Oracle Internet Directory

管理者ガイド

リリース 9.2

2002 年 7 月

部品番号：J06304-01

ORACLE®

Oracle Internet Directory 管理者ガイド , リリース 9.2

部品番号：J06304-01

原本名：Oracle Internet Directory Administrator's Guide, Release 9.2

原本部品番号：A96575-01（Vol.1）、A96576-01（Vol.2）

原本著者：Richard Smith

原本協力者：Jeffrey Levinger, Sheryl Edwards, Tridip Bhattacharya, Ramakrishna Bollu, Saheli Dey, Bruce Ernst, Rajinder Gupta, Ajay Keni, Stephen Lee, Jeff Levinger, David Lin, Michael Mesaros, Radhika Moolky, Hari Sastry, David Saslav, Daniele Schechter, Gurudat Shakshikumar, Amit Sharma, Daniel Shih, Saurabh Shrivastava, Uppili Srinivasan, Tsai Rung-Huang, Valarie Moore

目次

2 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

第 II 部　基本的なディレクトリ管理

5　Oracle ディレクトリ・サーバーの管理

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 ディレクトリにおけるグローバリゼーション・サポート

9 属性一意性

第 III 部　ディレクトリのセキュリティ

10　ディレクトリ・セキュリティの概要

11　Secure Sockets Layer（SSL）とディレクトリ

12　ディレクトリ・アクセス制御

第 IV 部　ディレクトリの配置

13　一般的な配置の考慮事項

14　Oracle のコンポーネントと Oracle Internet Directory

15 ディレクトリ・ベースのアプリケーション・セキュリティ

16 ユーザー認証資格証明のディレクトリ格納

17 パスワード・ポリシー

18 容量計画に関する考慮事項

19 チューニングに関する考慮事項

20 高可用性とフェイルオーバーに関する考慮事項

第 V 部　ディレクトリ・レプリケーション

21 ディレクトリ・レプリケーションの概要

22 Oracle ディレクトリ・レプリケーション・サーバーの管理

23 データベース・コピー・プロシージャを使用したノードの追加

第 VI 部　ディレクトリとクラスタ

24 クラスタ構成でのフェイルオーバー

25 Oracle9*i* Real Application Clusters 環境でのディレクトリ・フェイルオーバー

第 VII 部 ディレクトリ・プラグイン

26 Oracle Internet Directory のプラグイン・フレームワーク

第 VIII 部 Oracle Directory Integration Platform

27 Oracle Directory Integration Platform の概要とコンポーネント

28 Oracle Directory Synchronization Service

29 Oracle Directory Provisioning Integration Service

30 Oracle Directory Integration Server の管理

31 Oracle Directory Integration Platform におけるセキュリティ

32 Oracle Directory Integration Platform におけるディレクトリのブートストラップ

33 Oracle Human Resources との同期化

34 iPlanet Directory Server との同期化

35 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 アクセス制御ディレクティブ書式

C スキーマ要素

D Oracle Internet Directory のアップグレード

E 他のディレクトリからのデータの移行

F LDAP フィルタ定義

G トラブルシューティング

用語集

索引

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レーション・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
- このマニュアルの構成
- 関連文書
- 表記規則

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。

表 1 に示すように、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。

表 1　各管理タスク領域に関連する項

管理タスク領域	このマニュアルの関連する項
ルーチン管理	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	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 第 VI 部 : Oracle Internet Directory およびクラスタ 第 VII 部 : Oracle Internet Directory プラグイン
Oracle Internet Directory とその他のディレクトリとの統合	第 VIII 部 : Oracle Directory Integration Platform

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「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「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・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、様々な管理ツールの使用方法について説明します。管理ツールには、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があります。

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「ディレクトリにおける グローバリゼーション・サポート」

この章では、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。

第 9 章「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 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 10 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 11 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 12 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・ポイントの概要を提供し、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 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 13 章「一般的な配置の考慮事項」

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 14 章「Oracle のコンポーネントと Oracle Internet Directory」

Oracle の多くのコンポーネントが、Oracle Internet Directory を様々な用途に使用します。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 15 章「ディレクトリ・ベースのアプリケーション・セキュリティ」

この章では、Oracle Internet Directory でのアクセス制御ポリシー・ポイントの格納方法を活用して、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について説明します。

第 16 章「ユーザー認証資格証明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「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 18 章「容量計画に関する考慮事項」

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 19 章「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 20 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 V 部 : ディレクトリ・レプリケーション

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 21 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「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 22 章「Oracle ディレクトリ・レプリケーション・サーバーの管理」

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 23 章「データベース・コピー・プロシージャを使用したノードの追加」

この章では、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。

第 VI 部 : Oracle Internet Directory およびクラスタ

第 VI 部では、Oracle Internet Directory でのクラスタのサポートについて説明します。

第 24 章「クラスタ構成でのフェイルオーバー」

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 25 章「Oracle9i Real Application Clusters 環境でのディレクトリ・フェイルオーバー」

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

第 VII 部 : Oracle Internet Directory プラグイン

第 26 章「Oracle Internet Directory のプラグイン・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 VIII 部 : Oracle Directory Integration Platform

第 VIII 部では、Oracle Directory Integration 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 27 章「Oracle Directory Integration Platform の概要とコンポーネント」

この章では、Oracle Directory Integration 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 28 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 29 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 30 章「Oracle Directory Integration Server の管理」

この章では、Oracle Directory Integration 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 31 章「Oracle Directory Integration Platform におけるセキュリティ」

この章では、Oracle Directory Integration Platform におけるセキュリティの最も重要な面について説明します。

第 32 章「Oracle Directory Integration 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 Platform の使用開始に当たって実行する必要のある初期セットアップ・タスクについて説明します。

第 33 章「Oracle Human Resources との同期化」

従業員のデータを Oracle Internet Directory に格納しており、Oracle Human Resources を使用して、このデータを作成、変更および削除する場合は、両者の間でデータが同期し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 34 章「iPlanet Directory Server との同期化」

この章では、Oracle Internet Directory integration solution for the iPlanet Directory Server を使用して、Oracle Internet Directory と iPlanet Directory Server を同期化する方法について説明します。

第 35 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 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「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 C「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 D「Oracle Internet Directory のアップグレード」

この付録では、Oracle Internet Directory リリース 2.1.1 から Oracle Internet Directory リリース 2（9.2）へアップグレードする方法について説明します。

付録 E「他のディレクトリからのデータの移行」

この付録では、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。

付録 F「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、読込み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 G「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。

関連文書

詳細は、次のマニュアルを参照してください。

- Oracle Directory Manager および Oracle Enterprise Manager から使用できるオンライン・ヘルプ。
- Oracle9*i* 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』
  - 『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』
  - 『Oracle9*i* Application Server 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、インストレーション・マニュアル、ホワイト・ペーパーまたはその他の関連文書は、OTN-J（Oracle Technology Network Japan）に接続すれば、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。次の URL で登録できます。

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

OTN-J のユーザー名とパスワードを取得済みであれば、次の OTN-J Web サイトの文書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）
- 次を初めとする Internet Engineering Task Force（IETF）のドキュメント。

- http://www.ietf.org（IETF のホームページ）
- http://www.ietf.org/html.charters/ldapext-charter.html（ldapext の Charter と LDAP Draft）
- http://www.ietf.org/html.charters/ldup-charter.html（LDUP の Charter と Draft）
- http://www.ietf.org/rfc/rfc2254.txt、『The String Representation of LDAP Search Filters』
- http://www.ietf.org/rfc/rfc1823.txt、『The LDAP Application Program Interface』

- http://www.openldap.org（OpenLDAP Community）

表記規則

このマニュアル・セットの本文とコード例に使用されている表記規則について説明します。

- 本文の表記規則
- コード例の表記規則
- Windows オペレーティング・システムの表記規則

本文の表記規則

本文中には、特別な用語が一目でわかるように様々な表記規則が使用されています。次の表は、本文の表記規則と使用例を示しています。

表記規則	意味	例
太字	太字は、本文中に定義されている用語または用語集に含まれている用語、あるいはその両方を示します。	この句を指定する場合は、**索引構成表**を作成します。
固定幅フォントの大文字	固定幅フォントの大文字は、システムにより指定される要素を示します。この要素には、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、パッケージとメソッドの他、システム指定の列名、データベース・オブジェクトと構造体、ユーザー名、およびロールがあります。	この句は `NUMBER` 列に対してのみ指定できます。 `BACKUP` コマンドを使用すると、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指定要素を示します。この要素には、コンピュータ名とデータベース名、ネット・サービス名、接続識別子の他、ユーザー指定のデータベース・オブジェクトと構造体、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があります。 **注意：**一部のプログラム要素には、大文字と小文字の両方が使用されます。この場合は、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` ファイルに指定されています。 データ・ファイルと制御ファイルのバックアップを `/disk1/oracle/dbs` ディレクトリに作成します。 `department_id`、`department_name` および `location_id` の各列は、`hr.departments` 表にあります。 初期化パラメータ `QUERY_REWRITE_ENABLED` を `true` に設定します。 `oe` ユーザーで接続します。 これらのメソッドは `JRepUtil` クラスに実装されます。

表記規則	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。*old_release* は、アップグレード前にインストールしたリリースです。

コード例の表記規則

コード例では、SQL、PL/SQL、SQL*Plus またはその他のコマンドラインを示します。次のように、固定幅フォントで、通常の本文とは区別して記載されています。

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

次の表は、コード例の記載上の表記規則とその使用例を示しています。

表記規則	意味	例
[ ]	大カッコで囲まれている項目は、1 つ以上のオプション項目を示します。大カッコ自体は入力しないでください。	DECIMAL (*digits* [, *precision*])
{ }	中カッコで囲まれている項目は、そのうちの 1 つのみが必要であることを示します。中カッコ自体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肢を区切るために使用します。オプションのうち 1 つを入力します。縦線自体は入力しないでください。	{ENABLE | DISABLE} [COMPRESS | NOCOMPRESS]
...	水平の省略記号は、次のどちらかを示します。	
	■ 例に直接関係のないコード部分が省略されていること。	CREATE TABLE ... AS *subquery*;
	■ コードの一部が繰返し可能であること。	SELECT *col1*, *col2*, ... , *coln* FROM employees;
. . .	垂直の省略記号は、例に直接関係のない数行のコードが省略されていることを示します。	SQL> SELECT NAME FROM V$DATAFILE; NAME ---------- /fs1/dbs/tbs_01.dbf /fs1/dbs/tbs_02.dbf . . . /fs1/dbs/tbs_09.dbf 9 rows selected.

表記規則	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、示されているとおりに入力してください。	`acctbal NUMBER(11,2);` `acct  CONSTANT NUMBER(4) := 3;`
イタリック	イタリックの文字は、特定の値を指定する必要のあるプレースホルダまたは変数を示します。	`CONNECT SYSTEM/`*`system_password`* `DB_NAME = `*`database_name`

大文字	大文字は、システムにより指定される要素を示します。これらの用語は、ユーザー定義用語と区別するために大文字で記載されています。大カッコで囲まれている場合を除き、記載されているとおりの順序とスペルで入力してください。ただし、この種の用語は大 / 小文字区別がないため、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を示します。
	注意：一部のプログラム要素には、大文字と小文字の両方が使用されます。この場合は、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;`

Windows オペレーティング・システムの表記規則

次の表は、Windows オペレーティング・システムの表記規則と使用例を示しています。

表記規則	意味	例
「スタート」→を選択	プログラムの起動方法。	Database Configuation 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。
ファイル名とディレクトリ名	ファイルとディレクトリ名では、大 / 小文字は区別されません。特殊文字のうち 左山カッコ（<)、右山カッコ（>)、コロン（:)、二重引用符（"）、スラッシュ（/)、パイプ（|）およびハイフン（-）は使用できません。特殊文字のうち円記号（¥）は、引用符で囲まれている場合にも要素のセパレータとして扱われます。ファイル名が¥¥で始まる場合、Windows では汎用命名規則を使用しているものとみなされます。	`c:¥winnt"¥"system32` は `C:¥WINNT¥SYSTEM32` と同じです。

表記規則	意味	例
C:¥>	現行のハード・ディスク・ドライブを示す Windows のコマンド・プロンプトを表します。コマンド・プロンプト内のエスケープ文字はカレット（^）です。プロンプトには、現在作業中のサブディレクトリが反映されます。このマニュアルでは、コマンド・プロンプトと呼んでいます。	C:¥oracle¥oradata>
特殊文字	特殊文字のうち円記号（¥）は、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必要な場合があります。カッコと一重引用符（'）には、エスケープ文字は不要です。エスケープ文字と特殊文字の詳細は、Windows オペレーティング・システムのマニュアル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 ホーム名を表します。ホーム名は、英数字で 16 文字以内です。ホーム名に使用できる特殊文字は、アンダースコアのみです。	C:¥> net start Oracle*HOME_NAME*TNSListener

表記規則	意味	例
ORACLE_HOME と *ORACLE_BASE*	Oracle8 リリース 8.0 以前では、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はデフォルトで次のいずれかの名前のトップレベルの *ORACLE_HOME* ディレクトリに置かれていました。 ■ Windows NT の場合は `C:¥orant` ■ Windows 98 の場合は `C:¥orawin98` 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。すべてのサブディレクトリがトップレベルの *ORACLE_HOME* ディレクトリにあるとはかぎりません。*ORACLE_BASE* というトップレベル・ディレクトリがあり、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最新の Oracle リリースをインストールする場合、最初の Oracle ホーム・ディレクトリのデフォルト設定は `C:¥oracle¥ora`*nn* で、*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* の直下にあります。 このマニュアルでは、すべてのディレクトリ・パスの例が、OFA の表記規則に従って示されています。	`%`*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 リリース 9.2 の概要
- Oracle Internet Directory リリース 9.0.2 で導入された新機能
- Oracle Internet Directory リリース 3.0.1 で導入された新機能
- Oracle Internet Directory リリース 2.1.1 で導入された新機能

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、Delegated Administration Service とそのツールが Oracle9*i* Application Server のコンポーネントとなっています。このリリースの Oracle Internet Directory からは、Oracle9*i* データベース・サーバーと併用するための Delegated Administration Service が付属していません。Web アプリケーションと Oracle9*i* Application Server アプリケーションの管理には、Oracle9*i* Application Server に付属の Oracle Internet Directory を使用することをお薦めします。これにより、Delegated Administration Service ベースのツールなど、自己管理ツールを使用してディレクトリ配置をサポートできます。また、これらのツールが中間層環境と確実に統合されます。同様に、Delegated Administration Service ベースのツールの開発と配置には、Oracle9*i* 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： 19-11 ページ「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 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 27 章「Oracle Directory Integration 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 を改善した、より複雑なバージョンです。
  - **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、10-7 ページ「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 17 章「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、この識別名は ou=people の直下で一意でした。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。

Oracle Internet Directory と同期化するアプリケーションでは、識別名以外の属性を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、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。

- **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「ユーザー認証資格証明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 Oracle9*i* 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 10 章「ディレクトリ・セキュリティの概要」
  - 5-21 ページ「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」

- **Oracle9*i* 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 Oracle9*i* Application Server の中央コンポーネントとして機能します。Oracle9*i* 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 14 章「Oracle のコンポーネントと Oracle Internet Directory」

- **Oracle Enterprise Manager（OEM）の統合**－新しく拡張された標準の Enterprise Manager Console 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： 5-26 ページ「ディレクトリ・サーバーの監視、デバッグおよび監査」

- **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。
  - ホスト・サブスクライバ・ドメインの構成
  - 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

  高水準の Oracle Enterprise Manager の Graphical User Interface（GUI）では使用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・タスクが、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 26 章「Oracle Internet Directory のプラグイン・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： 5-36 ページ「別名エントリの間接参照」

- **Delegated Administration Service の拡張**

  Delegated Administration Service は、Delegated Administration Service ユニットと呼ばれる個々の事前定義済み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、Delegated Administration Service 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・コンソールーこれは、Delegated Administration Service 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、サブスクライバおよびエンド・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 Oracle9*i*AS 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。

- **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。

  関連項目： 付録 D「Oracle Internet Directory のアップグレード」

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。

- **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： 13-12 ページ「1 つのホストにおける複数の Oracle Internet Directory インストールの実行」

- **Delegated Administration Service**

  この新しいサービスによって、ディレクトリのユーザーは、管理者を介さずに、各自の個人データ（住所、電話番号、写真など）を変更できます。また、アクセス権限のあるディレクトリの他の部分を検索することもできます。これによって、ディレクトリ管理者は企業内の他のタスクを遂行できるようになります。

  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 24 章「クラスタ構成でのフェイルオーバー」

- **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 25 章「Oracle9i Real Application Clusters 環境でのディレクトリ・フェイルオーバー」

- **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。

- **Oracle Directory Integration 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 VIII 部：「Oracle Directory Integration 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：

  - 概念の説明は、「パスワード・ポリシー」を参照してください。
  - 第 17 章「パスワード・ポリシー」

- **パフォーマンスと拡張性の強化**
- **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。

  関連項目： 付録 D「Oracle Internet Directory のアップグレード」

- **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：

  - 概念の説明は、2-8 ページの「属性オプション」を参照してください。
  - 7-11 ページ「Oracle Directory Manager を使用した属性オプション付きエントリの管理」
  - 7-15 ページ「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：

  - 概念の説明は、21-6 ページの「変更ログの削除」を参照してください。
  - 22-12 ページ「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」

- **次の操作属性の拡張サポート**

  - **creatorsName**
  - **createTimestamp**
  - **modifiersName**
  - **modifyTimestamp**

  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：

  - 概念の説明は、2-5 ページの「属性情報の種類」を参照してください。
  - `createTimestamp` 属性を使用した検索操作の例は、A-23 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： 付録 E「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る場合に役立ちます。

  関連項目： A-56 ページ「OID データベース統計収集ツール」

- **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 を改善した、より複雑なバージョンです。
  - **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：

  - 概念の説明は、10-7 ページ「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 17 章「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：

    - このツールの簡単な説明は、4-13 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。
    - 22-30 ページ「管理者操作キュー操作ツールの使用」
    - 22-30 ページ「OID 調停ツールの使用」

- **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： 22-26 ページ「レプリケーション・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 Platform に置き換えられました。詳細は、第 27 章「Oracle Directory Integration 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。

  関連項目： 付録 D「Oracle Internet Directory のアップグレード」

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。

1

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
- LDAP とは
- Oracle Internet Directory とは
- Oracle 製品における Oracle Internet Directory の使用方法

ディレクトリとは

ディレクトリは、複雑な情報を簡単に検索できるように編成します。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。コンピュータ以外の場面（オフライン）で使用しているディレクトリの例としては、電話帳や図書館のカード目録、百貨店のカタログなどがあります。

分散コンピュータ・システムを持つ企業は、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オンライン・ディレクトリを使用しています。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。

この項では、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 : 特別な用途を指定された多数のディレクトリ

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・アプリケーションが、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。

オンライン・ディレクトリ	リレーショナル・データベース
主に読込み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。
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・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 : 特別な用途を指定された多数のディレクトリ

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、複数の場所に格納された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 : 個別の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。

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 バージョン 3

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（参照とも呼ばれます）: 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（DIT）**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）**および **Transport Layer Security（TLS）**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広範囲でかつ拡張可能なフレームワークが提供されています。
- 拡張性 : 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/rfc.html`
- LDAP に関する参考資料のその他のリストは、xxxv ページの「関連文書」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「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、拡張性、耐久性および可用性を組み合せたものです。

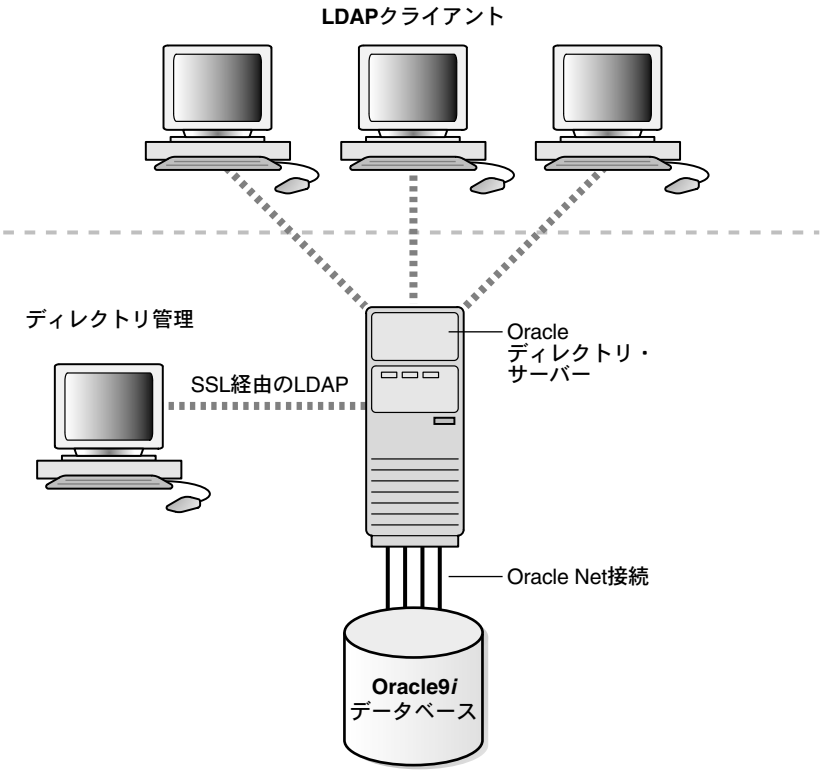
この項では、次の項目について説明します。

- Oracle Internet Directory のアーキテクチャ
- Oracle Internet Directory のコンポーネント
- Oracle Internet Directory の利点

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 はこの関係を示しています。

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。
  - OID サーバー・インスタンスを管理する Oracle Enterprise Manager の Web ベース・インタフェース内のツール。管理者は、これらのツールを使用して標準的なブラウザからリアルタイム・イベントや統計を監視でき、必要な場合は、これらの今後のデータを新しい履歴リポジトリに収集するプロセスを開始できます。
- Oracle Directory Integration Platform（Oracle Directory Integration Server を含む）。これを使用して、接続ディレクトリやサブスクライブしたアプリケーションを Oracle Internet Directory と同期化できます。Oracle Directory Integration Platform を使用して独自の接続エージェントを開発し、配置することもできます。

関連項目： 第 VIII 部「Oracle Directory Integration Platform」

Oracle Internet Directory の利点

Oracle Internet Directory の大きな利点は、拡張性、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。

拡張性

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 レプリケーション（Oracle9i 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、すべての Oracle 製品で使用されています。Oracle Internet Directory は、Oracle Directory Integration 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 製品における Oracle Internet Directory の使用方法

Oracle Internet Directory によって、Oracle のコンポーネントは、簡単で対費用効果の高いアプリケーション環境の管理、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、および企業の各分散ディレクトリ間での統合ポイントを実現できます。この項では、例を示して説明します。

簡単で対費用効果の高い管理

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。ネット・サービス名は、クライアントの接続文字列内で接続識別子として機能します。ディレクトリ・サーバーは、これらの接続識別子を接続記述子に変換し、クライアントに戻します。

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

- サーバーの構成情報、電子メール固有のユーザー作業環境およびユーザーが記録したボイスメールの挨拶の保存と取得
- 電子メール受信者リストの検証
- 電子メール配布リストの表示と管理
- ランタイム・パラメータの保存（その結果、Oracle Unified Messaging 管理者は分散インストールを容易に管理できます）

統合されたセルフ・サービスのエンタープライズ・ポータル（**Oracle9*i*AS Portal** を使用）は、Oracle Internet Directory にアクセスして共通のユーザー属性とグループ属性を格納します。

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、ユーザーを SSL ではなく LDAP メカニズムを使用して認証します。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 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、単一の集中管理された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は、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です。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* 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が透過的です。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、再度認証せずにアクセスできます。

Oracle9*i*AS 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。

分散ディレクトリの統合

Oracle Directory Integration Platform は、Oracle Internet Directory を中央ディレクトリとして使用することで、複数のディレクトリを統合するためのインタフェースとサービスの集合です。

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

- Oracle のすべてのコンポーネントは、あらかじめ Oracle Internet Directory に統合されているため、ユーザーが各コンポーネントをディレクトリ・サービスに統合する必要はありません。
- 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。各アプリケーションを各ディレクトリに時間をかけて統合する必要はありません。

2

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。

- 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
- ディレクトリ・スキーマ
- セキュリティ
- グローバリゼーション・サポート
- Oracle Internet Directory のアーキテクチャ
- 例 : Oracle Internet Directory の動作
- 分散ディレクトリ
- Oracle Directory Integration Platform
- Oracle コンポーネントと Oracle Internet Directory

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、xxxv ページの「関連文書」を参照してください。

エントリ

ディレクトリ内のオブジェクトに関する情報の各集合は**エントリ**と呼ばれます。たとえば、一般的な電話帳には個人に関するエントリ、図書館のカード式目録には本に関するエントリが含まれています。同様に、オンライン・ディレクトリには、従業員、会議室、E-Commerce パートナまたはプリンタなどの共有ネットワーク・リソースに関するエントリなどが含まれています。

オンライン・ディレクトリ内の各エントリは、**識別名（DN）**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（DIT）**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

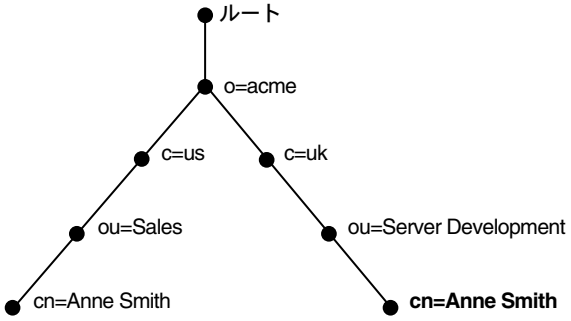


図 2-1 のディレクトリ情報ツリーは、どちらも Acme Corporation に所属する、Anne Smith という名前の 2 人の従業員のエントリを図示しています。この図のディレクトリ情報ツリーは、地理的および組織的な系統に従って構造化されています。左の分岐で表されている Anne Smith は米国の Sales 部門に勤務し、もう一方の Anne Smith は英国の Server Development 部門に勤務しています。

右の分岐で表されている 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（RDN）**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。識別名は、このように各相対識別名をカンマで区切って順に並べたものです。

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）。

エントリに対して迅速で効率的な操作を行うために、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。エントリ・キャッシングと呼ばれるこの方法によって、Oracle Internet Directory のパフォーマンスが強化されます。比較的小規模または中規模の企業では特に有用です。

注意： Oracle Internet Directory リリース 9.2 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。

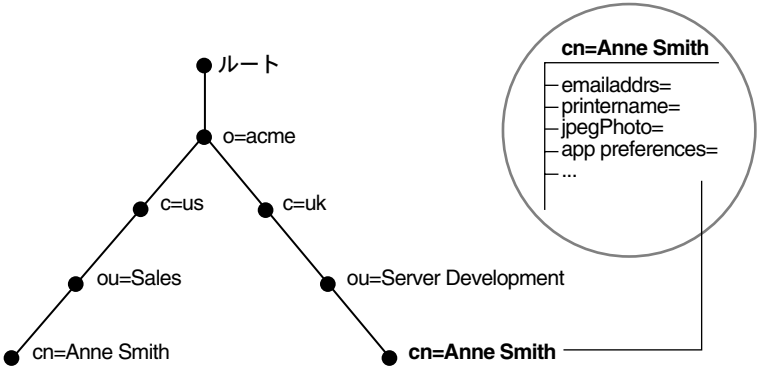
関連項目： 第 7 章「ディレクトリ・エントリの管理」

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
- 属性オプション

属性情報の種類

属性には 2 種類の情報があります。

- アプリケーション情報

  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。

- 操作情報

  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。操作情報は、**ルート・ディレクトリ固有のエントリ**に格納されます。

指定したどの属性にもアプリケーション情報または操作情報のいずれかを保持できますが、両方保持することはできません。

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`	エントリの作成者の名前
`modifyTimestamp`	UTC でのエントリの作成時間

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、5-14 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、一般的な LDAP 属性のいくつかを示します。

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。エントリの属性として組み込む JPEG イメージのパスとファイル名（`/photo/audrey.jpg` など）。
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）。
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 が用意している専用の属性のリストは、付録 C「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、RFC 2252 で指定されている構文のほとんどを認識するため、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、RFC 2252 構文の認識に加え、一部の LDAP 構文を適用します。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： C-6 ページ「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： C-9 ページ「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、cn;lang-fr=Jean では、基本属性は cn であり、この基本属性のフランス語の値は cn;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 cn;lang-fr=Jean が、cn 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、次の識別名は不適切です。cn;lang-fr=Jean, ou=sales,o=acme,c=uk

---

関連項目：

- 7-11 ページ「Oracle Directory Manager を使用した属性オプション付きエントリの管理」
- 7-15 ページ「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すが、それ以外の属性はオプションです。

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。

インストール時には、いくつかの専用オブジェクト・クラスと同様に、標準的な LDAP オブジェクト・クラスを Oracle Internet Directory が用意します。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。

- 既存のオブジェクト・クラスへのオプション属性の追加
- 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 C「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。

- サブクラス、スーパークラスおよび継承
- オブジェクト・クラスの型

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。導出元のオブジェクト・クラスは、その**スーパークラス**と呼ばれています。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。各エントリは、複数のオブジェクト・クラスによって定義された属性を継承できます。

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フレームワークのみ継承し、属性値は継承しません。

---

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構造型オブジェクト・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。

- 抽象型
- 構造型
- 補助型

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**の次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（ACL）**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・ポイント

関連項目： アクセス制御ポリシー・ポイントおよび ACL の詳細は、2-14 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。

構造型オブジェクト・クラス

これらのオブジェクト・クラスは、構造規則を使用して、指定したオブジェクト・クラスの下に作成可能なオブジェクト・クラス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・クラスの下に直接入力できません。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、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。たとえば、あるエントリを 2 つのオブジェクト・クラスのメンバーとして定義し、そのエントリに、これら 2 つのオブジェクト・クラスに属していない追加属性を割り当てるとします。この場合、その追加属性を含んだ補助型オブジェクト・クラスを新たに作成して、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。これは、既存のオブジェクト・クラスを再定義せずに属性を追加する 1 つの方法です。

構造型オブジェクト・クラスとは異なり、補助型クラスではエントリの格納位置は制限されません。

注意： Oracle Internet Directory は、構造規則を強制していません。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。

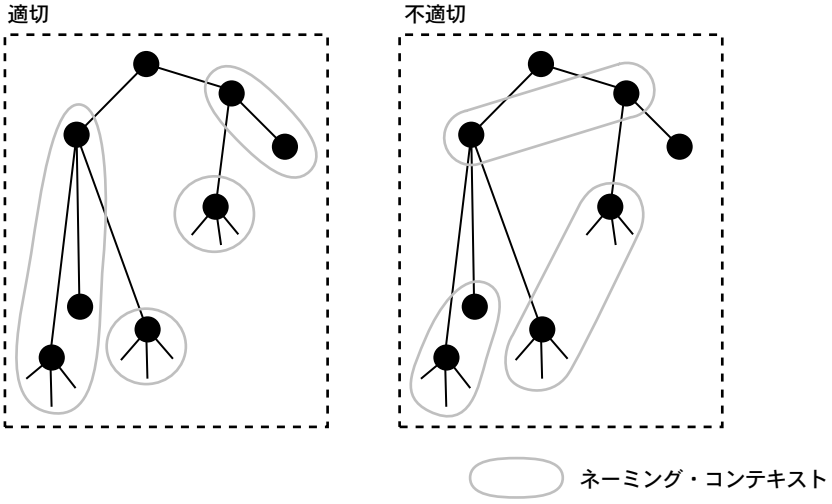
関連項目： 第 6 章「ディレクトリ・スキーマの管理」

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。サブツリーは連続している必要があります。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 は、有効なネーミング・コンテキストと無効なネーミング・コンテキストを示しています。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 有効なネーミング・コンテキストと無効なネーミング・コンテキスト



ユーザーが特定のネーミング・コンテキストを検索できるようにするには、Oracle Directory Manager または ldapmodify を使用して、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、5-20 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。

ディレクトリ・スキーマ

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。ディレクトリ・スキーマはこの情報を、**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します。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スキーマ定義を保持します。

`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。

関連項目：

- 第 6 章「ディレクトリ・スキーマの管理」
- Oracle Internet Directory でインストールされる標準および専用のスキーマ要素のリストは、付録 C「スキーマ要素」を参照してください。

セキュリティ

Oracle Internet Directory は、情報保護のための強力な機能を提供します。たとえば次のようなものです。

- データ整合性 : 送信中にデータが変更されないことを保証します。
- データ・プライバシ : 送信中にデータが不適切に検出されないことを保証します。
- 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込み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 : パスワードのセキュリティを保証します。

さらに重要なことは、企業やホスティングされた環境では、これらの機能すべてを使用してアプリケーションのメタデータへのアクセスを制御できるという点です。このメタデータとは、アプリケーションの動作とアクセスできるユーザーを制御するための情報です。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 10 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。

