------- ------------- ---------------------- ------------- ------------- ----
rid1     my_host       MY_HOST1.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid1  MDS
rid2     my_host       MY_HOST2.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid2  RMS
-------- ------------- ---------------------- ------------- ------------- ----

================================================================================
```

例 2: -DELNODE オプション

この例では、MY_HOST1.MY_COMPANY.COM および MY_HOST2.MY_COMPANY.COM で構成される DRG から MY_HOST2.MY_COMPANY.COM が削除されます。これを実行するには、次のコマンドを発行します。

```
remtool -delnode -v -conn repadmin/repadmin@MY_HOST1.MY_COMPANY.COM
```

結果は次のとおりです。

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :

-------- ------------ ---------------------- ------------ ------------ ----
Instance Host Name     Global Name            Version      Replicaid    Site
Name                                                                    Type
-------- ------------ ---------------------- ------------ ------------ ----
rid1     my_host      MY_HOST1.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid1  MDS
rid2     my_host      MY_HOST2.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid2  RMS
-------- ------------ ---------------------- ------------ -----------------
Do you want to continue? [y/n] : y

Enter globalname of node to be deleted : MY_HOST2.MY_COMPANY.COM

------------------------------------------------------------------------------
Deleting an existing node...

MY_HOST1.MY_COMPANY.COM : Dropping replication site MY_HOST2.MY_COMPANY.COM from
replication group LDAP_REP...
MY_HOST2.MY_COMPANY.COM : Dropping replication group LDAP_REP...
MY_HOST2.MY_COMPANY.COM : Unscheduling push job to MY_HOST1.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to MY_HOST1.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to MY_HOST1.MY_COMPANY.COM...
Enter "SYSTEM" user password for "MY_HOST2.MY_COMPANY.COM" database at "my_host"
host :
MY_HOST2.MY_COMPANY.COM : Dropping replication administrator repadmin...
MY_HOST1.MY_COMPANY.COM : Unscheduling push job to MY_HOST2.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to MY_HOST2.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to MY_HOST2.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Deleting replication agreement entry my_host_rid2...
CORRECTED:
MY_HOST1.MY_COMPANY.COM : "my_host_rid2" hostname has been removed from replication
agreement entry as it is not part of DRG or was repeated.
------------------------------------------------------------------------------
Node MY_HOST2.MY_COMPANY.COM has been deleted from this DRG.
```

```
--------------------------------------------------------------------------------
Directory Replication Group (DRG) details :

-------- ------------ ---------------------- ------------ ------------ ----
Instance Host Name     Global Name            Version      Replicaid    Site
Name                                                                    Type
-------- ------------ ---------------------- ------------ ------------ ----
rid1      my_host       MY_HOST1.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid1  MDS
-------- ------------ ---------------------- ------------ ------------ ----
Warning : This replication group has only one node.
```

-ASRCLEANUP オプション

構文は次のとおりです。

```
remtool -asrcleanup [-v] [-conn[ect] rep_admin_name/rep_admin_password@connectid_of_
mds_or_rms]
```

-ASRCLEANUP オプションの使用方法

1. -ASRCLEANUP オプションを使用して、既存の ASR 設定をクリーンアップします。
2. -ASRCLEANUP オプションを使用して、不具合のある ASR 設定もクリーンアップできます。
3. -ASRCLEANUP オプションは、レプリケーションに関連するすべてのサイトの SYSTEM パスワードの入力をユーザーに要求します。

例 1: -ASRCLEANUP オプション

この例では、MY_HOST1.MY_COMPANY.COM および MY_HOST2.MY_COMPANY.COM で構成される DRG から ASR 設定がクリーンアップされます。これを実行するには、次のコマンドを発行します。

```
remtool -asrcleanup -v
```

結果は次のとおりです。

```
Enter replication administrator's name       : repadmin

Enter replication administrator's password   :
Enter global name of MDS                     : my_host1.my_company.com

MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :

-------- ------------ ---------------------- ------------ ------------ ----
Instance Host Name     Global Name            Version      Replicaid    Site
Name                                                                    Type
```

```
-------- ------------- ---------------------- ------------- ------------- ----
rid1      my_host       MY_HOST1.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid1  MDS
rid2      my_host       MY_HOST2.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid2  RMS
-------- ------------- ---------------------- ------------- ------------- ----
Do you want to continue? [y/n] : y

--------------------------------------------------------------------------------
Cleaning up...

MY_HOST1.MY_COMPANY.COM : Dropping replication site MY_HOST2.MY_COMPANY.COM from
replication group LDAP_REP...
MY_HOST2.MY_COMPANY.COM : Dropping replication group LDAP_REP...
MY_HOST2.MY_COMPANY.COM : Unscheduling push job to MY_HOST1.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to MY_HOST1.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to MY_HOST1.MY_COMPANY.COM...
Enter "SYSTEM" user password for "MY_HOST2.MY_COMPANY.COM" database at "my_host"
host :
MY_HOST2.MY_COMPANY.COM : Dropping replication administrator repadmin...
MY_HOST1.MY_COMPANY.COM : Dropping replication group LDAP_REP...
MY_HOST1.MY_COMPANY.COM : Unscheduling push job to MY_HOST2.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to MY_HOST2.MYCOMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to MY_HOST2.MY_COMPANY.COM...
Enter "SYSTEM" user password for "MY_HOST1.MY_COMPANY.COM" database at "my_host"
host :
MY_HOST1.MY_COMPANY.COM : Dropping replication administrator repadmin...
--------------------------------------------------------------------------------
ASR setup has been cleaned up.
--------------------------------------------------------------------------------
```

-ASRRECTIFY オプション

構文は次のとおりです。

```
remtool -asrrectify [-v] [-conn[ect] rep_admin_name/rep_admin_password@connectid_of_
mds_or_rms]
```

-ASRRECTIFY オプションの使用方法

1. -ASRRECTIFY オプションを使用して、Oracle9*i* Advanced Replication 設定の問題を検出し、修正します。
2. -ASRRECTIFY オプションはエラーのレポートおよび修正を行います。
3. このオプションを実行する前に Oracle Internet Directory サーバーを停止することをお薦めします。

4. -ASRRECTIFY オプションを使用するには、すべてのノードが稼働中である必要があります。いずれかのノードが稼働していない場合、-ASRRECTIFY オプションは正常に実行されません。
5. 必要に応じて、SYSTEM ユーザー・パスワードの入力を求めるプロンプトが表示されます。

例 1: -ASRRECTIFY オプション

この例では、MY_HOST1.MY_COMPANY.COM および MY_HOST2.MY_COMPANY.COM で構成される DRG で ASR 設定エラーが検出され、修正されます。これを実行するには、次のコマンドを発行します。

```
remtool -asrrectify -v -conn repadmin/repadmin@my_host1.my_company.com

MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :

-------- ------------- ---------------------- ------------- ------------- ----
Instance Host Name     Global Name            Version       Replicaid     Site
Name                                                                      Type
-------- ------------- ---------------------- ------------- ------------- ----
rid1      my_host      MY_HOST1.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid1  MDS
rid2      my_host      MY_HOST2.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid2  RMS
-------- ------------- ---------------------- ------------- ------------- ----
Do you want to continue? [y/n] : y

------------------------------------------------------------------------------
Rectifying ASR setup...

MY_HOST1.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST2.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST1.MY_COMPANY.COM : Verifying replication administrator roles...
MY_HOST2.MY_COMPANY.COM : Verifying replication administrator roles...
MY_HOST1.MY_COMPANY.COM : Verifying database links...
MY_HOST2.MY_COMPANY.COM : Verifying database links...
MY_HOST1.MY_COMPANY.COM : Verifying purge job...
MY_HOST2.MY_COMPANY.COM : Verifying purge job...
MY_HOST1.MY_COMPANY.COM : Verifying scheduled links...
MY_HOST2.MY_COMPANY.COM : Verifying scheduled links...
MY_HOST1.MY_COMPANY.COM : Verifying availability of replication objects...
MY_HOST2.MY_COMPANY.COM : Verifying availability of replication objects...
MY_HOST1.MY_COMPANY.COM : Verifying replication group...
MY_HOST1.MY_COMPANY.COM : Quiescing replication activity...
MY_HOST1.MY_COMPANY.COM : Adding object TABLE ODS.ASR_CHG_LOG to replication group
LDAP_REP...
MY_HOST1.MY_COMPANY.COM : Generating replication support for TABLE ODS.ASR_CHG_
```

```
LOG...
CORRECTED:
MY_HOST1.MY_COMPANY.COM : Replication support has been generated for TABLE ODS.ASR_
CHG_LOG.
MY_HOST1.MY_COMPANY.COM : Quiescing replication activity...
MY_HOST1.MY_COMPANY.COM : Adding object TABLE ODS.ODS_CHG_STAT to replication group
LDAP_REP...
MY_HOST1.MY_COMPANY.COM : Generating replication support for TABLE ODS.ODS_CHG_
STAT...
CORRECTED:
MY_HOST1.MY_COMPANY.COM : Replication support has been generated for TABLE ODS.ODS_
CHG_STAT.
MY_HOST1.MY_COMPANY.COM : Resuming replication activity...
MY_HOST2.MY_COMPANY.COM : Verifying replication group...
MY_HOST1.MY_COMPANY.COM : Resuming replication activity...
MY_HOST1.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying replication agreement entry...

--------------------  -----  -----  -----  -----  -----  -----  -----
DB Name               Init   Repl   DB     Purge  Sch.   Repl   Repl
                      Param  Admin  Links  Job    Links  Group  Agrmt
                             Role                             Entry
--------------------  -----  -----  -----  -----  -----  -----  -----
MY_HOST1.MY_COMPANY.  Chkd   Chkd   Chkd   Chkd   Chkd   Crtd   Chkd
MY_HOST2.MY_COMPANY.  Chkd   Chkd   Chkd   Chkd   Chkd   Chkd   Chkd
--------------------  -----  -----  -----  -----  -----  -----  -----
Legends :
  Chkd  - Checked. No errors.
  Crtd  - ASR setup errors were found and corrected.
  Err   - Error occurred while doing ASR setup verification.
  NCrtd - ASR setup has errors, but not corrected.
--------------------------------------------------------------------------------
Summary of findings:
CORRECTED:
MY_HOST1.MY_COMPANY.COM : Replication support has been generated for TABLE ODS.ASR_
CHG_LOG.

CORRECTED:
MY_HOST1.MY_COMPANY.COM : Replication support has been generated for TABLE ODS.ODS_
CHG_STAT.
--------------------------------------------------------------------------------
```

例 2: -ASRRECTIFY オプション

この例では、MY_HOST1.MY_COMPANY.COM および MY_HOST2.MY_COMPANY.COM で構成される DRG で ASR 設定エラーが削除され、修正されます。ここで、remtool は、ユーザーが ASR の設定後に MY_HOST2.MY_COMPANY.COM のグローバル名を NEWNAME.MY_COMPANY.COM に変更していることを検出します。remtool は、このエラーを修正後、他のチェックを続行します。これを実行するには、次のコマンドを発行します。

```
remtool -asrrectify -v -conn repadmin/repadmin@my_host1.my_company.com
```

結果は次のとおりです。

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
Enter "SYSTEM" user password for "MY_HOST2.MY_COMPANY.COM" database at "my_host"
host :
NEWNAME.MY_COMPANY.COM : Renaming global name to MY_HOST2.MY_COMPANY.COM (instance
name : rid2, hostname : my_host)
CORRECTED:
MY_HOST2.MY_COMPANY.COM : Global name of database "rid2" at host "my_host" has been
changed to MY_HOST2.MY_COMPANY.COM.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
CORRECTED:
MY_HOST2.MY_COMPANY.COM : Global name of database "rid2" at host "my_host" has been
changed to MY_HOST2.MY_COMPANY.COM.
Directory Replication Group (DRG) details :

-------- ------------- ---------------------- ------------- ------------- ----
Instance Host Name     Global Name            Version       Replicaid     Site
Name                                                                      Type
-------- ------------- ---------------------- ------------- ------------- ----
rid1      my_host      MY_HOST1.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid1  MDS
rid2      my_host      MY_HOST2.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid2  RMS
-------- ------------- ---------------------- ------------- ------------- ----
Do you want to continue? [y/n] : y

-------------------------------------------------------------------------------
Rectifying ASR setup...

MY_HOST1.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST2.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST1.MY_COMPANY.COM : Verifying replication administrator roles...
MY_HOST2.MY_COMPANY.COM : Verifying replication administrator roles...
MY_HOST1.MY_COMPANY.COM : Verifying database links...
MY_HOST2.MY_COMPANY.COM : Verifying database links...
MY_HOST1.MY_COMPANY.COM : Verifying purge job...
MY_HOST2.MY_COMPANY.COM : Verifying purge job...
MY_HOST1.MY_COMPANY.COM : Verifying scheduled links...
MY_HOST2.MY_COMPANY.COM : Verifying scheduled links...
```

```
MY_HOST1.MY_COMPANY.COM : Verifying availability of replication objects...
MY_HOST2.MY_COMPANY.COM : Verifying availability of replication objects...
MY_HOST1.MY_COMPANY.COM : Verifying replication group...
MY_HOST1.MY_COMPANY.COM : Resuming replication activity...
MY_HOST2.MY_COMPANY.COM : Verifying replication group...
MY_HOST1.MY_COMPANY.COM : Resuming replication activity...
MY_HOST1.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying replication agreement entry...

--------------------  -----  -----  -----  -----  -----  -----  -----
DB Name               Init   Repl   DB     Purge  Sch.   Repl   Repl
                      Param  Admin  Links  Job    Links  Group  Agrmt
                             Role                             Entry
--------------------  -----  -----  -----  -----  -----  -----  -----
MY_HOST1.MY_COMPANY.  Chkd   Chkd   Chkd   Chkd   Chkd   Chkd   Chkd
MY_HOST2.MY_COMPANY.  Chkd   Chkd   Chkd   Chkd   Chkd   Chkd   Chkd
--------------------  -----  -----  -----  -----  -----  -----  -----
Legends :
  Chkd  - Checked. No errors.
  Crtd  - ASR setup errors were found and corrected.
  Err   - Error occurred while doing ASR setup verification.
  NCrtd - ASR setup has errors, but not corrected.
--------------------------------------------------------------------------------
```

-ASRVERIFY オプション

構文は次のとおりです。

```
remtool -asrverify [-v] [-conn[ect] rep_admin_name/rep_admin_password@connectid_of_
mds_or_rms]
```

-ASRVERIFY オプションの使用方法

1. このオプションは、ASR 設定の問題の検出にのみ使用されます。エラーをレポートしますが、修正は行いません。
2. このオプションは、Oracle Internet Directory サーバーの稼働中に実行できます。
3. いずれかのノードで、レプリケーション管理者アカウントが誤って削除された場合、`-asrverify`" オプションは正常に実行されません。この場合は、`-asrrectify` オプションを使用して、レプリケーション管理者アカウントを作成し、DRG に追加できます。
4. チェック対象の DRG のいずれかのノードのレプリケーション管理者アカウントのパスワードが誤って変更された場合、`-asrverify` オプションは正常に実行されません。この場合は、`-asrrectify` オプションを使用して、レプリケーション管理者アカウントを変更し、DRG に追加できます。

5. Oracle9*i* Advanced Replication 設定後にいずれかのノードのグローバル名が変更されると、-asrverify オプションは、エラーをレポートして停止します。-asrrectify オプションを使用して、前のグローバル名に戻し、他の問題を修正できます。
6. このオプションを実行するには、すべてのノードが稼働中である必要があります。

例 1: -ASRVERIFY オプション

この例では、2 つのノードで構成される DRG で ASR 設定のエラーが検出されます。これを実行するには、次のコマンドを発行します。

```
remtool -asrverify -v -conn repadmin/repadmin@my_host1.my_company.com
```

結果は次のとおりです。

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :

-------------------- ---------------------- ------------ ------------ ----
Instance Host Name     Global Name             Version       Replicaid     Site
Name                                                                       Type
-------------------- ---------------------- ------------ ------------ ----
rid1     my_host      MY_HOST1.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid1   MDS
rid2     my_host      MY_HOST2.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid2   RMS
------------------------------------------- ------------ -----------------
--------------------------------------------------------------------------------
Verifying ASR setup...

MY_HOST1.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST2.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST1.MY_COMPANY.COM : Verifying replication administrator roles...
MY_HOST2.MY_COMPANY.COM : Verifying replication administrator roles...
MY_HOST1.MY_COMPANY.COM : Verifying database links...
MY_HOST2.MY_COMPANY.COM : Verifying database links...
MY_HOST1.MY_COMPANY.COM : Verifying purge job...
MY_HOST2.MY_COMPANY.COM : Verifying purge job...
MY_HOST1.MY_COMPANY.COM : Verifying scheduled links...
MY_HOST2.MY_COMPANY.COM : Verifying scheduled links...
MY_HOST1.MY_COMPANY.COM : Verifying availability of replication objects...
MY_HOST2.MY_COMPANY.COM : Verifying availability of replication objects...
MY_HOST1.MY_COMPANY.COM : Verifying replication group...
ASR SETUP ERROR/WARNING:
MY_HOST1.MY_COMPANY.COM : Replication support is not available for TABLE ODS.ASR_
CHG_LOG.
ASR SETUP ERROR/WARNING:
MY_HOST1.MY_COMPANY.COM : Replication support is not available for TABLE ODS.ODS_
CHG_STAT.
MY_HOST2.MY_COMPANY.COM : Verifying replication group...
```

```
ASR SETUP ERROR/WARNING:
MY_HOST2.MY_COMPANY.COM : Replication support is not available for TABLE ODS.ASR_
CHG_LOG.
ASR SETUP ERROR/WARNING:
MY_HOST2.MY_COMPANY.COM : Replication support is not available for TABLE ODS.ODS_
CHG_STAT.
MY_HOST1.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying replication agreement entry...

--------------------  -----  -----  -----  -----  -----  -----  -----
DB Name               Init   Repl   DB     Purge  Sch.   Repl   Repl
                      Param  Admin  Links  Job    Links  Group  Agrmt
                             Role                             Entry
--------------------  -----  -----  -----  -----  -----  -----  -----
MY_HOST1.MY_COMPANY.  Chkd   Chkd   Chkd   Chkd   Chkd   NCrtd  Chkd
MY_HOST2.MY_COMPANY.  Chkd   Chkd   Chkd   Chkd   Chkd   NCrtd  Chkd
--------------------  -----  -----  -----  -----  -----  -----  -----
Legends :
  Chkd  - Checked. No errors.
  Crtd  - ASR setup errors were found and corrected.
  Err   - Error occurred while doing ASR setup verification.
  NCrtd - ASR setup has errors, but not corrected.
--------------------------------------------------------------------------------
Summary of findings:
ASR SETUP ERROR/WARNING:
MY_HOST1.MY_COMPANY.COM : Replication support is not available for TABLE ODS.ASR_
CHG_LOG.

ASR SETUP ERROR/WARNING:
MY_HOST1.MY_COMPANY.COM : Replication support is not available for TABLE ODS.ODS_
CHG_STAT.

ASR SETUP ERROR/WARNING:
MY_HOST2.MY_COMPANY.COM : Replication support is not available for TABLE ODS.ASR_
CHG_LOG.

ASR SETUP ERROR/WARNING:
MY_HOST2.MY_COMPANY.COM : Replication support is not available for TABLE ODS.ODS_
CHG_STAT.
--------------------------------------------------------------------------------
```

-DISPASRERR オプション

構文は次のとおりです。

```
remtool -dispasrerr [-v] [-conn[ect] rep_admin_name/rep_admin_password@connectid_of_
mds_or_rms]
```

-DISPASRERR オプションの使用方法

1. このオプションは、DRG 内の ASR エラーの表示に使用されます。
2. このオプションによって、ASR 管理リクエスト・エラーと遅延トランザクション・エラーが表示されます。

例 : -DISPASRERR オプション

この例では、MY_HOST1.MY_COMPANY.COM および MY_HOST2.MY_COMPANY.COM で構成される DRG の ASR エラーがレポートされます。これを実行するには、次のコマンドを発行します。

```
remtool -dispasrerr -v -conn repadmin/repadmin@my_host1.my_company.com

MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :

-------- ------------ ---------------------- ------------ ------------ ----
Instance Host Name     Global Name            Version      Replicaid    Site
Name                                                                    Type
-------- ------------ ---------------------- ------------ ------------ ----
rid      my_host      MY_HOST1.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid1 MDS
rid2     my_host      MY_HOST2.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid2 RMS
-------- ------------ ---------------------- ------------ ------------ ----
--------------------------------------------------------------------------------
Following administrative request errors were found at MY_HOST1.MY_COMPANY.COM

-------------------  -------------------  ------------------------------
Admin request        Request raised at    Error
raised by
-------------------  -------------------  ------------------------------
REPADMIN             MY_HOST1.MY_COMPANY.  ORA-23309: object ODS.ASR_CHG_L
REPADMIN             MY_HOST1.MY_COMPANY.  ORA-23309: object ODS.ODS_CHG_S
REPADMIN             MY_HOST1.MY_COMPANY.  ORA-23416: table "ODS"."ODS_CHG
REPADMIN             MY_HOST1.MY_COMPANY.  ORA-23308: object ODS.ODS_CHG_S
REPADMIN             MY_HOST1.MY_COMPANY.  ORA-23416: table "ODS"."ASR_CHG
REPADMIN             MY_HOST1.MY_COMPANY.  ORA-23308: object ODS.ASR_CHG_L
-------------------  -------------------  ------------------------------
--------------------------------------------------------------------------------
Following deferred transaction errors were found at MY_HOST1.MY_COMPANY.COM
```

```
---------------  ---------------  ---------------  ----------------------------
Deferred         Deferred Trans   Destination      Error
Transaction ID   Origin DB
---------------  ---------------  ---------------  ----------------------------
1.2.3733         MY_HOST1.MY_COM  MY_HOST1.MY_COM  ORA-01403: no data found

---------------  ---------------  ---------------  ----------------------------
No deferred transaction errors were found at MY_HOST2.MY_COMPANY.COM
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
```

-DISPQSTAT オプション

構文は次のとおりです。

```
remtool -dispqstat [-v] [-conn[ect] rep_admin_name/rep_admin_password@connectid_of_
mds_or_rms]
```

1. このオプションは、ASR ベースのレプリケーションを使用する DRG のキュー統計の表示に使用されます。LDAP ベースのレプリケーションを使用する DRG には使用できません。
2. ASR および LDAP ベースのレプリケーションを使用する DRG の場合は、ASR ベースのレプリケーションを使用するノードのキュー統計のみを表示します。

例 : -DISPQSTAT オプション

この例では、MY_HOST1.MY_COMPANY.COM および MY_HOST2.MY_COMPANY.COM で構成される DRG のキュー統計がレポートされます。これを実行するには、次のコマンドを発行します。

```
remtool -dispqstat -v -conn repadmin/repadmin@my_host1.my_company.com
```

結果は次のとおりです。

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :

-------- ------------ ---------------------- ------------ ------------ ----
Instance Host Name     Global Name            Version      Replicaid    Site
Name                                                                    Type
-------- ------------ ---------------------- ------------ ------------ ----
rid1     my_host      MY_HOST1.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid1 MDS
rid2     my_host      MY_HOST2.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid2 RMS
-------- ------------ ---------------------- ------------ ------------ ----
Queue Statistics :
-------------- -------------- --------- --------- --------- --------- ---------
```

```
   Supplier       Consumer       New      Retry     Purge      HIQ    Change #
-------------- -------------- --------- --------- --------- --------- ---------
MY_HOST1.MY CO MY_HOST1.MY CO     3         9         10        6      2003
MY_HOST1.MY CO MY HOST2.MY CO     2         7         8         5      2001
MY_HOST2.MY CO MY_HOST1.MY CO     2         8         5         8      2002
MY_HOST2.MY CO MY_HOST2.MY CO     2        10         7         8      2000
-------------- -------------- --------- --------- --------- --------- ---------
Legends
  New: No. of new change logs
  Retry: No. of change logs in retry queue
  Purge: No. of change logs in purge queue
  HIQ: No. of change logs in Human Intervention Queue (HIQ)
  Change # : Last applied change log no.
```

-SUSPENDASR オプション

構文は次のとおりです。

```
remtool -suspendasr [-v] [-conn[ect] rep_admin_name/rep_admin_password@connectid_of_
mds_or_rms]
```

-SUSPENDASR オプションの使用方法

1. このオプションを使用して、DRG がレプリケーションに使用する Oracle9*i* Advanced Replication アクティビティを一時停止します。
2. Oracle9*i* Advanced Replication アクティビティの一時停止中、レプリケーションは実行できません。

例 : -SUSPENDASR オプション

この例では、MY_HOST1.MY_COMPANY.COM および MY_HOST2.MY_COMPANY.COM で構成される DRG のレプリケーション・アクティビティが一時停止されます。これを実行するには、次のコマンドを発行します。

```
remtool -suspendasr -v -conn repadmin/repadmin@my_host1.my_company.com
```

結果は次のとおりです。

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :

-------- ------------ ---------------------- ------------ ------------ ----
Instance Host Name     Global Name            Version      Replicaid    Site
Name                                                                    Type
-------- ------------ ---------------------- ------------ ------------ ----
rid      my_host      MY_HOST1.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid1 MDS
rid2     my_host      MY_HOST2.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid2 RMS
```

```
-------- ------------ ---------------------- ------------ ------------ ----
--------------------------------------------------------------------------------
Altering replication status...

MY_HOST1.MY_COMPANY.COM : Quiescing replication activity...
--------------------------------------------------------------------------------
Replication status has been altered successfully.
--------------------------------------------------------------------------------
```

-RESUMEASR オプション

構文は次のとおりです。

```
remtool -resumeasr [-v] [-conn[ect] rep_admin_name/rep_admin_password@connectid_of_
mds_or_rms]
```

-RESUMEASR オプションの使用方法

1. このオプションを使用して、レプリケーションに ASR を使用する DRG の ASR アクティビティを再開します。

例 : -RESUMEASR オプション

この例では、MY_HOST1.MY_COMPANY.COM および MY_HOST2.MY_COMPANY.COM で構成される DRG のレプリケーション・アクティビティが再開されます。これを実行するには次のコマンドを発行します。

```
remtool -resumeasr -v -conn repadmin/repadmin@MY_HOST1.MY_COMPANY.COM
```

結果は次のとおりです。

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :

-------- ------------ ---------------------- ------------ ------------ ----
Instance Host Name     Global Name            Version      Replicaid    Site
Name                                                                    Type
-------- ------------ ---------------------- ------------ ------------ ----
rid1      my_host      MY_HOST1.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid1  MDS
rid2      my_host      MY_HOST2.MY_COMPANY.COM OID 9.0.4.0.0 my_host_rid2  RMS
-------- ------------ ---------------------- ------------ ------------ ----
--------------------------------------------------------------------------------
Altering replication status...

MY_HOST1.MY_COMPANY.COM : Resuming replication activity...
--------------------------------------------------------------------------------
Replication status has been altered successfully.
--------------------------------------------------------------------------------
```

-PADDNODE オプション

構文は次のとおりです。

```
remtool -paddnode [-v] [-bind <hostname>:<port>/<replication_dn_password>]
```

-PADDNODE オプションの使用方法

1. このオプションを使用して、読取り専用レプリカまたは読取り専用部分レプリカをノード（サプライヤ・ノード）に追加できます。
2. サプライヤ・ノードは、レプリケーション用 ASR またはレプリケーション用 LDAP（あるいはその両方）を使用する DRG の一部にできます。
3. 追加する新規レプリカは、DRG の一部にはできません。
4. -bind オプションを使用してサプライヤ・ディレクトリの詳細情報を指定しない場合、サプライヤの詳細情報の指定を求めるプロンプトが表示されます。
5. サプライヤの詳細情報が有効な場合は、remtool によって、DRG 内にノードがある場合は、それらすべてのノードが識別され、コンシューマの詳細情報が求められる前にサプライヤの詳細情報が表示されます。
6. コンシューマ・ディレクトリの詳細情報の取得後、DRG に複数のノードがある場合、サプライヤの replicaid の指定を求めるプロンプトが表示されます。ここで、ユーザーは、LDAP ベースのレプリケーションを使用する DRG のいずれかのノードの replicaid を指定できます。
7. ASR ベースのレプリカをサプライヤとして指定する場合またはこの指定を求めるプロンプトが表示された場合、ユーザーは、ASR ベースのレプリカを -bind オプションでサプライヤとして指定する必要があります。
8. レプリカを追加すると、remtool によって、サプライヤ・レプリカで使用可能なネーミング・コンテキストが「*」とともに一覧に表示されます。「*」は DSE を除くすべてのディレクトリがレプリケーションに含まれることを示します。ユーザーは、必須ネーミング・コンテキストを選択してディレクトリの一部をレプリケートするか、「*」を選択してディレクトリ全体をレプリケートすることを選択できます。ユーザーがネーミング・コンテキストを選択しない場合は、ネーミング・コンテキストもレプリケーションの対象となりません。
9. remtool には、ユーザーがレプリケーションに含まれるネーミング・コンテキストを指定するかどうかに関係なく、レプリケーション用の `cn=oraclecontext` ネーミング・コンテキストが含まれます。

例 1: -PADDNODE オプション

この例では、レプリケート対象のネーミング・コンテキストをディレクトリ・サーバー ldap://my_host:3040 に指定することによって、ディレクトリ・サーバー ldap://my_host:3060 が部分読取り専用レプリカとして追加されます。これを実行するには、次のコマンドを発行します。

```
remtool -paddnode -v -bind my_host:3040/ods
```

結果は次のとおりです。

```
Directory Replication Group (DRG) details :

--- ----------------- ---------------------- ---------------------- -----
Sl  Replicaid         Directory Information   Supplier Information    Repl.
No.                                                                  Type
--- ----------------- ---------------------- ---------------------- -----
001 my_host_rid       my_host:3040             --                    RW

--- ----------------- ---------------------- ---------------------- -----
Enter consumer directory details:
Enter hostname of host running OID server    : my_host

Enter port on which OID server is listening  : 3060

Enter replication dn password                :
-------------------------------------------------------------------------------
ldap://my_host:3060 [my_host_rid2] : Modifying entry orclreplicaid=my_host_
rid2,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Modifying entry orclreplicaid=my_host_
rid1,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Adding entry
orclagreementid=000002,orclreplicaid=my_host_rid1,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Adding entry orclreplicaid=my_host_
rid2,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Adding entry cn=replication
dn,orclreplicaid=my_host_rid2,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry orclreplicaid=my_host_
rid1,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry
orclagreementid=000002,orclreplicaid=my_host_rid1,cn=replication configuration...
ldap://my_host:3040 [my_host_rid] : Adding entry
cn=includednamingcontext000001,orclagreementid=000002,orclreplicaid=usunnae07_
prep,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry
```

```
cn=includednamingcontext000001,orclagreementid=000002,orclreplicaid=usunnae07_
prep,cn=replication configuration...
------------------------------------------------------------------------------
Replica ldap://my_host:3060(my_host_rid2) has been added to this DRG.
------------------------------------------------------------------------------
Directory Replication Group (DRG) details :

--- ----------------- ---------------------- ---------------------- -----
Sl  Replicaid         Directory Information   Supplier Information    Repl.
No.                                                                  Type
--- ----------------- ---------------------- ---------------------- -----
001 my_host_rid1       my_host:3040           --                      RW

002 my_host_rid2       my_host:3060           my_host_rid1            RO

--- ----------------- ---------------------- ---------------------- -----
Replica ldap://my_host:3060 (my_host_rem2) can be made partial replica by specifying
naming contexts to be replicated.

------------------------------------------------------------------------------
List of available naming contexts in supplier replica ldap://my_host:3040 (my_host_
rid1) :

    1. * [replicate whole directory]
    2. dc=com
    3. dc=org
    4. dc=net
    5. dc=edu
Enter naming context (e-end, q-quit) : dc=org

Enter naming context (e-end, q-quit) : dc=edu

Enter naming context (e-end, q-quit) : e

Following naming contexts will be included for replication:
------------------------------------------------------------------------------
    1. dc=org
    2. dc=edu
Do you want to continue? [y/n] : y

ldap://my_host:3040 [my_host_rid1] : Adding entry
cn=includednamingcontext000002,orclagreementid=000002,orclreplicaid=my_host_
rid,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry
cn=includednamingcontext000002,orclagreementid=000002,orclreplicaid=my_host_
rid,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Adding entry
```

```
cn=includednamingcontext000003,orclagreementid=000002,orclreplicaid=my_host_
rid,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry
cn=includednamingcontext000003,orclagreementid=000002,orclreplicaid=my_host_
rid,cn=replication configuration...

-------------------------------------------------------------------------------
Selected naming contexts have been included for replication.
-------------------------------------------------------------------------------
```

例 2: -PADDNODE オプション

この例では、ディレクトリ・サーバー ldap://my_host:3060 がディレクトリ・サーバー ldap://my_host:3040 に部分レプリカとして追加されます。これは、LDAP ベースのレプリケーションを使用する ldap://my_host:3040 および ldap://my_host:3080 で構成される DRG の一部です。ユーザーは my_host:3040 または my_host:3080 のいずれかに接続し、コンシューマ・レプリカを my_host:3040 に追加できます。

この例では、次のコマンドを発行します。

```
remtool -paddnode -v -bind my_host:3040/ods
```

結果は次のとおりです。

```
Directory Replication Group (DRG) details :

--- ----------------- ---------------------- ---------------------- -----
Sl  Replicaid         Directory Information   Supplier Information    Repl.
No.                                                                  Type
--- ----------------- ---------------------- ---------------------- -----
001 my_host_rid1      my_host:3040            --                     RW

002 my_host_rid3      my_host:3080            my_host_rid1           RO

--- ----------------- ---------------------- ---------------------- -----
Enter consumer directory details:
Enter hostname of host running OID server    : my_host

Enter port on which OID server is listening  : 3060

Enter replication dn password                :
Enter replicaid of the supplier              : my_host_rid1
-------------------------------------------------------------------------------
ldap://my_host:3060 [my_host_r[my_host_rid1]id2] : Modifying entry orclreplicaid=my_
host_rid2,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Modifying entry orclreplicaid=my_host_
rem,cn=replication configuration...
```

```
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Adding entry
orclagreementid=000003,orclreplicaid=my_host_rid,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Adding entry orclreplicaid=my_host_
rem2,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Adding entry cn=replication
dn,orclreplicaid=my_host_rem2,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry orclreplicaid=my_host_
rem2,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry cn=replication
dn,orclreplicaid=my_host_rem2,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry orclreplicaid=my_host_
rem,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry
orclagreementid=000002,orclreplicaid=my_host_rem,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry
orclagreementid=000003,orclreplicaid=my_host_rid,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry cn=replication
dn,orclreplicaid=my_host_rid,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry orclreplicaid=my_host_
rem3,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry cn=replication
dn,orclreplicaid=my_host_rid3,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry
orclagreementid=000003,orclreplicaid=my_host_rid,cn=replication configuration...
-------------------------------------------------------------------------------
Replica ldap://my_host:3060(my_host_rem2) has been added to this DRG.
-------------------------------------------------------------------------------
Directory Replication Group (DRG) details :

--- ----------------- ---------------------- ---------------------- -----
Sl  Replicaid         Directory Information   Supplier Information    Repl.
No.                                                                  Type
--- ----------------- ---------------------- ---------------------- -----
001 my_host_rid1       my_host:3040              --                    RW

002 my_host_rid2      my_host:3060              my_host_rid1           RO

003 my_host_rid3      my_host:3080              my_host_rid1           RO

--- ----------------- ---------------------- ---------------------- -----
Replica ldap://my_host:3060 (my_host_rid2) can be made partial replica by specifying
naming contexts to be replicated.
-------------------------------------------------------------------------------

List of available naming contexts in supplier replica ldap://my_host:3040 (my_host_
```

```
rid1) :

    1. *  [replicate whole directory]
Enter naming context (e-end, q-quit) : e

--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
```

例 3: -PADDNODE オプション

この例では、OID サーバー ldap://my_host:3080 が OID サーバー ldap://my_host:3040 に部分レプリカとして追加されます。これは、ASR ベースのレプリケーションを使用する ldap://my_host:3040 および ldap://my_host:3060 で構成される DRG の一部です。この場合、ユーザーは、my_host:3040 に接続してコンシューマ・レプリカを my_host:3040 に追加する必要があります。この例では、次のコマンドを発行します。

```
remtool -paddnode -v -bind my_host:3040/ods
```

結果は次のとおりです。

```
Directory Replication Group (DRG) details :

--- ------------------ ---------------------- ---------------------- -----
Sl  Replicaid          Directory Information   Supplier Information    Repl.
No.                                                                   Type
--- ------------------ ---------------------- ---------------------- -----
001 my_host_rid1       my_host:3040           my_host_rid2           RW

002 my_host_rid2       --                     my_host_rid1           RW

--- ------------------ ---------------------- ---------------------- -----
Enter consumer directory details:
Enter hostname of host running OID server    : my_host

Enter port on which OID server is listening  : 3080

Enter replication dn password                :
Enter replicaid of the supplier              : my_host_rid1

--------------------------------------------------------------------------------
ldap://my_host:3080 [my_host_rid3] : Modifying entry orclreplicaid=my_host_
rem3,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Modifying entry orclreplicaid=my_host_
rem,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
```

```
ldap://my_host:3040 [my_host_rid1] : Adding entry
orclagreementid=000002,orclreplicaid=my_host_rem,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Adding entry orclreplicaid=my_host_
rem3,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Adding entry cn=replication
dn,orclreplicaid=my_host_rem3,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry orclreplicaid=my_host_
rem,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry
orclagreementid=000002,orclreplicaid=my_host_rem,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry cn=replication
dn,orclreplicaid=my_host_rem,cn=replication configuration...
-------------------------------------------------------------------------------
Replica ldap://my_host:3080(my_host_rem3) has been added to this DRG.
-------------------------------------------------------------------------------
Directory Replication Group (DRG) details :

--- ----------------- ---------------------- ---------------------- -----
Sl  Replicaid         Directory Information   Supplier Information    Repl.
No.                                                                  Type
--- ----------------- ---------------------- ---------------------- -----
001 my_host_rid1      my_host:3040            my_host_rid2           RW

002 my_host_rid2      --                      my_host_rid1           RW

003 my_host_rid3      my_host:3080            my_host_rid1           RO

--- ----------------- ---------------------- ---------------------- -----
Replica ldap://my_host:3080 (my_host_rid3) can be made partial replica by specifying
naming contexts to be replicated.
Do you want to continue? [y/n] : y

-------------------------------------------------------------------------------
List of available naming contexts in supplier replica ldap://my_host:3040 (my_host_
rid1) :

    1. * [replicate whole directory]
    2. dc=com
    3. dc=org
    4. dc=net
    5. dc=edu
Enter naming context (e-end, q-quit) : *

Enter naming context (e-end, q-quit) : e

Following naming contexts will be included for replication:
-------------------------------------------------------------------------------
```

```
    1. *
Do you want to continue? [y/n] : y

ldap://my_host:3040 [my_host_rid] : Adding entry
cn=includednamingcontext000002,orclagreementid=000002,orclreplicaid=my_host_
rid,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry
cn=includednamingcontext000002,orclagreementid=000002,orclreplicaid=my_host_
rid,cn=replication configuration...
-------------------------------------------------------------------------------
Selected naming contexts have been included for replication.
-------------------------------------------------------------------------------
```

-PDELNODE オプション

構文は次のとおりです。

```
remtool -pdelnode [-v] [-bind <hostname>:<port#>/<repl_dn_password>]
```

-PDELNODE オプションの使用方法

1. このオプションを使用して、読取り専用レプリカまたは読取り専用部分レプリカを DRG から削除できます。
2. このオプションを使用して、ASR ベースのレプリカは削除できません。ASR ベースのレプリカの削除には、-delnode オプションを使用する必要があります。

例 1: -PDELNODE オプション

この例では、-PADDNODE オプションの例 3 で作成された DRG から、レプリカ ldap://my_host:3080 が削除されます。この DRG は - ldap://my_host:3040、ldap://my_host:3060、ldap://my_host:3080 の 3 つのレプリカで構成されていて、このうち ldap://my_host:3040 と ldap://my_host:3060 では ASR ベースのレプリケーションが使用され、ldap:my_host:3040 と ldap://my_host:3080 では LDAP ベースのレプリケーションが使用されます。レプリカ ldap://my_host:3080 を削除するには、ldap://my_host:3040 または ldap://my_host:3080 のいずれかのバインド詳細情報を定義する必要があります。

注意： ldap://my_host:3060 にバインドするとすべてのレプリカの詳細情報が定義されますが、そのバインド詳細情報を定義して、レプリカ ldap://my_host:3080 を削除することはできません。

この例では、次のコマンドを発行します。

```
remtool -pdelnode -v -bind my_host:3040/ods
--------------------------------------------------------------------------------
Directory Replication Group (DRG) details :
--- ----------------- ---------------------- ---------------------- -----
Sl   Replicaid         Directory Information    Supplier Information   Repl.
No.                                                                   Type
--- ----------------- ---------------------- ---------------------- -----
001  my_host_rid1       my_host:3040           my_host_rid2           RW

002  my_host_rid2       --                     my_host_rid1           RW

003  my_host_rid3       my_host:3080           my_host_rid1           RO

--- ----------------- ---------------------- ---------------------- -----
Enter replicaid of the replica to be deleted : my_host_rid3

--------------------------------------------------------------------------------
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Deleting entry
orclagreementid=000002,orclreplicaid=my_host_rid1,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Deleting entry orclreplicaid=my_host_
rem3,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Modifying entry orclreplicaid=my_host_
rem3,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Modifying entry ...
ldap://my_host:3080 [my_host_rid3] : Deleting entry orclreplicaid=my_host_
rem,cn=replication configuration...
--------------------------------------------------------------------------------
Replica ldap://my_host:3080(my_host_rid3) has been deleted from this DRG.
--------------------------------------------------------------------------------
Directory Replication Group (DRG) details :

--- ----------------- ---------------------- ---------------------- -----
Sl  Replicaid          Directory Information   Supplier Information    Repl.
No.                                                                   Type
--- ----------------- ---------------------- ---------------------- -----
001 my_host_rid1       my_host:3040           my_host_rid2            RW

002 my_host_rid2       --                     my_host_rid1            RW

--- ----------------- ---------------------- ---------------------- -----
```

例 2: -PDELNODE オプション

この例では、3 つのレプリカで構成される DRG から、1 つのレプリカが削除されます。3 つのレプリカはすべて LDAP ベースのレプリケーションを使用します。削除するレプリカは、これら 3 つのレプリカのいずれかにバインドして削除できます。

この例では、次のコマンドを発行します。

```
remtool -pdelnode -v -bind my_host:3040/ods
------------------------------------------------------------------------------
Directory Replication Group (DRG) details :

--- ----------------- ---------------------- ---------------------- -----
Sl  Replicaid         Directory Information   Supplier Information    Repl.
No.                                                                  Type
--- ----------------- ---------------------- ---------------------- -----
001 my_host_rid1      my_host:3040           --                      RW

002 my_host_rid3      my_host:3080           my_host_rid1            RO

003 my_host_rid2      my_host:3060           my_host_rid1            RO

--- ----------------- ---------------------- ---------------------- -----
Enter replicaid of the replica to be deleted : my_host_rid3

------------------------------------------------------------------------------
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Deleting entry
orclagreementid=000003,orclreplicaid=my_host_rem,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Deleting entry orclreplicaid=my_host_
rem3,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Deleting entry
orclagreementid=000003,orclreplicaid=my_host_rem,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Deleting entry orclreplicaid=my_host_
rem3,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Modifying entry orclreplicaid=my_host_
rem3,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Modifying entry ...
ldap://my_host:3080 [my_host_rid3] : Deleting entry orclreplicaid=my_host_
rem,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Deleting entry orclreplicaid=my_host_
rem2,cn=replication configuration...
------------------------------------------------------------------------------
Replica ldap://my_host:3080(my_host_rid3) has been deleted from this DRG.
------------------------------------------------------------------------------
Directory Replication Group (DRG) details :

--- ----------------- ---------------------- ---------------------- -----
```

```
Sl  Replicaid          Directory Information   Supplier Information    Repl.
No.                                                                    Type
--- ------------------ ---------------------- ---------------------- -----
001 my_host_rid1       my_host:3040           --                     RW

002 my_host_rid2       my_host:3060           my_host_rid            RO

--- ------------------ ---------------------- ---------------------- -----
```

-PCHGPWD オプション

構文は次のとおりです。

```
remtool -pchgpwd [-v] [-bind <hostname>:<port>/<replication_dn_password>]
```

-PCHGPWD オプションの使用方法

1. このオプションを使用して、レプリケーション識別名のパスワードを変更します。
2. -bind オプションによって識別された Oracle Internet Directory サーバーのレプリケーション識別名が変更されます。
3. 識別されたレプリカのレプリケーション識別名のパスワードが、Oracle Internet Directory リポジトリと Wallet の両方で変更されます。
4. レプリカがレプリケーションに関連する場合、パスワードは、ローカル・レプリカのレプリケーション識別名用の他のレプリカで変更されます。ASR ベースのレプリケーションとは異なり、各レプリカのレプリケーション識別名パスワードは、他のパスワードと同じにする必要はありません。
5. このオプションは、レプリケーション識別名パスワードの変更が必要な Oracle Internet Directory サーバーが実行されているホストで実行する必要があります。Wallet のパスワードも変更する必要があるため、この条件は必須です。この条件が満たされていない場合は、remtool によってエラーがレポートされます。（例 2 を参照）

例 1: -PCHGPWD オプション

この例では、レプリカ `ldap://my_host:3040/ods` のパスワードが変更されます。これを実行するには、次のコマンドを発行します。

```
remtool -pchgpwd -v -bind my_host:3040/ods
```

結果は次のとおりです。

```
Directory Replication Group (DRG) details :

--- ------------------ ---------------------- ---------------------- -----
Sl  Replicaid          Directory Information   Supplier Information    Repl.
No.                                                                    Type
--- ------------------ ---------------------- ---------------------- -----
```

```
001 my_host_rid1       my_host:3040             --                     RW

002 my_host_rid3       my_host:3080             my_host_rid1           RO

--- ----------------- ---------------------- ---------------------- -----
-------------------------------------------------------------------------------
Replication DN password of ldap://my_host:3040 (my_host_rem) associated with
database 'rid' will be changed.
Do you want to continue? [y/n] : y

Enter new password of replication DN         :
Reenter new password of replication DN       :
-------------------------------------------------------------------------------
ldap://my_host:3040 [my_host_rid1] : Modifying entry cn=replication
dn,orclreplicaid=my_host_rem,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Modifying entry cn=replication
dn,orclreplicaid=my_host_rem,cn=replication configuration...
-------------------------------------------------------------------------------
Password has been changed.
-------------------------------------------------------------------------------
```

例 2: -PCHGPWD オプション

この例では、ユーザーが、異なるホストからレプリカ my_host:3040 のパスワードの変更を試行します。これを実行するには、次のコマンドを発行します。

```
remtool -pchgpwd -v -bind my_host:3040/ods
```

結果は次のとおりです。

```
Directory Replication Group (DRG) details :

--- ----------------- ---------------------- ---------------------- -----
Sl  Replicaid         Directory Information   Supplier Information   Repl.
No.                                                                 Type
--- ----------------- ---------------------- ---------------------- -----
001 my_host_rid1      my_host:3040           --                     RW

002 my_host_rid3      my_host:3080           my_host_rid1           RO

--- ----------------- ---------------------- ---------------------- -----
-------------------------------------------------------------------------------
Replication DN password of ldap://my_host:3040 (my_host_rid1) associated with
database 'rid1' will be changed.
Do you want to continue? [y/n] : y

Enter new password of replication DN         :
Reenter new password of replication DN       :
```

```
--------------------------------------------------------------------------------
ldap://my_host:3040 : Invoke the remtool at host my_host to change the password of
ldap://my_host:3040 replica.
--------------------------------------------------------------------------------
Error occurred while changing password of replica ldap://my_host:3040(my_host_rid1).
ldap://my_host:3040 : Invoke the remtool at host my_host to change the password of
ldap://my_host:3040 replica.
```

-PCLEANUP オプション

```
The syntax is:
remtool -pcleanup -v -bind my_host:3040/ods
```

-PCLEANUP オプションの使用方法

1. このオプションを使用して、LDAP ベースのレプリケーション設定をクリーンアップできます。
2. このオプションを使用して、不完全または不具合のある LDAP ベースのレプリケーション設定を持つレプリカをクリーンアップできます。不完全または不具合のある LDAP ベースのレプリケーション設定の場合、レプリケーション環境管理ツールでは、`-bind` オプションで識別されるレプリカのみがクリーンアップされます。レプリケーション構成情報が破損している場合またはレプリケーション識別名エントリが使用可能でない場合は、スーパー・ユーザーの識別名およびパスワードを求めるプロンプトが表示されます。
3. このオプションは、LDAP ベースのレプリケーション設定のクリーンアップのみに使用可能で、ASR ベースのレプリケーション設定には使用できません。

例 1: -PCLEANUP オプション

この例では、LDAP ベースのレプリケーションに関連する 3 つのレプリカを持つ DRG のレプリケーション設定がクリーンアップされます。

この例では、次のコマンドを発行します。

```
remtool -pcleanup -v -bind my_host:3040/ods
```

結果は次のとおりです。

```
Directory Replication Group (DRG) details :

--- ----------------- ---------------------- ---------------------- -----
Sl  Replicaid         Directory Information   Supplier Information    Repl.
No.                                                                  Type
--- ----------------- ---------------------- ---------------------- -----
001 my_host_rid1      my_host:3040            --                     RW

002 my_host_rid3      my_host:3080           my_host_rid1            RO
```

```
003 my_host_rid2       my_host:3060            my_host_rid1             RO

--- ----------------- ---------------------- ---------------------- -----
DRG identified by replica ldap://my_host:3040 (my_host_rid1) will be cleaned up.
Do you want to continue? [y/n] : y

-------------------------------------------------------------------------------
ldap://my_host:3040 [my_host_rid1] : Modifying entry orclreplicaid=my_host_
rem,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Deleting entry
orclagreementid=000002,orclreplicaid=my_host_rem,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Deleting entry
orclagreementid=000003,orclreplicaid=my_host_rem,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Deleting entry orclreplicaid=my_host_
rem3,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Deleting entry orclreplicaid=my_host_
rem2,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Modifying entry orclreplicaid=my_host_
rem3,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Modifying entry ...
ldap://my_host:3080 [my_host_rid3] : Modifying entry ...
ldap://my_host:3080 [my_host_rid3] : Deleting entry orclreplicaid=my_host_
rem,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Deleting entry orclreplicaid=my_host_
rem2,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Modifying entry orclreplicaid=my_host_
rem2,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Modifying entry ...
ldap://my_host:3060 [my_host_rid2] : Modifying entry ...
ldap://my_host:3060 [my_host_rid2] : Deleting entry orclreplicaid=my_host_
rem3,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Deleting entry cn=replication
dn,orclreplicaid=my_host_rem3,cn=replication configuration...
-------------------------------------------------------------------------------
Replica ldap://my_host:3040(my_host_rid1) has been cleaned up.
-------------------------------------------------------------------------------
```

例 2: -PCLEANUP オプション

この例では、-pcleanup オプションを使用して、不具合のある LDAP ベースのレプリケーション設定をクリーンアップする方法を示します。

手順 1: まず、レプリカ ldap://my_host:3040 を ldap://my_host:3060 に追加します。レプリケーションの設定中にエラーが発生し、その結果、設定に不具合が含まれます。

```
remtool -paddnode -v -bind my_host:3040/ods

Directory Replication Group (DRG) details :

--- ------------------ ---------------------- ---------------------- -----
Sl  Replicaid          Directory Information   Supplier Information    Repl.
No.                                                                   Type
--- ------------------ ---------------------- ---------------------- -----
001 my_host_rid1       my_host:3040           --                     RW

--- ------------------ ---------------------- ---------------------- -----
Enter consumer directory details:
Enter hostname of host running OID server    : my_host
Enter port on which OID server is listening  : 3060
Enter replication dn password                :
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Error occurred while adding partial replica ldap://my_host:3060.
ldap://my_host:3060 : Failed to add entry orclreplicaid=my_host_rid1,cn=replication
configuration.
DSA is unwilling to perform

ldap://my_host:3060 : Failed to read replication configuration information.
```

手順 2: 再度 ldap://my_host:3040 を ldap://my_host:3060 に追加し、その結果、エラーが発生します。

```
remtool -paddnode -v -bind my_host:3040/ods
ldap://my_host:3060 : Failed to read replication configuration information.
```

手順 3: 前述の paddnode プロシージャでエラーが発生しため、新規ノードを追加できません。このため、-pcleanup をコールして設定をクリーンアップします。クリーンアップが完了すると、-paddnode を再起動して新規レプリカを追加できます。

```
remtool -pcleanup -v -bind my_host:3040/ods
ldap://my_host:3060 : Failed to read replication configuration information.
Error occurred while getting replication configuration information.
This tool will try to rectify the problem if super user DN and password are
provided.
Do you want to continue? [y/n] : y

Enter superuser DN                           : cn=orcladmin

Enter superuser password                     :
```

```
Enter new password of replication DN         :
Reenter new password of replication DN       :
-------------------------------------------------------------------------------
Directory Replication Group (DRG) details :

--- ------------------ ---------------------- ---------------------- -----
Sl  Replicaid          Directory Information   Supplier Information    Repl.
No.                                                                   Type
--- ------------------ ---------------------- ---------------------- -----
001 my_host_rid1       my_host:3040           --                     RW

002 my_host_rid2       my_host:3060           my_host_rid1           RO

--- ------------------ ---------------------- ---------------------- -----
DRG identified by replica ldap://my_host:3040 (my_host_rem) will be cleaned up.
Do you want to continue? [y/n] : y

-------------------------------------------------------------------------------
ldap://my_host:3040 [my_host_rid1] : Modifying entry orclreplicaid=my_host_
rem,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Deleting entry
orclagreementid=000002,orclreplicaid=my_host_rem,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Deleting entry orclreplicaid=my_host_
rem2,cn=replication configuration...
-------------------------------------------------------------------------------
Replica ldap://my_host:3040(my_host_rem) has been cleaned up.
-------------------------------------------------------------------------------
```

-PRESETPWD オプション

構文は次のとおりです。

```
remtool -presetpwd -v -bind my_host:3040/ods
```

-PRESETPWD オプションの使用方法

1. このオプションを使用して、レプリケーション識別名のパスワードを再設定します。
2. レプリケーション識別名パスワードを再設定するには、スーパー・ユーザーの識別名とパスワードが必要です。
3. レプリケーション識別名パスワードを再設定するには、スーパー・ユーザーの識別名とパスワードが必要です。
4. このオプションは、このディレクトリが含まれている DRG の他のディレクトリでは、パスワードを再設定しません。

例 : -PRESETPWD オプション

この例では、次のコマンドを発行して、レプリカ my_host:3040 のパスワードを再設定します。

```
remtool -presetpwd -v -bind my_host:3040/ods
```

結果は次のとおりです。

```
Enter superuser DN                          : cn=orcladmin

Enter superuser password                    :
-------------------------------------------------------------------------------
Replication DN password of ldap://my_host:3040 (my_host_rem) associated with
database 'rid1' will be reset.
Do you want to continue? [y/n] : y

Enter new password of replication DN        :
Reenter new password of replication DN      :
-------------------------------------------------------------------------------
ldap://my_host:3040 [my_host_rid1] : Modifying entry cn=replication
dn,orclreplicaid=my_host_rid1,cn=replication configuration...
-------------------------------------------------------------------------------
Password has been changed.
-------------------------------------------------------------------------------
```

-PCHGWALPWD オプション

構文は次のとおりです。

```
remtool -pchgwalpwd -v -bind my_host:3040/ods
```

-PCHGWALPWD オプションの使用方法

1. このオプションは、Wallet パスワードの変更のみに使用します。
2. このオプションは、Wallet パスワードを、Oracle Internet Directory リポジトリに格納されたレプリケーション識別名パスワードに設定します。
3. バインド詳細情報は、Wallet パスワードが変更されるディレクトリのバインド詳細情報と同じにする必要があります。
4. このオプションは、RAC 環境で有効です。

例 : -PCHGWALPWD オプション

この例では、レプリカ ldap://my_host:3040 のレプリケーション識別名のパスワードが Wallet の Oracle Internet Directory リポジトリ内のパスワードに設定されます。これを実行するには、次のコマンドを発行します。

```
remtool -pchgwalpwd -v -bind my_host:3040/ods
```

結果は次のとおりです。

```
Directory Replication Group (DRG) details :

--- ------------------ ---------------------- ---------------------- -----
Sl  Replicaid          Directory Information   Supplier Information    Repl.
No.                                                                   Type
--- ------------------ ---------------------- ---------------------- -----
001 my_host_rid1       my_host:3040           --                     RW

002 my_host_rid3       my_host:3080           my_host_rid1           RO

--- ------------------ ---------------------- ---------------------- -----
--------------------------------------------------------------------------------
Replication DN password of ldap://my_host:3040 (my_host_rid1) associated with
database 'rid' will be set in wallet.
Do you want to continue? [y/n] : y
```

パスワードが変更されました。

Oracle Directory Integration and Provisioning Platform コマンドライン・ツールの構文

この項では、次の項目について説明します。

- Directory Integration and Provisioning Assistant
- ldapUploadAgentFile.sh ツールの構文
- ldapCreateConn.sh ツール構文
- ldapDeleteConn.sh ツール構文
- StopOdiServer.sh ツールの構文
- schemasync ツールの構文
- Oracle Directory Integration and Provisioning Server 登録ツール（odisrvreg）
- プロビジョニング・サブスクリプション・ツール （oidprovtool）の構文

Directory Integration and Provisioning Assistant

表 A-26 に、Directory Integration and Provisioning Assistant および対応するコマンドを使用して実行可能なタスクを示します。各タスクの詳細情報の参照先も示します。

表 A-26　Directory Integration and Provisioning Assistant の機能の概要

タスク	コマンド	詳細情報の参照先

同期プロファイルの作成、変更または削除	`createprofile`
	`modifyprofile`
	`deleteprofile`
		A-107 ページの「同期プロファイルの作成、変更および削除」

Oracle Internet Directory 内のすべてのプロファイル名の表示	`listprofiles`	A-114 ページの「Oracle Internet Directory 内のすべての同期プロファイルの表示」
特定のプロファイルの詳細の表示	`showprofile`	A-115 ページの「特定の同期プロファイルの詳細の表示」
同期開始前の Oracle Internet Directory と接続ディレクトリの統一	`bootstrap`	A-109 ページの「Directory Integration and Provisioning Assistant を使用したディレクトリのブートストラップ」
Oracle Directory Integration and Provisioning Server が Oracle Internet Directory への接続時に使用する Wallet パスワードの設定	`wpasswd`	A-115 ページの「Oracle Directory Integration and Provisioning Server に対する Wallet パスワードの設定」
Oracle Directory Integration Platform 管理者のパスワードの再設定	`chgpasswd`	A-114 ページの「Oracle Directory Integration and Provisioning Platform 管理者のパスワードの変更」
認証管理ノード間での統合プロファイルの移動	`reassociate`	A-115 ページの「認証管理ノード間での統合プロファイルの移動」

Directory Integration and Provisioning Assistant のコマンドライン・インタフェースは次のとおりです。

dipassistant *command* [-help]

command := *Directory Integration and Provisioning Assistant command*

```
Directory Integration and Provisioning Assistant command :=
        createprofile [cp]
        | modifyprofile [mp]
        | deleteprofile [dp]
        | listprofiles[lsprof]
        | showprofile[sp]
```

```
| bootstrap [bs]
| wpasswd [wp]
| chgpasswd [cpw]
| reassociate [rs]
```

特定のコマンドのヘルプを参照するには、次のとおり入力します。

```
dipassistant command -help
```

同期プロファイルの作成、変更および削除

Directory Integration and Provisioning Assistant を使用して同期プロファイルを作成、変更または削除するための構文は次のとおりです。

```
dipassistant createprofile | modifyprofile | deleteprofile
[-host host name] [-port port number] [-dn bind_DN] [-passwd password]
{-file file name | -profile profile name } [propName1=value]
[propName2=value]... [-configset configset_number]
```

次に例を示します。

```
dipassistant createprofile -host myhost -port 3060 -passwd xxxx
-file import.profile -configset 1

dipassistant modifyprofile -host myhost -port 3060 -passwd xxxx
-file import.profile -dn xxxx -passwd xxxx -profile myprofile
[propName1=value]
[propName2=value]...

dipassistant deleteprofile -profile myprofile [-host myhost] [-port 3060] [-dn xxxx]
[-passwd xxxx] [-configset 1]
```

A-107 ページの表 A-27 に、Directory Integration and Provisioning Assistant を使用して同期プロファイルを作成、変更または削除するためのパラメータを示します。

表 A-27 Directory Integration and Provisioning Assistant を使用して同期プロファイルを作成、変更および削除するためのパラメータ

パラメータ	説明
-host	Oracle Internet Directory が実行されているホスト。デフォルト値はローカル・ホストの名前です。
-port	Oracle Internet Directory が起動されたポート。デフォルトは 389 です。
-dn	ディレクトリに対しての識別に使用されるバインド識別名。デフォルト値は Oracle Directory Integration and Provisioning Platform 管理者の識別名です。

表 A-27 Directory Integration and Provisioning Assistant を使用して同期プロファイルを作成、変更および削除するためのパラメータ（続き）

パラメータ	説明
-passwd	ディレクトリに対してのバインド中に使用されるバインド識別名のパスワード。
-file	すべてのプロファイル・パラメータを含むファイル。 **関連項目：**パラメータのリストとその説明は、A-108 ページの表 A-28 を参照してください。
-configset	プロファイルの関連付けが必要な構成設定エントリの番号。
-profile	変更が必要なプロファイル。

表 A-28 に、createprofile コマンドと modifyprofile コマンドによって想定されるプロパティが示します。既存のプロファイルの修正時に、デフォルトは想定されません。ファイル内に指定された属性のみが変更されます。

表 A-28 CreateProfile コマンドと ModifyProfile コマンドによって想定されるプロパティ

パラメータ	説明	デフォルト
odip.profile.name	プロファイルの名前。	-
odip.profile.password	プロファイルにアクセスするためのパスワード	-
odip.profile.status	DISABLE または ENABLE。	DISABLE
odip.profile.syncmode	同期の方向。変更がサード・パーティから Oracle Internet Directory に伝播される場合、同期のモードは IMPORT です。変更がサード・パーティのディレクトリに伝播される場合、同期のモードは EXPORT です。	IMPORT
odip.profile.retry	エラーが発生して統合サーバーが終了する前に、プロファイルを実行可能な最大回数。	4
odip.profile.schedinterval	統合サーバーによるプロファイルの連続実行の間隔。前回の実行が完了していない場合、その実行が完了するまで次の実行は再開しません。	1 分
odip.profile.agentexecommand	NON-LDAP インタフェースの場合、LDIF 形式で情報を生成するためのコマンド。	-
odip.profile.condirurl	サード・パーティ・ディレクトリの位置 [hostname:port]。	-
odip.profile.condiraccount	サード・パーティ・ディレクトリへの接続に使用されるバインド識別名またはユーザー名。	-
odip.profile.condirpassword	サード・パーティ・ディレクトリに対しての識別に使用されるパスワード。	-

表 A-28 CreateProfile コマンドと ModifyProfile コマンドによって想定されるプロパティ（続き）

パラメータ	説明	デフォルト
odip.profile.interface	データ交換に LDAP、LDIF、DB、TAGGED のいずれの形式を使用するかを示すインジケータ。	LDAP
odip.profile.configfile	実行に使用される追加のプロファイル固有の情報を含むファイルの名前。	-
odip.profile.mapfile	マッピング・ルールを含むファイルの名前。	-
odip.profile.condirfilter	Oracle Internet Directory へのインポート前に、接続ディレクトリから読み込まれた変更に対して適用する必要があるフィルタ。	-
odip.profile.oidfilter	接続ディレクトリへのエクスポート前に、Oracle Internet Directory から読み込まれた変更に対して適用する必要があるフィルタ。	-
odip.profile.lastchgnum	最後に適用された変更番号。エクスポート・プロファイルの場合、この番号は Oracle Internet Directory で最後に適用された番号を指しますが、インポート・プロファイルの場合、この番号は接続ディレクトリで最後に適用された変更番号を指します。	-

Directory Integration and Provisioning Assistant を使用したディレクトリのブートストラップ

bootstrap コマンドのコマンドライン・インタフェースは次のとおりです。

```
dipassistant bootstrap { -profile profile_name [-host host_name] [-port port_number]
-dn bind_DN [-passwd password] [-log log_file] [-logseverity severity] [-trace
trace_file] [-tracelevel trace_level] [-loadparallelism <#nThrs>] [-loadretry
<retryCnt>] | -cfg file_name }
```

例 :

```
dipassistant bs –cfg bootstrap cfg
```

または

```
dipassistant bs -host myhost –port 3060 –dn cn=orcladmin –password xxxx –profile
iPlanetProfile
```

表 A-29 deleteprofile コマンドのパラメータ

パラメータ	説明
-cfg	ブートストラップの実行に必要なすべてのパラメータを含む構成ファイル。 **関連項目：**パラメータのリストとその説明は、A-111 ページの表 A-30 を参照してください。
-host	Oracle Internet Directory が実行されていたホスト。
-port	Oracle Internet Directory が起動されたポート。
-dn	ディレクトリに対しての識別に使用されるバインド識別名。
-password	ディレクトリに対してのバインド中に使用されるバインド識別名のパスワード。
-profile	プロファイル名。
-log	ログ・ファイル。このパラメータを指定しない場合、デフォルトでは OH/ldap/odi/bootstrap.log にログ情報が書き込まれます。
-logseverity	ログの重要度 1 ～ 15。1 は INFO、2 は WARNING、3 は DEBUG、4 は ERROR、またはこれらの任意組合せ。指定しない場合は、INFO および ERROR メッセージのみが記録されます。
-trace	デバッグのためのトレース・ファイル。
-trace level	トレース・レベル。
-loadRetry	宛先へのロードが失敗した場合、エントリに「不良エントリ」のマークが付く前に実行可能な再試行の回数。
-loadparallelism	Oracle Internet Directory へのロードが複数のスレッドを使用してパラレルで実行されることを示すインジケータ。たとえば、-loadparallelism 5 は、5 つのスレッドが作成され、それぞれが Oracle Internet Directory へのエントリのロードをパラレルで試行することを示します。

ブートストラップ・コマンドによって想定されるプロパティ

表 A-30 ブートストラップ・プロパティ

プロパティ	説明	必須	デフォルト
odip.bootstrap.srctype	ブートストラップのソースが LDAP と LDIF のいずれかを示すインジケータ。有効な値は LDAP または LDIF です。	はい	-
odip.bootstrap.desttype	ブートストラップの宛先が LDAP と LDIF のいずれかを示すインジケータ。有効な値は LDAP または LDIF です。	はい	-
odip.bootstrap.srcurl	LDAP ソース・タイプの場合はソース・ディレクトリの位置。LDIF の場合は、LDIF ファイルの位置。 **注意 :** LDAP の場合、想定される形式は host[:port] です。LDIF の場合、想定される形式はファイルの絶対パスです。	はい	-
odip.bootstrap.desturl	LDAP の場合は、宛先ディレクトリの位置。LDIF の場合は、LDIF ファイルの位置。 **注意 :** LDAP の場合、想定される形式は host[:port] です。LDIF の場合、想定される形式はファイルの絶対パスです。	はい	-
odip.bootstrap.srcsslmode	ブートストラップのソースへの接続に SSL ベースの認証を使用する必要があるかどうかを示すインジケータ。TRUE の値は、SSL ベースの認証を使用する必要があることを示します。	いいえ	FALSE

表 A-30 ブートストラップ・プロパティ（続き）

プロパティ	説明	必須	デフォルト
odip.bootstrap.destsslmode	ブートストラップの宛先への接続に SSL ベースの認証を使用する必要があるかどうかを示すインジケータ。TRUE は、SSL ベースの認証を使用する必要があることを示します。 **注意 :** LDIF の場合、このパラメータは無効です。	いいえ	FALSE
odip.bootstrap.srcdn	ソース URL への補足。LDIF バインドの場合、このパラメータは無効です。ただし、LDAP の場合、このパラメータはバインド識別名を指定します。	LDAP の場合のみ	-
odip.bootstrap.destdn	接続先 URL への補足。LDIF バインドの場合、このパラメータは無効です。ただし、LDAP の場合、このパラメータはバインド識別名を指定します。	LDAP の場合のみ	-
odip.bootstrap.srcpasswd	ソースへのバインド・パスワード。LDAP バインドの場合、このパスワードはセキュリティとして使用されます。このファイルではパスワードを指定しないことをお薦めします。	いいえ	-
odip.bootstrap.destpasswd	バインド・パスワード。LDAP バインドの場合、このパスワードはセキュリティ資格証明として使用されます。 このファイルではパスワードを指定しないことをお薦めします。	いいえ	-
odip.bootstrap.mapfile	属性とドメインのマッピングを含むマップ・ファイルの位置。	いいえ	-

表 A-30 ブートストラップ・プロパティ（続き）

プロパティ	説明	必須	デフォルト
odip.bootstrap.logfile	ログ・ファイルの位置。このファイルがすでに存在する場合は、追加されます。デフォルトのログ・ファイルは、*$ORACLE_HOME*/ldap/odi/log ディレクトリに作成された bootstrap.log です。	いいえ	ディレクトリ *$ORACLE_HOME*/ldap/odi/ に作成されたファイル bootstrap.log
odip.bootstrap.logseverity	記録する必要があるログ メッセージのタイプ。 INFO - 1 WARNING - 2 DEBUG – 4 ERROR - 8 **注意：**これらのタイプの組合せも使用されます。たとえば、WARNING および ERROR のメッセージのみ必要な場合は、8+2 の値、10 を指定します。同様に、すべてのメッセージのタイプを選択する場合は、1 + 2 + 4 + 8 = 15 を使用します。	いいえ	1 + 8 = 9
odip.bootstrap.loadparallelism	処理されたデータを宛先にロードするために使用する Writer スレッドの数を示す数値。	いいえ	1-
odip.bootstrap.loadretry	エントリのロードに失敗した場合の再試行回数を示すインジケータ。	いいえ	5
odip.bootstrap.trcfile	トレース・ファイルの位置。このファイルがすでに存在する場合は、上書きされます。	いいえ	*$ORACLE_HOME*/ldap/odi/log/bootstrap.trc
odip.bootstrap.trclevel	トレース・レベル	いいえ	3

Oracle Directory Integration and Provisioning Platform 管理者のパスワードの変更

dipadmin アカウントのデフォルトのパスワードは、インストール中に選択した ias_admin のパスワードと同じです。このコマンドを使用すると、dipadmin アカウントのパスワードを再設定できます。このパスワードを再設定するには、orcladmin アカウントのセキュリティ資格証明が必要です。

次に例を示します。

```
$ dipassistant chgpasswd -passwd orcladmin password -host oid.heman.com
-port 3060
```

Assistant によって、新しいパスワードの入力を求める次のようなプロンプトが表示されます。

```
New Password:
Confirm Password:
```

Oracle Internet Directory 内のすべての同期プロファイルの表示

listprofiles コマンドによって、Oracle Internet Directory 内のすべての同期プロファイルのリストが表示されます。次に例を示します。

```
$ dipassistant listprofiles -passwd dipadmin password -host oid.heman.com
-port 3060
```

このコマンドによって、次のサンプル・リストが表示されます。

```
IplanetExport
IplanetImport
ActiveImport
ActiveExport
LdifExport
LdifImport
TaggedExport
TaggedImport
OracleHRAgent
ActiveChgImp
```

注意： ここに示すリストは、インストール中に作成されたデフォルトのプロファイルのセットです。

特定の同期プロファイルの詳細の表示

showprofile コマンドによって、特定の同期プロファイルの詳細が表示されます。次に例を示します。

```
$ dipassistant showprofile -passwd dipadmin password -host oid.heman.com
-port 3060 -profile ActiveImport
```

このコマンドによって、次のサンプル出力が表示されます。

```
odip.profile.version = 1.0
odip.profile.lastchgnum = 0
odip.profile.interface = LDAP
odip.profile.oidfilter = orclObjectGUID
odip.profile.schedinterval = 60
odip.profile.name = ActiveImport
odip.profile.syncmode = IMPORT
odip.profile.retry = 5
odip.profile.debuglevel = 0
odip.profile.status = DISABLE
```

Oracle Directory Integration and Provisioning Server に対する Wallet パスワードの設定

WPasswd コマンドを使用すると、Oracle Directory Integration and Provisioning Server が Oracle Internet Directory への接続時に使用する Wallet パスワードを指定できます。このコマンドを使用するには、次のように入力します。

```
dipassistant wp
```

Directory Integration and Provisioning Assistant によって、パスワードの入力および確認を求められます。

認証管理ノード間での統合プロファイルの移動

Directory Integration and Provisioning Assistant を使用して、ディレクトリ統合プロファイルを別のノードに移動し、それらを相互に再度関連付けることができます。たとえば、中間層コンポーネントが特定の Oracle Identity Management インフラストラクチャに関連付けられている場合、そのインフラストラクチャのノード内に存在するすべての統合プロファイルを新しいインフラストラクチャのノードに移動できます。

表 A-31 に、再度関連付ける場合の規則を示します。

表 A-31 ディレクトリ統合プロファイルを再度関連付ける場合の規則

状況	処置
統合プロファイルが 2 つ目の Oracle Internet Directory ノードに存在しない	統合プロファイルは、2 つ目の Oracle Internet Directory ノードにコピーされ、コピー完了後無効になります。これは、アプリケーションで有効にする必要があります。統合プロファイルの `lastchangenumber` 属性は、2 つ目の Oracle Internet Directory ノードの現行の最終変更番号に変更されます。
統合プロファイルが 2 つ目の Oracle Internet Directory ノードに存在する	両方の統合プロファイルが、次の方法で調停されます。 ■ ノード1のプロファイルの新しい属性がノード2のプロファイルに追加されます。 ■ 既存の同じ属性の場合は、ノード 1 のプロファイルの値によってノード 2 のプロファイルの属性が上書きされます。 ■ プロファイルは、コピー完了後無効になります。これは、アプリケーションで有効にする必要があります。 ■ 統合プロファイルの `lastchangenumber` 属性が 2 つ目の Oracle Internet Directory ノードの現行の最終変更番号に変更されます。

再度関連付けるには、次のとおり入力します。

```
dipassistant reassociate [-src_ldap_host <hostName>]
[-src_ldap_port <portNo>] [-src_ldap_dn <bindDn>] [-src_ldap_passwd
<password>] -dst_ldap_host <hostName> [-dst_ldap_port <portNo>]
[-dst_ldap_dn <bindDn>] [-dst_ldap_passwd <password>] [-log <logfile>]
Options:
-src_ldap_host <hostName> : Host where OID-1 runs
-src_ldap_port <portNo> : Port at which OID-1 runs
-src_ldap_dn <bindDn> : Bind Dn to connect to OID-1
-src_ldap_passwd <password> : Bind Dn password to connect to OID-1
-dst_ldap_host <hostName> : Host where OID-2 runs
-dst_ldap_port <portNo> : Port at which OID-2 runs
-dst_ldap_dn <bindDn> : Bind Dn to connect to OID-2
-dst_ldap_passwd <password> : Bind Dn password to connect to OID-2
-log <logFile> : Log file
```

デフォルト：

```
src_ldap_host - localhost, src_ldap_port & dst_ldap_port - 389
src_ldap_dn & dst_ldap_dn - cn=orcladmin account
```

例：

```
dipassistant reassociate -src_ldap_host oid1.mycorp.com ¥
-dst_ldap_host oid2.mycorp.com -src_ldap_passwd xxxx ¥
-dst_ldap_passwd xxxx

dipassistant rs -help
```

ログ・ファイルの位置を指定していない場合は、デフォルトで `$ORACLE_HOME/ldap/odi/log/reassociate.log` が作成されます。

Oracle Internet Directory 10*g*（9.0.4）での Directory Integration and Provisioning Assistant の制限

このリリースの Directory Integration and Provisioning Assistant では、次の機能はサポートされません。

- Oracle Internet Directory に対する SSL ベースの認証
- スキーマの同期化
- -cfg オプションが指定されているブートストラップ・プロセスの終了時に自動的に行われるプロファイルの作成
- マッピング・ファイルの検証
- 不具合があったエントリ・ファイルの作成

Directory Integration and Provisioning Assistant の次の要素はテストされていません。

- SSL 接続を介した接続ディレクトリのブートストラップ
- プロファイルに対して同期が行われている場合の modifyprofile コマンドの使用

表 A-32 に、Directory Integration and Provisioning Assistant のブートストラップ・コマンドの制限を示します。

表 A-32 Directory Integration and Provisioning Assistant でのブートストラップの制限

ブートストラップのタイプ	制限
LDIF-to-LDIF	なし
LDAP-to-LDIF	エントリが多数の場合、ブートストラップは、サイズ制限超過のエラーを返して正常に実行されない場合があります。この問題を解決するには、ブートストラップの実行元であるサーバーで次のことが必要です。 ■ ページ化された結果の制御（OID 1.2.840.113556.1.4.319）をサポートする。現在、Microsoft Active Directory のみがこの制御をサポートする LDAP ディレクトリです。 ■ サーバー側のサイズ制限パラメータに適切な値を設定する。 ■ 独自のインポート / エクスポート・ツールを使用し、データのダンプを取得して、LDIF-to-LDIF または LDIF-to-LDAP を使用してブートストラップを実行する。
LDIF -to-LDAP	なし
LDAP-to-LDAP	LDAP-to-LDIF と同様

ldapUploadAgentFile.sh ツールの構文

ディレクトリの同期時に、LdapUploadAgentFile.sh を使用してマッピング情報と構成情報をロードします。

```
ldapUploadAgentFile.sh -name  profile_name
-config configset_the_profile_is_associated_with
-LDAPhost  directory_server_host
-LDAPport  directory_server_port
-binddn  DN_that_can_modify_the_profile   >
-bindpass password_for_the_bind_DN
-attrtype  "MAP" | "ATTR"
-filename complete_path_of_file_to_be_uploaded
```

表 A-33 ldapUploadAgentFile.sh の引数

引数	説明
Name	情報のロードが必要な統合プロファイルの名前。
Config	プロファイルが属している configset。
LDAPhost	ディレクトリ・サーバーのホスト。
LDAPport	ディレクトリ・サーバーのポート。
Binddn	プロファイル・エントリを変更するためのアクセス権限を持つディレクトリ・ユーザーのバインド識別名。デフォルトは cn=orcladmin です。
Bindpass	バインド識別名に対応するパスワード。デフォルトは welcome です。
AttrType	ロードするファイルのタイプ。マッピング・ファイルをロードする場合は、「MAP」を指定します。構成情報ファイルをロードする場合は、「ATTR」を指定します。
Filename	アップロードするファイルの完全パス名。

注意： Directory Integration and Provisioning Assistant を使用して、次の操作を実行することもできます。次のいずれかの値を入力します。

```
dipassistant mp [options] odip.profile.mapfile=your map
file


dipassistant mp [options] odip.profile.configfile= your
configuration file
```

関連項目： ldapUploadAgentFile.sh を使用する場合については、第 33 章「Oracle Directory Synchronization Service」を参照してください。

ldapCreateConn.sh ツール構文

統合プロファイルは、コマンドライン・ツール ldapcreateConn.sh を使用して作成できます。このツールは、次のディレクトリにあります。

$*ORACLE_HOME*/ldap/admin/

次の例では、「HRMS」という名前の統合プロファイルを構成設定 2 で作成します。

```
ldapcreateConn.sh
        -name agent_name>
        [ -type  <IMPORT | EXPORT > ] ¥
        [ -agentpwd agent_password ] ¥
        [ -config configset_to_associate_with ] ¥
        [ -LDAPhost directory_server_host ]
        [ -LDAPport directory_server_port ] ¥
        [ -binddn DN_of_super_user] ¥
        [ -bindpass   Bind_password ] ¥                                    [
        [-retry   maximum_retry_count_on_synchronization_errors ] ¥
        [ -poll polling_interval_for_synchronization ] ¥
        [ -host host_on_which_to_run_agent ] ¥
        [ -conndirurl  connected_directory_URL ] ¥
        [ -conndiracct connected_directory_account_information ] ¥
        [ -conndirpwd connected_directory_account_password ] ¥
        [ -execmd command_line_for_the_agent ]  ¥
        [ -iftype interface_type ]      ¥                                   [
        -condirfilter connected_directory_matching_filter ]¥
        [ -oidfilter OID_matching_filter ] ¥
        [ -U SSL_authentication_mode ]
        [ -W wallet_location ]¥
        [ -P wallet_password ]
```

表 A-34 ldapcreateConn.sh を使用して登録するための引数

引数	説明
Name	統合プロファイルの名前。一意である必要があります。
Type	IMPORT または EXPORT。デフォルトは IMPORT です。
Agentpwd	プロファイルを保護するためのパスワード。デフォルトは welcome です。
Config	構成設定番号。デフォルトは 1 です。
LDAPhost	ディレクトリ・サーバーのホスト。デフォルトは現行のホストです。
LDAPport	ディレクトリ・サーバー・ポート。デフォルトはポート 389 です。
Binddn	統合プロファイルの作成権限を持つディレクトリ・ユーザーのバインド識別名。デフォルトは cn=orcladmin です。
Bindpass	バインド・パスワード。デフォルトは welcome です。
Retry	サーバーによる同期エラーの検出によって実行される再試行の最大回数。デフォルトは 5 です。

表 A-34 ldapcreateConn.sh を使用して登録するための引数（続き）

引数	説明
Poll	プロファイルのスケジューリング間隔。デフォルトは 60 秒です。
Host	現在使用されています。暫定的に、DIP サーバーが実行されているマシンの名前に設定する必要があります。
Conndirurl	接続ディレクトリのアクセス情報。
Conndiracct	接続ディレクトリ・アカウント。
Conndirpwd	接続ディレクトリ・アカウントのパスワード。
Execmd	パートナ・エージェントを実行するための OS コマンドライン。
Iftype	インタフェース・タイプ。デフォルトは TAGGED です。
Condirfilter	接続ディレクトリの照合フィルタ。
Oidfilter	OID 照合フィルタ。

注意： Directory Integration and Provisioning Assistant の createprofile オプションを使用してもこの操作を実行できます。

ldapDeleteConn.sh ツール構文

同期プロファイルは、コマンドライン・ツール ldapDeleteConn.sh を使用して登録解除できます。このツールは、ディレクトリ *$ORACLE_HOME*/ldap/admin/ にあります。

構文は次のとおりです。

```
ldapdeleteConn.sh [ -name Profile_Name ]
 -LDAPhost <LDAP server host> (default is local host)]
           [ -LDAPport directory_server_port> (default 389)]
           [ -binddn SuperUserDN (default cn=orcladmin ) ]
           [ -bindpass   password (default=welcome) ]
           [ -config configset_associated_with_agent ]
           [ -U <SSL_authentication_mode> ]
           [ -W Wallet_location ]
           [ -P Wallet_password ]
           [ -help | -usage ]
```

次の例では、プロファイル・エントリを登録解除し、構成設定 2（config 2）のエントリから分離します。

```
ldapDeleteConn.sh name HRMS config 2
```

注意： Directory Integration and Provisioning Assistant の `deleteprofile` オプションを使用してもこの操作を実行できます。

StopOdiServer.sh ツールの構文

OID モニターおよび OIDCTL ツールを使用できないクライアントのみのインストール環境では、OIDCTL ツールを使用せずに Directory Integration and Provisioning Server を起動できます。サーバーを停止するには、stopOdiServer.sh ツールを使用します。

このツールのパス名は次のとおりです。
`$ORACLE_HOME/ldap/admin/stopodiserver.sh`

使用方法は次のとおりです。

```
$ORACLE_HOME/ldap/admin/stopodiserver.sh
        [ -LDAPhost LDAP_server_host ]
        [ -LDAPport LDAP_server_port ]
        [ -binddn super_user_dn (default cn=orcladmin ) ]
        [ -bindpass   bind_password (default=welcome) ]
        -instance instance_number_to_stop
```

表 A-35 Oracle Directory Integration and Provisioning Server を停止するための引数

引数	説明
LDAPhost	ディレクトリ・サーバーのホスト。デフォルトは現行のホストです。
LDAPport	ディレクトリ・サーバーのポート。デフォルトはポート 389 です。
Binddn	統合プロファイルの作成権限を持つディレクトリ・ユーザーのバインド識別名。デフォルトは cn=orcladmin です。
Bindpass	バインド・パスワード。デフォルトは welcome です。
Instance	停止する Oracle Directory Integration and Provisioning Server のインスタンス番号。

注意： Windows オペレーティング・システムでシェル・スクリプト・ツールを実行するには、次のいずれかの UNIX エミュレーション・ユーティリティが必要です。

- Cygwin 1.3.2.2-1 以上
  サイト : `http://sources.redhat.com`
- MKS Toolkit 6.1
  サイト : `http://www.datafocus.com/`

schemasync ツールの構文

schemasync ツールを使用すると、Oracle ディレクトリ・サーバーとサード・パーティの LDAP ディレクトリとの間で、スキーマ要素（つまり、属性とオブジェクト・クラス）を同期化できます。

schemasync の使用方法は次のとおりです。

```
$ORACLE_HOME/bin/schemasync
        -srchost source_LDAP_directory
        -srcport source_LDAP_port_numbert
        -srcdn privileged_DN_in_source_directory_to_access_schema
        -srcpwd password
        -dsthost destination_LDAP_directory
        -dstport destination_LDAP_port
        -dstdn privileged_dn_in_destination_directory_to_access_schema
        -dstpwd password
        [-ldap]
```

注意： -ldap パラメータはオプションです。このパラメータを指定した場合、スキーマの変更は、ソース LDAP ディレクトリから接続先 LDAP ディレクトリに直接適用されます。また、このパラメータを指定しない場合、スキーマの変更は、次の LDIF ファイルに格納されます。

- $*ORACLE_HOME*/ldap/odi/data/attributetypes.ldif
  このファイルには、新規属性の定義が格納されます。
- $*ORACLE_HOME*/ldap/odi/data/objectclasses.ldif
  このファイルには、新規オブジェクト・クラスの定義が格納されます。

-ldap を指定しない場合は、ldapmodify を使用して、これらの 2 つのファイルから、属性の型、オブジェクト・クラスの順に定義をアップロードする必要があります。

スキーマの同期中に発生したエラーは、次のファイルにログ記録されます。

- $*ORACLE_HOME*/ldap/odi/log/attributetypes.log
- $*ORACLE_HOME*/ldap/odi/log/objectclasses.log

Oracle Directory Integration and Provisioning Server 登録ツール（odisrvreg）

Oracle Directory Integration and Provisioning Server をディレクトリに登録する場合は、このツールで、ディレクトリにエントリが作成され、Directory Integration and Provisioning Server 用のパスワードが設定されます。登録エントリがすでに存在する場合は、このツールを使用して既存のパスワードを再設定できます。また、odisrvreg ツールは、$*ORACLE_HOME*/ldap/odi/conf に odisrvwallet_*hostname* と呼ばれるローカル・ファイルも作成します。このファイルは、Directory Integration and Provisioning Server のプライベート Wallet として機能し、Directory Integration and Provisioning Server はこのファイルを起動時に使用して、ディレクトリにバインドします。

表 A-36 に、Oracle Directory Integration and Provisioning Server 登録ツールで使用するパラメータを示します。odisrvreg を SSL モードで実行し、-U、-W および -P パラメータを使用して、ツールとディレクトリ間の通信を完全に保護することもできます。この 3 つのパラメータについても、表 A-36 に示します。

Directory Integration and Provisioning Server を登録するには、次のコマンドを入力します。

```
odisrvreg -h host_name -p port -D binddn -w bindpasswd -I passwd [-U ssl_mode -W
wallet -P wallet_password]
```

表 A-36　ODISRVREG の引数の説明

引数	説明
-h *host_name*	Oracle ディレクトリ・サーバーのホスト名。
-p *port_number*	ディレクトリ・サーバーが実行されているポート番号。
-D *binddn*	バインド識別名。バインド識別名には、Directory Integration and Provisioning Server の登録エントリを作成する認可が必要です。
-lhost	コールド・フェイルオーバー・クラスタ構成の仮想ホスト名。
-w *bindpasswd*	バインド・パスワード。
-U *SSL mode*	認可なしの場合は 0（ゼロ）を指定します。認可する場合は、1 を指定します。
-W *Wallet location*	SSL 証明書が格納される Oracle Wallet の位置。
-P *Wallet password*	Oracle Wallet をオープンするための Wallet パスワード。

プロビジョニング・サブスクリプション・ツール （oidprovtool）の構文

プロビジョニング・サブスクリプション・ツールを使用して、ディレクトリ内のプロビジョニング・プロファイル・エントリを管理します。具体的には、次の操作の実行に使用します。

- 新規プロビジョニング・プロファイルの作成。作成された新規プロビジョニング・プロファイルは、Oracle Directory Integration and Provisioning Platform で処理できるように、使用可能な状態に設定されます。
- 既存のプロビジョニング・プロファイルの無効化。
- 無効なプロビジョニング・プロファイルの有効化。
- 既存のプロビジョニング・プロファイルの削除。
- 指定したプロビジョニング・プロファイルの現行ステータスの取得。
- 既存のプロビジョニング・プロファイル内にあるすべてのエラーの消去。

プロビジョニング・サブスクリプション・ツールは、プロビジョニング・プロファイル・エントリの位置とスキーマの詳細をツールのコール元から保護します。コール元からは、アプリケーションとサブスクライバの組合せによって、プロビジョニング・プロファイルを一意に識別します。システムには、サブスクライバごとに、1 つのアプリケーションに 1 つのプロビジョニング・プロファイルのみ存在できるという制約があります。

注意： Windows オペレーティング・システムでシェル・スクリプト・ツールを実行するには、次のいずれかの UNIX エミュレーション・ユーティリティが必要です。

- Cygwin 1.3.2.2-1 以上
  サイト : `http://sources.redhat.com`
- MKS Toolkit 6.1
  サイト : `http://www.datafocus.com/`

実行可能ファイルの名前は oidProvTool で、`$ORACLE_HOME/bin` に格納されています。

このツールを起動するには、次のコマンドを使用します。

```
oidprovtool param1=param1_value  param2=param2_value param3=param3_value ...
```

プロビジョニング・サブスクリプション・ツールが受け入れるパラメータは次のとおりです。

表 A-37 プロビジョニング・サブスクリプション・ツールのパラメータ

名前	説明	操作	必須 / オプション
operation	実行するサブスクリプション操作。このパラメータに指定できる値は、「create」、「enable」、「disable」、「delete」、「status」および「reset」です。ツールを起動するたびに 1 つの操作のみ実行できます。	すべて	必須
ldap_host	サブスクリプション操作を実行するディレクトリ・サーバーのホスト名。指定しない場合は、デフォルト値の localhost が使用されます。	すべて	オプション
profile_status	プロファイルのステータス（ENABLED/ DISABLED）。デフォルトは ENABLED です。	作成	オプション
profile_mode	IBOUND/OUTBOUND/BOTH。デフォルトは OUTBOUND です。	作成	オプション
profile_debug	プロファイルが Oracle Directory Integration and Provisioning Server によって実行されるデバッグ・レベル。	すべて	オプション
sslmode	プロビジョニング・サブスクリプション・ツールを SSL モードで実行するかどうかを示します。値 0 は非 SSL モードを、値 1 は SSL モードを示します。	すべて	オプション
ldap_port	LDAP サーバーが要求をリスニングする TCP/IP ポート。指定しない場合は、デフォルト値の 389 が使用されます。	すべて	オプション

表 A-37 プロビジョニング・サブスクリプション・ツールのパラメータ（続き）

名前	説明	操作	必須 / オプション
ldap_user_dn	ユーザーのかわりに操作が実行される場合、そのユーザーの LDAP 識別名。すべてのユーザーに、プロビジョニング・サブスクリプション操作の実行権限があるわけではありません。LDAP ユーザーにプロビジョニング・サブスクリプション操作の実行権限を付与または制限する方法については、管理ガイドを参照してください。	すべて	必須
ldap_user_password	ユーザーのかわりに操作が実行される場合、そのユーザーのパスワード。	すべて	必須
application_dn	プロビジョニング・サブスクリプション操作が実行されるアプリケーションの LDAP 識別名。application_dn パラメータと organization_dn パラメータの組合せによって、サブスクリプション・ツールはプロビジョニング・プロファイルを一意に識別します。	すべて	必須
organization_dn	プロビジョニング・サブスクリプション操作が実行される組織の LDAP 識別名。application_dn パラメータと organization_dn パラメータの組合せによって、サブスクリプション・ツールはプロビジョニング・プロファイルを一意に識別します。	すべて	必須
interface_name	PL/SQL パッケージのデータベース・スキーマ名。値の書式は、[Schema].[PACKAGE_NAME] です。	作成のみ	必須
interface_type	イベントを伝播する必要があるインタフェースのタイプ。有効な値は PLSQL です（指定しない場合は、これがデフォルトとして使用されます）。	作成のみ	オプション

表 A-37 プロビジョニング・サブスクリプション・ツールのパラメータ（続き）

名前	説明	操作	必須 / オプション
interface_connect_info	データベース接続文字列。この文字列の書式は、[HOST]:[PORT]:[SID]:[USER_ID]:[PASSWORD] です。	作成のみ	必須
interface_version	インタフェース・プロトコルのバージョン。有効な値は 1.0 または 1.1 です。1.0 は古いインタフェースです。指定しない場合は、これがデフォルトとして使用されます。	作成のみ	オプション
interface_additional_info	インタフェースに関する追加情報。現在は使用されていません。	作成のみ	オプション
schedule	このプロファイルに関するスケジューリング情報。この値は、DIP がこのプロファイルを処理するまでの間隔の秒数です。指定しない場合は、デフォルト値の 3600 が使用されます。	作成のみ	オプション
max_retries	プロビジョニング・サービスが、失敗したイベント送信を再試行する回数。指定しない場合は、デフォルト値の 5 が使用されます。	作成のみ	オプション
event_subscription	DIP がこのアプリケーションに通知を送信する必要があるイベント。この文字列の書式は、「[USER]GROUP]:[*対象のドメイン* >]:[DELETE]ADD]MODIFY(< カンマで区切られた属性名のリスト >)]」です。異なる値を持つパラメータを複数回リストに含めると、複数の値を指定できます。指定しない場合は、デフォルトとして、USER:< 組織識別名 >:DELETE GROUP:< 組織識別名 >:DELETE が使用されます。つまり、組織識別名に属するユーザーとグループの削除通知が送信されます。	作成のみ	オプション

OID データベース・パスワード・ユーティリティ（oidpasswd）構文

OID データベース・パスワード・ユーティリティを使用して、次の操作を実行できます。

- Oracle Internet Directory データベースへのパスワードを変更します。

  Oracle Internet Directory は、Oracle データベースへの接続時にパスワードを使用します。このパスワードのデフォルトは、Oracle Application Server 管理者のパスワードとしてインストール時に指定した値と同じです。OID データベース・パスワード・ユーティリティを使用すると、このパスワードを変更できます。

- Oracle Internet Directory データベース・パスワード用の oidlpwdldap1 という Wallet、および Oracle ディレクトリ・レプリケーション・サーバー・パスワード用の `oidpwdr`*`sid`* という Wallet を作成します。

  `sid` は環境変数 *`SID`* からではなく、接続データベースから取得されます。

  `create_wallet=true` オプションを使用して、ODS Wallet を生成する前に、ODS データベースに対して自己認証を行うための ODS パスワードを取得する必要があります。デフォルトの ODS パスワードは Oracle Application Server 管理者のパスワードと同じです。

- ロックされているディレクトリ・スーパー・ユーザー・アカウント（`cn=orcladmin`）のロックを解除します。

OID データベース・パスワード・ユーティリティの構文は次のとおりです。

```
oidpasswd  [connect=connect_string ]  [change_oiddb_pwd=true |
create_wallet=true | unlock_su_acct=true]
```

Oracle Internet Directory データベースへのパスワードの変更

Oracle Internet Directory データベースのパスワードを変更するには、次のとおり入力します。

```
oidpasswd [connect=connect string ] [change_oiddb_pwd=true]
```

オプションを指定していない場合でも、Oracle Internet Directory データベースのパスワードはツールによって変更されます。

OID データベース・パスワード・ユーティリティは、現行のパスワードの入力を要求します。現行のパスワードの次に新規パスワードを入力し、続いて確認のため新規パスワードを再入力します。

OID データベース・パスワード・ユーティリティは、変更されるパスワードはローカル・データベース（*`ORACLE_HOME`* と `ORACLE_`*`SID`* で定義）のものであるとデフォルトでみなされています。リモート・データベースのパスワードを変更する場合は、`connect=`*`connect_string`* オプションを使用する必要があります。

次に例を示します。

```
$ oidpasswd
current password: ods
new password: newsupersecret
confirm password: newsupersecret
password set.
```

注意：

- パスワードの入力時、ユーザーの入力値は画面に表示されません。
- OID データベース・ユーティリティを使用して Oracle Internet Directory データベースへのパスワードを変更する場合は、常に、oidemdpasswd ユーティリティも実行する必要があります。これによって、Oracle Enterprise Manager Daemon（Oracle Enterprise Manager のコンポーネント）で、パスワードを適切にキャッシュし、起動時に ODS スキーマに接続することができます。oidemdpasswd ユーティリティを実行すると、Oracle Internet Directory のプロセスを Oracle Enterprise Manager から監視できます。

Oracle Internet Directory データベースのパスワードおよび Oracle ディレクトリ・レプリケーション・サーバーのパスワード用の Wallet の作成

Oracle Internet Directory データベースのパスワードおよびディレクトリ・レプリケーション・サーバーのパスワード用の Wallet を作成するには、次のとおり入力します。

```
oidpasswd [connect=connect string] create_wallet=true
```

この場合、引数 create_wallet は必須です。接続文字列以外の他のオプションは指定できません。

スーパー・ユーザー・アカウントのロック解除

ロックされているディレクトリ・スーパー・ユーザー・アカウント（cn=orcladmin）をロック解除するには、次のとおり入力します。

```
oidpasswd [connect=connect string] unlock_su_acct=true
```

引数 unlock_su_acct は必須です。接続文字列以外の他のオプションは指定できません。

OID データベース統計収集ツール（oidstats.sh）の構文

oidstats.sh ツールを使用して様々なデータベース ods スキーマ・オブジェクトを分析し、統計を見積もります。このツールは、*$ORACLE_HOME*/ldap/admin/ ディレクトリに格納されています。このツールでは、ods データベース・ユーザーのパスワードが要求されます。ディレクトリへのデータの初回ロードを含め、ディレクトリ・データに大幅な変更がある場合は、このユーティリティを実行する必要があります。

バルク・ロード・ツール（bulkload.sh）以外の手段でデータをディレクトリにロードする場合は、ロード後に OID データベース統計収集ツールを実行する必要があります。Oracle のオプティマイザが LDAP 操作に対応する問合せについて最適の実行計画を選択するには、統計収集が必要です。OID データベース統計収集ツールは、Oracle Internet Directory デーモンを停止せずに必要に応じて実行できます。

注意： ディレクトリへの移入に bulkload ユーティリティを使用しない場合は、oidstats.sh ツールを実行して、検索パフォーマンスの深刻な低下を回避する必要があります。

注意： Windows オペレーティング・システムでシェル・スクリプト・ツールを実行するには、次のいずれかの UNIX エミュレーション・ユーティリティが必要です。

- Cygwin 1.3.2.2-1 以上
  サイト：`http://sources.redhat.com`
- MKS Toolkit 6.1
  サイト：`http://www.datafocus.com/`

OID データベース統計収集ツールは、次の構文を使用します。

```
oidstats.sh [ -connect connect_string ]
            [ -all ]
            [ -cat catalog_name ]
            [ -pct percent ]
           [ -help | -usage ]
```

パラメータは、次のとおりです。

パラメータ	説明	デフォルト
`connect` *connect_string*	データベース接続文字列	*ORACLE_SID*
`all`	すべてのカタログ表と識別名カタログに関する統計の見積り	すべてのカタログ
`cat` *catalog_name*	すべてのカタログ（all）または特定のカタログ（例 : ct_cn）に関する統計の見積り	なし
`pct` *percent*	サンプルとして抽出するデータの割合（パーセント）	100

例 : OID データベース統計収集ツールの使用

次の各例では、ORACLE_*SID* とデフォルトのユーザー名およびパスワードが有効であるとみなします。

次の例では、すべての表の 100% のサンプル・データに基づいて統計を見積もります。

```
oidstats.sh -all -pct 100
```

次の例では、すべての表の 50% のサンプル・データに基づいて統計を見積もります。

```
oidstats.sh -all -pct 50
```

次の例では、CT_CN 表の 50% のサンプル・データに基づいて統計を見積もります。

```
oidstats.sh -cat ct_cn -pct 50
```

次の例では、すべてのカタログ表の 40% のサンプル・データに基づいて統計を見積もります。

```
oidstats.sh -cat all -pct 40
```

OID 移行ツール（ldifmigrator）の構文

データをアプリケーション固有のリポジトリから Oracle Internet Directory に移行する場合は、OID 移行ツールを使用します。OID 移行ツールは、LDIF ファイルを作成します。このファイルは、標準のコマンドライン・ツールを使用してディレクトリ・サーバーにロードできます。このツールへの入力は、置換変数が含まれた疑似 LDIF ファイルです。このツールの名前は ldifmigrator で、*ORACLE_HOME*/bin に格納されています。

ldifmigrator ツールの構文は次のとおりです。