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・サポートでは、シングルバイト文字とマルチバイト文字の双方を使用します。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・エントリは次のようになります。

```
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、簡体字中国語キャラクタ・セットの文字列に相当します。

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 Server（ODISRV）は、常にデフォルトで 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）。

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。Java では、UCS-2 が文字（英文字を含む）を処理する最も簡単な方法です。Java クライアントは、標準的な Java パッケージを使用して UCS-2 と UTF-8 を相互に変換します。この変換機能によって、Oracle Directory Manager は、UTF-8 を使用する LDAP バージョン 3 のプロトコルを処理できます。

関連項目：

- Oracle Internet Directory の主なコンポーネントの詳細は、2-15 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 のグローバリゼーション・サポートの使用方法は、第 8 章「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、『Oracle9*i* Database グローバリゼーション・サポート・ガイド』を参照してください。

注意： 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。

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 ディレクトリ・サーバー・インスタンス
- 構成設定エントリ

Oracle Internet Directory のノード

2-16 ページの図 2-4 は、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ています。

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。

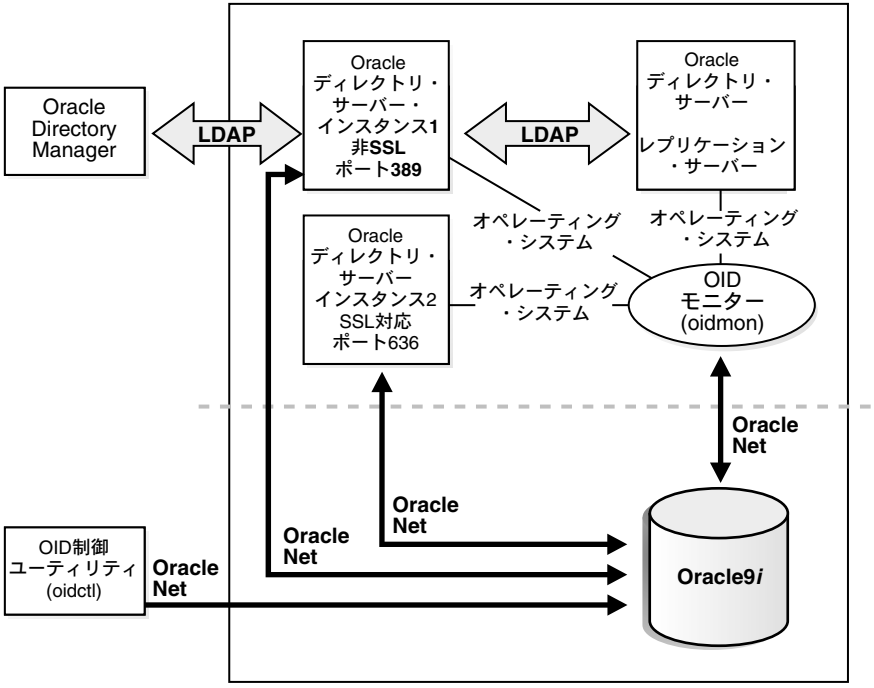
- **OID 制御ユーティリティ**
- Oracle ディレクトリ・サーバー・インスタンス 1 非 SSL ポート 389
- Oracle ディレクトリ・サーバー・インスタンス 2SSL 対応ポート 636
- **OID モニター**

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



注意： 図 2-4 のデータベースは、ディレクトリ・サーバー・プロセスと同じノードにあります。しかし、データベースとの接続はすべて、**Oracle Call Interface（OCI）**と **Oracle Net Services** を介するため、別のサーバー上のデータベースを使用できます。

Oracle Internet Directory のノード（図 2-4）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	LDAP 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ます。ディレクトリ・サーバー・インスタンスは、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、ディレクトリの要求に応答します。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。 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。
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ます。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・サーバーをインストールして使用するかどうかは選択できます。
Oracle9*i* データベース	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、サーバーと同じノードにも別のノードにも常駐できます。

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

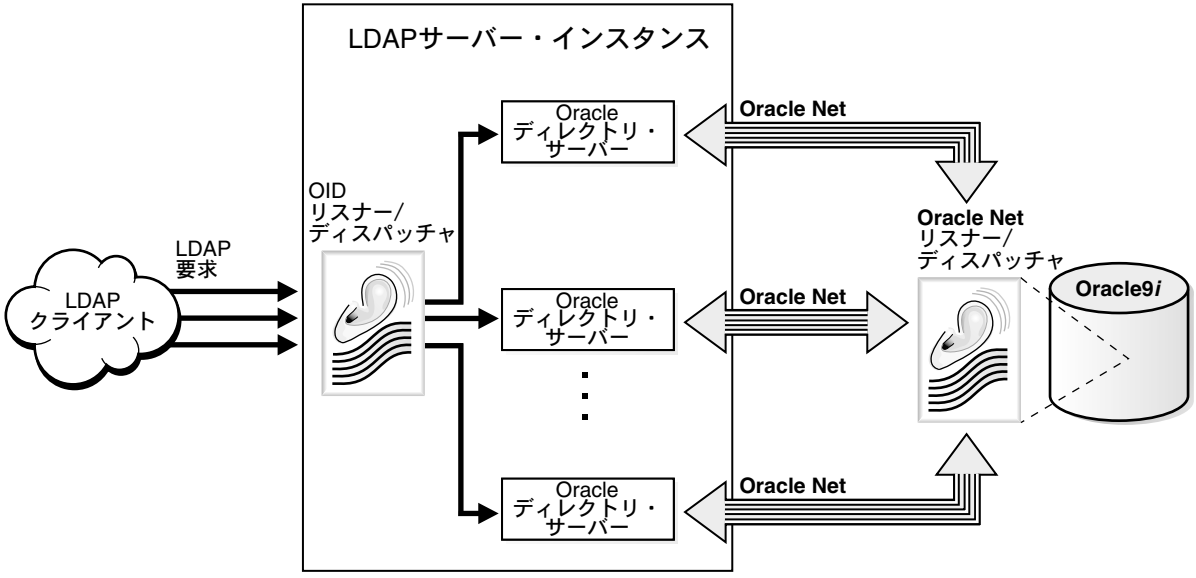
コンポーネント	説明
OID モニター（OIDMON）	LDAP のサーバー・プロセスを開始、モニターおよび終了します。レプリケーション・サーバーをインストールすると、OID モニターがこれを制御します。OID 制御ユーティリティ（OIDCTL）を使用してディレクトリ・サーバー・インスタンスを起動または停止するコマンドを発行すると、そのコマンドはこのプロセスによって解釈されます。 OID モニターは、管理者が OID 制御ユーティリティで行う LDAP サーバー・インスタンスの起動と停止の要求を処理します。また、OID モニターはサーバーを監視し、例外的な理由で実行が停止した場合に再起動させます。 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



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。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。各操作のワーカー・スレッドが、それぞれクライアント要求を処理します。

構成パラメータ `ORCLMAXCC` に設定した数値によって、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。

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）と呼ばれるディレクトリ・エントリに格納されます。構成設定エントリは、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 configset 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。特定のパラメータを変更した新しい構成設定エントリを必要に応じて追加することによって、カスタマイズされた構成設定エントリを作成できます。このエントリを表示、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「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、C-5 ページの「構成設定エントリの属性」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・サーバーが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、物理的にはそのデータを複数のサーバーに分散できます。これによって、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、ディレクトリに多数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、各ディレクトリ・サーバーには、他と重複しないネーミング・コンテキストが 1 つ以上格納されます。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。

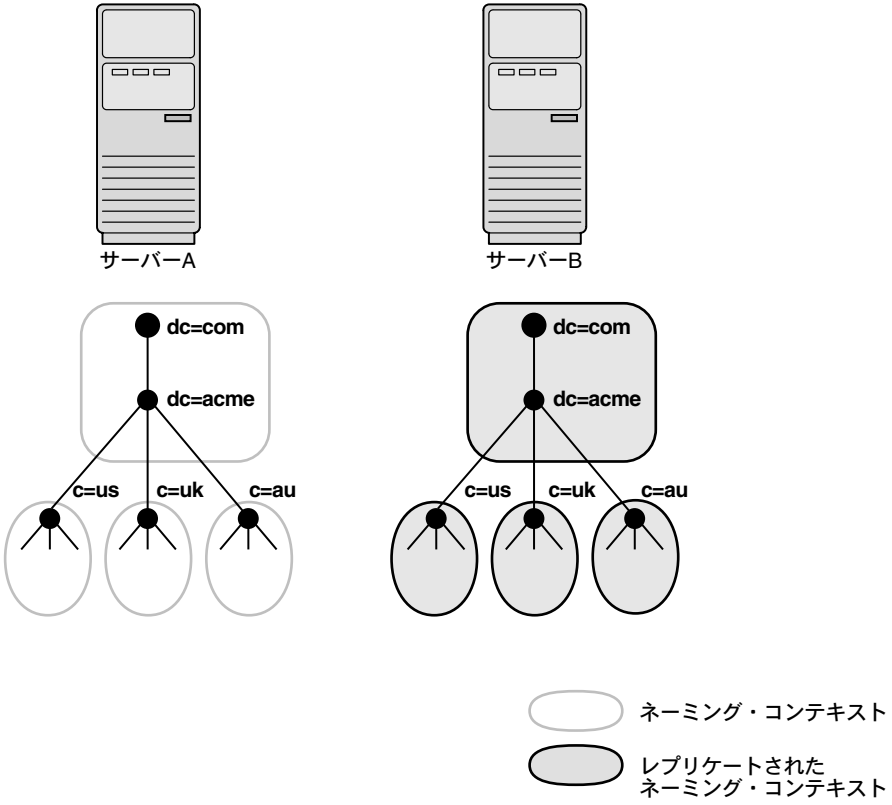
- レプリケーション
- パーティション化
- ナレッジ参照と参照
- 参照の種類

レプリケーション

レプリケーションでは、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、より多くのサーバーを使用して問合せを処理することによってパフォーマンスが向上します。また、ある箇所で発生した障害から派生するリスクを排除できるため信頼性が向上します。

図 2-6 は、レプリケート・ディレクトリを示しています。

図 2-6 レプリケート・ディレクトリ



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。ディレクトリ・サーバーには、読取り専用レプリカと更新可能レプリカの両方を保持できます。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。

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

トリに更新を送信したとします。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。

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。

関連項目： レプリケーションの詳細は、第 21 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* レプリケーションのアーキテクチャ、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。

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 は、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ています。

図 2-7 パーティション化されたディレクトリ

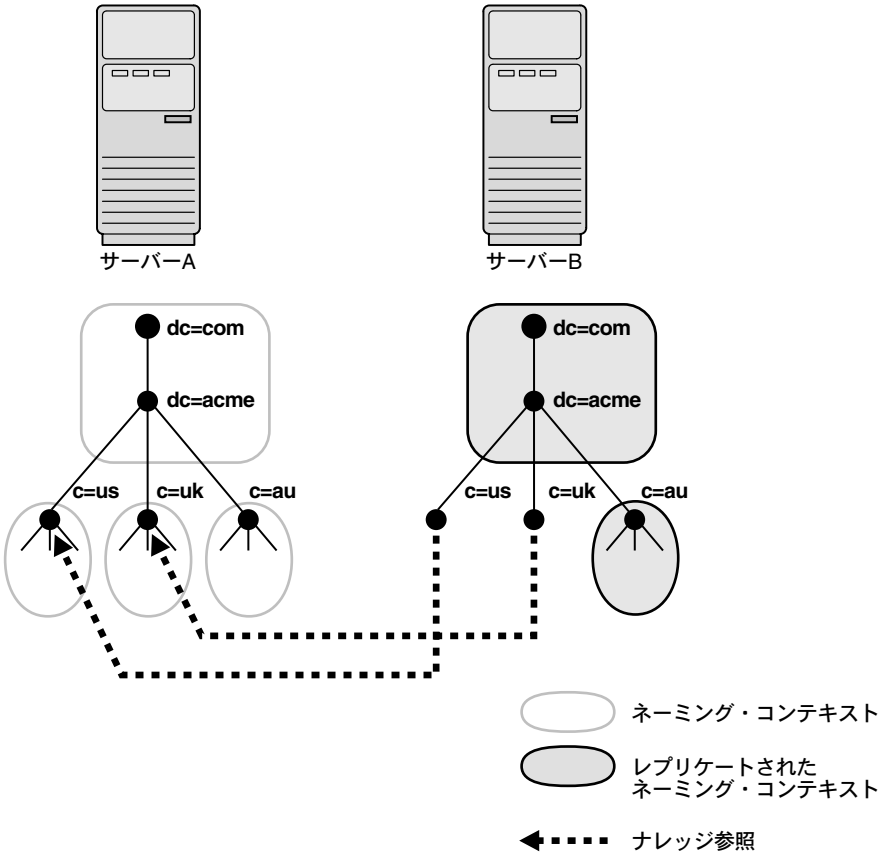


図 2-7 では、サーバー A に次の 4 つのネーミング・コンテキストが常駐しています。

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

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

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。

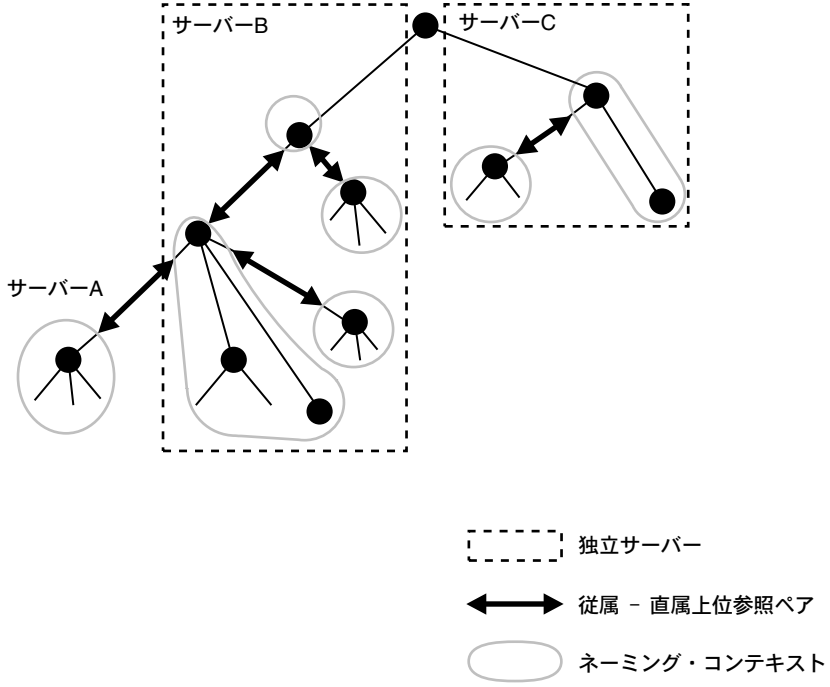
ナレッジ参照と参照

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。図 2-7 のサーバー B は、ナレッジ参照を使用して、サーバー A の c=us と c=uk のネーミング・コンテキストを指し示します。クライアントがサーバー A に常駐している情報をサーバー B に要求すると、サーバー B は、サーバー A への 1 つ以上の参照をクライアントに提供します。その後、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。上位ナレッジ参照によって、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を指し示します。

たとえば、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。

参照の種類

参照には次の 2 つの種類があります。

- スマート参照

  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

  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。デフォルト参照は通常、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： 7-21 ページ「ナレッジ参照と参照の管理」

Oracle Directory Integration Platform

Oracle Directory Integration Platform を使用すると、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。

この項では、次の項目について説明します。

- メタディレクトリ
- Oracle Directory Integration Platform 環境

メタディレクトリ

今日の企業では、ERP システム、データベース・アプリケーション、メッセージ・システムおよびネットワーク・オペレーティング・システム（NOS）などのアプリケーションに関する情報を格納するため、複数のディレクトリを配置することが多くなっています。異なるディレクトリを数多く管理していると、次のような問題が発生します。

- コストの増大－複数の管理者が、複数の場所に格納された同じ情報をメンテナンスする必要があります。
- 一貫性のないデーターあるディレクトリで更新された情報を他のすべてのディレクトリで使用できません。

メタディレクトリは、1 つの仮想ディレクトリを構成し、すべての企業ディレクトリ間で情報を同期化することで、これらの問題を解決します。メタディレクトリでは中央での集中管理を行うため、管理コストを低減でき、企業全体にわたってデータに一貫性を持たせて最新の状態にしておくことができます。

メタディレクトリ環境では、たとえば各従業員ごとにグローバル・ディレクトリ・エントリを作成できます。このエントリには、人事管理アプリケーション、メッセージ・システムまたは NOS データベースなど、様々な同期化されたディレクトリからのデータを移入できます。ユーザーは、各**接続ディレクトリ**と同期化された最新のデータを含むものとして、このグローバル・エントリにアクセスできます。

また、同期化プロセスでは、既存のすべてのデータ所有権ポリシーが遵守されていることを確認できます。たとえば、従業員の給与属性の値を変更する権限を、人事部門のみに付与することができます。

Oracle Directory Integration Platform 環境

Oracle Directory Integration Platform によって、企業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。このプラットフォームは、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。

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（Oracle9*i*AS Portal など）が配置されている可能性もあります。このサービスはプロビジョニングと呼ばれ、Oracle Directory Integration Platform は、それらのアプリケーションに必要な通知を提供します。

統合の特性に基づいて、Oracle Directory Integration 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 － 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 － ユーザーのステータスまたは情報に対する変更を反映するために、定期的にターゲット・アプリケーションに通知を送信します。

関連項目： 第 VIII 部 :「Oracle Directory Integration Platform」

Oracle コンポーネントと Oracle Internet Directory

Oracle Internet Directory により、Oracle コンポーネントでは次の作業が可能になります。

- 複数のアプリケーション環境で、ユーザーごとに単一のグローバル ID をメンテナンスできます。
- コンポーネントの構成情報を中央に格納して管理できます。

環境には、次の 2 つの一般的なタイプがあります。

- ホスティングされた環境－このタイプの環境では、アプリケーション・サービス・プロバイダなどの 1 つの企業が、他の複数の企業による Oracle コンポーネントの使用を可能にして、その情報を格納します。このようにホスティングされた環境では、ホスティングを行う企業はデフォルト・サブスクライバと呼ばれ、ホスティングされる企業はサブスクライバと呼ばれます。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します。この他に、**委任管理者**と呼ばれる管理者がいる場合があります。このタイプの管理者は、特定のサブスクライバ・ドメインで、または特定のアプリケーションに対するロールを実行します。
- ホスティングされていない環境－このタイプの環境にはサブスクライバはいません。Oracle コンポーネントとともに使用するために Oracle Internet Directory をインストールする企業が、デフォルト・サブスクライバと呼ばれます。

Oracle Internet Directory を使用する Oracle コンポーネントの使用を簡単に開始できるように、Oracle Internet Directory のインストール中に、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。このデフォルトの DIT フレームワークは、環境がホスティングされるかどうかにかかわらず同じです。また、このフレームワークは柔軟であるため、配置のニーズに合せて変更できます。

Oracle Internet Directory のインストール中に、Oracle Universal Installer によって次のものが作成されます。

- ベース・スキーマ要素。属性とオブジェクト・クラスです。Internet Engineering Task Force（IETF）によって定義されているものと、Oracle コンポーネントに固有のものがあります。
- ルート Oracle コンテキスト。サイト全体のすべての Oracle コンポーネントに共通する情報のディレクトリ・コンテナです。
- デフォルト・サブスクライバの Oracle コンテキスト。サブスクライバのサブツリーにあるすべての Oracle コンポーネントに共通する情報が含まれます。
- サブスクライバの Oracle コンテキスト。サブスクライバのサブツリーにあるすべての Oracle コンポーネントに共通する情報が含まれます。
- 各サブスクライバのデフォルトのパスワード・ポリシー。このパスワード・ポリシーは、サブスクライバ・ユーザー・ベースで全ユーザーに適用されます。

関連項目：

Oracle コンポーネントで Oracle Internet Directory を使用する方法およびデフォルト・スキーマと DIT の詳細は、第 14 章「Oracle のコンポーネントと Oracle Internet Directory」を参照してください。

Oracle コンポーネントを使用する環境のセキュリティ構成など、Oracle Internet Directory とともにインストールされるセキュリティ構成の詳細は、3-10 ページの「タスク 3: デフォルト・セキュリティ構成の再設定」を参照してください。

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。

この章では、次の項目について説明します。

- タスク 1: OID モニターの開始
- タスク 2: サーバー・インスタンスの起動
- タスク 3: デフォルト・セキュリティ構成の再設定
- 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
- タスク 5: OID データベース統計収集ツールの実行
- ログ・ファイルの位置

タスク 1: OID モニターの開始

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。

注意： OID モニターおよび OID 制御ユーティリティを使用せずにディレクトリ・サーバーを起動することも可能ですが、オラクル社ではこれらを使用することをお薦めします。これによって、ディレクトリ・サーバーが予期せずに停止しても、OID モニターが自動的にディレクトリ・サーバーを起動します。

この項では、次の項目について説明します。

- OID モニターの開始
- OID モニターの停止

OID モニターの開始

OID モニターを開始する手順は、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。
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=net_service_name] [sleep=seconds] start
```

引数	説明
`connect=net_service_name`	接続するデータベースのネット・サービス名を指定します。`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。
`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。

次のようなコマンドを実行します。

```
oidmon connect=dbs1 sleep=15 start
```

OID モニターの停止

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=net_service_name] stop
```

引数	説明
connect=*net_service_name*	接続するデータベースのネット・サービス名を指定します。tnsnames.ora ファイルに設定されているネット・サービス名です。
stop	OID モニターのプロセスを停止します。

次のようなコマンドを実行します。

```
oidmon connect=dbsl stop
```

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、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。

注意： ディレクトリ・サーバーが同じマシン上にある場合は、複数インスタンスを実行できます。たとえば、サーバーの一方を SSL モードで実行し、他方を非 SSL モードで実行できます。ただし、特定のデータベース・サーバーを使用するディレクトリ・サーバー・インスタンスは、すべて同じコンピュータ上で実行する必要があります。たとえば、コンピュータ C のデータベース・サーバーに対して、2 つのディレクトリ・サーバーを、一方はコンピュータ A で、他方はコンピュータ B で実行することはできません。ただし、両方のディレクトリ・サーバーがコンピュータ A にあれば、その 2 つをコンピュータ B のデータベース・サーバーに対して実行できます。

注意： OID 制御ユーティリティのインスタンス・フラグの値は、常に 1 以上に設定してください。

この項では、次の項目について説明します。

- Oracle 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・インスタンスの停止
- 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・インスタンスの停止
- ディレクトリ・サーバー・インスタンスの再起動
- 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・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=net_service_name server=oidldapd instance=server_instance_number
[configset=configset_number] [flags=' -p port_number -work maximum_number_of_worker_
threads_per_server -debug debug_level -l change_logging' -server number_of_server_
processes] start
```

引数	説明
`connect=net_service_name`	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=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。
`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。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。
`-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。
`-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。
`-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。

引数	説明
`-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。
`-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。
`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

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ときは、常に OID モニターが実行中であることが必要です。

コマンド・プロンプトで、次のコマンドを入力します。

```
oidctl connect=net_service_name server=OIDLDAPD instance=server_instance_number stop
```

次のようなコマンドを実行します。

```
oidctl connect=dbs1 server=oidldapd instance=3 stop
```

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=net_service_name 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
```

引数	説明
connect=*net_service_name*	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。

引数	説明
-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*]	競合の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

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ときは、常に OID モニターが実行中であることが必要です。

コマンド・プロンプトで、次のコマンドを入力します。

```
oidctl connect=net_service_name server=OIDREPLD instance=server_instance_number stop
```

次のようなコマンドを実行します。

```
oidctl connect=dbs1 server=oidrepld instance=1 stop
```

ディレクトリ・サーバー・インスタンスの再起動

OID モニターと OID 制御ユーティリティを使用している場合は、ディレクトリ・サーバーの停止と再起動を 1 つのコマンド `restart` で実行できます。予定のリフレッシュ時刻を待たず、サーバーのキャッシュを即時にリフレッシュする場合は、この方法が便利です。再起動したディレクトリ・サーバーは、停止前と同じパラメータを保持しています。再起動コマンドに新しいパラメータを指定して、既存のパラメータを変更することはできません。

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=net_service_name server={oidldapd|oidrepld}
instance=server_instance_number  restart
```

ディレクトリ・サーバー・インスタンスを起動、停止または再起動するときは、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。

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、ユーザーがディレクトリ・サーバーを起動するために指定した構成パラメータをすべてオーバーライドし、ハードコードされたデフォルト・パラメータを使用して、構成設定を使用可能な状態に戻すことができます。このオプションは、LDAP サーバーにデフォルトの configset（`configset=0`）を用意できない場合にのみ使用してください。

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=net_service_name server=oidldapd instance=1 flags='-p port_number -f'
```

フラグ内に `-f` オプションを指定すると、定義済みの構成設定が `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。

タスク 3: デフォルト・セキュリティ構成の再設定

Oracle Internet Directory は、この項で後述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。最初に、環境のニーズに対応し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受け取るようにする必要があります。

サブエントリ subSchemaSubEntry とその子オブジェクトにはディレクトリに関する情報が格納されているため、オラクル社では、これらに対するアクセスを制御することを特にお薦めします。

また、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込み、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

デフォルトのアクセス・ポリシー

初めてインストールした Oracle Internet Directory のデフォルトの構成では、ディレクトリ情報ツリー内の様々なポイントで次のポリシーが設定されています。

ルート DSE でのデフォルトのアクセス・ポリシー

- すべてのユーザーには、エントリの参照権限があります。
- ユーザー・セキュリティ管理グループおよびユーザー（自身）には、各自の userpkcs12、orcluserpkcs12hint、userpassword、orclpassword および orclpasswordverifier の各属性に対する完全なアクセス権限があります。ただし、他のグループおよびユーザーの属性に対するアクセス権限はありません。
- ユーザー（自身）には、各自の orclpassword 属性と orclpasswordverifier 属性に対する完全なアクセス権限がありますが、他のユーザーの同じ属性に対するアクセス権限はありません。
- すべてのユーザーには、userpkcs12、orcluserpkcs12hint、userpassword、orclpassword および orclpasswordverifier 以外のすべての属性に対して検索、読込みおよび比較を行うアクセス権限があります。

デフォルトのサブスクライバ・ネーミング・コンテキストのユーザー・コンテナでのデフォルトのアクセス・ポリシー

ユーザー・コンテナは、cn=users,o=oracle,dc=com です。

- サブスクライバ DAS ユーザー作成グループは、cn=oracledascreateuser,cn=groups,cn=oraclecontext,*distinguished_name_of_subscriber* です。このグループのメンバーには、オブジェクト・クラス orcluser のエントリを参照および追加する権限があります。
- サブスクライバ DAS ユーザー削除グループは、cn=oracledasdeleteuser,cn=groups,cn=oraclecontext,*distinguished_name_of_subscriber* です。このグループのメンバーには、オブジェクト・クラス orcluser のエントリを参照および削除する権限があります。
- サブスクライバ DAS ユーザー編集グループは、cn=oracledasedituser,cn=groups,cn=oraclecontext,*distinguished_name_of_subscriber* です。このグループのメンバーには、オブジェクト・クラス orcluser のエントリを参照する権限があります。
- サブスクライバ DAS ユーザー編集グループには、オブジェクト・クラス orcluser のエントリで、userpassword も含めたすべての属性に対する完全なアクセス権限があります。ユーザー（自身）には、各自の属性に対する完全なアクセス権限があります。他のユーザーにあるのは、これらの属性を参照する権限のみです。
- 認証サービス・グループは、cn=authenticationServices,cn=groups,cn=oraclecontext,*distinguished_name_of_subscriber* です。このグループのメンバーには、userpassword に対する比較権限がありますが、他のユーザーには一切権限がありません。
- ベリファイア・サービス・グループには、authpassword および orclpasswordverifier に対して読込み、検索および比較を行う権限があります。ユーザー（自身）には、各自のベリファイア属性に対する完全なアクセス権限がありますが、他のユーザーにはありません。

デフォルトのサブスクライバ・ネーミング・コンテキストのグループ・コンテナでのデフォルトのアクセス・ポリシー

グループ・コンテナは、`cn=groups,`*`distinguished_name_of_subscriber`*`,` `cn=OracleContext` です。

- サブスクライバ DAS ユーザー作成グループには、オブジェクト・クラス `orclgroup` のエントリを参照および追加する権限があります。
- オブジェクト・クラス `orclgroup` の非表示グループ・エントリを追加、削除または参照できるのは、そのエントリの所有者のみです。他のユーザーに一切権限はありません。このようなエントリの属性を読込み、検索、書込みおよび比較する権限は、そのエントリの所有者にのみ付与されます。
- オブジェクト・クラス `orclgroup` の Public グループ・エントリの所有者は、そのエントリを参照、追加および削除できます。また、次のグループはこの Public グループ・エントリを参照できます。
  - DAS ユーザー作成グループ
  - DAS ユーザー編集グループ
  - DAS ユーザー削除グループ

  このようなエントリの属性を読込み、検索、書込みおよび比較する権限は、そのエントリの所有者と DAS ユーザー編集グループにのみ付与されます。

Oracle コンテキスト管理者に対するデフォルトのアクセス・ポリシー

Oracle コンテキスト管理者コンテナは、`cn=OracleContextAdmins,` `cn=groups,cn=OracleContext,`*`distinguished_name_of_subscriber`* です。

Oracle コンテキスト管理者グループのメンバーには、特定の Oracle コンテキスト全体に対する完全な管理権限があります。グループが存在している Oracle コンテキストに対する完全なアクセス権限もあります。

Oracle9*i* Application Server 管理者に対するデフォルトのアクセス・ポリシー

Oracle9*i* Application Server 管理者コンテナは、`cn=IASAdmins,cn=groups,cn=OracleContext,`*`distinguished_name_of_subscriber`* です。

Oracle9*i* Application Server 管理者グループのメンバーには、指定された Oracle コンテキストの Oracle9*i* Application Server 製品ノード全体に対する完全な管理権限があります。さらに、次の権限が付与されます。

- 個々の製品でアプリケーション・エンティティ・オブジェクトを作成する権限
- これらのアプリケーション・エンティティのプロキシとなる権限

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「概念およびアーキテクチャ」を参照してください。
- セキュリティを構成するために使用する管理ツールについては、第 4 章「ディレクトリ管理ツール」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 12 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 14 章「Oracle のコンポーネントと Oracle Internet Directory」を参照してください。
- コマンドライン・ツールの構文と使用方法は、付録 C「スキーマ要素」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 をインストールした時点での、このパスワードのデフォルトは ODS 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-56 ページの「OID データベース・パスワード・ユーティリティ」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。統計の収集は、Oracle オプティマイザが LDAP 操作に対応する問合せを実行する際に、最適な計画を選択するために不可欠です。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いつでも実行できます。

注意： Windows オペレーティング・システムでこの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 1.0。サイト： `http://sources.redhat.com/cygwin/`
- MKS Toolkit 5.1 または 6.0。サイト： `http://www.datafocus.com/products/`

関連項目： A-56 ページ「OID データベース統計収集ツール」

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 3-1 に各コンポーネントと対応するログ・ファイルの位置をリストします。

表 3-1 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	`$ORACLE_HOME/ldap/odi/log/`*`AgentName`*`.err`（*`AgentName`* にはエージェント名が入ります）
Directory Integration Server（odisrv）	`$ORACLE_HOME/ldap/log/odisrv`*`XX`*`.log`（*`XX`* には Oracle Directory Integration 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）
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 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
- 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、2-15 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	参照箇所
Windows NT	「スタート」メニューから、「プログラム」>「*ORACLE_HOME*」>「Oracle Internet Directory」>「Oracle Internet Directory」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警告が表示されます。「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。

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」をクリックします。「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。

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、そのエントリをブラウズして選択します。 ■ そのユーザーのエントリに対する**識別名（DN）**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」ボックスに入力します。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」ボックス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、5-21 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。

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」フィールド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」をクリックします。 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。 **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」をクリックします。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。 **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」をクリックします。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。
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クリックします。 **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。 **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」をクリックします。

フィールド	説明
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 が作成済みであること。

関連項目：

- SSL を使用可能にする方法は、第 11 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、11-3 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」タブを選択してください。
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。

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。

フィールド	説明
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」をクリックします。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」をクリックすると、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

次の表は、メニュー・バーからアクセスできるメニューの一覧と説明です。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。

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。 取消 : 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 : オブジェクト・クラスを検索します。
ビュー	リフレッシュ : データベース上での変更内容を画面表示に反映するために、メモリーに格納されているデータを更新します。 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。 エントリのリフレッシュ : 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・エントリのリフレッシュ : 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。 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警告が表示されます。 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

メニュー	メニュー項目
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 4-1 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

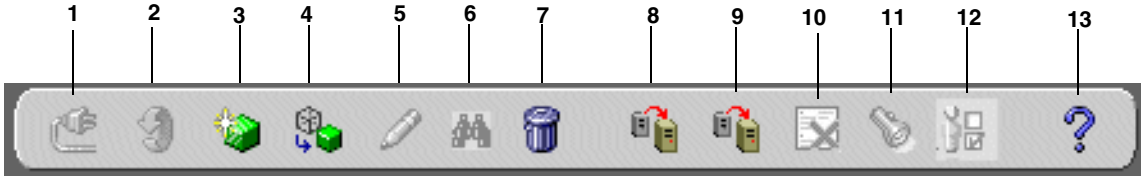


表 4-1 Oracle Directory Manager のツールバー

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	リフレッシュ : 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 サーバー」>「*Directory Server Instance*」>「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 サーバー」>「*Directory Server Instance*」>「サーバーの管理」>「属性」の順にナビゲートすると、このボタンで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	エントリのリフレッシュ : 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。
9	サブツリー・エントリのリフレッシュ : 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。
10	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警告が表示されます。

表 4-1 Oracle Directory Manager のツールバー（続き）

ボタン	用途
11	検索 : ACP 検索の構成を可能にします。
12	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。
13	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「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」>「切断」の順に選択します。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 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）プロセス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。

次の表に、Oracle Directory Manager が管理するタスクの領域および Oracle Directory Manager を各領域で使用するための参照箇所を示します。

タスクの領域	参照箇所
スキーマの管理	6-6 ページ「Oracle Directory Manager を使用したオブジェクト・クラスの管理」 6-16 ページ「Oracle Directory Manager を使用した属性の管理」
エントリの管理	7-2 ページ「Oracle Directory Manager を使用したエントリの管理」
アクセス制御ポリシー・ポイント（ACP）の管理	12-12 ページ「Oracle Directory Manager を使用したアクセス制御の管理」 12-43 ページ「コマンドライン・ツールを使用したアクセス制御の管理」
パーティション化とレプリケーション	第 22 章「Oracle ディレクトリ・レプリケーション・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。
- バルク・ツールー他のアプリケーションのデータを使用して大量のディレクトリ・エントリを作成または管理します。
- 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。

> **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。

表 4-2 に、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 4-2 Oracle Internet Directory コマンドライン・ツール

ツール	説明	詳細情報の参照先
Oracle Internet Directory サーバーの起動、停止および監視		
OID 制御ユーティリティ（OIDCTL）	OID 制御ユーティリティは、サーバーの起動および停止を行うためのコマンドライン・ツールです。コマンドは、OID モニターのプロセスによって解釈され、実行されます。	概念の説明は、2-15 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-5 ページの「OID 制御ユーティリティ」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と、OID モニターがこれを制御します。OID 制御ユーティリティ（OIDCTL）を使用してディレクトリ・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釈されます。	概念の説明は、2-15 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」を参照してください。
エントリの管理		
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-11 ページ「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-13 ページ「ldapaddmt の構文」

表 4-2 Oracle Internet Directory 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
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-15 ページ「ldapbind 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-16 ページ「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-18 ページ「ldapmoddn 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-20 ページ「ldapsearch の構文」
属性の管理		
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。	構文と使用方法は、A-25 ページの「カタログ管理ツール」を参照してください。 6-31 ページ「コマンドライン・ツールを使用した属性の索引付け」 6-27 ページ「Oracle Directory Manager を使用した属性の索引付け」
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-27 ページ「ldapcompare 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-28 ページ「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-34 ページ「ldapmodifymt の構文」
バルク操作の実行		
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-36 ページ「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するときに使用します。	A-37 ページ「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-28 ページ「ldapmodify の構文」

表 4-2 Oracle Internet Directory 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
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・サーバーで読込み可能な 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-41 ページ「ldifwrite の構文」
レプリケーションの管理		
OID 調停ツール	レプリケーション競合が発生した場合、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、指定した回数に応じてそれらの適用を試みます。指定した回数を超えて失敗が続いた場合、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。そこから、レプリケーション・サーバーはより短い間隔で変更アプリケーション・プロセスを繰り返しながら管理者によるアクションを待ちます。 このとき、必要な手順は次のとおりです。 **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。	22-30 ページ「OID 調停ツールの使用」 OID 調停ツールの構文と動作の説明は、A-45 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。変更をパージ・キューに移動すると、その後は変更ログのエントリが再適用されなくなります。	22-30 ページ「管理者操作キュー操作ツールの使用」 A-43 ページ「管理者操作キュー操作ツール」
同期とプロビジョニングの管理		
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-53 ページ「プロビジョニング・サブスクリプション・ツール」
oidmuplf.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-48 ページ「oidmuplf.sh ツール」
oidmcrep.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-49 ページ「oidmcrep.sh ツール」
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-51 ページ「oidmdelp.sh ツール」

表 4-2 Oracle Internet Directory 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
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 Directory Integration Server を起動できます。	A-51 ページ「stopodis.sh ツール」
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-52 ページ「schemasync ツール」
アプリケーション固有のリポジトリからの移行		
OID 移行ツール	このツールを使用して、アプリケーション固有のリポジトリから Oracle Internet Directory にデータを移行します。	A-58 ページ「OID 移行ツール」
データベース統計の監視		
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期ロードも含め、ディレクトリのデータに重要な変更がある場合は常に、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。統計の収集は、Oracle オプティマイザが LDAP 操作に対応する問合せを実行する際に、最適な計画を選択するために不可欠です。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いつでも実行できます。	A-56 ページ「OID データベース統計収集ツール」
データベース・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（oidpasswd）	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 をインストールした時点では、このパスワードのデフォルトは ODS 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。	A-56 ページ「OID データベース・パスワード・ユーティリティ」

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 1.0。サイト：`http://sources.redhat.com/cygwin/`
- MKS Toolkit 5.1 または 6.0。サイト：`http://www.datafocus.com/products/`

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。

タスク	参照箇所
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	6-29 ページ「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	6-16 ページ「Oracle Directory Manager を使用した属性の管理」
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	7-13 ページ「コマンドライン・ツールを使用したエントリの管理」
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「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-37 ページ「bulkload の構文」 A-2 ページ「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「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	6-13 ページ「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	6-6 ページ「Oracle Directory Manager を使用したオブジェクト・クラスの管理」

タスク	参照箇所
レプリケーションの管理	
レプリケーションの設定	第 22 章「Oracle ディレクトリ・レプリケーション・サーバーの管理」
レプリケーション変更の競合の解消	22-28 ページ「手動での競合の解消」
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	22-30 ページ「管理者操作キュー操作ツールの使用」
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 12 章「ディレクトリ・アクセス制御」
SSL の設定	第 11 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	5-11 ページ「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「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「ディレクトリ・サーバーへの接続」 4-11 ページ「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」
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	5-14 ページ「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。

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
- 検索の構成
- ディレクトリ・サーバーの監視、デバッグおよび監査
- アクティブ・サーバー・インスタンスの情報の表示
- Oracle 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

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。

注意： ディレクトリ・サーバーが同じマシン上にある場合は、複数インスタンスを実行できます。たとえば、サーバーの一方を SSL モードで実行し、他方を非 SSL モードで実行できます。ただし、特定のデータベース・サーバーを使用するディレクトリ・サーバー・インスタンスは、すべて同じコンピュータ上で実行する必要があります。たとえば、コンピュータ C のデータベース・サーバーに対して、2 つのディレクトリ・サーバーを、一方はコンピュータ A で、他方はコンピュータ B で実行することはできません。ただし、両方のディレクトリ・サーバーがコンピュータ A にあれば、その 2 つをコンピュータ B のデータベース・サーバーに対して実行できます。

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、3-3 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。

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

構成設定エントリ管理のための事前の考慮事項

デフォルトの構成設定 configset0 の値は変更できますが、すべての変更が、新規に作成するあらゆる構成設定エントリに影響します。これは、新規の構成設定エントリすべてに対して、configset0 の値がテンプレートとして使用されるためです。

実行しているサーバーのインスタンスすべてに対しては有効ではない値を変更するときは、構成設定エントリを新規に作成することをお薦めします。この方法は、Oracle ディレクトリ・サーバー・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、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 は、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ています。

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

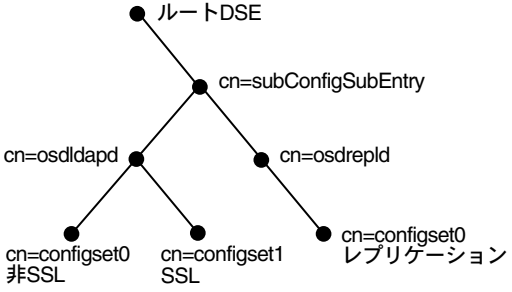


図 5-1 は、次のものを表しています。

- 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 がオフ状態の 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 がオン状態の 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）

関連項目：

- SSL の構成パラメータの詳細は、第 11 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 22 章「Oracle ディレクトリ・レプリケーション・サーバーの管理」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、C-5 ページの「構成設定エントリの属性」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を直接変更することはできません。構成設定エントリ内のパラメータを変更し、そのエントリを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、3-10 ページの「タスク 3: デフォルト・セキュリティ構成の再設定」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」>「*Directory Server Instance*」>「サーバーの管理」の順に展開し、「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」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。
2. 右側のペインで、特定のインスタンスを選択します。「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： 5-9 ページ「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テンプレートとして使用できます。以降は、作成した構成設定エントリからコピーして、別の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からのコピーによる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で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」>「*Directory Server Instance*」>「サーバーの管理」>「ディレクトリ・サーバー」の順に展開し、「デフォルト構成設定」を選択します。
2. ツールバーの「類似項目の作成」ボタンをクリックします。「構成設定」ダイアログ・ボックスに「一般」タブが表示されます。
3. 次の表の説明に従って、各フィールドに情報を入力します。

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。
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。

4. 「SSL 設定」タブを選択し、次の表の説明に従って、各フィールドに情報を入力します。

フィールド	説明
SSL 使用可能	非保護操作のみの場合は 0（ゼロ）を設定します。デフォルト・ポートは 839 で、この値未満に変更可能です。 SSL 認証のみの場合は 1 を設定します。デフォルト・ポートは 636 で、この値未満に変更可能です。 非保護操作と SSL 認証の両方の場合は 2 を設定します。
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 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 Wallet パスワード	サーバー側 Wallet のパスワードを入力します。このパスワードは、Wallet の作成時に設定されています。パスワードを変更する場合は、このパラメータを変更する必要があります。
SSL Wallet パスワードの確認	パスワードを変更するときは、このフィールドに新規パスワードを再度入力します。
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。
非 SSL ポート	デフォルトの非 SSL ポートは 839 です。非 SSL ポートは変更できます。

5. 「適用」をクリックします。

注意： アクティブ・ディレクトリ・サーバー・インスタンスには、再起動するまで変更内容が適用されません。3-8 ページの「ディレクトリ・サーバー・インスタンスの再起動」を参照してください。

関連項目：

- 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。
- 5-26 ページ「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」

既存の構成設定エントリからのコピーによらない構成設定エントリの追加 既存の構成設定からコピーせずに、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」>「*Directory Server Instance*」>「サーバーの管理」>「ディレクトリ・サーバー」の順に展開し、「デフォルト構成設定」を選択します。
2. ツールバーの「作成」ボタンをクリックします。「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。次の表の説明に従って、フィールドに値を入力します。

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。
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。

3. 「SSL 設定」タブを選択し、次の表の説明に従って、各フィールドに情報を入力します。

フィールド	説明
SSL 使用可能	SSL 認証を使用可能にするときに選択します。このチェックボックスを選択しない場合、SSL は使用されないため、このページの他のパラメータを設定する必要はありません。
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 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 Wallet パスワード	サーバー側 Wallet のパスワードを入力します。このパスワードは、Wallet の作成時に設定されています。パスワードを変更する場合は、このパラメータを変更する必要があります。
SSL Wallet パスワードの確認	パスワードを変更するときは、このフィールドに新規パスワードを再度入力します。
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。

4. 「OK」をクリックします。

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」>「*Directory Server Instance*」>「サーバーの管理」>「ディレクトリ・サーバー」の順に展開し、変更する構成設定エントリを選択します。右側のペインのタブ・ページに、構成設定が表示されます。

   次の表の説明に従って、「一般」タブのフィールドの値を変更します。

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。
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。

   どの値も変更できます。「適用」をクリックして変更値を保存してください。

2. 「SSL 設定」タブを選択します。次の表の説明に従って、フィールドを変更します。

フィールド	説明
SSL 使用可能	SSL 認証を使用可能にするときに選択します。このチェックボックスを選択しない場合、SSL は使用されないため、このページの他のパラメータを設定する必要はありません。
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。

フィールド	説明

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 Wallet パスワード	サーバー側 Wallet のパスワードを入力します。このパスワードは、Wallet の作成時に設定されています。パスワードを変更する場合は、このパラメータを変更する必要があります。
SSL Wallet パスワードの確認	パスワードを変更するときは、このフィールドに新規パスワードを再度入力します。
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。

3. 新規構成設定エントリ用に設定した各パラメータを確認した後、「適用」をクリックします。
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。

注意： アクティブ・ディレクトリ・サーバー・インスタンスには、再起動するまで変更内容が適用されません。3-8 ページの「ディレクトリ・サーバー・インスタンスの再起動」を参照してください。

関連項目： 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、「サーバーの管理」>「ディレクトリ・サーバー」の順に展開します。
2. ナビゲータ・ペインで、削除する構成設定エントリを選択します。
3. ツールバーの「削除」ボタンをクリックします。

注意： アクティブ・ディレクトリ・サーバー・インスタンスには、再起動するまで変更内容が適用されません。3-8 ページの「ディレクトリ・サーバー・インスタンスの再起動」を参照してください。

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、Wallet パスワードは welcome 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
orclsslwalletpasswd:welcome
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。前述の例のファイル名が newconfigs の場合、ldapadd コマンドは次のようになります。

   ```
   ldapadd [options] -f newconfigs
   ```

   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-11 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、C-5 ページの「構成設定エントリの属性」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。たとえば、入力ファイルの名前が `configfile` の場合、ldapmodify コマンドは次のようになります。

```
ldapmodify [options] -f configfile
```

関連項目：

- A-2 ページ「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-28 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、C-5 ページの「構成設定エントリの属性」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（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： 2-5 ページ「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、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。

次の表は、Oracle Directory Manager に表示される各システム操作属性フィールドの説明です。

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 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
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
索引付き属性の位置	すべての索引付き属性を含むエントリの識別名。	`cn=catalogs`	いいえ

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・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
レプリケーション状態の位置	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
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
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
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
スキーマ定義の位置	スキーマの識別名。	cn=subschemasubentry	いいえ
サポートされた制御リスト	任意の LDAP 操作の拡張情報。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。サポートされている制御属性の値は、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
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** ■ **MD5** ■ 暗号化なし ■ **SHA** ■ **UNIX Crypt**	MD4	はい
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

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
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、「読込み / 書込み」か「読込み専用」のいずれかに変更できます。レプリケーション時はデフォルトを「読込み専用」に変更してください。	読込み / 書込み	選択肢は「読込み / 書込み」および「読込み専用」です。
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	はい
サーバー処理の制限時間	検索の最大実行時間（秒）。	3600	はい
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
アップグレード進行中	アップグレード用に予約済みです。	FALSE	いいえ
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
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 の最大バイト数を指定します。	100M	はい
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
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

フィールド	説明	デフォルト値	変更可能？
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
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）。	2.1.1.0.0	いいえ

ldapmodify を使用したシステム操作属性の設定

変更可能なシステム操作属性は、次のとおりです。

属性	説明	デフォルト
`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。	なし
`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 ■ 暗号化なし ■ SHA ■ UNIX Crypt	MD4
`orclSizeLimit`	検索で戻されるエントリの最大数。	1000

属性	説明	デフォルト
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。レプリケーション時はデフォルトを「読込み専用」に変更してください。	読込み / 書込み
orclTimeLimit	検索の最大実行時間（秒）。	3600
orclecacheenabled	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。	1
orclecachemaxsize	エントリ・キャッシュが使用できる RAM の最大バイト数。	100M
orclecachemaxentries	エントリ・キャッシュ内に存在可能な最大エントリ数。	25,000
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 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
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。	1
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。	1

属性	説明	デフォルト
`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。	`1`
`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。	60
`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。	0

注意： マルチサーバー OID インスタンスでのエントリ・キャッシングは、orclecacheenabled の値に関係なく自動的に使用禁止になります。

関連項目： ldapmodify の詳細とそのオプションのリストは、A-28 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。そのためには、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

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

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「命名コンテキスト」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。検索「参照」をクリックして検索ウィンドウを開くこともできます。
3. 「適用」をクリックします。

ldapmodify を使用したネーミング・コンテキストの公開

次の例の入力ファイルは、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。

10-5 ページの「間接認証」で説明されているように、通常**プロキシ・ユーザー**はファイアウォールまたは RADIUS サーバーなど、中間層のある環境で使用されます。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。

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。

関連項目： アクセス権限の設定方法は、第 12 章「ディレクトリ・アクセス制御」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ています。平文で送信するために、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」を展開します。
2. 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。
3. 「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。

   次の表は、「システム・パスワード」タブ・ページのフィールドのリストと説明です。

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 `welcome` 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・ログイン名を入力します。ゲストには、そのディレクトリ内の**アクセス制御ポリシー・ポイント**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。

4. 「システム・パスワード」タブ・ページ内の適切なフィールドを編集します。変更内容を保存するには、「適用」をクリックします。

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 を使用して次の適切な属性を変更します。

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

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-28 ページの「ldapmodify の構文」を参照してください。

検索の構成

検索で戻されるエントリの最大数および検索の完了までの最大時間（秒）を設定できます。この 2 つの設定には、Oracle Directory Manager または ldapmodify のいずれかを使用します。

この項では、次の項目について説明します。

- Oracle Directory Manager を使用した検索の構成
- ldapmodify を使用した検索の構成

Oracle Directory Manager を使用した検索の構成

検索で戻されるエントリの最大数および検索に費やす最大時間を設定するには、Oracle Directory Manager を使用します。

Oracle Directory Manager を使用した、検索で戻されるエントリの最大数の設定

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. 「適用」をクリックします。

Oracle Directory Manager を使用した、検索の最大時間の設定

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「サーバー処理の制限時間」フィールドに、検索の完了までの最大秒数を入力します。デフォルトは 3600 です。
3. 「適用」をクリックします。

ldapmodify を使用した検索の構成

ldamodify を使用すると、検索で戻されるエントリの最大数および検索に費やす最大時間を設定できます。

ldapmodify を使用した、検索で戻されるエントリの最大数の設定

次の例では、検索で戻されるエントリの最大数は 500 に変更されます。