```
ldifmigrator [options] {parameter_name=value ...}
{s_SubVar=value ... }
```

表 A-38 に、このツールで使用するコマンドライン・パラメータの詳細を示します。

表 A-38 ldifmigrator のパラメータ

パラメータ	必須	説明
Input_file	はい	置換変数が含まれるファイル。
Output_file	はい	このツールで生成されるファイルの名前。
-lookup	いいえ	このフラグを指定すると、特定の置換変数の値がディレクトリ・サーバーから取得されます。host パラメータを使用して指定する変数の名前については、次の表を参照してください。-lookup フラグが指定されている場合、host パラメータは必須です。
Host	必須（参照モードの場合のみ）	ディレクトリ・サーバー名。-lookup フラグが指定されている場合、このパラメータは必須です。
Port	いいえ	ディレクトリ・サーバーがリスニングされているポート。指定しない場合は、ポート 389 が使用されます。
DN	必須（参照モードの場合のみ）	バインド識別名。-lookup フラグが指定されている場合、このパラメータは必須です。
Password	いいえ	バインド・パスワード。
Subscriber	いいえ	属性が置換変数として使用されるサブスクライバ。指定しない場合は、ルート Oracle コンテキストに指定されているデフォルト認証管理レルムが使用されます。
s_SubsVar1.N	いいえ	ユーザーが指定するカスタム置換変数。

次の表では、事前定義の置換変数について説明します。参照モードで実行されている OID 移行ツールは、Oracle Internet Directory を参照することで、これらの変数の値を自動的に判別できます。

表 A-39 事前定義の置換変数

変数名	意味	OID 移行ツールがこの変数の値を判別する方法
%s_UserContainerDN%	すべてのユーザーが追加されるエントリの識別名。	この変数によって、レルム固有の Oracle コンテキストにある `cn=Common,cn=Products` のエントリから、`orclCommonUserSearchBase` 属性の値が割り当てられます。
%s_GroupContainerDN%	すべての Public グループが追加されるエントリの識別名。	この変数によって、レルム固有の Oracle コンテキストにある `cn=Common,cn=Products` のエントリから、`orclCommonGroupSearchBase` 属性の値が割り当てられます。
%s_UserNicknameAttribute%	認証管理レルムのユーザー・エントリに使用するニックネーム属性。	この変数によって、レルム固有の Oracle コンテキストにある `cn=Common,cn=Products` のエントリから、`orclCommonNicknameAttribute` 属性の値が割り当てられます。
%s_SubscriberDN%	認証管理レルムに対応する LDAP エントリの識別名。	単純なサブスクライバ名を指定すると、移行ツールは、属性 `orclSubscriberSearchBase` と属性 `orclSubscriberNickNameAttr` を使用し、ルート Oracle コンテキストにあるエントリ `cn=Common,cn=Products` から、そのサブスクライバ名を識別名に解決します。
%s_SubscriberOracleContextDN%	レルム固有の Oracle コンテキストの識別名。	最初にレルムの識別名が前述のように計算され、次に文字列 `cn=OracleContext` がその識別名の前に付加されます。
%s_RootOracleContextDN%	ルート Oracle コンテキストの識別名。	現在は、`cn=OracleContext` にハードコードされています。

表 A-39 事前定義の置換変数（続き）

変数名	意味	OID 移行ツールがこの変数の値を判別する方法
%s_CurrentUserDN%	LDIF ファイルをロードするユーザーの識別名。この識別名は、最低 1 名のメンバーが必要なグループの作成をブートストラップするときに、必要となる場合があります。	移行ツールでは、この識別名が認証情報の一部としてコマンドラインで指定されることを前提にしています。

OID 移行ツールが事前定義の置換変数の値を取得するのは、参照モードの場合のみです。ユーザーは、参照モードでこれらの置換変数の値を任意にオーバーライドできます。オーバーライドするには、コマンドラインで変数およびオーバーライドする値を指定します。ユーザーは、コマンドラインで、前述の表にリストされている以外の置換変数とその値を指定することもできます。

例 : OID 移行ツールの使用方法

次の内容の入力ファイル sample.dat を考えてみます。

```
dn: cn=jdoe, %s_UserContainerDN%
sn: Doe
%s_UserNicknameAttribute%: jdoe
objectClass: inetOrgPerson
objectClass: orclUserV2
title: Member of Technical Staff
homePhone: 415-584-5670
homePostalAddress: 234 Lez Drive$ Redwood City$ CA$ 94402
ou: %s_UserOrganization%
```

次の各項では、OID 移行ツールを使用して前述のテンプレート・ファイルを有効な LDIF に変換し、Oracle Internet Directory にロード可能にする方法を説明します。

参照モードでの移行ツールの使用

この例では、Oracle ディレクトリ・サーバーが環境内にあり、配置では、移行ツールを使用してディレクトリ・サーバーを参照し、特定の置換変数を判別します。次のコマンドを発行します。

```
$ldifmigrator "input_file=sample.dat" "output_file=sample.ldif" -lookup
"host=ldap.acme.com" "subscriber=acme" "s_UserOrganization=Development"
```

このコマンドを実行すると、ldap.acme.com で実行中のディレクトリ・サーバーに接続し、サブスクライバ acme に対する次の置換変数の値が取得されます。

変数名	ldap.acme.com から取得される値
%s_UserContainerDN%	cn=Users,o=acme,dc=com
%s_ UserNicknameAttribute%	uid

OID 移行ツールは、これらの変数以外に、s_UserOrganization と呼ばれるコマンドライン変数も取得し、この変数のすべての内容に値 Development を代入します。この場合、sample.ldif に格納されたツールの出力は次のとおりです（代入された値はイタリック体で示されています）。

```
dn: cn=jdoe,cn=Users,o=Acme,dc=com
sn: Doe
uid: jdoe
objectClass: inetOrgPerson
objectClass: orclUserV2
title: Member of Technical Staff
homePhone: 415-584-5670
homePostalAddress: 234 Lez Drive$ Redwood City$ CA$ 94402
ou: Development
```

Lookup オプションを指定しない場合の OID 移行ツールの使用

-lookup オプションを使用しない場合は、すべての値をコマンドラインで指定すると、前述の例に示す出力と同じ結果が得られます。次のコマンドラインの例は、参照モードを指定しない場合の移行ツールの使用方法を示しています。

```
$ldifmigrator "input_file=sample.dat" "output_file=sample.ldif"  "s_
UserContainerDN=cn=Users,o=Acme,dc=com" "s_UserNicknameAttribute=uid" "s_
UserOrganization=Development"
```

参照モードで取得した置換変数値のオーバーライド

配置で OID 移行ツールを参照モードで使用した場合でも、1 つ以上の事前定義の置換変数値をオーバーライドできます。これを行うには、オーバーライドする値をコマンドラインで指定します。次のコマンドラインは、UserNickNameAttribute を cn に設定して、デフォルトの uid をオーバーライドする方法を示しています。

```
$ldifmigrator "input_file=sample.dat" "output_file=sample.ldif" -lookup
"host=ldap.acme.com" "subscriber=acme" "s_UserOrganization=Development"
"s_UserNicknameAttribute=cn"
```

このコマンドを実行すると、ldap.acme.com で実行中のディレクトリ・サーバーに接続し、サブスクライバ acme に対する次の置換変数の値が取得されます。

表 A-40 サブスクライバ acme の置換変数

変数名	ldap.acme.com から取得される値
%s_UserContainerDN%	cn=Users,o=acme,dc=com
%s_ UserNicknameAttribute%	uid（この値は、コマンドラインの指定でオーバーライドされます）

s_UserNicknameAttribute はコマンドラインで指定されるため、OID 移行ツールは、ディレクトリから取得する値を無視し、コマンドラインで指定された値を使用します。移行ツールはこれらの変数以外に、s_UserOrganization と呼ばれるコマンドライン変数も取得し、この変数のすべての内容に値 Development を代入します。この場合、sample.ldif に格納されたツールの出力は次のとおりです（代入された値はイタリック体で示されています）。

```
dn: cn=jdoe,cn=Users,o=Acme,dc=com
sn: Doe
cn: jdoe
objectClass: inetOrgPerson
objectClass: orclUserV2
title: Member of Technical Staff
homePhone: 415-584-5670
homePostalAddress: 234 Lez Drive$ Redwood City$ CA$ 94402
ou: Development
```

ロード機能

このツールのユーザーは、ロード機能を使用してデータを Oracle Internet Directory に直接ロードできます。エントリがすでにディレクトリに存在する場合は、そのディレクトリのエントリがログ・ファイルに記録されます。ディレクトリ・エントリを追加すると、追加権限が不十分、親エントリが存在しないなどの他の理由によっても追加が失敗する場合があります。コマンドライン・ツールでは、ユーザー情報をディレクトリにロードする新しいオプション -load を使用できます。

調停機能

Oracle Application Server 10*g*（9.0.4）で使用可能なユーザー移行ツール機能は、*i*AS コンポーネントの旧バージョンが Oracle Internet Directory に移行されるすべてのユーザーに対して事実上のソースである場合にのみ有効です。ただし、実際の配置では、次の要件も発生します。

- 移行されるユーザーが Oracle Internet Directory ですでに定義されている。
- 複数の個別のアプリケーションを Oracle Internet Directory に移行する必要がある。

これらの要件に対処するために、新しいオプション -reconcile がユーザー移行ツールに追加されています。このオプションには、-reconcile SAFE | SAFE_EXTENDED | NORMAL という引数が必要です。

表 A-41 -reconcile を使用する場合の様々なモード

オプションの引数	説明
-reconcile SAFE	ディレクトリ内のユーザー・エントリの存在をチェックします。
-reconcile NORMAL	すべての新規属性が追加され、Oracle Internet Directory にすでに存在する属性の値が新しい値に置換されることをチェックします。
-reconcile SAFE_EXTENED	すべての新規属性が追加されますが、既存の属性の場合は、新しい値を追加しようとすると、その新しい値が既存の値セットに追加されます。

例 A-1 -reconcile SAFE オプション

ディレクトリに存在しない属性のみを追加する場合、このオプションを使用します。前述のユーザー・エントリの場合、ユーザー移行ツールは、この LDIF エントリを解析し、s_subscriber_user_base および s_nickname_attr の値を置換します。次に、このツールは、ディレクトリから jsmith のエントリを取得します。ディレクトリに jsmith のエントリがない場合、初めてこのエントリが追加されます。一方、前述の定義どおり、このエントリが属性とともにディレクトリに存在する場合は、ディレクトリに存在しない属性のみが追加されます。前述のエントリでは、homePhone と homePostalAddress のみが追加されます。

ディレクトリの Jsmith のエントリは、次のようになります。

```
dn: cn=jsmith, dc=oracle, dc=com
cn: jsmith
sn: Smith
orclGlobalID: 86A8485163303EBEE034080020AB67AA
uid: jsmith
objectClass: inetOrgPerson
objectClass: orclUser2
title: Member of Technical Staff
homePhone: 650-584-5670
homePostalAddress: 232 Gonzalez Drive$ San Francisco$ CA$ 94404
```

例 A-2 -reconcile NORMAL オプション

ディレクトリに存在する属性を上書きする場合、このオプションを使用します。前述のユーザー・エントリの場合、ユーザー移行ツールは、この LDIF エントリを解析し、s_subscriber_user_base および s_nickname_attr の値を置換します。次に、このツールは、ディレクトリから jsmith のエントリを取得します。ディレクトリに jsmith のエントリがない場合、初めてこのエントリが追加されます。一方、前述の定義どおり、このエントリが属性とともにディレクトリに存在する場合は、ディレクトリに存在しない属性のみが追加されます。次に、すでに存在する属性が削除され、新しい値の属性が追加されます。前述のエントリでは、homePhone と homePostalAddress が追加され、属性 title の属性値が新しい値に置換されます。

ディレクトリの Jsmith のエントリは、次のようになります。

```
dn: cn=jsmith, dc=oracle, dc=com
cn: jsmith
sn: Smith
orclGlobalID: 86A8485163303EBEE034080020AB67AA
uid: jsmith
objectClass: inetOrgPerson
objectClass: orclUser2
title: Principle Member of Technical Staff
homePhone: 650-584-5670
homePostalAddress: 232 Gonzalez Drive$ San Francisco$ CA$ 94404
```

例 A-3 -reconcile SAFE_EXTENDED オプション

既存の属性に値を追加する場合、このオプションを使用します。前述のユーザー・エントリの場合、ユーザー移行ツールは、この LDIF エントリを解析し、s_subscriber_user_base および s_nickname_attr の値を置換します。次に、このツールは、ディレクトリから jsmith のエントリを取得します。ディレクトリに jsmith のエントリがない場合、初めてこのエントリが追加されます。一方、前述の定義どおり、このエントリが属性とともにディレクトリに存在する場合は、属性 homePhone と homePostalAddress が追加され、既存の属性 title には新しい値が追加されます。

ディレクトリの Jsmith のエントリは、次のようになります。

```
dn: cn=jsmith, dc=oracle, dc=com
cn: jsmith
sn: Smith
orclGlobalID: 86A8485163303EBEE034080020AB67AA
uid: jsmith
objectClass: inetOrgPerson
objectClass: orclUser2
title: Member of Technical Staff
title: Principle Member of Technical Staff
homePhone: 650-584-5670
homePostalAddress: 232 Gonzalez Drive$ San Francisco$ CA$ 94404
```

表 A-42 -reconcile SAFE 型の LDIF レコード

Sno	エントリ Changetype	属性 Changetype	アクション
1	Add/No Change type	-	新規属性のみを追加します。
2	Modrdn/Moddn	-	ldifmigrator ツールは、この変更タイプをサポートしません。
3	Delete	-	ディレクトリからエントリを削除しません。
4	Modify	add	この属性を追加します。エントリがディレクトリに存在しない場合は、レコードを無効として無視します。属性が存在しない場合はこの属性を追加し、存在する場合は無視します。
5	-do-	replace	エントリに属性が含まれていない場合は、この属性が追加されます。エントリに属性が含まれている場合は、属性への変更を無視して、適用しません。エントリがディレクトリにない場合は、エントリを無効エントリとして無視します。
6	-do-	delete	属性への変更を無視して、適用しません。

表 A-43 -reconcile NORMAL 型の LDIF レコード

Sno	エントリ Changetype	属性 Changetype	説明
1	Add/No Change type	-	ディレクトリにない属性を追加し、すでに存在する属性を置換します。
2	Modrdn/Moddn	-	ldifmigrator ツールは、この変更タイプをサポートしません。
3	Delete	-	ディレクトリからエントリを削除します。
4	Modify	add	エントリに属性が含まれていない場合は、この属性が追加されます。エントリに属性が含まれている場合は、この属性を、指定した属性に置換します。エントリがディレクトリに存在しない場合は、レコードを無効として無視します。
5	-do-	replace	エントリに属性が含まれていない場合は、この属性が追加されます。エントリに属性が含まれている場合は、この属性を、指定した属性に置換します。エントリ自身がディレクトリにない場合は、レコードを無効として無視します。
6	-do-	delete	ディレクトリから指定した属性を削除します。

表 A-44 -reconcile SAFE_EXTENDED 型の LDIF レコード

Sno	エントリ Changetype	属性 Changetype	説明
1	Add/No Change type	-	新規属性のみを追加します。エントリが存在しない場合は、新規エントリを作成します。
2	Modrdn/Moddn	-	ldifmigrator ツールは、この変更タイプをサポートしません。
3	Delete	-	ディレクトリからエントリを削除しません。
4	Modify	add	この属性を追加します。エントリがディレクトリに存在しない場合は、レコードを無効として無視します。属性が存在しない場合はこの属性を追加し、存在する場合は新しい値をディレクトリに追加します。
5	-do-	replace	エントリに属性が含まれていない場合は、この属性が追加されます。エントリに属性が含まれている場合は、属性への変更を無視して、適用しません。エントリがディレクトリにない場合は、エントリを無効エントリとして無視します。
6	-do-	delete	属性への変更を無視して、適用しません。

OID 移行ツール・エラー・メッセージ

OID 移行ツールで表示できるエラー・メッセージは次のとおりです。

表 A-45 OID 移行ツール・エラー・メッセージ

メッセージ	原因	対処方法
環境変数 *ORACLE_HOME* が定義されていません。	*ORACLE_HOME* が定義されていません。	環境変数 *ORACLE_HOME* を設定してください。
入力パラメータ解析中にエラーが発生しました。確認してください。	未指定の必須パラメータがあります。必須パラメータは、Input_File、Output_File および 1 つ以上の置換変数です。	入力パラメータを正しく指定してください。`-help` オプションを使用すると、使用方法が表示されます。
Input_File パラメータが指定されていません。指定してください。	Input_File パラメータは必須パラメータです。	入力パラメータを正しく指定してください。`-help` オプションを使用すると、使用方法が表示されます。
Output_File パラメータが指定されていません。指定してください。	Output_File パラメータは必須パラメータです。	入力パラメータを正しく指定してください。`-help` オプションを使用すると、使用方法が表示されます。
指定された入力ファイルは存在しません。	ファイルの場所が誤って指定されています。	入力ファイルのパスをチェックしてください。

表 A-45 OID 移行ツール・エラー・メッセージ（続き）

メッセージ	原因	対処方法
入力ファイルをチェックしてください。0 バイトの入力ファイルです。	入力ファイルにエントリがありません。	疑似 LDIF エントリを持つ有効なファイルを指定してください。
出力ファイルを作成できません。出力ファイルはすでに存在します。	出力ファイルはすでに存在します。	Output_File フラグをチェックしてください。
アクセスが拒否されました。入力ファイルから読み込むことができません。	指定された入力ファイルに対する読取り権限がありません。	入力ファイルの読取り権限をチェックしてください。
アクセスが拒否されました。出力ファイルに作成できません。	出力ファイルを作成するための権限がありません。	出力ファイルの作成に必要な、ディレクトリの権限をチェックしてください。
ディレクトリ・サーバー名が指定されていません。-lookup オプションが使用されているときは、host パラメータを指定する必要があります	-lookup オプションが指定されている場合、host パラメータは必須です。	host パラメータを指定してください。
bind Dn パラメータが指定されていません。-lookup オプションが使用されているときは、DN パラメータを指定する必要があります	-lookup オプションが指定されている場合、DN パラメータは必須です。	DN パラメータを指定してください。
指定されたポート番号は無効です。	ポート番号は数値で指定する必要があります。	ポート番号パラメータをチェックしてください。
ディレクトリへ接続を確立することができません。入力パラメータ（host、port、DN および password）を確認してください。	指定のホストとポートでディレクトリ・サーバーを稼働できないか、または資格証明が無効です。	host、port、DN および password の各パラメータをチェックしてください。*$ORACLE_HOME*/ldap/install/LDIFMig_YYYY_MM_DD_HH_SS.log file をチェックしてください。
ディレクトリからサブスクライバ情報を取り出している際にネーミング例外が発生しました。入力パラメータを確認してください。	指定された認証管理レルムがディレクトリに存在しません。	realm パラメータをチェックしてください。
すべての置換変数が指定されたディレクトリ・サーバーで定義されていません。	認証管理レルム・エントリに必須属性が含まれていない場合、このエラーが発生します。	ディレクトリ内のレルム・エントリをチェックしてください
Oracle Internet Directory への LDIF データの移行中にエラーが発生しました。	処理中になんらかの障害（ディレクトリ・サーバーやディスクの障害など）が発生した場合に、このエラーが発生します。	エラー・メッセージを管理者にレポートしてください。

エラーが発生した場合、ログ・メッセージは次のファイルにログ記録されます。
$ORACLE_HOME/ldap/install/LDIFMig_YYYY_MM_DD_HH_SS.log

B

Oracle Internet Directory のスキーマ要素

この付録では、Oracle Internet Directory でサポートされている各種スキーマ要素の概要を説明します。これらの要素の大部分は、Internet Engineering Task Force（IETF）の ldapext および ASID ワーキング・グループによる定義に従って使用されています。

関連項目： 次の URL を参照してください。

- `http://www.ietf.org`（IETF のホームページの ldapext の Charter と LDAP Draft、LDUP の Charter と Draft）
- `http://www.iana.org`（Internet Assigned Numbers Authority のホームページ。オブジェクト識別子に関する情報）

この付録では、次の項目について説明します。

Oracle Internet Directory で施行されている IETF Requests for Comments（RFC）

Oracle Internet Directory では、Internet Engineering Task Force（IETF）の次の Requests for Comments（RFC）が施行されます。各 RFC は IETF の Web サイト `http://www.ietf.org` で入手可能です。

表 B-1　Oracle Internet Directory で施行されている RFC

RFC	タイトル
1777	Lightweight Directory Access Protocol
1778	The String Representation of Standard Attribute Syntaxes
1779	A String Representation of Distinguished Names
1960	A String Representation of LDAP Search Filters
2079	Definition of an X.500 Attribute Type and an Object Class to Hold Uniform Resource Identifiers (URIs)
2247	Using Domains in LDAP/X.500 Distinguished Names
2251	Lightweight Directory Access Protocol (v3)
2252	Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions
2253	Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names
2254	The String Representation of LDAP Search Filters
2255	The LDAP URL Format
2256	A Summary of the X.500(96) User Schema for use with LDAP v3

Oracle Internet Directory で施行されている IETF Draft

Oracle Internet Directory では、次の 2 つの IETF Draft が施行され、それぞれ IETF の Web サイト `http://www.ietf.org` で入手可能です。

- "Definition of the inetOrgPerson LDAP Object Class"
- "Referrals and Knowledge References in LDAP Directories"

Oracle Internet Directory 独自のスキーマ要素

Oracle Internet Directory 独自のスキーマには、次のカテゴリの属性とオブジェクト・クラスがあります。

- アクセス制御のスキーマ要素
- 監査ログのスキーマ要素
- 属性一意性のスキーマ要素
- 構成設定エントリのスキーマ要素
- デバッグ・ロギングのスキーマ要素
- 動的グループのスキーマ要素
- ガベージ・コレクションのスキーマ要素
- orclUserV2 オブジェクト・クラスのオプション属性
- Oracle Directory Integration and Provisioning Platform のスキーマ要素
- Oracle Internet Directory 構成のスキーマ要素
- Oracle Internet Directory サーバー管理機能のスキーマ要素
- パスワード・ポリシーのスキーマ要素
- パスワード・ベリファイアのスキーマ要素
- プラグインのスキーマ要素
- プラグインのスキーマ要素
- レプリケーションのスキーマ要素
- SSL スキーマ要素
- システム操作属性

この他に、Oracle Internet Directory のインストールには、特定の Oracle 製品で Oracle Internet Directory を使用できるようにするスキーマ要素も含まれています。これらのスキーマ要素の詳細は、各 Oracle 製品のドキュメントを参照してください。

アクセス制御のスキーマ要素

表 B-2　アクセス制御のスキーマ要素

オブジェクト・クラス	属性
orclPrivilegeGroup	orclEntryLevelACI、orclACI

監査ログのスキーマ要素

表 B-3　監査ログのスキーマ要素

オブジェクト・クラス	属性
OrclAuditOC	orclServerEvent、orcleventtype、orclauditattribute、orclauditmessage、orcleventtime、orcluserdn、orclSequence、orclAuditLevel、orclOpResult

属性一意性のスキーマ要素

表 B-4 属性一意性制約エントリ

属性名	必須	有効値	デフォルト値	デフォルト有効範囲
orcluniqueattrname	はい	任意の文字列	該当なし	該当なし
orcluniquescope	いいえ	次のいずれかの値 ■ base: ルート・エントリのみを検索 ■ onelevel: 1 レベルのみを検索 ■ sub: ディレクトリ全体を検索	sub	ディレクトリ全体を検索
orcluniqueenable	いいえ	0（無効）または 1（有効）	0	属性一意性を無効化
orcluniquesubtree	いいえ	任意の文字列	" "	ディレクトリ全体を検索
orcluniqueobjectclass	いいえ	任意の文字列	" "	すべてのオブジェクト・クラスを検索

関連項目： 8-8 ページの「コマンドライン・ツールを使用した属性一意性の有効化および無効化」

構成設定エントリのスキーマ要素

次の表に、ディレクトリ・サーバーのインスタンスの構成に使用される構成設定エントリの属性の全セットのリストとその説明を示します。

表 B-5 構成設定エントリの属性

属性	説明
orcldebugflag	このサーバー・インスタンスに関連付けられているデバッグ・レベル。configset0 のデフォルトは 0 です。値の範囲は 0 ～ 67108863 です。
orclmaxcc	データベースの最大同時接続数。configset0 のデフォルトは 10 です。この属性に負数は使用できません。
orclserverprocs	起動するサーバー・プロセスの数。configset0 のデフォルトは 1 です。この属性に負数は使用できません。
orclsslport	SSL モードのデフォルト・ポート（デフォルトは 636）。ディレクトリを保護モードで実行すると、デフォルト・ポート 636 でリスニングし、SSL ベースの TCP/IP 接続のみを受け入れます（ディレクトリを通常モードで実行すると、デフォルト・ポート 389 でリスニングし、通常の TCP/IP 接続を受け入れます）。複数の LDAP サーバー・インスタンスを追加するときは、このポートを変更することもできます。
orclnonsslport	非 SSL モードのデフォルト・ポート（デフォルトは 389）。
orclsslenable	SSL を使用可能または使用禁止にするフラグ。同じサーバーの異なるインスタンスを SSL 用または非 SSL 用に使用するときは、このフラグを使用できます。次の値のいずれかを使用できます。 ■ 0: 非保護操作のみの場合 ■ 1: SSL 認証のみの場合 ■ 2: 非保護操作と SSL 認証の両方の場合 デフォルトは 0（ゼロ）です。

表 B-5 構成設定エントリの属性（続き）

属性	説明
orclsslauthentication	フラグの値は、1、32 または 64 で、Oracle ディレクトリ・サーバーの各インスタンスに使用する認証のタイプを指定します。デフォルト値の 1 は、認証なしを意味します。異なるインスタンスに対しては、異なる値を同時に実行できます。サーバー認証、およびクライアントとサーバーの認証の値を指定する場合は、Wallet が必要です。次の 3 つの値のいずれかを使用できます。 ■ 1 = クライアントとサーバーのいずれも、他方に対して自己認証を行いません。証明書の送信または交換は行われません。「資格証明」タブの「SSL 使用可能」チェックボックスを選択して、このオプションを選択した場合は、SSL 暗号化 / 復号化のみが使用されます。 ■ 32 = サーバー認証。ディレクトリ・サーバーがクライアントに証明書を送信することによって、ディレクトリ・サーバーからクライアントに対してサーバー認証を行います。 ■ 64 = クライアントとサーバーの認証。クライアントとサーバーは、証明書を交換します。

orclsslwalleturl	Oracle Wallet の位置を設定します。この値は、Wallet の作成時に設定済です。Oracle Wallet の位置を変更する場合は、このパラメータを変更する必要があります。クライアントとサーバーの両方で Wallet の位置を設定する必要があります。たとえば UNIX では、このパラメータは次のように設定します。
	`file:/home/my_dir/my_wallet`
	Windows NT では、このパラメータは次のように設定します。
	`file:C:¥my_dir¥my_wallet`

orclsslversion	SSL のバージョン。デフォルトは 3 です。

デバッグ・ロギングのスキーマ要素

表 B-6　デバッグ・ロギングのスキーマ要素

属性	説明
orcldebugforceflush	ディレクトリ・サーバーによってメッセージが記録されたときに、デバッグ・メッセージをログ・ファイルに書き込むかどうかを指定します。これを使用可能にするには、値を 1 に設定します。これを使用禁止にするには、値を 0 に設定します。0 はデフォルト値です。 **関連項目：**10-9 ページの「ログ・ファイルへのトレース情報のフラッシュの強制」を参照してください。
orcldebugop	さらに絞り込んでロギングするには、これらの操作に対するデバッグの範囲を指定し、ログ情報を特定のディレクトリ・サーバー操作に制限します。 **関連項目：**10-7 ページの「操作デバッグ・ディメンションの設定」を参照してください。

動的グループのスキーマ要素

表 B-7 に、orclDynamicGroup オブジェクト・クラスの属性およびその説明を示します。

表 B-7　Connect By アサーションのための orclDynamicGroup 属性

属性	説明
orclConnectByAttribute	問合せのフィルタとして使用する属性。例：manager
orclConnectByStartingValue	orclConnectByAttribute 属性に指定した属性の識別名。例：Anne Smith

関連項目：　動的グループおよび Connect By アサーションについては、9-3 ページの「動的グループ」を参照してください。

ガベージ・コレクションのスキーマ要素

表 B-8 ガベージ・コレクションの構成パラメータ

属性	説明	必須	デフォルト値
orclPurgeBase	ガベージ・コレクション・タスクが適用される DIT のベース識別名	はい	ガベージ・コレクタの構成エントリ識別名の相対識別名
orclpurgestart	ガベージ・コレクタが起動を開始する時間（秒単位）。ガベージ・コレクタが使用可能な場合、この属性の値を 0 にすると、ガベージ・コレクタはすぐに使用可能になります。 書式は yyyymmddhhmmss です。	いいえ	NULL
orclpurgetargetage	ターゲット・オブジェクトの経過時間（時間単位）。この属性によって指定された時間よりも古いすべてのオブジェクトが消去されます。	いいえ	12（属性値が指定されていない場合は 10 日間）
orclPurgeInterval	ガベージ・コレクション・ジョブが再び実行される間隔（時間単位）。この間隔は、orclpurgestart 属性で指定された時点か、最終実行時間のいずれかから測定できます。	いいえ	24
orclpurgetransize	1 回のトランザクション・コミットで消去されるオブジェクト数。	いいえ	1000
orclpurgerun	この属性が追加または変更される場合は、常に、発行されたジョブがすぐに実行されることを示すインジケータ。	いいえ	該当なし
orclPurgeEnable	ガベージ・コレクタを使用可能または使用禁止にするフラグ。	いいえ	1
orclPurgeDebug	デバッグ・メッセージのコレクションを使用可能または使用禁止にするフラグ。	いいえ	0
orclpurgefilename	ガベージ・コレクションのロギング・メッセージを保存するファイル名。	いいえ	oidgc001
orclpurgefileloc	ログ・ファイルが保存されるファイルの絶対ディレクトリ。	いいえ	.（ピリオド）

事前定義されたガベージ・コレクタのスキーマ要素

Oracle Internet Directory は、ディレクトリ・サーバーのすべての不要なデータを同時にクリーンアップする、いくつかの事前定義されたガベージ・コレクタを提供します。この事前定義されたガベージ・コレクタは、次のとおりです。

- 監査ログのガベージ・コレクタ
- 変更ログのガベージ・コレクタ
- 一般統計のガベージ・コレクタ
- 健全性のガベージ・コレクタ
- セキュリティと更新イベントのガベージ・コレクタ
- システム・リソース・イベントのガベージ・コレクタ
- 削除済とマークされたエントリのガベージ・コレクタ

監査ログのガベージ・コレクタ

監査ログのガベージ・コレクタは、ディレクトリ・サーバーを監査するために作成された不要なエントリをクリーンアップします。

表 B-9 監査ログのガベージ・コレクタの属性

属性	説明	デフォルト値
orclPurgeBase	ガベージ・コレクション・タスクが適用されるネーミング・コンテキストのベース識別名。	cn=auditlog
orclpurgestart	ガベージ・コレクタが起動を開始する時間（秒単位）。ガベージ・コレクタが使用可能な場合、この属性の値を 0 にすると、ガベージ・コレクタはすぐに使用可能になります。 書式は yyyymmddhhmmss です。	NULL（Oracle Internet Directory がインストールされる当日の午前 12 時）
orclpurgetargetage	ターゲット・オブジェクトの経過時間（時間単位）。この属性によって指定された時間よりも古いすべてのオブジェクトが消去されます。	12 時間
orclPurgeInterval	ガベージ・コレクション・ジョブが再び実行される間隔（時間単位）。この間隔は、orclpurgestart 属性で指定された時点か、最終実行時間のいずれかから測定できます。	NULL（24 時間）
orclpurgetransize	1 回のトランザクション・コミットで消去されるオブジェクト数。	1000
orclpurgerun	この属性が追加または変更されるたびに、発行されたジョブがすぐに実行されます。	該当なし
orclPurgeEnable	ガベージ・コレクタを使用可能または使用禁止にするフラグ。	1

表 B-9 監査ログのガベージ・コレクタの属性（続き）

属性	説明	デフォルト値
orclPurgeDebug	デバッグ・メッセージの収集を使用可能または使用禁止にするフラグ。	0
orclpurgefilename	ガベージ・コレクションのロギング・メッセージを保存するファイル名。	oidgc001.log
orclpurgefileloc	ログ・ファイルが保存されるファイルの絶対ディレクトリ。	.（ピリオド）

変更ログのガベージ・コレクタ

変更ログのガベージ・コレクタは、ディレクトリのコンシュームされた変更ログ・エントリをクリーンアップします。

表 B-10 変更ログのガベージ・コレクタの属性

属性	説明	デフォルト値
orclPurgeBase	ガベージ・コレクション・タスクが適用されるネーミング・コンテキストのベース識別名。	cn=changelog
orclpurgestart	ガベージ・コレクタが起動を開始する時間（秒単位）。ガベージ・コレクタが使用可能な場合、この属性の値を 0 にすると、ガベージ・コレクタはすぐに使用可能になります。 書式は yyyymmddhhmmss です。	NULL（Oracle Internet Directory がインストールされる当日の午前 12 時）
orclpurgetargetage	ターゲット・オブジェクトの経過時間（時間単位）。この属性によって指定された時間よりも古いすべてのオブジェクトが消去されます。	12 時間
orclPurgeInterval	ガベージ・コレクション・ジョブが再び実行される間隔（時間単位）。この間隔は、orclpurgestart 属性で指定された時点か、最終実行時間のいずれかから測定できます。	NULL（24 時間）
orclpurgetransize	1 回のトランザクション・コミットで消去されるオブジェクト数。	1000
orclpurgerun	この属性が追加または変更されるたびに、発行されたジョブがすぐに実行されます。	該当なし
orclPurgeEnable	ガベージ・コレクタを使用可能または使用禁止にするフラグ。	1
orclPurgeDebug	デバッグ・メッセージの収集を使用可能または使用禁止にするフラグ。	0
orclpurgefilename	ガベージ・コレクションのロギング・メッセージを保存するファイル名。	oidgc001.log
orclpurgefileloc	ログ・ファイルが保存されるファイルの絶対ディレクトリ。	.（ピリオド）

一般統計のガベージ・コレクタ

一般統計のガベージ・コレクタは、ディレクトリ・サーバーに作成された不要な要約統計エントリをクリーンアップします。

表 B-11 一般統計のガベージ・コレクタの属性

属性	説明	デフォルト値
orclPurgeBase	ガベージ・コレクション・タスクが適用されるネーミング・コンテキストのベース識別名。	cn=orclgeneralstats,cn=orclsm
orclpurgestart	ガベージ・コレクタが起動を開始する時間（秒単位）。ガベージ・コレクタが使用可能な場合、この属性の値を 0 にすると、ガベージ・コレクタはすぐに使用可能になります。 書式は *yyyymmddhhmmss* です。	NULL（Oracle Internet Directory がインストールされる当日の午前 12 時）
orclpurgetargetage	ターゲット・オブジェクトの経過時間（時間単位）。この属性によって指定された時間よりも古いすべてのオブジェクトが消去されます。	12 時間
orclPurgeInterval	ガベージ・コレクション・ジョブが再び実行される間隔（時間単位）。この間隔は、orclpurgestart 属性で指定された時点か、最終実行時間のいずれかから測定できます。	NULL（24 時間）
orclpurgetransize	1 回のトランザクション・コミットで消去されるオブジェクト数。	1000
orclpurgerun	この属性が追加または変更されるたびに、発行されたジョブがすぐに実行されます。	該当なし
orclPurgeEnable	ガベージ・コレクタを使用可能または使用禁止にするフラグ。	1
orclPurgeDebug	デバッグ・メッセージの収集を使用可能または使用禁止にするフラグ。	0
orclpurgefilename	ガベージ・コレクションのロギング・メッセージを保存するファイル名。	oidgc001.log
orclpurgefileloc	ログ・ファイルが保存されるファイルの絶対ディレクトリ。	.（ピリオド）

健全性のガベージ・コレクタ

健全性のガベージ・コレクタは、ディレクトリ・サーバーに作成された不要な健全統計エントリをクリーンアップします。

表 B-12 健全性のガベージ・コレクタの属性

属性	説明	デフォルト値
orclPurgeBase	ガベージ・コレクション・タスクが適用されるネーミング・コンテキストのベース識別名。	cn=orclhealthstats, cn=orclsm
orclpurgestart	ガベージ・コレクタが起動を開始する時間（秒単位）。ガベージ・コレクタが使用可能な場合、この属性の値を 0 にすると、ガベージ・コレクタはすぐに使用可能になります。 書式は *yyyymmddhhmmss* です。	NULL（Oracle Internet Directory がインストールされる当日の午前 12 時）
orclpurgetargetage	ターゲット・オブジェクトの経過時間（時間単位）。この属性によって指定された時間よりも古いすべてのオブジェクトが消去されます。	12 時間
orclPurgeInterval	ガベージ・コレクション・ジョブが再び実行される間隔（時間単位）。この間隔は、orclpurgestart 属性で指定された時点か、最終実行時間のいずれかから測定できます。	NULL（24 時間）
orclpurgetransize	1 回のトランザクション・コミットで消去されるオブジェクト数。	1000
orclpurgerun	この属性が追加または変更されるたびに、発行されたジョブがすぐに実行されます。	該当なし
orclPurgeEnable	ガベージ・コレクタを使用可能または使用禁止にするフラグ。	1
orclPurgeDebug	デバッグ・メッセージの収集を使用可能または使用禁止にするフラグ。	0
orclpurgefilename	ガベージ・コレクションのロギング・メッセージを保存するファイル名。	oidgc001.log
orclpurgefileloc	ログ・ファイルが保存されるファイルの絶対ディレクトリ。	.（ピリオド）

セキュリティと更新イベントのガベージ・コレクタ

セキュリティと更新イベントのガベージ・コレクタは、ディレクトリ・サーバーのセキュリティおよび更新イベントを監視するために作成された不要なエントリをクリーンアップします。

表 B-13 セキュリティと更新イベントのガベージ・コレクタの属性

属性	説明	デフォルト値
orclPurgeBase	ガベージ・コレクション・タスクが適用されるネーミング・コンテキストのベース識別名。	cn=orclsecrefreshevents,cn=orclsm
orclpurgestart	ガベージ・コレクタが起動を開始する時間（秒単位）。ガベージ・コレクタが使用可能な場合、この属性の値を 0 にすると、ガベージ・コレクタはすぐに使用可能になります。 書式は *yyyymmddhhmmss* です。	NULL（Oracle Internet Directory がインストールされる当日の午前 12 時）
orclpurgetargetage	ターゲット・オブジェクトの経過時間（時間単位）。この属性によって指定された時間よりも古いすべてのオブジェクトが消去されます。	12 時間
orclPurgeInterval	ガベージ・コレクション・ジョブが再び実行される間隔（時間単位）。この間隔は、orclpurgestart 属性で指定された時点か、最終実行時間のいずれかから測定できます。	NULL（24 時間）
orclpurgetransize	1 回のトランザクション・コミットで消去されるオブジェクト数。	1000
orclpurgerun	この属性が追加または変更されるたびに、発行されたジョブがすぐに実行されます。	該当なし
orclPurgeEnable	ガベージ・コレクタを使用可能または使用禁止にするフラグ。	1
orclPurgeDebug	デバッグ・メッセージの収集を使用可能または使用禁止にするフラグ。	0
orclpurgefilename	ガベージ・コレクションのロギング・メッセージを保存するファイル名。	oidgc001.log
orclpurgefileloc	ログ・ファイルが保存されるファイルの絶対ディレクトリ。	.（ピリオド）

システム・リソース・イベントのガベージ・コレクタ

システム・リソース・イベントのガベージ・コレクタは、ディレクトリ・サーバーのシステム・リソース・イベントを監視するために作成された不要なエントリをクリーンアップします。

表 B-14 システム・リソース・イベントのガベージ・コレクタの属性

属性	説明	デフォルト値
orclPurgeBase	ガベージ・コレクション・タスクが適用されるネーミング・コンテキストのベース識別名。	cn=orclsysresourceevents, cn=orclsm
orclpurgestart	ガベージ・コレクタが起動を開始する時間（秒単位）。ガベージ・コレクタが使用可能な場合、この属性の値を 0 にすると、ガベージ・コレクタはすぐに使用可能になります。 書式は *yyyymmddhhmmss* です。	NULL（Oracle Internet Directory がインストールされる当日の午前 12 時）
orclpurgetargetage	ターゲット・オブジェクトの経過時間（時間単位）。この属性によって指定された時間よりも古いすべてのオブジェクトが消去されます。	12 時間
orclPurgeInterval	ガベージ・コレクション・ジョブが再び実行される間隔（時間単位）。この間隔は、orclpurgestart 属性で指定された時点か、最終実行時間のいずれかから測定できます。	NULL（24 時間）
orclpurgetransize	1 回のトランザクション・コミットで消去されるオブジェクト数。	1000
orclpurgerun	この属性が追加または変更されるたびに、発行されたジョブがすぐに実行されます。	該当なし
orclPurgeEnable	ガベージ・コレクタを使用可能または使用禁止にするフラグ。	1
orclPurgeDebug	デバッグ・メッセージの収集を使用可能または使用禁止にするフラグ。	0
orclpurgefilename	ガベージ・コレクションのロギング・メッセージを保存するファイル名。	oidgc001.log
orclpurgefileloc	ログ・ファイルが保存されるファイルの絶対ディレクトリ。	.（ピリオド）

削除済とマークされたエントリのガベージ・コレクタ

削除済とマークされたエントリのガベージ・コレクタは、削除されたとみなされる不要なエントリをクリーンアップします。

表 B-15 削除済とマークされたエントリのガベージ・コレクタの属性

属性	説明	デフォルト値
orclPurgeBase	ガベージ・コレクション・タスクが適用されるネーミング・コンテキストのベース識別名。	cn=tombstone
orclpurgestart	ガベージ・コレクタが起動を開始する時間（秒単位）。ガベージ・コレクタが使用可能な場合、この属性の値を 0 にすると、ガベージ・コレクタはすぐに使用可能になります。 書式は *yyyymmddhhmmss* です。	NULL（Oracle Internet Directory がインストールされる当日の午前 12 時）
orclpurgetargetage	ターゲット・オブジェクトの経過時間（時間単位）。この属性によって指定された時間よりも古いすべてのオブジェクトが消去されます。	12 時間
orclPurgeInterval	ガベージ・コレクション・ジョブが再び実行される間隔（時間単位）。この間隔は、orclpurgestart 属性で指定された時点か、最終実行時間のいずれかから測定できます。	NULL（24 時間）
orclpurgetransize	1 回のトランザクション・コミットで消去されるオブジェクト数。	1000
orclpurgerun	この属性が追加または変更されるたびに、発行されたジョブがすぐに実行されます。	該当なし
orclPurgeEnable	ガベージ・コレクタを使用可能または使用禁止にするフラグ。	1
orclPurgeDebug	デバッグ・メッセージの収集を使用可能または使用禁止にするフラグ。	0
orclpurgefilename	ガベージ・コレクションのロギング・メッセージを保存するファイル名。	oidgc001.log
orclpurgefileloc	ログ・ファイルが保存されるファイルの絶対ディレクトリ。	.（ピリオド）

Oracle Internet Directory ガベージ・コレクションのプラグイン

ガレージ・コレクション・フレームワークは、ガベージ・コレクション・エンジンをトリガーする Oracle Internet Directory プラグイン・フレームワークに依存します。この項では、ガベージ・コレクション・プラグインが様々な操作に使用する属性値のペアを説明します。

ガベージ・コレクタ作成の属性

ガベージ・コレクタを作成するには、ガベージ・コレクション・プラグインで、表 B-16 に示す属性値ペアを使用します。

表 B-16　ガベージ・コレクタ作成の属性値ペア

属性	値
orclpluginname	PurgeAdmin
orclplugintype	operational
orclplugintiming	post
orclpluginldapoperation	ldapadd
orclpluginsubscriberdnlist	cn=purgeconfig,cn=subconfigsubentry

ガベージ・コレクタ変更の属性

ガベージ・コレクタを変更するには、ガベージ・コレクション・プラグインで、表 B-17 に示す属性値ペアを使用します。

表 B-17　ガベージ・コレクタ変更の属性値ペア

属性	値
orclpluginname	PurgeAdmin
orclplugintype	operational
orclplugintiming	post
orclpluginldapoperation	ldapmodify
orclpluginsubscriberdnlist	cn=purgeconfig,cn=subconfigsubentry

ガベージ・コレクタ削除の属性

ガベージ・コレクタを削除するには、ガベージ・コレクション・プラグインで、表 B-18 に示す属性値ペアを使用します。

表 B-18　ガベージ・コレクタ削除の属性値ペア

属性	値
orclpluginname	PurgeAdmin
orclplugintype	operational
orclplugintiming	post
orclpluginldapoperation	ldapdelete
orclpluginsubscriberdnlist	cn=purgeconfig,cn=subconfigsubentry

orclUserV2 オブジェクト・クラスのオプション属性

orclUserV2 オブジェクト・クラスのオプション属性は次のとおりです。

表 B-19　orclUserV2 オブジェクト・クラスの属性

属性	説明
OrclPassword	データベース・サーバーに対する O3Logon と同様の、カスタム認証スキームに対する Oracle 固有のパスワードを識別します。
OrclHireDate	従業員が企業で勤務を開始する日付を指定します。
OrclDefaultProfileGroup	ユーザーのデフォルト・グループを指定するためのグループの名前（識別名）を保持します。ユーザーのデフォルト・プロファイルは、この属性値に基づいて作成できます。
OrclPasswordHint	ユーザーのかわりにパスワードを管理するために、ユーザーが設定する質問を指定します。
OrclPasswordHintAnswer	orclPasswordHint に対して設定する回答を指定します。
OrclTimeZone	ユーザーの事務所の場所に基づいた地理的なタイムゾーンを示します。有効な値は、EST、PST、GMT など 3 文字のタイムゾーン値です。
OrclIsVisisble	個人検索アプリケーションでユーザー・エントリを表示するかどうかを指定します。
OrclDisplayPersonalInfo	ホワイト・ページ検索で、ユーザーの個人情報を表示するかどうかを指定します。

表 B-19 orclUserV2 オブジェクト・クラスの属性（続き）

属性	説明
OrclWorkflowNotificationPref	Oracle Workflow に対する通知方法を指定します。
OrclMaidenName	ユーザーの旧姓を指定します。
OrclDateOfBirth	ユーザーの誕生日を指定します。
orclActiveStartDate	ユーザーが Oracle Application Server Single Sign-On Server に対して正常に認証を開始できる日付を指定します。値は、協定世界時の書式で表します。
orclActiveEnddate	この日を過ぎるとユーザーが Oracle Application Server Single Sign-On Server に対して認証が不可能になる日付を指定します。値は、協定世界時の書式で表します。

Oracle Directory Integration and Provisioning Platform のスキーマ要素

表 B-20 サード・パーティ・ディレクトリの統合プロファイルの属性

属性	説明
一般情報	-
プロファイル名（orclodipAgentName）	統合する特定のサード・パーティ・ディレクトリのプロファイル名。この属性は必須です。
同期モード（orclodipSynchronizationMode）	Oracle Internet Directory と接続ディレクトリ間での同期の方向。 IMPORT はサード・パーティ・ディレクトリから Oracle Internet Directory への変更のインポートを示します。 EXPORT は Oracle Internet Directory からサード・パーティ・ディレクトリへの変更のエクスポートを示します。
プロファイル・ステータス（orclOdipAgentControl）	プロファイルが使用可能か使用禁止かを示すインジケータ。デフォルトは「DISABLE」です。この値は「ENABLE」に設定する必要があります。
プロファイル・パスワード（orclodipProfilePassword）	プロファイルが Oracle Internet Directory へのバインドで使用するパスワード。インポートの場合、変更はプロファイル名と同様に識別情報に対しても行われます。デフォルトの値は welcome です。 **注意：**セキュリティ上の理由から、このパスワードは変更してください。

表 B-20 サード・パーティ・ディレクトリの統合プロファイルの属性（続き）

属性	説明
スケジューリングの間隔 (orclODIPSchedulingInterval)	接続ディレクトリが Oracle Internet Directory と同期化されるまでの間隔（秒単位）。デフォルトは 600 です。 この属性は変更できます。
最大試行回数 (orclodipSyncRetryCount)	失敗した場合に Oracle Directory Integration and Provisioning Server がサード・パーティ・ディレクトリ・コネクタの実行を試行する最大回数。デフォルトは 5 です。
プロファイルのバージョン	このプロファイルが作成された Oracle Directory Integration and Provisioning Platform のバージョン。デフォルト値は 1.0 です。この属性は変更できません。
デバッグ・レベル (orclodipdebuglevel)	任意のプロファイルに必要なデバッグのレベルを示す識別子。 この値を最大デバッグ・レベルの 63 に設定します。 **関連項目：**10-6 ページの「デバッグ・ロギング・レベルの設定」を参照してください。
実行情報	-
エージェント実行コマンド (orclodipAgentExeCommad)	Directory Integration and Provisioning Server が使用する、コネクタ実行可能ファイルの名前と引数のリスト。このリストは、コネクタの起動時に、コマンドライン引数として渡すことができます。 **関連項目：**コマンドラインで引数を渡す一般的な使用方法は、第 39 章「Oracle Human Resources との同期化」を参照してください。
接続ディレクトリ・アカウント (orclodipConDirAccessAccount)	コネクタが同期で使用する、接続ディレクトリ内の有効なユーザー・アカウント。この値は、統合している接続ディレクトリ固有です。たとえば、SunONE 同期コネクタの場合は、これは SunONE ディレクトリ・サーバー内の有効なバインド識別名です。Human Resources コネクタの場合は、これは Oracle Human Resources データベース内の有効なユーザー識別子です。他のコネクタの場合のユーザー・アカウントは、コマンドライン引数としてコネクタの起動時に渡すことができます。 **関連項目：**コマンドラインで引数を渡す一般的な使用方法は、第 39 章「Oracle Human Resources との同期化」を参照してください。

表 B-20 サード・パーティ・ディレクトリの統合プロファイルの属性（続き）

属性	説明
接続ディレクトリ・アカウント・パスワード（orclodipConDirAccessPassword）	接続ディレクトリへの接続に対して、orclOdipConDirAccessAccount 属性で指定されたユーザーが使用するパスワード。この値は、統合しているサード・パーティ・ディレクトリ固有です。たとえば、SunONE 同期コネクタの場合は、これは SunONE ディレクトリ・サーバー内の有効なバインド・パスワードです。Human Resources エージェントの場合のパスワードは、Oracle Human Resources データベース・パスワードです。
追加構成情報（orclodipAgentConfigInfo）	コネクタが Oracle Internet Directory に格納する構成情報。この構成情報は、コネクタの起動時に、Directory Integration and Provisioning Server によってコネクタに渡されます。この情報は属性として格納され、Directory Integration and Provisioning Server はその内容を認識しません。コネクタの実行がスケジューリングされている場合、属性の値はそのコネクタが処理できるように、*$ORACLE_HOME*/ldap/odi/conf/*profile_name*.cfg ファイルに格納されます。 ファイルは、Directory Integration and Provisioning Assistant または ldapuploadagentfile.sh ツールを使用してアップロードしてください。アップロードは、インポートとエクスポートの両方のエージェントについて実行してください。 **関連項目：** ■ A-106 ページの「Directory Integration and Provisioning Assistant」 ■ A-118 ページの「ldapUploadAgentFile.sh ツールの構文」
接続ディレクトリの URL（orclOdipConDirURL）	接続ディレクトリへの接続に必要な接続詳細。このパラメータは、ホスト名とポート番号を *host*:*port*:*sslmode* の形式で示します。 SSL を使用して接続するには、*host*:*port*:1 を入力します。 ディレクトリに接続するための証明書が Wallet に格納され、その場所がファイル odi.properties に指定されていることを確認します。 **注意：**SSL を使用して SunONE Directory Server に接続するには、サーバー証明書を Wallet にロードする必要があります。 **関連項目：**『Oracle Advanced Security 管理者ガイド』の Oracle Wallet Manager についての章を参照してください。

表 B-20 サード・パーティ・ディレクトリの統合プロファイルの属性（続き）

属性	説明
インタフェース・タイプ (orclodipInterfaceType)	同期に使用するデータ形式またはプロトコル。次の値がサポートされます。 ■ LDIF: LDIF ファイルとの間のインポートまたはエクスポート。 ■ TAGGED: タグ付きファイルとの間のインポートまたはエクスポート。タグ付きファイルは、LDIF 形式と同様に、Oracle Directory Integration and Provisioning Server がサポートする独自の形式です。 ■ LDAP: LDAP 準拠のディレクトリとの間のインポートまたはエクスポート。 ■ DB: Oracle9*i* データベース・サーバー・ディレクトリとの間のインポートまたはエクスポート。
マッピング情報	-
マッピング・ルール (orclodipAttributeMappingRules)	マッピング・ルールを格納するための属性。マッピング・ルールは、Directory Integration and Provisioning Assistant または ldapuploadagentfile.sh ツールを使用してファイルに格納します。 **関連項目：** ■ 33-5 ページの「マッピング・ルールとその形式」 ■ 33-7 ページの「マッピング・ルール属性の形式」 ■ A-106 ページの「Directory Integration and Provisioning Assistant」
接続ディレクトリの照合フィルタ (orclodipConDirMatchingFilter)	この属性は、サード・パーティ・ディレクトリの変更ログに適用するフィルタを指定します。この属性は、インポート・プロファイルで使用されます。インポートとエクスポートの統合プロファイルの両方が使用可能な場合、フィルタは、インポート・プロファイルに次のように設定する必要があります。 Modifiersname != *connected_directory_account* この設定によって、同じ変更が 2 つのディレクトリ間で無期限に交換されることを防止します。 混乱を避けるため、このアカウントを同期化固有にします。

表 B-20 サード・パーティ・ディレクトリの統合プロファイルの属性（続き）

属性	説明
OID 照合フィルタ（orclOdipOIDMatchingFilter）	エクスポート・プロファイルでは、この属性は Oracle Internet Directory 変更ログ・コンテナに適用するフィルタを指定します。この属性は、エクスポート・プロファイルで使用されます。インポートとエクスポートの統合プロファイルの両方が使用可能な場合、フィルタは、エクスポート・プロファイルに次のように設定する必要があります。 `Modifiersname != orclodipagentname=iPlanetImport, cn=subscriber profile,cn= changelog subscriber,cn=oracle internet directory` この設定によって、同じ変更が 2 つのディレクトリ間で無期限に交換されることを防止します。 インポート・プロファイルでは、この属性は Oracle Internet Directory と接続ディレクトリ間のエントリをマッピングするためのキーを指定します。この属性は、識別名をキーとして使用できない場合に便利です。
ステータス情報	-
OID の最後に適用された変更番号（orclLastAppliedChangeNumber）	エクスポート操作で、Oracle Internet Directory から接続ディレクトリに適用された最後の変更。デフォルト値は 0（ゼロ）です。これを Oracle Internet Directory の lastchangenumber 属性の値に設定します。LDAP を使用してブートストラップするために Directory Integration and Provisioning Assistant を使用した場合、ブートストラップ・プロセスの最後にこの値が自動的に設定されます。 これは、エクスポート・プロファイルでのみ有効です。
最終実行時間（orclodipLastExecutionTime）	Oracle Directory Integration and Provisioning Server が統合プロファイルを正常に実行した最新の日時に設定されたステータス属性。書式は dd-mon-yyyy hh:mm:ss で、hh は 24 時間書式での時刻です。この属性は、プロファイル作成中に初期化されます。
前回成功実行日時（orclodipLastSuccessfulExecution Time）	Oracle Directory Integration and Provisioning Server が統合プロファイルを正常に実行した最新の日時に設定されたステータス属性。書式は dd-mon-yyyy hh:mm:ss で、hh は 24 時間書式での時刻です。

表 B-20 サード・パーティ・ディレクトリの統合プロファイルの属性（続き）

属性	説明
同期ステータス (orclodipSynchronizationStatus)	最後に実行した同期のステータスで、成功または失敗のいずれかです。 最初は、この属性の値は Yet to be executed になっています。この属性は読取り専用です。
同期エラー (orclodipSynchronizationErrors)	最後の実行に失敗した場合のエラーを説明するメッセージ。このパラメータは Oracle Directory Integration and Provisioning Server によって更新されます。この属性は読取り専用です。
最後に適用された変更番号 (orclodipConDirLastAppliedChgNum)	インポート操作で、接続ディレクトリから Oracle Internet Directory に適用された最後の変更。デフォルト値は 0（ゼロ）です。これを Oracle Internet Directory の lastchangenumber 属性の値に設定します。LDAP を使用してブートストラップするために Directory Integration and Provisioning Assistant を使用した場合、ブートストラップ・プロセスの最後にこの値が自動的に設定されます。 これは、インポート・プロファイルでのみ有効です。

関連項目： SunONE Directory Server との統合の詳細は、42-8 ページの「デフォルト・パラメータの更新」を参照してください。

Oracle Internet Directory 構成のスキーマ要素

表 B-21 Oracle Internet Directory 構成パラメータ

オブジェクト・クラス	属性
subconfig、 orclConfigSet、 orclLDAPSubConfig、 orclREPLSubConfig、 orclcontainerOC、 subregistry、 orclLDAPInstance、 orclREPLInstance、 orclIndexOC、 orcleventLog、 orclEvents	orcldebugflag、orclMaxCC、orclDBType、orclSuffix、 orclDITRoot、orclSuName、orclSuPassword、 orclSizeLimit、orclTimeLimit、orclGuName、 orclGuPassword、orclServerProcs、 orclconfigsetnumber、orclhostname、 orclIndexedAttribute、orclCatalogEntryDN、 orclServerMode、orclPrName、orclPrPassword、 orclUseEncrypt、orclDirectoryVersion

Oracle Internet Directory サーバー管理機能のスキーマ要素

表 B-22 Oracle Internet Directory サーバー管理機能の属性

属性	説明
orclStatsFlag	Oracle Internet Directory サーバー管理機能フレームワークを使用可能にするかどうかを示します。使用可能にするには、1 に設定します。使用禁止にするには、0（ゼロ）に設定します。
orclStatsPeriodicity	サンプル統計を収集する頻度、つまり間隔（分単位）を指定します。1（分単位）以上を設定します。 OrclStatsLevel が有効で（ユーザー統計が実行されていて）ユーザー数が少ない場合は、この属性に大きい値を指定します。逆に、ユーザー数が多い場合は、小さい値を指定します。
OrclEventLevel	記録する必要があるセキュリティおよびシステムに関連する重要なイベントを指定します。デフォルトは 0 で、重要ではないイベントは記録されません。 スーパー・ユーザー、プロキシ・ユーザー、レプリケーション・ログイン以外のイベントについては、orclStatsFlag 属性 1 の値を設定します。 **関連項目：**監視できる重要なイベントのリストは、10-22 ページの「重要なイベントの構成」を参照してください。
OrclStatsLevel	ユーザーの統計収集のレベルを指定します。このリリースで有効な値は、1 のみです。この値を指定すると、ディレクトリおよび各操作を実行するユーザーに対するバインド操作および比較操作の数が収集されます。
OrclMaxTcpIdleConnTime	アイドル状態として記録される、アイドル接続の最大 TCP 接続時間（分単位）を指定します。このデフォルト値は、120 分（2 時間）です。この属性の値は、DSA 構成設定属性 orclLDAPconnTimeOut の値未満にする必要があることに注意してください。

パスワード・ポリシーのスキーマ要素

pwdPolicy オブジェクト・クラスは、所定の DIT に一組のユーザーのパスワード・ポリシー情報が含まれる補助オブジェクト・クラスです。これには、ディレクトリ全体のパスワード・ポリシー情報を定義する属性が含まれます。

表 B-23 に、pwdPolicy オブジェクト・クラスの属性およびその説明を示します。これらの各属性のデフォルト値は 0（ゼロ）です。これらは単一値の属性です。ただし、orclpwdIllegalValues は複数値の属性です。

表 B-23 pwdPolicy オブジェクト・クラスの属性

属性	ポリシー	説明
orclpwdAlphaNumeric	パスワード内の数字の数	パスワードに必要な数字の文字数。デフォルトでは、1 文字の数字が必要です。つまり、デフォルト値は 1 です。
orclpwdencryptionenable	ユーザー・パスワードの可逆暗号化を使用可能にする	値が TRUE の場合、ユーザー・パスワードは可逆暗号化形式で保存されます。
orclpwdIllegalValues	パスワード無効値	有効なパスワードとして値を使用できない一般的な語と属性の型が含まれる複数値属性。デフォルトでは、すべての語をパスワードの値として使用できます。
orclpwdipmaxfailure	IP のロックアウト失敗の最大数	アカウントがロックされた後、特定の IP アドレスからログイン失敗の最大数を指定します。
orclpwdToggle	旧パスワードを新規パスワードに変更	ユーザーの旧パスワードを新規パスワードとして使用できるかどうかを指定します。デフォルトは使用可能です。デフォルト値は 1 です。
orlcpwdiplockout	IP ロックアウト	特定の IP アドレスにアカウント・ロックアウトを施行するかどうかを指定します。TRUE の値は、ロックアウトを施行します。デフォルトは FALSE です。
pwdAllowUserChange	ユーザー定義パスワード	ユーザーが自身のパスワードを変更できるかどうかを示すインジケータ。変更が許可されている場合、ユーザーは Idapmodify を使用してパスワードを変更できます。変更が許可されていない場合は、ディレクトリ・サーバーはユーザーにパスワードを変更する権限があることを検証します。ユーザーが適切な権限を持っていない場合、ディレクトリ・サーバーはクライアントにエラー・メッセージを送信します。 デフォルトでは、ユーザー定義パスワードが許可されています。

表 B-23 pwdPolicy オブジェクト・クラスの属性（続き）

属性	ポリシー	説明
pwdCheckSyntax	パスワード構文のチェック	構文チェックを実行するかどうかを示すインジケータ。1 の場合、構文チェックが実行されます。デフォルト値は 1 です。 デフォルトでは、パスワード構文チェックはオンに設定されており、ユーザー・パスワードに 1 文字の数字を含める必要があります。
orclpwdpolicyenable	パスワード・ポリシーを使用可能または使用禁止にする	使用可能 =1 使用禁止 =0
pwdExpireWarning	パスワードの期限切れ警告	パスワードが期限切れになる前に、ディレクトリ・サーバーからユーザーに警告が送信される期間（秒数）。パスワードに有効期限が設定してある場合、デフォルトでは期限切れ前にディレクトリ・サーバーからユーザーに警告は送信されません。 この警告は、ユーザーがログオンするたびに送信されます。期限切れになる前にユーザーがパスワードを変更しなかった場合、管理者がパスワードを変更するまで、ユーザーはロックアウトされます。 この機能を有効にするには、クライアントのアプリケーションがこの機能に対応している必要があります。 デフォルトは 0（ゼロ）で、警告は送信されません。 例 : pwdMaxAge が 7200、pwdExpireWarning が 3600 の場合、パスワードは 2 時間後に期限切れになります。最終 1 時間でバインドしている場合は、パスワードの期限切れが近いことが警告されます。
pwdFailureCountInterval	パスワード失敗のカウント間隔	パスワードの失敗回数がユーザー・エントリから削除されるまでの秒数。この属性が存在しない場合またはその値が 0（ゼロ）の場合、失敗回数は削除されません。デフォルトは 0（ゼロ）です。
pwdGraceLoginLimit	パスワード期限切れ後の猶予期間ログインの数	パスワードの期限切れ後に許可する猶予期間ログインの最大数。デフォルトでは、猶予期間ログインは許可されません。デフォルト値は 3 です。

表 B-23 pwdPolicy オブジェクト・クラスの属性（続き）

属性	ポリシー	説明
pwdInHistory	パスワードの履歴数	ディレクトリ・サーバーが保存するユーザーの過去のパスワード数。ユーザーが、ディレクトリ・サーバーに格納されているパスワードを再利用しようとすると、そのパスワードは拒否されます。ディレクトリ・サーバーは、デフォルトではパスワードの履歴を保持しません。
pwdLockout	パスワードのロックアウト	ユーザーのバインド試行が pwdmaxFailure で指定された回数、連続して失敗した場合、ユーザーをディレクトリからロックアウトするかどうかを指定します。このポリシー属性の値が 1 の場合、ユーザーはロックアウトされます。この属性が存在しない場合またはその値が 0（ゼロ）の場合、ユーザーはロックアウトされず、pwdMaxFailure の値は無視されます。デフォルトでは、アカウントのロックアウトが施行されます。3 回連続してログインに失敗すると、アカウントはロックされます。
pwdLockoutDuration	アカウント・ロックアウト継続時間	次の両方に該当する場合にユーザーがディレクトリからロックアウトされる秒数。 ■ アカウントのロックアウトが有効な場合。 ■ pwdMaxFailure で指定された回数以上の試行を行うと、ディレクトリへのバインドが不可能になる場合。 特定の時間の間または管理者がパスワードを再設定するまでの間、ユーザーをロックアウトできます。デフォルト値の 0（ゼロ）では、ユーザーは永久にロックアウトされます。
pwdMaxAge	パスワード有効期限	指定したパスワードの最大有効期限（秒数）。この属性が存在しない場合またはその値が 0（ゼロ）の場合、パスワードは期限切れになりません。デフォルトのパスワード有効期限は 60 日です。
pwdMaxFailure	パスワード失敗の最大数	ユーザー・アカウントがロックされるまでの、連続したバインド失敗回数。この属性が存在しない場合またはその値が 0（ゼロ）の場合、バインドの失敗によってアカウントがロックされることはなく、パスワードのロックアウト・ポリシーの値は無視されます。デフォルトは 4 です。
pwdMinLength	パスワードの最小文字数	パスワードに必要な最小文字数。デフォルトの最小文字数は 5 です。ただし、この属性の値には少なくとも 1 を指定する必要があります。

表 B-23 pwdPolicy オブジェクト・クラスの属性（続き）

属性	ポリシー	説明
pwdMustChange	再設定後のパスワード変更	最初のログイン後またはパスワードが管理者によって再設定された後、ユーザーがパスワードを変更する必要があるかどうかを示すインジケータ。このオプションが使用可能である場合、ユーザー定義パスワードが使用禁止になっていても、ユーザーはパスワードを変更する必要があります。デフォルトでは、ユーザーは再設定後にパスワードを変更する必要はありません。

関連項目： 15-4 ページの「概要 : 認証管理レルムに対するパスワード・ポリシーの設定」

また、前述の pwdpolicysubentry に加え、オブジェクト・クラスの Top には、各ユーザー・エントリに対するユーザー・パスワードの状態情報を保持するために、次の操作属性が含まれています。

表 B-24 TOP オブジェクト・クラスのパスワード・ポリシーの操作属性

属性	説明
orclrevpwd	ユーザー・パスワードの可逆暗号化値。この属性は、パスワード・ポリシー・エントリの属性 orclpwdencryptionenable が TRUE に設定されている場合にのみ生成されます。orclrevpwd 属性は、SSL サーバー認証メカニズムおよび SSL クライアントとサーバー認証メカニズムでのみ問合せが可能です。非 SSL セッションでは、この属性の問合せはできません。 **関連項目：** 16-2 ページの「Oracle Internet Directory に対する認証用パスワード・ベリファイアの格納および管理」
orclpwdipaccountlockedtime	ユーザーが特定の IP アドレス以外からロックアウトされた時刻
orclpwdlastlogintime	ユーザーによる最終ログインのタイムスタンプ
pwdAccountLockedTime	ユーザーのアカウントがロックされた日時。
pwdChangedtime	ユーザー・パスワードが作成または変更されたときのタイムスタンプ。
pwdExpirationWarned	ユーザーにパスワードの期限切れ警告が初めて送信された日時。
pwdFailuretime	ユーザーが連続してログインに失敗したときのタイムスタンプ。

表 B-24 TOP オブジェクト・クラスのパスワード・ポリシーの操作属性（続き）

属性	説明
pwdGraceUseTime	ユーザーによる各猶予期間ログインのタイムスタンプ。
pwdHistory	ユーザーが以前に使用したパスワードの履歴。
pwdReset	パスワードが再設定されたため、最初の認証でユーザーがパスワードを変更する必要があることを示すインジケータ。

関連項目： 15-4 ページの「概要 : 認証管理レルムに対するパスワード・ポリシーの設定」

パスワード・ベリファイアのスキーマ要素

ディレクトリと Oracle コンポーネントの両方とも、ユーザー・パスワードをユーザー・エントリに格納しますが、格納する属性は異なります。ディレクトリは、userPassword 属性にユーザー・パスワードを格納しますが、Oracle コンポーネントは、ユーザー・パスワード・ベリファイアを authPassword、orclPasswordVerifier または orclpassword 属性に格納します。Oracle コンポーネントで使用する各属性の説明は、B-29 ページの表 B-25 を参照してください。

表 B-25 ユーザー・エントリにパスワード・ベリファイアを格納するための属性

属性	説明
authPassword	パスワードが、ディレクトリに対してユーザー認証を行うために使用するパスワード userpassword と同じ場合に、パスワードを Oracle コンポーネントに格納するための属性。この属性の値は、userpassword 属性の値と同期します。 複数の異なるアプリケーションで、ディレクトリに使用したクリア・テキスト・パスワードと同じパスワードの入力をユーザーに要求できます。ただし、各アプリケーションでは、異なるアルゴリズムを使用してそのパスワードがハッシュされる場合があります。この場合は、同じクリア・テキスト・パスワードが、複数の異なるパスワード・ベリファイアのソースとなります。 この属性は複数値の属性であるため、異なるアプリケーションがこのユーザーのクリア・テキスト・パスワードに対して使用する他のすべてのベリファイアを格納できます。userpassword 属性を変更すると、すべてのアプリケーションの authpasswords が再生成されます。

表 B-25 ユーザー・エントリにパスワード・ベリファイアを格納するための属性（続き）

属性	説明
orclPasswordVerifier	パスワードが、ディレクトリに対してユーザー認証を行うために使用するパスワード userpassword と異なる場合に、パスワードを Oracle コンポーネントに格納するための属性。この属性の値は、userpassword 属性の値とは同期しません。 authPassword と同様に、この属性は複数値の属性であるため、異なるアプリケーションがこのユーザーのクリア・テキスト・パスワードに対して使用する他のすべてのベリファイアを格納できます。
orclPassword	エンタープライズ・ユーザー用の 03LOGON ベリファイアのみを格納するための属性。03LOGON ベリファイアは、userpassword 属性と同期し、デフォルトでは、orcluserv2 オブジェクト・クラスに関連付けられたすべてのユーザー・エントリに対して生成されます。 Oracle Internet Directory をインストールすると、デフォルトではルート Oracle コンテキストにデータベース・セキュリティ・プロファイルのエントリが作成されます。このエントリの存在によって、orcluserv2 オブジェクト・クラスに関連付けられたユーザー・エントリを対象とする 03LOGON ベリファイアが生成されます。

これらの属性の型には、属性サブタイプとして appID があります。この属性サブタイプで特定のアプリケーションを一意に識別します。たとえば、appID はアプリケーション・エントリの ORCLGUID にできます。この属性サブタイプは、アプリケーションのインストール時に生成されます。

プラグインのスキーマ要素

orclPluginConfig オブジェクト・クラスは、すべてのプラグイン・エントリに関連付ける必要がある構造型オブジェクト・クラスです。このスーパークラスは top です。表 B-26 に、その属性および説明を示します。

表 B-26 プラグインの属性名と属性値

属性名	属性値	必須
Cn	プラグイン・エントリ名	はい
orclPluginAttributeList	プラグインの実行を制御する、セミコロンで区切られた識別名のリスト。ターゲット属性がリストに含まれている場合は、プラグインが呼び出されます。	いいえ
orclPluginEnable	0 = 使用禁止（デフォルト） 1 = 使用可能	いいえ
orclPluginEntryProperties	LDAP 検索フィルタ・タイプの値は、この属性で指定する必要があります。たとえば、orclPluginEntryProperties:(&(objectclass=inetorgperson)(sn=Cezanne)) を指定した場合、ターゲット・エントリに inetorgperson と同等の objectclass および Cezanne と同等の sn が含まれていると、そのプラグインは起動しません。	いいえ
orclPluginIsReplace	操作時タイミングのプラグインの場合のみ 0 = 使用禁止（デフォルト） 1 = 使用可能	いいえ
orclPluginKind	PL/SQL	いいえ
orclPluginLDAPOperation	次のいずれかの値です。 ldapcompare ldapmodify ldapbind ldapadd ldapdelete ldapsearch	はい

表 B-26 プラグインの属性名と属性値（続き）

属性名	属性値	必須
orclPluginName	プラグイン・パッケージ名	はい
orclPluginRequestGroup	セミコロンで区切られたグループのリストで、プラグインの実行を制御します。このグループを使用して、プラグインを実際に起動するユーザーを指定できます。 たとえば、プラグインの登録時に orclpluginrequestgroup:cn=security,cn=groups,dc=oracle,dc=com を指定すると、グループ cn=security,cn=groups,dc=oracle,dc=com に属するユーザーが LDAP 要求を送信しないかぎり、プラグインは起動しません。	いいえ
orclPluginRequestNegGroup	セミコロンで区切られたグループのリストで、プラグインの実行を制御します。このグループを使用して、プラグインを起動できないユーザーを指定できます。たとえば、プラグインの登録時に orclpluginrequestneggroup:cn=security,cn=groups,dc=oracle,dc=com を指定すると、グループ cn=security,cn=groups,dc=oracle,dc=com に属するユーザーが LDAP 要求を送信しても、プラグインは起動しません。	いいえ
orclPluginResultCode	LDAP の結果コードを指定する整数値。この値を指定すると、LDAP 操作がこの結果コードの状態の場合にのみ、プラグインが起動します。 この属性は POST プラグイン・タイプにのみ有効です。	いいえ
orclPluginShareLibLocation	動的リンク・ライブラリのファイル位置。この値が未指定の場合、Oracle Internet Directory サーバーはプラグイン言語を PL/SQL とみなします。	いいえ

表 B-26 プラグインの属性名と属性値（続き）

属性名	属性値	必須

orclPluginSubscriberDNList	セミコロンで区切られた識別名のリストで、プラグインの実行を制御します。次に例を示します。
	orclPluginSubscriberDNList=
	dc=COM,c=us;
	dc=us,dc=oracle,dc=com;
	dc=org,dc=us;
	o=IMC,c=US
	LDAP 操作のターゲット識別名がリストに含まれている場合は、プラグインが起動されます。
		いいえ

orclPluginTiming	次のいずれかの値です。 pre when post **関連項目：**これらの値の説明は、45-2 ページの「ディレクトリ・サーバー・プラグインの概要」を参照してください。	いいえ
orclPluginType	次のいずれかの値です。 operational attribute password_policy syntax matchingrule **関連項目：**『Oracle Internet Directory アプリケーション開発者ガイド』の Oracle Internet Directory サーバーのプラグイン・フレームワークに関する章を参照してください。	はい
orclPluginVersion	サポート対象のプラグイン・バージョン番号	いいえ

リソース情報のスキーマ要素

この項では、次のものの属性について説明します。

- リソース・アクセス記述子（RAD）
- リソース・タイプ情報

リソース・アクセス記述子オブジェクトには、属性およびその説明が含まれています。

表 B-27 リソース・アクセス記述子（RAD）の属性

属性	説明
orclResourceName	接続情報が保持されているリソースの名前を指定します。
orclOwnerGlobalID	設定項目が格納されるユーザーまたはグループを指定します。この属性の値は、ユーザー・エントリまたはグループ・エントリの GUID（orclGlobalID）属性の値と同じです。この属性は、自己管理アクセス・ポリシーを一般的なポリシーとして抽象化する場合およびユーザーの GUID を指定して設定項目を問い合せる場合に有効です。 たとえば、Acme Corporation のユーザー John Doe が、自身の拡張設定項目を格納する必要があるとします。この場合、実際のユーザー・エントリの大半は、ユーザーおよびユーザーの認証資格証明に関するホワイト・ページ情報となります。また、このユーザー・エントリには、ユーザーを一意に識別する属性の 1 つとして orclGUID も含まれます。リソース・アクセス情報の格納中、orclOwnerGlobalID 属性の値の指定には、同じ orclGUID 属性の値が使用されます。実行時、すべてのアプリケーションでユーザー John Doe のグローバル識別子が認識されるため、アプリケーションを使用して、このユーザーのすべての設定項目値に対するディレクトリを簡単に問い合せることができます。
orclApplicationGUID	ユーザー設定項目が格納されているアプリケーション・エンティティのグローバル識別子を指定します。この属性の値は、アプリケーション・エンティティの GUID（orclGUID）属性の値と同じです。この属性は、ユーザーに関するアプリケーション固有のリソース・アクセス情報をユーザーのコンテナ・オブジェクトに格納する場合に有効です（2-34 ページの図 2-10 を参照）。
orclResourceTypeName	リソース（データベース、XMLPDS、JDBCPDS など）の名前を指定します。
displayName	リソースに関連付ける表示名を指定します。
description	orclResourceTypeName に関連付ける説明を指定します。
orclUserIDAttribute	リソースにアクセスするためのユーザー識別子の値を指定します。
orclPasswordAttribute	リソースにアクセスするためのパスワードの値を指定します。
orclFlexAttribute1	追加の情報を指定します（リソース・タイプで必要な場合）。
orclFlexAttribute2	追加の情報を指定します（リソース・タイプで必要な場合）。
orclFlexAttribute3	追加の情報を指定します（リソース・タイプで必要な場合）。
OrclUserModifiable	この RAD エントリの作成対象ユーザーが、データを変更できるかどうかを指定します。

表 B-28 リソース・タイプ情報の属性

属性	説明
orclResourceTypeName	リソース（データベース、XMLPDS、JDBCPDS など）の名前を指定します。
displayName	orclResourceTypeName に関連付ける表示名を指定します。
description	orclResourceTypeName に関連付ける説明を指定します。
javaClassName	ユーザー認証（DBAuth、XMLPDSAuth、JDBCPDSAuth）を実行する製品で使用される完全修飾されたクラス名を指定します。
orclUserIDAttribute	エンコードされたリソース・アクセス・データ内のユーザー識別子の属性を指定します。
orclPasswordAttribute	エンコードされたリソース・アクセス・データ内のパスワードの属性を指定します。
orclConnectionFormat	リソースに関連付けられた接続文字列の構成に使用される書式を指定します。
OrclFlexAttribute1	特定のリソース・タイプに必要な場合は、追加情報を格納するための GUL ラベルを指定します。
OrclFlexAttribute2	特定のリソース・タイプに必要な場合は、追加情報を格納するための GUL ラベルを指定します。
OrclFlexAttribute3	特定のリソース・タイプに必要な場合は、追加情報を格納するための GUL ラベルを指定します。

レプリケーションのスキーマ要素

表 B-29 レプリケーションのスキーマ要素

オブジェクト・クラス	属性
changeLogEntry、 changeStatusEntry、 orclReplAgreementEntry	orclGUID、changeNumber changeType、changes、 orclParentGUID、server、changeLog、 changeStatus、orclChangeRetryCount、 orclAgreementId、orclReplicationProtocol、 orclUpdateSchedule、targetDN、 orclIncludedNamingcontexts、 orclExcludedNamingcontexts、 orclDirReplGroupDSAs、orclExcludedAttributes、 orclreplicaDN

注意： このリリースでは、targetDN 属性をフィルタとして使用できません。フィルタを使用すると、操作に失敗します。

レプリケーション・サーバーの構成パラメータ

表 B-30 に、レプリケーション・サーバーの構成設定エントリの属性およびその説明を示します。このエントリの識別名は、cn=configset0,cn=osdrepld,cn=subconfigsubentry です。

表 B-30 ディレクトリ・レプリケーション・サーバーの構成パラメータ

パラメータ名	説明	デフォルト値	変更可能？
modifyTimestamp	エントリの作成または変更の時間。		いいえ
modifiersName	エントリを作成または変更した人の名前。		いいえ
orclChangeRetryCount	単一値の属性。変更エントリを管理者操作キューに移動するまでの適用処理の再試行回数。このパラメータの値は 1 以上にする必要があります。	10	はい
orclThreadsPerSupplier	変更ログを処理するために、ディレクトリ・レプリケーション・サーバーが各サプライヤに提供するワーカー・スレッドの数。このパラメータの値は 1 以上にする必要があります。	5	はい

関連項目： 25-35 ページの「ディレクトリ・レプリケーション・サーバーの構成パラメータの表示および変更」

レプリカ・サブエントリ属性

表 B-31 レプリカ・サブエントリの属性

属性	説明
OrclReplicaID	レプリカ・サブエントリのネーミング属性。この値は、インストール時に初期化される各ディレクトリ・サーバー・ノードに対し一意です。インストール時に割り当てられるこの属性の値は、各ディレクトリ・ノードに対し一意で、ルート DSE の orclreplicaID 属性の値と一致します。この値は変更できません。

表 B-31 レプリカ・サブエントリの属性（続き）

属性	説明
orclReplicaURI	このレプリカに接続する際に使用できる ldapURI 形式の情報が含まれます。
orclReplicaSecondaryURI	orclReplicaURI 値を使用できない場合に使用可能な ldapURI 形式のアドレスを含みます。
orclReplicaType	「読取り専用」、「読取り / 書込み」などのレプリカのタイプを定義します。 指定可能な値は次のとおりです。 ■ 0（読取り / 書込み） ■ 1（読取り専用）
orclReplicaState	ブートストラップ、オンラインなどのレプリカの状態を定義します。指定可能な値は次のとおりです。 ■ 0（ブートストラップ） ■ 1（オンライン） ■ 2（オフライン）
OrclReplicaVersion	Oracle Internet Directory レプリカのバージョン

関連項目： 24-14 ページの「レプリカ・サブエントリ」

レプリケーション承諾エントリの属性

表 B-32 レプリケーション承諾エントリの属性

属性	説明
orclagreementID	レプリケーション承諾エントリのネーミング属性。このパラメータは変更できません。
OrclReplicaDN	LDAP ベースのレプリケーション専用。レプリケーション承諾でコンシューマを識別するために、レプリカの識別名を指定する必要があります。このパラメータは変更できません。

表 B-32 レプリケーション承諾エントリの属性（続き）

属性	説明
OrclReplicationPortocol	レプリカへの伝播を変更するために、レプリケーション・プロトコルを定義します。指定可能な値は次のとおりです。 ■ ODS_ASR_1.0（Oracle9*i* Advanced Replication ベースのプロトコル） ■ ODS_LDAP_1.0（LDAP ベースのレプリケーション） このパラメータは変更できません。
OrclDirReplGroupDSAs	Oracle9*i* Advanced Replication ベースのグループの場合は、このレプリケーション・グループのすべてのノードの orclreplicaid 値。このリストは、グループのすべてのノードで同一であることが必要です。この属性は変更可能です。 この属性は、LDAP ベースの承諾に適用できません。
orclUpdateSchedule	新規の変更および再試行される変更のレプリケーションの更新間隔。この値は分単位です。この属性は変更可能です。
OrclHIQSchedule	ディレクトリ・レプリケーション・サーバーが変更適用プロセスを繰り返す間隔（分単位）。この属性は変更可能です。
OrclLDAPConnKeepAlive	ディレクトリ・レプリケーション・サーバーをディレクトリ・サーバーに常時接続しておくか、様々なスケジュールに基づいた変更ログ処理が行われるたびに接続するかを定義する属性。このフィールドは変更可能です。
Orcllastappliedchangenumber	この属性は、LDAP ベースのレプリケーション承諾でサプライヤに関するコンシューマ・レプリカのステータスを示します。この属性は、Oracle9*i* Advanced Replication ベースの承諾に適用しません。 このパラメータは変更できません。
orclexcludednamingcontexts	Oracle9*i* Advanced Replication ベースの承諾の場合、この複数値の属性は、レプリケーションから除外する 1 つ以上のサブ・ツリーを指定します。 この属性は変更可能です。

関連項目： 24-14 ページの「レプリケーション承諾エントリ」

レプリケーション・ネーミング・コンテキスト・オブジェクト

レプリケーション・ネーミング・コンテキスト・オブジェクトのコンテナは、相対識別名の cn=replication namecontext を含むエントリです。このコンテナは、インストール時に orclagreementID エントリの下に作成されます。cn=replication namecontext エントリには、表 B-33 に示す属性があります。

表 B-33 レプリケーション・ネーミング・コンテキスト・エントリの属性

属性	説明
orclincludednamingcontexts	部分レプリカに含まれるネーミング・コンテキスト。 この属性は単一の値です。ネーミング・コンテキスト・オブジェクトごとに、一意のサブ・ツリーのみを指定できます。 部分レプリケーションでは、orclexcluednamingcontexts 属性に指定されたサブツリーを除き、ネーミング・コンテキストに含まれているサブツリーはすべてレプリケートされます。 **注意：**この属性に従って 1 つ以上の部分レプリカを定義するのは、LDAP ベースのレプリケーション承諾のみです。この属性に Oracle9*i* Advanced Replication ベースのレプリケーション承諾の任意の値が含まれている場合、この属性は無視されます。 この属性は変更可能です。
orclexcludednamingcontexts	LDAP ベースのレプリケーションでは、この属性の値は、含まれているネーミング・コンテキスト内に配置されたサブツリーのルートを指定し、レプリケーションから除外します。 この属性は複数値です。orclincludednamingcontexts 属性で指定されたネーミング・コンテキスト内から、部分レプリケーションから除外するサブツリーを指定できます。 この属性は変更可能です。
orclexcludedattributes	含まれているネーミング・コンテキスト内で、レプリケーションから除外する属性。 この属性は複数値です。 **注意：**この属性は、部分レプリケーションのみに有効です。

SSL スキーマ要素

注意： これらの属性の値は、構成エントリの一部として格納されています。

SSL 属性：orclsslAuthentication、orclsslEnable、orclsslWalletURL、orclsslPort、orclsslVersion

関連項目：

- デバッグ・レベルの詳細は、10-6 ページの「OID 制御ユーティリティを使用したデバッグ・ロギング・レベルの設定」を参照してください。
- Oracle Wallet の位置と Oracle Wallet のパスワードの設定の詳細は、『Oracle Advanced Security 管理者ガイド』を参照してください。

システム操作属性

変更可能なシステム操作属性は、次のとおりです。

表 B-34 変更可能なシステム操作属性

属性	説明
namingContexts	このサーバーに格納されているネーミング・コンテキストの最上位識別名。ネーミング・コンテキストとして識別名を公開するには、スーパー・ユーザー権限を持っている必要があります。 このフィールドにデフォルトの設定はありません。
orclCryptoScheme	パスワードを暗号化するハッシュ・アルゴリズム。オプションは次のとおりです。 ■ MD4 ■ MD5 ■ 暗号化を使用しない ■ SHA ■ SSHA ■ UNIX Crypt デフォルトは MD4 です。
orclSizeLimit	検索で戻されるエントリの最大数。
orclServerMode	サーバーにデータを書き込むことができるかどうかを指定します。有効な値は、read-only および read-write です。デフォルトは read-write です。

表 B-34 変更可能なシステム操作属性（続き）

属性	説明
orclTimeLimit	検索の最大実行時間（秒）。デフォルトは 3600 です。
orclecacheenabled	2-3 ページの「エントリ・キャッシング」で説明されたエントリ・キャッシングを使用可能にするかどうかを指定します。使用可能にする場合は 1、使用禁止にする場合は 0（ゼロ）です。デフォルトは 1 です。

orclecachemaxentrysize	エントリ・キャッシュでキャッシュできるエントリの最大バイト・サイズ。サイズが orclecachemaxentrysize を超える任意のエントリはキャッシュされません。多数のバイナリ属性を含むエントリ、あるいは member または uniquemember 属性、およびキャッシュが必要な場合は、orclecachemaxentrysize を適切な値に増加させます。
	デフォルトは 1MB です。
	この属性は、エントリ cn=dsaconfig,cn=configsets,cn=oracle internet directory です。
	この値を変更するには、次のようにします。
	`ldapmodify -p port -D cn=orcladmin -w adminpassword << EOF`
	`dn: cn=dsaconfig,cn=configsets,cn=oracle internet directory`
	`changetype: modify`
	`replace: orclecachemaxentrysize`
	`orclecachemaxentrysize: new_integer_value`
	`EOF`

orclecachemaxsize	エントリ・キャッシュが使用できる RAM の最大バイト数。デフォルトは 100M です。
orclecachemaxentries	エントリ・キャッシュ内に存在可能な最大エントリ数。デフォルトは 25,000 です。
orclDIPRepository	ディレクトリ・レプリケーション・サーバーで使用され、Oracle Directory Integration and Provisioning Server でコンシュームするために、変更ログがコンシューマ・ノードで生成されるかどうかを示します。 デフォルトは FALSE です。
orclEnableGroupCache	ディレクトリ・サーバー内の権限グループと ACL グループのキャッシュ。このキャッシュを使用すると、ACI で権限グループと ACP グループが使用される場合に、ユーザーに対するアクセス制御評価のパフォーマンスが改善されます。 権限グループのメンバーシップが頻繁に変化しない場合は、グループ・キャッシュを使用します。このメンバーシップが頻繁に変化する場合は、グループ・キャッシュをオフにするのが最善の方法です。これは、このような場合、グループ・キャッシュの計算によってオーバーヘッドが増大するためです。 デフォルトは 1 です。

表 B-34 変更可能なシステム操作属性（続き）

属性	説明
orclMatchDNEnabled	検索要求のベース識別名が見つからないと、ディレクトリ・サーバーは、指定されたベース識別名と一致する、最も近い識別名を戻します。ディレクトリ・サーバーが最も近い一致識別名の検索を試行するかどうかは、この属性によって制御されます。この属性を 1 に設定すると、一致識別名の処理が使用可能になります。0 に設定すると、一致識別名の処理が使用禁止になります。デフォルトは 1 です。
Orclanonymousbindsflag	匿名バインドを許可するかどうかを指定します。1 に設定すると、匿名バインドが許可されます。0（ゼロ）に設定すると許可されません。デフォルトは 1 です。
orclStatsPeriodicity	サンプル統計を収集する頻度、つまり間隔（分単位）を指定します。1（分単位）以上を設定します。デフォルトは 60 です。
orclStatsFlag	Oracle Internet Directory サーバー管理機能フレームワークを使用可能にするかどうかを示します。使用可能にするには、1 に設定します。使用禁止にするには、0（ゼロ）に設定します。デフォルトは 0（ゼロ）です。
orclLDAPconnTimeOut	ディレクトリ・サーバーによってクローズされるアイドル状態の LDAP 接続の最大接続時間（分単位）を指定します。これは、DSA 構成設定（DN:"cn=dsaconfig,cn=configsets,cn=oracle internet directory"）属性で、その値は ldapmodify を使用して設定できます。デフォルトは 0（ゼロ）です。
OrclEventLevel	記録する、セキュリティとシステム・リソースに関連する重要なイベントを指定します。デフォルトは 0 で、重要ではないイベントは記録されません。 スーパー・ユーザー、プロキシ、およびレプリケーション・ログイン以外のイベントについては、この機能を使用可能にするために orclStatsFlag 属性の値を 1 に設定する必要もあります。 **関連項目：**監視できる重要なイベントのリストは、10-22 ページの「重要なイベントの構成」を参照してください。

注意： 同じデータベースに接続する複数のディレクトリ・サーバー・インスタンス、または同じディレクトリ・サーバー・インスタンスに複数のサーバー・プロセスがある場合、エントリ・キャッシングが自動的に使用禁止になります。これは、orclecacheenabled 属性の値とは無関係です。

関連項目： 5-9 ページの「システム操作属性の設定」

LDAP 構文

構文は、属性が保持できる値の型を定義します。Oracle Internet Directory は、RFC 2252 で指定されている構文の大部分を認識するため、そのドキュメントに記述されている構文の大部分を属性と関連付けることができます。Oracle Internet Directory は、ほとんどの LDAP 構文を認識した上で、一部の LDAP 構文を施行します。

この項では、次のサブセクションについて説明します。

Oracle Internet Directory で施行されている LDAP 構文

Oracle Internet Directory では、次の LDAP 構文が施行されています。

- DN
- Facsimile Telephone Number
- OID（オブジェクト識別子）
- Telephone Number

> **注意：** これらの属性に指定する値は、RFC 2252 で指定されている構文に準拠している必要があります。

Oracle Internet Directory が認識する汎用 LDAP 構文

次の LDAP 構文は、一般的に使用されている構文です。

Attribute Type Description

Numeric String

Boolean

Object Class Description

Certificate

Octet String

Directory String

OID

DN

Presentation Address

Facsimile Telephone Number

Printable String

INTEGER

Telephone Number

JPEG

UTC Time

Name And Optional UID

Oracle Internet Directory が認識するその他の LDAP 構文

前項の一般的に使用されている LDAP 構文以外に、Oracle Internet Directory では、次の LDAP 構文が認識されます。

Access Point

LDAP Schema Description

ACI Item

LDAP Syntax Description

Audio

Mail Preference

Binary

Master And Shadow Access Points

Bit String

Matching Rule

Certificate List

Matching Rule Use Description

Certificate Pair

MHS OR Address

Country String

Modify Rights

Data Quality Syntax

Name Form Description

Delivery Method

Object Class Description

DIT Content Rule Description

Octet String

DIT Structure Rule Description

Other Mailbox

DL Submit Permission

Postal Address

DSA Quality Syntax

Protocol Information

DSE Type

Substring Assertion

Enhanced Guide

Subtree Specification

Fax

Supplier And Consumer

Generalized Time

Supplier Information

Guide

Supplier Or Consumer

IA5 String

Supported Algorithm

LDAP Schema Definition

Teletex TerminalIdentifier

Telex Number

属性値のサイズ

構文では、属性値に対して特定のサイズ制約が定義されていません。ただし、構文を使用すると、属性値のサイズを指定できます。Oracle Internet Directory が属性に 'len' 特性を指定することはありません。

たとえば、属性 foo のサイズを 64 に制限するには、属性を次のように定義します。

(*object_identifier_of_attribute* NAME 'foo' EQUALITY caseIgnoreMatch SYNTAX '*object_identifier_of_syntax*{64}')

> **関連項目：** 属性値の詳細は、RFC2251 の 4.1.6 項を参照してください。http://www.ietf.org でこの RFC を検索できます。

一致規則

Oracle Internet Directory では、スキーマで次の一致規則定義が認識されます。

accessDirectiveMatch

IntegerMatch

bitStringMatch

numericStringMatch

caseExactMatch

objectIdentifierFirstComponentMatch

caseExactIA5Match

ObjectIdentifierMatch

caseIgnoreIA5Match

OctetStringMatch

caseIgnoreListMatch

presentationAddressMatch

caseIgnoreMatch

protocolInformationMatch

caseIgnoreOrderingMatch