```
ldapmodify -h myhost -p 389 -v <<EOF
dn:
changetype: modify
replace: orclsizelimit
orclsizelimit: 500
EOF
```

ldapmodify を使用した、検索の最大時間の設定

次の例では、検索の最大時間は 2400 に変更します。

```
ldapmodify -h myhost -p 389 -v <<EOF
dn:
changetype: modify
replace: orcltimelimit
orcltimelimit: 2400
EOF
```

関連項目： A-28 ページ「ldapmodify の構文」

ディレクトリ・サーバーの監視、デバッグおよび監査

この項では、次の項目について説明します。

- デバッグ・ロギング・レベルの設定
- 監査ログの使用方法

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。

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たデバッグ・ロギング・レベルの設定

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。

   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。表 5-1 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合計し、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 5-1 は、デバッグ・ロギング・レベルの全リストです。

表 5-1 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	ファンクション・コールのトレース
2	パケット・ハンドリングのデバッグ
4	大容量トレースのデバッグ（レベル 1 を超える情報量）
8	接続管理（ネットワーク・アクティビティ関連）
16	サーバー / クライアント間の送受信パケット
32	検索フィルタの処理
64	構成ファイルの処理
128	アクセス制御リストの処理
256	各接続に関する操作と結果のログ
512	送信エントリのログ
1024	バックエンド（つまり、データベース）での通信のログ
2048	エントリの解析
4096	スキーマ関連の操作
32768	レプリケーション固有の操作
65535	潜在的なすべてのデバッグ操作 / データ

たとえば、ファンクション・コールのトレース（1）と接続管理（8）を有効にするには、次のようにデバッグ・レベルとして 9（8 + 1 = 9）を入力します。

```
oidctl server=oidldapd instance=1 flags='-debug 9' restart
oidctl server=oidrepld instance=1 flags='-h my_host -p 389 -d 9' 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。

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、開発者による監査ログ・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、5-30 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、5-31 ページの「監査レベルの設定」を参照してください。
- 5-32 ページ「Oracle Directory Manager を使用した監査ログ・エントリの検索」
- 5-34 ページ「ldapsearch を使用した監査ログ・エントリの検索」
- A-16 ページ「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。

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。たとえば、次のようになります。 `orcleventtime: 199811281010z`

属性	説明
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。6-31 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。

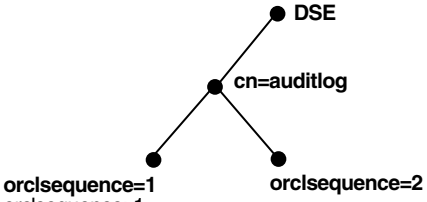
関連項目：

- カタログ化属性の詳細は、A-25 ページの「カタログ管理ツール」を参照してください。
- top の詳細は、2-10 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。図 5-2 を参照してください。

図 5-2 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 5-2 は、監査可能なイベントとその監査レベルを示しています。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 5-2 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
バインド	バインドに失敗した例	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（DSE）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

表 5-2 監査可能なイベント（続き）

イベント	説明	監査レベル
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。
3. 使用する監査レベルのチェックボックスを選択します。
4. 「適用」をクリックします。

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、次を除き、双方とも監査ログに入力されます。

- 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。

`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、3-8 ページの「ディレクトリ・サーバー・インスタンスの再起動」を参照してください。

> **関連項目：** 各監査レベルの説明は、5-30 ページの「監査可能なイベント」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、次の 3 つのイベントを監査するとします。

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、3-8 ページの「ディレクトリ・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」>「*Directory Server Instance*」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。オプションは次のとおりです。

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。
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。
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。
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。
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。
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。
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。

   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。

ボタン	説明
新規作成	「検索基準」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、「検索基準」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	「検索基準」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。

ボタン	説明
OR	「検索基準」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。

6. 「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。
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、「プロパティの表示」をクリックします。「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、5-24 ページの「検索の構成」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-20 ページ「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 net_service_name -base "cn=auditlog"
```

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. 「サーバーの管理」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」をクリックします。「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。

Oracle 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、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 をインストールした時点では、このパスワードのデフォルトは ODS 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-56 ページ「OID データベース・パスワード・ユーティリティ」

別名エントリの間接参照

この項では、別名エントリ間接参照の概要について説明し、使用モデルおよび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。

- 別名エントリ間接参照の概要
- 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

別名エントリ間接参照の概要

LDAP ディレクトリの別名エントリによって、1 つのエントリが別のエントリを指し示すことができます。したがって、厳密には階層構造でない構造を考え出すことができます。別名エントリは、UNIX ファイル・システムのシンボリック・リンクまたは Windows NT ファイル・システムのショートカットのような機能を実行します。

図 5-3 の `ou=uk sales,ou=global sales,o=oracle,c=us` エントリは、`ou=sales,o=oracle,c=uk` エントリを指し示す別名エントリです。（すべての情報と同様に）ポインタは、属性（別名エントリの別名化されたオブジェクト名の属性）として保持されます。別名エントリとディレクトリのオブジェクト・エントリとを区別するために、別名エントリには特別なオブジェクト・クラス別名があります。

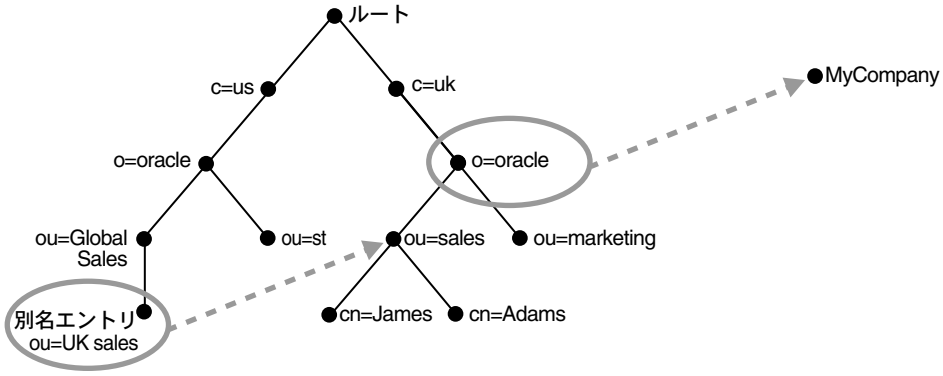
別名オブジェクト・クラスの定義

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

別名化されたオブジェクト名の定義

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

図 5-3 別名エントリの例



`ou=uk sales,ou=global sales,o=oracle,c=us` を参照すると、LDAP サーバーによって、その参照は実際のエントリ `ou=sales,o=oracle,c=uk` に自動的に変更されます。このプロセスは、別名間接参照と呼ばれます。

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。

- 別名エントリの追加
- ベース検索
- 1 レベルの検索
- サブツリーの検索
- 別名エントリの変更

別名エントリの追加

次の LDIF を使用して、通常のエントリと実際のエントリを指し示す別名エントリを作成します。手順に従って情報を追加すると、結果は図 5-4 のツリーのようになります。

1. 次のエントリで sample.ldif ファイルを作成します。

```
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
aliasObjectName:  cn=John Doe, o=oracle, c=us
```

2. 次のコマンドを使用して、エントリをディレクトリに追加します。

```
ldapadd -p <port> -h <host> -f  sample.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、LDAP 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、5-41 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 5-4 sample.ldif ファイルの作成結果を示すツリー

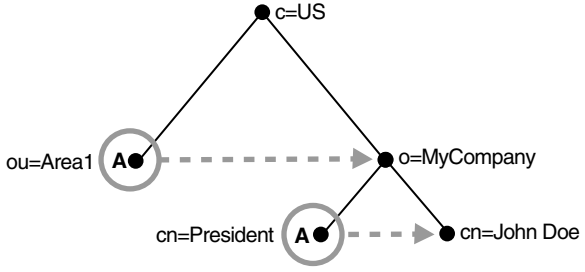


図 5-4 の文字 A は、別名エントリを表します。

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

ベース検索

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。

たとえば、次のようにフィルタとして "objectclass=*" を指定し、-deref オプションを LDAP_DEREF_FINDING に設定して、"ou=Area1,c=us" のベース検索を実行します。

```
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調査し、位置が特定された場合はその位置をユーザーに戻します。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、LDAP サーバーは別名エントリを自動的に間接参照し、間接参照エントリを戻します。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=oracle,c=us が戻されます。

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。

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。

フラグは、次のとおりです。

フラグ	内容
LDAP_DEREF_NEVER	-a never
LDAP_DEREF_FINDING	-a find

ldapsearch の間接参照フラグのデフォルトは LDAP_DEREF_NEVER（つまり、-a never）で、LDAP サーバーは別名エントリの間接参照を実行しません。

たとえば、次のようにフィルタとして "objectclass=*" を指定し、-deref オプションを LDAP_DEREF_FINDING（-a find）に設定して、"ou=Area1,c=us" の 1 レベル検索を実行します。

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

LDAP サーバーは、検索操作を 2 つのステップで実行します。

1. LDAP サーバーは、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した LDAP サーバーは、ベース以下のすべての 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、LDAP サーバーは、ベースの検索中（最初のステップ）に自動的に間接参照しますが、ベースの 1 レベル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=oracle,c=us 以下の 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=oracle,c=us です。

この検索では、cn=President,o=oracle,c=us および cn=John Doe,o=oracle,c=us が戻ります。

サブツリーの検索

サブツリー検索は、ベース、子、孫（ファミリ・ツリー）を検索します。

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。

フラグは、次のとおりです。

フラグ	内容
LDAP_DEREF_NEVER	-a never
LDAP_DEREF_FINDING	-a find

ldapsearch の間接参照フラグのデフォルトは LDAP_DEREF_NEVER（つまり、-a never）で、LDAP サーバーは別名エントリの間接参照を実行しません。

たとえば、次のようにフィルタとして "objectclass=*" を指定し、-deref オプションを LDAP_DEREF_FINDING に設定して、"ou=Area1,c=us" のサブツリー検索を実行します。

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

LDAP サーバーは、検索操作を 2 つのステップで実行します。

1. LDAP サーバーは、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した LDAP サーバーは、ベース以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、LDAP サーバーは、ベースの検索中（最初のステップ）に自動的に間接参照しますが、ベース以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=oracle,c=us 以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=oracle,c=us です。

この検索では、次の情報が戻されます。

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

別名エントリの変更

別名エントリは変更することができます。

たとえば、次のエントリを使用して sample.ldif ファイルを作成します。

```
dn: cn=President, o=oracle, c=us
changetype : modify
replace: aliasObjectName
aliasObjectName:  cn=XYZ, o=oracle, 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 sample.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 5-3 エントリ別名間接参照メッセージ

メッセージ	説明
別名に問題があります。	次のいずれかの問題が発生した場合に、このエラー・メッセージがクライアントに戻ります。 別名は間接参照されたが、ディレクトリ情報ツリー内のエントリを指し示していない場合。 親が別名である別名エントリを追加しようとした場合。
別名の参照解除に問題があります。	アクセス制御上の問題のため、ユーザーによる別名の間接参照が許可されていない場合は、このエラー・メッセージがクライアントに戻ります。
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がサーバーで見つからない場合は、このエラー・メッセージがクライアントに戻ります。
識別名の構文に誤りがあります。	別名エントリを追加または変更する際、`aliasedObjectName` に指定した値に無効な識別名の構文が含まれている場合は、LDAP サーバーがクライアントに `invalidDNSyntax` 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た場合は、LDAP サーバーが成功メッセージを戻します。 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	間接参照エントリに対するアクセス権限がユーザーにない場合は、このエラー・メッセージが戻ります。

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
- 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
- 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
- 一致規則の表示
- 構文の表示

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、次の特徴があります。

- 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でのデータの編成方法に関するすべての情報が含まれています。属性の型および適用される構文と一致規則が含まれます。オブジェクト・クラスと呼ばれる、属性の様々なグループ化も含まれています。

この章では、これらの各要素について説明します。

関連項目： 2-13 ページ「ディレクトリ・スキーマ」

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、2-9 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・コンポーネントのリストは、付録 C「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。

- オブジェクト・クラスの追加のガイドライン
- オブジェクト・クラスの変更のガイドライン
- 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・クラスの追加のガイドライン

ディレクトリ・エントリを追加するときは、そのエントリのオブジェクト・クラスを選択します。エントリの属性は、そのエントリが割り当てられているオブジェクト・クラスで決まります。

エントリは、上位から下位の順序でロードする必要があります。エントリを追加するときは、その親エントリがすべて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・オブジェクトが用意されているため、通常は問題は発生しません。

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。

エントリがオブジェクト・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であってもかまいません。オプション属性は、必ずしもディレクトリ・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： 6-15 ページ「属性管理の概要」

管理者は通常、オブジェクト・クラスに存在する属性に基づいて、そのオブジェクト・クラスをエントリに割り当てます。ただし、**スーパークラス**を使用すると、継承を利用できます。つまり、エントリ用に選択したオブジェクト・クラスにスーパークラスの階層を設定し、そのスーパークラスから必須属性とオプション属性を継承できます。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。

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。ある人物のエントリ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、すなわち 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。

関連項目： これらの用語の概念の説明は、2-10 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。また、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：

- 6-6 ページ「Oracle Directory Manager を使用したオブジェクト・クラスの管理」
- 6-13 ページ「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、次の項目について説明します。

- Oracle Directory Manager を使用したオブジェクト・クラスの検索
- 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
- Oracle Directory Manager を使用したオブジェクト・クラスの追加
- Oracle Directory Manager を使用したオブジェクト・クラスの変更
- Oracle Directory Manager を使用したオブジェクト・クラスの削除

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「スキーマの管理」を選択します。「スキーマの管理」タブ・ページが、右側のペインに表示されます。
2. 右側のペインの右下の「オブジェクト・クラスの検索」ボタンをクリックするか、メニュー・バーから「編集」>「オブジェクト・クラスの検索」をクリックします。「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。
3. 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。オプションは次のとおりです。

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。
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。

オプション	説明
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。
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。
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。

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。

4. 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。オプションは次のとおりです。

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。
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。

フィルタ	説明
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。

5. 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。

6. 「検索基準」フィールドの下に、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。

ボタン	説明
新規作成	「検索基準」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、検索基準バーが削除されている場合にのみ使用可能です。
AND	「検索基準」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	「検索基準」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。

7. 「検索」をクリックします。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「スキーマの管理」を展開します。「スキーマの管理」ペインにある各タブに、スキーマの次のコンポーネントが表示されます。
   - オブジェクト・クラス
   - 属性
   - 構文
   - 一致規則
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・ページのオブジェクト・クラスをクリックします。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。
3. 「オブジェクト・クラス」ダイアログ・ボックスは、次のとおりです。
   - 属性の継承元のオブジェクト・クラスが「スーパー・クラス」ボックスにリストされます。
   - 必須属性が「必須属性」ボックスにリストされます。
   - オプション属性が「オプション属性」ボックスにリストされます。

   各属性が検索式で使用できるように索引付けされているかどうかが、各ボックスに示されています。

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」の順に展開し、「スキーマの管理」を選択します。
2. 次のいずれかの方法を選択します。
   - 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。
   - 右側のペインの下の「作成」ボタンをクリックします。
   - 「操作」メニューから、「オブジェクト・クラスの作成」を選択します。

   「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。

   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・クラスを選択して、「類似項目の作成」をクリックする方法もあります。ダイアログ・ボックスが表示され、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。

3. 次の表に説明されている各フィールドに、情報を入力します。

フィールド	説明
名前	作成するオブジェクト・クラスの名前を入力します。
オブジェクト ID	オブジェクト識別子を入力します。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・クラスの型を指定します。「抽象型」、「構造型」、「補助型」、「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を指定します。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を指定します。「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を指定します。「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。

4. 「OK」をクリックします。

関連項目：

- 2-10 ページ「オブジェクト・クラスの型」
- 2-10 ページ「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「スキーマの管理」を選択し、「オブジェクト・クラス」タブを選択します。
2. 「オブジェクト・クラス」タブ・ページで、変更するオブジェクト・クラスをダブルクリックします。「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。
3. 次の表に説明されている各フィールドの情報を変更または追加します。

フィールド	説明
名前	作成するオブジェクト・クラスの名前を入力します。
オブジェクト ID	オブジェクト識別子を入力します。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・クラスの型を指定します。「抽象型」、「構造型」、「補助型」、「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を指定します。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を指定します。「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を指定します。「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。

4. 「OK」をクリックします。

関連項目：

- 2-10 ページ「オブジェクト・クラスの型」
- 2-10 ページ「サブクラス、スーパークラスおよび継承」

Oracle Directory Manager を使用したオブジェクト・クラスの削除

注意： 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。

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。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。

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、6-14 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「スキーマの管理」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」をクリックします。

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-28 ページ「ldapmodify の構文」

この項では、次の例について説明します。

- 例 : 新規オブジェクト・クラスの追加
- 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

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 Oracle 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 )  )
```

属性管理の概要

この項では、次の項目について説明します。

- 属性の追加に関する規則
- 属性の変更に関する規則
- 属性の削除に関する規則

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、2-4 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。

Oracle Directory Manager を使用した属性の管理

この項では、次の項目について説明します。

- Oracle Directory Manager を使用したすべてのディレクトリ属性の表示
- Oracle Directory Manager を使用した属性の検索
- Oracle Directory Manager を使用した属性の追加
- Oracle Directory Manager を使用した属性の変更
- Oracle Directory Manager を使用した属性の削除
- Oracle Directory Manager を使用した属性の索引付け

関連項目：

- 属性オプションの詳細は、2-8 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、7-11 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 7-15 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。

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」>「*directory server instance*」の順に展開し、「スキーマの管理」を選択します。
2. 右側のペインで「属性」タブを選択します。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。次に、「属性」タブ・ページに表示される表の各列の説明を示します。

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	様々な属性を説明する語。
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。
使用方法	属性の使用方法を指定する規格。`userApplications`、`directoryOperation`、`distributedOperation` および `dSAOperation` という 4 つのオプションがあります。
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	正規表現の一致に使用されます。
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。
スーパー	各属性のスーパー属性。

関連項目： 特定のエントリの属性を表示する方法は、7-5 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「スキーマの管理」を選択します。「スキーマの管理」タブ・ページが、右側のペインに表示されます。
2. 「属性」タブ・ページを選択します。
3. 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。
4. 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。オプションは次のとおりです。

フィールド	説明
名前	検索する属性の名前。
索引付け	索引付き属性のリスト。
オブジェクト ID	検索する属性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 で始まる属性のリストが表示されます。
説明	属性の説明列に記述されている語。
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。この規則を使用して、特定の構文を使用している属性の検索範囲を絞り込むことができます。
サイズ	このオブジェクトの最大サイズ。
使用方法	属性の使用方法を指定する規格。userApplications、directoryOperation、distributedOperation および dSAOperation のいずれか 1 つを入力して、検索範囲を絞り込みます。
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	正規表現の一致に使用されます。
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。
スーパー	検索する属性のスーパー属性。

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。オプションは次のとおりです。

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。
「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。

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。

7. 「検索基準」フィールドの下に、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。

ボタン	説明
新規作成	「検索基準」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、「検索基準」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	「検索基準」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	「検索基準」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。

8. 「検索」をクリックします。検索結果が、「検索 : 属性」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。

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」の順に展開し、「スキーマの管理」を選択します。
2. 次のいずれか 1 つを行います。
   - 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。
   - 右側のペインで「属性」タブを選択し、「属性」タブ・ページの下の「作成」ボタンをクリック。
   - 「操作」メニューから、「属性の作成」を選択。「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。

3. 次の表の説明に従って、「一般」タブの各フィールドに値を入力します。

フィールド	説明
名前	この属性の名前を入力します。
オブジェクト ID	この属性のオブジェクト ID を入力します。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 サイトで参照できます。
説明	説明を記述するオプションのフィールドです。
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を入力します。
サイズ	このオブジェクトの最大サイズを入力します。
単一値	このチェックボックスを選択すると、この属性の型の値が最大 1 つであることを指定できます。

4. 「拡張」タブを選択します。次の表の説明に従って、各フィールドに値を入力します。

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	一致する正規表現を指定します。

フィールド	説明
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」ボタンをクリックします。「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」をクリックします。 **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」をクリックします。

5. 「OK」をクリックします。

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「スキーマの管理」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、6-4 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「スキーマの管理」を選択します。
2. 右側のペインで「属性」タブを選択します。
3. 「属性」タブ・ページで、コピーする属性を選択します。
4. 右側のペインの下の「類似項目の作成」ボタンをクリックします。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。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、次の表の説明に従って各フィールドに値を入力します。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。

フィールド	説明
名前	この属性の名前を入力します。
オブジェクト ID	この属性のオブジェクト ID を入力します。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 サイトで参照できます。
説明	説明を記述するオプションのフィールドです。
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を入力します。
サイズ	このオブジェクトの最大サイズを入力します。
単一値	このチェックボックスを選択すると、この属性の型の値が最大 1 つであることを指定できます。

6. 「拡張」タブを選択し、次の表の説明に従って各フィールドに値を入力します。

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	一致する正規表現を指定します。
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」ボタンをクリックします。「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」をクリックします。 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」をクリックします。

7. 「OK」をクリックします。

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「スキーマの管理」を選択します。
2. 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。
3. 「編集」をクリックします。「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。
4. 「一般」タブを選択し、次の表の説明に従って各フィールドに値を入力します。

フィールド	説明
名前	この属性の名前を入力します。
オブジェクト ID	この属性のオブジェクト ID を入力します。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 サイトで参照できます。
説明	説明を記述するオプションのフィールドです。
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を入力します。
サイズ	このオブジェクトの最大サイズを入力します。
単一値	このチェックボックスを選択すると、この属性の型の値が最大 1 つであることを指定できます。

5. 「拡張」タブを選択し、次の表の説明に従って各フィールドに値を入力します。

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	一致する正規表現を指定します。
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」ボタンをクリックします。「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」をクリックします。 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」をクリックします。

6. 「OK」をクリックします。

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「スキーマの管理」を選択します。
2. 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。
3. 「削除」をクリックします。

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、6-31 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」で説明されてい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
- C-9 ページの「一致規則」にリストされているように、Oracle Internet Directory でサポートされる一致規則を持つ
- 属性の名前が 28 文字未満

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「スキーマの管理」を選択します。
2. 右側のペインで「属性」タブを選択します。「属性」タブに、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

6-20 ページの「Oracle Directory Manager を使用した属性の追加」の説明にあるように属性を作成する場合は、「新規属性の型」ダイアログ・ボックスを使用します。そのダイアログ・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てください。

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「スキーマの管理」を選択します。
2. 右側のペインで「属性」タブを選択します。
3. 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。
4. 「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。この項では、次の項目について説明します。

- ldapmodify を使用した属性の追加と変更
- ldapmodify を使用した属性の削除
- コマンドライン・ツールを使用した属性の索引付け

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_filename
```

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' )
```

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-28 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、6-33 ページの「構文の表示」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_filename
```

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-28 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、6-33 ページの「構文の表示」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
- C-9 ページの「一致規則」にリストされているように、Oracle Internet Directory でサポートされる一致規則を持つ
- 属性の名前が 28 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-28 ページ「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-25 ページ「カタログ管理ツール」

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の索引を削除しないでください。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。

一致規則の表示

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」>「*Directory Server Instance*」の順に展開し、「スキーマの管理」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。これには次のようなものがあります。

列見出し	意味
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

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-20 ページ「ldapsearch の構文」

構文の表示

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「スキーマの管理」を選択します。
2. 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: この構文の一意な識別子

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-20 ページ「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「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
- Oracle Directory Manager を使用した特定エントリの属性の表示
- Oracle Directory Manager を使用したエントリの追加
- Oracle Directory Manager を使用したエントリの変更
- Oracle Directory Manager を使用した属性オプション付きエントリの管理

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」>「*Directory Server Instance*」>「エントリ管理」の順に展開して、そのサブツリーを表示します。

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」>「*Directory Server Instance*」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・ビュー」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。オプションは次のとおりです。

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。

フィルタ	説明
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」「完全に一致する」「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。
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。

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。

ボタン	説明
新規作成	「検索基準」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、「検索基準」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	「検索基準」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	「検索基準」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。

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：** ■ 6-27 ページ「Oracle Directory Manager を使用した属性の索引付け」 ■ 6-31 ページ「コマンドライン・ツールを使用した属性の索引付け」

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、5-24 ページの「検索の構成」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、6-17 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. 「Oracle Internet Directory サーバー」>「*Directory Server Instance*」の順に展開し、「エントリ管理」を選択します。
2. 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。
3. 「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。
4. 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。
5. 「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。
6. 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」>「*Directory Server Instance*」の順に展開し、「エントリ管理」を選択します。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。
2. 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。
3. 「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。
4. 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。
5. 「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. 「Oracle Internet Directory サーバー」>「*Directory Server Instance*」の順に展開し、「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」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。
5. 「オブジェクト・クラス」ボックスの右側の「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 `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。
7. 「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、「`userPassword`」ウィンドウまでスクロールします。
8. Anne Smith 用のパスワードを入力します。

Oracle Directory Manager を使用したグループ・エントリの追加

グループ・エントリは、エントリのリスト（例 : 電子メール・リスト）を含むエントリです。グループ・エントリは、オブジェクト・クラス `orclPrivilegeGroup` をサブクラスとして持つ、`groupOfNames` 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。

エントリが `groupOfNames` オブジェクト・クラスに属している場合は複数値の属性 `member` に、`groupOfUniqueNames` オブジェクト・クラスに属している場合は属性 `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。

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」>「*Directory Server Instance*」の順に展開し、「エントリ管理」を選択します。
2. 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。
3. 「識別名」フィールドに、完全な識別名を入力します。「参照」ボタンを使用して、追加するエントリの親の識別名を探し、親の識別名の左に新規エントリの相対識別名を入力して、その後にカンマを付けることもできます。

4. 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。
5. 「スーパー・クラス・セレクタ」ダイアログ・ボックスで、top オブジェクト・クラスを選択し、「選択」ボタンをクリックします。「新規エントリ」ダイアログ・ボックスの「オブジェクト・クラス」ボックスに、top オブジェクト・クラスが表示されます。
6. 同様に、次の手順を実行します。
   a. 「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。
   b. 「スーパー・クラス・セレクタ」ダイアログ・ボックスから、「groupOfNames」または「groupOfUniqueNames」オブジェクト・クラスを選択します。
   c. 「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。
7. 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。ブラウズ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」をクリックします。「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、エントリを選択して「OK」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。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。
8. 「OK」をクリックします。

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。
- グループ・エントリのアクセス制御ポリシー・ポイントの設定方法は、12-3 ページの「アクセス制御グループ」を参照してください。
- アクセス権限の詳細は、2-14 ページの「グローバリゼーション・サポート」および第 12 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

Oracle Directory Manager は、次の規則を含む標準 LDAP 規則に従っています。

- エントリにオブジェクト・クラスを割り当て、その属性にデータを指定した後は、そのエントリが使用しているオブジェクト・クラスを変更できません。

  たとえば、オブジェクト・クラスの `Person` と `Organizational Role` を使用するエントリを構成する場合は、このエントリに後で別のオブジェクト・クラスを追加できません。

- すでにいくつかのエントリが使用しているオブジェクト・クラスには、必須属性を追加できません。オプション属性は追加できます。いくつかのエントリがすでに使用し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。これらのエントリに対しては、オプション属性は空の属性として追加されます。

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. 「OK」をクリックします。

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、7-8 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、「`userPassword`」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 リリース 9.2 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. 「Oracle Internet Directory サーバー」>「*Directory Server Instance*」>「エントリ管理」の順に展開して、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。
2. 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。
3. 「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。
4. 「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。
5. 「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。
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. 「Oracle Internet Directory サーバー」>「*Directory Server Instance*」>「エントリ管理」の順に展開して、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。
2. 「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。
3. 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。
4. フィールドの値を変更します。
5. 「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. 「Oracle Internet Directory サーバー」>「*Directory Server Instance*」>「エントリ管理」の順に展開して、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。
2. 「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。
3. 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。
4. フィールドの値を削除します。
5. 「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。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箇所を示します。

ツール	タスク	構文と使用方法
ldapsearch	ディレクトリ・エントリを検索します。	A-20 ページ「ldapsearch 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-15 ページ「ldapbind の構文」
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-11 ページ「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-13 ページ「ldapaddmt 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-28 ページ「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-34 ページ「ldapmodifymt の構文」
ldapdelete	エントリを削除します。	A-16 ページ「ldapdelete 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-27 ページ「ldapcompare の構文」

ツール	タスク	構文と使用方法
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を改名します。 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-18 ページ「ldapmoddn の構文」

例 : ldapadd を使用したユーザー・エントリの追加

次の例は、John という従業員のユーザー・エントリを追加する、`entry.ldif` という名前の LDIF ファイルです。

```
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` 属性では、`cn;lang-fr` および `cn;lang-en-us` という 2 つのオプションを指定しています。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）属性を持つ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： 2-8 ページ「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。

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-56 ページの「OID データベース統計収集ツール」を参照してください。
- これらのツールの概要は、4-13 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・ユーティリィティが必要です。

- Cygwin 1.0。サイト：`http://sources.redhat.com/cygwin/`
- MKS Toolkit 5.1 または 6.0。サイト：`http://www.datafocus.com/products/`

この項では、次の項目について説明します。

- タスク 1: Oracle サーバーのバックアップ
- タスク 2: Oracle Internet Directory のパスワードの準備
- 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
- タスク 4: SQL*Loader 用の入力ファイルの生成
- タスク 5: 入力ファイルのロード
- バルク・ロードに失敗した場合

タスク 1: Oracle 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： 『Oracle9*i* ユーザー管理バックアップおよびリカバリ・ガイド』

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-56 ページ「OID データベース・パスワード・ユーティリティ」

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 net_service_name -check path_to_ldif-filename
```

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。このステップで、LDIF データは SQL*Loader 固有の形式に変換されます。

```
bulkload.sh -connect net_service_name -generate ldif-filename
```

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。このステップで、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 net_service_name -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-41 ページ「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-39 ページ「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-36 ページ「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「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

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。

8

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。

この章では、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、2-14 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
- 非 UTF-8 データベースの使用方法
- 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
- 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
- クライアント環境における NLS_LANG の設定
- 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

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、『Oracle9*i* Database グローバリゼーション・サポート・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、『Oracle9*i* Database グローバリゼーション・サポート・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レーション・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、『Oracle9*i* Database グローバリゼーション・サポート・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「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込みます。

- 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。

この項では、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。

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`

クライアント環境における NLS_LANG の設定

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、『Oracle9*i* Database 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、『Oracle9*i* Database グローバリゼーション・サポート・ガイド』および『Oracle9*i* Database 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・データの読込み / 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」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。

次のようなコマンドを実行します。

```
bulkload.sh -connect net_service_name -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 1.0。サイト : `http://sources.redhat.com/cygwin/`
- MKS Toolkit 5.1 または 6.0。サイト : `http://www.datafocus.com/products/`

---

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。

次のようなコマンドを実行します。

```
ldifwrite -c net_service_name -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。

次のようなコマンドを実行します。

```
bulkdelete.sh -connect net_service_name -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 1.0。サイト：http://sources.redhat.com/cygwin/
- MKS Toolkit 5.1 または 6.0。サイト：http://www.datafocus.com/products/

---

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。

次のようなコマンドを実行します。

```
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 1.0。サイト：http://sources.redhat.com/cygwin/
- MKS Toolkit 5.1 または 6.0。サイト：http://www.datafocus.com/products/

9

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。

この章では、次の項目について説明します。

- 概要
- 概念
- 要件
- 既知の制限事項

概要

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。たとえば、識別名が `uid=dlin, ou=people, o=oracle` の場合、この識別名は `ou=people` の直下で一意でした。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。

Oracle Internet Directory と同期化するアプリケーションでは、識別名以外の属性を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、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。属性一意性は、エントリが変更されるたびに、指定された属性の値が一意であることを保証するチェックを実施します。

ユーザーは次の各範囲内で属性一意性を定義できます。

- ディレクトリ全体
- 1 つのサブツリー
- 1 つのオブジェクト・クラス

概念

属性一意性の制約は、操作前トリガーに類似しています。これは、LDAP 操作を実行する前に、ディレクトリ・サーバーがすべての更新操作をチェックすることを意味します。ディレクトリ・サーバーは、属性および監視対象のディレクトリ・サーバーに構成された接尾辞（サブツリー）に操作を適用するかどうかを判断します。

ディレクトリ・サーバーが監視している属性と接尾辞に更新操作が適用され、その更新操作によって同じ属性値を持つ 2 つのエントリが生じる場合、サーバーは操作を終了し、制約違反エラーをクライアントに戻します。

ディレクトリ・サーバーは、次の範囲で属性一意性チェックを実行します。

- 単一の属性
- 属性ごとに 1 つのサブツリー
- 1 つのオブジェクト・クラス

注意： 属性一意性は、カタログ化属性でのみ機能します。

複数の属性について一意性をチェックするには、チェックする各属性に対して一意性制約のインスタンスを個別に作成する必要があります。

属性一意性制約を構成するには、次の異なる方法があります。

- ディレクトリ全体での属性一意性を定義できます。
- 属性ごとに 1 つのサブツリー内での属性一意性を定義できます。

  たとえば、Oracle が Company1 と Company2 のディレクトリをホスティングしているとします。`uid=dlin,ou=people,o=Company1,dc=oracle,dc=com` のエントリを追加する場合は、`o=Company1,dc=oracle,dc=com` サブツリー内のみ、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。
- 1 つのオブジェクト・クラス内での属性一意性を定義できます。

  たとえば、ID はオブジェクト・クラス「machine」に対して一意の属性であり、オブジェクト・クラス「person」に対しても一意の属性であると仮定します。Oracle Internet Directory で属性一意性を適用すると、同じ ID を持つ 2 台のマシンまたは同じ ID を持つ 2 人を Oracle Internet Directory にロードしようとすると、属性一意性の制約違反エラーがクライアントに戻ります。マシン ID と個人 ID は、同じ値でもかまいません。

要件

この項では、属性一意性に関する要件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。

- 属性一意性の作成
- 属性一意性の有効化と無効化
- サブツリーの指定
- 属性一意性ポリシーの削除
- 構成インタフェース
- 定義されたポリシーの位置およびモデル
- ポリシー有効範囲決定規則
- 属性一意性機能の適用

属性一意性の作成

ディレクトリ内の特定の属性が常に一意の値になるようにするには、チェックする属性に対して属性一意性のインスタンスを作成する必要があります。たとえば、メール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、メールに関連付けられた属性一意性のインスタンスを作成する必要があります。

2 つの異なる一意性ポリシーが属性に関連付けられていて、一方のポリシーの有効範囲が他方の有効範囲のサブセットである場合は、より外側（より高いレベル）のポリシーが優先されます。

ディレクトリ全体での属性一意性の作成

ディレクトリ全体にわたる属性一意性のインスタンスの作成に必要な入力情報は、値の一意性を適用する属性名です。

1 つのサブツリー内での属性一意性の作成

1 つ以上のサブツリー内での属性一意性のインスタンスを作成する場合に必要な入力情報は、次のとおりです。

- 値の一意性を適用する属性名
- 一意性制約を規程するサブツリーの位置

1 つのオブジェクト・クラス内での属性一意性の作成

1 つのオブジェクト・クラス内での属性一意性のインスタンスを作成する場合に必要な入力情報は、次のとおりです。

- 値の一意性を適用する属性名
- オブジェクト・クラス名

属性一意性の有効化と無効化

属性一意性を有効または無効にできます。

属性一意性を有効化する手順は、次のとおりです。

1. ldapmodify または ldapadd を使用して、属性一意性制約を追加します。
2. ポリシーが有効化されるようにディレクトリ・サーバーを再起動します。

属性一意性を無効化する手順は、次のとおりです。

1. ldapmodify または ldapdelete を使用して、属性一意性制約を削除します。
2. ポリシーが無効化されるように LDAP サーバーを再起動します。

サブツリーの指定

属性一意性を確認するための接尾辞またはサブツリーは、ポリシー・オブジェクトでサブツリー位置の属性を変更することによって指定できます。

ldapmodify コマンドライン・ツールを使用して、更新文が含まれている LDIF ファイルをディレクトリにインポートできます。

注意： 変更したポリシーを使用可能にするには、ディレクトリ・サーバーを再起動する必要があります。

属性一意性ポリシーの削除

ldapdelete コマンドライン・ツールを使用して、属性一意性ポリシーを削除します。

注意： ポリシー削除後、ポリシーを使用禁止にするためにディレクトリ・サーバーを再起動する必要があります。

構成インタフェース

表 9-2「属性一意性制約エントリ」に示すように、各属性一意性制約エントリには、次の属性があります。

表 9-1 属性一意性制約エントリの属性

属性	説明
orcluniqueattrname	この属性の指定は必須です。
orcluniquescope	この属性の指定はオプションで、次のいずれかの値を指定できます。 base onelevel sub この属性が未指定の場合は、sub がデフォルトで使用されます。
orcluniquesubtree	属性一意性制約を規程するサブツリーを指定できます。デフォルトでは、ルート・ディレクトリが規程されます。
orcluniqueobjectclass	属性一意性制約を規程するオブジェクト・クラスを指定できます。デフォルトでは、すべてのオブジェクト・クラスに規程されます。

定義されたポリシーの位置およびモデル

すべての属性一意性制約エントリは、cn=unique, cn=Common, cn=Products, cn=OracleContext に格納される必要があります。

表 9-2 に示すように、属性一意性制約エントリで orclunqiuescope、orcluniquesubtree または orcluniqueobjectclass が未指定の場合は、デフォルト値がそれぞれ適用されます。デフォルトでは、orcluniquescope はサブツリー、orcluniquesubtree はディレクトリ全体、orcluniqueobjectclass はすべてのオブジェクト・クラスです。

ポリシー有効範囲決定規則

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。

複数の属性一意性制約で、orcluniqueattrname の値が同一で、orcluniquesubtree の値が異なり、それらのサブツリーが重複する場合は、最大のサブツリー有効範囲を持つ属性一意性制約が有効となります。

複数の属性一意性制約で、orcluniqueattrname および orcluniquesubtree 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。

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。

複数の属性一意性制約で、orcluniqueattrname および orcluniqueobjectclass の値が同一で、orcluniquesubtree の値が異なり、それらのサブツリーが重複する場合は、最大のサブツリー有効範囲を持つ属性一意性制約が有効となります。

複数の属性一意性制約で、orcluniqueattrname、orcluniquesubtree および orcluniqueobjectclass の値がそれぞれ同一の場合は、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。

表 9-2 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	文字列	該当なし	該当なし
orcluniquescope	いいえ	次のいずれかの値	sub	
		base		ベースのみを検索
		onelevel		1 レベルを検索
		sub		サブツリーを検索

表 9-2 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
orcluniquesubtree	いいえ	文字列	""	ディレクトリ全体
orcluniqueobjectclass	いいえ	文字列	""	すべてのオブジェクト・クラス

属性一意性機能の適用

次の例は、Oracle Internet Directory を介して属性一意性機能を適用します。

使用例 : 米国オラクル社の全従業員について、従業員 ID がすべて一意であることを確認します。

解決策 : 次の手順に従って、属性一意性制約を作成して適用します。

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=Oracle Corporation, c=US
orcleuniqueobjectclass: person
```

2. 属性一意性機能を適用するには、次のコマンドを使用して属性一意性制約エントリをロードする必要があります。

```
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。

米国オラクル社の全従業員の従業員 ID に属性一意性が適用されます。

この制約を削除するには、次の手順を実行します。

1. 属性一意性エントリを削除します。
2. ディレクトリ・サーバーを再起動します。

既知の制限事項

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。

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、Oracle Internet Directory 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、2 台のマスターが、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動作します。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生じ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・サーバーによるものであるかどうかを判断してください。

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。

10

ディレクトリ・セキュリティの概要

この章では、Oracle Internet Directory で使用可能なセキュリティ機能について説明します。次の項目について説明します。

- データ整合性
- データ・プライバシ
- 認可
- 認証
- 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・ポリシー

データ整合性

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。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。

> **関連項目：** SSL の詳細は、第 11 章「Secure Sockets Layer（SSL）とディレクトリ」を参照してください。

データ・プライバシ

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 11 章「Secure Sockets Layer（SSL）とディレクトリ」を参照してください。

認可

認可は、ユーザーが権限を持つ情報のみを読込みまたは更新することを保証するプロセスです。ディレクトリ操作がディレクトリ・セッションの中で試みられた場合、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うえで必要な権限があるかどうかが確認されます。ユーザーに必要な権限がない場合、ディレクトリ・サーバーはこれらの操作を認めません。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・データを保護しています。この方法はアクセス制御と呼ばれます。

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、**アクセス制御情報アイテム**（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。このリストにある属性値によって、そのディレクトリ・オブジェクトに対するアクセス・ポリシーが管理されます。

ディレクトリ・オブジェクトに関連付けられているアクセス制御情報アイテム（ACI）は、様々なディレクトリ・ユーザー・エンティティ（対象）が、指定した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。したがって、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・ポイントは規定的です。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）**内の下位エントリすべて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・ポイントが適用される開始地点は、**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・ポイントを表します。

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、サブスクライバにディレクトリ管理を委任できます。必要であれば、サブスクライバから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、サブスクライバ・サブツリーの管理者は、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。他のサブスクライバ・サブツリーの管理者は、給与属性に関してこれとは異なるポリシーを確立して、適用できます。

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 ID を検証するために、Oracle Internet Directory では、直接認証と間接認証の 2 種類の一般的な認証を使用できます。

直接認証

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。

- Secure Sockets Layer（SSL）認証

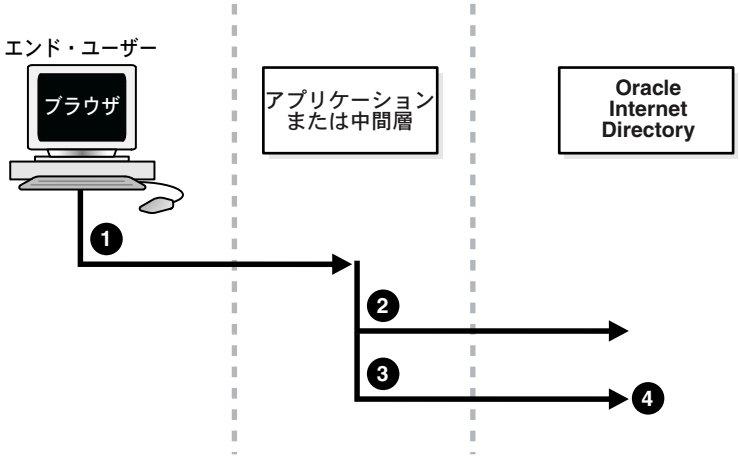
  信頼できる認証局が発行する証明書の交換が含まれます。

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（たとえば、ファイアウォールや RADIUS サーバーなどの中間層）を介して発生します。アプリケーションまたは中間層は、エンド・ユーザーの代理である**プロキシ・ユーザー**となり、エンド・ユーザーのかわりにディレクトリ操作を実行します。

次の図 10-1 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 10-1 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リクエスト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. この 2 回目のバインドは、ディレクトリ・サーバーによって、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認識されます。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。

* アプリケーションまたは中間層が必要なプロキシ権限を持っている場合、ディレクトリ・サーバーは、認証 ID をエンド・ユーザーの認証 ID 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。
* アプリケーションまたは中間層が必要なプロキシ権限を持っていない場合、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： 12-10 ページ「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、エンド・ユーザーのセッションから、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のセッション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、Oracle Internet Directory に対する問合せが含まれているリクエスト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。Oracle 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。

先行ユーザーがサービスを受けている間に、このアプリケーションの別のユーザーがそのサービスをリクエストした場合、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、先行ユーザーがサービスを受けていない場合は、新規接続を確立せずに既存の確立済み接続を何度も使用できます。

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 への認証用パスワード・ベリファイアの格納」

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。

- 指定し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 17 章「パスワード・ポリシー」を参照してください。

11

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
- このリリースの Oracle Internet Directory 固有の問題

関連項目： Oracle Internet Directory に関連した SSL の概要は、2-13 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 11-1 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・ニーズ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、C-5 ページの「構成設定エントリの属性」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たに変更された構成設定を参照できます。

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. Oracle Directory Manager のナビゲータ・ペインで、「Oracle Internet Directory サーバー」>「ディレクトリ・サーバー」>「サーバーの管理」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・ページを選択します。

   このタブ・ページでパラメータを変更して保存できます。このタブ・ページの各フィールドの説明を、次の表に示します。

フィールド	説明
SSL/non-SSL Enable	非保護操作のみの場合は 0（ゼロ）を設定します。デフォルト・ポートは 389 で、この値未満に変更可能です。 SSL 認証のみの場合は 1 を設定します。デフォルト・ポートは 636 で、この値未満に変更可能です。 非保護操作と SSL 認証の両方の場合は 2 を設定します。
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。

フィールド	説明

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 Wallet パスワード	サーバー側 Wallet のパスワードを入力します。このパスワードは、Wallet の作成時に設定されています。パスワードを変更する場合は、このパラメータを変更する必要があります。
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。
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。

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。
- Oracle Wallet Manager の使用方法は、『Oracle Advanced Security 管理者ガイド』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： 5-11 ページ「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」

このリリースの Oracle Internet Directory 固有の問題

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 リリース 9.2 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。

12

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・ポイントの概要および 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・ポイントの管理の概要
- 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
- ACL 評価の動作

関連項目：

- アクセス制御ポリシー・ポイントの実装と管理を開始する前に理解しておく必要のある概要については、2-13 ページの「セキュリティ」および第 10 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 B「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・ポイントの管理の概要

アクセス制御ポリシー・ポイントは、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： 12-47 ページ「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、12-3 ページの「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。構造の定義については、この章で後述します。

アクセス制御グループ

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、アクセス制御グループでそのグループを識別します。アクセス制御グループには、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、サブスクライバのサブツリー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 ID はサブスクライバのサブツリーでは認識されないため、そのサブツリーの ACP のみに依存している場合、ディレクトリ・サーバーによって必要なアクセスが制限されます。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、サブスクライバのサブツリーにある 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・サーバーによるアクセス制御グループ・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、アクセス制御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、アクセス制御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、他のアクセス制御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。

各アクセス制御グループ（ネストされているかどうかに関係なく）は、アクセス制御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。グループがアクセス制御グループのメンバーの場合でも、アクセス制御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。アクセス制御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 : アクセス制御グループ・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・ポイントを設定できます。

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・ポイントは、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・ポイントは、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。

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 B「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（つまり、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方法を指定します。次の 4 つのモードがあります。

- 簡易 : パスワードベースの簡易認証。
- SSL 認証なし : SSL ベースのクライアントに対する匿名またはパスワードベースの簡易認証。この方法では、SSL の暗号化機能のみを使用します。
- SSL 一方向 : サーバーの自己認証を伴う、SSL ベースのクライアントに対する匿名またはパスワードベースの認証。
- SSL 双方向 : SSL ベースのクライアントに対する SSL を使用した厳密認証。

バインド・モードの指定はオプションです。ディレクトリ・サーバーは、ユーザーのバインド・モードが、ユーザーが通信しようとするノードのバインド・モードと互換性があるかどうかを検証します。あるノードで指定されているバインド・モードは、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。たとえば、一方のノードで SSL 双方向認証を指定する場合は、もう一方のノードもこのタイプの認証を行うように構成する必要があります。

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 B「アクセス制御ディレクティブ書式」および付録 F「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。

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
読込み	属性値を読み込む権限。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

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・ポイントでは、エントリおよび属性の両方を対象に、すべての人に、エントリ内の全属性の「読込み」、「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

次の表では、LDAP 操作と、各操作の実行に必要なアクセス権をリストしています。

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

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）

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、3-10 ページの「タスク 3: デフォルト・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」をクリックします。

注意： 変更内容を反映するには、Oracle Directory Manager を再起動する必要があります。

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、「*Directory Server Instance*」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」をクリックします。

Oracle Directory Manager を使用した ACP の表示

12-13 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」>「*Directory Server Instance*」>「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」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」ペインには次の 3 つのフィールドがあります。

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。このポイントまでツリーを下位方向へナビゲートすると、このポイントへのパスがこのフィールドに表示されます。新しい ACP を作成する場合は、このフィールドに新規 ACP へのパスを入力する必要があります。
構造型アクセス項目（エントリ・レベル操作）	エントリへのアクセス権のリストです。「構造型アクセス項目」ボックスにリストされている項目は、次のカテゴリによってエントリを識別します。 ■ 責任者 : アクセス権を付与する人またはエンティティ（対象） ■ バインド・モード : バインド・モード（認証）が使用されているかどうか ■ アクセス権限 :「参照」、「追加」、「プロキシ」および「削除」 **関連項目 :** 構造的なアクセス項目の変更方法は、12-32 ページの「タスク 2: 構造型アクセス項目の変更」を参照してください。

フィールド	説明
コンテント・アクセス項目（属性レベル操作）	「エントリ・フィルタ」列に定義されているエントリまたはエンティティ内の属性に対するアクセス権のリストです。このウィンドウには次の列があります。 ■ 責任者 : アクセス権を付与する人またはエンティティ（対象） ■ バインド・モード : バインド・モード（認証）が使用されているかどうか ■ Op: 属性に対して実行される一致操作。選択肢は「EQ」（=）と「NEQ」（!=）です。 ■ 属性 : アクセス権が付与または否認される特定の属性（オブジェクト）。 ■ アクセス権限 :「読込み」、「検索」、「書込み」、「自己書込み」または「比較」。 **関連項目 :** コンテント・アクセス項目の変更方法は、12-35 ページの「タスク 3: コンテント・アクセス項目の変更」を参照してください。

12-13 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」>「*Directory Server Instance*」の順に展開し、「エントリ管理」を選択します。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。
2. 「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。
3. 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（つまり、エントリに関係する ACI）を構成します。
- タスク 3: コンテント・アクセス項目（つまり、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. 12-13 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」>「*Directory Server Instance*」の順に展開します。

   b. 「アクセス制御管理」を選択し、ステップ 2 に進みます。

   12-13 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」>「*Directory Server Instance*」>「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。次のいずれかの方法で、識別名を検索できます。

   - 「エントリへのパス」フィールド右側の「参照」をクリックします。
   - 「エントリ管理」の下のナビゲータ・ペインを検索します。

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（つまり、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 4 つのタブがあります。

2. ACP の下位エントリすべてを 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、次のステップに進みます。

   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. 「基準」バーの一番左のメニューから、属性の型を選択します。

   b. バーの中央のメニューから、次のフィルタ・オプションのいずれかを選択します。

フィルタ	説明
開始	属性値の始めの数文字のみを使用して検索します。
終了	指定した属性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。
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。
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。
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。アルファベットの先頭により近いエントリが、アルファベット順で上位とされます。
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。アルファベットの先頭により近いエントリが、アルファベット順で下位とされます。
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。たとえば、「cn」「存在」と指定すると、ツリーのそのレベルで、cn 属性値を持つすべてのエントリが取り出されます。

   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には、次の手順を実行します。

   a. 「基準」バーの一番左のメニューから、属性の型を選択します。

   b. バーの中央のメニューから、次のフィルタ・オプションのいずれかを選択します。

フィルタ	説明
開始	属性値の始めの数文字のみを使用して検索します。
終了	指定した属性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。
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。
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。
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。アルファベットの先頭により近いエントリが、アルファベット順で上位とされます。
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。アルファベットの先頭により近いエントリが、アルファベット順で下位とされます。
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。たとえば、「cn」「存在」と指定すると、ツリーのそのレベルで、cn 属性値を持つすべてのエントリが取り出されます。

   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・ページを選択します。

   a. 「バインド・モード」リストから、対象（つまり、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。次の 5 つのバインド・モードの中から選択します。

バインド・モード	説明
なし	認証なし
SSL 認証なし	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。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。
SSL 双方向	クライアントとサーバーは、相互に自己認証を行います。これは、相互に証明書を送信する方法で行われます。
簡易	クライアントは、ネットワーク上を平文で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。サーバーは、クライアントが送信した識別名とパスワードが、ディレクトリに保存されている識別名とパスワードに一致しているかどうかを検証します。

   バインド・モードは、対象の指定においてはオプションです。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バインド・モードは、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。

   b. アクセス権を付与するエンティティを指定します。

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込み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。

エンティティ	説明
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。

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: コンテント・アクセス項目の構成

1. コンテント・アクセス項目（つまり、属性に関係する ACI）を定義するには、「コンテント・アクセス項目」ウィンドウの下の「作成」をクリックします。「コンテント・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 の下位エントリすべてを 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、次のステップに進みます。

   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。適切な場合は、「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. 「基準」バーの一番左のメニューから、属性の型を選択します。
   b. バーの中央のメニューから、次のフィルタ・オプションのいずれかを選択します。

フィルタ	説明
開始	属性値の始めの数文字のみを使用して検索します。
終了	指定した属性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。
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。
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。
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。アルファベットの先頭により近いエントリが、アルファベット順で上位とされます。
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。アルファベットの先頭により近いエントリが、アルファベット順で下位とされます。
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。たとえば、「cn」「存在」と指定すると、ツリーのそのレベルで、cn 属性値を持つすべてのエントリが取り出されます。

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. 「バインド・モード」リストから、対象（つまり、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。次の 5 つのバインド・モードの中から選択します。

バインド・モード	説明
なし	認証なし
SSL 認証なし	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。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。
SSL 双方向	クライアントとサーバーは、相互に自己認証を行います。これは、相互に証明書を送信する方法で行われます。
簡易	クライアントは、ネットワーク上を平文で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。サーバーは、クライアントが送信した識別名とパスワードが、ディレクトリに保存されている識別名とパスワードに一致しているかどうかを検証します。

バインド・モードは、対象の指定においてはオプションです。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バインド・モードは、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。

b. アクセス権を付与するエンティティを指定します。

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込み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。

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、表 12-1 の説明に従って各項目を指定します。

表 12-1　属性に関するアクセス権

アクセス権	説明
読込み	属性値を読み込む権限。属性に対して読取り権限が与えられている場合でも、エントリ自体にブラウズ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。

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（つまり、エントリに関係する ACI）を構成します。
- タスク 3: コンテント・アクセス項目（つまり、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. 12-13 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」>「*Directory Server Instance*」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、ステップ 2 に進みます。

   12-13 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」>「*Directory Server Instance*」>「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。

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. ウィザードを使用して構造型アクセス項目（つまり、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。

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。

規範的な構造型アクセス項目を指定した場合は、ACP の下位エントリすべてをこの 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。

1. 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. 「基準」バーの一番左のメニューから、属性の型を選択します。
   b. バーの中央のメニューから、次のフィルタ・オプションのいずれかを選択します。

フィルタ	説明
開始	属性値の始めの数文字のみを使用して検索します。
終了	指定した属性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。
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。
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。
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。アルファベットの先頭により近いエントリが、アルファベット順で上位とされます。
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。アルファベットの先頭により近いエントリが、アルファベット順で下位とされます。
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。たとえば、「cn」「存在」と指定すると、ツリーのそのレベルで、cn 属性値を持つすべてのエントリが取り出されます。

   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」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。

2. 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には、次の手順を実行します。

   a. 「基準」バーの一番左のメニューから、属性の型を選択します。

   b. バーの中央のメニューから、次のフィルタ・オプションのいずれかを選択します。

フィルタ	説明
開始	属性値の始めの数文字のみを使用して検索します。
終了	指定した属性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。
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。
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。
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。アルファベットの先頭により近いエントリが、アルファベット順で上位とされます。
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。アルファベットの先頭により近いエントリが、アルファベット順で下位とされます。
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。たとえば、「cn」「存在」と指定すると、ツリーのそのレベルで、cn 属性値を持つすべてのエントリが取り出されます。

   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」を選択します。ウィザードによって、認証タイプ（バインド・モードと呼ばれます）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. バインド・モードは、対象の指定においてはオプションです。認証方式を設定しない場合、または「なし」を選択する場合は、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バインド・モードは、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（バインド・モード）を指定するには、「バインド・モード」リストから、対象（つまり、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。次の 5 つのバインド・モードの中から選択します。

   b. アクセス権を付与するエンティティを指定するには、次のいずれか 1 つを選択します。

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込み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。

4. 「次」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。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。

5. 「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ト・アクセス項目の構成

ウィザードを使用してコンテント・アクセス項目（つまり、属性に関係する ACI）を定義するには、「コンテント・アクセス項目」ウィンドウの下の「作成」をクリックします。最初の「コンテント・アクセス項目」ダイアログ・ボックスが表示されます。

規範的なコンテント・アクセス項目を指定した場合は、ACP の下位エントリすべてをこの ACP が管理します。規範的なコンテント・アクセス項目を希望する場合は、この最初の「コンテント・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。

1. 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. 「基準」バーの一番左のメニューから、属性の型を選択します。
   b. バーの中央のメニューから、次のフィルタ・オプションのいずれかを選択します。

フィルタ	説明
開始	属性値の始めの数文字のみを使用して検索します。
終了	指定した属性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。
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。
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。
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。アルファベットの先頭により近いエントリが、アルファベット順で上位とされます。
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。アルファベットの先頭により近いエントリが、アルファベット順で下位とされます。
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。たとえば、「cn」「存在」と指定すると、ツリーのそのレベルで、cn 属性値を持つすべてのエントリが取り出されます。

   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」をクリックします。アクセス権を付与する人の指定を要求する、2 番目の「コンテント・アクセス項目」ダイアログ・ボックスが表示されます。

2. 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（バインド・モードとも呼びます）を指定します。

   バインド・モードは、対象の指定においてはオプションです。認証方式を設定しない場合、または「なし」を選択する場合は、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バインド・モードは、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。

   次の 5 つのバインド・モードの中から選択します。

バインド・モード	説明
なし	認証なし
SSL 認証なし	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。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。
SSL 双方向	クライアントとサーバーは、相互に自己認証を行います。これは、相互に証明書を送信する方法で行われます。
簡易	クライアントは、ネットワーク上を平文で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。サーバーは、クライアントが送信した識別名とパスワードが、ディレクトリに保存されている識別名とパスワードに一致しているかどうかを検証します。

3. アクセス権を付与するエンティティを指定します。

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込み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。

エンティティ	説明
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。

4. 「次」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、「コンテント・アクセス項目」ダイアログ・ボックスが表示されます。
5. 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には、次の手順を実行します。
   a. 「コンテント・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」をクリックします。アクセス権の指定を要求する「コンテント・アクセス項目」ダイアログ・ボックスが表示されます。
6. 表 12-2 の説明に従って、付与する権限の種類を指定します。

表 12-2 属性に関するアクセス権

アクセス権	説明
読込み	属性値を読み込む権限。属性に対して読取り権限が与えられている場合でも、エントリ自体にブラウズ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。

7. 「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（つまり、エントリに関係する ACI）を変更します。
- タスク 3: コンテント・アクセス項目（つまり、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. 12-13 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」>「*Directory Server Instance*」>「アクセス制御管理」の順に展開します。「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、定義済みのすべての 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。

   12-13 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」>「*Directory Server Instance*」>「アクセス制御管理」の順に展開し、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。

   b. 「編集」をクリックします。「サブツリーの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。

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、12-17 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 の下位エントリすべてを ACP で管理する場合は、次のステップに進んでください。

   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. 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、次のフィルタ・オプションのいずれかを選択します。

フィルタ	説明
開始	属性値の始めの数文字のみを使用して検索します。
終了	指定した属性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。
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。
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。
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。アルファベットの先頭により近いエントリが、アルファベット順で上位とされます。
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。アルファベットの先頭により近いエントリが、アルファベット順で下位とされます。
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。たとえば、「cn」「存在」と指定すると、ツリーのそのレベルで、cn 属性値を持つすべてのエントリが取り出されます。

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ために 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には、次の手順を実行します。

   a. 「基準」バーの一番左のメニューから、属性の型を選択します。

   b. バーの中央のメニューから、次のフィルタ・オプションのいずれかを選択します。

フィルタ	説明
開始	属性値の始めの数文字のみを使用して検索します。
終了	指定した属性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。
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。
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。
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。アルファベットの先頭により近いエントリが、アルファベット順で上位とされます。
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。アルファベットの先頭により近いエントリが、アルファベット順で下位とされます。
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。たとえば、「cn」「存在」と指定すると、ツリーのそのレベルで、cn 属性値を持つすべてのエントリが取り出されます。

   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、ACI の対象（つまり、アクセス権を要求しているエンティティ）を指定します。

   a. 対象が使用するバインド・モードと呼ばれる認証のタイプを指定します。次の 5 つのバインド・モードの中から選択します。

バインド・モード	説明
なし	認証なし
SSL 認証なし	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。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。
SSL 双方向	クライアントとサーバーは、相互に自己認証を行います。これは、相互に証明書を送信する方法で行われます。
簡易	クライアントは、ネットワーク上を平文で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。サーバーは、クライアントが送信した識別名とパスワードが、ディレクトリに保存されている識別名とパスワードに一致しているかどうかを検証します。

バインド・モードは、対象の指定においてはオプションです。ディレクティブを適用する場合、あるノードで指定されているバインド・モードは、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。

b. アクセス権を付与するエンティティを指定します。

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込み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。

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（「参照」、「追加」、「削除」または「プロキシ」）を決定します。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。
   b. 「OK」をクリックします。

タスク 3: コンテント・アクセス項目の変更

新規コンテント・アクセス項目を追加、または既存のコンテント・アクセス項目を変更できます。

> **関連項目：** コンテント・アクセス項目の追加の詳細は、12-20 ページの「タスク 3: コンテント・アクセス項目の構成」を参照してください。

コンテント・アクセス項目を変更する手順は、次のとおりです。

1. 「コンテント・アクセス項目」ボックスで変更するコンテント・アクセス項目を選択し、「コンテント・アクセス項目」ウィンドウの下の「編集」をクリックします。「コンテント・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 の下位エントリすべてを 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、次のステップに進みます。

   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。適切な場合は、「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. 「基準」バーの一番左のメニューから、属性の型を選択します。
   b. バーの中央のメニューから、次のフィルタ・オプションのいずれかを選択します。

フィルタ	説明
開始	属性値の始めの数文字のみを使用して検索します。
終了	指定した属性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。
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。

フィルタ	説明
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。
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。アルファベットの先頭により近いエントリが、アルファベット順で上位とされます。
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。アルファベットの先頭により近いエントリが、アルファベット順で下位とされます。
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。たとえば、「cn」「存在」と指定すると、ツリーのそのレベルで、cn 属性値を持つすべてのエントリが取り出されます。

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. 「バインド・モード」リストから、対象（つまり、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。次の 5 つのバインド・モードの中から選択します。

バインド・モード	説明
なし	認証なし
SSL 認証なし	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。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。
SSL 双方向	クライアントとサーバーは、相互に自己認証を行います。これは、相互に証明書を送信する方法で行われます。
簡易	クライアントは、ネットワーク上を平文で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。サーバーは、クライアントが送信した識別名とパスワードが、ディレクトリに保存されている識別名とパスワードに一致しているかどうかを検証します。

バインド・モードは、対象の指定においてはオプションです。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バインド・モードは、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。

b. アクセス権を付与するエンティティを指定します。

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込み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。

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、表 12-1 の説明に従って各項目を指定します。

表 12-3　属性に関するアクセス権

アクセス権	説明
読込み	属性値を読み込む権限。属性に対して読取り権限が与えられている場合でも、エントリ自体にブラウズ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。

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」>「*Directory Server Instance*」>「エントリ管理」の順に展開します。次のいずれかの方法で起動できます。
   - 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。
   - 検索パネルを使用してエントリを検索し、エントリをダブルクリックして「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、「構造型アクセス項目」ボックスと「コンテント・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、入力した情報は、単に Oracle Directory Manager のキャッシュに入れられます。

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、読込みと変更は各パスワードの所有者（つまり、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」>「*Directory Server Instance*」の順に展開し、「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。
2. 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。

3. 「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」、「責任者」および「アクセス権限」の 3 つのタブがあります。

   ACP の下位エントリすべてに 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. 「責任者」タブ・ページを選択して、ACI の対象を定義します。「バインド・モード」リストから、使用中の環境に適した認証モードを選択します。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。

3. 「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ブラウズでき、追加や削除はできないようにアクセス権を変更します。

   b. 「OK」をクリックします。

コンテント・アクセス項目の構成 この例の 4 つの ACI は、同じ構造のコンテンツ項目情報を使用します。これらは、許可するコンテント・アクセスのみが異なります。次に、ACI のコンテント・アクセスを作成する方法を説明します。

コンテント・アクセス項目を定義する手順は、次のとおりです。

1. 「コンテント・アクセス項目」ボックスの下の「作成」をクリックします。「コンテント・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・ページで、「すべての人」を選択します。

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。

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。読込み、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。

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込み、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. 「コンテント・アクセス項目」ボックスの下の「作成」をクリックします。「コンテント・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。「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です。」をクリックします。
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。
4. 「アクセス権限」タブ・ページを選択します。

   読込み、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。
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` 属性の読込み、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、その属性の読込み、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込み、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. 「コンテント・アクセス項目」フィールドの下の「作成」をクリックして、「コンテント・アクセス項目」を表示します。
2. 「責任者」タブ・ページを選択します。「すべての人」を選択します。
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。
4. 「アクセス権限」タブ・ページを選択します。

   読込み、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。
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込み、ブラウズ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. 「コンテント・アクセス項目」フィールドの下の「作成」をクリックして、「コンテント・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。

   「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です。」をクリックします。
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。
4. 「アクセス権限」タブ・ページをクリックします。

   読込み、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。
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。

他に必要なアクセス制限があるかどうかを検討してください。使用中のディレクトリには、使用者を制限する必要のあるエントリや属性が多数存在している場合があります。

コマンドライン・ツールを使用したアクセス制御の管理

12-2 ページの「アクセス制御ポリシー・ポイントの管理の概要」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・ポイントの情報は、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 B「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-28 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 B「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 ドメイン内のエントリすべてについて、誰もがすべての属性を読込み、検索し、かつすべてのエントリをブラウズする権限をもつことになります。

dc=com の ACP 内の orclACI 属性

```
access to entry by * (browse)
access to attr=(*) by * (search, read)
```

属性の読込みを許可する際には、エントリにブラウズ権限を付与しなければ読込み権限がエントリの属性に付与されません。

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 によって規程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、削除およびブラウズ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、サブツリーのブラウズが可能ですが、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、本人による読込みおよび書込みが可能で、参照はどのユーザーも可能です。
- 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、読込みは可能ですが、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込み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)
```

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。

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 の評価の優先順位規則
- 同一オブジェクトに対する複数 ACI
- オブジェクトに対する排他的アクセス権
- グループの場合の ACL 評価

ACL の評価の優先順位規則

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` 属性の定義済み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。次のようなコマンドを実行します。

```
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。次のようなコマンドを実行します。

```
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。次のようなコマンドを実行します。

   ```
   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。次のようなコマンドを実行します。

   ```
   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。次のようなコマンドを実行します。

   ```
   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。次のようなコマンドを実行します。

   ```
   access to attr=(*)
   by group1 (read, write)
   ```

同一オブジェクトに対する複数 ACI

同じ ACP において、同一オブジェクトの ACI が 2 つ以上ある場合、チェックされる ACI は 1 つのみで、他はすべて無視されます。たとえば、同じ ACP において、同一エントリに対して次の 2 つの ACI が存在しているとします。

- ACI #1:

  ```
  access to entry
         by dn="cn=admin, dc=us,dc=acme,dc=com" (browse, add, delete)
  ```

- ACI #2:

  ```
  access to entry
         by dn="cn=manager,dc=us,dc=acme,dc=com" (search, read)
  ```

ACI #2 が最初にチェックされた場合は、ACI #1 で管理者に限定的に付与されているアクセス権は無視されます。この場合に管理者がエントリに対するアクセスを要求すると、そのアクセス権はこのレベルの階層では解決されません。解決するには、階層を段階的に上に移動して評価する必要があります。解決されない場合は、すべてのアクセス権が否認されます。

解決策は、同じ ACP において、このエントリに対して作成する ACI を 1 つのみにすることです。次のようなコマンドを実行します。

```
access to entry
    by dn="cn=admin, dc=us,dc=acme,dc=com" (browse, add, delete)
    by dn="cn=manager,dc=us,dc=acme,dc=com" (search, read)
```

同様に、属性レベルにおいて、次の 2 つの ACI が設定されているとします。

- ACI #1:

```
access to attr=(userpassword)
        by dnattr=(".*,dc=us,dc=acme,dc=com") (none)
```

- ACI #2:

```
access to attr=(userpassword)
        by self (read, write)
```

ACI #1 が最初に戻された場合は、ACI #2 でユーザー自身に付与されているアクセス権は無視されます。ユーザーがパスワードを変更しようとすると、アクセス権は付与されません。

エントリに対する ACI と同様に、解決策は、同じ ACP においてこの属性に対して作成する ACI を 1 つのみにすることです。次のようなコマンドを実行します。

```
access to attr=(userpassword)
    by dnattr=(".*,dc=us,dc=acme,dc=com) (none)
    by self (read, write)
```

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 によるその属性（またはエントリ）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。

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。

13

一般的な配置の考慮事項

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 : パーティションとレプリカ
- フェイルオーバーに関する考慮事項
- 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 インストールの実行

関連項目：

- 容量計画の詳細は、第 18 章「容量計画に関する考慮事項」を参照してください。
- 高可用性の詳細は、第 20 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 19 章「チューニングに関する考慮事項」を参照してください。
- クラスタ環境におけるフェイルオーバーの詳細は、第 VI 部の「ディレクトリとクラスタ」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

ディレクトリ情報ツリー（DIT）の構造とネーミングについて効果的なポリシーを設定するには、企業全体の調整と計画が必要です。たとえば、次のような疑問が生じます。

- 企業のディレクトリのネーミングと編成をどのようにして選択するのか？
- 企業の組織構造や地理的および国の境界を選択に反映させる必要があるか？
- 選択したものは、Novell の eDirectory ソリューションや Microsoft Active Directory などの NOS ディレクトリにシームレスにつながるか？

この項では、次の項目について説明します。

- ディレクトリ・エントリのネーミング
- ディレクトリ情報ツリーの階層と構造

ディレクトリ・エントリのネーミング

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。一方で、必要となる管理ポリシーが増加することにより、識別名がわかりにくくなります。

ディレクトリ情報ツリーの階層と構造

ディレクトリ情報ツリーは、DNS（ドメイン・ネーム・システム）と同様に、構造の中で階層になっています。企業に対応付けられた論理階層を反映するように、ディレクトリ情報ツリーを編成できます。その選択は、次のものに対応する必要があります。

- 企業全体のディレクトリ情報ツリー構造とネーミング・ポリシーは、部門単位の NOS ディレクトリの規則および制限と互換性を持つ必要があります。たとえば、ディレクトリ製品には、最初にドメインを定義して、組織単位と地域が論理的にそれらのドメインに従属することが必要な場合があります。また、**兄弟関係**ではないエントリに対しても、ドメイン内でディレクトリ名が一意であることを必須とするディレクトリ製品もあります。

- ディレクトリ編成は、明確で効果的なアクセス制御とレプリケーション・ポリシーを促進する必要があります。**ACL** 管理の委任が必須の企業では、データ所有権の境界を反映するようにディレクトリ情報ツリーを編成すると便利です。

  たとえば、主要な地域ごとに自律型データ・センターを持つ企業を仮定します。アメリカ（北米と南米）、ヨーロッパおよびアジア太平洋地域に 1 つずつあるとします。この企業が、地域のデータ・センターの管理の自律性を保ちながら、そのグローバル・ディレクトリを整理統合するとします。この企業は、**ネーミング・コンテキスト**が各地域に対応するようにディレクトリを編成する必要があります。これは、地域のニーズに合ったアクセス制御とレプリケーション・ポリシーの作成を容易にします。

- 企業の部門構造または組織階層を反映するようにディレクトリ階層を編成するのがよい場合があります。ほとんどの企業は頻繁に組織の再編成や部門の再構成を行うので、通常はこの方法はお薦めできません。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。

物理的な分散 : パーティションとレプリカ

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 1 箇所から他への接続

関連項目： 2-21 ページ「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
- パーティション化に関する考慮事項
- レプリケーションに関する考慮事項

理想的な配置

理想的には、中央の整理統合されたディレクトリ・サーバーにすべてのネーミング・コンテキストを格納することが、より単純かつ安全と考えられます。問題は、この中央のディレクトリ・サーバーが障害の発生箇所となった場合です。

単純な解決策は、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。

Oracle Internet Directory のマルチマスター・レプリケーションでは、ディレクトリの論理的な統合が容易です。どこでも更新可能な構成ができるので、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も、より効率的で費用がかからなくなりました。

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・ポイントを各ネーミング・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、13-7 ページの「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。

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能か、あるい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**アドバンスト・レプリケーション（ASR）**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い可用性

  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。

フェイルオーバーに関する考慮事項

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。

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 20 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。
- クラスタ環境におけるフェイルオーバーの詳細は、第 VI 部の「ディレクトリとクラスタ」を参照してください。

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
- サイズ設定に関する考慮事項
- チューニングに関する考慮事項

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

次の表は、Oracle Internet Directory の様々な配置の使用例に必要となる CPU の能力の概算レベルを、現在の経験に基づいて示したものです。

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。次の表は、様々なサイズのディレクトリ情報ツリーに必要な、概算のディスク領域要件を示しています。

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。次の表は、様々なディレクトリ情報ツリー・サイズのメモリー要件の見積りを示しています。

ディレクトリのタイプ	エントリ数	最低メモリー
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 18 章「容量計画に関する考慮事項」

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・テクニックは、次のようなものです。

  – 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テクニックの詳細は、第 19 章「チューニングに関する考慮事項」を参照してください。

1 つのホストにおける複数の Oracle Internet Directory インストールの実行

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。

関連項目： 同一ホスト上にある 2 つの Oracle Internet Directory のインストール間でレプリケーションを構成するには、22-31 ページの「ホストから独立したものとしてのノードの識別」を参照してください。

14

Oracle のコンポーネントと Oracle Internet Directory

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。この章で説明する内容は、次のとおりです。

- 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・ディレクトリ情報ツリー構造
- ホスト・アプリケーション環境のニーズに対応するためのデフォルト・ディレクトリ情報ツリー構造の変更方法

この章では、次の項目について説明します。

- Oracle のコンポーネントとディレクトリ使用の概要
- すぐに使用可能なデフォルト構成
- デフォルトのサブスクライバ構成
- Oracle のコンポーネントのセキュリティ要件

Oracle のコンポーネントとディレクトリ使用の概要

Oracle Internet Directory によって、Oracle のコンポーネントは次の内容を実現できます。

- アプリケーション環境全体で各ユーザーに対して単一のグローバル ID を保持できます。
- コンポーネントの構成情報を中央に格納して管理できます。

この章では、2 種類の一般的な環境について考察します。

- ホスト : 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・プロバイダのような 1 つの企業が、Oracle のコンポーネントを他の複数の企業で利用できるようにし、それらの企業にかわって情報を格納します。このようなホスティングされた環境の場合、ホスティングを行う企業はデフォルト・サブスクライバと呼ばれ、ホスティングされる企業はサブスクライバと呼ばれます。グローバル管理者は、ディレクトリ全体にわたるアクティビティを実行します。**委任管理者**と呼ばれる他のタイプの管理者が、特定のサブスクライバ・ドメイン内または特定のアプリケーションに対するロールを実行できます。
- 非ホスト : ホスティングされていない環境では、Oracle Internet Directory をインストールして Oracle のコンポーネントとともに使用する企業がデフォルト・サブスクライバと呼ばれ、サブスクライバは存在しません。

ディレクトリ・スキーマとディレクトリ情報ツリーの要件は、この両方の配置モデルに対応できるように柔軟に定義されています。

すぐに使用可能なデフォルト構成

Oracle のコンポーネントを Oracle Internet Directory とともに簡単に使用できるように、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が作成されます。デフォルトのディレクトリ情報ツリー・フレームワークは、ホスティングされた環境とホスティングされていない環境のいずれでも同じです。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、配置ニーズに応じて適切に変更できます。

Oracle Internet Directory のインストール時に、Oracle Universal Installer によって、次の内容が作成されます。

- ベース・スキーマ要素（つまり、属性とオブジェクト・クラス）。Internet Engineering Task Force（IETF）で定義されている要素と、Oracle コンポーネント固有の要素があります。
- ルート Oracle コンテキスト。サイト全体にわたる Oracle の全コンポーネントに共通する情報を格納するディレクトリ・コンテナです。
- デフォルト・サブスクライバの Oracle コンテキスト。サブスクライバのサブツリー内の Oracle の全コンポーネントに共通する情報が格納されます。

- サブスクライバの Oracle コンテキスト。サブスクライバのサブツリー内の Oracle の全コンポーネントに共通する情報が格納されます。
- 各サブスクライバのデフォルトのパスワード・ポリシー。このパスワード・ポリシーは、サブスクライバ・ユーザー・ベース内の全ユーザーに適用されます。

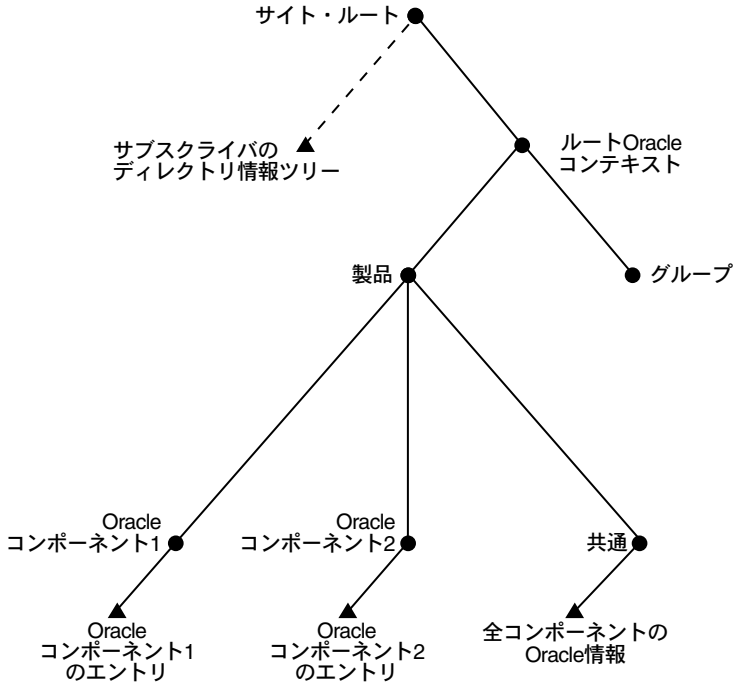
ルート Oracle コンテキスト

ルート Oracle コンテキストには、次の情報が格納されます。

- デフォルトのパラメータ設定、デフォルトのプロファイルおよびデフォルトの認可ポリシーなどのメタデータを含む、サイト全体の情報。
- 各サブスクライバに対して必要な情報を検索するための、ホスティングされた環境での Oracle のコンポーネント用検出メカニズム。

図 14-1 は、ルート Oracle コンテキストの編成を示しています。

図 14-1 ルート Oracle コンテキスト



次の検出関連情報は、ルート Oracle コンテキストに格納されます。

- サブスクライバ検索ベース（`orclSubscriberSearchBase`）

  この属性は、すべてのサブスクライバが配置されるディレクトリ情報ツリー内のノードを識別します。この属性は、サブスクライバの位置の特定が必要なすべての製品に対して共通のポイントを提供するため、ホスティングされた環境の場合は特に重要になります。たとえば、図 14-1 の「サブスクライバ」は、サブスクライバの位置を特定するための検索ベースとして機能します。ホスティングされていない環境の場合、この属性の値はデフォルト・サブスクライバの親を指し示します。

- サブスクライバ・ニックネーム属性（`orclSubscriberNickNameAttribute`）

  この属性は、サブスクライバ検索ベースの下でサブスクライバを検索するときに使用するニックネーム属性を識別します。たとえば、サブスクライバは通常、組織で表されるため、「o」属性をニックネーム属性として使用できます。

- デフォルト・サブスクライバ（`orclDefaultSubscriber`）

  この属性は、ディレクトリ情報ツリーのデフォルト・サブスクライバ・ノードを指し示します。

ホスティングされた環境とホスティングされていない環境のいずれでも、コンポーネントは `orclSubscriberSearchBase` 属性および `orclSubscriberNickNameAttribute` 属性を使用して、ディレクトリ情報ツリー内の正しいノードを検索します。適切なサブツリーを検出すると、コンポーネントは、そのサブツリーの Oracle コンテキストからサブスクライバ固有の必要な情報を取得します。