telephoneNumberMatch

distinguishedNameMatch

uniqueMemberMatch

generalizedTimeMatch

generalizedTimeOrderingMatch

Oracle Internet Directory では、属性値を比較するときに、このリストの中から次の一致規則が実際に実行されています。

distinguishedNameMatch

caseExactMatch

caseIgnoreMatch

numericStringMatch

IntegerMatch

telephoneNumberMatch

ユーザーを表現するスキーマ

ユーザーは、OrclUser、OrclUserV2 および inetOrgPerson の各オブジェクト・クラスを使用して表現されます。表 B-35 に、属性名を示します。

表 B-35 ユーザー属性

属性名	必須またはオプション	説明
OrclGUID	オプション	ユーザーを識別する一意のグローバル ID を指定します。
Cn	必須	ユーザーの名またはニックネーム（あるいはその両方）を指定します。
Sn	必須	ユーザーの姓を指定します。
GivenName	オプション	ユーザーの洗礼名を指定します。
MiddleName	オプション	ユーザーのミドルネームを指定します（ある場合）。
DisplayName	オプション	GUI ツールで表示用に使用する名前を指定します。
OrclMaidenName	オプション	ユーザーの旧姓を指定します（ある場合）。
OrclDateOfBirth	オプション	ユーザーの誕生日を生年月日（YYYYMMDD）形式で指定します。

表 B-35 ユーザー属性（続き）

属性名	必須またはオプション	説明
Street	オプション	ユーザーの職場の住所の番地を指定します。
L	オプション	ユーザーの職場の住所の市区町村を指定します。
PostalCode	オプション	ユーザーの職場の住所の郵便番号を指定します。
St	オプション	ユーザーの職場の住所の都道府県を指定します。
C	オプション	ユーザーの職場の住所の国を指定します。
EmployeeNumber	オプション	ユーザーの従業員番号を指定します(該当する場合)。
O	オプション	ユーザーが勤務する組織を指定します。
Title	オプション	ユーザーの肩書きを指定します。
Manager	オプション	ユーザーのマネージャの識別名を指定します。
OrclHireDate	オプション	ユーザーが組織に雇用された日を指定します。
Mail	オプション	ユーザーの電子メール・アドレスを指定します。
JpegPhoto	オプション	ユーザーの写真を指定します。
TelephoneNumber	オプション	ユーザーの職場の電話番号を指定します。
Mobile	オプション	ユーザーの携帯電話の番号を指定します。
Pager	オプション	ユーザーのポケットベルの番号を指定します。
FacsimileTelephone Number	オプション	ユーザーの Fax 番号を指定します。
HomePostalAddress	オプション	ユーザーの自宅の完全な住所を指定します。値は、住所の各コンポーネントを $ で区切って指定します。たとえば、XYZ Avenue Apt. 2 $ San Francisco CA $ 92345 $ USA のように指定します。

表 B-35 ユーザー属性（続き）

属性名	必須またはオプション	説明
HomePhone	オプション	ユーザーの自宅の電話番号を指定します。
UserPassword	オプション	ユーザーの認証に使用するパスワードを指定します。
OrclActiveStartDate	オプション	ユーザーの認証が許可される日時を指定します。値は、協定世界時（UTC）の書式で指定します。この属性を指定しない場合、ユーザーは即時に認証されます。
OrclActiveEndDate	オプション	ユーザーの認証が不許可になる日付を指定します。値は、UTC 時刻書式で指定します。
OrclPasswordHint	オプション	ユーザーのパスワードが不明になった場合のヒントを指定します。
OrclPasswordHint Answer	オプション	パスワードのヒントの質問に対する回答を指定します。
OrclIsEnabled	オプション	ユーザーが、現在、認証が許可されているかどうかを指定します。有効な値は、「ENABLED」（または、ユーザー・エントリに属性の指定なし）と「DISABLED」です。ユーザーは、「ENABLED」が指定されている場合か、ユーザー・エントリに属性の指定がない場合のみ、正常に認証できます。
PreferredLanguage	オプション	ユーザーとの通信に使用する言語を指定します。
OrclTimeZone	オプション	ユーザーの勤務先のタイムゾーンを指定します。
OrclDefaultProfile Group	オプション	ユーザーのプロファイルのデフォルトとして使用するグループの識別名を指定します。
OrclIsVisible	オプション	通常のユーザー検索でユーザーを表示するかどうかを指定します。有効な値は、TRUE（または、指定なし）と FALSE です。この属性を指定しない場合、ユーザーのレコードは参照可能になります。

表 B-35 ユーザー属性（続き）

属性名	必須またはオプション	説明
OrclDisplayPersonal Information	オプション	ユーザーが、ユーザー検索で個人情報を表示することを選択するかどうかを指定します。有効な値は、TRUE（または、指定なし）と FALSE です。
OrclWorkflow Notification Preference	オプション	ワークフロー通知のユーザーへの送信方法を指定します。

C

Oracle Internet Directory Graphical User Interface（GUI）の要素

この付録では、Oracle Directory Manager および Oracle Internet Directory セルフ・サービス・コンソールの様々なフィールドおよび制御デバイスについて説明します。次の項目について説明します。

Oracle Directory Manager のフィールド

この項では、次の項目について説明します。

Oracle Directory Manager のアクセス制御管理フィールド

表 C-1「アクセス制御管理」ペインのフィールド

フィールド	説明
サブツリー制御ポイントへのパス	ACP で定義されているパスが表示されます。
サブツリー制御ポイント	ACP が表示されます。

表 C-2 に認証の選択肢、つまりディレクトリに対してユーザーを認証できる方法とその説明を示します。

表 C-2「認証の選択」リストのフィールド

認証の選択	説明
MD5 ダイジェスト	MD5 ダイジェストを使用したバインドにより、「簡易」、「プロキシ」および「匿名」アクセスをブロックします。
PKCS12	PKCS12 を使用したバインドにより、「MD5 ダイジェスト」、「簡易」、「プロキシ」および「匿名」アクセスをブロックします。
プロキシ	■ プロキシ・ユーザーとしてバインドします。この認証オプションは、「匿名」アクセスをブロックします。

表 C-2「認証の選択」リストのフィールド（続き）

認証の選択	説明
簡易	■ パスワード・ベースの認証。このオプションは、「プロキシ」および「匿名」アクセス両方をブロックします。

表 C-3 に暗号化の選択肢、つまりデータを暗号化する方法とその説明を示します。

表 C-3「暗号化の選択」リストのフィールド

暗号化の選択	説明
SASL	Simple Authentication and Security Layer
SSL 認証なし	クライアントとサーバーのいずれも、相手に対して自己認証を行いません。証明書の送信または交換は行われません。この場合は、SSL 暗号化 / 復号化のみ使用されます。
SSL 一方向	ディレクトリ・サーバーのみ、クライアントに対して自己認証を行います。ディレクトリ・サーバーは、そのサーバーが認証されていることを証明する証明書をクライアントに送信します。

関連項目： 14-9 ページの「バインド・モード」

表 C-4「責任者」タブ・ページでアクセス権限を付与するエンティティ

エンティティ	説明
すべての人 (*)	エントリにアクセスする人すべて。
特定のグループ	事前に定義したグループ名。
特定のエントリ	事前に定義したディレクトリ・エントリ。
サブツリー	ディレクトリ内の選択したサブツリー全体。
セッション・ユーザーの識別名（DN）が属性により識別された場合	識別名がエントリ内の属性である人すべて。たとえば、グループ・エントリに対する読取りアクセス権をグループのメンバーに付与する場合があります。
セッション・ユーザーのグループが属性により識別された場合	識別名がエントリ内の属性であるグループすべて。
セッション・ユーザーの一意 ID（orclGUID）が属性により識別された場合	このエントリに対してアクセス権を付与または制限するエントリのグローバル・ユーザー識別子（`orclGUID`）。
セッション・ユーザーの識別名（DN）がアクセス・エントリと一致する場合	指定したエントリで正常にログインしている人すべて。

表 C-5 属性に関するアクセス権

アクセス権	説明
読取り	属性値を読み取る権限。属性に対して読取り権限が与えられている場合でも、エントリ自体に参照権限がないかぎり値は戻されません。
検索	検索フィルタで属性を使用する権限。
書込み	エントリの属性を変更 / 追加 / 削除する権限。
自己書込み	識別名のグループ・エントリ属性のリスト内で、ユーザー自身の追加 / 削除あるいは自身のエントリを変更を行う権限。このレベルを使用すると、メンバーがリスト上の自分自身をメンテナンスできます。たとえば、次のコマンドを実行すると、グループ内のユーザーが member 属性上で、自分自身の識別名のみを追加または削除できます。 `access to attr=(member) by dnattr=(member) (selfwrite)` `dnattr` セレクタは、member 属性にリストされているエンティティにアクセス権が適用されるように指定します。`selfwrite` アクセス権セレクタは、そのメンバーが、属性上で自分自身の識別名のみを追加または削除できるように指定します。
比較	属性値で比較操作を実行する権限。

Oracle Directory Manager の属性一意性フィールド

表 C-6「新規制約」ダイアログ・ボックスのフィールド

フィールド	説明
属性一意性制約名	作成する属性一意性制約の名前。
一意属性名	ディレクトリ・サーバーがチェックする属性。
一意属性のオブジェクト・クラス	属性一意性制約を施行する、person などのオブジェクト・クラス。デフォルトでは、すべてのオブジェクト・クラスに施行されます。
一意属性の有効範囲	属性制約の検索時にディレクトリ・サーバーが使用するフィルタ。たとえば、次のようなフィルタがあります。 ■ base: ルート・エントリのみの検索 ■ onelevel: 1 レベルのみの検索 ■ sub: ディレクトリ全体の検索
一意属性のサブツリー	属性一意性制約を施行するサブツリー。デフォルトでは、ルート・ディレクトリから施行されます。

Oracle Directory Manager のガベージ・コレクション管理フィールド

表 C-7「ガベージ・コレクタ」ウィンドウのフィールド

フィールド	説明
ガベージ・コレクタ名	このフィールドは変更できません。
パージ・ベース	ガベージ・コレクション・タスクが適用されるネーミング・コンテキストのベース識別名。このフィールドは変更できません。
デバッグのパージ	このガベージ・コレクタのデバッグ・ログを使用可能にするかどうかを示すインジケータ。
パージ使用可能ステータス	このガベージ・コレクタを使用可能または使用禁止にします。デフォルトは使用可能です。
ファイル位置のパージ	ログ・ファイルがあるディレクトリの絶対パス名。
ファイル名のパージ	ログ・ファイルの名前。
パージの間隔	ガベージ・コレクション・ジョブが再度実行されるまでの間隔(時間単位)。たとえば、この値を 12 に設定すると、ガベージ・コレクションは 12 時間ごとに実行されます。この属性はオプションです。デフォルト値は 24 です。
すぐにパージ	このフィールドに任意の値を入力し、「適用」を選択するとすぐにガベージ・コレクションが開始されます。その時点で、このフィールドの値は自動的に NULL に戻ります。
パージの開始	ガベージ・コレクタが最初に実行される時間（秒単位）です。書式は、*YYYYMMDDHH24MISS* です。この属性はオプションです。デフォルト値が 0（ゼロ）の場合、ガベージ・コレクタはすぐに使用可能になります。
パージのターゲット期間	ターゲット・オブジェクトの経過時間（時間単位）です。指定された時間より古いオブジェクトは、午前 0 時に消去されます。この属性はオプションです。デフォルト値は 12 です。
パージのトランザクション・サイズ	1 回のトランザクション・コミットで消去されるオブジェクト数。この属性はオプションです。デフォルト値は 1000 です。

Oracle Directory Manager のパスワード・ポリシーに関するフィールド

表 C-8 パスワード・ポリシーの「一般」タブ・ページのフィールド

フィールド	説明
OID パスワード・ポリシーを使用可能にする	デフォルトの Oracle Internet Directory パスワード・ポリシーを使用不可にするには、「使用不可」を選択します。デフォルトは使用可能です。
パスワードを変更する際には、旧パスワードも指定	パスワードを変更する場合に、ユーザーが新規パスワードとともに旧パスワードを指定する必要があるかどうかを指定します。デフォルトでは、旧パスワードは不要です。
パスワード期限切れ後の猶予期間ログインの数	パスワードの期限切れ後に許可する猶予期間ログインの最大数。デフォルトでは、猶予期間ログインは許可されません。デフォルト値は 3 です。
パスワードの期限切れ警告	ユーザーがパスワードを変更する必要がある、パスワードの期限切れまでの秒数を入力します。 ディレクトリ・サーバーは、次の 2 つの条件に該当する場合にパスワードの期限切れ警告を送信します。 ■ ユーザーのパスワードの期限に関する属性が設定されている場合 ■ この属性も使用可能になっている場合 その時点から、ユーザーに対しパスワードを変更する秒数が指定されます。指定の秒数でユーザーがパスワードを変更しなかった場合、パスワードは期限切れとなり、管理者がパスワードを変更するまでユーザーはロックアウトされます。 たとえば、次のような場合があります。 ■ 「パスワード有効期限」が 7200 に設定されている場合、パスワードは 2 時間後に期限切れとなります。 ■ 「パスワードの期限切れ警告」が 3600 に設定されている場合、パスワードは 1 時間後に期限切れとなります。 この例では、最終 1 時間でバインドしている場合、パスワードの期限切れが近いことが警告されます。この時間内でパスワードを変更しなかった場合、パスワードは期限切れとなり、管理者がパスワードを変更するまでロックアウトされます。 この機能を有効にするには、クライアントのアプリケーションがこの機能に対応している必要があります。 デフォルトは 0（ゼロ）で、警告は送信されません。

表 C-8 パスワード・ポリシーの「一般」タブ・ページのフィールド（続き）

フィールド	説明
パスワード有効期限	指定したパスワードが有効である秒数を入力します。たとえば、この属性の値を 7200 に設定した場合、パスワードは設定した時間から 2 時間で期限切れとなります。 この属性が存在しない場合、あるいはその値が 0（ゼロ）の場合、パスワードは期限切れになりません。デフォルトのパスワード有効期限は 60 日です。
パスワード・ポリシー・エントリ	パスワード・ポリシー・エントリの相対識別名が表示されます。このフィールドは編集できません。
パスワード・ポリシー・エントリへのパス	パスワード・ポリシー・エントリの完全な識別名が表示されます。このフィールドは編集できません。

表 C-9 パスワード・ポリシーの「アカウントのロックアウト」タブ・ページのフィールド

フィールド	説明
グローバル・ロックアウト継続時間	次の両方に該当する場合に、ユーザーがグローバル・ディレクトリからロックアウトされる秒数を入力します。 ■ グローバル・ロックアウトが有効な場合 ■ pwdMaxFailure で指定された回数以上の試行を行うと、ディレクトリへのバインドが不可能になる場合。 特定の時間の間または管理者がパスワードを再設定するまでの間、ユーザーをロックアウトできます。デフォルト値は 24 時間です。
パスワード失敗のカウント間隔	パスワードの失敗回数がユーザー・エントリから削除されるまでの秒数を入力します。
パスワード失敗の最大数	ユーザー・アカウントがロックされるまでの連続バインド失敗回数を入力します。

表 C-10 パスワード・ポリシーの「IP のロック・アウト」タブ・ページのフィールド

フィールド	説明
IP のロックアウト継続時間	特定の IP アドレスに対し、アカウント・ロックアウトを施行する秒数を指定します。
IP のロックアウト失敗の最大数	アカウントがロックされた後、特定の IP アドレスからログイン失敗の最大数を指定します。

表 C-11 パスワード・ポリシーの「パスワード構文」タブ・ページのフィールド

フィールド	説明
パスワードの最小文字数	パスワードに必要な最小文字数を指定します。
パスワード内の数字の数	パスワードに必要な数字の文字数を指定します。
パスワードの履歴数	ディレクトリ・サーバーに保存される、ユーザーの過去のパスワード数を指定します。ユーザーが、ディレクトリ・サーバーに格納されているパスワードを再利用しようとすると、そのパスワードは拒否されます。ディレクトリ・サーバーは、デフォルトではパスワードの履歴を保持しません。
パスワード無効値	有効なパスワードとして値を使用できない一般的な語と属性の型を入力します。デフォルトでは、すべての語をパスワードの値として使用できます。

Oracle Directory Manager のパスワード・ベリファイア・フィールド

表 C-12「パスワード検証プロファイル」ダイアログ・ボックスのフィールド

フィールド	説明
パスワード検証エントリへのパス	このパスワード検証エントリの完全識別名。このフィールドを使用して、特定のパスワード検証エントリの位置を特定します。このフィールドは変更できません。
パスワード検証エントリ	このパスワード・ベリファイアの相対識別名。このフィールドは変更できません。
所有者	この検証エントリの管理者の識別名。このフィールドは変更可能です。
アプリケーション ID	Oracle アプリケーションの一意の識別子。この ID は、アプリケーションのインストール時に生成されます。このフィールドは変更できません。

Oracle パスワード・パラメータ	このパスワード・ベリファイアを生成するための情報を含むパラメータ。このフィールドを使用して、このパスワード・ベリファイアのハッシング・アルゴリズムを指定します。構文は次のとおりです。
	`crypto:`*`hashing_algorithm`*
	たとえば、ORCLLM ハッシング・アルゴリズムを使用している場合は、次のように入力します。
	`crypto:ORCLLM`
	SASL/MD5 を使用している場合は、次のように入力します。
	`crypto:SASL/MD5 $ realm:dc=com`

Oracle Directory Manager のプラグイン管理フィールド

関連項目： 45-4 ページの「プラグインの登録と管理」

表 C-13「新規プラグイン」ダイアログ・ボックス

フィールド	説明
「必須プロパティ」タブ・ページ	
プラグイン・エントリ名	たとえば、cn=my_plugin などです。このフィールドは必須です。
プラグインの種類	PL/SQL です。このフィールドは必須です。
プラグイン LDAP 操作	次のいずれかの値です。 ■ ldapcompare ■ ldapmodify ■ ldapbind ■ ldapadd ■ ldapdelete ■ ldapsearch このフィールドは必須です。
プラグイン・パッケージ名	このフィールドは必須です。

表 C-13「新規プラグイン」ダイアログ・ボックス（続き）

フィールド	説明
プラグイン・タイプ	次のいずれかの値です。 ■ `operational`: 操作プラグインは、既存の LDAP 操作を補強します。通常のディレクトリ・サーバー操作の前後に実行するか、操作に追加して実行するかによって、操作プラグインが実行する作業は異なります。 ■ `attribute`: 属性ベースのプラグインは属性値の追加または変更を行い、またその属性に関連する様々な LDAP 操作に追加されるタスクを実行します。たとえば、ディレクトリに、あるクレジット・カード番号を追加するときは常に暗号化すると仮定します。このためには、クレジット・カード番号属性に対するプラグインを作成し、クレジット・カード番号が追加された場合、そのプラグインがコールされ、その番号を暗号化するように指定することができます。同様に、検索によりクレジット・カード番号を取得した後、そのプラグインがコールされ、その番号を復号化するように指定することも可能です。 ■ `replacement`: すべての LDAP 操作には、モジュールの順序があります。たとえば、ldapmodify 操作には属性値チェック、スキーマ・チェック、ACL 評価、ディレクトリ変更に関してそれぞれモジュールがあります。置換プラグインによりモジュールを置換し、必要に応じて操作をカスタマイズできます。この型のプラグイン・モジュールが失敗すると、関連付けられている LDAP 操作も失敗します。 このフィールドは必須です。 **関連項目：**第 45 章「Oracle Internet Directory プラグイン・フレームワーク」を参照してください。
「オプション・プロパティ」タブ・ページ	
プラグイン使用可能	次のいずれかの値です。 ■ 0 = 使用禁止（デフォルト） ■ 1 = 使用可能 この属性はオプションです。
プラグイン・エントリ・プロパティ	LDAP 検索フィルタ・タイプ。たとえば、`orclPluginEntryProperties:(&(objectclass=inetorgperson)(sn=Cezanne))` を指定した場合、ターゲット・エントリに `inetorgperson` と同等の `objectclass` および `Cezanne` と同等の `sn` が含まれていると、そのプラグインは起動しません。

表 C-13「新規プラグイン」ダイアログ・ボックス（続き）

フィールド	説明
プラグインの置換	操作時タイミングのプラグインの場合のみ。次のいずれかの値です。 ■ 使用不可（デフォルト） ■ 使用可能 このプロパティは、「プラグイン LDAP 操作」のプロパティが ldapbind、ldapcompare または ldapmodify の場合のみ使用可能です。 この属性はオプションです。
プラグインのリクエスト・グループ	グループ・リストで、プラグインの実行を制御します。このグループを使用して、プラグインを実際に起動するユーザーを指定できます。 たとえば、プラグインの登録で、`cn=security,cn=groups,dc=oracle,dc=com` と指定していると、`cn=security,cn=groups,dc=oracle,dc=com` グループのメンバーから LDAP のリクエストがあるまで、プラグインは起動しません。
プラグインの結果コード	LDAP の結果コードを指定する整数値。この値を指定すると、LDAP 操作がこの結果コードの状態の場合にのみ、プラグインが起動します。 この属性は POST プラグイン・タイプにのみ有効です。
プラグイン・サブスクライバの DN リスト	セミコロンで区切られた識別名のリストで、プラグインの実行を制御します。たとえば、次のようなリストです。 `orclPluginSubscriberDNList=dc=COM,c=us; dc=us,dc=oracle,dc=com;dc=org,dc=us;o=IMC,c=US` LDAP 操作のターゲット識別名がリストに含まれている場合、プラグインが起動されます。
プラグインのタイミング	次のいずれかの値です。 ■ pre-- ディレクトリ・サーバーが LDAP 操作を実行する前にコールするプラグインに対する値。 ■ when-- ディレクトリ・サーバーが LDAP 操作の標準処理に追加してコールするプラグインに対する値。 ■ post-- ディレクトリ・サーバーが LDAP 操作を実行した後にコールするプラグインに対する値。 この属性はオプションです。
プラグイン・バージョン	サポート対象のプラグイン・バージョン番号。この属性はオプションです。

Oracle Directory Manager のレプリケーション・フィールド

表 C-14　レプリケーション・サーバーの「構成設定」の「一般」タブ・ページのフィールド

フィールド	説明
変更の再試行数	競合解消プロセスが、各更新の適用を断念して、問題をログに記録するまでの試行回数を入力します。デフォルトは 10 です。このフィールドは変更可能です。
サプライヤ当たりのスレッド数	変更ログを処理するために、ディレクトリ・レプリケーション・サーバーが各サプライヤに提供するワーカー・スレッドの数を入力します。デフォルトは 5 です。このフィールドは変更可能です。

関連項目： 25-36 ページの「Oracle Directory Manager を使用したディレクトリ・レプリケーション・サーバーの構成パラメータの変更」

表 C-15「ASR 承諾」タブ・ページのフィールド

フィールド	説明
除外されたネーミング・コンテキスト	レプリケーションから除外されるサブツリーのルート。 この属性は複数値です。このフィールドは変更可能です。
HIQ スケジュール	ディレクトリ・レプリケーション・サーバーが変更適用プロセスを繰り返す間隔（分単位）。このフィールドは変更可能です。
LDAP 接続を継続して維持	この属性は、ディレクトリ・レプリケーション・サーバーをディレクトリ・サーバーに常時接続するか、様々なスケジュールに基づいた変更ログ処理が行われるたびに接続するかを定義します。このフィールドは変更可能です。
レプリカ承諾 ID	レプリケーション承諾エントリのネーミング属性。
レプリカ承諾プロトコル	この属性は、変更をレプリカに伝播するためのレプリケーション・プロトコルを定義します。 指定可能な値は次のとおりです。 ■ ODS_ASR_1.0（Oracle9*i* Advanced Replication ベースのレプリケーション） ■ ODS_LDAP_1.0（LDAP ベースのレプリケーション）

表 C-15「ASR 承諾」タブ・ページのフィールド（続き）

フィールド	説明
レプリケーション・グループ・ノード	Oracle9*i* Advanced Replication ベースのグループの場合は、このレプリケーション・グループのすべてのノードの orclreplicaid 値を入力します。このリストは、グループのすべてのノードで同一であることが必要です。 この属性は、LDAP ベースのレプリケーション承諾には適用されません。
更新スケジュール	新規の変更および再試行される変更のレプリケーションの更新間隔。この値は分単位です。このフィールドは変更可能です。

表 C-16「レプリカ・ノード」の「一般」タブ・ページのフィールド

属性	説明
レプリカ ID	レプリカ・サブエントリのネーミング属性。この値は、インストール時に初期化される各ディレクトリ・サーバー・ノードに対し一意です。インストール時に割り当てられるこの属性の値は、各ディレクトリ・ノードに対し一意で、ルート DSE の orclreplicaID 属性の値と一致します。この値は変更できません。
レプリカ 2 次 URI	orclReplicaURI 値を使用できない場合に使用可能な ldapURI 形式のアドレスを含みます。
レプリカ状態	ブートストラップ、オンラインなどのレプリカの状態を定義します。次のいずれかの値を指定します。 ■ 0（ブートストラップ） ■ 1（オンライン） ■ 2（オフライン）
レプリカ・タイプ	「読取り専用」、「読取り / 書込み」などのレプリカのタイプを定義します。 次のいずれかの値を指定します。 ■ 0（読取り / 書込み） ■ 1（読取り専用）
レプリカ URI	このレプリカに接続する際に使用できる ldapURI 形式の情報を指定します。

表 C-16「レプリカ・ノード」の「一般」タブ・ページのフィールド（続き）

属性	説明
関連項目	Oracle Internet Directory に使用されるインフラストラクチャ・データベースの識別名。このフィールドは変更できません。

表 C-17「レプリカ承諾」タブ・ページの列

列	説明
コンシューマ・レプリカ DN	この属性は、レプリケーション承諾においてコンシューマを識別するためのレプリカの識別名を指定します。 このフィールドは変更可能です。
HIQ スケジュール	ディレクトリ・レプリケーション・サーバーが変更適用プロセスを繰り返す間隔（分単位）。このフィールドは変更可能です。
LDAP 接続を継続して維持	この属性は、ディレクトリ・レプリケーション・サーバーをディレクトリ・サーバーに常時接続するか、様々なスケジュールに基づいた変更ログ処理が行われるたびに接続するかを定義します。このフィールドは変更可能です。
最後に適用された変更番号	この属性は、LDAP ベースのレプリケーション承諾でサプライヤに関するコンシューマ・レプリカのステータスを示します。この属性は、Oracle9*i* Advanced Replication ベースの承諾に適用しません。
レプリカ承諾 ID	レプリケーション承諾エントリのネーミング属性。
レプリケーション・プロトコル	この属性は、変更をレプリカに伝播するためのレプリケーション・プロトコルを定義します。 指定可能な値は次のとおりです。 ■ ODS_ASR_1.0（Oracle9*i* Advanced Replication ベースのレプリケーション） ■ ODS_LDAP_1.0（LDAP ベースのレプリケーション）
更新スケジュール	新規の変更および再試行される変更のレプリケーションの更新間隔。この値は分単位です。このフィールドは変更可能です。

表 C-18「レプリカのネーミング・コンテキスト」タブ・ページのフィールド

フィールド	説明
除外された属性	部分レプリケーションのみに使用します。 含まれているネーミング・コンテキスト内で、レプリケーションから除外する属性。 この属性は複数値です。
除外されたネーミング・コンテキスト	レプリケーションから除外されるサブツリーのルート。 この属性は複数値です。このフィールドは変更可能です。 LDAP ベース・レプリケーションでは、`orclincludednamingcontexts` 属性で指定されたネーミング・コンテキスト内から LDAP ネーミング・コンテキスト・オブジェクト内に 1 つ以上のサブツリーを指定し、部分レプリケーションから除外できます。 Oracle9*i* Advanced Replication に基づいたレプリケーションでは、1 つ以上のサブツリーを指定してレプリケーションから除外できます。
包含されたネーミング・コンテキスト	部分レプリカに含まれるネーミング・コンテキスト。 この属性は単一の値です。ネーミング・コンテキスト・オブジェクトごとに、一意のサブ・ツリーのみを指定できます。 部分レプリケーションでは、`orclexcludednamingcontexts` 属性に指定されたサブツリーを除き、ネーミング・コンテキストに含まれているサブツリーはすべてレプリケートされます。 **注意：**この属性に従って 1 つ以上の部分レプリカを定義するのは、LDAP ベースのレプリケーション承諾のみです。この属性に Oracle9*i* Advanced Replication ベースのレプリケーション承諾の任意の値が含まれている場合、この属性は無視されます。 この属性は変更可能です。

関連項目： 25-30 ページの「LDAP ベースの部分レプリケーションでのレプリケート対象の決定」

表 C-19「変更ログ」ウィンドウのフィールド

フィールド	説明
変更ログ番号	この変更の一意の識別子。
変更ログ操作	この変更を行った操作の種類（追加、削除、変更、比較など）。
変更ログ・ターゲット DN	この変更が行われたエントリの識別名。

表 C-19「変更ログ」ウィンドウのフィールド（続き）

フィールド	説明
変更ログ・ターゲット DN の変更	エントリに対して行われた変更。
変更リトライ回数	レプリケートされた環境内の他のノードに対してこの変更を適用しようとした回数。
Modifier's Name	この変更を実行したユーザーの名前。
操作時間	変更が行われた日時。
Orcl GUID	変更が行われたエントリの Global Unique Identifier。
Orcl Parent GUID	変更が行われたエントリの親の Global Unique Identifier。
サーバー名	この変更を発行したサーバーの名前。

Oracle Directory Manager のスキーマ管理フィールド

関連項目： 第 6 章「ディレクトリ・スキーマの管理」

この項では、次の項目について説明します。

Oracle Directory Manager のオブジェクト・クラス・フィールド

表 C-20 Oracle Directory Manager の検索時にリストされるオブジェクト・クラス・プロパティ

オプション	説明
名前	検索するオブジェクト・クラスの名前。たとえば、「名前」「完全一致」「subAcl」と指定すると、subAcl オブジェクト・クラスを検索できます。

表 C-20 Oracle Directory Manager の検索時にリストされるオブジェクト・クラス・プロパティ（続き）

オプション	説明
オブジェクト ID	検索するオブジェクト・クラスのオブジェクト識別子。たとえば、「オブジェクト ID」「次の文字で始まる」「2.5.2」と指定すると、オブジェクト ID が 2.5.2 で始まるオブジェクト・クラスのリストが表示されます。 オブジェクト識別子は、IETF 規格に基づいた、標準化された数値順序です。一意、かつ組織内に設定されたシステムに準拠したものである必要があります。通常この値は、ANSI または ISO など、登録機関によって割り当てられた ID から導出されます。
説明	「説明」フィールドに含まれている語。たとえば、「説明」「含む」「Shoe」と指定すると、説明列に *shoe* を含むオブジェクト・クラスのリストが表示されます。説明を記述するオプションのフィールドです。
型	検索するオブジェクト・クラスの型。「抽象型」、「構造型」または「補助型」のいずれかを指定します。
スーパー・クラス	検索するオブジェクト・クラスのスーパークラス。「追加」をクリックすると「スーパー・クラス・セレクタ」ダイアログ・ボックスが表示され、追加するスーパークラスを選択できます。
必須属性	検索するオブジェクト・クラスの必須属性。たとえば、「必須属性」「含む」「cn」と指定すると、cn 属性が必須の、すべてのオブジェクト・クラスのリストが表示されます。
オプション属性	検索するオブジェクト・クラスのオプション属性。

表 C-21 オブジェクト・クラスの検索フィルタ

フィルタ	説明
開始	検索するオブジェクト・クラスのプロパティの、始めの数文字のみ使用して検索します。たとえば、「型」「次の文字で始まる」「aux」と指定すると、補助型オブジェクト・クラスの全リストが表示されます。
終了	検索するオブジェクト・クラスのプロパティの、終わりの数文字のみ使用して検索します。たとえば、「型」「終了」「ral」と指定すると、構造型オブジェクト・クラスの全リストが表示されます。
含む	値の位置を限定せずに、ユーザーの入力値が選択したプロパティに含まれているオブジェクト・クラスを検索します。たとえば、「オプション属性」「含む」「cn」と指定すると、cn がオプション属性であるすべてのオブジェクト・クラスのリストが表示されます。

表 C-21 オブジェクト・クラスの検索フィルタ（続き）

フィルタ	説明
完全一致	選択したプロパティが入力値に完全に一致するオブジェクト・クラスを検索します。たとえば、「スーパー・クラス」「完全一致」「person」と指定すると、スーパークラスとして person を持つすべてのオブジェクト・クラスのリストが表示されます。
以上	選択したプロパティが数値順またはアルファベット順でユーザーの入力値より大か等しいオブジェクト・クラスを検索します。たとえば、「名前」「以上」「orcl」と指定すると、orcl で始まるオブジェクト・クラスから、アルファベットの最後の文字で始まるオブジェクト・クラスまでのリストが表示されます。
以下	選択したプロパティが数値順またはアルファベット順で入力値より小か等しいオブジェクト・クラスを検索します。たとえば、「名前」「以下」「orcl」と指定すると、orcl で始まるオブジェクト・クラスから、アルファベットの最初の文字で始まるオブジェクト・クラスまでのリストが表示されます。
存在	選択したプロパティが存在するすべてのオブジェクト・クラスを検索します。たとえば、「必須属性」「存在」と指定すると、必須属性を含むすべてのオブジェクト・クラスのリストが表示されます。

表 C-22 Oracle Directory Manager のオブジェクト・クラスの検索時に使用されるボタン

ボタン	説明
新規作成	「**基準**」フィールドに、新しい検索基準バーを作成します。このボタンは、**基準**バーが削除されている場合にのみ使用可能です。
AND	「**基準**」フィールドに、別の検索基準バーを作成します。指定した 2 つの基準を両方満たすオブジェクト・クラスをすべて検索します。
OR	「**基準**」フィールドに、別の検索基準バーを作成します。指定した 2 つの属性のいずれかを持つオブジェクト・クラスをすべて検索します。
NOT	選択した検索基準バーの基準を除外し、指定した基準を満たさないオブジェクト・クラスをすべて取り出します。
削除	選択した検索基準バーを削除します。

表 C-23「新規オブジェクト・クラス」ダイアログ・ボックスのフィールド

オプション	説明
名前	オブジェクト・クラスの名前
オブジェクト ID	オブジェクト識別子。これは、IETF 規格に基づいた、標準化された数値順序です。一意、かつ組織内に設定されたシステムに準拠したものである必要があります。通常この値は、ANSI または ISO など、登録機関によって割り当てられた ID から導出されます。
説明	このオプションのフィールドは、説明の記述のみに使用します。
型	オブジェクト・クラスの型。「抽象型」、「構造型」、「補助型」または「なし」のいずれかを指定します。
スーパー・クラス	このオブジェクト・クラスを導出するクラスです。このオブジェクト・クラスは、選択したスーパークラスの属性をすべて継承します。構造型オブジェクト・クラスの場合は、そのスーパークラスの 1 つとして必ず top を設定する必要があります。「追加」をクリックすると「スーパー・クラス・セレクタ」ダイアログ・ボックスが表示され、追加するスーパークラスを選択できます。
必須属性	値の入力が必要な属性です。「追加」をクリックすると「必須属性セレクタ」ダイアログ・ボックスが表示され、追加する必須属性を選択できます。
オプション属性	値が必須ではない属性です。「追加」をクリックすると「オプション属性セレクタ」ダイアログ・ボックスが表示され、追加するオプション属性を選択できます。

Oracle Directory Manager の属性フィールド

表 C-24 Oracle Directory Manager の「属性」タブ・ページの列

列	説明
名前	属性の標準化型名。
索引付け	属性が索引付けされているかどうかを示すチェックボックス。
オブジェクト ID	各属性の標準化オブジェクト識別子。
説明	各属性を説明する語。
構文	データ・エントリに関して各属性の型に適用される標準化規則。
サイズ	各オブジェクトの最大サイズ。

表 C-24 Oracle Directory Manager の「属性」タブ・ページの列（続き）

列	説明
使用方法	属性の使用方法を指定する規格。次の 4 つのオプションがあります。 ■ userApplications ■ directoryOperation ■ distributedOperation ■ dSAOperation
順序	値に対して設定される優先順位を指定する規格。
等価	比較と検索操作における等価の判断方法を指定する規格。
サブストリング	一致する正規表現の文字列。
単一値	ある 1 つの最大値を含む属性の型。
スーパー	各属性のスーパー属性。

表 C-25 属性の検索フィルタ

オプション	説明
開始	プロパティの値の始めの数文字のみを使用して検索します。たとえば、「構文」「次の文字で始まる」「1.3」と指定すると、構文識別子が 1.3 で始まるすべての属性のリストが表示されます。
終了	プロパティの値の終わりの数文字のみを使用して検索します。たとえば、「名前」「終了」「License」と指定すると、carLicense など、License で終わるすべての属性のリストが表示されます。
含む	入力した値を含んだプロパティを持つ属性を検索します。たとえば、「順序」「含む」「time」と指定すると、「順序」列に time という語を含むすべての属性のリストが表示されます。
完全一致	指定した属性プロパティ内の値に完全に一致する値を検索します。たとえば、「等価」「完全一致」「caseIgnoreMatch」と指定すると、caseIgnoreMatch 一致規則を持つすべての属性のリストが表示されます。
以上	数値順またはアルファベット順でユーザーの入力値より大か等しいプロパティを持つ属性を検索します。たとえば、「名前」「以上」「orcl」と指定すると、orcl で始まる属性からアルファベットの最後の文字で始まる属性までのリストが表示されます。
以下	数値順またはアルファベット順でユーザーの入力値以下のプロパティを持つ属性を検索します。たとえば、「名前」「以下」「orcl」と指定すると、orcl で始まる属性からアルファベットの最初の文字で始まる属性までのリストが表示されます。

表 C-25 属性の検索フィルタ（続き）

オプション	説明
存在	選択した属性プロパティが存在しているすべての属性を検索します。たとえば、「説明」「存在」と指定すると、「説明」フィールドにテキストがあるすべての属性のリストが表示されます。

表 C-26 Oracle Directory Manager の属性の検索時に使用されるボタン

ボタン	説明
新規作成	「**基準**」フィールドに、新しい検索基準バーを作成します。このボタンは、「**基準**」フィールドに何も表示されていないときのみ使用可能です。
AND	「**基準**」フィールドに、別の検索基準バーを作成します。指定した 2 つのプロパティが両方ある属性をすべて検索します。
OR	「**基準**」フィールドに、別の検索基準バーを作成します。指定した 2 つのプロパティのいずれかを持つ属性をすべて検索します。
NOT	選択した検索基準バーの基準を除外し、指定したプロパティがない属性をすべて検索します。
削除	選択した検索基準バーを削除します。

表 C-27「新規属性の型」ダイアログ・ボックス「一般」タブ・ページのフィールド

フィールド	説明
名前	この属性の名前。
オブジェクト ID	この属性のオブジェクト ID。オブジェクト ID は、IETF 規格に基づいた、標準化された数値順序です。値は一意であることが必要です。通常この値は、ANSI または ISO など、登録機関によって割り当てられた ID から導出されます。 標準識別子の説明は、現行の LDAP 規格を参照してください。LDAP 規格は IETF の Web サイト `http://www.ietf.org` で参照できます。
説明	説明の記述のみに使用するオプションのフィールド。
構文	データ・エントリに関してこの属性の型に適用される標準化規則。
サイズ	このオブジェクトの最大サイズ。
単一値	この属性の型の値が最大 1 つであることを示します。

表 C-28「新規属性の型」ダイアログ・ボックス「拡張」タブ・ページのフィールド

フィールド	説明
索引付け	このフィールドを選択するとこの属性が索引に追加され、検索で使用できるようになります。等価の一致規則を持つ属性のみが索引付けできます。
使用方法	属性の使用方法を指定する規格を指定します。オプションは次のとおりです。 ■ `userApplications` ユーザーが値を入力する必要がある属性（例：`telephoneNumber`） ■ `directoryOperation` ディレクトリ・サーバーによって値が入力される属性（例：`creatorName` または `timeStamp`） ■ `distributedOperation` ■ `dSAOperation` サーバーの内部操作用に使用される属性（例：orclUpdateSchedule）
順序	値に対して設定される優先順位を指定する規格を指定します。
等価	比較と検索操作における等価の判断方法を指定する規格を指定します。
サブストリング	一致規則を指定します。
スーパー	この属性のスーパー属性を追加します。この手順は、次のとおりです。 **1.** このフィールドの横の「追加」ボタンを選択します。「スーパー属性セレクタ」が表示されます。 **2.** 追加するスーパー属性を選択して、「選択」を選択します。 **3.** 必要に応じてこの処理を繰り返します。 「スーパー」フィールドからスーパー属性を削除するには、削除する属性を選択して、「削除」を選択します。

Oracle Directory Manager の一致規則フィールド

表 C-29「一致ルール」タブ・ページのフィールド

列見出し	説明
名前	属性一致規則の名前
オブジェクト ID	この一致規則の一意な識別子
説明	一致規則を説明する語（オプション）
構文	この一致規則に使用される構文

Oracle Directory Manager のコンテンツ規則管理フィールド

表 C-30「新規コンテンツ・ルール」ダイアログ・ボックスのフィールド

フィールド	説明
構造型オブジェクト・クラス	このコンテンツ規則を割り当てる構造型オブジェクト・クラスの名前。
オブジェクト ID	作成するコンテンツ規則の一意な識別子。
ラベル	このコンテンツ規則のわかりやすい名前。
補助クラス	指定の構造型オブジェクト・クラスに関連付ける属性を持つ補助型オブジェクト・クラス。補助型クラスを指定する手順は、次のとおりです。 **1.** 「追加」を選択すると、「補助クラス・セレクタ」ダイアログ・ボックスが表示されます。 **2.** 追加する補助型クラスを選択します。 **3.** 「選択」を選択します。「新規コンテンツ・ルール」ダイアログ・ボックスに戻ります。「補助クラス」フィールドに指定した補助型クラスが表示されます。
必須属性	指定の構造型オブジェクト・クラスに関連付ける必須属性。必須属性を指定する手順は、次のとおりです。 **1.** 「追加」を選択すると、「必須属性セレクタ」ダイアログ・ボックスが表示されます。 **2.** 追加する必須属性を選択します。この属性に索引付けをする場合、「索引付け」列の対応するチェックボックスを選択します。 **3.** 「選択」を選択します。「新規コンテンツ・ルール」ダイアログ・ボックスに戻ります。「必須属性」フィールドに指定した必須属性が表示されます。
オプション属性	指定の構造型オブジェクト・クラスに関連付けるオプションの属性。オプション属性を指定する方法は次のとおりです。 **1.** 「追加」を選択すると、「オプション属性セレクタ」ダイアログ・ボックスが表示されます。 **2.** 追加するオプション属性を選択します。この属性に索引付けをする場合、「索引付け」列の対応するチェックボックスを選択します。 **3.** 「選択」を選択します。「新規コンテンツ・ルール」ダイアログ・ボックスに戻ります。「オプション属性」フィールドに指定したオプション属性が表示されます。

表 C-31「コンテンツ・ルール」ダイアログ・ボックスのフィールド

フィールド	説明
構造型オブジェクト・クラス	このコンテンツ規則を割り当てる構造型オブジェクト・クラスの名前。
オブジェクト ID	作成するコンテンツ規則の一意な識別子。
ラベル	このコンテンツ規則のわかりやすい名前。
補助クラス	指定の構造型オブジェクト・クラスに関連付ける属性を持つ補助型オブジェクト・クラス。補助型クラスを指定する手順は、次のとおりです。 **1.** 「追加」を選択すると、「補助クラス・セレクタ」ダイアログ・ボックスが表示されます。 **2.** 追加する補助型クラスを選択します。 **3.** 「選択」を選択します。「新規コンテンツ・ルール」ダイアログ・ボックスに戻ります。「補助クラス」フィールドに指定した補助型クラスが表示されます。
必須属性	指定の構造型オブジェクト・クラスに関連付ける必須属性。必須属性を指定する手順は、次のとおりです。 **1.** 「追加」を選択すると、「必須属性セレクタ」ダイアログ・ボックスが表示されます。 **2.** 追加する必須属性を選択します。この属性に索引付けをする場合、「索引付け」列の対応するチェックボックスを選択します。 **3.** 「選択」を選択します。「新規コンテンツ・ルール」ダイアログ・ボックスに戻ります。「必須属性」フィールドに指定した必須属性が表示されます。
オプション属性	指定の構造型オブジェクト・クラスに関連付けるオプションの属性。オプション属性を指定する方法は次のとおりです。 **1.** 「追加」を選択すると、「オプション属性セレクタ」ダイアログ・ボックスが表示されます。 **2.** 追加するオプション属性を選択します。この属性に索引付けをする場合、「索引付け」列の対応するチェックボックスを選択します。 **3.** 「選択」を選択します。「新規コンテンツ・ルール」ダイアログ・ボックスに戻ります。「オプション属性」フィールドに指定したオプション属性が表示されます。

Oracle Directory Manager のサーバーの管理フィールド

この項では、次の項目について説明します。

- Oracle Directory Manager の構成設定フィールド
- Oracle Directory Manager のシステム操作属性フィールド
- Oracle Directory Manager のスーパー・ユーザー、ゲスト・ユーザーおよびプロキシ・ユーザー・フィールド
- Oracle Directory Manager の問合せ最適化フィールド
- Oracle Directory Manager のエントリ検索フィールドおよびボタン

Oracle Directory Manager の構成設定フィールド

関連項目： 5-4 ページの「Oracle Directory Manager を使用したサーバーの構成設定エントリの管理」

表 C-32「構成設定」ダイアログ・ボックス：「一般」タブ・ページのフィールド

フィールド	説明
DB の最大接続数	1 つのディレクトリ・サーバー・プロセスで処理可能なデータベースの同時接続数を入力します。デフォルトは 10 です。
子プロセスの数	単一のインスタンスが起動できるサーバー・プロセスの数を入力します。デフォルトは 1 です。
非 SSL ポート	デフォルトの非 SSL ポートは 389 です。この非 SSL ポートは変更できます。
設定	構成設定エントリの番号を入力します。デフォルトの構成設定は 0（ゼロ）です。異なる構成設定を必要な数だけ設定できます。複数のインスタンスで同じパラメータを必要とする場合は、同一の構成設定を使用できます。設定番号は変更可能です。
SASL 認証モード	デフォルト値は 1 です。このリリースの Oracle Internet Directory では、これ以外の値はサポートされていません。
SASL メカニズム	デフォルト値は DIGEST-MD5 です。このリリースの Oracle Internet Directory では、これ以外の値はサポートされていません。
SASL 暗号の選択	この複数値属性のデフォルト値は次のとおりです。 ■ RC4-56 ■ DES ■ 3DES

表 C-33「構成設定」:「SSL 設定」タブ・ページのフィールド

フィールド	説明
SSL 認証	次の中から 1 つ選択します。 ■ SSL 認証なし : クライアントとサーバーのいずれも、相手に対して自己認証を行いません。証明書の送信または交換は行われません。この場合は、SSL 暗号化 / 復号化のみ使用されます。 ■ SSL クライアントとサーバーの認証 : クライアントとサーバーは相互に自己認証を行い、相互に証明書を送信します。 ■ SSL サーバー認証 : ディレクトリ・サーバーのみ、クライアントに対して自己認証を行います。ディレクトリ・サーバーは、そのサーバーが認証されていることを証明する証明書をクライアントに送信します。
SSL 使用可能	次の中から 1 つ選択します。 ■ SSL と Non-SSL の両方 : 非保護操作と SSL 認証両方の場合。 ■ Non-SSL のみ : 非保護操作のみの場合。デフォルト・ポートは 389 で、この SSL ポート・フィールドで変更可能です。 ■ SSL のみ : SSL 認証の場合。デフォルト・ポートは 636 で、この SSL ポート・フィールドで変更可能です。

SSL Wallet URL	サーバー側の SSL Wallet の位置を入力します。Wallet の位置を変更する場合は、このパラメータを変更する必要があります。クライアントとサーバーの両方で Wallet の位置を設定する必要があります。たとえば UNIX では、このパラメータは次のように設定します。
	`file:/home/my_dir/my_wallet`
	Windows NT では、このパラメータは次のように設定します。
	`file:C:¥my_dir¥my_wallet`

SSL ポート	デフォルトの SSL ポートは 636 です。SSL ポートは変更できます。

Oracle Directory Manager のシステム操作属性フィールド

関連項目： 5-9 ページの「Oracle Directory Manager を使用したシステム操作属性の設定」

表 C-34 Oracle Directory Manager に表示されるシステム操作属性

フィールド	説明	デフォルト値	変更可能？
匿名ユーザーによるバインドを許可	匿名バインドを許可するかどうかを示します。1 に設定すると、匿名バインドが許可されます。0（ゼロ）に設定すると許可されません。	1	はい
代替サーバー	ローカル・サーバーとの接続が失われた場合に、クライアントは、この属性にリストされているサーバーの 1 つにアクセスすることができます。ローカル・サーバーと同じネーミング・コンテキストのセットを持つ、システム内の他の Oracle ディレクトリ・サーバーを指定します。書式は次のとおりです。 ldap://*host_name*:*port_number* **関連項目：**26-5 ページの「Oracle Directory Manager を使用した代替サーバー・リストの設定」を参照してください。	なし	はい
構成設定の位置	このサーバーに最上位のネーミング・コンテキストを保持しているエントリの識別名。	`cn=subconfigsubentry`	いいえ
重大イベント・レベル	記録する必要があるセキュリティおよびシステムに関連する重要なイベントを指定します。 スーパー・ユーザー、プロキシ、およびレプリケーション・ログイン以外のイベントについては、この機能を使用可能にするために `orclStatsFlag` 属性の値を 1 に設定する必要もあります。 **関連項目：**監視できる重要なイベントのリストは、10-22 ページの「重要なイベントの構成」を参照してください。	0	はい

表 C-34 Oracle Directory Manager に表示されるシステム操作属性（続き）

フィールド	説明	デフォルト値	変更可能？
DIP リポジトリ	ディレクトリ・レプリケーション・サーバーで使用され、Oracle Directory Integration and Provisioning Server でコンシュームするために、変更ログがコンシューマ・ノードで生成されるかどうかを示します。	FALSE	はい
ディレクトリ・バージョン	使用している Oracle Internet Directory のバージョン（リリース）。	9.0.4.0.0	いいえ
エントリ・キャッシュを使用可能にする	エントリ・キャッシング（2-3 ページの「エントリ・キャッシング」を参照）を使用可能にするかどうかを指定します。使用可能にする場合は 1、使用禁止にする場合は 0（ゼロ）です。	1	はい
グループ・キャッシュを使用可能にする	ディレクトリ・サーバー内の権限グループと ACL グループのキャッシュ。このキャッシュを使用すると、ACI で権限グループと ACP グループが使用される場合に、ユーザーに対するアクセス制御評価のパフォーマンスが改善されます。 権限グループのメンバーシップが頻繁に変化しない場合は、グループ・キャッシュを使用します。このメンバーシップが頻繁に変化する場合は、グループ・キャッシュをオフにするのが最善の方法です。これは、このような場合、グループ・キャッシュの計算によってオーバーヘッドが増大するためです。	1	はい
MatchDN 処理を使用可能にする	検索要求のベース識別名が見つからないと、ディレクトリ・サーバーは、指定されたベース識別名と一致する、最も近い識別名を戻します。ディレクトリ・サーバーが最も近い一致識別名の検索を試行するかどうかは、この属性によって制御されます。この属性を 1 に設定すると、一致識別名の処理が使用可能になります。0 に設定すると、一致識別名の処理が使用禁止になります。	1	はい

表 C-34 Oracle Directory Manager に表示されるシステム操作属性（続き）

フィールド	説明	デフォルト値	変更可能？
統計の収集を使用可能にする	Oracle Internet Directory サーバー管理機能フレームワークを使用可能にするかどうかを示すインジケータです。使用可能にするには、1 に設定します。使用禁止にするには、0（ゼロ）に設定します。	0	はい
エントリ・キャッシュ・サイズ（バイト）	エントリ・キャッシュが使用できる RAM の最大バイト数。	100M	はい
索引付き属性の位置	すべての索引付き属性を含むファイルの識別名を指定します。	cn=catalogs	いいえ
エントリ・キャッシュ内の最大エントリ	エントリ・キャッシュ内に存在可能な最大エントリ数を指定します。	25,000	はい
TCP 接続の最大アイドル時間	アイドル状態の接続を終了するまでの時間を指定します。	120	
ネーミング・コンテキスト	このサーバーに格納されている、公開するネーミング・コンテキストの最上位識別名を指定します。ネーミング・コンテキストとして識別名を公開するには、スーパー・ユーザー権限を持っている必要があります。	なし	はい
暗号化パスワード	パスワードを暗号化するハッシュ・アルゴリズム。オプションは次のとおりです。 ■ MD4 セキュア・ハッシュ・アルゴリズム ■ MD5 セキュア・ハッシュ・アルゴリズム ■ 暗号化を使用しない ■ **SHA** ■ **UNIX Crypt**	MD4	はい
プロセス・インスタンスの位置	このサーバーにインスタンス・レジストリを保持しているエントリの識別名。	cn=subregistrysubentry	いいえ
問合せエントリの返送制限	検索で戻されるエントリの最大数。	1000	はい
レプリカ ID	レプリケーション承諾のノードの一意識別子。		

表 C-34 Oracle Directory Manager に表示されるシステム操作属性（続き）

フィールド	説明	デフォルト値	変更可能？
レプリケーション承諾	レプリケーション承諾を保持しているエントリの識別名。	cn=orclareplagreements	いいえ
レプリケーション・ログの位置	このサーバーに変更ログを保持しているエントリの識別名。	cn=changelog	いいえ
レプリケーション・ステータスの位置	このサーバーに変更ステータスを保持しているエントリの識別名。	cn=changestatus	いいえ
スキーマ定義の位置	スキーマの識別名。	cn=subschemasubentry	いいえ
サーバー・モード	サーバーにデータを書き込むことができるかどうかを示します。この値は、「読取り / 書込み」か「読取り専用」のいずれかに変更できます。レプリケーション処理時はデフォルトを「読取り専用」に変更してください。	読取り / 書込み	選択肢は「読取り / 書込み」、「読取り / 更新」および「読取り専用」です。
サーバー処理の制限時間	検索の最大実行時間（秒）	3600	はい
変更ログ属性の簡易変更	マルチマスター・レプリケーション・グループでは、特定の属性値の変更で発生した競合を解消するために多くのリソースが必要な場合があります。このフィールドでその属性を指定することにより、パフォーマンス低下を回避できます。 このフィールドで属性を指定すると、その属性の値の変更は変更ログに反映されます。ただし、マルチマスター・レプリケーション・グループでは、この属性に対する競合解消はオフとなります。	uniquemember member	はい
統計収集間隔	サンプル統計を収集する頻度、つまり間隔（分単位）を指定します。1（分単位）以上を設定します。	60	はい
統計レベル	Oracle Internet Directory サーバー管理機能フレームワークを使用可能にするかどうかを指定します。使用可能にするには、1 に設定します。使用禁止にするには、0（ゼロ）に設定します。	0	はい

表 C-34 Oracle Directory Manager に表示されるシステム操作属性（続き）

フィールド	説明	デフォルト値	変更可能？
サポートされた制御リスト	任意の LDAP 操作の拡張情報を入力します。Oracle Internet Directory がサポートしている制御の種類は、`supportedcontrol` 属性の値としてルート DSE にリストされています。制御の各種類には、LDAP 規格で定義されているオブジェクト識別子が関連付けられています。`supportedcontrol` 属性の値は、制御の種類に割り当てられた標準のオブジェクト識別子です。	`manageDSACtrl`	いいえ
サポートされている拡張子	このリリースの Oracle Internet Directory がサポートしている LDAP 操作に対する独自拡張機能の一意識別子です。 リリース 9.0.4 では、拡張操作が 1 つあります。この操作は、プラグインが、データベースの PL/SQL パッケージを使用してディレクトリ・サーバーへバインドできるようにします。	2.16.840.1.113894.1.9.1	いいえ
サポートされる LDAP のバージョン	Oracle Internet Directory でサポートしている LDAP のバージョンです。	`LDAP Version 2` `LDAP Version 3`	いいえ
サポートされている SASL メカニズム	クライアントの一部では、Simple Authentication and Security Layer（SASL）を使用できます。このフィールドは、ディレクトリ・サーバーがサポートしている認証メカニズムを示します。 **関連項目：** ■ 12-9 ページの「SASL 対応クライアントが Digest-MD5 を使用してディレクトリ・サーバーに対して認証する方法」 ■ 12-9 ページの「SASL 対応クライアントが外部認証を使用してディレクトリ・サーバーに対して認証する方法」	`DIGEST-MD5`	いいえ
アップグレード進行中	アップグレード用に予約済です。	FALSE	いいえ

Oracle Directory Manager のスーパー・ユーザー、ゲスト・ユーザーおよびプロキシ・ユーザー・フィールド

関連項目： 5-12 ページの「Oracle Directory Manager を使用したスーパー・ユーザー、ゲスト・ユーザーおよびプロキシ・ユーザーの管理」

表 C-35「システム・パスワード」タブ・ページのフィールド

フィールド	説明
スーパー・ユーザー名	スーパー・ユーザーの名前を入力するか、「参照」をクリックし検索します。デフォルトは `orcladmin` です。
スーパー・ユーザー・パスワード	スーパー・ユーザーのパスワードを入力します。デフォルトは、インストール時に Oracle Application Server 管理者に指定したパスワード（ias_admin）と同じです。このパスワードはすぐに変更してください。
ゲストのログイン名	ゲスト・ログイン名を入力するか、「参照」をクリックし検索します。ゲストには、そのディレクトリ内の**アクセス制御リスト**で指定されている権限が与えられます。デフォルトは `guest` です。
ゲストのログイン・パスワード	ゲスト・ログイン・パスワードを入力します。デフォルトは `guest` です。
プロキシ・ログイン名	プロキシ・ログイン名を入力するか、「参照」をクリックし検索します。プロキシ・ユーザーには、そのディレクトリ内の ACP で指定されている権限が与えられます。デフォルトは `proxy` です。
プロキシ・ログイン・パスワード	プロキシ・ログイン・パスワードを入力します。デフォルトは `proxy` です。このパスワードはすぐに変更してください。

Oracle Directory Manager の問合せ最適化フィールド

関連項目： 21-12 ページの「Oracle Directory Manager を使用したスキュー属性の検索の最適化」

表 C-36「問合せの最適化」タブ・ページのフィールド

フィールド	説明
低カーディナリティの属性	スキュー属性として指定する属性を入力します。 **関連項目：**スキュー属性の詳細は、21-11 ページの「検索の最適化」を参照してください。
一般名	スキュー属性に関する情報を持つエントリの共通名 `dsaconfig`。このフィールドは変更できません。

表 C-36「問合せの最適化」タブ・ページのフィールド（続き）

フィールド	説明
識別名	スキュー属性に関する情報を持つエントリの識別名。このフィールドは変更できません。
LDAP 接続タイムアウト	ディレクトリ・クライアントが、接続が終了するまでアイドル状態を保持する最大時間（秒）を入力します。デフォルトは 0 です。これはタイムアウトがないことを意味します。
キャッシュ内の最大エントリ・サイズ	キャッシュに格納できるエントリ・サイズの上限を指定します。デフォルトは 5000、つまり 5KB です。
オブジェクト・クラス	dsaconfig エントリに関連付けられたオブジェクト・クラス。
時間制限モード	5-9 ページの「システム操作属性の設定」の説明に従って、サーバー処理の制限時間を設定する場合は、検索の完了までの最大時間（秒）を指定します。 このフィールドでは、サーバーのパフォーマンスを調整するために、検索時間を厳密に設定するかおおよその時間に設定します。正確な時間に設定すると、検索は必ず指定した秒数で終了します。おおよその時間に設定すると、検索は指定した秒数から 2 秒の範囲内で終了します。作業負荷が低い場合は、後者の方がより高いパフォーマンスを得られます。

Oracle Directory Manager のエントリ検索フィールドおよびボタン

表 C-37 エントリの検索フィルタ

フィルタ	説明
開始	属性の値の始めの数文字のみを使用して検索します。たとえば、「cn」「次の文字で始まる」「Fran」と指定すると、cn 属性が Fran で始まるすべてのエントリが取り出されます。この場合は、Frank、Fran、Frances、Franklin などが取り出されます。
終了	指定した属性の値の終わりの数文字のみを使用してエントリを検索します。たとえば、「cn」「終了」「son」と指定すると、Baldisson、Jacobson、Johnson などが取り出されます。
含む	値の位置を限定せずに、ユーザーの入力値が指定した属性に含まれているエントリを検索します。たとえば、「cn」「含む」「Wins」と指定すると、cn 属性に wins を含むエントリがすべて取り出されます。この場合は、Winslow、Czerwinski、Winship などが取り出されます。
完全一致	指定した属性がユーザーの入力値に一致するエントリを検索します。たとえば、「cn」「完全一致」「Franklin Baldwins」と指定すると、cn 属性の値が Franklin Baldwins のエントリがすべて取り出されます。

表 C-37 エントリの検索フィルタ（続き）

フィルタ	説明
以上	指定した属性が、数値順またはアルファベット順で入力値より大か等しいエントリを検索します。たとえば、「cn」「以上」「Frank」と指定すると、cn 属性の範囲が、Frank からアルファベットの最後の文字までのエントリがすべて取り出されます。
以下	指定した属性が、数値順またはアルファベット順で入力値より小か等しいエントリを検索します。たとえば、「cn」「以下」「Frank」と指定すると、Frank からアルファベットの最初の文字までの cn 属性がすべて取り出されます。
存在	指定した属性を持つエントリが、ツリーのそのレベルに存在するかどうかを判断します。この関連の使用に値の入力は不要です。「cn」「存在」と指定すると、ツリーのそのレベルで、cn 属性を持つエントリがすべて取り出されます。

表 C-38 エントリ検索ボタン

ボタン	説明
新規作成	「**基準**」フィールドに、新しい検索基準バーを作成します。このボタンは、「**基準**」フィールドに何も表示されていないときのみ使用可能です。
AND	「**基準**」フィールドに、別の検索基準バーを作成します。指定した両方の属性を持つエントリをすべて検索します。たとえば、`cn=Baldwins And title=Laborer` と指定すると、cn が Baldwins で、かつ title が laborer のエントリがすべて取り出されます。
OR	「**基準**」フィールドに、別の検索基準バーを作成します。指定した属性のいずれかを持つエントリをすべて検索します。たとえば、`title=Laborer Or title=Foreman` と指定すると、title が laborer または foreman の従業員がすべて取り出されます。
NOT	選択した検索基準バーの基準を除外し、指定した基準を満たさないエントリをすべて取り出します。たとえば、`cn=Frank Not title=Laborer` と指定すると、cn が Frank で、title が laborer ではない個人がすべて取り出されます。
削除	選択した検索基準バーを削除します。

表 C-38 エントリ検索ボタン（続き）

ボタン	説明
拡張	検索に属性オプションを含ませる場合に、検索基準バーを追加します。この場合は次の構文を使用します。*attribute;attribute_option filter attribute_option_value* たとえば、`cn;lang_sp=J*` と指定すると、文字 J で始まる `cn;lang_sp=` の属性オプション値をすべて取り出します。 **注意：**属性オプション値を検索に使用するには、その属性オプションの親属性が索引付けされている必要があります。たとえば、属性オプション `carLicense;lang_sp` を検索に使用するには、`carLicense` 属性が索引付けされている必要があります。 **関連項目：** ■ 6-16 ページの「Oracle Directory Manager を使用した属性の索引付け」 ■ 6-19 ページの「コマンドライン・ツールを使用した属性の索引付け」

Oracle Directory Manager の SSL 管理フィールド

関連項目：

- C-26 ページの表 C-33
- 13-3 ページの「Oracle Directory Manager を使用した SSL パラメータの構成」

表 C-39「SSL 設定」タブ・ページのフィールド

フィールド	説明
SSL 認証	次の中から 1 つ選択します。 ■ SSL 認証なし : クライアントとサーバーのいずれも、相手に対して自己認証を行いません。証明書の送信または交換は行われません。「資格証明」タブの「SSL 使用可能」チェックボックスを選択して、このオプションを選択した場合は、SSL 暗号化 / 復号化のみが使用されます。 ■ SSL クライアントとサーバーの認証 : クライアントとサーバーの認証。クライアントとサーバーは、証明書を交換します。 ■ SSL サーバー認証 : サーバー認証。ディレクトリ・サーバーがクライアントに証明書を送信することによって、ディレクトリ・サーバーからクライアントに対してサーバー認証を行います。

表 C-39「SSL 設定」タブ・ページのフィールド（続き）

フィールド	説明
SSL 使用可能	次の中から 1 つ選択します。 ■ **SSL と Non-SSL の両方** : 非保護操作と SSL 認証両方の場合。 ■ **Non-SSL のみ** : 非保護操作のみの場合。 ■ **SSL のみ** : SSL 認証のみの場合。

SSL Wallet URL	サーバー側の SSL Wallet の位置を入力します。Wallet の位置を変更する場合は、このパラメータを変更する必要があります。クライアントとサーバーの両方で Wallet の位置を設定する必要があります。たとえば UNIX では、このパラメータは次のように設定します。
	`file:/home/my_dir/my_wallet`
	Windows NT では、このパラメータは次のように設定します。
	`file:C:¥my_dir¥my_wallet`

SSL ポート	デフォルトの SSL ポートは 636 です。SSL ポートは変更できます。

Oracle Directory Manager の同期フィールド

ディレクトリ統合プロファイルを登録するフィールド

表 C-40 Oracle Directory Manager の同期に関する「一般」タブ・ページのフィールド

フィールド	説明
プロファイル名	プロファイルの名前を指定します。入力した名前は、この統合プロファイルの識別名の相対識別名コンポーネントとして使用されます。たとえば、プロファイル名 `MSAccess` を指定して、`orclodipagentname=MSAccess,cn=subscriber profile, cn=changelog subscriber, cn=oracle internet directory` という名前の統合プロファイルを作成します。 このフィールドは必須です。このフィールドにデフォルトの設定はありません。
同期モード	インポート操作かエクスポート操作かを指定します。インポート操作は、接続ディレクトリの変更を Oracle Internet Directory に移します。エクスポート操作は、Oracle Internet Directory から接続ディレクトリに変更を送信します。 このフィールドは必須です。デフォルトは `IMPORT` です。

表 C-40 Oracle Directory Manager の同期に関する「一般」タブ・ページのフィールド（続き）

フィールド	説明
プロファイル・ステータス	プロファイルが使用可能か使用禁止かを指定します。 このフィールドは必須です。デフォルトは ENABLE です。
プロファイル・パスワード	Directory Integration and Provisioning Server がプロファイルのかわりに Oracle Internet Directory にバインドするときに使用するパスワードを指定します。このフィールドは必須で、デフォルトは welcome です。
スケジューリングの間隔	接続ディレクトリと Oracle Internet Directory の同期の、試行間隔の秒数を指定します。 このフィールドは必須です。デフォルトは 60 です。
最大試行回数	Directory Integration and Provisioning Server が同期を無効化するまでに同期を試行する回数の、最大数を指定します。このフィールドは必須です。 デフォルトは 5 です。最初の再試行は最初の失敗の 1 分後に行われます。2 回目の再試行は 2 回目の失敗の 2 分後に、後続の再試行は n 回目の失敗の n 分後に行われます。
プロファイルのバージョン	このプロファイルが作成された Oracle Directory Integration and Provisioning Platform のバージョン。

表 C-41 Oracle Directory Manager の同期に関する「実行」タブ・ページのフィールド

フィールド	説明

エージェント実行コマンド	Directory Integration and Provisioning Server がエージェントを実行するために使用するエージェント実行可能ファイルの名前と引数を指定します。
	このフィールドはオプションです。デフォルトはありません。
	一般的な実行コマンドは、次の形式です。
	`odicmd user=%orclodipcondirAccessAccount pass=%orclodipcondiraccesspassword`
	`odicmd` は、実行するコマンドです（パスに指定されている場合に使用可能、またはフルパス名で指定）。
	`user=%orclodipcondirAccessAccount pass=%orclodipcondiraccesspassword`
	はコマンドライン引数です。ユーザー（`user`）に渡される値は `orclodipcondiraccessaccount` 属性から、パス（`pass`）に渡される値は `orclodipcondiraccesspassword` 属性から導出されます。
	一般的な例は、Oracle Human Resources エージェントにあります。

接続されたディレクトリ・アカウント	コネクタまたはエージェントが接続ディレクトリにアクセスするために使用するアカウントを指定します。たとえば、接続ディレクトリがデータベースの場合、アカウントは `Scott` などになります。接続ディレクトリが別の LDAP 準拠ディレクトリの場合は、アカウントは `cn=Directory Manager` などになります。 このフィールドはオプションです。このフィールドにデフォルトの設定はありません。
接続されたディレクトリ・アカウントのパスワード	コネクタまたはエージェントが接続ディレクトリにアクセスするときに使用するパスワードを指定します。このフィールドはオプションです。このフィールドにデフォルトの設定はありません。
追加構成情報	このフィールドには、Directory Integration and Provisioning Server がエージェントに渡す追加情報が表示されます。このフィールドは Oracle Directory Manager で変更できません。このフィールドを変更する唯一の方法は、ldapuploadagentfile.sh を使用することです。このフィールドにデフォルトの設定はありません。

表 C-41 Oracle Directory Manager の同期に関する「実行」タブ・ページのフィールド（続き）

フィールド	説明
接続ディレクトリの URL	接続ディレクトリへの接続に必要な接続詳細。このパラメータは、ホスト名とポート番号を *host*:*port*:*sslmode* の形式で示します。 SSL を使用して接続するには、*host*:*port*:1 を入力します。 ディレクトリに接続するための証明書が Wallet に格納され、その場所がファイル odi.properties に指定されていることを確認します。 **注意：**SSL を使用して SunONE Directory Server に接続するには、サーバー証明書を Wallet にロードする必要があります。 **関連項目：**『Oracle Advanced Security 管理者ガイド』の Oracle Wallet Manager についての章を参照してください。
インタフェース・タイプ	インポート・ファイルまたはエクスポート・ファイルが使用する形式。オプションは、DB、LDAP、LDIF および TAGGED です。このフィールドはオプションです。デフォルトは TAGGED です。

表 C-42 Oracle Directory Manager の同期に関する「マッピング」タブ・ページのフィールド

フィールド	説明
マッピング・ルール	このフィールドには、接続ディレクトリと Oracle Internet Directory の間でデータを変換するためのマッピング・ルールが表示されます。このフィールドにデフォルトの設定はありません。 **注意：**マッピング・ルール・ファイルは、Oracle Directory Manager では編集できません。ファイルのマッピング・ルールは手動で編集し、提供されたスクリプト ldapuploadagentfile.sh を使用してプロファイルにアップロードします。付録 A「LDIF およびコマンドライン・ツールの構文」を参照してください。
接続ディレクトリの照合フィルタ	接続ディレクトリのエントリを一意に識別する属性を指定します。
OID の照合フィルタ	Oracle Internet Directory のレコードを一意に識別する属性を指定します。この属性は、Oracle Internet Directory と接続ディレクトリを同期化するためのキーとして使用されます。このフィールドはオプションです。

表 C-43 Oracle Directory Manager の同期に関する「ステータス」タブ・ページのフィールド

フィールド	説明
OID 前回適用された変更番号 (インポート操作のみ)	エクスポート操作に、接続ディレクトリに適用された Oracle Internet Directory からの最後の変更の識別子を指定します。デフォルトは 0 です。エンド・ユーザーはこのフィールドを必要に応じて意識的に変更できます。プロファイルは、使用禁止モードにしてください。番号が増加した場合、元の値と新しい値の間に番号付けされた変更ログ・エントリは適用されません。
最終実行時間	エージェントが実行された最新の絶対日時。デフォルトは、コネクタの作成日時です。このフィールドを変更すると誤解を招く恐れがあります。
最終正常実行時間	エージェントの実行が成功した最新の絶対日時。デフォルトは、コネクタの作成日時です。このフィールドを変更すると誤解を招く恐れがあります。
同期ステータス	同期の成功または失敗。
同期エラー	最後のエラー・メッセージ。このフィールドは変更できません。このフィールドにデフォルトの設定はありません。
最後に適用された変更番号 (エクスポート操作のみ)	接続ディレクトリに正常に適用された最新の変更ログ・エントリの数。エンド・ユーザーはこのフィールドを必要に応じて意識的に変更できます。プロファイルは、使用禁止モードにしてください。番号が増加した場合、元の値と新しい値の間に番号付けされた変更ログ・エントリは適用されません。
ブートストラップ・ステータス	

Oracle Internet Directory セルフ・サービス・コンソールのフィールド

この項では、次の項目について説明します。

- Oracle Internet Directory セルフ・サービス・コンソールのユーザー管理フィールド
- Oracle Internet Directory セルフ・サービス・コンソールの認証管理レルム・フィールド
- Oracle Internet Directory セルフ・サービス・コンソールのリソース・アクセス情報フィールド

Oracle Internet Directory セルフ・サービス・コンソールのユーザー管理フィールド

表 C-44「新規属性の追加」ウィンドウのフィールド

フィールド	説明
ディレクトリ属性名	属性名
UI ラベル	ユーザー・インタフェースに表示する属性に、わかりやすい名前を指定します。たとえば、sn 属性を、インタフェースでは *Last Name* と表示することができます。
必須フィールド	ユーザーの作成および変更時に属性を必須にするかどうかを指定します。インタフェースに表示される必須属性は、フィールドの左にアスタリスク（*）が付いています。このチェックボックスを選択しない場合、属性はオプションになります。
表示可能	属性を検索結果に表示させるかどうかを、このチェックボックスを選択して指定します。
自己編集可能	エンド・ユーザーが「マイ・プロファイルの編集」ウィンドウを使用して、自分のエントリにあるこの属性の値を変更できるようにするかどうかを指定します。
パスワードのリセットの検証	ユーザーが自分のパスワードを忘れてしまった場合、この属性を使用してユーザーを確認できるように指定するために選択します。
検索可能	デフォルトでは、ユーザーが検索要求を入力すると、Oracle Internet Directory セルフ・サービス・コンソールは cn、firstname、lastname および e-mail 属性に基づいた検索を実行します。検索可能な属性をカスタマイズすることができます。たとえば、追加した属性に基づいて検索を使用可能にする場合、このチェックボックスを選択します。検索を可能にする場合は、属性をカタログ化する必要があります。

表 C-44「新規属性の追加」ウィンドウのフィールド（続き）

フィールド	説明
UI タイプ	このフィールドに対しインタフェース・タイプを指定します。オプションは次のとおりです。 ■ 単一行テキスト : ユーザーが値を入力するテキスト・フィールド。 ■ 複数行テキスト : ユーザーが複数のテキスト行を入力できるテキスト領域。 ■ 事前定義リスト : ユーザーがドロップダウン・リストから値を選択するコンボ・ボックス。このインタフェース・タイプを選択すると、「LOV 値」テキスト領域が表示されます。このテキスト領域では、リストに値を入力し、入力を 1 回終了するごとに改行キーを押します。 ■ 日付 : ユーザーが日付（従業員の生年月日など）を入力するテキスト・フィールド。 ■ 参照と選択 : ユーザーが、マネージャのエントリまたは属性値などの識別名を必要とするエントリを参照可能にするボタン。 ■ 数値 : ユーザーが番号のみ（郵便番号など）を入力するテキスト・フィールド。

関連項目： 31-13 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用したユーザー・エントリの構成」

表 C-45「属性の編集」ウィンドウのフィールド

フィールド	説明
UI ラベル	ユーザー・インタフェースに表示する属性に、わかりやすい名前を指定します。たとえば、sn 属性を、インタフェースでは *Last Name* と表示することができます。
必須フィールド	ユーザーの作成および変更時に属性を必須にするかどうかを指定します。インタフェースに表示される必須属性は、フィールドの左にアスタリスク（*）が付いています。このチェックボックスを選択しない場合、属性はオプションになります。
表示可能	属性を検索結果に表示させるかどうかを、このチェックボックスを選択して指定します。
自己編集可能	エンド・ユーザーが「マイ・プロファイルの編集」ウィンドウを使用して、自分のエントリにあるこの属性の値を変更できるようにするかどうかを指定します。
パスワードのリセットの検証	ユーザーが自分のパスワードを忘れてしまった場合、この属性を使用してユーザーを確認できるように指定するために選択します。

表 C-45「属性の編集」ウィンドウのフィールド（続き）

フィールド	説明
検索可能	デフォルトでは、ユーザーが検索要求を入力すると、Oracle Internet Directory セルフ・サービス・コンソールは cn、firstname、lastname および e-mail 属性に基づいた検索を実行します。検索可能な属性をカスタマイズすることができます。たとえば、編集した属性に基づいて検索を使用可能にする場合、このチェックボックスを選択します。検索を可能にする場合は、属性をカタログ化する必要があります。
UI タイプ	このフィールドに対しインタフェース・タイプを指定します。オプションは次のとおりです。 ■ 単一行テキスト : ユーザーが値を入力するテキスト・フィールド。 ■ 複数行テキスト : ユーザーが複数のテキスト行を入力できるテキスト領域。 ■ 事前定義リスト : ユーザーがドロップダウン・リストから値を選択するコンボ・ボックス。このインタフェース・タイプを選択すると、「LOV 値」テキスト領域が表示されます。このテキスト領域では、リストに値を入力し、入力を 1 回終了するごとに改行キーを押します。 ■ 日付 : ユーザーが日付（従業員の生年月日など）を入力するテキスト・フィールド。 ■ 参照と選択 : ユーザーが、マネージャのエントリまたは属性値などの識別名を必要とするエントリを参照可能にするボタン。 ■ 数値 : ユーザーが番号のみ（郵便番号など）を入力するテキスト・フィールド。

関連項目： 31-13 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用したユーザー・エントリの構成」

表 C-46「権限の割当て」ウィンドウのフィールド

権限	付与されたアクセス権の説明
ユーザーの作成を許可	ユーザー・エントリの作成
ユーザーの編集を許可	ユーザー・エントリの変更
ユーザーの削除を許可	ユーザー・エントリの削除
グループの作成を許可	グループ・エントリの作成
グループの編集を許可	グループ・エントリの変更
グループの削除を許可	グループ・エントリの削除

表 C-46「権限の割当て」ウィンドウのフィールド（続き）

権限	付与されたアクセス権の説明
ユーザーへの権限の割当てを許可	ユーザーに対するアクセス権の割当て
グループへの権限の割当てを許可	グループに対するアクセス権の割当て
サービス管理の許可	ユーザーに対するサービスを管理するグループ・メンバーを使用可能にする。この権限が選択されている場合、グループ・メンバーが「**ディレクトリ**」タブ・ページにアクセスすると、このタブページ内の**サービス**・リンクは使用可能になります。
アカウント管理の許可	ユーザーに対するサービスを管理するグループ・メンバーを使用可能にする。この権限が選択されている場合、グループ・メンバーが「**ディレクトリ**」タブ・ページにアクセスすると、このタブページ内の**アカウント**・リンクは使用可能になります。
Oracle Delegated Administration Services 構成の許可	Oracle Delegated Administration Services ユーザー・インタフェースの構成

関連項目：

- 31-18 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用したユーザーへの権限の割当て」
- 31-21 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用したグループへの権限の割当て」

Oracle Internet Directory セルフ・サービス・コンソールの認証管理レルム・フィールド

表 C-47 ASP 管理者用の「認証管理レルムの作成」ウィンドウ

フィールド	説明
基本情報	
レルム名	このレルムに対して比較的短いレルム名を入力します。入力した名前は、このレルム・エントリの識別名として使用されます。このフィールドは必須です。
レルム連絡先	このレルムに関する問題の問合せ担当者の名前を入力します。
説明	このレルムに関する追加情報を入力します。このフィールドはオプションです。

表 C-47 ASP 管理者用の「認証管理レルムの作成」ウィンドウ（続き）

フィールド	説明
ロゴの管理	
レルム・ロゴを使用可能にする	このフィールドを選択すると、「認証管理レルムの構成」ウィンドウにレルム・ロゴが表示されます。
製品ロゴを使用可能にする	このフィールドを選択すると、「認証管理レルムの構成」ウィンドウに製品ロゴが表示されます。 **注意：**「レルム・ロゴを使用可能にする」および「製品ロゴを使用可能にする」が両方とも選択されている場合、レルム・ロゴが上部に、製品ロゴがその下に表示されます。
レルム・ロゴの更新	このレルムのロゴのパスおよびファイル名を入力するか、「**参照**」を選択してナビゲートします。

表 C-48「認証管理レルム」ウィンドウのフィールド

フィールド	説明
ディレクトリの構成	
ログイン名の属性	ユーザーがログイン時に本人の識別をするための属性を入力します。たとえば、`UID`、`EmployeeNumber`、`SSN` などです。 これはユーザーを一意に識別する属性です。Oracle Application Server Single Sign-On は、ログイン時にこの属性を使用してユーザーを特定します。この属性を変更する場合、各ユーザー・エントリにこの属性があり、一意であることを確認してください。ユーザー検索ベースでこの属性に属性一意性制約を設定することにより、一意性を施行できます。 このフィールドは必須です。
RDN の属性	ユーザー・エントリの相対識別名コンポーネントを作成するために使用する属性。このフィールドに入力する値は、「ログイン名の属性」フィールドで入力した値とは違う値にします。
ユーザー検索ベース	このレルムに対するユーザー・エントリが置かれるエントリの識別名を入力します。有効な識別名を入力し、ユーザーがこのコンテキストに存在する必要があります。ユーザー・ログイン時に、Oracle Application Server Single Sign-On によって、このコンテキストのユーザーが検索されます。 また、すべての ACL が適切に設定されていることを確認してください。ACL 間に不一致があると、ログイン処理または Oracle Internet Directory セルフ・サービス・コンソールの動作が中断します。 このフィールドは必須です。

表 C-48「認証管理レルム」ウィンドウのフィールド（続き）

フィールド	説明

ユーザー作成ベース	このレルムに対するユーザーが作成されるエントリの識別名を入力します。この識別名は、ユーザー検索ベースの識別名と同じである必要があります。
	ユーザー検索ベース下の異なるコンテキストにユーザーを分散する場合、この値をユーザー検索ベースの値と異なる値で設定できます。いずれの場合も、この識別名は、ユーザー検索ベースの識別名またはユーザー検索ベース下のコンテキストの識別名のいずれかである必要があります。たとえば、ユーザー検索ベースが `cn=users,dc=acme,dc=com` の場合、地域に基づいてユーザーを分別するには、この値を次のように設定します。
	`L=America, cn=users,dc=acme,dc=com`
	`L=Asia, cn=users,dc=acme,dc=com`
	`L=Europe, cn=users,dc=acme,dc=com`
	注意：Oracle Internet Directory セルフ・サービス・コンソールでは、これらのコンテキストが存在し、これらのコンテキストの権限が正しく設定されていると想定されています。

グループ検索ベース	このレルムに対するグループ・エントリが置かれるエントリの識別名を入力します。このフィールドは必須です。
グループ作成ベース	このレルムに対するグループが作成されるエントリの識別名を入力します。
検索結果制限	検索で表示される最大数を入力します。このフィールドは必須です。
ロゴの管理	
レルム・ロゴを使用可能にする	このフィールドを選択すると、「認証管理レルムの構成」ウィンドウにレルム・ロゴが表示されます。
製品ロゴを使用可能にする	このフィールドを選択すると、「認証管理レルムの構成」ウィンドウに製品ロゴが表示されます。 **注意：**「レルム・ロゴを使用可能にする」および「製品ロゴを使用可能にする」が両方とも選択されている場合、レルム・ロゴが上部に、製品ロゴがその下に表示されます。
レルム・ロゴの更新	このレルムのロゴのパスおよびファイル名を入力するか、「**参照**」を選択してナビゲートします。

関連項目：

- 31-11 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用した認証管理レルムの構成」
- 作成ベースおよび検索ベースを変更する場合の適切な設定手順は、付録 H「ユーザーおよびグループの作成ベースおよび検索ベースに対するアクセス制御の設定」を参照してください。

Oracle Internet Directory セルフ・サービス・コンソールのリソース・アクセス情報フィールド

表 C-49「リソース・タイプの作成」ウィンドウのフィールド

プロパティ	説明
表示名	ユーザー・インタフェースにリソース・タイプが表示されるきに使用する名前です。
説明	テキスト形式の説明で、リソース・タイプの用途およびそのリソース・タイプで入力する他の情報を説明します。
認証クラス	このフィールドは、空白のままにしておきます。

接続文字列	リソース用の Oracle Internet Directory に格納されている値を使用して、接続文字列を構成するための形式です。次に例を示します。
	■ Oracle9*i* データベース・サーバーまたは JDBC データ・ソースの場合、接続文字列形式は次のようになります。
	`orclUserIDAttribute/orclPasswordAttribute @orclFlexAttribute1`
	この文字列では、ユーザー名の後にスラッシュ、パスワード、アットマーク（@）および追加属性 1（たとえば、データベースの TNS 名に対する追加属性など）が続きます。この形式に準拠している接続文字列は、次に示す文字列のようになります。
	`scott/tiger@db1`
	■ Oracle Express では、接続文字列形式は次のようになります。
	server=orclFlexAttribute1/domain=orclFlexAttribute2/user=orclUserIDAttribute/password=orclPasswordAttribute
	この文字列では、server= の後に、1 つ目の追加属性、スラッシュ、domain=、2 つ目の追加属性、スラッシュおよびパスワードが続きます。この形式に準拠している接続文字列は、次に示す文字列のようになります。
	`server=a1/domain=a2/user=scott/password=tiger`

表 C-49「リソース・タイプの作成」ウィンドウのフィールド（続き）

プロパティ	説明
ユーザー名 /ID フィールド名	新規のリソース・アクセス情報を作成するときに、「リソースの作成」ウィンドウに表示される「ユーザー名」フィールドの表示名です。通常、この表示名は「ユーザー名」です。
パスワード・フィールド名	「リソースの作成」ウィンドウの「パスワード」フィールドの表示名です。通常、この表示名は「パスワード」です。
追加フィールド	「リソースの作成」ウィンドウで表示される、ユーザー名およびパスワード以外の追加フィールドの表示名です。たとえば、このフィールドの 1 つをサーバー名またはドメイン名を表示するように使用できます。通常、この表示名は「サーバー」または「ドメイン」のようにフィールドの内容を説明する名前になります。

D

LDAP フィルタ定義

この付録に記載されている文書は、Internet Engineering Task Force（IETF）の RFC2254 の許可を得て転載されています。この文書は、次の URL で参照できます。
`http://www.ietf.org`

この文書より後で発行された文書または他の情報が、ここに記載された内容より優先される場合があります。追加情報または補足情報は、前述の Web サイトおよび関連サイトをチェックしてください。

注意： オラクル社は、すべての保証を明示的にも暗黙的にも行いません。ここでいう保証には、この情報の使用がいかなる権利も侵害しないという保証や、特定の目的に対する商業性と適合性への暗示的な保証が含まれますが、これに限定されるものではありません。

ネットワーク・ワーキング・グループ T. Howes
Request for Comments: 2254 Netscape Communications 社
種類 : 標準化過程 1997 年 12 月

The String Representation of LDAP Search Filters

1. この文書の状態

この文書はインターネット・コミュニティにおけるインターネット標準化過程プロトコルを定義しています。改善のための議論と提案をお待ちしています。このプロトコルの標準化段階と状態については、最新版の「インターネット公式プロトコル標準」（STD 1）を参照してください。この文書の配布に制約はありません。

IESG からのメモ

この文書は、読取りアクセスと更新アクセスの両方を提供するディレクトリ・アクセス・プロトコルについて説明しています。更新アクセスでは安全な認証が要求されますが、この文書では、十分な認証メカニズムの実装を強制していません。

このような制限はありますが、この仕様は、RFC 2026 の 4.4.1 項に従い、標準勧告として IESG から承認されています。これは、次の理由によります。

a. このプロトコルの配置前に、プロトコルの実装と相互運用性のテストが奨励されるため（更新アクセスの有無に関係なく）

b. 読取り専用アプリケーションでは、このプロトコルの配置と使用が奨励されるため（たとえば、LDAP 以外の安全な方法で更新されたディレクトリへの問合せ言語として LDAP バージョン 3 を使用するアプリケーション）

c. LDAP バージョン 3 のディレクトリ・サーバーへの問合せ機能が必要な（更新機能は不要）他のインターネット標準化過程プロトコルの進展と配置の遅れを避けるため

必要な認証メカニズムが標準化されるまで、更新機能を使用するこの仕様に従って記述されたクライアントとサーバーは、認証レベルを許容し難いレベルまで低下させないかぎり、相互運用は不可能です。

LDAP バージョン 3 での必要な認証の標準勧告が承認されて RFC 文書として公開されるまで、更新機能を実装する LDAP バージョン 3 クライアントまたはサーバーの配置はお薦めできません。

2. 要約

Lightweight Directory Access Protocol（LDAP）[1] は、LDAP サーバーに送信される検索フィルタのネットワーク表現を定義します。検索フィルタを読みやすい書式で表現する共通の方法は、一部のアプリケーションで役立ちます。この文書は、LDAP 検索フィルタを表現するための読みやすい文字列書式を定義します。

RFC 1960 に替わるこの文書では、LDAP フィルタ文字列の定義が拡張され、LDAP バージョン 3 の拡張一致フィルタがサポートされ、あらゆる範囲の LDAP 検索フィルタの表現もサポートされます。

3. LDAP 検索フィルタ定義

LDAP バージョン 3 の検索フィルタは、[1] の 4.5.1 項で次のように定義されています。