たとえば、Oracle9*i*AS Single Sign-On は、ホスティングされた環境でユーザーを認証するためにこのフレームワークを使用します。Oracle9*i*AS Single Sign-On では、ユーザーがログインするときに、サブスクライバ名の指定を求めるプロンプトが表示されます。また、Oracle9*i*AS Single Sign-On Server では、エントリを検索するときに、`orclSubscriberSearchBase` 属性および `orclSubscriberNickName` 属性を使用して、ディレクトリ情報ツリー内の正しいサブスクライバ・ノードを検出します。サブスクライバ固有の情報が存在する位置を確認した後、サブスクライバ固有の Oracle コンテキストを調べてユーザーの位置を特定します。

クライアントがサブスクライバを指定しないと、Oracle Internet Directory では、ユーザーはデフォルト・サブスクライバ・サブツリーの情報を検索していると認識されます。

サブスクライバの Oracle コンテキスト

サブスクライバ固有の Oracle コンテキストには、次の情報が格納されます。

- サブスクライバのサブツリーで必要な情報を検索するための、Oracle のコンポーネント用検出メカニズム。
- サブスクライバに固有の Oracle コンポーネント・データ。
- 他のサブスクライバからサブスクライバを保護する、サブスクライバ・ノードのアクセス・ポリシー。
- 「共通」コンテナに配置される全ユーザーに適用可能なデフォルトのパスワード・ポリシー。`orclCommonUserSearchBase` 属性に適切な値を設定して、パスワード・ポリシーが正しく施行されるようにします。つまり、対応する属性が `orclCommonUserSearchBase` の値と一致する場合は常に、そのパスワード・ポリシーがユーザーに適用されます。

図 14-2 は、サブスクライバ固有の Oracle コンテキストの編成を示しています。

図 14-2 サブスクライバ固有の Oracle コンテキスト

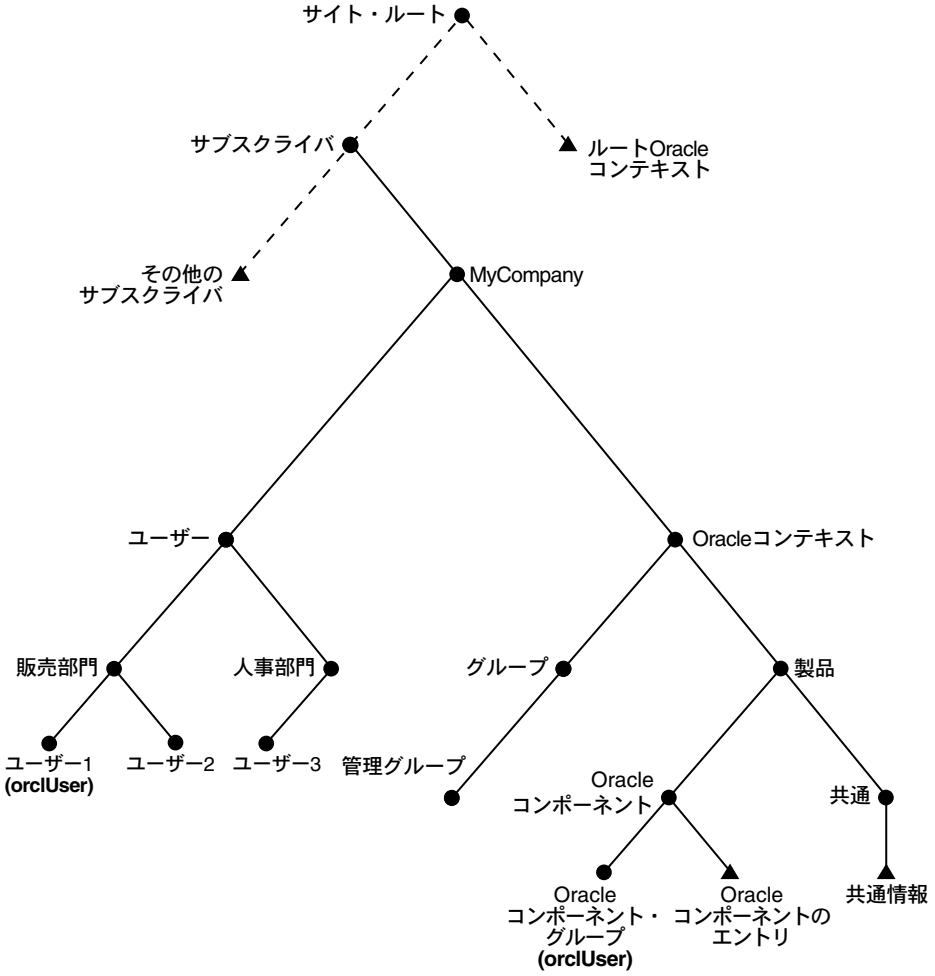


図 14-2 は、ある Oracle コンポーネント、およびすべてのコンポーネントに共通する情報を格納するディレクトリにおける、サブスクライバ全体の情報を示しています。次の 2 つの側面を表しています。

- デフォルト・サブスクライバの例を、「ユーザー」というコンテナの下に示しています。
- デフォルト・ユーザーの例を、「Oracle コンテキスト」というコンテナの下に示しています。

サブスクライバ固有の Oracle コンテキストの「共通」エントリには、ユーザーとグループの位置を特定するための情報が格納されています。具体的には、次の情報が含まれています。

- ユーザー検索ベース（`orclCommonUserSearchBase`）

  この属性は、サブスクライバのディレクトリ情報ツリーの中で、すべてのユーザーが配置されるノードを指定します。たとえば、図 14-2（14-6 ページ）の「ユーザー」は、サブスクライバの中でユーザーを検索する際の検索ベースとして機能します。

- ユーザー・ニックネーム属性（`orclCommonNickNameAttribute`）

  この属性は、ユーザー検索ベースの下でユーザーを検索するときに使用するニックネーム属性を指定します。たとえば、Oracle9*i*AS Single Sign-On では、ユーザーがログインするときに、この属性値の指定を求めるプロンプトが表示されます。

- グループ検索ベース（`orclCommonGroupSearchBase`）

  この属性は、サブスクライバのディレクトリ情報ツリーの中で、すべてのグループを検索できるノードを指定します。

- ユーザー・エントリの作成に使用されるオブジェクト・クラス（`orclUserObjectClass`）

  この属性は、サブスクライバ・ツリーの下でユーザー・エントリを作成するときに使用されるオブジェクト・クラスのリストを指定します。たとえば、`person`、`organizationalPerson`、`inetOrgPerson`、`orclUser` などがあります。

ホスティングされた環境の場合、複数のサブスクライバに対してコンポーネントの特定のインスタンスを専用化できます。たとえば、各サブスクライバは、Oracle9*i*AS Portal のコンポーネントの独自のインスタンスを保持できます。この場合、個々のサブスクライバに必要なインスタンス情報およびその他のデータは、各サブスクライバの Oracle コンテキストに格納されます。すべてのサブスクライバに必要な一般情報は、ルート Oracle コンテキストに格納されます。

図 14-2 のユーザーとサブスクライバ間の点線は、サブスクライバ・サブツリーを柔軟に編成できることを示しています。作成したユーザー・データは、異なる方法で格納できます。たとえば、次の格納方法があります。

- サブスクライバ・ノードの下に直接格納
- 14-8 ページの図 14-3 のようにサブスクライバ・ツリーの外部に格納

図 14-3 サブスクライバとサブスクライバのユーザー情報を個別に格納

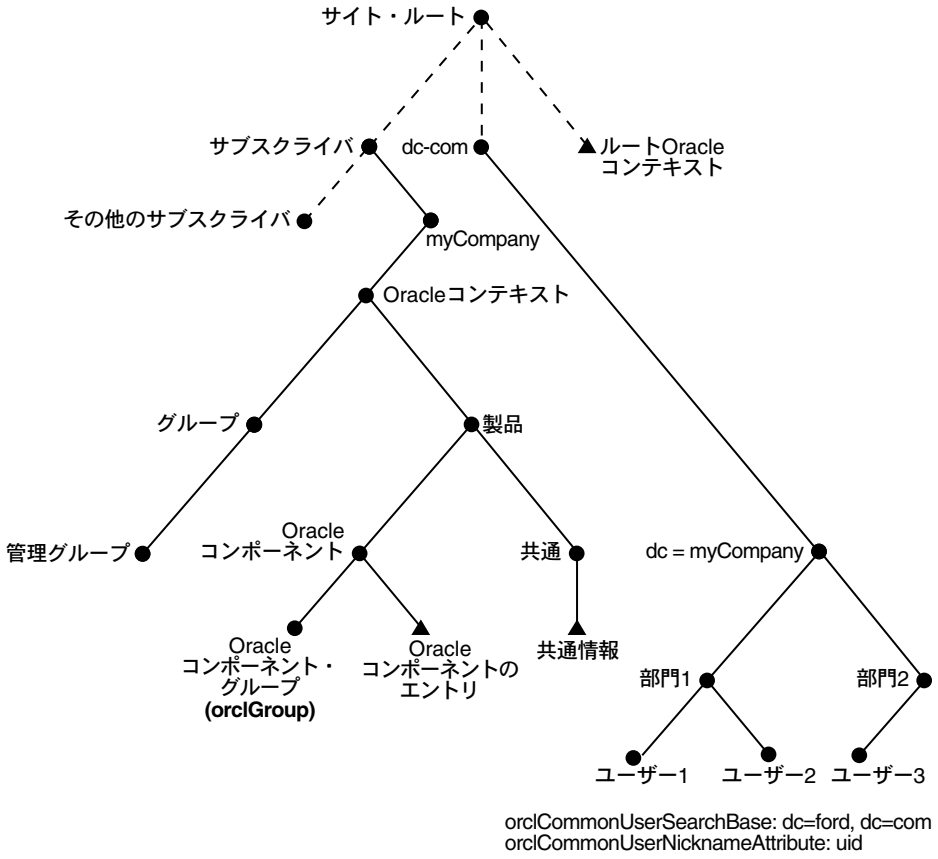
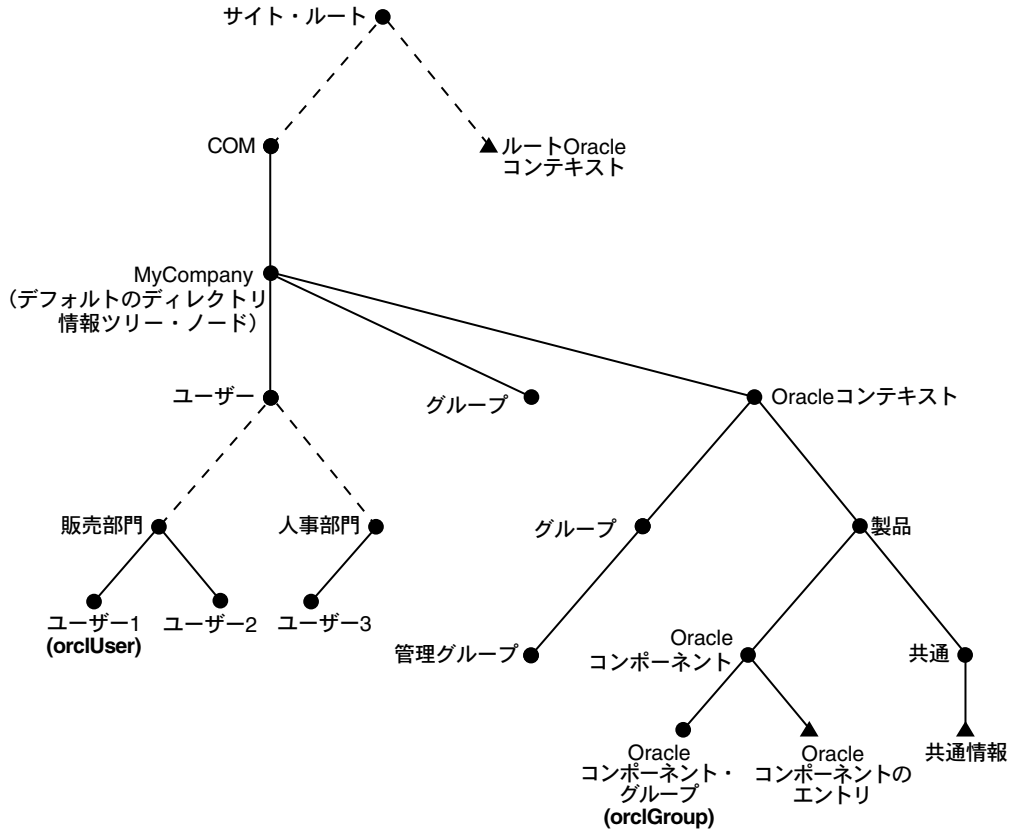


図 14-3 に示すように、サブスクライバのユーザーを、サブスクライバ・ノード自体の下に作成する必要はありません。図 14-3 の場合、各サブスクライバ固有の Oracle コンテキストの「共通」エントリで、`orclCommonUserSearchBase` 属性は、ユーザー・データが格納されているノード（`dc=myCompany,dc=com`）を指し示します。したがって、サブスクライバは、すでに保持している識別名をそのまま維持できます。異なるディレクトリ情報ツリー構造に移行する必要はありません。

デフォルトのサブスクライバ構成

図 14-4 は、ホスティングされていない環境でのデフォルト・サブスクライバのディレクトリ情報ツリーの例を示しています。

図 14-4 ホスティングされていない環境のデフォルト・ディレクトリ情報ツリー



Oracle Internet Directory のインストール時に、Oracle Universal Installer によって、Oracle Internet Directory をインストールしているサイトのドメイン情報が判断されます。この情報に基づいて、デフォルトのディレクトリ情報ツリー構造が確立されます。たとえば、Oracle Internet Directory が `My_Company.com` でインストールされると、Oracle Universal Installer はディレクトリ情報ツリーに次のノードを作成します。

- Oracle のすべてのコンポーネントに共通する情報を格納するルート Oracle コンテキスト
- 図 14-4 の `Com` で示されているノード
- My_Company ノードおよびその下の Oracle コンテキスト
- デフォルト・サブスクライバ・ノード（たとえば、My_Company.com）の下の「ユーザー」および「グループ」

企業でデフォルトのディレクトリ情報ツリーを使用する場合、ルート Oracle コンテキストでは何も構成する必要はありません。かわりに、配置するサブツリーの構造に従って、次の作業が必要です。

- デフォルト・サブスクライバ・ノードの Oracle コンテキストで、ユーザー検索ベースと関連検出情報を構成します。たとえば、14-9 ページの図 14-4 の配置では、ユーザー検索ベースと関連検出情報は、`cn=Products,cn=Oracle Context,o=GM` の下の「共通」コンテナにあります。
- 「ユーザー」コンテナにユーザー・エントリ、「グループ」コンテナにグループ・エントリを配置します（両方ともデフォルト・サブスクライバ・ノードの直下にあります）。

ホスティングされた環境の場合、サブスクライバは、ディレクトリ情報ツリーのデフォルト・サブスクライバ・ノード自体と同じレベルに作成します。

デフォルトのディレクトリ情報ツリー作成の一部として、各種ツールを使用してブートストラップを支援するシード・ユーザーも作成されます。ユーザーは、識別名 `cn=orclAdmin,cn=users,cn=my_company,dc=com` で識別されます。ユーザーの初期パスワードは、Oracle Internet Directory スーパー・ユーザーのパスワード（`cn=orcladmin`）と同じです。このユーザーにはデフォルトで、`cn=Users` コンテナ以下のユーザーの作成、削除および編集、または `cn=Groups` コンテナ以下のグループの作成、削除および編集が許可されています。

Oracle のコンポーネントのセキュリティ要件

多くの Oracle コンポーネントでは、Oracle Internet Directory 内のユーザー・エントリが管理され、それに対応する権限が必要です。次に例を示します。

- Oracle9*i*AS Single Sign-On Server では、ユーザーを認証するときに次が実行されます。
  - 独自の識別を使用して Oracle Internet Directory に接続します。
  - ユーザーが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します。

  このためには、Oracle9*i*AS Single Sign-On Server にユーザー・パスワードを比較する権限が必要です。さらに、Oracle9*i*AS Single Sign-On の Cookie をセットアップするには、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ために、Oracle9*i*AS 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として、Oracle Internet Directory にプロキシ・ユーザーとしてログインします。したがって、対応するプロキシ・ユーザー権限が必要です。

Oracle のコンポーネントで必要となる可能性のある権限には、次のものがあります。

- ユーザー・パスワードを読み込む権限と変更する権限
- ユーザー・パスワードを比較する権限
- アプリケーションにアクセスするユーザーにかわるプロキシとしての権限
- 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

デフォルトの Oracle Internet Directory セキュリティ構成は、配置のニーズにあわせて変更できます。特に、Oracle Internet Directory リリース 9.2 では、ユーザー・セキュリティ管理者グループと認証サービス・グループの構成を変更できます。

この項では、各グループについて説明します。次の項目について説明します。

- ユーザー・セキュリティ管理者グループ
- 認証サービス・グループ

ユーザー・セキュリティ管理者グループ

このグループは、セキュリティ関連の属性を管理します。このグループ自体は、Oracle Internet Directory のスーパー・ユーザー、または Oracle コンテキスト管理者グループのメンバーによって管理されます。

このグループの識別名は、`cn=oracleUserSecurityAdmins`、`cn=groups`、*`Oracle_Context_DN`* です。

デフォルトでは、Oracle Internet Directory はこのグループにルートの Oracle コンテキスト内で、`userpkcs12`、`orclpkcs12hint`、`userpassword`、`orclpassword` および `orclpasswordverifier` 属性の読込み、書込み、比較および検索を行う権限を付与します。

このグループのメンバーがサブスクライバの DIT を管理できるように、サブスクライバの Oracle コンテキスト内でこのグループに同様の権限を付与できます。

認証サービス・グループ

このグループは、Oracle Email Server などのような、Oracle Internet Directory に格納されているパスワードを使用してユーザーを認証するサービスで構成されます。この種のコンポーネントには、ユーザーが入力したパスワードを、そのユーザーの userpassword 属性の値と比較するための権限が必要です。

このグループ自体は、Oracle Internet Directory のスーパー・ユーザー、または Oracle コンテキスト管理者グループのメンバーによって管理されます。

このグループの識別名は、`cn=authenticationServices,cn=groups,`*`Oracle_Context_DN`* です。

デフォルトでは、Oracle Internet Directory はこのグループに、デフォルトのサブスクライバ DIT のユーザー・コンテナ内の `userpassword` 属性を比較する権限を付与します。

15

ディレクトリ・ベースのアプリケーション・セキュリティ

この章では、Oracle Internet Directory でのアクセス制御ポリシー・ポイントの格納方法を活用して、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。

- 委任ディレクトリの管理
- アプリケーション固有のアクセス制御
- ディレクトリのドメインとロール

委任ディレクトリの管理

Oracle Internet Directory では、ディレクトリのアクセス制御ポリシー・ポイントは LDAP 属性として格納されているため、それを変更できる管理者を制御するメタポリシーを設定できます。これにより、グローバル管理者は、特定のサブツリーの管理者に権限を割り当てることができます。たとえば、ホスティングされた環境にあるアプリケーションの管理者に、権限を付与できます。同様に、グローバル管理者は、部門の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。

したがって、次のように 2 段階のアクセス制御を実装できます。

- ユーザーの認可

  この場合、ディレクトリには、外部アプリケーションが読み取って、適用するアクセス制御ポリシー・ポイントが格納されます。ユーザーがアプリケーションを使用した操作を実行しようとすると、そのアプリケーションによって、そのユーザーがその操作を実行する正式な認可を持っているかどうかが検証されます。

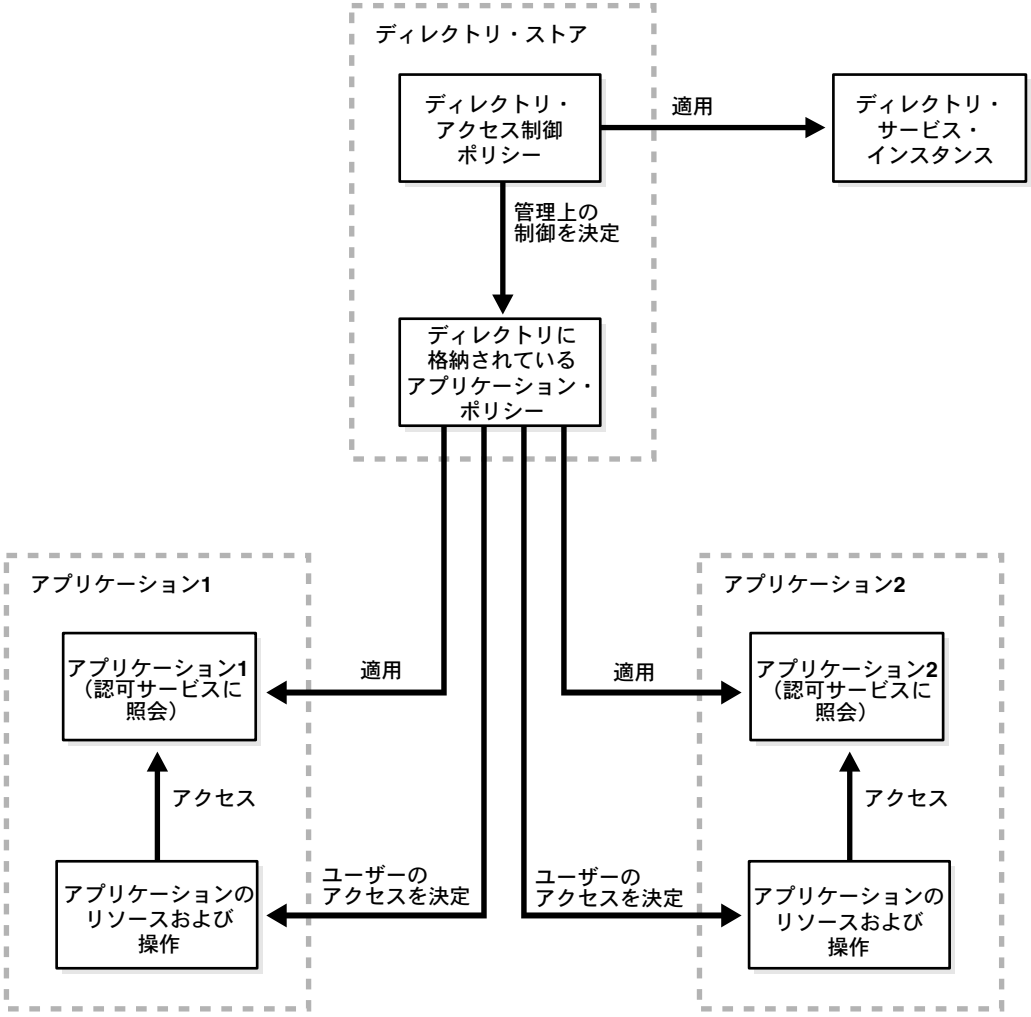
- 管理者の認可

  この場合、ディレクトリは、アプリケーション固有のすべてのアクセス制御ポリシー・ポイントに対する管理のトラスト・ポイントとして機能します。特定のアプリケーションのアクセス制御ポリシー・ポイントの管理者を決めるには、これらのアプリケーションに対するアクセス制御ポリシー・ポイントを、ディレクトリ・レベルで設定します。ユーザーがアプリケーション固有のアクセス制御ポリシー・ポイントを変更しようとすると、ディレクトリによって、そのユーザーがその変更を行う正式の認可を持っているかどうかが検証されます。

アプリケーション固有のアクセス制御

図 15-1 に、ホスティングされた環境におけるディレクトリのアクセス制御とアプリケーション固有のアクセス制御の仕組みとの関係を示します。

図 15-1 ディレクトリのアクセス制御とアプリケーション固有のアクセス制御



ディレクトリのドメインとロール

図 15-2 にディレクトリの様々なドメインと、それらのドメインに関連付けられているロールを示します。

図 15-2 ホスティングされた環境におけるディレクトリのドメインとロール

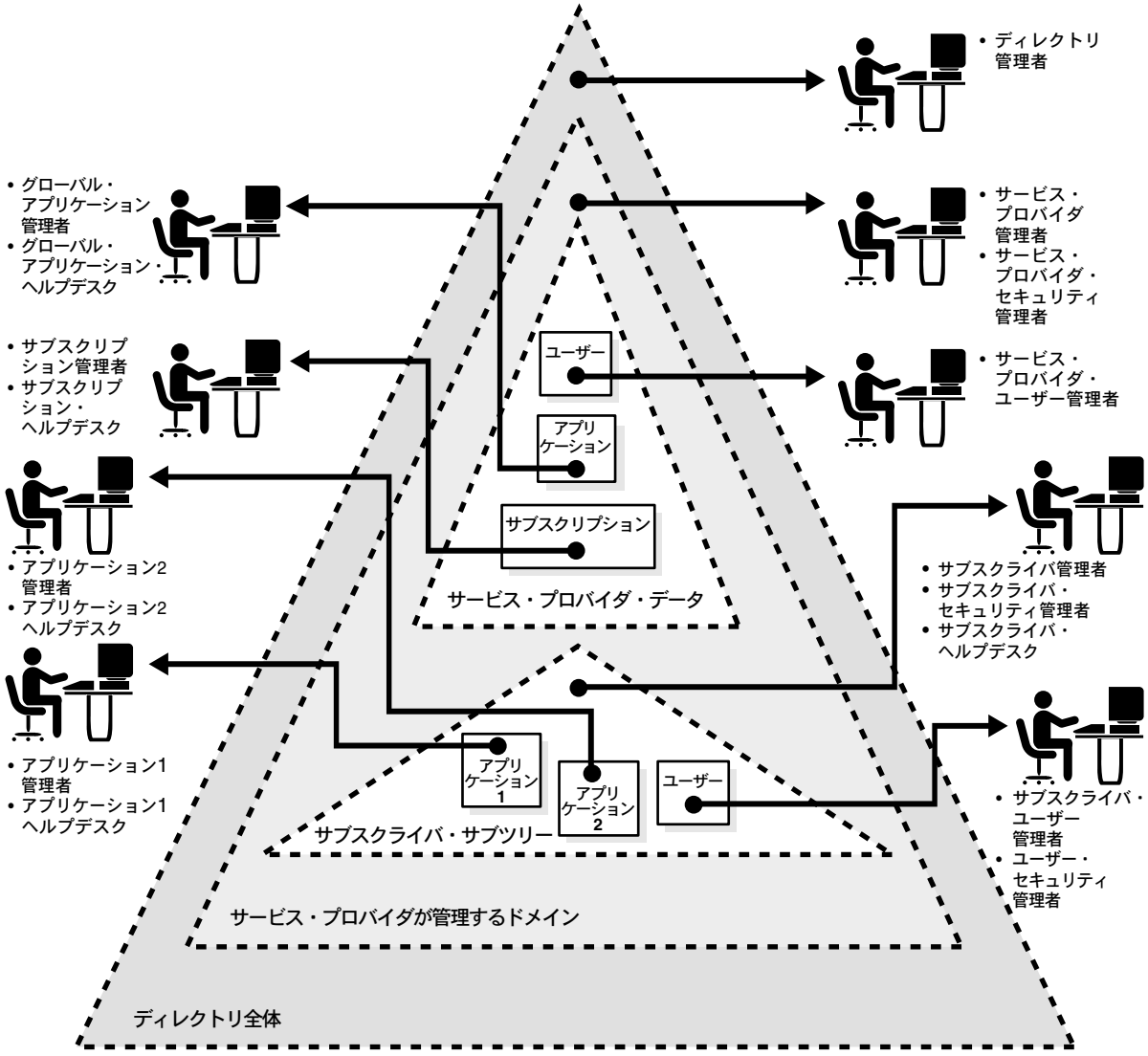


図 15-2 で、各三角形はディレクトリ情報ツリーの一部を表します。

- 最も外側の三角形がディレクトリ全体を表しています。ディレクトリの管理者は、ディレクトリ全体にわたる権限を持っています。
- 最も外側の三角形のすぐ内側にあるもう 1 つの三角形は、サービス・プロバイダが管理するドメインを表します。このドメインでは、エントリを新規に追加する権限が、サービス・プロバイダの管理者に委任されています。
- サービス・プロバイダが管理するドメイン内部では、ディレクトリ情報の所有権に基づいて権限がさらに他へ委任されます。たとえば、この委任は、ディレクトリの情報が特定のサブスクライバのみのものか、サービス・プロバイダにとってグローバルなものであるかによって変わります。

図 15-2 では、ディレクトリにサブスクライバが 1 人のみの場合を表しています。実際の状況ではサブスクライバは複数存在し、それぞれが他からの保護を必要とするドメインに属しています。

このモデルでの保護ドメインには、次のようなものがあります。

- ディレクトリ全体
- サービス・プロバイダが管理するドメイン
- サービス・プロバイダ固有のディレクトリ情報ツリー
- サブスクライバ固有のサブツリー
- ディレクトリにおけるアプリケーション固有の占有域
- ユーザー固有の情報

これらの保護ドメインは次のロールでサポートされています。これらのロールによって、サービス・プロバイダまたはサブスクライバはアクセス制御をカスタマイズできます。

- グローバル管理ロール

  このロールは、ディレクトリ全体に及ぶアクティビティを実行する権利を持ちます。

- サブスクライバ固有のロール

  これらのロールは、サブスクライバに固有のディレクトリ・ツリーのみに制限されます。

- アプリケーション固有のロール

  ディレクトリ対応アプリケーションをホスティングする場合、ディレクトリにおけるアプリケーション固有のロールがすべて必要になるわけではありません。しかし、そのアプリケーションが、ディレクトリにおけるその占有域に直接影響するようなロールで実行される場合、前述の推奨委任モデルに従うことが望ましいといえます。これによって、ディレクトリ固有の権限をユーザーに付与するとき、ディレクトリ・ベースの委任モデルを最大限に活用できます。

16

ユーザー認証資格証明のディレクトリ格納

この章では、エンド・ユーザーおよび管理者が簡単に管理できるように、セキュリティ資格証明を 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
- Oracle Internet Directory への認証用パスワード・ベリファイアの格納
- Oracle のコンポーネントに対する認証用パスワードの格納

ユーザー認証資格証明の集中格納の概要

Oracle Internet Directory では、セキュリティ資格証明をディレクトリ・データとして集中的に格納して、エンド・ユーザーと管理者が容易に管理できるようにします。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。大企業では、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化された状態にあります。パスワードが集中管理されていないと、管理者は、セキュリティを万全にできるほど速やかにすべての変更を実行できない可能性があります。

Oracle Internet Directory では、次の情報を格納します。

- 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 への認証用パスワード・ベリファイアの格納

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。

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、ルート・**ディレクトリ固有のエントリ（DSE）**の `orclCryptoScheme` 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み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。

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 よりも若干遅くなりますが、メッセージ・ダイジェスト値が大きくなることで、総当たり攻撃や反転攻撃に対してより強力に保護できます。
- **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

スーパー・ユーザーである場合は、次の操作を実行する必要があります。

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「Password Encryption」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
   - SHA
   - UNIX Crypt
   - なし（このオプションを選択すると、ユーザー・パスワードはクリア・テキストで保存されます）
3. 「適用」をクリックします。

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： 10-7 ページ「ディレクトリ認証用ユーザー・パスワードの保護」

Oracle のコンポーネントに対する認証用パスワードの格納

Oracle のコンポーネントは、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。

- パスワード・ベリファイアの概要
- パスワード・ベリファイアを格納するための属性
- 例 : パスワード検証の動作
- Oracle Directory Manager を使用したパスワード検証プロファイルの管理
- コマンドライン・ツールを使用したパスワード検証プロファイルの管理

パスワード・ベリファイアの概要

Oracle のコンポーネントは、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す。ハッシュ・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。

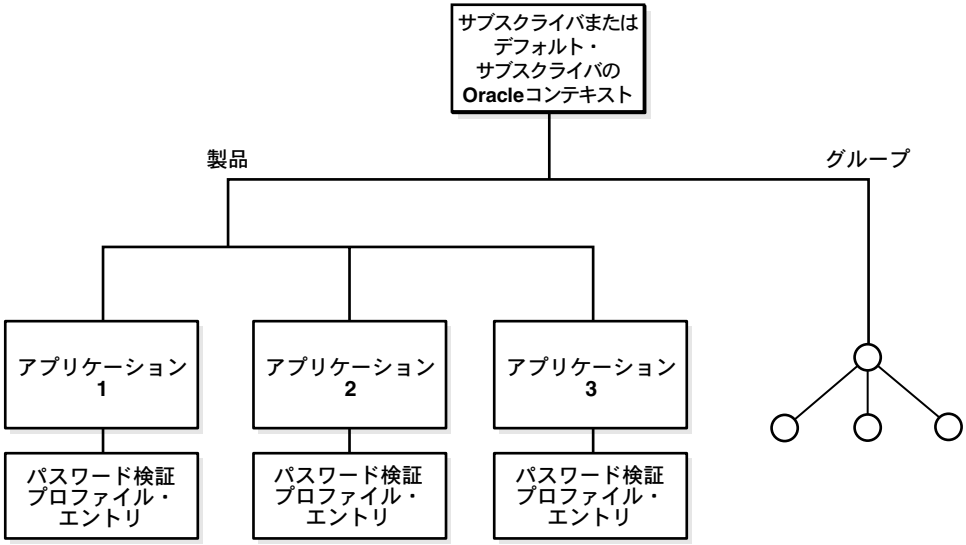
- **MD5**: MD4 が改善された、より複合的なバージョンです。
- **SHA**: Secure Hash Algorithm。**MD5** よりも長い 160 ビットのハッシュを生成します。このアルゴリズムは MD5 よりも若干遅くなりますが、メッセージ・ダイジェスト値が大きくなることで、総当たり攻撃や反転攻撃に対してより強力に保護できます。
- **UNIX Crypt**: UNIX ハッシング・アルゴリズムです。

- 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@subscriber のフォーマット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。図 16-1 に示すように、このエントリは、サブスクライバ固有またはデフォルトの Oracle コンテキストの下にある製品エントリの下のアプリケーション・エントリ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、指定されたサブスクライバの下のユーザーにのみ適用されます。異なるサブスクライバの下のユーザーには適用されません。サブスクライバの Oracle コンテキストの共通エントリにある `orclcommonusersearchbase` 属性に適切な値を設定して、ベリファイアが正しく生成されるようにします。この属性は、ベリファイアの生成が行われる前に設定しておく必要があります。

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

userPassword 属性にユーザー・パスワードを格納するディレクトリとは異なり、Oracle のコンポーネントは、ユーザー・エントリ内の 2 つの型のパスワード属性（authPassword と orclPasswordVerifier）のいずれか 1 つに、ユーザー・パスワード・ベリファイアを格納します。この 2 つの属性の型には、属性サブタイプとして appID があります。appID 属性は、Oracle アプリケーション・サーバーまたは認証識別情報を表現する一意の識別子です。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。たとえば、appID をアプリケーション・エントリの ORCLGUID にできます。この ID で特定のアプリケーションを一意に識別します。

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

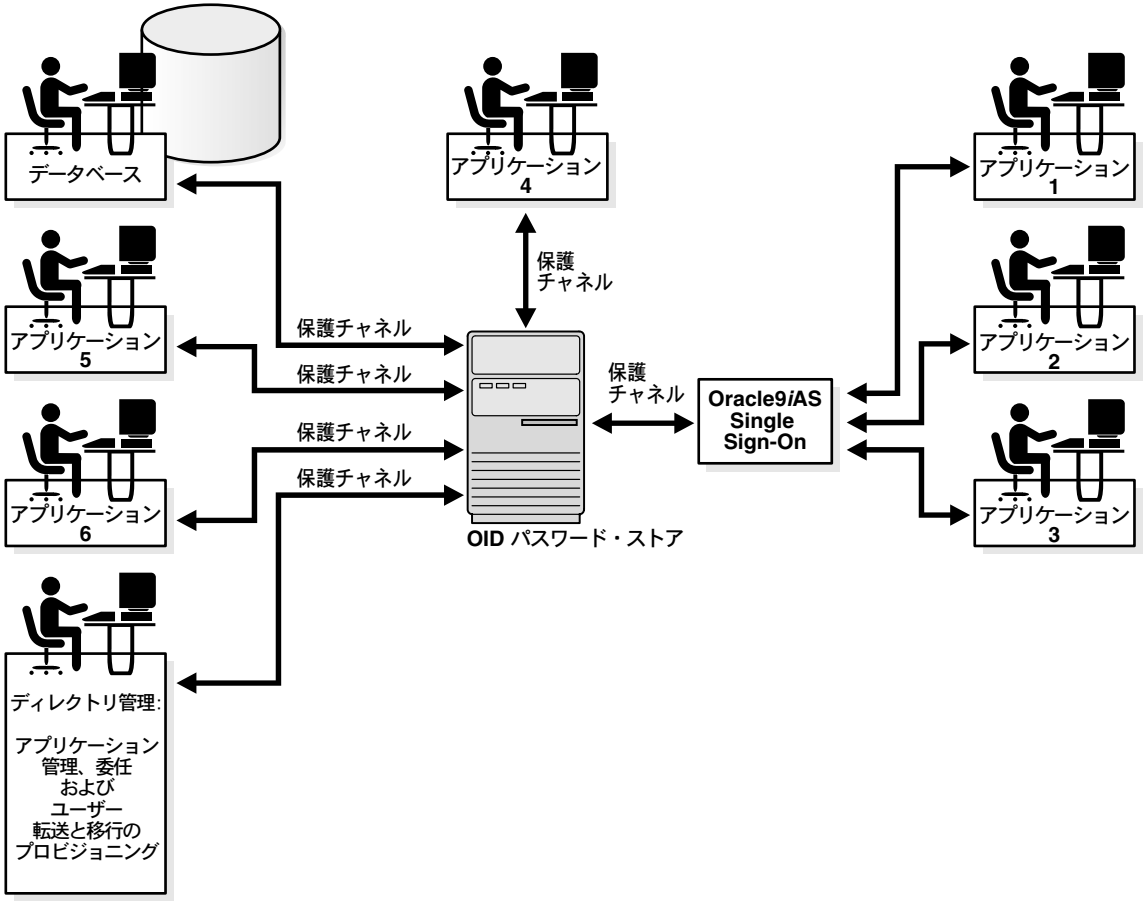
属性	説明
authPassword、appID	アプリケーションに対してユーザーを認証するパスワード。パスワードの値は、ディレクトリに対するユーザー認証に使用したパスワード（たとえば、userpassword など）と同じで、同期化されます。 複数の異なるアプリケーションで、ディレクトリに使用したクリア・テキスト・パスワードと同じパスワードの入力をユーザーに要求できます。ただし、各アプリケーションでは、異なるアルゴリズムを使用してそのパスワードがハッシュされる場合があります。この場合は、同じクリア・テキスト・パスワードが、複数の異なるパスワード・ベリファイアのソースとなります。 この属性は複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 が変更された場合は、すべてのアプリケーションの authpasswords が再生成されます。
orclPasswordVerifier、appID	アプリケーションに対してユーザーを認証するパスワード。ただし、authPassword 属性に格納されるパスワードとは異なり、ディレクトリに対して認証を行うパスワードとは別のものであるため、同期化されません。 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。

図 16-2 では、様々な Oracle の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。Oracle9*i*AS 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 userPassword 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
```

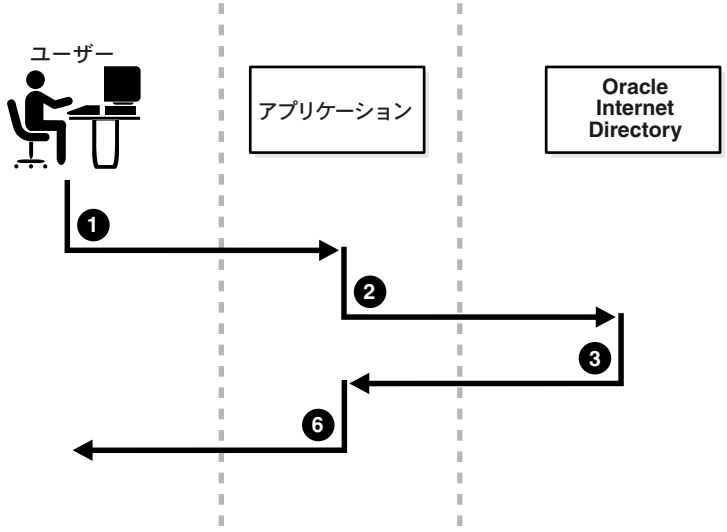
図 16-2 認証モデル



例 : パスワード検証の動作

図 16-3 は、パスワード検証の例を示しています。この例の Oracle のコンポーネントは、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、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。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。その後、ディレクトリ・サーバーは比較操作の結果をアプリケーションに通知します。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 app entity>" -w "<password>" -b "<dn of the
   user>" -a orclpasswordverifier; <appID> -v <password of the user>
   ```

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。

ディレクトリ・サーバーの比較操作を使用しない場合、アプリケーションは、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単純に取得します。次に、その値と計算したハッシュ値を比較します。2 つの値が一致した場合、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」>「*directory server instance*」の順に展開し、「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。
2. 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。表 16-2 は、このダイアログ・ボックスのフィールドとその説明です。
3. パスワード・ベリファイアの生成に使用するハッシング・アルゴリズムを変更するには、表 16-2 の説明に従って OrclPwdVerifierParams フィールドに新しい値を入力します。

表 16-2「パスワード検証プロファイル」ダイアログ・ボックス

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。
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。

表 16-2「パスワード検証プロファイル」ダイアログ・ボックス（続き）

フィールド	説明

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`

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管理

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。

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

次の例は、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

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
- 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
- エラー・メッセージ

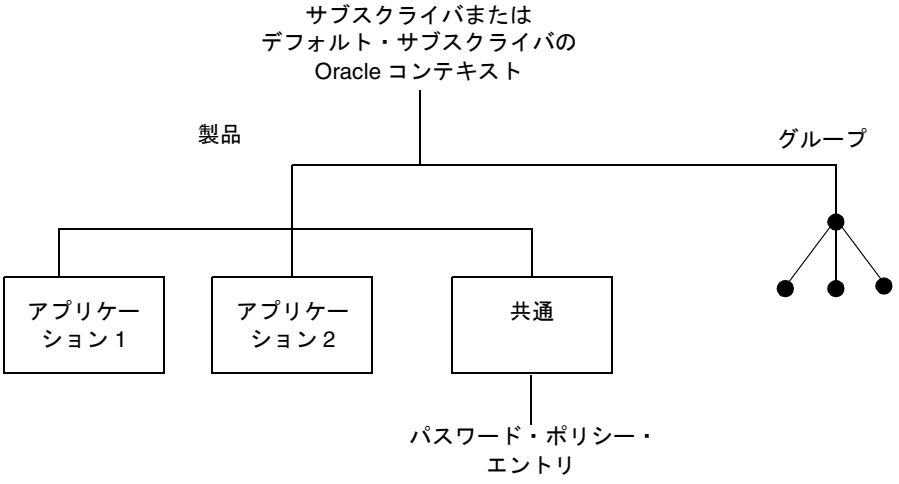
パスワード・ポリシーの概要

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。ディレクトリ・サーバーは、`ldapadd` および `ldapmodify` 操作時にパスワード・ポリシーの構文チェックを実行して、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しているかどうかを確認します。また、ディレクトリ・サーバーは、`ldapbind` および `ldapcompare` 操作時には、パスワード・ポリシーの状態チェックを実行します。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。

- 指定し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

Oracle Internet Directory のインストール時に、Oracle Universal Installer は、各サブスクライバに対して、必要なパスワード・ポリシー情報のすべてを含むパスワード・ポリシー・エントリを作成します。図 17-1 に示すように、このエントリは、サブスクライバまたはデフォルト・サブスクライバの Oracle コンテキストの下にある製品エントリの下の共通エントリ直下に配置されます。このパスワード・ポリシーは、指定されたサブスクライバの下の全ユーザーに適用されます。Oracle Internet Directory のパスワード・ポリシーは、`userpassword` 属性にのみ適用されます。サブスクライバの Oracle コンテキストの共通エントリにある orclcommonusersearchbase 属性に適切な値を設定して、パスワード・ポリシーが正しく施行されるようにします。この属性は、パスワード・ポリシーの変更が行われる前に設定しておく必要があります。

図 17-1 パスワード・ポリシー・エントリの位置



パスワード・ポリシーを確立するには、次の属性に値を割り当てます。

ポリシー	属性	説明
パスワード有効期限	pwdMaxAge	秒数で表した、指定したパスワードの有効期限。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。
パスワードの期限切れ警告	pwdExpireWarning	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。
パスワード有効期限	pwdGraceLoginLimit	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 0（ゼロ）です。
パスワード失敗の最大数	pwdLockout	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。
パスワード失敗の最大数	pwdMaxFailure	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。
パスワード失敗のカウント間隔	pwdFailureCountInterval	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。

ポリシー	属性	説明
アカウント・ロックアウト継続時間	pwdLockoutDuration	次の両方に該当する場合、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。
パスワード構文のチェック	pwdCheckSyntax	構文チェックを実行するかどうかを指定します。1 の場合、構文チェックが実行されます。デフォルトは使用可能です。
パスワードの最小文字数	pwdMinLength	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。
パスワード内の数字の数	orclpwdAlphaNumeric	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。
旧パスワードを新規パスワードに変更	orclpwdToggle	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。
パスワード無効値	orclpwdIllegalValues	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。

注意： 次の URL にある IETF Draft の 2001 年 7 月バージョンに示されるように、ユーザー・パスワードの値はすべて単一であるとされます。
http://ietf.org/internet-drafts/draft-behera-ldap-password-policy-05.txt

パスワード・ポリシーを作成するには、pwdPolicy 補助型オブジェクト・クラスを使用し、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。これらの値は、インストール時に設定します。このオブジェクト・クラスのエントリは、インストール時に作成されます。このエントリの識別名は、cn=pwdpolicyentry、cn=my_application、cn=products、cn=Oracle Context、o=*my_company*、dc=com です。リリース 9.2 では、指定したパスワード・ポリシーが指定したサブスクライバのディレクトリ情報ツリーに適用されます。各サブスクライバは、サブスクライバ独自のパスワード・ポリシーを保持できます。

このオブジェクト・クラスの属性は、次のとおりです。

- pwdMaxAge
- pwdGraceLoginLimit
- orclpwdAlphaNumeric
- pwdLockout
- pwdMinLength
- orclpwdToggle
- pwdLockoutDuration
- pwdCheckSyntax
- orclpwdIllegalValues
- pwdMaxFailure
- pwdFailureCountInterval
- pwdExpireWarning

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。

また、オブジェクト・クラスの最上位には、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維持するために、次の操作属性が含まれています。

- 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。
- pwdAccountLockedTime: ユーザーのアカウントがロックされた日時。
- pwdReset: この属性が使用可能な場合は、ユーザーに対してパスワードの変更を要求します。
- 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。

関連項目： 次の URL にある IETF Draft の 2001 年 7 月バージョン。
http://ietf.org/internet-drafts/draft-behera-ldap-password-policy-05.txt

Oracle Directory Manager を使用したパスワード・ポリシーの管理

Oracle Internet Directory のインストール時に、各サブスクライバに対してパスワード・ポリシー・エントリが作成されます。表 17-1 は、Oracle Directory Manager のパスワード・ポリシーに関するフィールドのリストとその説明です。

表 17-1 Oracle Directory Manager のパスワード・ポリシーに関するフィールド

フィールド	説明
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。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。デフォルトでは、ユーザーのパスワードは期限切れになりません。
アカウント・ロックアウト	リストから「使用可能」または「使用禁止」を選択します。
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を入力します。 ■ 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。
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。
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を入力します。デフォルトでは、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。パスワードが期限切れになる前にユーザーがパスワードを変更しない場合、ディレクトリ・サーバーはパスワードの変更を要求します。これは、管理者がパスワードを変更するまで、そのユーザーはロックアウトされることを意味します。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。
パスワード構文のチェック	構文チェックを適用するかどうかを指定します。1 の場合、構文チェックが実行されます。
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。

表 17-1 Oracle Directory Manager のパスワード・ポリシーに関するフィールド（続き）

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。
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。リストから「使用可能」を選択すると、旧パスワードを新規パスワードとして使用できます。

サブスクライバを作成する場合は、そのサブスクライバのパスワード・ポリシーも構成します。Oracle Directory Manager を使用して、後でパスワード・ポリシーを表示、リフレッシュおよび変更できます。ただし、パスワード・ポリシーの追加または削除はできません。

Oracle Directory Manager を使用したサブスクライバのパスワード・ポリシーの表示

サブスクライバのパスワード・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」>「*directory server instance*」>「パスワード・ポリシー管理」の順に展開します。ナビゲータ・ペインにサブスクライバのパスワード・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。

サブスクライバのパスワード・ポリシーを最新の内容に更新する場合は、「リフレッシュ」を選択します。

特定のサブスクライバのパスワード・ポリシーを表示するには、ナビゲータ・ペインで、表示するサブスクライバのパスワード・ポリシーを選択します。

Oracle Directory Manager を使用したサブスクライバのパスワード・ポリシーの変更

サブスクライバのパスワード・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」>「*directory server instance*」>「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、変更するサブスクライバのパスワード・ポリシーを選択します。
3. 右側のペインで、パスワード・ポリシーの各属性フィールドを変更します。
4. 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。

- 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
- コマンドライン・ツールを使用したサブスクライバのパスワード・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・ポリシーの設定

次の例は、pwdLockout 属性を有効にして、その値をデフォルト設定から 0（ゼロ）に変更します。

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: 1
```

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
```

コマンドライン・ツールを使用したサブスクライバのパスワード・ポリシーの管理

次の例を検証し、コマンドライン・ツールを使用してサブスクライバのパスワード・ポリシーを表示および変更する方法を習得します。

例 : コマンドライン・ツールを使用したサブスクライバのパスワード・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・ツールを使用したサブスクライバのパスワード・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
```

エラー・メッセージ

関連項目： G-9 ページ「パスワード・ポリシー違反のエラー・メッセージ」

18

容量計画に関する考慮事項

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
- ディレクトリの使用パターンの理解 : 事例
- I/O サブシステムの要件
- メモリー要件
- ネットワーク要件
- CPU 要件
- Acme Corporation の容量計画のまとめ

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。

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。

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。

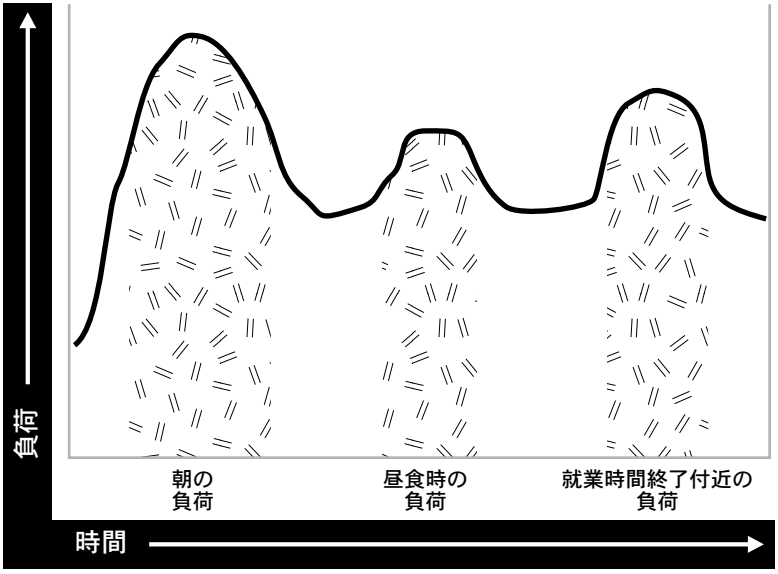
次の表は、1 日に発生する可能性があるすべてのディレクトリ参照回数を要約したものです。

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 18-1 のようになります。

図 18-1 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、勤務時間内の負荷を次のカテゴリに分割します（勤務時間は 1 日 8 時間と仮定します）。

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、インストレーション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
- ディスク領域要件の概算
- ディスク領域要件の詳細な計算

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・ファイルを組織化する方法のガイドラインは、第 19 章「チューニングに関する考慮事項」に記載されています。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ることができます。

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_IND_ATTRSTORE	ディレクトリ内の属性に関連する索引を格納。
OLTS_CT_DN	識別名カタログを格納。
OLTS_IND_CT_DN	識別名カタログに関連する索引を格納。
OLTS_CT_CN	一般名カタログを格納。
OLTS_CT_OBJCL	オブジェクト・クラス・カタログを格納。
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）を格納。
OLTS_IND_CT_STORE	ユーザー定義カタログに関連する索引を格納。
P1TS_ATTRSTORE	サーバー管理機能のためのカタログと属性表を格納。
P1TS_IND_ATTRSTORE	OID サーバー管理機能が取得した表の索引を格納。
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_TEMP	表の各種索引の作成に使用。すべての索引作成が正常に行われるように、十分な大きさに設定してください。
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。

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）。

変数名	説明
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限らないため、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。
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。

この表の変数を使用すると、個々の表領域のサイズを次のように計算できます。

表領域名	サイズ
OLTS_ATTR_STORE	`num_entries × { ((attrs_per_entry) × (avg_attrnam_len + avg_attr_size + 22)) + 6 × 35 } × db_storage_ovhd`
OLTS_IND_ATTRSTORE	`num_entries × (attrs_per_entry + 6) × 20`
OLTS_CT_DN	`num_entries × 2 × (avg_dn_size + 4)`

表領域名	サイズ
OLTS_IND_CT_DN	num_entries × 2 × (avg_dn_size × 3)
OLTS_CT_CN	num_entries × avg_dn_size × db_storage_ovhd
OLTS_CT_OBJCL	(num_entries × objectclass_per_entry × objectclass_size × db_storage_ovhd) + (num_auditlog_entries × 2 × avg_dn_size × db_storage_ovhd)
OLTS_CT_STORE	(entries_per_catalog × num_cataloged_attrs × avg_attr_size × db_storage_ovhd) + (num_entries × objectclass_per_entry × objectclass_size × db_storage_ovhd)
OLTS_IND_CT_STORE	(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)
P1TS_ATTRSTORE	num_stats_entries × ((avg_attrnam_len + avg_attr_size + 20) × attrs_per_stats_entry) × db_storage_ovhd × (orclstatsperiodicity ÷ 60) × 12)
P1TS_IND_ATTRSTORE	(num_stats_entries × attrs_per_stats_entry × 20) × ((orclstatsperiodicity ÷ 60) × 12)
OLTS_DEFAULT	(change_log_capacity × 4 × avg_attr_size × db_storage_ovhd × db_index_ovhd) + initial_num_entries × 2 × (avg_dn_size + 4)
OLTS_TEMP	(OLTS_IND_ATTR_STORE のサイズ) + (OLTS_IND_CT_STORE のサイズ)
SYSTEM	300MB

この表の計算式を使用すると、Oracle Internet Directory の広範囲にわたる様々な配置例に対して、正確な領域要件を計算できます。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。

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）
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。

表領域名	サイズ（バイト）	サイズ（MB）
OLTS_ATTRSTORE	2076180480	1980
OLTS_IND_ATTRSTORE	545259520	520
OLTS_CT_DN	92274688	88
OLTS_IND_CT_DN	251658240	240
OLTS_CT_CN	57671680	55
OLTS_CT_OBJCL	71303168	68
OLTS_CT_STORE	530579456	506
OLTS_IND_CT_STORE	1918894080	1830
P1TS_ATTRSTORE	104857600	100
P1TS_IND_ATTRSTORE	52428800	50
OLTS_DEFAULT	170917888	163
OLTS_TEMP	2533359616	2416
SYSTEM	314572800	300
合計サイズ	**8719958016**	**8316**

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、ボトルネックによって 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。

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' ×（attrs_per_entry + 6）×（avg_attrname_len + avg_attr_size + 72）

関連項目： SGA のチューニングの詳細は、第 19 章「チューニングに関する考慮事項」を参照してください。

次の表は、異なるディレクトリ構成別に最低メモリー要件を示したものです。

ディレクトリのタイプ	エントリ件数	最低メモリー
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）。次の表は、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）を示したものです。

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拡張性がもたらされることはほとんどありません。これは、多くの操作が純粋に CPU の限界ではないためです。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ることができます。

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・ポイントの数。

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 リリース 9.2 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 リリース 9.2 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。

- 指定した操作並行性については、別途の CPU リソースを追加することによって、より高いスループット（したがって、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（および待機時間）については、別途の CPU リソースを追加することによって、より高い操作並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 クライアントの並行性で 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 : 7GB ～ 11GB
- 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。

19

チューニングに関する考慮事項

第 18 章「容量計画に関する考慮事項」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
- 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、『Oracle9*i* データベース・リファレンス』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、『Oracle9*i* データベース概要』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 1.0。サイト：`http://sources.redhat.com/cygwin/`
- MKS Toolkit 5.1 または 6.0。
  サイト：`http://www.datafocus.com/products/`

関連項目： A-56 ページ「OID データベース統計収集ツール」

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 18 章「容量計画に関する考慮事項」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。

- 11（10+1）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並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' 台の並行性に対して、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' 台の同じ並行性に対して、'p' 件を超える高いスループットを達成できます。
- 'n' 台を超える高い並行性に対して、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 1.0。サイト：`http://sources.redhat.com/cygwin/`
- MKS Toolkit 5.1 または 6.0。
  サイト：`http://www.datafocus.com/products/`

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 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* 用の SGA のチューニング

SGA は、Oracle9*i* 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、『Oracle9*i* データベース・パフォーマンス・チューニング・ガイドおよびリファレンス』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、『Oracle9*i* データベース・パフォーマンス・チューニング・ガイドおよびリファレンス』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。

- 表領域の均衡化
- RAID

表領域の均衡化

Oracle Internet Directory のスキーマは、メンテナンスの容易性とパフォーマンスのために、インストール時にいくつかの表領域に分散されます。各表領域には、ディスク記憶域での共存に適し、グループ化された Oracle Internet Directory のスキーマ・オブジェクトが含まれています。可能な場合は、別々の論理ディスクに次のオブジェクトを分散するとさらに有効です。

> **関連項目：** 論理ディスクの詳細は、19-9 ページの「RAID」を参照してください。

次の表領域を分離してください。

- OLTS_ATTRSTORE と OLTS_IND_ATTRSTORE

  属性記憶域表とその索引を分離します。

- OLTS_CT_DN と OLTS_IND_CT_DN

  識別名カタログとその索引を分離します。

- OLTS_xxxx と OLTS_IND_xxxx

  （経験に基づいて、格納表領域と関連する索引を分離します。）

- OLTS_IND_ATTRSTORE と OLTS_IND_CT_DN

  属性格納表と識別名カタログ索引を交換します。交換すると、使用可能な論理ディスクが 2 つのみの場合にも有効です（一方の論理ディスクに OLTS_CT_DN と OLTS_IND_ATTRSTORE、他方の論理ディスクに OLTS_IND_CT_DN と OLTS_ATTRSTORE が格納されます）。

RAID

表領域の均衡化に関する情報は、Oracle Internet Directory の表領域を異なる論理ドライブに分散する方法として提供されています。表領域を分散すると、論理ドライブが他の論理ドライブとは異なるディスク上にあるとみなされるため、I/O がディスク間に分配されることを意味します。（同じ物理ディスク・メディア上の 2 つの論理ドライブは、異なる物理メディア上に配置されている 2 つの論理ドライブと同等の結合 I/O スループットを実際には提供しません。）論理ドライブを、ストライプ化されたディスク・サブシステムまたは RAID ディスク・サブシステム上に設定できる場合は、その論理ドライブの I/O 容量が増加します。しかし、前述の表領域の配置は、たとえば、ボリューム・マネージャの異なる論理ドライブを考慮する場合には依然として適切な方法です。

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。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、19-7 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 リリース 9.2 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
- クライアントの並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・セットと高いクライアントの並行性を必要とする大規模な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・インスタンスと Oracle のバッファ・キャッシュが、パフォーマンス面で優れたスケーラブル・アーキテクチャであることがわかります。

> **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、5-14 ページの「システム操作属性の設定」を参照してください。

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-56 ページの「OID データベース統計収集ツール」を参照してください。

20

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 の高可用性とフェイルオーバー機能、および配置のガイドラインを示します。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 Oracle9i 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、第 VI 部の「ディレクトリとクラスタ」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

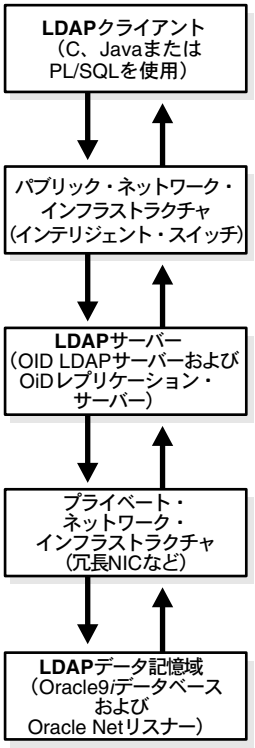
Oracle Internet Directory は、高度なシステム可用性を必要とするミッション・クリティカルなアプリケーションの配置ニーズに対処できるように設計されています。高度な可用性の実現には、システムのすべてのコンポーネントにおける冗長性の促進とすべてのインタフェースにおける障害検出とリカバリ（**フェイルオーバー**と呼ばれます）の促進が必要です。さらに、システム全体の可用性目標を達成するには、配置システム全体におけるアプリケーションに依存しない、ネットワーク・フェイルオーバー機能の統合が重要です。

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（20-2 ページを参照）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。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。

Oracle Internet Directory および Oracle9*i* のテクノロジ・スタック

図 20-1 は、Oracle Internet Directory スタックの様々なコンポーネントの概要を示したものです。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 20-1 Oracle Internet Directory および Oracle9*i* 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・トレラント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
- Oracle Internet Directory サーバーからの代替サーバー・リスト

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・サーバーに対する参照を所有することを想定しています。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。

注意： `AltServer` 属性の設定には ldapmodify を使用します。Oracle Directory Manager では設定できません。

関連項目： `AltServer` 属性の設定手順は、6-29 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 20-2 は、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たものです。

図 20-2 ネットワーク・レベルのフェイルオーバー

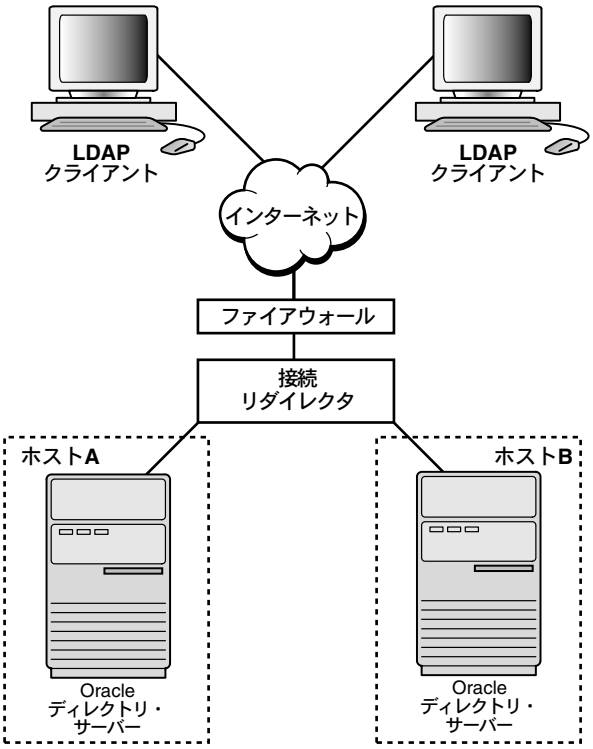


図 20-2 では、Oracle ディレクトリ・サーバー（OID LDAP サーバー）は、同じバックエンドのデータベースまたは異なるバックエンドのデータベースのいずれにも接続できます。この配置システムの場合、ネットワーク・レベルの接続リダイレクションは、ハードウェアとソフトウェア両方のソリューションによって実施できます。

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。コンピュータが回復すると、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 20-3 では、データベースと Oracle ディレクトリ・サーバー（OID 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 20-3 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）

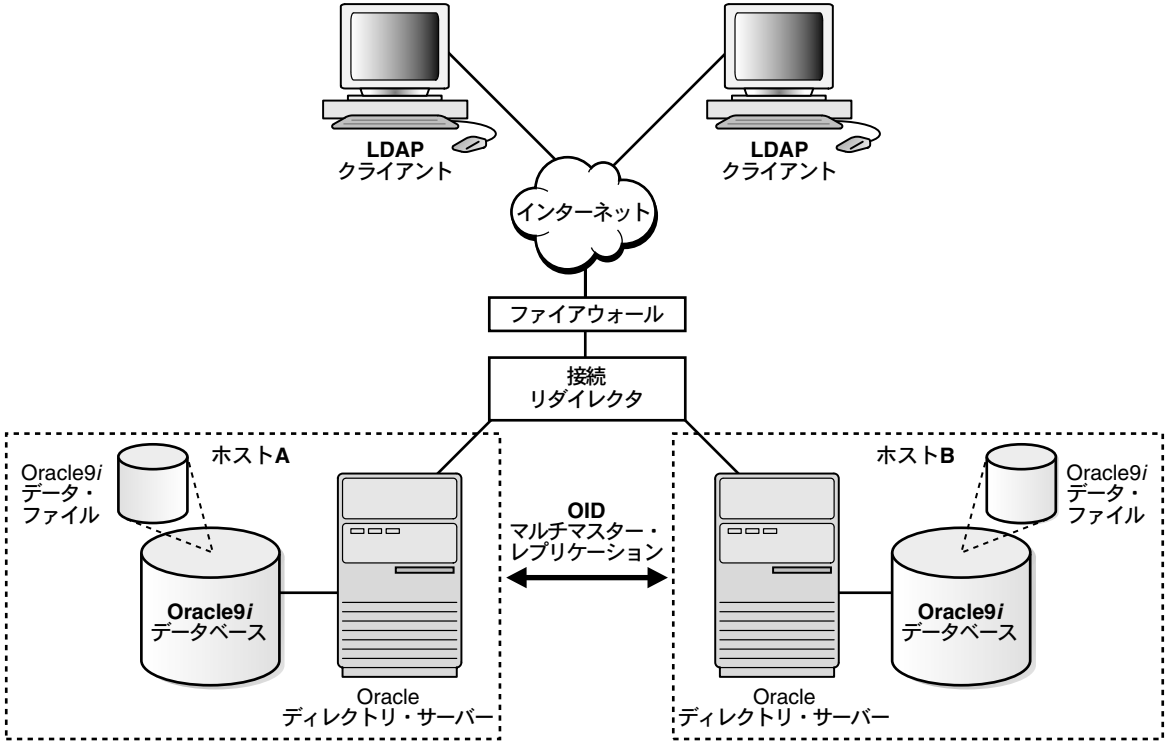
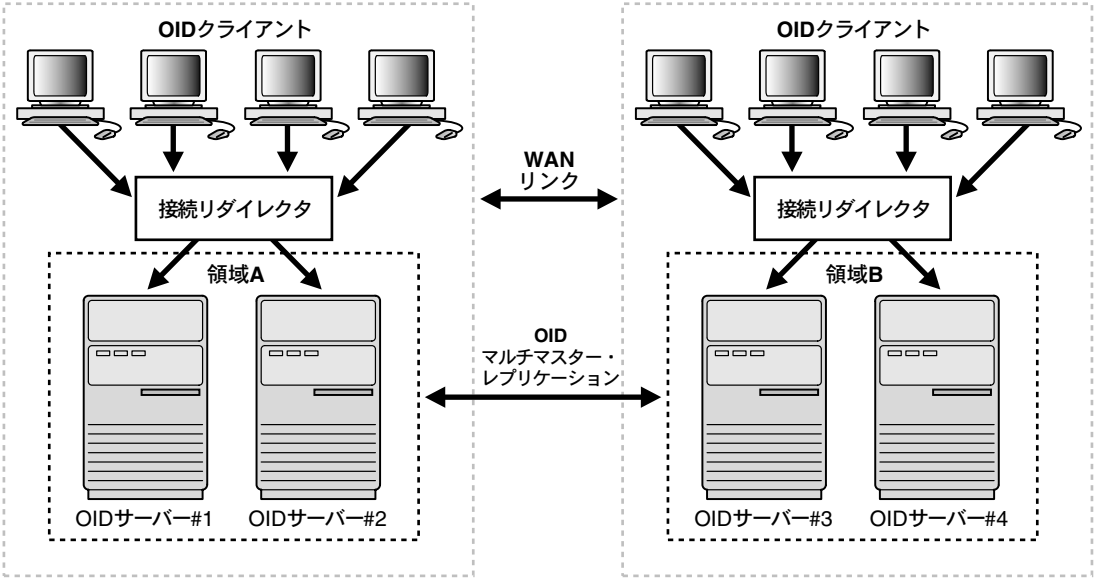


図 20-4 が示すように、相互にレプリケートする 2 つの Oracle Internet Directory ノードを各領域に設定できます。この構成は、大企業が配置しているグローバル・ディレクトリ・ネットワークの典型的な例で、前述の領域がそれぞれ、大陸または国に対応する場合などがあります。

図 20-4 配置例 2



第 V 部

ディレクトリ・レプリケーション

第 V 部では、レプリケーションの詳細および管理方法を説明します。第 V 部は、次の各章で構成されています。

21

ディレクトリ・レプリケーションの概要

2-21 ページの「分散ディレクトリ」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・グループとレプリケーション承諾
- Oracle9i レプリケーション
- レプリケーション・アーキテクチャ
- 変更ログの削除
- レプリケーションにおける競合の解消
- レプリケーション・プロセス

関連項目：

- レプリケーションの全般的かつ概念的な説明は、2-22 ページの「レプリケーション」を参照してください。
- レプリケーションの管理方法は、第 22 章「Oracle ディレクトリ・レプリケーション・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・グループとレプリケーション承諾

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・サーバーのセットを、ディレクトリ・レプリケーション・グループ（DRG）と呼びます。レプリケーション承諾と呼ばれる特別なディレクトリ・エントリには、DRG 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が記述されています。

ディレクトリ・サーバーは、変更ログ情報のサプライヤまたはコンシューマのどちらにもなります。Oracle Internet Directory は、この機能を使用してマルチマスター・レプリケーションをサポートしています。

図 21-1 に示されたディレクトリ・レプリケーション・グループでは、レプリケーション承諾内の 3 つのノードが、互に更新内容を共有しています。

図 21-1 ディレクトリ・レプリケーション・グループ

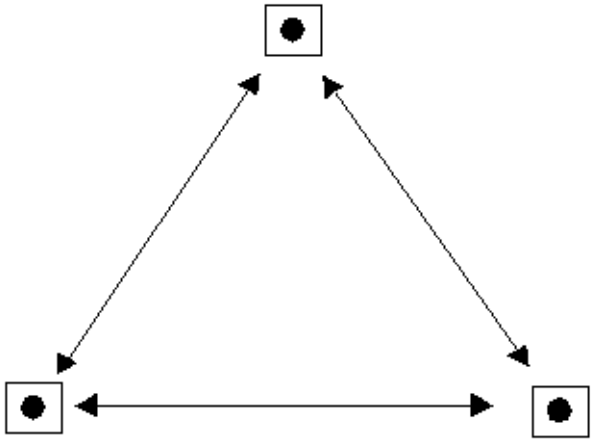


図 21-1 にある各黒丸は、Oracle Internet Directory のノードを表しています。承諾は各ノードで同一ですが、ローカル・ディレクトリ・サーバー上にパーティション化されたネーミング・コンテキストなどのローカル・オプションは異なります。各ノードのレプリケーション承諾には、変更内容を配布および受信する他のノードがすべてリストされています。

関連項目： レプリケーション承諾の構成方法は、22-12 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* レプリケーション

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トランスポートは、Oracle9*i* で使用可能な Oracle9*i* レプリケーションによって管理されます。この機能を使用すると、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ます。

Oracle9*i* レプリケーションは、ローカルの変更内容を蓄積し、コンシューマ・サーバー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・ストアから適用済みのリモートの変更内容を削除します。

Oracle9*i* レプリケーション環境では、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込みおよび更新アクセスが可能です。一般的な Oracle9*i* レプリケーション構成では、非同期データ伝播方式の行レベル・レプリケーションが使用されます。

Oracle9*i* レプリケーションは、実証済みのネットワーク・トレランスを提供し、そのデータ移送は、Oracle Enterprise Manager で制御およびモニターできます。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。

> **関連項目：** Oracle9*i* レプリケーションの詳細は、『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。

レプリケーション・アーキテクチャ

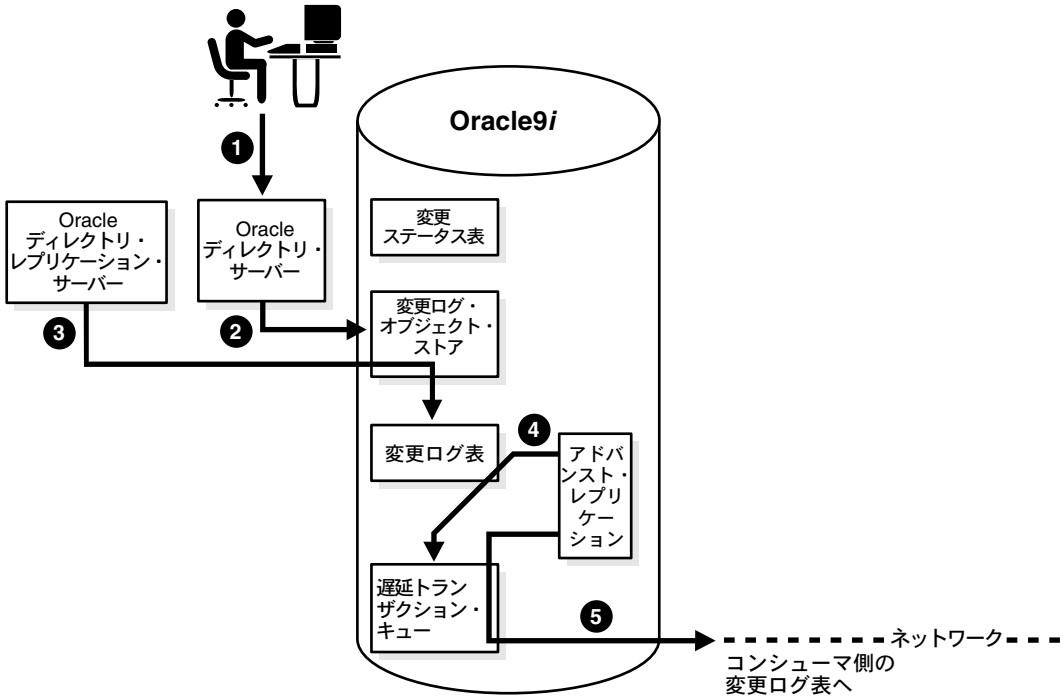
サプライヤ・サーバーは、変更内容を変更ログに書き込み、ディレクトリ変更を他のコンシューマ・サーバーに定期的にバッチで送信します。コンシューマ・サーバーは変更ログ・データを受信し、変更内容をローカルに適用します。

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。ローカルの変更内容はリモート・ノードに配布されてから、レプリケーション・サーバー処理によって適用されます。リモート・ノード上で変更を適用するために、クライアントとして機能するレプリケーション・サーバーは、ディレクトリ・サーバーにコマンドを送信し、ディレクトリ・サーバーがそのコマンドを実行します。

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。

サプライヤ側のレプリケーション・プロセス

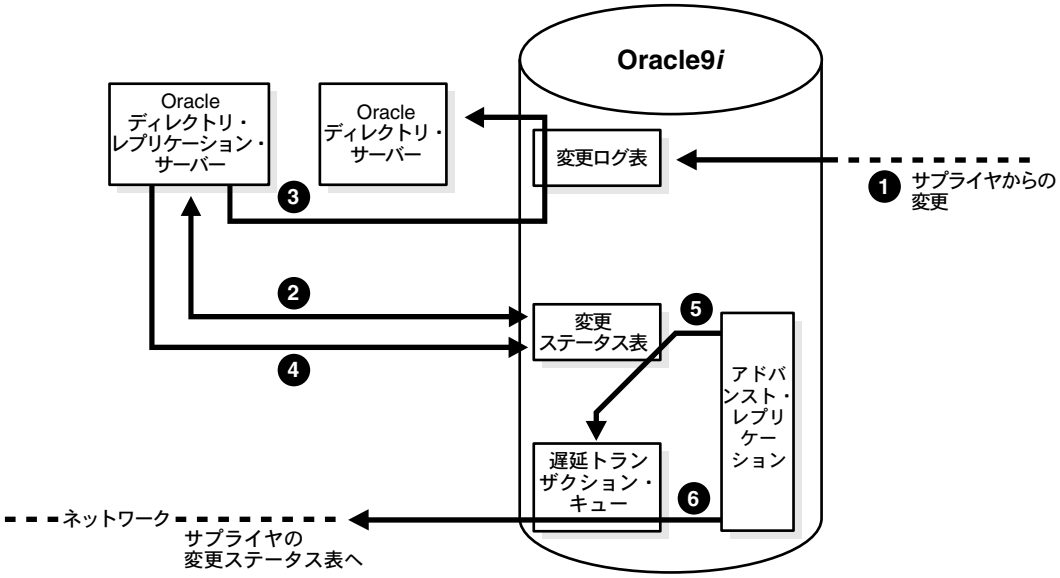
次の図および説明では、レプリケーション・プロセス中のサプライヤ側の動作を示します。



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* レプリケーションはその変更内容を遅延トランザクション・キューへ即座にコピーします。
5. スケジュールされた間隔が経過すると、Oracle9*i* レプリケーションは、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。

コンシューマ側のレプリケーション・プロセス

次の図および説明では、コンシューマ側のレプリケーション・プロセスを示します。



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* レプリケーションは、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* レプリケーションのレプリケーションの間隔が経過すると、Oracle9*i* レプリケーション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、適用済み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、22-12 ページの「レプリケーションの管理」を参照してください。

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。

  関連項目：

  - 22-13 ページ「Oracle Directory Manager を使用したレプリケーションの構成パラメータの表示と変更」
  - 22-14 ページ「コマンドライン・ツールを使用したレプリケーションの構成パラメータの変更」

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なんらかの理由で失敗すると、必ず発生します。

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

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が発生するレベル
- 競合の一般的な原因
- 競合の自動解消

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

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。そのような変更には、コンシューマに対する次のタイプの変更のいずれかが該当します。

- 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

- エントリが削除済み
- エントリがコンシューマに存在しない

存在する必要のないエントリが存在している場合は、以前に追加済みであるか、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

競合は通常、広域ネットワーク上で時折発生する通信速度の低下や送信エラーが原因で生ずる変更の時間的なずれが原因です。また、過去に生じた不整合が、タイムリに解消されていない場合に、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 C「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、付録 A「LDIF およびコマンドライン・ツールの構文」の「カタログ管理ツール」の項を参照してください。

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。次の項目について説明します。

- 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
- レプリケーション・プロセスがエントリを削除する動作
- レプリケーション・プロセスがエントリを変更する動作
- 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
- レプリケーション・プロセスが識別名を変更する動作

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 回目以降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。

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 回目以降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。

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、フィルタ処理済みの変更を適用し、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 回目以降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。

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 回目以降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。

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 回目以降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。

22

Oracle ディレクトリ・レプリケーション・サーバーの管理

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。

注意： リリース 9.2 では、Oracle Internet Directory のレプリケーションを使用できるのは、**Oracle9i レプリケーション（Oracle9i Replication）**をインストールしている場合のみです。これは、Oracle Internet Directory をスタンドアロンで購入した場合および Oracle9*i* Enterprise Edition に付属しています。Oracle9*i* レプリケーションは、Oracle9*i* Standard Edition には含まれません。

この章では、次の項目について説明します。

- 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
- レプリケーション・ノードの追加
- レプリケーション・ノードの削除
- 手動での競合の解消
- ホストから独立したものとしてのノードの識別
- レプリケーション設定のトラブルシューティング

関連項目： レプリケーションの概念の説明は、2-22 ページの「レプリケーション」を参照してください。

レプリケーションのインストールと構成

この項では、ノードでディレクトリ・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設定する方法を説明します。

ディレクトリ・サーバーのグループ内の各ノードには、同じ（1 つまたはセットの）**ネーミング・コンテキスト**の更新可能なコピー（更新可能レプリカとも呼ばれます）が保持されています。これらのネーミング・コンテキストは、レプリケーション処理によって相互に同期化されます。このノードのグループを、**ディレクトリ・レプリケーション・グループ（DRG）**と呼びます。

同じマシンに複数の Oracle Internet Directory インスタンスを配置する場合は、ホスト名では各ディレクトリ・サーバー・インスタンスを一意に識別できません。この場合は、レプリケーションをインストールおよび構成する前に 22-31 ページの「ホストから独立したものとしてのノードの識別」の指示に従ってください。

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には、次の一般的なタスクを実行します。

タスク 1: DRG の全ノードへの Oracle Internet Directory のインストール

タスク 2: Oracle9i レプリケーションのマスター定義サイト（MDS）として機能するノードの決定

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 レプリケーションの設定

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、22-21 ページの「レプリケーション・ノードの追加」を参照してください。
- Oracle Internet Directory リリース 9.2 には、複数の DRG で構成されている環境（ディレクトリ・ネットワーク）を作成するプロシージャとツールは用意されていません。
- 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。

タスク 1: DRG の全ノードへの Oracle Internet Directory のインストール

Oracle Internet Directory に必要な Oracle9*i* Enterprise Edition を通常の方法でインストールすると、**Oracle9i レプリケーション（Oracle9i Replication）** もインストールされます。これに対して、Oracle9*i* Standard Edition を通常の方法でインストールしても、Oracle9*i* レプリケーションはインストールされません。

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： Oracle Internet Directory のインストレーション・ドキュメントを参照してください。

タスク 2: Oracle9*i* レプリケーションのマスター定義サイト（MDS）として機能するノードの決定

マスター定義サイト（MDS） は任意の Oracle Internet Directory データベースで、管理者はそのデータベースで構成スクリプトを実行します。**リモート・マスター・サイト（RMS）** は、MDS 以外のサイトで、Oracle9*i* レプリケーションのメンバーであるサイトです。

管理者は **Oracle Net Services** を使用して、DRG を構成している MDS データベースとその他の全ノードに接続できることが必要です。

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* レプリケーションの設定

次の各項では、Oracle Internet Directory のインストレーション・スクリプトを使用して、Oracle9*i* レプリケーションをインストールおよび構成する方法を説明します。Oracle9*i* レプリケーションの上級ユーザーは、Oracle9*i* Replication Manager ツールを使用して Oracle9*i* レプリケーションを構成することもできます。

> **関連項目：** Oracle9*i* Replication Manager を使用した Oracle9*i* レプリケーションの構成方法は、『Oracle9*i* アドバンスト・レプリケーション』および Oracle9*i* 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* レプリケーション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 レプリケーションの構成

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。詳細は後述します。

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のみ必要です。
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のみ必要です。
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。