```
Filter ::= CHOICE {
        and             [0] SET OF Filter,
        or              [1] SET OF Filter,
        not             [2] Filter,
        equalityMatch   [3] AttributeValueAssertion,
```

```
        substrings        [4] SubstringFilter,
        greaterOrEqual    [5] AttributeValueAssertion,
        lessOrEqual       [6] AttributeValueAssertion,
        present           [7] AttributeDescription,
        approxMatch       [8] AttributeValueAssertion,
        extensibleMatch   [9] MatchingRuleAssertion
}
SubstringFilter ::= SEQUENCE {
        type    AttributeDescription,
        SEQUENCE OF CHOICE {
                initial       [0] LDAPString,
                any           [1] LDAPString,
                final         [2] LDAPString
        }
}
AttributeValueAssertion ::= SEQUENCE {
        attributeDesc   AttributeDescription,
        attributeValue  AttributeValue
}
MatchingRuleAssertion ::= SEQUENCE {
        matchingRule    [1] MatchingRuleID OPTIONAL,
        type            [2] AttributeDescription OPTIONAL,
        matchValue      [3] AssertionValue,
        dnAttributes    [4] BOOLEAN DEFAULT FALSE
}
AttributeDescription ::= LDAPString
AttributeValue ::= OCTET STRING
MatchingRuleID ::= LDAPString
```

AssertionValue ::= OCTET STRING

LDAPString ::= OCTET STRING

LDAPString は、ISO 10646 キャラクタ・セット [4] の UTF-8 エンコーディングに限定されます。AttributeDescription は、属性説明の文字列表現で、[1] で定義されます。

AttributeValue および AssertionValue OCTET STRING には、[2] で定義される書式があります。このフィルタは、[3] で定義される基本エンコーディング規則および [1] で説明されている簡略化によって、ネットワーク上の送受信用にエンコードされます。

4. 検索フィルタ文字列の定義

LDAP 検索フィルタの文字列表現は、[5] で定義される ABNF 表記規則に従って、次の構文で定義されます。フィルタの書式には、接頭辞の表記規則が使用されます。

```
filter     = "(" filtercomp ")"
filtercomp = and / or / not / item
and        = "&" filterlist
or         = "|" filterlist
not        = "!" filter
filterlist = 1*filter
item       = simple / present / substring / extensible
simple     = attr filtertype value
filtertype = equal / approx / greater / less
equal      = "="
approx     = "~="
greater    = ">="
less       = "<="
extensible = attr [":dn"] [":" matchingrule] ":=" value
           / [":dn"] ":" matchingrule ":=" value
present    = attr "=*"
substring  = attr "=" [initial] any [final]
initial    = value
any        = "*" *(value "*")
final      = value
attr       = AttributeDescription（[1] の 4.1.5 項より）
```

matchingrule = MatchingRuleId（[1] の 4.1.9 項より）

value = AttributeValue（[1] の 4.1.6 項より）

attr、matchingrule および value の構成は、[1] の該当する項で説明されています。

値に次の文字を含める必要がある場合、

文字	ASCII 値
*	0x2a
(	0x28
)	0x29
\	0x5c
NUL	0x00

その文字は、バックスラッシュ '\' 文字（ASCII 0x5c）の後に、エンコードする文字の ASCII 値を表す 2 桁の 16 進数としてエンコードする必要があります。2 桁の 16 進数の大 / 小文字の区別は重要ではありません。

この簡単なエスケープ方法によって、フィルタ解析のあいまいさを排除でき、LDAP で表現できるフィルタをヌル文字で終了する文字列として表現できます。ここにリストされていない文字も、この方法を使用してエスケープできます（たとえば、出力しない文字）。

たとえば、「cn」属性の値にアスタリスク「*」が含まれているかどうかをチェックするフィルタは、次のように表現されます。

「(cn=*\2a*)」

前述の構文にある substring および present の定義では、「attr=*」構成を定義できますが、この構成はフィルタの存在を示す場合にのみ使用します。

5. 例

この項では、この表記規則を使用して記述された検索フィルタの例をいくつか示します。

(cn=Babs Jensen)

(!(cn=Tim Howes))

(&(objectClass=Person)(|(sn=Jensen)(cn=Babs J*)))

(o=univ*of*mich*)

次の例は、extensible での一致の使用方法を示しています。

(cn:1.2.3.4.5:=Fred Flintstone)

(sn:dn:2.4.6.8.10:=Barney Rubble)

(o:dn:=Ace Industry)

(:dn:2.4.6.8.10:=Dino)

2 番目の例は、「:dn」の表記規則の使用方法を示しています。この例は、一致規則「2.4.6.8.10」を使用して比較を行い、一致を評価するときにエントリの識別名の属性をエントリの一部とみなすことを示します。

3 番目の例は、等価の一致を示しています。ただし、比較を行うときに識別名のコンポーネントをエントリの一部とみなす必要があります。

4 番目の例は、指定の一致規則をサポートする属性に適用するフィルタを示しています（その属性のオフ以降）。識別名に含まれる一致規則をサポートする属性も考慮する必要があります。

次の例は、エスケープ方法を示しています。

(o=Parens R Us \28for all your parenthetical needs\29)

(cn=*\2A*)

(filename=C:\5cMyFile)

(bin=\00\00\00\04)

(sn=Lu\c4\8di\c4\87)

最初の例は、カッコ文字を表現するためのエスケープ方法を示しています。2 番目の例は、値に含まれるアスタリスク「*」を、サブストリング・インジケータとして解析されないように表現する方法を示しています。3 番目の例は、バックスラッシュ文字のエスケープ方法を示しています。

4 番目の例は、4 バイト値の 0x00000004 に対するフィルタ検索を示し、任意のデータ（NULL 文字を含む）を表現するためのエスケープ方法を示しています。

最後の例は、非 ASCII の様々な UTF-8 文字を表すためのエスケープ方法を示しています。

6. セキュリティに関する考察

この文章は、LDAP 検索フィルタの文字列表現について説明しています。表現自体にはセキュリティ上考慮する点はありませんが、LDAP 検索フィルタのセキュリティについては考慮する必要があります。この検索フィルタは、データを取得するエントリを選択するために、LDAP サーバーによって解析されます。LDAP サーバーは、維持しているデータを不正アクセスから保護する必要があります。

7. 参照資料

[1] Wahl, M., Howes, T. および S. Kille、『Lightweight Directory Access Protocol (v3)』、RFC 2251、1997 年 12 月

[2] Wahl, M., Coulbeck, A., Howes, T. および S. Kille、『Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions』、RFC

2252、1997 年 12 月

[3] ASN.1 エンコーディング規則の仕様 : 基本、標準および

高度なエンコーディング規則、ITU-T リコメンデーション X.690、1994 年

[4] Yergeau, F.、『UTF-8, a transformation format of Unicode and ISO

10646』、RFC 2044、1996 年 10 月

[5] Crocker, D.、『Standard for the Format of ARPA Internet Text

Messages』、STD 11、RFC 822、1982 年 8 月

8. 執筆者連絡先

Tim Howes
Netscape Communications Corp.
501 E. Middlefield Road
Mountain View, CA 94043
USA
電話番号 : +1 415 937-3419
電子メール : howes@netscape.com

9. 完全な著作権

E

アクセス制御ディレクティブ書式

この付録では、**アクセス制御情報項目**（ACI）の書式（構文）について説明します。次の項目について説明します。

- orclACI のスキーマ
- orclEntryLevelACI のスキーマ

orclACI のスキーマ

ユーザー属性 orclACI で定義されているアクセス制御ディレクティブのスキーマは、次のとおりです。

```
OrclACI:
{ object_identifier NAME 'orclACI' DESC 'Stores an inheritable ACI' EQUALITY
accessDirectiveMatch SYNTAX 'accessDirectiveDescription'  USAGE
'directoryOperation'}

accessDirectiveDescription has the following BNF:
<accessDirectiveDescription>
                  ::= access to <object> [by <subject> ( <accessList> )]+

<object> ::= [attr <EQ-OR-NEQ> ( * | (<attrList>) ) | entry] [filter=(<ldapFilter>)]

<subject> ::= <entity> [<BindMode>] [Added_object_constraint=(<ldapFilter>)]

<entity> ::= * | self | dn="<regex>" | dnAttr=(<dn_attribute>) | group="<dn>" |
guidattr=(<guid_attribute>) | groupattr=(<group_attribute>)

BindMode=(LDAP_authentication_choice)|LDAP_security_choice)
LDAP_authentication_choice::= proxy | simple | MD5Digest | PKCS12
LDAP_security_choice::= SSLNoAuth | SSLOneWay | SASL

<accessList> ::= <access> | <access>, <accessList>

<access> ::= none | compare | search | browse | proxy | read | selfwrite | write |
add | delete | nocompare | nosearch | nobrowse | noproxy |noread | noselfwrite |
nowrite | noadd | nodelete

<attrList> ::=  <attribute name> | <attribute name>,<attrList>

<EQ-OR-NEQ> ::=  = | !=

<regex> ::= <dn> | *,<dn_of_any_subtree_root>
```

注意： 前述の正規表現は、任意の式に合わせるためのものではありません。構文で許可されているのは、ワイルド・カードの後にカンマと有効な識別名が続く式のみです。*<dn_of_any_subtree_root>* で示されている識別名は、いくつかのサブツリーのルートを指定することを意味しています。

orclEntryLevelACI のスキーマ

ユーザー属性 orclEntryLevelACI で定義されているエントリ・レベルのアクセス制御ディレクティブのスキーマは、次のとおりです。

```
"orclEntryLevelACI":
{ object_identifier NAME 'orclEntryLevelACI' DESC 'Stores entry level ACL Directive'
EQUALITY accessDirectiveMatch SYNTAX 'orclEntryLevelACIDescription'
USAGE 'directoryOperation' }

<orclEntryLevelACIDescription>
::= access to <object> [by <subject> ( <accessList> )]+
```

F

データベース・コピー・プロシージャを使用したディレクトリ・ノードの追加

この付録では、データベース・コピー・プロシージャ（**コールド・バックアップ**とも呼ばれます）を使用して、既存のレプリケート・システムに新しいノードを追加する方法について説明します。

注意： このプロシージャには、Oracle のデータ・ファイルをコピーする処理が含まれているため、パフォーマンスは基礎となるネットワークに依存します。基礎となるネットワークが弱い場合は、第 25 章「Oracle ディレクトリ・レプリケーションの管理」に記載されている方法を実施するか、またはテープやディスクなどのメディアに、圧縮した Oracle データ・ファイルを物理的にコピーする方法をお薦めします。ネットワークに関する詳細は、ローカル・システムの管理者またはネットワーク管理者に相談してください。

このプロシージャは、Oracle データベースをよく理解している人のみ実施してください。

この章では、次の項目について説明します。

前提事項

このマニュアルは、Optimal Flexible Architecture（OFA）に従って UNIX ディレクトリが作成されていることを前提としています。Optimal Flexible Architecture（OFA）は、効率的で信頼性のある Oracle データベースを構築するための一連の構成ガイドラインです。

> **関連項目：** OFA の詳細は、使用しているオペレーティング・システム用の Oracle インストレーション・ガイドを参照してください。

スポンサ・ディレクトリ・サイトの環境

スポンサ・サイトの環境を設定します。この章で使用される例では、ホスト名は rst-sun です。

```
Hostname    = rst-sun
ORACLE_BASE = /private/oracle/app/oracle
ORACLE_HOME = /private/oracle/app/oracle/product/8.1.6
ORACLE_SID  = LDAP
LD_LIBRARY_PATH = $ORACLE_HOME/lib
NLS_LANG    = AMERICAN_AMERICA.AL32UTF8
datafile location = /private/oracle/oradata/LDAP
Dump destination =  /private1/oracle/app/oracle/admin/LDAP/pfile,
                    /private1/oracle/app/oracle/admin/LDAP/bdump,
                    /private1/oracle/app/oracle/admin/LDAP/cdump,
                    /private1/oracle/app/oracle/admin/LDAP/udump,
                    /private1/oracle/app/oracle/admin/LDAP/create
```

新規ディレクトリ・サイトの環境

新規ディレクトリ・サイトの環境を設定します。この章で使用される例では、新規サイトは、dsm-sun というノード上にあります。

```
Hostname = dsm-sun
ORACLE_BASE = /private1/oracle/app/oracle
ORACLE_HOME = /private1/oracle/app/oracle/product/8.1.6
ORACLE_SID  = NLDAP
LD_LIBRARY_PATH = $ORACLE_HOME/lib
NLS_LANG = AMERICAN_AMERICA.UTF8
   datafile location = /private1/oracle/oradata/NLDAP
   Dump destination =  /private1/oracle/app/oracle/admin/NLDAP/pfile,
                       /private1/oracle/app/oracle/admin/NLDAP/bdump,
                       /private1/oracle/app/oracle/admin/NLDAP/cdump,
                       /private1/oracle/app/oracle/admin/NLDAP/udump,
                       /private1/oracle/app/oracle/admin/NLDAP/create
```

注意： Oracle データベースまたは Oracle ディレクトリのインストール後、Database Configuration Assistant を使用して、データ・ファイルのディレクトリを作成します。OFA の定義に従って、様々な UNIX パーティション下の新規ノードに、新規ディレクトリを作成してください。

スポンサ・ノードで実行されるタスク

スポンサ・ノードで次の手順を実行します。

1. コマンドライン・プロンプトで、SQL*Plus を実行します。

```
$ sqlplus /nolog
SQL> connect /as sysdba
SQL> ALTER DATABASE BACKUP CONTROLFILE TO TRACE;
```

このコマンドは、ユーザー・ダンプ出力先ディレクトリ（/private1/oracle/app/oracle/admin/LDAP/udump）にトレース・ファイルを作成します。

ファイルは次の書式で作成されます。

$ORACLE_SID_*ora_processid*.trc

たとえば、次のように入力します。

ldap_ora_4765.trc

2. LDAP サーバーとレプリケーション・サーバーおよび OID モニター・プロセスを停止します。OID モニター・プロセスを停止する前に、LDAP サーバーとレプリケーション・サーバーが停止していることを確認してください。

```
$ oidctl connect=connect_string server=oidrepld instance=instance_number stop
$ oidctl connect=connect_string server=oidldapd instance=instance_number stop
$ oidmon connect=connect_string stop
```

これらのコマンドで、*connect_string* はそのノードの tnsnames.ora ファイル内に記述されているネット・サービス名です。

3. その他のノードで、LDAP レプリケーション・サーバーのみ停止します。

```
$ oidctl connect=connect_string server=oidrepld instance=instance_number stop
```

スポンサ・ノードを除くすべてのノードで、この手順を繰り返します。対応するノードの適切なネット・サービス名を指定してください。

4. **マスター定義サイト**で次のスクリプトを実行して、**Oracle9i Advanced Replication** を静止させます。

```
ldaprepl.sh -quiesce
```

プロンプトが表示された場合は、Oracle のグローバル名と MDS のレプリケーション管理パスワードを入力します。

注意： Windows オペレーティング・システムでシェル・スクリプト・ツールを実行するには、次のいずれかの UNIX エミュレーション・ユーティリティが必要です。

- Cygwin 1.3.2.2-1 以上
  サイト：`http://sources.redhat.com`
- MKS Toolkit 6.1
  サイト：`http://www.datafocus.com/`

注意： この手順は、マスター定義サイトでのみ実施できます。

この時点で、他のノードは LDAP 編集のみ使用可能で、レプリケーションは行われません。

5. 環境の静止後、スポンサ・ノードでのみデータベースと Oracle Net Services リスナーを停止します。

```
$ lsnrctl [listener_name] stop  (By default listener name is LISTENER)
$ sqlplus /nolog
SQL> connect /as sysdba
SQL> shutdown normal
SQL> exit
```

6. 手順 1 で作成されたトレース・ファイルを、同じディレクトリ内の新規ファイル `newdb.sql` にコピーします。

```
$ cd $ORACLE_BASE/admin/LDAP/udump
$ cp ldap_ora_4765.trc newdb.sql
```

7. テキスト・エディタを使用して `newdb.sql` を編集し、START NOMOUNT までの行を削除します。

```
CREATE CONTROLFILE REUSE SET DATABASE database_name RESETLOG
```

8. データベースやログ・ファイルの UNIX ディレクトリの位置を、新規ノードのディレクトリを指すように変更します。次のサンプル・ファイル newdb.sql を参考にしてください。

```
Begin newdb.sql
CREATE CONTROLFILE REUSE SET DATABASE "LDAP" RESETLOGS
MAXLOGFILES 16
MAXLOGMEMBERS 2
MAXDATAFILES 255
MAXINSTANCES 1
MAXLOGHISTORY 100
LOGFILE
GROUP 1 '/private2/oracle/oradata/NLDAP1/log1_NLDAP.dbf'  SIZE 1M,
GROUP 2 '/private2/oracle/oradata/NLDAP1/log2_NLDAP.dbf'  SIZE 1M
DATAFILE
'/private2/oracle/oradata/NLDAP1/sys0_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/rbs1_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/attrs1_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/dncat1_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/cncat1_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/objcl1_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/cats1_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/default1_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/temp1_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/iattrs1_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/idncat1_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/icncat1_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/iobjcl1_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/icats1_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/temp2_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/cats2_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/attrs2_NLDAP.dbf'
;
 End newdb.sql
```

9. $ORACLE_HOME/dbs の initLDAP.ora ファイルと configLDAP.ora ファイルを、それぞれ initNLDAP.ora と configNLDAP.ora にコピーします。

```
$cd $ORACLE_HOME/dbs
$cp initLDAP.ora initNLDAP.ora
$cp configLDAP.ora configNLDAP.ora
```

10. コピーしたファイル（initNLDAP.ora）を編集し、パラメータ JOB_QUEUE_PROCESS をコメント化します。次のパラメータを変更します。

```
db_name = LDAP  （パラメータがファイル initNLDAP.ora にない場合はファイル
configNLDAP.ora を変更）
ifile = UNIX_directory_location_of_the_new_config_file/ configNLDAP.ora
```

11. コピーしたファイル configNLDAP.ora を編集し、次のパラメータを変更します。

```
cdump =  UNIX_directory_location_of_the_new_node
udump  = UNIX_directory_location_of_the_new_node
bdump  = UNIX_directory_location_of_the_new_node
control_files = UNIX_directory_location_of_the_new_node
```

12. tnsnames.ora ファイルを編集して、新規ノードに関連する情報を記述します。次のサンプル・ファイルを参考にしてください。

```
Begin tnsnames.ora

ldap1.world =
   (description=
      (address=(protocol=tcp)(host=rst-sun)(port=1521))
      (connect_data=(sid=LDAP))
   )
ldap2.world =
   (description=
      (address=(protocol=tcp)(host=eas-sun10)(port=1521))
      (connect_data=(sid=LDAP))
   )
ldap3.world =
   (description=
      (address=(protocol=tcp)(host=dsm-sun)(port=1521))
      (connect_data=(sid=NLDAP))
   )