```
net_service_name =
    (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のみ必要です。

初期化パラメータ・ファイル `init.ora` 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から再起動します。

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。system@*net_service_name* と system@*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* レプリケーションの構成

レプリケーション・グループの Oracle9*i* レプリケーションを構成するには、MDS から次の手順を実行します。

1. UNIX プロンプトから、Oracle Internet Directory ソフトウェアの所有者アカウントとしてログオンします。
2. ディレクトリを次のディレクトリに変更します。
   - UNIX: `$ORACLE_HOME/ldap/bin`
   - Windows NT: `%ORACLE_HOME%¥ldap¥bin`

   注意 : 次の手順に進む前に、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。次のことを確認してください。

   - Oracle Internet Directory データベースが起動されていて、実行中であること
   - Oracle Internet Directory のリスナーが起動されていて、実行中であること
   - 接続記述子が正しいこと
   - システム・パスワードが正しいこと

3. MDS から、DRG の全ノードで Oracle Internet Directory データベースのインスタンスおよびリスナーのすべてが実行されていることを確認します。
4. MDS のコマンド・プロンプトで次のスクリプトを実行し、「注意」の前提条件を満たしていることを確認します。

   ```
   ldaprepl.sh -asrsetup
   ```

注意：

- UNIX の場合、コマンド・シェルでこのスクリプトを実行する前に、環境変数 *$ORACLE_HOME* を設定します。
- Windows NT の場合、MKS Toolkit または Cygwin UNIX エミュレーション・ツールがインストールされている場合のみ、このスクリプトを実行できます。

ldaprepl.sh は、次の複数の操作を実行します。

- MDS の構成
- リモート・マスター・サイトの構成
- すべてのサイトで、レプリケーションの送信ジョブを構成
- MDS でのレプリケーションの再開
- すべての手順が正常に完了したことを検証
- すべてのノードで、デフォルトのレプリケーション承諾を構成

このスクリプトを実行すると、次の表にある情報が、最初に MDS に対して要求されます。

要求される情報	定義
MDS グローバル名	`tnsnames.ora` ファイルにリストされている、MDS データベースのネット・サービス名
MDS のシステム・パスワード	マスター定義サイトのシステム・パスワード

MDS に関するこの情報を提供すると、次に、その他のマスター・サイトのグローバル名とシステム・パスワードが要求されます。

その他のマスター・サイトに関する必要な情報を提供すると、次に、レプリケーション管理パスワードが要求されます。これによって、全ノードでレプリケーション管理者用のデータベース・アカウントを作成できるようになります。レプリケーション管理者は、後でノードを追加または削除する場合に、このパスワードが必要です。

全サイトの指定が終了すると、指定した情報が一覧表示され、確認を要求されます。情報に誤りがある場合は、「`N`」をクリックします。スクリプトが最初から実行され、MDS の情報が再度要求されます。

すべての情報の指定が終了すると、情報の確認を要求されます。情報が正しい場合は「`Y`」をクリックします。スクリプトによって、サイトの構成が開始されます。

この処理は、システム・リソースと DRG 内のノード数によっては長時間にわたる場合があります。処理の経過は、継続的に通知されます。

注意： 完了前に処理を中断した場合は、最初から実行しなおす必要があります。処理を中断しても、再インストレーションに悪影響を及ぼすことはありません。

エラーが表示された場合は、22-32 ページの「レプリケーション設定のトラブルシューティング」を参照してください。

関連項目：

- 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。

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 net_service_name -check -generate file_with_absolute_path_name
   ```

2. 同じノードで、次のコマンドを入力します。

   ```
   bulkload.sh -connect net_service_name_1 -load
   ```

3. データがすべてのノードにロードされるまで、*net_service_name_1* を DRG の別のノードのネット・サービス名に置換して、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 net_service_name_2 -load
   ```

   その後、次のコマンドを入力します。

   ```
   bulkload.sh -connect net_service_name_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 1.0。サイト：`http://sources.redhat.com/cygwin/`
- MKS Toolkit 5.1 または 6.0。
  サイト：`http://www.datafocus.com/products/`

関連項目：

- 構文と使用方法は、A-37 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、次のコマンドを実行します。

```
oidctl connect=net_service_name server=oidldapd instance=instance_number_of_ldap_
server flags='-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_ldap_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、次のコマンドを入力します。

```
oidctl connect=net_service_name server=oidrepld instance=1
   flags='-h host_name_of_this_computer -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・サーバーで行わ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・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： 21-7 ページ「レプリケーションにおける競合の解消」

注意： タスク 3 で実行した ldaprepl スクリプトによって、レプリケーション・サーバーを起動できる通常のデフォルトが設定されています。これらのデフォルトを変更する場合は、22-12 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」>「*directory server instance*」>「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。

レプリケーションの管理

レプリケーションをインストールして構成した後で、サーバー構成およびレプリケーション承諾用のデフォルト・パラメータを必要に応じて変更できます。レプリケーション承諾は、変更内容を共有する（レプリケーション・グループ内の）メンバー・ノードをリストするエントリです。レプリケーション承諾は、ディレクトリ・レプリケーション・サーバーの実行時にロードされる、レプリケーション・サーバーの構成パラメータによって参照されます。

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は、特別な属性としてディレクトリ・エントリに格納されています。レプリケーション・パラメータとレプリケーション承諾は、Oracle Internet Directory と同様に構成できます。次のどちらかを行うことができます。

- Oracle Directory Manager を使用して、22-13 ページおよび 22-17 ページの説明に従って、構成エントリおよび承諾エントリを表示および変更します。
- コマンドライン・ツール（ldapadd や ldapmodify など）を使用して、22-14 ページおよび 22-18 ページの説明に従って、構成エントリおよび承諾エントリを変更します。

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。

この項では、この 2 つの使用方法および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

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は、レプリケーション・サーバーの**構成設定エントリ**に格納されています。識別名は次のとおりです。

```
cn=configset0,cn=osdrepld,cn=subconfigsubentry
```

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。`orclDirReplGroupAgreement` 属性にはレプリケーション承諾識別子が含まれています。このリリースでは、レプリケーション承諾は 1 つのみ設定できます。

表 22-1 は、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です。

表 22-1　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
orclPurgeSchedule	単一値の属性。パージ（ガベージ・コレクション）間隔を分単位で指定します。適用済みのエントリや候補の変更に従って削除されたエントリを除去します。このスレッドは、設定した頻度に基づいて定期的に起動されます。このパラメータの値は 1 以上にする必要があります。	10 分	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
orclDirReplGroupAgreement	複数値の属性。このサーバーに管理責任がある対称型レプリケーション承諾を識別します。	orclagreementid=000001、cn=orclreplagreements	いいえ
orclChangeLogLife	単一値の属性。変更ログ・ストア内のエントリの存続時間を時間単位で指定します。0（ゼロ）は変更番号ベースの削除であることを示します。 **関連項目：**21-6 ページ「変更ログの削除」	0	はい

Oracle Directory Manager を使用したレプリケーションの構成パラメータの表示と変更

レプリケーション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」>「*directory server instance*」>「サーバーの管理」>「レプリケーション・サーバー」の順に展開します。
2. パラメータを表示または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。

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。

構成パラメータが「一般」タブ・ページに表示されます。このタブ・ページは、レプリケーションの構成パラメータの表示と、その多くの変更に使用します。次の表は、このタブ・ページのフィールドの説明です。

フィールド	説明
タイムスタンプの変更	エントリの作成または変更の時間（**UTC（Coordinated Universal Time）**）。このパラメータは変更できません。
Modifier's Name	エントリを作成または変更した人の名前。このパラメータは変更できません。
変更リトライ回数	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。
パージ・スケジュール	ガベージ・コレクションの間隔（分）を入力します。レプリケーションのガベージ・コレクション・スレッドは、適用済みのエントリや候補の変更に従って削除されたエントリを除去します。デフォルトは 10 です。
サプライヤあたりのスレッド数	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。
設定	構成の識別子を入力します。
変更ログの存続時間	変更ログ・オブジェクトの存続期間（時間）を入力します。 **関連項目：**21-6 ページ「変更ログの削除」

コマンドライン・ツールを使用したレプリケーション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-28 ページの「ldapmodify の構文」で説明されている構文を使用してください。

ldapmodify を使用したガベージ・コレクション間隔の変更 この例では、`mod.ldif` という名前の入力ファイルを使用して、ガベージ・コレクションの間隔をデフォルトの 10 分から 30 分に変更します。

1. `mod.ldif` を次のように編集します。

```
dn: cn=configset0,cn=osdrepld,cn=subconfigsubentry
changetype: modify
replace: orclPurgeSchedule
orclPurgeSchedule: 30
```

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 -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。

ldapmodify を使用した「変更ログの存続時間」パラメータの変更 この例では、mod.ldif という名前の入力ファイルを使用して、「変更ログの存続時間」パラメータを 10 時間に変更します。

1. mod.ldif を次のように編集します。

```
dn: cn=configset0,cn=oidrepld,cn=subconfigsubentry
changetype: modify
replace: orclChangeLogLife
orclChangeLogLife: 10
```

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 -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。

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. 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 -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。

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. 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 -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、3-8 ページの「ディレクトリ・サーバー・インスタンスの再起動」を参照してください。

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*,cn=orclreplagreements

このエントリには、この承諾のメンバーであるノードにのみ関係する属性が含まれています。複数のレプリケーション承諾を作成し、情報交換が行われているノード間でレプリケーションを管理できますが、Oracle Directory Manager を使用してサーバーの起動メッセージで参照できるのは、その中の 1 つのみです。Oracle Internet Directory リリース 9.2 の場合、使用できるレプリケーション承諾は 1 つのみです。

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。

注意： 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：

- 22-17 ページ「Oracle Directory Manager を使用したレプリケーション承諾のパラメータの表示と変更」
- 22-18 ページ「ldapmodify を使用したレプリケーション承諾のパラメータの変更」
- 22-31 ページ「ホストから独立したものとしてのノードの識別」

Oracle Directory Manager を使用した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」>「*directory server instance*」>「サーバーの管理」>「レプリケーション・サーバー」の順に展開し、「デフォルト構成設定」を選択します。
2. 右側のペインで、「承諾」タブを選択してレプリケーション承諾を表示します。

   このタブ・ページの各フィールドの説明は、次の表に記載されています。属性をダブルクリックすると、パラメータを表示でき、その一部を変更することもできます。

フィールド	説明	デフォルト値	変更可能？
承諾 ID	レプリケーション承諾の一意識別子。	000001	いいえ
除外されたネーミング・コンテキスト	複数値の属性。このレプリケーション承諾から除外されるネーミング・コンテキストを指定します。他のレプリカから送信されたこれらのネーミング・コンテキスト内のエントリへの変更は、ローカル・ノードでは適用されません。	なし	はい
レプリケーション・グループ・ノード	複数値の属性。対称型レプリケーション承諾のメンバーとなるノードを指定します。ここで指定したノードは、互いに更新内容を共有します。		はい
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。	1	はい

フィールド	説明	デフォルト値	変更可能？
Orcl HIQSchedule	管理者操作キューのレプリケーションの更新間隔。この値は分単位です。通常は orclUpdateSchedule よりも大きい値です。更新の再試行が競合の解消に失敗した場合、管理者はこの時間でディレクトリ情報ツリー構造を変更できます。	10	はい
レプリケーション・プロトコル	このレプリケーション承諾で使用されるレプリケーション・プロトコルを指定します。サポートされているプロトコルは、Oracle9*i* レプリケーションです。	ODS_ASR_1.0	いいえ

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。

3. 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 を使用したレプリケーション承諾のパラメータの変更

次の表は、レプリケーション承諾のパラメータのリストおよび説明です。

パラメータ	説明	デフォルト値	変更可能？
`orclAgreementID`	レプリケーション承諾の一意識別子。	000001	いいえ
`orclExcludedNamingcontexts`	複数値の属性。このレプリケーション承諾から除外されるネーミング・コンテキストを指定します。他のレプリカから送信されたこれらのネーミング・コンテキスト内のエントリへの変更は、ローカル・ノードでは適用されません。	なし	はい
`orclDirReplGroupDSAs`	複数値の属性。対称型レプリケーション承諾のメンバーとなるノードを指定します。ここで指定したノードは、互いに更新内容を共有します。		はい

パラメータ	説明	デフォルト値	変更可能？
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。	1	はい
OrclHIQSchedule	管理者操作キューのレプリケーションの更新間隔。この値は分単位です。通常は orclUpdateSchedule よりも大きい値です。更新の再試行が競合の解消に失敗した場合、管理者はこの時間でディレクトリ情報ツリー構造を変更できます。	10	はい
orclReplicationProtocol	このレプリケーション承諾で使用されるレプリケーション・プロトコルを指定します。サポートされているプロトコルは、Oracle9*i* レプリケーションです。	ODS_ASR_1.0	いいえ

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。

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=orclreplagreements
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 -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、識別名に orclagreementid=000001,cn=orclreplagreements 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。

22-21 ページの「レプリケーション・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 リリース 9.2 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。

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

Oracle9*i* レプリケーション管理者は、-chgpaswd ユーティリティを使用して、すべてのノードで Oracle9*i* レプリケーション管理用のパスワードを変更できます。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。

```
ldaprepl.sh -chgpswd
```

-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すると、3 回まで再度入力が要求されます。

レプリケーション・ノードの追加

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 を使用する方法

  この方法の方が、次の方法よりもより簡単です。この章で説明するのは、こちらの方法です。処理を完全に自動化でき、生成されたファイルは部分レプリケーションに使用できます。ディレクトリが非常に大規模である場合以外は、この方法を使用してください。100 万個のエントリがあるディレクトリであれば、この方法でのバックアップに約 7 時間を要します。

- コールド・バックアップを使用する方法

  この方法（第 23 章「データベース・コピー・プロシージャを使用したノードの追加」を参照）は、完全には自動化できません。部分レプリケーションに再利用することもできません。ただし、ディレクトリ・サーバーの規模が大きい場合は、コールド・バックアップの方が時間がかかりません。たとえばディレクトリのエントリが 100 万個を超えるような場合は、この方法を採用してください。

レプリケーション・ノードを追加する前に、次の準備を行います。

- 22-4 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。
- 新規ノードにデータが存在していないことを確認します。既存のデータは、**ディレクトリ・レプリケーション・グループ（DRG）**の他のメンバーにレプリケートされません。既存のデータをレプリケートする手順は、次のとおりです。

  1. ldapsearch を `-L` オプション付きで使用して、データを LDIF ファイルに抽出します。
  2. エクスポートしたすべてのエントリを新規ノードから削除します。
  3. 新規ノードを DRG に追加した後、ldapadd を使用して新規データを他のノードにレプリケートしたり、エクスポートしたデータを再ロードできます。

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: 全ノードでディレクトリ・レプリケーション・サーバーを停止

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 レプリケーション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ディレクトリ・レプリケーション・サーバーを起動

タスク 7: bulkload を使用して新規ノードにデータをロード

タスク 8: 新規ノードで LDAP サーバーを起動

タスク 9: 新規ノードでディレクトリ・レプリケーション・サーバーを起動

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、次のタイプの項目が、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: DRG の全ノードへの Oracle Internet Directory のインストール」を開始する前に、これら 3 つのタイプの項目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: 全ノードでディレクトリ・レプリケーション・サーバーを停止

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

oidctl connect=net_service_name server=oidldapd restart
```

このコマンドは、スポンサ・ノードで実行中の全 Oracle ディレクトリ・サーバーを読取り専用モードで再起動します。ディレクトリ・サーバーの再起動には、約 15 秒を要します。

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。

さらに、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を要する場合があるため、バックアップ処理中に「タスク 4: Oracle9i レプリケーション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 db_connect_string -b "" -f output_ldif_file
```

タスク 4: Oracle9*i* レプリケーション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・ノードから、次のスクリプトを実行します。

```
ldaprepl.sh -addnode
```

このスクリプトは、次の複数の操作を実行します。

- スポンサ・ノードおよびその他の既存**マスター・サイト**で Oracle9*i* レプリケーションを静止。
- マスター・サイトと新規ノードの構成。マスター・サイトとは、スポンサ・ノード以外のサイトで、LDAP レプリケーションのメンバーであるサイトのことです。
- すべてのサイト（新規ノードを含む）でレプリケーションの送信ジョブを構成。
- すべての手順が正常に完了したことをチェック。（長時間を要する場合があります。）
- ノード追加後の操作の実行。

スクリプトを実行すると、表 22-2 にリストされている情報を、最初にスポンサ・ノード、次に既存のマスター・サイトについて要求されます。

表 22-2　ldaprepl.sh で要求される情報

要求される情報	定義
MDS グローバル名	tnsnames.ora ファイルにリストされている、MDS データベースのネット・サービス名
MDS のシステム・パスワード	マスター定義サイトのシステム・パスワード

既存のマスター・サイトをすべて確認して、N を入力します。追加するノードのグローバル名、そのノードのシステム・パスワードおよびレプリケーション管理者のデータベース・アカウント・パスワードの入力が要求されます。情報の指定が終了すると、指定した情報が一覧表示され、確認を要求されます。

情報に誤りがある場合は、「N」をクリックします。スクリプトが最初から実行され、同じ情報が要求されます。情報が正しい場合は「Y」を入力します。スクリプトによって、サイトの構成が開始されます。

この処理は、システム・リソースと DRG のサイズによって、長時間を要する場合があります。処理の経過は、継続的に通知されます。

注意： なんらかの理由で完了前に処理を中断する必要がある場合は、最初から実行しなおす必要があります。

エラーが表示された場合は、22-32 ページの「レプリケーション設定のトラブルシューティング」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

oidctl connect=net_service_name server=oidldapd restart
```

注意： タスク 5 は、タスク 2 と類似しています。唯一異なるのは、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）に設定されることです。

タスク 6: 新規ノード以外の全ノードでディレクトリ・レプリケーション・サーバーを起動

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 を使用して新規ノードにデータをロード

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 -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 1.0。サイト：`http://sources.redhat.com/cygwin/`
- MKS Toolkit 5.1 または 6.0。
  サイト：`http://www.datafocus.com/products/`

タスク 8: 新規ノードで LDAP サーバーを起動

LDAP 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: 新規ノードでディレクトリ・レプリケーション・サーバーを起動

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、22-12 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、bulkload.sh を使用してデータをノードに追加しないでください。かわりに、ldapadd を使用してください。

レプリケーション・ノードの削除

DRG からノードを削除することもできます。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、このノードを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。

エントリが 100 万個未満のディレクトリからレプリケーション・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: 全ノードでディレクトリ・レプリケーション・サーバーを停止

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: すべてのノードでディレクトリ・レプリケーション・サーバーを起動

注意： 以降の各タスクで示されているコマンドを実行するには、次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 を開始する前に、3 つの変数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: 全ノードでディレクトリ・レプリケーション・サーバーを停止

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=net_service_name 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

OID 制御ユーティリティおよび **OID モニター**を停止します。

関連項目：

- OID 制御ユーティリティの停止方法は、3-6 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。
- OID モニターの停止方法は、3-3 ページの「OID モニターの停止」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。

```
ldaprepl.sh -delnode
```

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 1.0。サイト：`http://sources.redhat.com/cygwin/`
- MKS Toolkit 5.1 または 6.0。
  サイト：`http://www.datafocus.com/products/`

このスクリプトは次の操作を実行します。

- MDS およびその他の既存**マスター・サイト**で **Oracle9i レプリケーション（Oracle9i Replication）**を静止
- `Directory Replication Group` パラメータからノードを削除
- すべての手順が正常に完了したことを検証

スクリプトを実行すると、MDS のグローバル名、削除するノードのグローバル名およびレプリケーション管理者のパスワードの入力が要求されます。情報の指定が終了すると、指定

した情報が一覧表示され、確認を要求されます。情報に誤りがある場合は、「N」をクリックします。スクリプトが最初から実行され、同じ情報が要求されます。情報が正しい場合は「Y」を入力します。スクリプトによって、サイトの構成が開始されます。

この処理は、システム・リソースと DRG のサイズによって、長時間を要する場合があります。処理の経過は、継続的に通知されます。

注意： なんらかの理由で完了前に処理を中断する必要がある場合は、最初から実行しなおす必要があります。

タスク 4: すべてのノードでディレクトリ・レプリケーション・サーバーを起動

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=net_service_name server=oidrepld instance=1
flags='-h host -p port' start
```

手動での競合の解消

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モニター
- 競合解消メッセージの例
- 管理者操作キュー操作ツールの使用
- OID 調停ツールの使用

レプリケーション変更の競合のモニター

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たな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、ログを定期的にモニターすることが重要です。

レプリケーション変更の競合をモニターするには、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使用

管理者操作キュー操作ツールによって、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。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. 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： A-43 ページ「管理者操作キュー操作ツール」

OID 調停ツールの使用

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。

関連項目： 構文および OID 調停ツールの動作の説明は、A-45 ページの「OID 調停ツール」を参照してください。

ホストから独立したものとしてのノードの識別

ほとんどの配置システムでは、DRG 内のノードは Oracle Internet Directory がインストールされているホストの名前で一意に識別されます。ただし、同じホストに複数の Oracle Internet Directory がインストールされているときは、ホスト名は一意のノード識別子になりません。この場合、ルート DSE の `orclReplicaId` 属性を使用する必要があります。

ホスト名ではなく `orclReplicaId` を使用して DRG 内のノードを識別するときは、この項の手順に従います。

注意： すべてのノードの `orclReplicaId` ルート DSE 属性の変更が完了するまでは、DRG 内のノードを更新しないでください。

---

1. DRG 内の各ノードで、`orclReplicaId` に一意の値を与えます。たとえば、同じコンピュータに 3 つのノードがあり、それぞれ対応するディレクトリ・サーバーがポート 1、ポート 2 およびポート 3 で実行されている場合は、次の変更を実行します。

```
ldapmodify -v -h host -p port1  << EOF
dn:
changetype: modify
replace: orclreplicaid
orclreplicaid : replica001

ldapmodify -v -h host -p port2  << EOF
dn:
changetype: modify
replace: orclreplicaid
orclreplicaid : replica002

ldapmodify -v -h host -p port3  << EOF
dn:
changetype: modify
replace: orclreplicaid
orclreplicaid : replica003
```

2. すべてのノードで `orclreplicaid` の変更が完了した後、22-2 ページの「レプリケーションのインストールと構成」の説明に従ってレプリケーション設定を実行します。

3. 22-18 ページの「ldapmodify を使用したレプリケーション承諾のパラメータの変更」の説明に従って DRG を変更するときは、`orclreplicaid` に割り当てた値と同じ値を `orcldirreplgroupdsas` 属性に与えます。前述の例を使用する場合は、`orcldirreplgroupdsas` 属性に値 `replica001`、`replica002` および `replica003` を指定します。

注意： レプリケーションの設定が完了した後は、`orclreplicaId` 属性を変更しないでください。

レプリケーション設定のトラブルシューティング

レプリケーションの設定に失敗した場合は、次の内容を実行してください。

1. 次のチェックを行います。
   `$ORACLE_HOME/ldap/admin/logs/ldaprepl.log` ファイルをチェックして、状態を調べてください。

2. ディレクトリ `$ORACLE_HOME/ldap/admin` に移動し、次のコマンドを実行してレプリケーション・ジョブの状態をチェックしてください。

   ```
   sqlplus system/password@net_service_name @ldaplogq.sql
   ```

   DRG のノードごとにこのコマンドを実行します。状態が正常な場合は、このコマンドの発行によって、行が選択されることはありません。行が選択され、その中に失敗のステータスとエラー・メッセージが含まれている場合は、Oracle9*i* レプリケーションの設定に失敗したことを意味しています。この場合は、次のいずれかの方法で対処します。

   - スクリプトを最初から実行する
   - 『Oracle9*i* アドバンスト・レプリケーション』でトラブルシューティングの章を参照する
   - Oracle9*i* レプリケーションの専門家に問い合せて、エラー・メッセージの情報から解決策を判断する

   関連項目：

   - 22-7 ページ「MDS でのディレクトリ・レプリケーション用の Oracle9i レプリケーションの構成」
   - 22-23 ページ「タスク 4: Oracle9i レプリケーション追加ノードの設定の実行」

23

データベース・コピー・プロシージャを使用したノードの追加

この章では、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 22 章「Oracle ディレクトリ・レプリケーション・サーバーの管理」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
- スポンサ・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
- スポンサ・ノードで実行されるタスク
- 新規ノードで実行されるタスク
- 検証プロセス

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

例：

`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=net_service_name server=oidrepld instance=instance_number stop
$ oidctl connect=net_service_name server=oidldapd instance=instance_number stop
$ oidmon connect=net_service_name stop
```

これらのコマンドで、*net_service_name* 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=net_service_name 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（MDS）**で次のスクリプトを実行して、**Oracle9i レプリケーション（Oracle9i 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 1.0。サイト：`http://sources.redhat.com/cygwin/`
- MKS Toolkit 5.1 または 6.0。
  サイト：`http://www.datafocus.com/products/`

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   （デフォルトのリスナー名は LISTENER です）
$ 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。

```
newdb.sql 始め
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'
;
newdb.sql 終わり
```

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 （ファイル initNLDAP.ora にパラメータが存在しない場合、ファイル configNLDAP.ora を変更します）

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。

```
tnsnames.ora 始め

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))
   )

tnsnames.ora 終わり
```

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。

```
listener.ora 始め

# 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

listener.ora 終わり
```

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、次のコマンドを実行します。

```
$ >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。

   oratab 始め

   ```
   NLDAP:/private1/oracle/app/oracle/product/8.1.6:N
   *:/private1/oracle/app/oracle/product/8.1.6:N
   ```

   oratab 終わり

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レーションを実行できます。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 1.0。サイト：`http://sources.redhat.com/cygwin/`
- MKS Toolkit 5.1 または 6.0。
  サイト：`http://www.datafocus.com/products/`

関連項目： Oracle9*i* のインストレーション・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レーション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、23-7 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。次のようなコマンドを実行します。

```
 $ cd /private1/oracle/app/oracle/admin/NLDAP/udump
                 （つまり、$ORACLE_BASE/admin/SID/udump です）
$ 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 （開始する前にパラメータ job_queue_process をコメント化しません）
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 です）
$ 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* レプリケーション・カタログを作成する必要があります。新規ノードで Oracle9*i* レプリケーション・カタログから MDS の定義を削除して Oracle9*i* レプリケーション・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* レプリケーションを構成するには、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 1.0。サイト：`http://sources.redhat.com/cygwin/`
- MKS Toolkit 5.1 または 6.0。
  サイト：`http://www.datafocus.com/products/`

---

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* レプリケーション・ベースのレプリケーションのメンバー・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生じることがありますが、この遅延は 2 ～ 3 分ほどです。

第 VI 部

ディレクトリとクラスタ

第 VI 部は次の各章で構成されています。

24

クラスタ構成でのフェイルオーバー

この章では、次の項目について説明します。

- 概要
- クラスタ化された環境でのフェイルオーバーの構成
- クラスタ化された環境でのフェイルオーバーの動作

概要

Oracle Internet Directory リリース 9.2 では、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。

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 アドレスを使用することになります。

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。

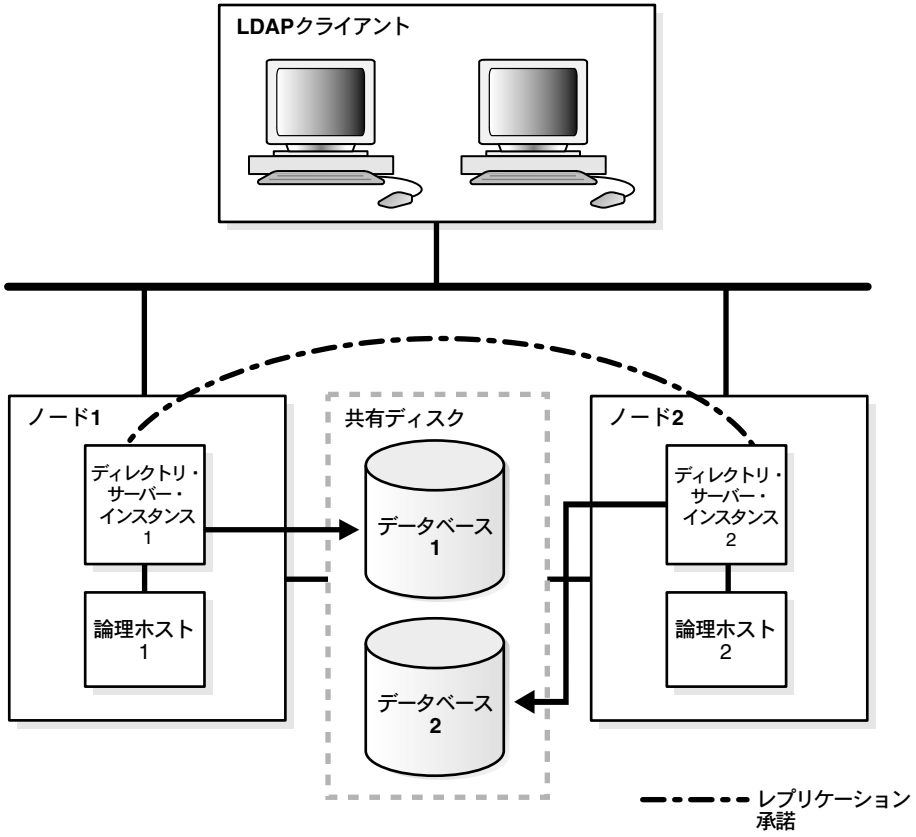
クライアントは、ディレクトリ・サーバーの論理ホスト名およびアドレスを使用してディレクトリ・サーバーに接続します。論理ホストが新規物理ホストにフェイルオーバーした場合は、このフェイルオーバーはクライアントに対して透過的です。

論理ホストは、ディスク記憶域に物理的にアクセスできる複数のクラスタ・ノードに常駐できます。通常、クラスタは論理ホストをいくつでもサポートでき、1 つの物理サーバーまたはクラスタ・ノードは複数の論理ホストとして使用できます。

このフェイルオーバー・メカニズムは、レプリケート環境もサポートします。

図 24-1 は、ハードウェア・クラスタにおける Oracle Internet Directory の構成のサンプルを示しています。

図 24-1 2 ノード・クラスタでの Oracle Internet Directory の構成



この構成は、次のように動作します。

- 物理ノード 1 が論理ホスト 1 をマスターする。
- 物理ノード 2 が論理ホスト 2 をマスターする。
- 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るディレクトリ・サーバー・インスタンス 1 が、論理ホスト 1 で動作する。
- 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るディレクトリ・サーバー・インスタンス 2 が、論理ホスト 2 で動作する。
- 両ディレクトリ・サーバー・インスタンスは、共有ディスクにそれぞれのディレクトリ・データ・ストア（Oracle データベース）を持つ。
- ディレクトリ・サーバー・インスタンス 1 とディレクトリ・サーバー・インスタンス 2 は、レプリケーション承諾内にある。

クライアントは、論理ホスト 1 のホスト名とアドレスを使用してディレクトリ・サーバー・インスタンス 1 に接続します。同様に、クライアントは、論理ホスト 2 のホスト名とアドレスを使用してディレクトリ・サーバー・インスタンス 2 に接続します。

クラスタ化された環境でのフェイルオーバーの構成

この項では、クラスタ化された環境でのフェイルオーバーの構成方法を説明します。

注意： Oracle Internet Directory のインストレーションの最後に、ディレクトリ・サーバー・インスタンスおよび OID モニターがデフォルトで起動します。論理ホストで Oracle Internet Directory を実行するには、ディレクトリ・サーバー・インスタンスおよび OID モニターを停止し、オプションのフラグ `-host` または `-h` を使用して再起動する必要があります。これは、ディレクトリを更新する前に行ってください。この方法により、変更ログの生成の際、ディレクトリ・サーバーは論理ホスト名を確実に使用することになります。

次の項目について説明します。

- 手順 1: OID モニターの起動
- 手順 2: OID 制御ユーティリティを使用したディレクトリ・サーバーまたはディレクトリ・レプリケーション・サーバーの起動
- 手順 3: ディレクトリ・サーバーと OID モニターの停止と再起動

手順 1: OID モニターの起動

OID モニターを起動するときは、オプションの host 引数を使用し、この引数を論理ホスト名に設定します。次の例では、OID モニターがディレクトリ・ストア my_net_service に接続し、論理ホスト my_host のディレクトリ・サーバー・インスタンスを監視します。

```
oidmon [connect=my_net_service] host=my_host
```

手順 2: OID 制御ユーティリティを使用したディレクトリ・サーバーまたはディレクトリ・レプリケーション・サーバーの起動

OID 制御ユーティリティを使用してディレクトリ・サーバーを起動するときは、オプションのフラグ -host または -h を使用し、このフラグを論理ホスト名に設定します。次の例では、OID 制御ユーティリティが、OID モニターに論理ホスト my_host のディレクトリ・サーバー・インスタンスを起動させます。

```
oidctl connect=my_net_service server=oidldapd instance=1 flags="-h my_host" start
```

同様に、OID 制御ユーティリティ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ときは、オプションのフラグ -host または -h を使用し、このフラグを論理ホスト名に設定します。次の例では、OID 制御ユーティリティが、OID モニターに論理ホスト my_host のディレクトリ・レプリケーション・サーバー・インスタンスを起動させます。

```
oidctl connect=my_net_service server==oidrepld instance=1 flags="-h my_host" start
```

注意： レプリケーション承諾は、物理ホスト名ではなく論理ホスト名を使用する必要があります。

レプリケート環境で論理ホストを使用する場合は、Oracle Internet Directory の新規インストールが必要です。リリース 3.0.1 より前のレプリケーション環境からアップグレードしている場合、レプリケーション承諾のホスト名が論理ホスト名と異なるため、レプリケーションは動作しません。

手順 3: ディレクトリ・サーバーと OID モニターの停止と再起動

論理ホストで Oracle Internet Directory を実行するには、ディレクトリ・サーバー・インスタンスおよび OID モニターを停止し、オプションのフラグ `-host` または `-h` を使用して再起動します。これは、ディレクトリを更新する前に行ってください。この方法により、変更ログの生成の際、ディレクトリ・サーバーは論理ホスト名を確実に使用することになります。

関連項目：

- 3-6 ページ「Oracle ディレクトリ・サーバー・インスタンスの停止」
- 3-3 ページ「OID モニターの停止」
- 3-4 ページ「Oracle ディレクトリ・サーバー・インスタンスの起動」
- 3-2 ページ「OID モニターの開始」

クラスタ化された環境でのフェイルオーバーの動作

図 24-2 は、フェイルオーバーが発生してディレクトリ・サーバーが再起動される例を示しています。

図 24-2 フェイルオーバー後の Oracle Internet Directory のノード

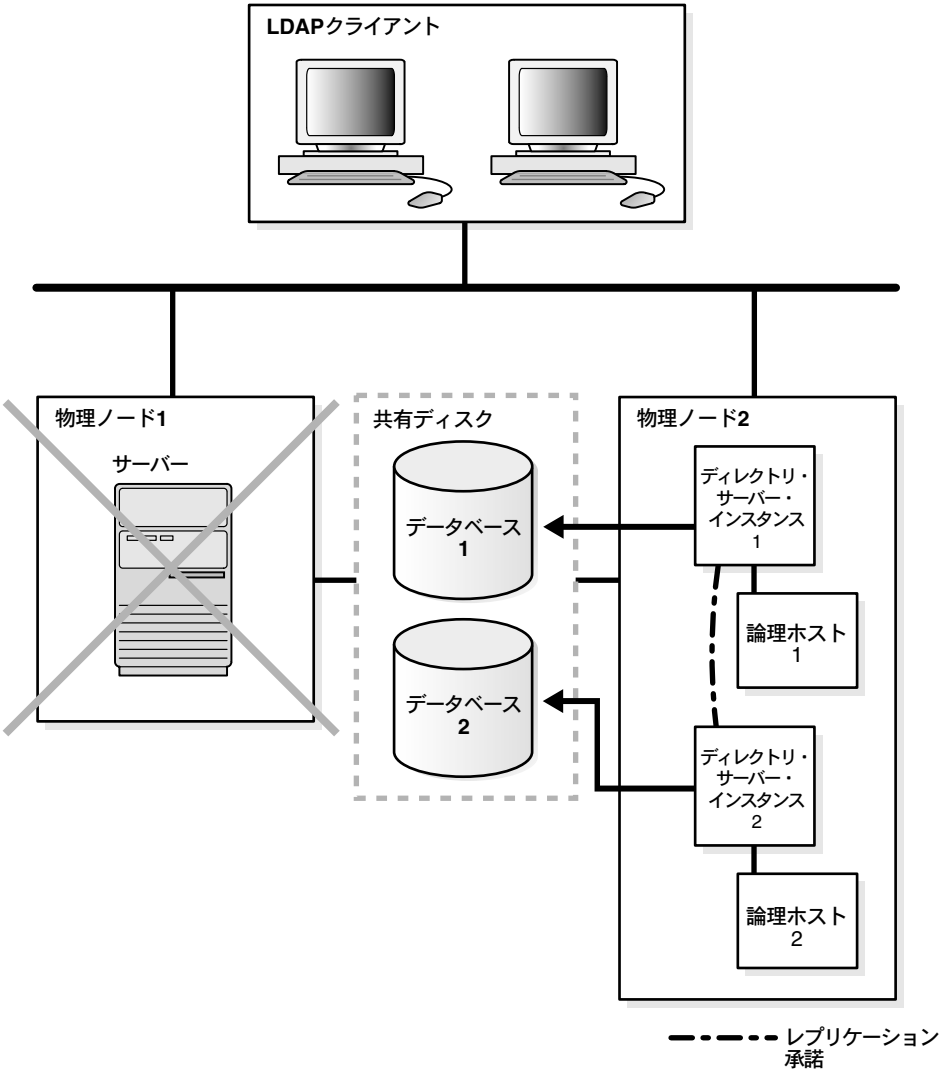


図 24-2 では、物理ノード 1 に障害が発生します。この時点で、論理ホスト 1 がフェイルオーバーして物理ノード 2 にマスターされます。これが完了した後、ディレクトリ・サーバー・インスタンス 1 を再起動する必要があります（つまり、ホスト名として論理ホスト 1 を指定して OID モニターを再起動する必要があります）。

このディレクトリ・サーバー・インスタンス 1 のフェイルオーバーは、ディレクトリ・サーバー・インスタンス 1 に接続している LDAP クライアントに対して透過的です。これらのクライアントは、引き続き論理ホスト 1 のホスト名とアドレスを使用してディレクトリ・サーバー・インスタンス 1 に接続します。

フェイルオーバー後、ディレクトリ・サーバー・インスタンス 1 は、変更ログの生成の際に引き続き論理ホスト 1 のホスト名を使用します。ディレクトリ・サーバー・インスタンス 1 とディレクトリ・サーバー・インスタンス 2 の間のレプリケーション承諾は、フェイルオーバー前と同様に継続します。

25

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

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。

- Oracle9i Real Application Clusters 環境での Oracle ディレクトリ・サーバー
- Oracle9i Real Application Clusters 環境での Oracle ディレクトリ・レプリケーション・サーバー

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、接続に障害が起きた場合、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

ディレクトリ・サーバーは、クラスタ・データベースを実行しているノードとは異なるノードで実行できます。ディレクトリ・サーバーを実行するコンピュータが、クラスタの一部である場合があります。

この項では、次の項目について説明します。

- 基本的な高可用性の構成の Oracle Internet Directory
- デフォルトの N ノード構成の Oracle Internet Directory

基本的な高可用性の構成の Oracle Internet Directory

このケースでは、単一のディレクトリ・サーバーが、それぞれが異なるノードで実行される 2 つ以上の Real Application Clusters インスタンスに接続します。この使用例は構成が容易で、プライマリ・インスタンスが実行されているノードで、ハードウェアまたはソフトウェアの障害発生後に高いリジリエンスが得られます。