End tnsnames.ora
```

13. ファイル listener.ora を list.bak にコピーします。コピーしたファイル list.bak を編集して、新規ノードに関連する情報を記述します。次のサンプル・ファイルを参考にしてください。

```
Begin listener.ora

# The KEY value for the IPC protocol may be anything, and
# is not related to either the TCP hostname or database SID.

LISTENER =
  (ADDRESS_LIST =
```

```
        (ADDRESS=(PROTOCOL= IPC)(KEY= LDAP))
        (ADDRESS=(PROTOCOL= IPC)(KEY= PNPKEY))
        (ADDRESS=(PROTOCOL= TCP)(Host= dsm-sun)(Port= 1521))
  )
SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (GLOBAL_DBNAME= dsm-sun.us.oracle.com)
      (ORACLE_HOME= /private1/oracle/app/oracle/product/8.1.6)
      (SID_NAME = NLDAP)
    )
    (SID_DESC =
      (SID_NAME = extproc)
      (ORACLE_HOME = /private1/oracle/app/oracle/product/8.1.6)
      (PROGRAM = extproc)
    )
  )
STARTUP_WAIT_TIME_LISTENER = 0
CONNECT_TIMEOUT_LISTENER = 10
TRACE_LEVEL_LISTENER = OFF

End listener.ora
```

tnsnames.ora ファイルと listener.ora ファイルは、$ORACLE_HOME/network/admin または /var/opt/oracle、あるいは環境変数 TNS_ADMIN が指し示すディレクトリ内にあります。

14. 更新した tnsnames.ora ファイルをすべてのノードにコピーします。各ノードの現行の tnsnames.ora の位置にコピーするように注意してください。tnsnames.ora ファイルは、FTP を使用して他のノードにコピーできます。ファイルは、必ず ASCII モードで転送してください。

tnsnames.ora ファイルを新規ノードにコピーする前に、新規ノードに Oracle データベース・ソフトウェアをインストールします。また、listener.ora ファイルのかわりの list.bak ファイルと sqlnet.ora ファイルを、スポンサ・ノードから新規ノードにコピーします。

15. すべてのデータ・ファイルのアーカイブを作成し、アーカイブしたファイルを圧縮します。たとえば、次のように入力します。

```
$ >oradb.tar
```

このコマンドは、ディレクトリ内に空のファイルを作成します。アーカイブが作成されるパーティションに、十分な領域があることを確認してください。

```
$ find / -name *.dbf -print -exec tar rvf  absolute_path_of_the_directory_which_
contains_oradb.tar {} ¥;
```

次のコマンドは、拡張子が .dbf のすべてのファイルを、ルート・ディレクトリから検索します。ノードにインストールされているデータベース・サーバーのインスタンスが 1 つのみで、データ・ファイルが *.dbf 拡張子で終わっていることを前提としています。

```
$ find / -name *.log -print -exec tar rvf absolute_path_of_the_directory_which_
contains_oradb.tar
$ compress oradb.tar
```

このプロシージャは、ファイルのバックアップ方式を示す 1 つの例です。Oracle データ・ファイルは、この方法で絶対パス内でバックアップされます。データ・ファイルをリストアするときに、柔軟に対応できるように、現行のディレクトリからファイルをバックアップすることをお薦めします。データベースをバックアップする前に、システム管理者と相談してください。

新規ノードで実行されるタスク

新規ノードで次の手順を実行します。

1. 新規ノード（dsm-sun）にログインします。
2. すべてのデータベース・ノードで、新規インスタンス用に oratab ファイルを適切に編集します。構文はサンプル・ファイルを参照してください。

   ```
   Begin oratab

   NLDAP:/private1/oracle/app/oracle/product/8.1.6:N
   *:/private1/oracle/app/oracle/product/8.1.6:N

   End oratab
   ```

3. 新規ディレクトリ・サイトに環境変数が設定されていることを確認します。

4. Oracle データベースと Oracle ディレクトリ・サーバーをインストールします。Oracle データベースと Oracle ディレクトリ・サーバーのソフトウェアのみのインストールを実行します。データベース・ファイルが新しいマシンにコピーされる前であれば、いつでも新規ノードで Oracle データベースと Oracle ディレクトリ・サーバーのソフトウェアのインストールを実行できます。データベースとディレクトリ・サーバーに、インストール後のアクティビティ（root.sh）を実行してください。

   注意： Windows オペレーティング・システムでシェル・スクリプト・ツールを実行するには、次のいずれかの UNIX エミュレーション・ユーティリティが必要です。

   - Cygwin 1.3.2.2-1 以上
     サイト：http://sources.redhat.com
   - MKS Toolkit 6.1
     サイト：http://www.datafocus.com/

   関連項目： Oracle9*i* のインストール・マニュアルを参照してください。

   新規ノードに Oracle データベースと Oracle ディレクトリ・サーバーのインストールがすでに実行されている場合は、手順 5 に進んでください。

5. initNLDAP.ora ファイルと configNLDAP.ora ファイルをスポンサ・ノード（rst-sun）から UNIX ディレクトリ $ORACLE_BASE/ADMIN/NLDAP/PFILE の新規ノードにコピーします。新規マシンへのファイルのコピーには、FTP などのツールを使用します。転送モードが ASCII であることを確認してください。

6. $ORACLE_HOME/DBS から $ORACLE_BASE/ADMIN/NLDAP/PFILE へのシンボリック・リンクを作成します。

```
$ ln -s $ORACLE_BASE/admin/NLDAP/pfile/initNLDAP.ora
       $ORACLE_HOME/dbs/initNLDAP.ora
$ ln -s $ORACLE_BASE/admin/NLDAP/pfile/configNLDAP.ora
       $ORACLE_HOME/dbs/configNLDAP.ora
```

7. スポンサ・ノードの手順で作成したアーカイブ・ファイルを、FTP などのツールを使用してコピーします（このファイルは、F-7 ページの手順 15 で作成しています）。転送モードをバイナリに設定します。

```
ftp> open rst-sun
Connected to rst-sun.us.oracle.com.
220 rst-sun FTP server (UNIX(r) System V Release 4.0) ready.
Name (rst-sun:oracle):
331 Password required for oracle.
Password:
```

```
230 User oracle logged in.
ftp> cd /private1/oracle/oradata/LDAP
250 CWD command successful.
ftp> binary
200 Type set to I.
ftp> mget oradb.tar.Z
```

データ・ファイルが非常に大きく（数 GB または数 TB）、ネットワーク帯域幅が狭い場合は、スポンサ・ノードから新規ノードにコピーするとき、テープやディスクなどのメディアに、圧縮したファイルを物理的にコピーする方法をお薦めします。

8. スポンサ・ノードの設定の手順 6 で作成した newdb.sql ファイルを、バックグラウンドのユーザー・ダンプ出力先ディレクトリにコピーします。newdb.sql ファイルのみ ASCII モードで転送する必要があります。たとえば、次のように入力します。

```
 $ cd /private1/oracle/app/oracle/admin/NLDAP/udump
                （つまり、$ORACLE_BASE/admin/SID/udump）
$ ftp
ftp> open rst-sun
ftp> cd /private1/oracle/app/oracle/admin/LDAP/udump
ftp> mget newdb.sql
```

9. UNIX シェル・プロンプトで、次のコマンドを実行します。

```
$ sqlplus /nolog
SQL> connect /as sysdba
SQL> startup nomount
SQL> @newdb.sql
SQL> shutdown normal
SQL> startup （起動する前に、パラメータ job_queue_process のコメントを解除する）
SQL>exit
$ lsnrctl start
```

10. スポンサ・ノードにログインして、スポンサ・ノード（例 : rst-sun）でデータベースとリスナーを起動します。

```
$ telnet rst-sun
$ sqlplus /nolog
SQL> connect /as sysdba
SQL> startup
SQL> exit
$ lsnrctl start （デフォルトのリスナー名は LISTENER）
$ exit
```

11. スポンサ・ノードがマスター・サイトの場合は、手順 12 に進んでください。

新規ノードが MDS のバックアップ・データベース・コピーを使用して作成されている場合は、マスター定義カタログを削除して、基礎となる Oracle9*i* Advanced Replication カタログを作成する必要があります。新規ノードで Oracle9*i* Advanced Replication カタログから MDS の定義を削除して Oracle9*i* Advanced Replication カタログを追加するには、次のスクリプトを実行します。

```
$ cd $ORACLE_HOME/ldap/admin
$ sqlplus repadmin/repadmin
SQL> @ldapdropmds.sql
SQL> @ldapcreindex.sql
```

要求された場合は、新規ノードのグローバル名を指定してください。

12. Oracle9*i* Advanced Replication を構成するには、シェル・プロンプトで次のコマンドを実行します。

```
$ ldaprepl.sh -addnode
```

注意： Windows オペレーティング・システムでシェル・スクリプト・ツールを実行するには、次のいずれかの UNIX エミュレーション・ユーティリティが必要です。

- Cygwin 1.3.2.2-1 以上
  サイト : `http://sources.redhat.com`
- MKS Toolkit 6.1
  サイト : `http://www.datafocus.com/`

---

13. LDAP レプリケーション承諾を更新して、新規ノードを組み込みます。

LDIF ファイルのサンプルは次のとおりです。

```
dn: orclagreementid=000001, cn=orclreplagreements
changetype: modify
add: orcldirreplgroupdsas
orcldirreplgroupdsas: dsm-sun
```

14. すべてのノード（新規ノードとスポンサ・ノードを含む）で、LDAP レプリケーション・サーバーを起動します。

検証プロセス

SQL*Plus を使用して Oracle データベースにログインし、ユーザー名 ODS を指定し、要求に従ってパスワード ods を指定します。

すべてのノードで ods_chg_stat 表をチェックし、同一の正しい行が含まれているかどうかをチェックします。ods_chg_stat 表には、（ノード数）×（ノード数）行が含まれている必要があります。たとえば、Oracle9*i* Advanced Replication ベースのレプリケーションのノードが 2 つあり、3 番目のノードを追加した場合、ods_chg_stat の行は各ノードで 9（3 × 3）行です。各行の内容を次の表で示します。

サプライヤ	コンシューマ	変更番号
ノード 1	ノード 2	番号 1
ノード 1	ノード 3	番号 2
ノード 1	ノード 1	番号 3
ノード 2	ノード 1	番号 4
ノード 2	ノード 2	番号 5
ノード 2	ノード 2	番号 6
ノード 3	ノード 1	0
ノード 3	ノード 2	0
ノード 3	ノード 3	0

コンシューマ名とサプライヤ名が同じ行には、サプライヤ側でアウトバウンド変更ログの処理スレッドが処理した最終変更が含まれています。サプライヤ名とコンシューマ名が異なる行には、サプライヤからそのコンシューマに対して、すでに処理された最終変更番号が含まれています。

ノード 3 は新規ノードであるため、ノード 3 による変更はまだありません。したがって、サプライヤとしてのノード 3 の変更番号は 0（ゼロ）です。

すべてのノードの行が同一になるまでに時間的な遅延が発生することがありますが、この遅延は 2 ～ 3 分ほどです。

G

ディレクトリにおけるグローバリゼーション・サポート

Oracle Internet Directory ではグローバリゼーション・サポートを使用して、システム固有の言語でデータの格納、処理および取得を行います。グローバリゼーション・サポートは、Oracle Internet Directory のユーティリティとエラー・メッセージを、システム固有の言語とロケールに自動的に調整します。

この付録では、Oracle Internet Directory で使用されるグローバリゼーション・サポートと、Oracle Internet Directory 環境における様々なコンポーネントとツールに必要な環境変数 NLS_LANG について説明します。

> **関連項目：** グローバリゼーション・サポートを構成する前に、2-12 ページの「グローバリゼーション・サポート」を参照してください。

この章では、次の項目について説明します。

環境変数 NLS_LANG

NLS_LANG パラメータには、language、territory および charset の 3 つのコンポーネントがあります。形式は次のとおりです。

```
NLS_LANG = language_territory.charset
```

各コンポーネントは、グローバリゼーション・サポート機能のサブセットの作用を制御します。

コンポーネント	説明
language	Oracle メッセージ、曜日および月の名前に使用する言語などの規則を指定します。サポートしているそれぞれの言語には、American English（米語）、French（フランス語）または German（ドイツ語）などの固有の名前があります。言語引数によって、地域およびキャラクタ・セットの引数のデフォルト値が指定され、その結果、territory または charset のいずれか（あるいはその両方）を省略できます。 language を指定しない場合、デフォルトでは American English（米語）になります。 **関連項目：**言語の完全なリストは、『Oracle グローバリゼーション・ガイド』を参照してください。
territory	デフォルトのカレンダ、照合、日付、通貨単位および数値書式などの規則を指定します。サポートしているそれぞれの地域には、America（アメリカ）、France（フランス）または Canada（カナダ）などの固有の名前があります。 territory を指定しない場合、デフォルト値では America になります。 **関連項目：**地域の完全なリストは、『Oracle グローバリゼーション・ガイド』を参照してください。
charset	クライアント・アプリケーションが使用するキャラクタ・セット（通常はユーザー端末で使用するキャラクタ・セット）を指定します。サポートしているそれぞれのキャラクタ・セットには、US7ASCII、WE8ISO8859P1、WE8DEC、WE8EBCDIC500、JA16EUC などの一意の頭字語があります。それぞれの言語には、デフォルトのキャラクタ・セットが対応付けられています。システムで使用可能な言語のデフォルト値については、オペレーティング・システムのインストール・ガイドまたは管理者ガイドを参照してください。 **関連項目：**キャラクタ・セットの完全なリストは、『Oracle グローバリゼーション・ガイド』を参照してください。

注意： NLS_LANG 定義のコンポーネントは、すべてオプションです。特に指定しない項目はデフォルト値になります。

territory または charset を指定する場合、先行デリミタを入力する必要があります。先行デリミタは、territory の場合はアンダースコア（_）で、charset の場合はピリオド（.）です。先行デリミタがないと、値全体が言語名として解析されます。

コマンドラインで、NLS_LANG を環境変数として設定できます。次は、NLS_LANG の適切な値の例です。

- AMERICAN_AMERICA.AL32UTF8
- JAPANESE_JAPAN.AL32UTF8

非 UTF-8 データベースの使用方法

Oracle ディレクトリ・サーバーとデータベース・ツールは、非 UTF-8、つまり UTF8 または AL31UTF8 でないデータベース上で実行できますが、クライアント・キャラクタ・セットにある文字がすべて、文字コードが同じかどうかにかかわらず、データベース・キャラクタ・セットに含まれているかどうかを確認してください。キャラクタ・セットが異なると、ldapadd、ldapdelete、ldapmodify または ldapmodifydn 操作中にデータが消失する可能性があります。たとえば、シングルバイト文字のみを使用する基礎となるデータベース上で、マルチバイト・キャラクタ・セットを使用して ldapadd 操作を実行すると仮定します。入力するバイトのすべてがデータベースで受け入れられるわけではないため、データが消失します。

LDIF ファイルでのグローバリゼーション・サポートの使用方法

関連項目： A-2 ページの「LDAP Data Interchange Format（LDIF）の構文」

属性の型は必ず ASCII 文字列で、マルチバイト文字は使用できません。Oracle Internet Directory は、属性の型名にマルチバイト文字をサポートしていません。ただし、Oracle Internet Directory は、属性の値にマルチバイト文字の使用をサポートしています。たとえば、簡体字中国語（.ZHS16GBK）のキャラクタ・セットのマルチバイト文字を使用できます。

属性値は、異なる方法でエンコードできます。この方法でエンコードされた値は、Oracle Internet Directory のツールで正しく解釈できます。次に例を 2 つあげます。

- ASCII 文字列のみを含む LDIF ファイル
- UTF-8 エンコーディング文字列を含む LDIF ファイル

ASCII 文字列のみを含む LDIF ファイル

この例では、属性値の文字列も ASCII 文字列です。

すべてのツールがデフォルトで UTF-8 キャラクタ・セットを使用しており、ASCII は UTF-8 の正しいサブセットであるため、いずれのツールもこのファイルを解釈できます。キーボードで ASCII 文字列の値をそのまま入力する場合も同様です。

UTF-8 エンコーディング文字列を含む LDIF ファイル

この例では、属性値の文字列も UTF-8 文字列です。

デフォルトでは、すべてのツールで UTF8 キャラクタ・セット（Oracle キャラクタ・セット名は AL32UTF8）が使用されるため、これらのファイルはどのツールでも解析できます。キーボードで UTF-8 文字列の値を入力する場合も同様です。

このようなファイルでは、一部の文字がマルチバイトの可能性があります。マルチバイト・キャラクタ文字列は、属性値として LDIF ファイルで使用したり、キーボードで入力できます。それらの文字列は、ネイティブ・キャラクタ・セットまたは UTF-8 でエンコードできます。さらに、ネイティブ文字列または UTF-8 文字列の BASE64 エンコーディング形式も可能です。

次のケースを説明します。

- ケース 1: ネイティブ文字列（非 UTF-8）
- ケース 2: UTF-8 文字列
- ケース 3: BASE64 でエンコードされた UTF-8 文字列
- ケース 4: BASE64 でエンコードされたネイティブ文字列

ディレクトリ・サーバーは UTF-8 エンコーディング文字列のみを理解し、UTF-8 エンコーディング文字列を受信することを想定しているため、ケース 1、3 および 4 は、LDAP サーバーに送信する前に、UTF-8 文字列に変換しておく必要があります。

ケース 1: ネイティブ文字列（非 UTF-8）

コマンドライン・ツール、ldifwrite および bulkmodify で、`-E` 引数を使用します。bulkload および bulkdelete ツールでは、`-encode` 引数を使用します。

この例では、簡体字中国語のネイティブ文字列を UTF-8 に変換しています。ベース識別名は、簡体字中国語で記述できます。

```
ldapsearch -h my_host -p 389 -E ".ZHS16GBK" -b base_DN  -s base  "objectclass=*"
```

ケース 2: UTF-8 文字列

変換は不要です。

ケース 3: BASE64 でエンコードされた UTF-8 文字列

コマンドライン・ツール ldifwrite および bulkmodify で -E 引数を使用したり、bulkload や bulkdelete で -encode 引数を使用する必要はありません。Oracle Internet Directory のツールは、BASE64 でエンコードされた UTF-8 文字列を UTF-8 文字列に自動的にデコードします。

ケース 4: BASE64 でエンコードされたネイティブ文字列

コマンドライン・ツール、ldifwrite および bulkmodify で、-E 引数を使用します。bulkload および bulkdelete ツールでは、-encode 引数を使用します。

Oracle Internet Directory のツールは、BASE64 でエンコードされたネイティブ文字列を、単純なネイティブ文字列に自動的にデコードします。その後、ネイティブ文字列は対応する UTF-8 文字列に変換されます。

注意： 1 つの入力ファイルで使用できる言語セットは 1 つのみです。

コマンドライン・ツールでのグローバリゼーション・サポートの使用方法

Oracle Internet Directory のコマンドライン・ツールは、キーボード入力または LDIF ファイル入力を次の方法で読み取ります。

- ASCII 文字のみ
- 非 ASCII 入力（ネイティブ言語キャラクタ・セット）
- UTF-8 またはネイティブ文字列の BASE64 でエンコードされた値（LDIF ファイル入力のみ）

LDIF ファイルまたはキーボードからの入力として使用されているキャラクタ・セットが UTF-8 以外の場合、コマンドライン・ツールは、LDAP サーバーに送信する前に、その入力を UTF-8 形式に変換する必要があります。

コマンドライン・ツールで入力を UTF-8 に変換するには、各ツールの使用時に -E 引数を指定します。

次の項目について説明します。

- 各ツールを使用するときの -E 引数の指定
- 例 : コマンドライン・ツールでの -E 引数の使用方法

各ツールを使用するときの -E 引数の指定

-E 引数で指定しないかぎり、クライアント・ツールでは常にキャラクタ・セットが UTF-8（Oracle キャラクタ・セット名は AL32UTF8）であるとみなされます。-E 引数が指定されていると、BASE64 でエンコードされた値はデコードされ、次にデコードされたバッファが UTF-8 に変換されます。たとえば、-E ".ZHS16GBK" と指定すると、デコードされたバッファは、LDAP サーバーに送信される前に、簡体字中国語から UTF-8 に変換されます。

-E 引数を指定すると、-E 引数で指定したキャラクタ・セット（-E ".*character_set*"）が UTF-8 キャラクタ・セットに正しく変換されます。

コマンドライン・ツールは、-E 引数を使用して、-E 引数に指定されたキャラクタ・セットで入力を処理します。出力は、環境変数 NLS_LANG で指定されたキャラクタ・セットで表示します。

たとえば、簡体字中国語のキャラクタ・セット（.ZHS16GBK）でエンコードされた LDIF ファイルからのエントリを ldapadd を使用して追加するには、次のように入力します。

```
ldapadd -h myhost -p 389 -E ".ZHS16GBK" -f my_ldif_file
```

この例では、LDAP サーバーに送信される前に、文字が ldapadd ツールによって ".ZHS16GBK"（簡体字中国語のキャラクタ・セット）から ".AL32UTF8"（UTF-8 キャラクタ・セット）に変換されます。

例 : コマンドライン・ツールでの -E 引数の使用方法

次の表は、-E 引数を各コマンドライン・ツールで正しく使用する方法の補足例を示したものです。各例のコマンドは、値 ".ZHS16GBK" で指定されている簡体字中国語から UTF-8 にデータを変換します。たとえば、各コマンドの -D オプションと -w オプションの値が簡体字中国語で記述されます。-E 引数を指定すると、これらの値が UTF-8 に変換されます。

次の表の例には、.ZHS16GBK キャラクタ・セットに属している実際のキャラクタは含まれていないことに注意してください。したがって、これらの例は -E 引数の指定なしで動作します。ただし、引数の値に .ZHS16GBK キャラクタ・セット内の実際のキャラクタが含まれる場合は、-E 引数を使用する必要があります。

> **関連項目：** 各コマンドライン・ツールの構文と使用方法は、付録 A「LDIF およびコマンドライン・ツールの構文」を参照してください。

クライアント環境における NLS_LANG の設定

ツール	例
ldapbind	`ldapbind -h my_host -p 389 -E ".ZHS16GBK" -D "o=acme,c=us" -w my_password`
ldapsearch	`ldapsearch -h my_host -p 389 -E ".ZHS16GBK" -D "o=acme,c=us" -w my_password`
ldapadd	`ldapadd -h my_host -p 389 -E ".ZHS16GBK" -D "o=acme,c=us" -w my_password`
ldapaddmt	`ldapaddmt -h my_host -p 389 -E ".ZHS16GBK" -D "o=acme,c=us" -w my_password`
ldapmodify	`ldapmodify -h my_host -p 389 -E ".ZHS16GBK" -D "o=acme,c=us" -w my_password`
ldapmodifymt	`ldapmodifymt -h my_host -p 389 -E ".ZHS16GBK" -D "o=acme,c=us" -w my_password`
ldapdelete	`ldapdelete -h my_host -p 389 -E ".ZHS16GBK" -D "o=acme,c=us" -w my_password`
ldapcompare	`ldapcompare -h my_host -p 389 -E ".ZHS16GBK" -D "o=acme,c=us" -w my_password -b "ou=Construction,ou=Manufacturing,o=acme,c=us" -a title -v manager`
ldapmoddn	`ldapmoddn -h my_host -p 389 -E ".ZHS16GBK" -D "o=acme,c=us" -w my_password -b "cn=Franklin Badlwins,ou=Construction,ou=Manufacturing,c=us,o=acme" -N "ou=Contracting,ou=Manufacturing,o=acme,c=us" -r`

クライアントで必要な出力が UTF-8 の場合は、環境変数 NLS_LANG を設定する必要はありません。この場合、環境変数 NLS_LANG はデフォルトで .AL32UTF8 に設定され、クライアントからサーバーへの入力の過程およびサーバーからクライアントへの出力の過程で、キャラクタ・セット変換の必要はありません。

クライアントで必要な出力が UTF-8 以外の場合は、環境変数 NLS_LANG を設定する必要があります。この設定によって、UTF-8 キャラクタ・セットからクライアントが要求したキャラクタ・セットに正しく変換されます。

たとえば、環境変数 NLS_LANG が簡体字中国語のキャラクタ・セットに設定されている場合、コマンドライン・ツールは、そのキャラクタ・セットで出力を表示します。環境変数が設定されていない場合、出力にはデフォルトで UTF-8 キャラクタ・セットが使用されます。

注意： Windows を使用している場合、サーバーの起動後にコマンドライン・ツールを使用するには、MS-DOS ウィンドウで NLS_LANG を再設定する必要があります。MS-DOS セッションのコード・ページに一致するキャラクタ・セットを設定してください。UTF-8 は使用できません。MS-DOS セッションでコマンドライン・ツールに使用するキャラクタ・セットの詳細は、『Oracle Database 10*g* for Windows インストレーション・ガイド』を参照してください。

Oracle Internet Directory とともに、事前にインストールされた Oracle9*i* リリース 2（9.2）のデータベースを使用している場合、データベース・キャラクタ・セットも UTF-8 に設定する必要があります。詳細は、『Oracle グローバリゼーション・ガイド』および『Oracle Database 10*g* for Windows インストレーション・ガイド』を参照してください。

レジストリの NLS_LANG パラメータの値を変更しないように注意してください。

バルク・ツールでのグローバリゼーション・サポートの使用方法

Oracle Internet Directory は、LDIF ファイルのテキスト・データの読取り / 書込みを、LDAP で指定されている UTF-8 エンコーディングで常に行います。

この項では、次の各バルク・ツールに使用する引数の例を紹介します。

- bulkload でのグローバリゼーション・サポートの使用方法
- ldifwrite でのグローバリゼーション・サポートの使用方法
- bulkdelete でのグローバリゼーション・サポートの使用方法
- bulkmodify でのグローバリゼーション・サポートの使用方法

関連項目： 各バルク・ツールの引数のリストは、「バルク操作コマンドライン・ツールの構文」を参照してください。

bulkload でのグローバリゼーション・サポートの使用方法

コマンドに引数 `-encode "character_set"` を追加します。この入力の LDIF ファイルは `"character_set"` でエンコードされています。

たとえば、次のように入力します。

```
bulkload.sh -connect connect_string -encode ".ZHS16GBK" my_ldif_file
```

注意： Windows オペレーティング・システムでシェル・スクリプト・ツールを実行するには、次のいずれかの UNIX エミュレーション・ユーティリティが必要です。

- Cygwin 1.3.2.2-1 以上
  サイト : `http://sources.redhat.com`
- MKS Toolkit 6.1
  サイト : `http://www.datafocus.com/`

ldifwrite でのグローバリゼーション・サポートの使用方法

ldifwrite ユーティリティは常に、マルチバイト文字列に対して BASE64 でエンコードされた値を書き出します。

BASE64 エンコーディングは、ディレクトリ・サーバーに格納されている UTF-8 文字列または ldifwrite の実行時に環境変数 NLS_LANG の設定で指定されたネイティブ文字列にも使用できます。

たとえば、次のように入力します。

```
ldifwrite -c connect_string -b baseDN -f output_file
```

環境変数 NLS_LANG が未設定の場合または *language_territory*.AL32UTF8 に設定されている場合、この例では、出力の LDIF ファイルにマルチバイト文字の BASE64 でエンコードされた UTF-8 文字列が含まれます。

この LDIF ファイルを ldapaddmt でディレクトリに再ロードするには、次の構文を使用します。

```
ldapaddmt -h my_host -p port_number -f output_file
```

この場合、デコードされた BASE64 文字列はすでに UTF-8 でエンコードされており、サーバーに送信できる状態であるため、-E 引数は不要です。

環境変数 NLS_LANG が UTF-8 以外のキャラクタ・セット（たとえば、".ZHS16GBK"）に設定されている場合は、出力の LDIF ファイルには、簡体字中国語（.ZHS16GBK）文字列の BASE64 でエンコードされた値が含まれます。

ldapaddmt を使用してこの LDIF ファイルをディレクトリに再ロードするには、次の構文を使用します。

```
ldapaddmt -h host -p port -E ".ZHS16GBK" -f my_input_file.LDIF
```

この場合、デコードされた BASE64 文字列は簡体字中国語であり、サーバーに送信する前に UTF-8 文字列に変換する必要があるため、-E 引数が必要です。

bulkdelete でのグローバリゼーション・サポートの使用方法

引数 -encode ".*character_set*" をコマンドに追加します。

たとえば、次のように入力します。

```
bulkdelete.sh -connect connect_string -encode ".ZHS16GBK" -base
"ou=manufacturing,o=acme,c=us"
```

この例では、-base オプションの値に、ZHS16GBK ネイティブ・キャラクタ・セット（簡体字中国語）を使用できます。

注意： Windows オペレーティング・システムでシェル・スクリプト・ツールを実行するには、次のいずれかの UNIX エミュレーション・ユーティリティが必要です。

- Cygwin 1.3.2.2-1 以上
  サイト：http://sources.redhat.com
- MKS Toolkit 6.1
  サイト：http://www.datafocus.com/

---

bulkmodify でのグローバリゼーション・サポートの使用方法

引数 -E ".*character_set*" をコマンドに追加します。

たとえば、次のように入力します。

```
bulkmodify.sh -c my_service_name -E ".ZHS16GBK" -b "ou=manufacturing,o=acme,c=us" -r
title -v Foreman -f "objectclass=*"
```

この例では、-b、-v および -f の各引数の値を簡体字中国語キャラクタ・セットを使用して指定できます。

注意： Windows オペレーティング・システムでシェル・スクリプト・ツールを実行するには、次のいずれかの UNIX エミュレーション・ユーティリティが必要です。

- Cygwin 1.3.2.2-1 以上
  サイト：http://sources.redhat.com
- MKS Toolkit 6.1
  サイト：http://www.datafocus.com/

H

ユーザーおよびグループの作成ベースおよび検索ベースに対するアクセス制御の設定

ユーザー検索ベース、ユーザー作成ベース、グループ検索ベース、グループ作成ベースを変更すると、新しいコンテナに対するアクセス制御を適切に設定する必要があります。この付録では、次の項目について説明します。

- ユーザー検索ベースおよびユーザー作成ベースに対するアクセス制御の設定
- グループ検索ベースおよびグループ作成ベースに対するアクセス制御の設定

ユーザー検索ベースおよびユーザー作成ベースに対するアクセス制御の設定

1. 次の内容で、LDIF（user_aci.ldif）ファイルを作成します。

```
--- BEGIN LDIF file contents---
dn: %usersearch_or_createbase_dn%
changetype: modify
add: orclaci
orclaci: access to entry by group="cn=oracledascreateuser,
cn=groups,cn=OracleContext,%subscriberdn%"
added_object_constraint=(objectclass=orcluser*) (browse,add) by group="cn=Common
User Attributes, cn=Groups,cn=OracleContext,%subscriberdn%" (browse) by
group="cn=PKIAdmins, cn=groups, cn=OracleContext,%subscriberdn%" (browse)
orclaci: access to entry filter=(objectclass=inetorgperson) by
group="cn=oracledascreateuser, cn=groups,cn=OracleContext,%subscriberdn%"
added_object_constraint=(objectclass=orcluser*) (browse,add) by
group="cn=oracledasdeleteuser, cn=groups,cn=OracleContext,%subscriberdn%"
(browse,delete) by group="cn=oracledasedituser,
cn=groups,cn=OracleContext,%subscriberdn%" (browse) by
group="cn=UserProxyPrivilege, cn=Groups,cn=OracleContext,%subscriberdn%"
(browse,
proxy) by dn="orclApplicationCommonName=DASApp, cn=DAS,
cn=Products,cn=oraclecontext" (browse,proxy) by self (browse, nodelete, noadd)
by
group="cn=Common User Attributes, cn=Groups,cn=OracleContext,%subscriberdn%"
(browse) by * (browse, noadd, nodelete)
orclaci: access to attr=(*) filter=(objectclass=inetorgperson) by
group="cn=oracledasedituser, cn=groups,cn=OracleContext,%subscriberdn%"
(read,search,write,compare) by self (read,search,write,selfwrite,compare) by *
(read,
nowrite, nocompare)
orclaci: access to attr=(userPassword) filter=(objectclass=inetorgperson) by

group="cn=OracleUserSecurityAdmins,cn=Groups,cn=OracleContext,%subscriberdn%"
(read,search,write,compare) by group="cn=oracledasedituser,
cn=groups,cn=OracleContext,%subscriberdn%" (read,search,write,compare) by self
(read,search,write,selfwrite,compare) by group="cn=authenticationServices,
cn=Groups,cn=OracleContext,%subscriberdn%" (compare) by * (none)
orclaci: access to attr=(authpassword, orclpasswordverifier, orclpassword) by
group="cn=oracledasedituser,cn=groups,cn=OracleContext,%subscriberdn%"
(read,search,write,compare) by
group="cn=verifierServices,cn=Groups,cn=OracleContext,%subscriberdn%" (search,
read,
compare) by self (search,read,write,compare) by * (none)
orclaci: access to attr=(orclpwdaccountunlock) by
group="cn=oracledasedituser,cn=groups,cn=OracleContext,%subscriberdn%" (write)
```

```
by *
(none)
orclaci: access to attr=(usercertificate, usersmimecertificate) by
group="cn=PKIAdmins,cn=Groups,cn=OracleContext,%subscriberdn%" (read, search,
write, compare) by self (read, search, compare) by * (read, search, compare)
orclaci: access to attr=(mail) by

group="cn=EmailAdminsGroup,cn=EmailServerContainer,cn=Products,cn=OracleContext"
(write) by group="cn=oracledasedituser,
cn=groups,cn=OracleContext,%subscriberdn%"
(read,search,write,compare)
orclaci: access to attr=(orclguid, orclisenabled, modifytimestamp,mail) by
group="cn=Common User Attributes, cn=Groups,cn=OracleContext,%subscriberdn%"
(read, search, compare) by group="cn=oracledasedituser,
cn=groups,cn=OracleContext,%subscriberdn%" (read,search,write,compare) by *
(read,
nowrite, nocompare)
orclaci: access to attr=(orclpasswordhintanswer) by group="cn=Common User
Attributes,
cn=Groups,cn=OracleContext,%subscriberdn%" (read, search, compare) by self
(read,search,write,selfwrite,compare) by * (noread, nowrite, nocompare)
orclaci: access to attr=(orclpasswordhint) by group="cn=Common User Attributes,
cn=Groups,cn=OracleContext,%subscriberdn%" (read, search, compare) by self
(read,search,write,selfwrite,compare) by

group="cn=OracleUserSecurityAdmins,cn=Groups,cn=OracleContext,%subscriberdn%"
(read,search,write,compare) by * (noread, nowrite, nocompare)
orclaci: access to attr=(displayName, preferredlanguage,

orcltimezone,orcldateofbirth,orclgender,orclwirelessaccountnumber,cn,uid,homepho
ne,telephonenumber)
by group="cn=Common User Attributes, cn=Groups,cn=OracleContext,%subscriberdn%"
(read, search, compare) by group="cn=oracledasedituser,
cn=groups,cn=OracleContext,%subscriberdn%" (read,search,write,compare) by self
(read,search,write,selfwrite,compare) by * (read, nowrite, nocompare)
      -
add: orclentrylevelaci
orclentrylevelaci: access to entry by group="cn=oracledascreateuser,
cn=groups,cn=OracleContext,%subscriberdn%"
added_object_constraint=(objectclass=orcluser*) (browse, add) by * (browse)
---END LDIF file contents------
```

2. `%subscriberdn%` をサブスクライバの DN に置き換え、`%usersearch_or_createbase_dn%` を、新しいユーザー検索 / 作成ベースが示すコンテナの新しい DN 値に置き換えます。

3. 次のように、ldapmodify コマンドを入力します。

```
ldapmodify -p <oidport> -h <oidhost> -D cn=orcladmin -w <Instance  Password> -v
-f  user_aci.ldif
```

グループ検索ベースおよびグループ作成ベースに対するアクセス制御の設定

1. 次の内容で、ldif（group_aci.ldif）ファイルを作成します。

```
--- BEGIN LDIF file contents---
dn: %groupsearch_or_createbase_dn%
changetype: modify
add: orclaci
orclaci: access to entry by group="cn=IASAdmins,
cn=groups,cn=OracleContext,%subscriberdn%"
added_object_constraint=(objectclass=orclcontainer) (browse,add)
orclaci: access to entry by group="cn=oracledascreategroup,
cn=groups,cn=OracleContext,%subscriberdn%"
added_object_constraint=(objectclass=orclgroup*) (browse,add) by
group="cn=Common
Group Attributes, cn=Groups,cn=OracleContext,%subscriberdn%" (browse)
orclaci: access to entry filter=(&(objectclass=orclgroup)(orclisvisible=false))
by
groupattr=(owner) (browse, add, delete) by dnattr=(owner) (browse, add, delete)
by
group="cn=Common Group Attributes, cn=Groups,cn=OracleContext,%subscriberdn%"
(browse) by * (none)
orclaci: access to entry
filter=(&(objectclass=orclgroup)(!(orclisvisible=false))) by
group="cn=oracledascreategroup, cn=groups,cn=OracleContext,%subscriberdn%"
added_object_constraint=(objectclass=orclgroup) (browse,add) by
group="cn=oracledasdeletegroup, cn=groups,cn=OracleContext,%subscriberdn%"
(browse,delete) by group="cn=oracledaseditgroup,
cn=Groups,cn=OracleContext,%subscriberdn%" (browse) by groupattr=(owner)
(browse,
add, delete) by dnattr=(owner) (browse, add, delete) by group="cn=Common Group
Attributes, cn=Groups,cn=OracleContext,%subscriberdn%" (browse)
orclaci: access to attr=(*)
filter=(&(objectclass=orclgroup)(orclisvisible=false)) by
groupattr=(owner) (read,search,write,compare) by dnattr=(owner)
(read,search,write,compare) by * (none) by group="cn=Common Group Attributes,
cn=Groups,cn=OracleContext,%subscriberdn%" (read, search, compare)
orclaci: access to attr=(*)
filter=(&(objectclass=orclgroup)(!(orclisvisible=false))) by
groupattr=(owner) (read,search,write,compare) by dnattr=(owner)
```

```
(read,search,write,compare)  by group="cn=oracledaseditgroup,
cn=groups,cn=OracleContext,%subscriberdn%" (read,search,write,compare) by
group="cn=Common Group Attributes, cn=Groups,cn=OracleContext,%subscriberdn%"
(read, search, compare)
      -
add: orclentrylevelaci
orclentrylevelaci: access to entry by group="cn=oracledascreategroup,
cn=groups,cn=OracleContext,%subscriberdn%"
added_object_constraint=(objectclass=orclgroup) (browse, add) by
group="cn=IASAdmins, cn=groups,cn=OracleContext,%subscriberdn%"
added_object_constraint=(objectclass=orclcontainer) (browse,add) by * (browse)
---END LDIF file contents------
```

2. %subscriberdn% をサブスクライバの DN に置き換え、%groupsearch_or_createbase_dn% を、新しいグループ検索 / 作成ベースが示すコンテナの新しい DN 値に置き換えます。
3. 次のように、ldapmodify コマンドを入力します。

```
ldapmodify -p oidport -h oidhost -D cn=orcladmin -w Instance Password -v -f
group_aci.ldif
```

トラブルシューティング

この付録では、Oracle Internet Directory の実行時またはインストール時に発生する可能性のある一般的な問題について説明します。次の項目について説明します。

- インストール時のエラー
- 管理エラー・メッセージとその原因

インストール時のエラー

Oracle9*i* データベース・サーバーのインストールおよび構成時には、データベースのキャラクタ・セットを UTF-8 に設定することをお薦めします。別のキャラクタ・セットを選択することもできますが、その場合、データベースのキャラクタ・セットとディレクトリ・データに互換性があることを確認してください。たとえば、日本語のデータベースのキャラクタ・セットを選択して繁体字中国語のディレクトリ・データを格納することはできません。

管理エラー・メッセージとその原因

この項では、発生する可能性のある Oracle ディレクトリ・サーバーのすべてのエラー・メッセージを示します。各メッセージに続いて、そのエラーに関して最も可能性の高い原因が記述されています。

次の項目について説明します。

- スキーマ変更が原因の Oracle データベース・サーバー・エラー
- Oracle ディレクトリ・サーバーから戻される標準エラー・メッセージ
- その他のエラー・メッセージ

スキーマ変更が原因の Oracle データベース・サーバー・エラー

ORA-1562

原因 : ロールバック・セグメント領域に収まらないスキーマ・コンポーネントを追加しようとすると、このエラーが発生し、変更はコミットされません。この問題を解決するには、データベース・サーバーのロールバック・セグメントのサイズを増やします。

Oracle ディレクトリ・サーバーから戻される標準エラー・メッセージ

表 I-1 に、標準のエラー・メッセージとその原因を示します。Oracle Internet Directory では、これ以外のメッセージも戻されます。標準以外のメッセージとその説明は、I-6 ページの「その他のエラー・メッセージ」を参照してください。

表 I-1 標準のエラー・メッセージ

エラー	原因
00: 成功しました	操作が正常に完了しました。
01: 操作エラー	要求の処理時に、サーバーで一般的なエラーが発生しました。

表 I-1 標準のエラー・メッセージ（続き）

エラー	原因
02: プロトコル・エラー	クライアント要求が、LDAP プロトコル要件（書式や構文など）を満たしていません。このエラーは、次の状況で発生する可能性があります。 ■ サーバーで、受信した要求の解析時にデコード・エラーが発生した場合。 ■ エントリに属性の型を追加する追加要求または変更要求で、値が指定されていない場合。 ■ SSL 資格証明の読取りでエラーが発生した場合。 ■ 変更操作で指定されたタイプが不明な場合（LDAP_MOD_ADD、LDAP_MOD_DELETE および LDAP_MOD_REPLACE 以外）。 ■ 検索範囲が不明な場合。
03: 時間制限を超えました。	検索時間が指定した制限時間を超えました。検索の制限時間が未指定の場合、Oracle Internet Directory では、デフォルトの制限時間である 1 時間が使用されます。
04: サイズ制限を超えました。	検索の問合せに一致するエントリが、指定したサイズ制限を超えました。検索のサイズ制限が未指定の場合、Oracle Internet Directory では、デフォルトのサイズ制限が使用されます。
05: 比較結果は FALSE です。	指定した値は、エントリ内の値と同一ではありません。
06: 比較結果は TRUE です。	指定した値は、エントリ内の値と同一です。
07: 厳密認証はサポートされていません。	バインド方法がサーバーでサポートされていません。
08: 厳密認証が必要です。	厳密認証が必要です。現在、Oracle Internet Directory はこのメッセージを戻しません。
09: 受信した結果と参照は一部分です。	サーバーから参照が戻されました。
10: LDAP 参照エラー	サーバーから参照が戻されました。
11: LDAP 管理制限エラー	現在、Oracle Internet Directory はこのメッセージを戻しません。
12: 最大拡張機能はサポートされていません。	指定した要求はサポートされていません。
16: 該当する属性がありません。	要求で指定したエントリ内に、該当する属性は存在していません。
17: 属性タイプが未定義です。	指定した属性の型が、スキーマ内で定義されていません。

表 I-1 標準のエラー・メッセージ（続き）

エラー	原因
18: 一致しません。	指定した一致規則は、その属性の型に適合しません。現在、Oracle Internet Directory はこのメッセージを戻しません。
19: 制約違反です。	要求内の値が、特定の制約に違反しています。
20: タイプまたは値が存在しています。	属性に指定した値が重複しています。
21: 構文に誤りがあります。	指定した属性の構文に誤りがあります。検索の場合は、フィルタの構文に誤りがあります。
32: 該当するオブジェクトがありません。	操作用に指定したベースが存在していません。
33: 別名に問題があります。	現在、Oracle Internet Directory はこのメッセージを戻しません。
34: 識別名の構文に誤りがあります。	識別名構文にエラーがあります。
35: オブジェクトはリーフです。	そのエントリはリーフ（終端エントリ）です。現在、Oracle Internet Directory はこのメッセージを戻しません。
36: 別名の参照解除に問題があります。	現在、Oracle Internet Directory はこのメッセージを戻しません。
48: 認証が正しくありません。	現在、Oracle Internet Directory はこのメッセージを戻しません。
49: 資格証明が無効です。	資格証明が正しくないため、バインドに失敗しました。
50: アクセス権限が不十分です。	クライアントに、この操作を実行するためのアクセス権限がありません。
51: ディレクトリ・サービス・エージェントがビジー状態です。	サーバーは、これ以上のクライアント接続を受け入れることができません。現在、Oracle Internet Directory はこのメッセージを戻しません。
52: ディレクトリ・サービス・エージェントが利用不可です。	サーバーと通信できません。現在、Oracle Internet Directory はこのメッセージを戻しません。
53: ディレクトリ・サービス・エージェントが実行不可の状態です。	一般的なエラーか、またはサーバーが読取り専用モードです。
54: ループが検出されました。	現在、Oracle Internet Directory はこのメッセージを戻しません。
64: 命名違反です。	現在、Oracle Internet Directory はこのメッセージを戻しません。

表 I-1 標準のエラー・メッセージ（続き）

エラー	原因
65: オブジェクト・クラス違反です。	エントリに対する変更が、オブジェクト・クラスの定義に違反しています。
66: リーフ以外での操作は許可されていません。	削除対象のエントリに子エントリがあります。
67: 相対識別名での操作は許可されていません。	相対識別名属性でこの操作は実行できません。たとえば、エントリの相対識別名属性を削除することはできません。
68: すでに存在しています。	追加条件が重複しています。
69: オブジェクト・クラスを変更できません。	現在、Oracle Internet Directory はこのメッセージを戻しません。
70: 結果が大きすぎます。	現在、Oracle Internet Directory はこのメッセージを戻しません。
80: 不明なエラー	現在、Oracle Internet Directory はこのメッセージを戻しません。
81: LDAP サーバーと通信できません。	LDAP サーバーと通信できません。このメッセージは SDK から戻されます。
82: ローカル・エラー	クライアントで内部エラーが発生しました。このメッセージはクライアントの SDK から戻されます。
83: コード化エラー	クライアントで、要求をエンコーディングするときにエラーが発生しました。このメッセージは SDK から戻されます。
84: デコード・エラー	クライアントで、要求をデコードするときにエラーが発生しました。このメッセージは SDK から戻されます。
85: 時間切れです。	クライアントが、その操作に指定したタイムアウトに達しました。このメッセージは SDK から戻されます。
86: 認証方式が不明です。	認証方式が、クライアントの SDK で理解されません。
87: 検索フィルタが正しくありません。	検索フィルタが正しくありません。
88: ユーザーが操作を取り消しました。	ユーザーが操作を取り消しました。
89: LDAP ルーチンのパラメータが正しくありません。	LDAP ルーチンに対するパラメータが正しくありません。
90: メモリー不足です。	メモリー不足です。

その他のエラー・メッセージ

表 I-2 に、その他のエラー・メッセージとその原因を示します。これらのメッセージには、エラー・コードは表示されません。

後述のメッセージの一部で使用されているパラメータ・タグは、Oracle Internet Directory アプリケーションによって、対応する実行時の値に置換されます。

表 I-2 その他のエラー・メッセージ

エラー	原因
(string には文字列が入ります) string 属性が見つかりません。	特定の属性の型が、スキーマに定義されていません。
< パラメータ > が属性 < パラメータ > に見つかりません。	値がその属性に見つかりません。(ldapmodify)
オブジェクト・クラス < パラメータ > のスキーマ情報が管理ドメインに含まれていません。	要求で指定したオブジェクト・クラスが、スキーマに存在していません。
クラスの追加に使用した OID< パラメータ > は別のクラスで使用されています。	指定したオブジェクト識別子が重複しています。(スキーマ変更)
属性 < パラメータ > はすでに使用されています。	属性名が重複しています。(スキーマ変更)
属性 < パラメータ > に構文エラーがあります。	属性名の定義に構文エラーがあります。(スキーマ変更)
属性 < パラメータ > はスキーマでサポートされていません。	属性が定義されていません。(すべての操作)
属性 < パラメータ > は単一の値です。	属性は単一値です。(ldapadd および ldapmodify)
属性 < パラメータ > がエントリに存在していません。	エントリに、この属性は存在していません。(ldapmodify)
属性の定義が正しくありません。	属性の定義に構文エラーがあります。(スキーマ変更)
現在はサポートされていません。	このバージョンの LDAP 要求は、このサーバーではサポートされていません。
削除対象のエントリが見つかりません。	削除操作に指定した識別名が見つかりません。

表 I-2 その他のエラー・メッセージ（続き）

エラー	原因
変更対象のエントリが見つかりません。	要求で指定したエントリが見つかりません。
< パラメータ > をエントリに追加中にエラーが発生しました。	modify の add 操作が呼び出されたときに戻されました。システム・リソースが使用できないことが原因と考えられます。
属性値の暗号化時にエラーが発生しました。	ユーザー・パスワードの暗号化時にエラーが発生しました。（すべての操作）
DN の正規化でエラーが発生しました。	指定された識別名（DN）が無効です。DN の解析時に構文エラーが見つかりました。（すべての操作）
< パラメータ > 属性のハッシングでエラーが発生しました。	属性に対するハッシュ・エントリの作成時にエラーが発生しました。（スキーマ変更）
< パラメータ > オブジェクト・クラスのハッシングでエラーが発生しました。	オブジェクト・クラスに対するハッシュ・エントリの作成時にエラーが発生しました。（スキーマ変更）
スキーマ・ハッシュの作成でエラーが発生しました。	スキーマに対するハッシュ表作成時にエラーが発生しました。（スキーマ変更）
< パラメータ > の置換でエラーが発生しました。	この属性の置換でエラーが発生しました。（ldapmodify）
属性 < パラメータ > に対する値の正規化時にエラーが発生しました。	属性に対する値の正規化時にエラーが発生しました。（すべての操作）
< パラメータ > が必須またはオプションの属性リストで見つかりません。	指定した属性が、オブジェクト・クラスの要件どおりに、必須属性またはオプション属性のリストに存在していません。
この機能は組み込まれていません。	その機能または要求が現在はサポートされていません。
無効な非同期通信インタフェースは < パラメータ > です。	要求で指定した特定のアクセス制御情報アイテム（ACI）が無効です。
必須属性 < パラメータ > が管理ドメイン < パラメータ > に定義されていません。	未定義の属性を参照しています。（スキーマ変更）
必須属性が不足しています。	特定のエントリに対する必須属性が、特定のオブジェクト・クラスの要件どおりに存在していません。

表 I-2 その他のエラー・メッセージ（続き）

エラー	原因
一致規則 < パラメータ > が定義されていません。	サーバーに一致規則が定義されていません。（スキーマ変更）
最大接続数に達しました。	LDAP サーバーへの最大同時接続数に達しました。
DN を変更せずにエントリの命名属性を変更しようとしています。	ldap_modify を使用して、命名属性を変更することはできません。cn などの命名属性は識別名の要素です。
新しい親が見つかりません。	識別名の変更操作で指定した新しい親が存在していません。（ldapmodifydn）
オブジェクトはすでに存在しています。	エントリが重複しています。（ldapadd および ldapmodifydn）
オブジェクト ID< パラメータ > はすでに使用されています。	指定したオブジェクト識別子が重複しています。（スキーマ変更）
オブジェクト・クラス < パラメータ > はすでに使用されています。	オブジェクト・クラス名が重複しています。（スキーマ変更）
オブジェクト・クラスの属性が不足しています。	この特定のエントリに対するオブジェクト・クラスの属性が不足しています。
OID< パラメータ > に構文エラーがあります。	オブジェクト識別子の定義に構文エラーがあります。（スキーマ変更）
エントリ内の属性の 1 つに重複した値があります。	作成中のエントリで、同じ属性に対して値を 2 つ入力しました。
< パラメータ > での操作は許可されていません。	このエントリでの操作は許可されていません。（変更、追加および削除）
ディレクトリ・サーバー・エントリでの操作は許可されていません。	ディレクトリ・サーバー・エントリで、この操作を行うことはできません。（削除）
オプション属性 < パラメータ > が管理ドメイン < パラメータ > に定義されていません。	未定義の属性を参照している可能性があります。（スキーマ変更）
ディレクトリ内に親のエントリが見つかりません。	親エントリが存在していません。（ldapadd および ldapmodifydn）

表 I-2 その他のエラー・メッセージ（続き）

エラー	原因
スーパー・オブジェクト < パラメータ > が管理ドメイン < パラメータ > に定義されていません。	スーパー・タイプが、存在していないクラスを参照しています。（スキーマ変更）
スーパー・タイプが未定義です。	スーパー・タイプが存在していません。（スキーマ変更）
スーパー・ユーザーの追加は許可されていません。	スーパー・ユーザーのエントリを作成することはできません。（ldapadd）
構文 < パラメータ > が未定義です。	構文がサーバーに定義されていません。（スキーマ変更）
RDN で指定された属性または値がエントリ内に存在していません。	相対識別名（RDN）として指定した属性値がエントリ内に存在していません。（ldapadd）
検索範囲が不明です。	LDAP 要求で指定した検索範囲が認識されません。
このバージョンはサポートされていません。	このバージョンの LDAP 要求は、このサーバーではサポートされていません。

パスワード・ポリシー違反のエラー・メッセージ

I-9 ページの表 I-3 に、パスワード・ポリシー違反が発生した結果、クライアントに送信されるエラー・メッセージを示します。エラー・コードは、標準の LDAP エラー・コードではありません。このエラー・メッセージは、LDAP 結果の追加情報の一部として送信されます。

表 I-3 パスワード・ポリシー違反のエラー・メッセージ

エラー番号	例外	コメントまたは解消方法
9000	GSL_PWDEXPIRED_EXCP	パスワードが期限切れです。管理者に問い合せてパスワードを変更してください。
9001	GSL_ACCOUNTLOCKED_EXCP	アカウントがロックされています。管理者に問い合せてください。
9002	GSL_EXPIREWARNING_EXCP	パスワードが `pwdexpirewarning` 秒後に期限切れになります。すぐにパスワードを変更してください。
9003	GSL_PWDMINLENGTH_EXCP	パスワードの長さは、`pwdminlength` 文字以上必要です。
9004	GSL_PWDNUMERIC_EXCP	パスワードには、少なくとも `orclpwdalphanumeric` の数字を含める必要があります。

表 I-3（続き）パスワード・ポリシー違反のエラー・メッセージ

エラー番号	例外	コメントまたは解消方法
9005	GSL_PWDNULL_EXCP	パスワードに NULL は設定できません。
9006	GSL_PWDINHISTORY_EXCP	新規パスワードは、旧パスワードと同じにはできません。
9007	GSL_PWDILLEGALVALUE_EXCP	新規パスワードは、orclpwdillegalvalues と同じにはできません。
9008	GSL_GRACELOGIN_EXCP	パスワードが期限切れです。pwdgraceloginlimit の猶予期間ログインが残っています。
9050	GSL_ACCTDISABLED_EXCP	アカウントが使用禁止になっています。管理者に問い合せてください。

パスワード・ポリシー制御

表 I-4 パスワード・ポリシー制御

オブジェクト識別子	例外	説明
2.16.840.1.113894.1.8.6	OID_PASSWORD_REQUEST_CONTROL	クライアントがサーバーから応答を受けるために送信する要求制御。
2.16.840.1.113894.1.8.7	OID_PASSWORD_EXPWARNING_CONTROL	pwdExpireWarning 属性が使用可能で、クライアントが要求制御を送信した場合にサーバーが送信する応答制御。応答制御値には、パスワード有効期限（秒単位）が含まれます。
2.16.840.1.113894.1.8.8	OID_PASSWORD_GRACELOGIN_CONTROL	猶予期間ログインが設定され、クライアントが要求制御を送信した場合にサーバーが送信する応答制御。応答制御値には、残りの猶予期間ログイン数が含まれます。
2.16.840.1.113894.1.8.9	OID_PASSWORD_MUSTCHANGE_CONTROL	パスワードの強制再設定が使用可能で、クライアントが要求制御を送信した場合にサーバーが送信する応答制御。クライアントは、この制御を受信するとすぐにユーザーに強制的にパスワードを変更させる必要があります。

用語集

ACI

「**アクセス制御情報項目**」を参照。

ACL

「**アクセス制御リスト**」を参照。

ACP

「**アクセス制御ポリシー・ポイント**」を参照。

API

「**Application Program Interface（API）**」を参照。

Application Program Interface（API）

指定したアプリケーションのサービスにアクセスするための一連のプログラム。たとえば、LDAP 対応のクライアントは、LDAP API で使用可能なプログラム・コールを通して、ディレクトリ情報にアクセスする。

Cipher Suite

SSL において、ネットワークのノード間でメッセージ交換に使用される認証、暗号化およびデータ整合性アルゴリズムのセット。SSL ハンドシェイク時に、2 つのノード間で折衝し、メッセージを送受信するときに使用する Cipher Suite を確認する。

configset

「**構成設定エントリ**」を参照。

DES

データ暗号化規格。1970 年代に IBM 社と米国政府によって公式規格として開発されたブロック暗号。

DIB

「**ディレクトリ情報ベース**」を参照。

Directory Integration and Provisioning Server

Oracle Directory Integration Platform 環境で、Oracle Internet Directory と**接続ディレクトリ**との間でデータの同期化を実行するサーバー。

DIS

「**Directory Integration and Provisioning Server**」を参照。

DIT

「**ディレクトリ情報ツリー**」を参照。

DN

「**識別名**」を参照。

DRG

「**ディレクトリ・レプリケーション・グループ**」を参照。

DSA

「**ディレクトリ・システム・エージェント**」を参照。

DSE

「**ディレクトリ固有のエントリ**」を参照。

DSA 固有のエントリ。異なる DSA に同じディレクトリ情報ツリー名を保持できるが、内容は異なる必要がある。つまり、DSE を保持している DSA に固有の内容を保持できる。DSE は、それを保持している DSA に固有の内容を含むエントリである。

Global Unique Identifier（GUID）

エントリがディレクトリに追加されると、システムで生成され、エントリに挿入される識別子。マルチマスター・レプリケート環境で、DN ではなく GUID がエントリを一意に識別する。エントリの GUID をユーザーが変更することはできない。

GUID

「**Global Unique Identifier（GUID）**」を参照。

Internet Engineering Task Force（IETF）

新しいインターネット標準仕様の開発に従事する主要機関。インターネット・アーキテクチャおよびインターネットの円滑な操作の発展に関わるネットワーク設計者、運営者、ベンダーおよび研究者による国際的な団体である。

Internet Message Access Protocol（IMAP）

プロトコルの 1 種。クライアントは、このプロトコルを使用して、サーバー上の電子メール・メッセージに対するアクセスおよび操作を行う。リモートのメッセージ・フォルダ（メールボックスとも呼ばれる）を、ローカルのメールボックスと機能的に同じ方法で操作できる。

LDAP

「**Lightweight Directory Access Protocol（LDAP）**」を参照。

LDAP Data Interchange Format（LDIF）

LDAP コマンドライン・ユーティリティに使用する入力ファイルをフォーマットするための一連の規格。

LDIF

「**LDAP Data Interchange Format（LDIF）**」を参照。

Lightweight Directory Access Protocol（LDAP）

標準的で拡張可能なディレクトリ・アクセス・プロトコル。LDAP は、LDAP クライアントとサーバーが通信を行うための共通言語である。業界標準のディレクトリ製品（Oracle Internet Directory など）をサポートする設計規則のフレームワーク。

MD4

128 ビットのハッシュまたはメッセージ・ダイジェスト値を生成する一方向ハッシュ関数。1 ビットでもファイルの値が変更された場合、そのファイルの MD4 チェックサムは変更される。元のファイルと同じ結果を MD4 で生成するようにファイルを偽造することはほぼ不可能である。

MD5

MD4 の改善されたバージョン。

MDS

「**マスター定義サイト**」を参照。

MTS

「**共有サーバー**」を参照。

OEM

「**Oracle Enterprise Manager**」を参照。

OID 制御ユーティリティ（OID Control Utility）

サーバーの起動と停止のコマンドを発行するコマンドライン・ツール。コマンドは、**OID モニター**のプロセスによって解析され、実行される。

OID データベース・パスワード・ユーティリティ（OID Database Password Utility）

Oracle Internet Directory が Oracle データベースに接続するときのパスワードの変更に使用されるユーティリティ。

OID モニター（OID Monitor）

Oracle ディレクトリ・サーバー・プロセスの開始、監視および終了を実行する Oracle Internet Directory のコンポーネント。レプリケーション・サーバー（インストールされている場合）および Oracle Directory Integration and Provisioning Server の制御も行う。

Oracle Call Interface（OCI）

Application Program Interface（API）の 1 つ。これにより、第三世代言語のネイティブ・プロシージャやファンクション・コールを使用して、Oracle データベース・サーバーにアクセスし、SQL 文の実行のすべての段階を制御するアプリケーションを作成できる。

Oracle Delegated Administration Services

Oracle Delegated Administration Services ユニットと呼ばれる個々の事前定義済サービスのセットで、ユーザーのかわりにディレクトリ操作を実行する。Oracle Internet Directory セルフ・サービス・コンソールによって、Oracle Internet Directory を使用する Oracle アプリケーションおよびサードパーティ・アプリケーションの両方の管理ソリューションを容易に開発および配布できる。

Oracle Directory Integration and Provisioning Server

Oracle Directory Integration Platform 環境で、Oracle Internet Directory の変更イベントを監視し、ディレクトリ統合プロファイルの情報に基づいてアクションを行うデーモン・プロセス。

Oracle Directory Integration Platform

Oracle Internet Directory のコンポーネントの 1 つ。Oracle Internet Directory のような中央 LDAP ディレクトリの周囲のアプリケーションを統合するために開発されたフレームワーク。

Oracle Directory Manager

Oracle Internet Directory を管理するための、Graphical User Interface（GUI）を備えた Java ベースのツール。

Oracle Enterprise Manager

Oracle 製品の 1 つ。グラフィカルなコンソール、エージェント、標準的なサービスおよびツールを組合せ、Oracle 製品を管理するための統合された包括的なシステム管理プラットフォームを提供する。

Oracle Identity Management

すべての企業識別情報および企業内の様々なアプリケーションへのアクセスを集中的かつ安全に管理するための配置を可能にするインフラストラクチャ。

Oracle Internet Directory

分散ユーザーやネットワーク・リソースに関する情報の検索を可能にする、一般的な用途のディレクトリ・サービス。LDAP バージョン 3 と Oracle9*i* の高度のパフォーマンス、スケーラビリティ、耐久性および可用性を組み合せたもの。

Oracle Net Services

Oracle のネットワーク製品ファミリの基礎。Oracle Net Services を使用すると、サービスやアプリケーションを異なるコンピュータに配置して通信できる。Oracle Net Services の主な機能には、ネットワーク・セッションの確立およびクライアント・アプリケーションとサーバー間のデータ転送がある。Oracle Net Services は、ネットワーク上の各コンピュータに配置される。ネットワーク・セッションの確立後は、Oracle Net Services はクライアントとサーバーのためのデータ伝達手段として機能する。

Oracle PKI 証明書使用条件

証明書でサポートされる Oracle アプリケーション・タイプを定義する。

Oracle Wallet Manager

セキュリティ管理者が、クライアントとサーバー上での公開鍵セキュリティ資格証明の管理に使用する Java ベースのアプリケーション。

関連項目：『Oracle Advanced Security 管理者ガイド』

Oracle9*i* Advanced Replication

2 つの Oracle データベース間で、データベースの表を継続的に同期化できる Oracle9*i* の機能。

peer-to-peer レプリケーション（peer-to-peer replication）

マルチマスター・レプリケーションまたは n-way レプリケーションとも呼ばれる。同等に機能する複数サイトがレプリケートされたデータのグループを管理できるようにするレプリケーションのタイプ。このようなレプリケーション環境では、各ノードはサプライヤ・ノードであると同時にコンシューマ・ノードであり、各ノードでディレクトリ全体がレプリケートされる。

PKCS #12

公開鍵暗号規格（PKCS）。RSA Data Security, Inc. の PKCS #12 は、個人的な認証資格証明を、通常 **Wallet** と呼ばれる形式で保管および転送するための業界標準である。

point-to-point レプリケーション（point-to-point replication）

ファンアウト・レプリケーション（fan-out replication）とも呼ばれる。サプライヤがコンシューマに直接レプリケートするレプリケーションのタイプ。コンシューマは 1 つ以上の他のコンシューマにレプリケートできる。レプリケーションには、完全レプリケーションと部分レプリケーションがある。

RDN

「**相対識別名**」を参照。

SASL

「**Simple Authentication and Security Layer（SASL）**」を参照。

Secure Hash Algorithm（SHA）

長さが 264 ビット未満のメッセージを取得して、160 ビットのメッセージ・ダイジェスト値を生成するアルゴリズム。このアルゴリズムは MD5 よりも若干速度が遅くなるが、大きなメッセージ・ダイジェストによって、総当り攻撃や反転攻撃に対処できる。

Secure Sockets Layer（SSL）

ネットワーク接続を保護するために Netscape Communications Corporation が開発した業界標準プロトコル。SSL では公開鍵インフラストラクチャ（PKI）を使用して、認証、暗号化およびデータ整合性を実現している。

SGA

「**システム・グローバル領域**」を参照。

SHA

「**Secure Hash Algorithm（SHA）**」を参照。

Simple Authentication and Security Layer（SASL）

接続ベースのプロトコルに認証サポートを追加する方法。この仕様を使用するために、プロトコルには、ユーザーを識別してサーバーに対して認証を行い、オプションで、以降のプロトコル対話に使用するセキュリティ・レイヤーを規定するコマンドが含まれる。このコマンドには、SASL 方式を識別する必須引数がある。

SLAPD

スタンドアロンの LDAP デーモン。

SSL

「**Secure Sockets Layer（SSL）**」を参照。

subACLSubentry

ACL 情報が含まれた特定のタイプのサブエントリ。

subSchemaSubentry

スキーマ情報が含まれた特定のタイプの**サブエントリ**。

TLS

「**Transport Layer Security（TLS）**」を参照。

Transport Layer Security（TLS）

インターネット上の通信プライバシを提供するプロトコル。このプロトコルによって、クライアント / サーバー・アプリケーションは、通信時の盗聴、改ざんまたはメッセージの偽造を防止できる。

Unicode

汎用キャラクタ・セットのタイプ。16 ビットの領域にエンコードされた 64K 個の文字の集合。既存のほとんどすべてのキャラクタ・セット規格の文字をすべてエンコードする。世界中で使用されているほとんどの記述法を含む。Unicode は Unicode Inc. によって所有および定義される。Unicode は標準的なエンコーディングであり、異なるロケールで値を伝達できることを意味する。しかし、Unicode とすべての Oracle キャラクタ・セットとの間で、情報の損失なしにラウンドトリップ変換が行われることは保証されない。

UNIX Crypt

UNIX 暗号化アルゴリズム。

UTC（Coordinated Universal Time）

世界中のあらゆる場所で共通の標準時間。以前から現在に至るまで広くグリニッジ時（GMT）または世界時と呼ばれており、UTC は名目上は地球の本初子午線に関する平均太陽時を表す。UTC 形式である場合、値の最後に z が示される（例 : 200011281010z）。

UTF-16

Unicode の 16 ビット・エンコーディング。Latin-1 文字は、この規格の最初の 256 コード・ポイントである。

UTF-8

文字ごとに連続した 1、2、3 または 4 バイトを使用する **Unicode** の可変幅 8 ビット・エンコーディング。0 ～ 127 の文字（7 ビット ASCII 文字）は 1 バイトでエンコードされ、128 ～ 2047 の文字では 2 バイト、2048 ～ 65535 の文字では 3 バイト、65536 以上の文字は 4 バイトを必要とする。このための Oracle キャラクタ・セット名は AL32UTF8（Unicode 3.1 規格用）となる。

Wallet

個々のエンティティに対するセキュリティ資格証明の格納と管理に使用される抽象的な概念。様々な暗号化サービスで使用するために、資格証明の格納と取出しを実現する。Wallet Resource Locator（WRL）は、Wallet の位置を特定するために必要な情報をすべて提供する。

X.509

公開鍵の署名に使用される ISO の一般的な形式。

アクセス制御情報項目（Access Control Information Item: ACI）

どのディレクトリ・データに対して、誰がどのタイプのアクセス権限を持っているかを判断する属性。この属性には、エントリに関係する構造型アクセス項目と、属性に関係するコンテント・アクセス項目に関する 1 組の規則が含まれている。両方のアクセス項目に対するアクセス権限を、1 つ以上のユーザーまたはグループに付与できる。

アクセス制御ポリシー・ポイント（Access Control Policy Point: ACP）

セキュリティ・ディレクティブを含むエントリ。このディレクティブは、**ディレクトリ情報ツリー**内のすべての下位エントリに適用される。

アクセス制御リスト（Access Control List: ACL）

アクセス・ディレクティブのグループ。管理者が定義する。ディレクティブは、特定のクライアントまたはクライアントのグループ、あるいはその両方に対して、特定データへのアクセスのレベルを付与する。

アドバンスト・レプリケーション（Advanced Replication: AR）

「**Oracle9i Advanced Replication**」を参照。

アドバンスト・レプリケーション（ASR）

「**Oracle9i Advanced Replication**」を参照。

暗号化（cryptography）

データのエンコードとデコードを行い、保護メッセージを生成する作業。

暗号化（encryption）

メッセージの内容を、宛先の受信者以外の第三者が読むことのできない形式（暗号文）に変換する処理。

一方向関数（one-way function）

一方向への計算は容易だが、逆の計算（反対方向への計算）は非常に難しい関数。

一方向ハッシュ関数（one-way hash function）

可変サイズの入力を取得して、固定サイズの出力を作成する**一方向関数**。

一致規則（matching rule）

検索または比較操作における、検索対象の属性値と格納されている属性値との間の等価性の判断。たとえば、`telephoneNumber` 属性に関連付けられた一致規則では、(650) 123-4567 を (650) 123-4567 または 6501234567 のいずれか、あるいはその両方と一致させることができる。属性の作成時に、その属性を一致規則と対応付けることができる。

委任管理者（delegated administrator）

ホスティングされた環境では、アプリケーション・サービス・プロバイダなどの 1 企業が、他の複数の企業に Oracle コンポーネントを使用可能にして、その情報を格納する。この種の環境では、グローバル管理者はディレクトリ全体にまたがるアクティビティを実行する。委任管理者と呼ばれる他の管理者は、特定の認証管理レルムでのロール、または特定のアプリケーションに対してのロールを持つ。

インスタンス（instance）

「ディレクトリ・サーバー・インスタンス」を参照。

インポート・エージェント（import agent）

Oracle Directory Integration Platform 環境で、Oracle Internet Directory にデータをインポートするエージェント。

インポート・データ・ファイル（import data file）

Oracle Directory Integration Platform 環境で、インポート・エージェントによってインポートされたデータを格納するファイル。

エクスポート・エージェント（export agent）

Oracle Directory Integration Platform 環境で、Oracle Internet Directory からデータをエクスポートするエージェント。

エクスポート・データ・ファイル（export data file）

Oracle Directory Integration Platform 環境で、エクスポート・エージェントによってエクスポートされたデータを格納するファイル。

エクスポート・ファイル（export file）

「エクスポート・データ・ファイル」を参照。

エントリ（entry）

ディレクトリの基本単位で、ディレクトリ・ユーザーに関係のあるオブジェクトに関する情報が含まれている。

応答時間（response time）

要求の発行から応答の完了までの時間。

オブジェクト・クラス（object class）

名前を持った属性のグループ。属性をエントリに割り当てるときは、その属性を保持しているオブジェクト・クラスをそのエントリに割り当てる。

同じオブジェクト・クラスに関連するオブジェクトはすべて、同じ属性を共有する。

介在者（man-in-the-middle）

第三者によるメッセージの不正傍受などのセキュリティ攻撃。第三者、つまり介在者は、メッセージを復号化して再暗号化し（元のメッセージを変更する場合と変更しない場合がある）、元のメッセージの宛先である受信者に転送する。これらの処理はすべて、正当な送受信者が気付かないうちに行われる。この種のセキュリティ攻撃は、**認証**が行われていない場合にのみ発生する。

外部エージェント（external agent）

Oracle Directory Integration and Provisioning Server に依存しないディレクトリ統合エージェント。Oracle Directory Integration and Provisioning Server は外部エージェントに対して、スケジューリング、マッピングまたはエラー処理の各サービスを提供しない。外部エージェントは、通常、サード・パーティのメタディレクトリ・ソリューションを Oracle Directory Integration Platform に統合するときに使用する。

鍵（key）

暗号化において広く使用されているビット列。データの暗号化と復号化を可能にする。鍵は別の数学的な操作にも使用される。暗号が与えられると、鍵によって、平文から暗号文へのマッピングが判断される。

鍵のペア（key pair）

公開鍵とそれに対応する**秘密鍵**のペア。

「公開鍵と秘密鍵のペア」を参照。

仮想 IP アドレス（virtual IP address）

コールド・フェイルオーバー・クラスタ構成では、各物理ノードに独自の物理 IP アドレスと物理ホスト名がある。単一のシステムであるというイメージを外部に示すために、クラスタは、クラスタ内のどの物理ノードにも変更できる動的 IP アドレスを使用する。これは、仮想 IP アドレスと呼ばれる。

仮想ホスト名（virtual host name）

コールド・フェイルオーバー・クラスタ構成で、仮想 IP アドレスに対応するホスト名。

簡易認証（simple authentication）

ネットワークでの送信時に暗号化されない識別名とパスワードを使用して、クライアントがサーバーに対して自己認証を行うプロセス。簡易認証オプションでは、クライアントが送信した識別名とパスワードと、ディレクトリに格納されている識別名とパスワードが一致していることをサーバーが検証する。

管理領域（administrative area）

ディレクトリ・サーバー上の 1 つのサブツリー。そのエントリは、1 つの管理認可レベル（スキーマ、ACL および共通属性）で制御される。

競合（contention）

リソースの競合。

兄弟関係（sibling）

1 つ以上の他のエントリと同じ親を持ったエントリ。

共有サーバー（shared server）

多数のユーザー・プロセスが、非常に少数のサーバー・プロセスを共有できるように構成されたサーバー。これにより、サポートされるユーザー数が増える。共有サーバー構成では、多数のユーザー・プロセスがディスパッチャに接続する。ディスパッチャは、複数の着信ネットワーク・セッション要求を共通キューに送る。複数のサーバー・プロセスの共有プールの中で、あるアイドル状態の共有サーバー・プロセスが共通キューから要求を取り出す。これは、サーバー・プロセスの小規模プールで大量のクライアントを処理できることを意味する。専用サーバーと対比。

クラスタ（cluster）

単一のコンピューティング・リソースとして使用される、相互接続された使用可能なすべてのコンピュータの集合。ハードウェア・クラスタによって、高可用性およびスケーラビリティが実現する。

グループ検索ベース（group search base）

Oracle Internet Directory のデフォルトのディレクトリ情報ツリーで、すべてのグループを検索できる認証管理レルムのノード。

グローバル管理者（global administrator）

ホスティングされた環境では、アプリケーション・サービス・プロバイダなどの 1 企業が、他の複数の企業に Oracle コンポーネントを使用可能にして、その情報を格納する。この種の環境では、グローバル管理者はディレクトリ全体にまたがるアクティビティを実行する。

継承（inherit）

オブジェクト・クラスが別のクラスから導出されたときに、導出元のオブジェクト・クラスの多数の特性も導出（継承）されること。同様に、属性のサブタイプも、そのスーパータイプの特性を継承する。

ゲスト・ユーザー（guest user）

匿名ユーザーではなく、特定のユーザー・エントリも持っていないユーザー。

コールド・バックアップ（cold backup）

データベース・コピー・プロシージャを使用して、新規 **DSA** ノードを既存のレプリケート・システムに追加する手順。

公開鍵（public key）

公開鍵暗号において一般に公開される鍵。主に暗号化に使用されるが、署名の検証にも使用される。

公開鍵暗号（public-key cryptography）

公開鍵と秘密鍵を使用する方法に基づいた暗号化。

公開鍵暗号（public-key encryption）

メッセージの送信側が、受信側の公開鍵でメッセージを暗号化するプロセス。配信されたメッセージは、受信側の秘密鍵で復号化される。

公開鍵と秘密鍵のペア（public/private key pair）

数学的に関連付けられた 2 つの数字のセット。1 つは秘密鍵、もう 1 つは公開鍵と呼ばれる。公開鍵は通常広く使用可能であるのに対して、秘密鍵はその所有者のみ使用可能である。公開鍵で暗号化されたデータは、それに関連付けられた秘密鍵でのみ復号化でき、秘密鍵で暗号化されたデータは、それに関連付けられた公開鍵でのみ復号化できる。公開鍵で暗号化されたデータを、同じ公開鍵で復号化することはできない。

構成設定エントリ（configuration set entry）

ディレクトリ・サーバーの特定インスタンスに関する構成パラメータを保持しているディレクトリ・エントリ。複数の構成設定エントリを格納でき、実行時に参照できる。構成設定エントリは、DSE の subConfigsubEntry 属性で指定されているサブツリー内でメンテナンスされる。DSE 自体は、サーバーの起動対象である関連の**ディレクトリ情報ベース**に常駐している。

コンシューマ（consumer）

レプリケーション更新の宛先となるディレクトリ・サーバー。スレーブと呼ばれることもある。

コンテキスト接頭辞（context prefix）

ネーミング・コンテキストのルートの **DN**。

サービス時間（service time）

要求の開始から、その要求に対する応答の完了までの時間。

サブエントリ（subentry）

サブツリー内のエントリ・グループに適用可能な情報が含まれているエントリのタイプ。情報には次の 3 つのタイプがある。

- アクセス制御ポリシー・ポイント
- スキーマ規則
- 共通属性

サブエントリは、管理領域のルートのすぐ下に位置している。

サブクラス（subclass）

別のオブジェクト・クラスから導出されたオブジェクト・クラス。導出元のオブジェクト・クラスは、その**スーパークラス**と呼ばれる。

サブスキーマ DN（subschema DN）

独立したスキーマ定義を持つディレクトリ情報ツリー領域のリスト。

サブタイプ（subtype）

オプションを持たない同じ属性に対して、1 つ以上のオプションを持つ属性。たとえば、American English をオプションとして持つ commonName（cn）属性は、そのオプションを持たない commonName（cn）属性のサブタイプである。逆に、オプションを持たない commonName（cn）属性は、オプションを持つ同じ属性の**スーパータイプ**である。

サプライヤ（supplier）

レプリケーションにおいて、ネーミング・コンテキストのマスター・コピーを保持しているサーバー。マスター・コピーから**コンシューマ**・サーバーに更新を供給する。

参照（referral）

ディレクトリ・サーバーがクライアントに提供する情報。要求する情報を見つけるためにクライアントが接続する必要がある他のサーバーを示す。

「**ナレッジ参照**」も参照。

識別名（distinguished name: DN）

ディレクトリ・エントリの一意名。親エントリの個々の名前がすべて、下からルート方向へ順に結合されて構成されている。

思考時間（think time）

ユーザーが実際にプロセッサを使用していない時間。

システム・グローバル領域（System Global Area: SGA）

共有メモリー構造の 1 グループ。1 つの Oracle データベース・インスタンスに関するデータと制御情報が含まれている。複数のユーザーが同じインスタンスに同時に接続した場合、そのインスタンスの SGA 内のデータはユーザー間で共有される。したがって、SGA は共有グローバル領域と呼ばれることもある。バックグラウンド・プロセスとメモリー・バッファの組合せは、Oracle インスタンスと呼ばれる。

システム固有のエージェント（native agent）

Oracle Directory Integration Platform 環境において、**Directory Integration and Provisioning Server** の制御下で実行されるエージェント。**外部エージェント**と対比。

システム操作属性（system operational attribute）

ディレクトリ自体の操作に関係する情報を保持する属性。一部の操作情報は、サーバーを制御するためにディレクトリによって指定される（例 : エントリのタイムスタンプ）。アクセス情報などのその他の操作情報は、管理者が定義し、ディレクトリ・プログラムの処理時に、そのプログラムによって使用される。

従属参照（subordinate reference）

エントリのすぐ下から始まるネーミング・コンテキストの参照位置を、ディレクトリ情報ツリー内の下位方向に指し示すナレッジ参照。

上位参照（superior reference）

ディレクトリ情報ツリー内で、参照先の DSA が保持しているすべてのネーミング・コンテキストより上位のネーミング・コンテキストを保持している DSA を上位方向に指し示すナレッジ参照。

証明書（certificate）

公開鍵に対して識別情報を安全にバインドする ITU x.509 v3 の標準データ構造。証明書は、エンティティの公開鍵が、信頼できる機関（**認証局**）によって署名されたときに有効となる。この証明書は、そのエンティティの情報が正しいこと、および公開鍵がそのエンティティに実際に属していることを保証する。

証明連鎖（certificate chain）

エンド・ユーザーまたはサブスクライバの証明書とその認証局の証明書を含む、順序付けられた証明書のリスト。

信頼できる証明書（trusted certificate）

一定の信頼度を有すると認定された第三者の識別情報。信頼できる証明書は、識別情報の内容がそのエンティティと一致していることを検証するときに使用される。一般的に、信頼されている認証局によってユーザーの証明書が発行される。

スーパークラス（superclass）

別のオブジェクト・クラスの導出元のオブジェクト・クラス。たとえば、オブジェクト・クラス person は、オブジェクト・クラス organizationalPerson のスーパークラスである。後者の organizationalPerson は、person のサブクラスであり、person に含まれている属性を継承する。

スーパータイプ（supertype）

1 つ以上のオプションを持つ同じ属性に対して、オプションを持たない属性。たとえば、オプションを持たない commonName（cn）属性は、オプションを持つ同じ属性のスーパータイプである。逆に、American English をオプションとして持つ commonName（cn）属性は、そのオプションを持たない commonName（cn）属性のサブタイプである。

スーパー・ユーザー（super user）

一般的には、ディレクトリ情報へのあらゆるアクセスが可能な特別なディレクトリ管理者。

スキーマ（schema）

属性、オブジェクト・クラスおよびそれらに対応する一致規則の集合。

スケーラビリティ（scalability）

使用可能なハードウェア・リソースに応じて、そのハードウェア・リソースによってのみ制限されるシステムの機能。

スポンサ・ノード（sponsor node）

レプリケーションにおいて、新規ノードに初期データを設定するために使用されるノード。

スマート・ナレッジ参照（smart knowledge reference）

ナレッジ参照エントリが検索の有効範囲内にあるときに戻されるナレッジ参照。要求された情報を格納しているサーバーを示す。

スループット（throughput）

Oracle Internet Directory が単位時間ごとに処理する要求の数。通常、「操作 / 秒」（1 秒当りの操作件数）で表される。

スレーブ（slave）

「コンシューマ」を参照。

整合性（integrity）

受信メッセージの内容が、送信時の元のメッセージの内容から変更されていないことを保証すること。

セカンダリ・ノード（secondary node）

コールド・フェイルオーバー・クラスタ構成で、ファイルオーバー時に移動されるアプリケーションの移動先のクラスタ・ノード。

関連項目： 用語集 -22 ページの「プライマリ・ノード」

セッション鍵（session key）

1 つのメッセージまたは 1 つの通信セッションの継続時間中に使用される、対称鍵暗号方式の鍵。

接続記述子（connect descriptor）

特別にフォーマットされた、ネットワーク接続の接続先の説明。接続記述子には、宛先サービスとネットワーク・ルート情報が含まれる。

宛先サービスを示すには、その Oracle9*i* リリース 2（9.2）データベースに対応するサービス名、あるいは Oracle リリース 8.0 またはバージョン 7 のデータベースに対応する Oracle システム識別子（SID）を使用する。ネットワーク・ルートは、少なくとも、ネットワーク・アドレスによってリスナーの位置を提供する。

接続ディレクトリ（connected directory）

Oracle Directory Integration Platform 環境で、それ自体（たとえば、Oracle Human Resource データベース）と Oracle Internet Directory との間で完全なデータの同期が必要な情報リポジトリ。

相対識別名（relative distinguished name: RDN）

ローカルの最下位レベルのエントリ名。エントリのアドレスを一意に識別するために使用される他の修飾エントリ名は含まれない。たとえば、`cn=Smith,o=acme,c=US` では、`cn=Smith` が相対識別名である。

属性（attribute）

エントリの性質を説明する断片的な情報項目。1 つのエントリは 1 組の属性から構成され、それぞれが**オブジェクト・クラス**に所属する。さらに、各属性にはタイプと値があり、タイプは属性の情報の種類を説明するものであり、値には実際のデータが格納されている。

属性一意性（attribute uniqueness）

指定した 2 つの属性に同じ値が含まれていないようにする Oracle Internet Directory 機能。企業ディレクトリと同期しているアプリケーションで、属性を一意キーとして使用することを可能にする。

属性構成ファイル（attribute configuration file）

Oracle Directory Integration Platform 環境で、接続ディレクトリに関係のある属性を指定するファイル。

属性値（attribute value）

エントリで表出される情報の特定の値。たとえば、jobTitle 属性に対する値には manager がある。

属性の型（attribute type）

属性に含まれている情報の種類（例：jobTitle）。

その他の情報リポジトリ（other information repository）

Oracle Internet Directory 以外のすべての情報リポジトリ。Oracle Directory Integration and Provisioning Platform 環境では、Oracle Internet Directory が**中央ディレクトリ**として機能する。

待機時間（latency）

指定したディレクトリ操作が完了するまでのクライアントの待機時間。待機時間は、空費時間として定義される場合がある。ネットワーク通信では、待機時間は、ソースから宛先へパケットが移動する時間として定義される。

待機時間（wait time）

要求の発行から応答の開始までの時間。

単一鍵ペア Wallet（single key-pair wallet）

単一のユーザー**証明書**とその関連する**秘密鍵**が含まれる **PKCS #12** 形式の **Wallet**。**公開鍵**は証明書に埋め込まれている。

中央ディレクトリ（central directory）

Oracle Directory Integration Platform 環境で、中央リポジトリとして機能するディレクトリ。Oracle Directory Integration and Provisioning Platform 環境では、Oracle Internet Directory が中央ディレクトリになる。

データ整合性（data integrity）

受信メッセージの内容が、送信時の元のメッセージの内容から変更されていないことを保証すること。

ディレクトリ固有のエントリ（directory-specific entry: DSE）

ディレクトリ・サーバー固有のエントリ。異なるディレクトリ・サーバーに同じディレクトリ情報ツリー名を保持できるが、内容は異なる必要がある。つまり、DSE を保持しているディレクトリに固有の内容を保持できる。DSE は、それを保持しているディレクトリ・サーバーに固有の内容を含むエントリである。

ディレクトリ・サーバー・インスタンス（directory server instance）

ディレクトリ・サーバーの個々の起動のこと。異なるディレクトリ・サーバーの起動（それぞれ、同じまたは異なる構成設定エントリと起動フラグで起動）は、異なるディレクトリ・サーバー・インスタンスと呼ばれる。

ディレクトリ・システム・エージェント（directory system agent: DSA）

ディレクトリ・サーバーを表す X.500 の用語。

ディレクトリ情報ツリー（directory information tree: DIT）

エントリの DN で構成されるツリー形式の階層構造。

ディレクトリ情報ベース（directory information base: DIB）

ディレクトリに保持されているすべての情報の完全なセット。DIB は、**ディレクトリ情報ツリー**内で、階層的に相互に関連するエントリで構成されている。

ディレクトリ同期プロファイル（directory synchronization profile）

Oracle Internet Directory と外部システム間の同期の実現方法を記述した特殊な**ディレクトリ統合プロファイル**。

ディレクトリ統合プロファイル（directory integration profile）

Oracle Directory Integration Platform 環境での、Oracle Directory Integration and Provisioning Platform による外部システムとの通信方法および通信内容を示す Oracle Internet Directory のエントリ。

ディレクトリ・ネーミング・コンテキスト（directory naming context）

「**ネーミング・コンテキスト**」を参照。

ディレクトリ・プロビジョニング・プロファイル（directory provisioning profile）

Oracle Directory Integration and Provisioning Platform がディレクトリ対応アプリケーションに送信するプロビジョニング関連通知の性質を記述した特殊な**ディレクトリ統合プロファイル**。

ディレクトリ・レプリケーション・グループ（directory replication group: DRG）

レプリケーション承諾のメンバーであるディレクトリ・サーバーの集合。

デフォルト・ナレッジ参照（default knowledge reference）

ベース・オブジェクトがディレクトリになく、操作がサーバーによってローカルに保持されていないネーミング・コンテキストで実行されたときに戻される**ナレッジ参照**。デフォルト・ナレッジ参照は、一般的にディレクトリ・パーティション化対策についてより多くのナレッジを持つサーバーに送信する。

デフォルト認証管理レルム（default identity management realm）

ホスティングされた環境では、アプリケーション・サービス・プロバイダなどの 1 企業が、他の複数の企業に Oracle コンポーネントを使用可能にして、その情報を格納する。このようなホスティングされた環境では、ホスティングしている企業はデフォルト認証管理レルムと呼ばれ、ホスティングされている企業はそれぞれディレクトリ情報ツリー内のその企業独自の認証管理レルムに関連付けれる。

デフォルト・レルム位置（default realm location）

デフォルト認証管理レルムのルートを識別するルート Oracle コンテキストでの属性。

同時クライアント数（concurrent clients）

Oracle Internet Directory とのセッションを確立しているクライアントの総数。

同時実行性（concurrency）

複数の要求を同時に処理できる機能。同時実行性メカニズムの例には、スレッドおよびプロセスなどがある。

同時操作数（concurrent operations）

すべての同時クライアントの要求に基づいてディレクトリで実行されている操作の数。一部のクライアントではセッションがアイドル状態の可能性があるため、この数は同時クライアントの数と必ずしも同じではない。

特定管理領域（specific administrative area）

次の 3 つの側面を制御する管理領域。

- サブスキーマ管理
- アクセス制御管理
- 共通属性管理

特定管理領域では、この 3 つの管理の側面のうち 1 つが制御される。特定管理領域は、自律型管理領域の一部である。

匿名認証（anonymous authentication）

ディレクトリがユーザー名とパスワードの組合せを要求せずにユーザーを認証するプロセス。各匿名ユーザーは、匿名ユーザー用に指定された権限を行使する。

トラスト・ポイント（trustpoint）

「信頼できる証明書」を参照。

ナレッジ参照（knowledge reference）

リモート **DSA** に関するアクセス情報（名前とアドレス）およびそのリモート DSA が保持している **DIT** のサブツリーの名前。ナレッジ参照は、参照とも呼ばれる。

ニックネーム属性（nickname attribute）

ディレクトリ全体のユーザーを一意に識別するために使用する属性。この属性のデフォルト値は uid。アプリケーションでは、この属性を使用して単純なユーザー名が完全な識別名に変換される。ユーザー・ニックネーム属性を複数値にはできない。つまり、ユーザーは同じ属性名で格納される複数のニックネームを所有できない。

認可（authorization）

オブジェクトまたはオブジェクトのセットへのアクセスのためにユーザー、プログラムまたはプロセスに与えられる許可。

認証（authentication）

コンピュータ・システム内のユーザー、デバイスまたはその他のエンティティの識別情報を検証するプロセス。多くの場合、システム内のリソースへのアクセスを許可する前提条件として使用される。

認証管理（identity management）

組織でネットワーク・エンティティのセキュリティ・ライフ・サイクル全体を管理するプロセス。通常、組織のアプリケーション・ユーザーの管理を指す。セキュリティ・ライフ・サイクルの手順には、アカウント作成、一時停止、権限変更およびアカウント削除が含まれる。管理されるネットワーク・エンティティには、デバイス、プロセス、アプリケーション、またはネットワーク環境で対話する必要があるその他のすべてのものが含まれる。認証管理プロセスで管理されるエンティティには、組織外のユーザー（顧客、取引先、Web サービスなど）も含まれる。

認証管理レルム（identity management realm）

すべてが同じ管理ポリシーによって管理されている識別情報の集合。企業では、イントラネットへのアクセス権限を所有しているすべての従業員は 1 つのレルムに属し、企業の公開アプリケーションにアクセスするすべての外部ユーザーは別のレルムに属する。認証管理レルムは、特別なオブジェクト・クラスが関連付けられた特定のエントリでディレクトリ内に表される。

認証管理レルム固有の Oracle コンテキスト（identity management realm-specific Oracle Context）

各認証管理レルムに含まれた Oracle コンテキスト。これには、次の情報が格納されている。

- 認証管理レルムのユーザー・ネーミング・ポリシー（ユーザーに名前を付け、配置する方法）
- 必須認証属性
- 認証管理レルム内のグループの位置
- 認証管理レルムに対する権限の割当て（レルムにユーザーを追加する権限の割当てなど）
- レルムに関するアプリケーション固有のデータ（認可など）

認証局（certificate authority: CA）

他のエンティティ（ユーザー、データベース、管理者、クライアント、サーバーなど）が本物であることを証明する、信頼性できるサード・パーティ。認証局は、ユーザーの識別情報を検証し、認証局の秘密鍵を使用して署名した証明書を発行する。

ネーミング・コンテキスト（naming context）

完全に 1 つのサーバーに常駐しているサブツリー。サブツリーは連続している必要がある。つまり、サブツリーの最上位の役割を果たすエントリから始まり、下位方向にリーフ・エントリまたは従属ネーミング・コンテキストへの**ナレッジ参照**（参照とも呼ばれる）のいずれかまでを範囲とする必要がある。単一のエントリからディレクトリ情報ツリー全体までを範囲とすることができる。

ネーミング属性（naming attribute）

Oracle Delegated Administration Services または Oracle Internet Directory Java API を使用して作成した新規ユーザー・エントリの相対識別名を構成するために使用する属性。この属性のデフォルト値は cn。

ネット・サービス名（net service name）

接続記述子に変換されるサービスの単純な名前。ユーザーは、接続するサービスに対する接続文字列内のネット・サービス名に従ってユーザー名とパスワードを渡すことによって、接続要求を開始する。次に例を示す。

```
CONNECT username/password@net_service_name
```

必要に応じて、ネット・サービス名は次のような様々な場所に格納できる。

- 各クライアントのローカル構成ファイル（tnsnames.ora）
- ディレクトリ・サーバー
- Oracle Names Server
- NDS、NIS、CDS などの外部ネーミング・サービス

パーティション（partition）

一意の重複していないディレクトリ・ネーミング・コンテキスト。1 つのディレクトリ・サーバーに格納されている。

バインド（binding）

ディレクトリに対して認証を行うプロセス。

ハッシュ（hash）

アルゴリズムを使用してテキスト文字列から生成される数値。ハッシュ値は、テキスト文字列より大幅に短くなる。ハッシュの数値は、セキュリティの目的とデータに対する高速アクセスの目的で使用する。

ハンドシェイク（handshake）

2 台のコンピュータが通信セッションを開始するために使用するプロトコル。

秘密鍵（private key）

公開鍵暗号における秘密鍵。主に復号化に使用されるが、デジタル署名とともに暗号化にも使用される。

ファンアウト・レプリケーション（fan-out replication）

point-to-point レプリケーションとも呼ばれる。サプライヤがコンシューマに直接レプリケートするレプリケーションのタイプ。コンシューマは 1 つ以上の他のコンシューマにレプリケートできる。レプリケーションには、完全レプリケーションと部分レプリケーションがある。

フィルタ（filter）

データ（通常、検索対象のデータ）を限定する方法。フィルタは、`cn=susie smith,o=acme,c=us` のように常に識別名で表される。

フェイルオーバー（failover）

障害を認識し、リカバリする処理。コールド・フェイルオーバー・クラスタ構成で、1 つのクラスタ・ノード上で実行されているアプリケーションは、他のクラスタ・ノードに透過的に移行される。この移行時に、クラスタ上のサービスにアクセスするクライアントは一時的に接続できず、フェイルオーバーが完了した後、再接続する必要がある場合がある。

復号化（decryption）

暗号化されたメッセージ（暗号文）の内容を、元の可読書式（平文）に変換する処理。

プライマリ・ノード（primary node）

コールド・フェイルオーバー・クラスタ構成で、指定した時間にアプリケーションが実行されるクラスタ・ノード。

関連項目： 用語集 -16 ページの「セカンダリ・ノード」

プロキシ・ユーザー（proxy user）

通常、ファイアウォールなどの中間層を備えた環境で利用されるユーザー。このような環境では、エンド・ユーザーは中間層に対して認証を行う。この結果、中間層はエンド・ユーザーにかわってディレクトリにログインする。プロキシ・ユーザーには ID を切り替える権限があり、一度ディレクトリにログインすると、エンド・ユーザーの ID に切り替える。次に、その特定のエンド・ユーザーに付与されている認可を使用して、エンド・ユーザーのかわりに操作を実行する。

プロビジョニング・アプリケーション（provisioned applications）

ユーザーおよびグループの情報が Oracle Internet Directory に一元化される環境にあるアプリケーション。これらのアプリケーションは、一般的に Oracle Internet Directory 内の該当する情報に対する変更に関心がある。

プロビジョニング・エージェント（provisioning agent）

Oracle 固有のプロビジョニング・イベントを外部またはサード・パーティのアプリケーション固有のイベントに変換するアプリケーションまたはプロセス。

プロファイル（profile）

「ディレクトリ統合プロファイル」を参照。

平文（plaintext）

暗号化されていないメッセージ・テキスト。

変更ログ（change logs）

ディレクトリ・サーバーに加えられた変更を記録するデータベース。

マスター・サイト（master site）

レプリケーションにおいて、マスター定義サイト以外のサイトで、LDAP レプリケーションのメンバーであるサイト。

マスター定義サイト（master definition site: MDS）

レプリケーションにおいて、管理者が構成スクリプトを実行する Oracle Internet Directory のデータベース。

マッピング・ルール・ファイル（mapping rules file）

Oracle Directory Integration Platform 環境で、Oracle Internet Directory 属性と接続ディレクトリの属性との間のマッピングを指定するファイル。

マルチマスター・レプリケーション（multimaster replication）

peer-to-peer または n-way レプリケーションとも呼ばれる。同等に機能する複数のサイトがレプリケートされたデータのグループを管理できるようにするレプリケーションのタイプ。マルチマスター・レプリケーション環境では、各ノードはサプライヤ・ノードであると同時にコンシューマ・ノードであり、各ノードでディレクトリ全体がレプリケートされる。

メタディレクトリ（metadirectory）

企業のすべてのディレクトリ間で情報を共有するディレクトリ・ソリューション。すべてのディレクトリを 1 つの仮想ディレクトリに統合する。集中的に管理できるため、管理コストを削減できる。ディレクトリ間でデータが同期化されるため、企業内のデータに一貫性があり最新であることが保証される。

ユーザー検索ベース（user search base）

Oracle Internet Directory のデフォルトのディレクトリ情報ツリーで、すべてのユーザーが配置される認証管理レルムのノード。

猶予期間ログイン（grace login）

パスワード期限切れ前の指定された期間内に行われるログイン。

リモート・マスター・サイト（remote master site: RMS）

レプリケート環境における**マスター定義サイト**以外のサイトで、Oracle9*i* Advanced Replication のメンバーであるサイト。

リレーショナル・データベース（relational database）

構造化されたデータの集合。同一の列のセットを持つ 1 つ以上の行で構成される表にデータが格納される。Oracle では、複数の表のデータを容易にリンクできる。このため、Oracle はリレーショナル・データベース管理システム、すなわち RDBMS と呼ばれる。Oracle はデータを複数の表に格納し、さらに表間の関係を定義できる。このリンクは両方の表に共通の、1 つ以上のフィールドに基づいて行われる。

ルート DSE（root DSE）

ルート・ディレクトリ固有のエントリを参照。

ルート Oracle コンテキスト（Root Oracle Context）

Oracle Identity Management インフラストラクチャでは、ルート Oracle コンテキストは、インフラストラクチャのデフォルト認証管理レルムへのポインタを含む Oracle Internet Directory のエントリである。単純な名前を指定して認証管理レルムの位置を特定する方法の詳細も含まれる。

ルート・ディレクトリ固有のエントリ（root directory specific entry）

ディレクトリに関する操作情報を格納するエントリ。情報は複数の属性に格納されている。

レジストリ・エントリ（registry entry）

Oracle ディレクトリ・サーバーの起動（**ディレクトリ・サーバー・インスタンス**と呼ばれる）に関連する実行時情報が含まれているエントリ。レジストリ・エントリはディレクトリ自体に格納され、対応するディレクトリ・サーバー・インスタンスが停止するまで保持される。

レプリカ（replica）

ネーミング・コンテキストの個々のコピー。1 つのサーバー内に格納されている。

レプリケーション承諾（replication agreement）

ディレクトリ・レプリケーション・グループ内のディレクトリ・サーバー間におけるレプリケーションの関係を記述する特別なディレクトリ・エントリ。

レルム検索ベース（realm search base）

すべての認証管理レルムを含むディレクトリ情報ツリー内のエントリを識別するルート Oracle コンテキストでの属性。この属性は、単純なレルム名をディレクトリ内の対応するエントリにマッピングする際に使用される。

論理ホスト（logical host）

コールド・フェイルオーバー・クラスタ構成で、1 つ以上のディスク・グループおよびホスト名と IP アドレスのペア。論理ホストは、クラスタ内の物理ホストにマップされる。この物理ホストは、論理ホストのホスト名と IP アドレスを使用する。

索引

数字

A

B

C

D

E

G

I

J

K

L

M

N

O

P

R

S

T

U

V

W

あ

い

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

つ

て

と

な

に

ね

の

は

ひ

ふ

へ

ほ

ま

る

れ

ろ

わ