図 25-1 は、設定の詳細を示しています。

図 25-1 基本的な高可用性の構成の Oracle Internet Directory

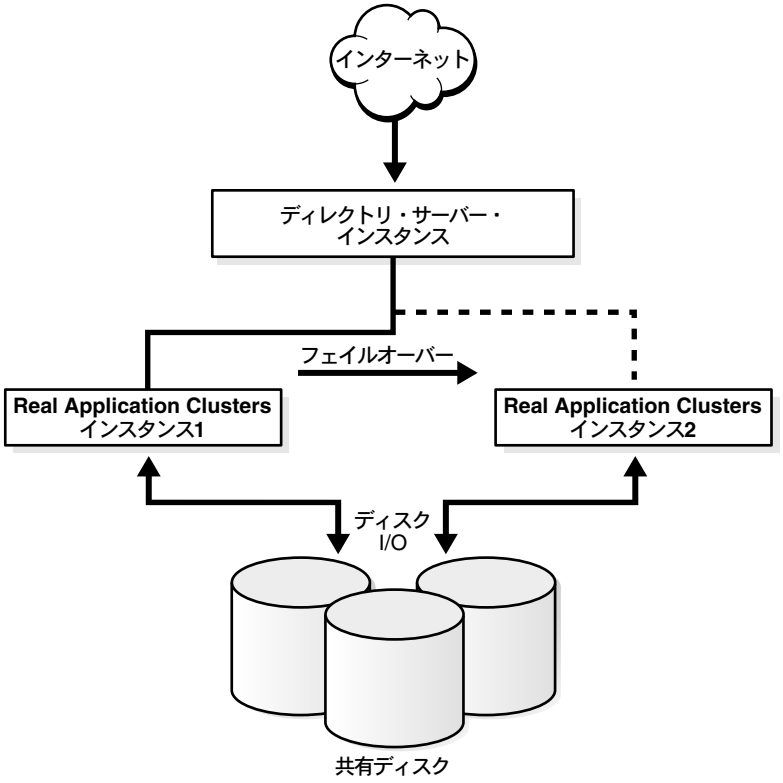


図 25-1 は、3 ノード・クラスタを示しています。Real Application Clusters インスタンス 1 はノード 1 で実行されます。Real Application Clusters インスタンス 2 はノード 2 で実行されます。ディレクトリ・サーバー・インスタンスはノード 3 で実行されます。

通常、ディレクトリ・サーバー・インスタンスは、プライマリ・インスタンスであるノード 1 の Real Application Clusters インスタンスと通信します。しかし、ノード 1 でハードウェアまたはソフトウェアの障害が発生した場合は、Oracle Net Services は、セカンダリ・インスタンスであるノード 2 の Real Application Clusters インスタンスにデータベース要求をリダイレクトできます。

プライマリ・インスタンスを指定するには、初期化ファイルで、両方のインスタンスの ACTIVE_INSTANCE_COUNT パラメータを 1 に設定します。最初に起動したインスタンスがプライマリ・インスタンスになります。

プライマリ・インスタンスは、セカンダリ・インスタンス・リスナーからの接続だけでなく、ローカル・リスナーからの接続を受け入れることもできます。セカンダリ・インスタンスはローカル・リスナーにセカンダリ・インスタンスとして登録され、プライマリ・インスタンスと同様に、ACTIVE_INSTANCE_COUNT パラメータは 1 に設定されます。プライマリ・インスタンスに障害が発生した場合は、セカンダリ・インスタンスがプライマリ・ロールを引き受け、そのリスナーに登録されます。障害が発生したインスタンスが再び起動できた場合、このインスタンスがセカンダリ・インスタンスとして同じことを行います。フェイルオーバーが構成されている場合は、障害が発生したプライマリ・インスタンスへのディレクトリ・サーバー接続がセカンダリ・インスタンスにフェイルオーバーします。

次に、接続時フェイルオーバー用に構成された tnsnames.ora ファイルの例を示します。この例では、LOAD_BALANCE を OFF に設定する必要があります。

```
MY_CLUSTER =
  (DESCRIPTION =
    (LOAD_BALANCE = OFF)
    (ADDRESS = (PROTOCOL = TCP)(HOST = my_host_1)(PORT = 1521))
    (ADDRESS = (PROTOCOL = TCP)(HOST = my_host_2)(PORT = 1521))
    (CONNECT_DATA = (SERVICE_NAME = my_cluster.my_company.com))
  )
MY_CLUSTER_1 =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = my_host_2)(PORT = 1521))
    (CONNECT_DATA =
      (SERVICE_NAME = my_cluster.my_company.com)
      (INSTANCE_NAME = my_cluster_1)
    )
  )
MY_CLUSTER_2 =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = my_host_1)(PORT = 1521))
    (CONNECT_DATA =
      (SERVICE_NAME = my_cluster.my_company.com)
      (INSTANCE_NAME = my_cluster_2)
    )
  )
```

次に、my_host_1 で接続時フェイルオーバー用に構成された listener.ora ファイルの例を示します。

```
LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS_LIST =
        (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC0))
      )
      (ADDRESS_LIST =
        (ADDRESS = (PROTOCOL = TCP)(HOST = my_host_1)(PORT = 1521))
      )
    )
  )
```

次に、透過的アプリケーション・フェイルオーバー（TAF）用に構成された tnsnames.ora ファイルの例を示します。

```
MY_CLUSTER =
  (DESCRIPTION =
    (FAILOVER = ON)
    (LOAD_BALANCE = OFF)
    (ADDRESS = (PROTOCOL = TCP)(HOST = my_host_1)(PORT = 1521))
    (ADDRESS = (PROTOCOL = TCP)(HOST = my_host_2)(PORT = 1521))
    (CONNECT_DATA = (SERVICE_NAME = my_cluster.my_company.com)
      (FAILOVER_MODE = (TYPE = SELECT) (METHOD = PRECONNECT)
                       (BACKUP = ops1))
    )
  )
MY_CLUSTER_1 =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = my_host_2)(PORT = 1521))
    (CONNECT_DATA =
      (SERVICE_NAME = my_cluster.my_company.com)
      (INSTANCE_NAME = ops1)
    )
  )
MY_CLUSTER_2 =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = my_host_1)(PORT = 1521))
    (CONNECT_DATA =
      (SERVICE_NAME = my_cluster.my_company.com)
      (INSTANCE_NAME = my_cluster_2)
    )
  )
```

次に、my_host_1 で透過的アプリケーション・フェイルオーバー（TAF）用に構成された listener.ora ファイルの例を示します。

```
LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS_LIST =
        (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC0))
      )
      (ADDRESS_LIST =
        (ADDRESS = (PROTOCOL = TCP)(HOST = my_host_1)(PORT = 1521))
      )
    )
  )
```

注意： データベース障害が発生したときのディレクトリ・サーバーの状態によっては、Oracle Internet Directory が透過的アプリケーション・フェイルオーバーを正常に管理できない場合があります。この場合、Oracle Internet Directory はログ・ファイルに「ORA-03113 通信チャネルで end-of-file が検出されました。」と記録し、稼働中のデータベース・インスタンスに対して新規データベース接続を再確立します。

LDAP 操作中にフェイルオーバーが発生すると、クライアントは「DSA unwilling to perform」または「ldapbind: Operations」エラーを受け取ります。この場合は、クライアントはディレクトリ・サーバーに要求を再発行するだけで済みます。

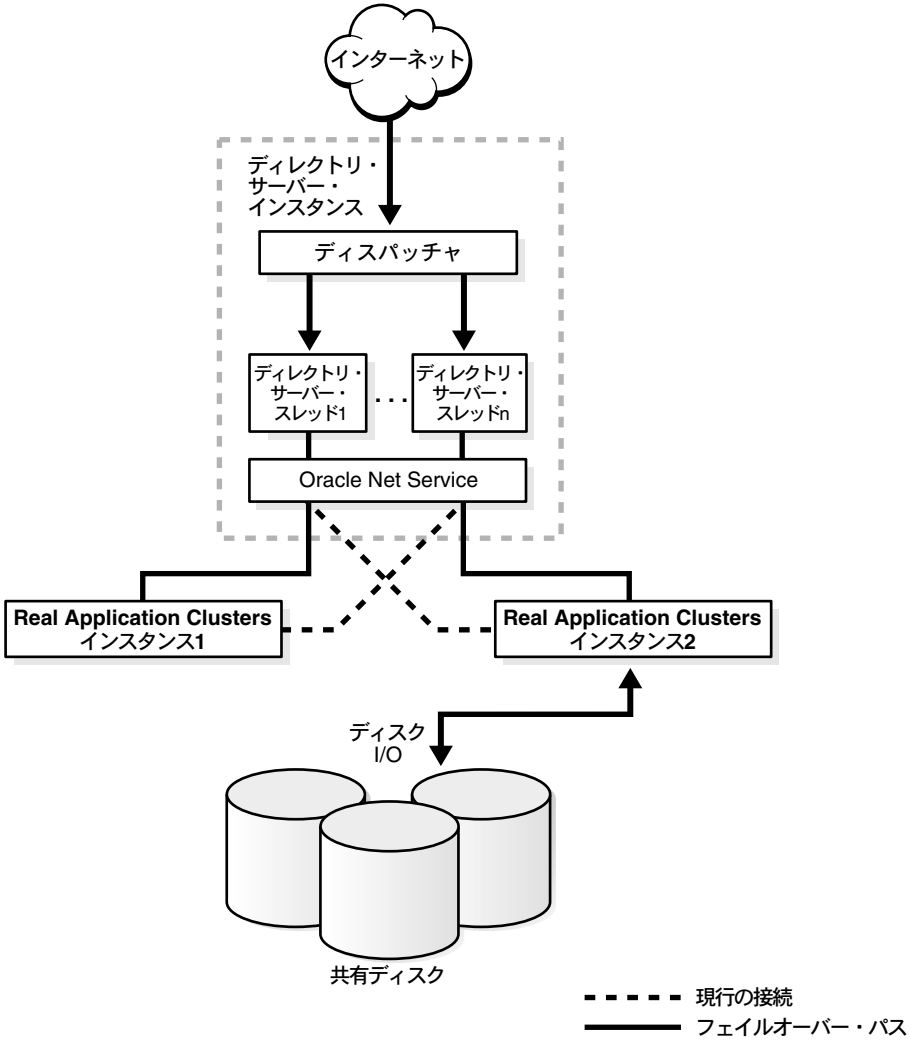
デフォルトの N ノード構成の Oracle Internet Directory

このケースでは、複数のディレクトリ・サーバー・スレッドが存在し、異なるノードにある 2 つ以上の Real Application Clusters インスタンスに接続します。これは、Oracle Net Services の LOAD_BALANCE パラメータを ON に設定することにより実現できます。

図 25-2 は、3 ノード・クラスタを示しています。Real Application Clusters インスタンス 1 はノード 1 で実行されます。Real Application Clusters インスタンス 2 はノード 2 で実行されます。ディレクトリ・サーバー・スレッド 1 とディレクトリ・サーバー・スレッド 2 を持つディレクトリ・サーバー・インスタンスは、ノード 3 で実行されます。

関連項目： LOAD_BALANCE パラメータの設定方法は、『Oracle9*i* Net Services 管理者ガイド』を参照してください。

図 25-2 1 つのノードの単一のディレクトリ・サーバー・インスタンスと、複数の Real Application Clusters インスタンス



Oracle Net Services による LDAP 要求の経路指定によっては、図 25-2 のすべてのノードが実行されているときに、ディレクトリ・サーバー・スレッド 1 が Real Application Clusters インスタンス 1 に接続し、ディレクトリ・サーバー・スレッド 2 が Real Application Clusters インスタンス 2 に接続する場合があります。受信したディレクトリ・サーバーへの LDAP 要求は、両方のディレクトリ・データベース接続にラウンドロビン法で配布されます。ノード 1 でハードウェアまたはソフトウェアの障害が発生した場合は、ディレクトリ・サーバー・スレッド 1 は、接続時フェイルオーバーまたは Oracle Net の透過的アプリケーション・フェイルオーバーを使用して、Real Application Clusters インスタンス 2 に再接続します。

この使用例では、より高い可用性と拡張性が得られます。データベースまたはデータベース・ホストに障害が発生した場合は、接続時フェイルオーバーまたは Oracle Net の透過的アプリケーション・フェイルオーバーの使用により、リジリエンスが得られます。さらに、複雑な LDAP サブツリー検索でより高いスループットが得られます。

この使用例でシステムを構成するには、次の様々な例の構成ファイルを検証します。

次の例は、接続時フェイルオーバー用に構成された `tnsnames.ora` ファイルを示します。

```
MY_CLUSTER =
  (DESCRIPTION =
    (LOAD_BALANCE = ON)
    (ADDRESS = (PROTOCOL = TCP)(HOST = my_host_1)(PORT = 1521))
    (ADDRESS = (PROTOCOL = TCP)(HOST = my_host_2)(PORT = 1521))
    (CONNECT_DATA = (SERVICE_NAME = my_cluster.my_company.com))
  )
MY_CLUSTER_1 =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = my_host_2)(PORT = 1521))
    (CONNECT_DATA =
      (SERVICE_NAME = my_cluster.my_company.com)
      (INSTANCE_NAME = my_cluster_1)
    )
  )
MY_CLUSTER_2 =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = my_host_1)(PORT = 1521))
    (CONNECT_DATA =
      (SERVICE_NAME = my_cluster.my_company.com)
      (INSTANCE_NAME = my_cluster_2)
    )
  )
```

次の例は、my_host_1 で接続時フェイルオーバー用に構成された listener.ora ファイルを示します。

```
# LISTENER.ORA Network Configuration
# Generated by Oracle configuration tools.

LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS_LIST =
        (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC0))
      )
      (ADDRESS_LIST =
        (ADDRESS = (PROTOCOL = TCP)(HOST = my_host_1)(PORT = 1521))
      )
    )
  )
```

次の 2 つの例は、透過的アプリケーション・フェイルオーバー（TAF）用に構成された、my_host_1 用と my_host_2 用の 2 つの tnsnames.ora ファイルを示します。

my_host_1 の tnsnames.ora は、次のようになります。

```
MY_CLUSTER =
  (DESCRIPTION =
    (FAILOVER = ON)
    (LOAD_BALANCE = ON)
    (ADDRESS = (PROTOCOL = TCP)(HOST = my_host_1)(PORT = 1521))
    (ADDRESS = (PROTOCOL = TCP)(HOST = my_host_2)(PORT = 1521))
    (CONNECT_DATA = (SERVICE_NAME = my_cluster.my_company.com)
      (FAILOVER_MODE = (TYPE = SELECT) (METHOD = PRECONNECT)
                       (BACKUP = my_host_1))
    )
  )
MY_CLUSTER_1 =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = my_host_2)(PORT = 1521))
    (CONNECT_DATA =
      (SERVICE_NAME = my_cluster.my_company.com)
      (INSTANCE_NAME = my_company_1)
    )
  )
```

```
MY_CLUSTER_2 =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = my_host_1)(PORT = 1521))
    (CONNECT_DATA =
      (SERVICE_NAME = my_cluster.my_company.com)
      (INSTANCE_NAME = my_company_2)
    )
  )
```

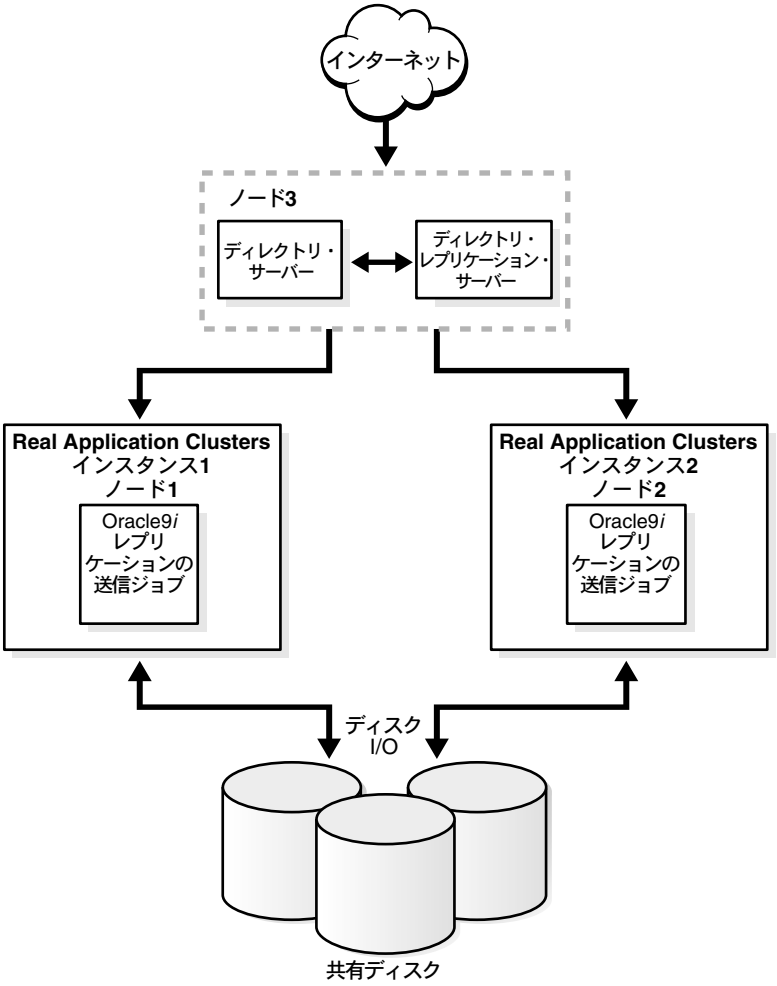
my_host_2 の tnsnames.ora は、次のようになります。

```
MY_CLUSTER =
  (DESCRIPTION =
    (FAILOVER = ON)
    (LOAD_BALANCE = ON)
    (ADDRESS = (PROTOCOL = TCP)(HOST = my_host_1)(PORT = 1521))
    (ADDRESS = (PROTOCOL = TCP)(HOST = my_host_2)(PORT = 1521))
    (CONNECT_DATA = (SERVICE_NAME = my_cluster.my_company.com)
      (FAILOVER_MODE = (TYPE = SELECT) (METHOD = PRECONNECT)
                       (BACKUP = my_company_2))
    )
  )
MY_CLUSTER_1 =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = my_host_1)(PORT = 1521))
    (CONNECT_DATA =
      (SERVICE_NAME = my_cluster.my_company.com)
      (INSTANCE_NAME = my_cluster_1)
    )
  )
MY_CLUSTER_2 =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = my_host_2)(PORT = 1521))
    (CONNECT_DATA =
      (SERVICE_NAME = my_cluster.my_company.com)
      (INSTANCE_NAME = my_cluster_2)
    )
  )
```

Oracle9*i* Real Application Clusters 環境での Oracle ディレクトリ・レプリケーション・サーバー

図 25-3 は、Oracle9*i* Real Application Clusters 環境での Oracle ディレクトリ・レプリケーション・サーバーの一例です。

図 25-3 Oracle9*i* Real Application Clusters 環境でのディレクトリ・レプリケーション・サーバー



この構成には 3 つのノードが存在します。ディレクトリ・サーバー・インスタンスはノード 3 で実行され、Real Application Clusters インスタンスはノード 1 およびノード 2 で実行されます。すべてのノードが実行されているときは、ディレクトリ・レプリケーション・サーバーはディレクトリ・サーバー・インスタンスに接続し、Oracle9*i* レプリケーションの送信ジョブは両方の Real Application Clusters インスタンスで実行されています。ノード 3 でハードウェア障害が発生すると、ノード 2 のディレクトリ・レプリケーション・サーバーが再起動し、ディレクトリ・サーバー・インスタンス 2 に接続します。ノード 2 でハードウェア障害が発生すると、クラスタの再構成後、Oracle9*i* レプリケーションの送信ジョブは Real Application Clusters インスタンス 1 で継続されます。

この使用例では、データベースまたはデータベース・ホストにレプリケーション・データ転送の（すなわち、Oracle9*i* レプリケーションの送信ジョブの）障害が発生した場合のリジリエンスが得られます。または、ディレクトリ・サーバー・インスタンスまたはホストの障害、またはディレクトリ・レプリケーション・サーバーの障害が発生した場合のリジリエンスも得られます。

第 VII 部

ディレクトリ・プラグイン

第 VII 部は次の章で構成されています。

26

Oracle Internet Directory のプラグイン・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。

- ディレクトリ・サーバー・プラグインの概要
- 操作ベースのプラグイン
- プラグインの登録

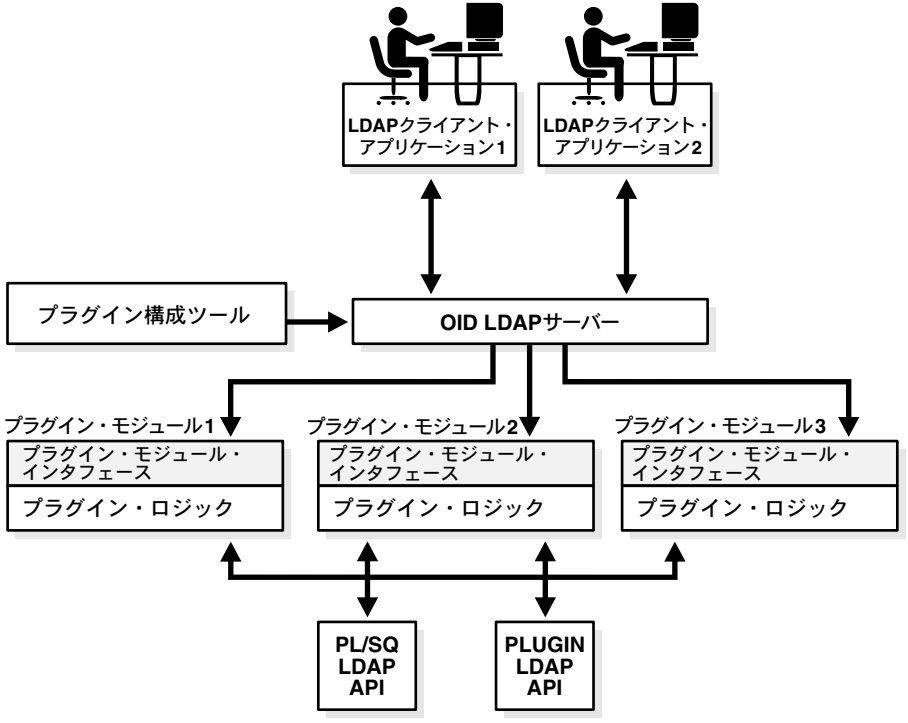
ディレクトリ・サーバー・プラグインの概要

Oracle Internet Directory は、ディレクトリ・サーバー・プラグインの PL/SQL パッケージをサポートしています。様々な機能をディレクトリ・サーバーに追加できます。次に示すのは、一部の機能のみです。

- 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。

図 26-1 Oracle Internet Directory サーバーのプラグイン・フレームワーク



操作ベースのプラグイン

この項では、Oracle Internet Directory のプラグイン・フレームワークがサポートする操作ベースのプラグインについて説明します。操作ベースのプラグインは、通常のディレクトリ・サーバー操作の前後または操作に追加して実行されます。

表 26-1 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みの内容をロールバックしません。
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。

プラグインの登録

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、プラグインのエントリを `cn=plugin,cn=subconfigsubentry` に作成します。

orclPluginConfig オブジェクト・クラス

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。このオブジェクト・クラスは構造化オブジェクト・クラスで、そのスーパー・クラスが最上位です。表 26-2 は、プラグインの属性のリストおよび説明を示しています。

表 26-2 プラグインの属性名と属性値

属性名	属性値	必須	オプション
Cn	プラグイン・エントリ名	○	
orclPluginName	プラグイン・パッケージ名	○	

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。
		○	

orclPluginKind	PL/SQL		○
orclPluginEnable	0 = 使用禁止（デフォルト） 1 = 使用可能		○
orclPluginVersion	サポート対象のプラグイン・バージョン番号		○
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。		○

表 26-2 プラグインの属性名と属性値（続き）

属性名	属性値	必須	オプション

orclPluginLDAPOperation	次のいずれかの値です。
	`ldapcompare`
	`ldapmodify`
	`ldapbind`
	`ldapadd`
	`ldapdelete`
	`ldapsearch`
			○

orclPluginTiming	次のいずれかの値です。
	`pre`
	`when`
	`post`
			○

orclPluginIsReplace	0 = 使用禁止（デフォルト） 1 = 使用可能 操作時タイミングのプラグインの場合のみ		○
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。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。		○

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

プラグインは Oracle Internet Directory サーバーに追加する必要があります。その結果、サーバーは適時に実行する必要がある追加操作を認識できます。

プラグインが Oracle Internet Directory バックエンド・データベースに対して正常にコンパイルされると、新規エントリが作成され、`cn=plugin,cn=subconfigsubentry` に配置されます。

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（`my_ldif_file.ldif`）は、次のとおりです。

例 1: 操作ベースのプラグインのエントリの作成

次の例は、オブジェクトを作成する LDIF ファイルの例です。

```
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: 操作ベースのプラグインのエントリの作成

```
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。

第 VIII 部

Oracle Directory Integration Platform

第 VIII 部では、Oracle Directory Integration 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 Platform の構成方法および使用方法について説明します。第 VIII 部は、次の各章で構成されています。

27

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

この章では、Oracle Directory Integration Platform、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 Platform
- Oracle Directory Integration Platform が必要な理由
- 同期とプロビジョニングおよび両者の相違点
- Oracle Directory Synchronization Service
- Oracle Directory Provisioning Integration Service
- Oracle Directory Integration Server
- ディレクトリ統合ツールキット
- 管理ツールと監視ツール
- 例 : Oracle Directory Integration Platform の配置

Oracle Directory Integration Platform

Oracle Directory Integration 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 と統合できます。このプラットフォームは、Oracle Internet Directory のデータと、アプリケーション固有のディレクトリ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。

たとえば、企業は次のようなニーズを持っています。

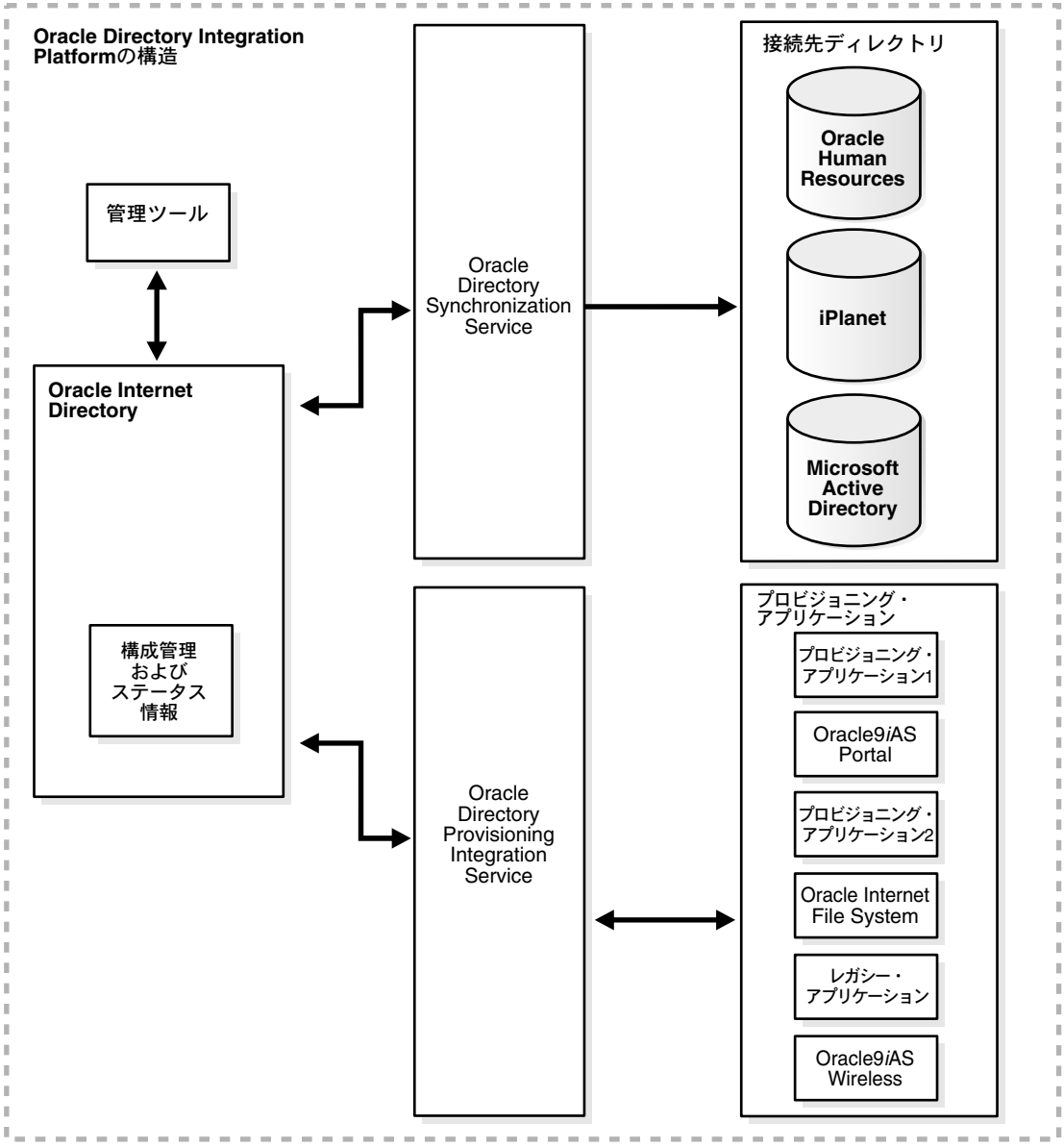
- Oracle Human Resources のデータベースにある従業員レコードと Oracle Internet Directory との同期化。Oracle Directory Integration Platform は、この同期化を提供します。
- 変更が Oracle Internet Directory に適用されるたびに、Oracle9*i*AS Portal などの LDAP 対応アプリケーションに通知されること。Oracle Directory Integration Platform は、これらのアプリケーションにプロビジョニングと呼ばれるサービスを介して通知します。

Oracle Directory Integration Platform は、統合のタイプに応じて 2 つの異なるサービスを提供します。

- Oracle Directory Synchronization Service －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。
- Oracle Directory Provisioning Integration Service －ユーザーのステータスまたは情報の変更を反映するために、定期的にターゲット・アプリケーションに通知を送信します。

27-3 ページの図 27-1 は、Oracle Directory Integration Platform の構造を示しています。

図 27-1 Oracle Directory Integration Platform の構造



Oracle Directory Integration Platform が必要な理由

様々な LDAP 対応のアプリケーションや接続ディレクトリの中央リポジトリとして Oracle Internet Directory を使用することで、管理に必要な時間やリソース・コストを大幅に削減できます。これらの利点を実現するには、接続先エンティティが必要な情報を確実に取得および提供できることが必要です。

次の使用例は、企業でのこれらのニーズの発生と、Oracle Directory Integration Platform を使用してそのニーズに対応する方法を示しています。

- 同期
  - サード・パーティの LDAP ディレクトリに対応するため、Oracle による LDAP 対応アプリケーションの配置を希望する場合があります。しかし、Oracle アプリケーションの実行が保証されるのは、Oracle Internet Directory に対してのみです。したがって、この配置では、Oracle Internet Directory とサード・パーティ・ディレクトリ間でのデータの同期が必要です。
  - メタディレクトリ・ソリューション（企業内の各種リポジトリを Oracle Internet Directory に統合する）の配置を希望するため、同期が必要になる場合があります。
- プロビジョニング
  - Oracle9*i*AS Portal、Oracle Internet File System および Oracle9*i*AS Wireless など、LDAP 対応の Oracle コンポーネントの配置を希望する場合があります。これらのコンポーネントに関するユーザーまたはグループのプロビジョニングは、Oracle Internet Directory に統合されているため、リポジトリ内のユーザーまたはグループの変更は、それらのコンポーネントに通知する必要があります。
  - 中央の Oracle Internet Directory 内のユーザー・エントリまたはグループ・エントリに変更があった場合に、そのことが通知される必要があるカスタム・リレーショナル・アプリケーションを開発および配置している場合があります。この通知の必要性は、Oracle Directory Integration Platform のプロビジョニング統合サービスによって対応できます。

同期とプロビジョニングおよび両者の相違点

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。

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。

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および提供するためには、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。同期の目標は、ユーザーの名前、グループ・メンバーシップまたは権限以外のデータ要素を含むディレクトリ情報について、変更を共有し、一貫性を保持することにあります。

ディレクトリの Oracle Internet Directory への接続を決定した場合は、必ずそのディレクトリに関する同期プロファイルを作成する必要があります。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、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

プロビジョニング統合プロファイルは、アプリケーションのインストール時に作成する必要があります。プロビジョニング・サブスクリプション・ツールを使用すると、必要な情報を指定してプロファイルを作成できます。

同期とプロビジョニングの相違点

プロビジョニングと同期には、表 27-1 のように操作上に重要な相違があります。

表 27-1 ディレクトリ同期とプロビジョニング統合の相違点

サービス	プロビジョニング統合	ディレクトリ同期
アクションの時期	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。	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。
メンテナンス作業	最小限の作業 : インストール時にアプリケーション・エンド・ポイントを登録するのみです。	作業あり : マッピング・ルールとエージェントの設定が必要です。
通信方向	1 方向 : Oracle Internet Directory からプロビジョニング・アプリケーションへ。	2 方向 : Oracle Internet Directory から接続ディレクトリへ、またはその逆。
データの種類	プロビジョニング対象のユーザーとグループに制限。	ディレクトリ内のあらゆるデータ。
例	Oracle9*i*AS Portal	Oracle Human Resources

Oracle Directory Synchronization Service

Oracle Directory Integration Platform 環境における接続ディレクトリは、その内容が Oracle Directory Synchronization Service を介して Oracle Internet Directory と同期化されているディレクトリです。

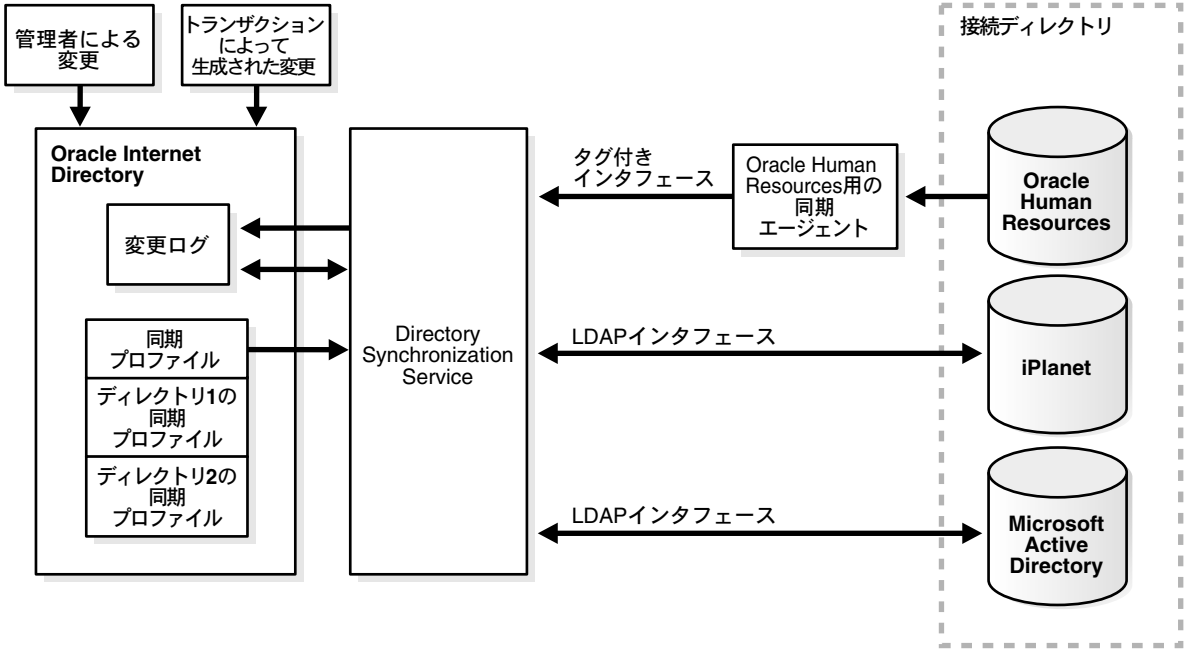
Oracle Internet Directory はすべての情報の中央ディレクトリで、他のすべてのディレクトリと同期しています。この同期には、次の 2 つの方向があります。

- 1 方向 : たとえば、一部の接続ディレクトリ（Oracle Human Resources など）は、変更を Oracle Internet Directory に提供しますが、Oracle Internet Directory から変更を受け取りません。
- 2 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、従業員バッジ番号は、Oracle Human Resources では処理対象ですが、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がなく、同期化する必要はありません。これに対して、従業員識別番号は関係があるため、同期化する必要があります。

Oracle Directory Synchronization Service のコンポーネント間の相互作用は、図 27-2 を参照してください。

図 27-2 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、適切な変更を提供します。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 Exchange または Lotus Notes などが含まれます。Oracle Directory Integration 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 では、ユーザーまたはグループ情報の変更について通知を受ける各アプリケーションに対して、プロビジョニング・プロファイルが必要です。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、グループおよび操作を指定します。

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。

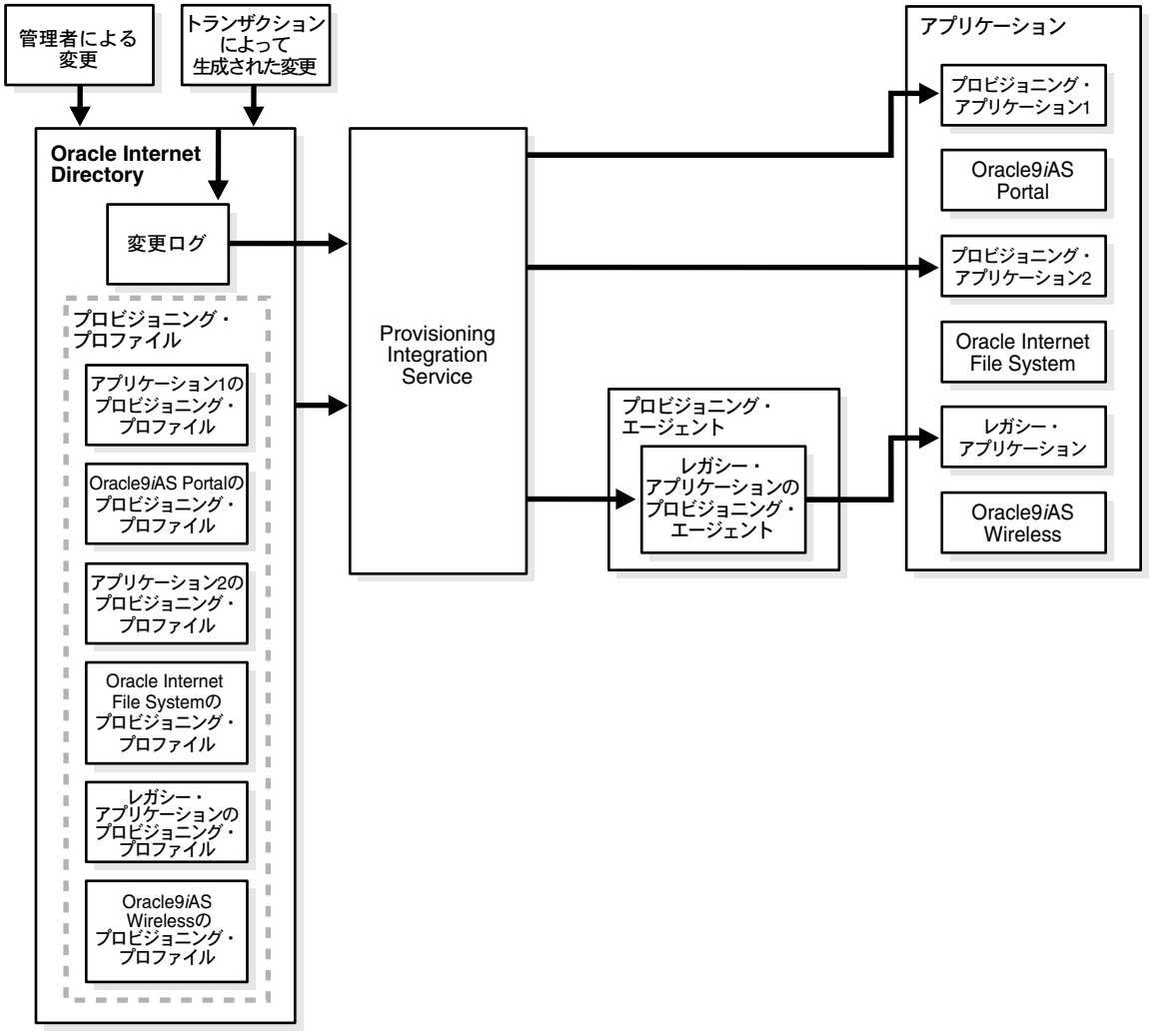
> **関連項目：** プロビジョニング・サブスクリプション・ツールの詳細は、A-53 ページの「プロビジョニング・サブスクリプション・ツール」を参照してください。

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。

レガシー・アプリケーション、つまり、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フォーマットに変換するように、特別に設計および構築する必要があります。

図 27-3 はこれらの相互作用を、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ています。

図 27-3 Oracle Directory Provisioning Integration Service の相互作用



Oracle Directory Integration Server

Oracle Directory Integration 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。Oracle Directory Integration Server では、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データを接続ディレクトリに送信
  - 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 30 章「Oracle Directory Integration 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、自分のソリューションを Oracle Directory Integration 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

  - 次のいずれかを使用してスケジューリングまたはデータ・マッピングを行うために、Oracle Internet Directory のディレクトリ統合コネクタを登録または変更するインタフェース。
    - Oracle Directory Manager
    - 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コマンドライン・ツール
- Oracle Directory Integration 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 ファイルからのデータのバルク・インポート
  - LDIF ファイルへの Oracle Internet Directory 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 によって送信されるイベント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 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
- Oracle Enterprise Manager

Oracle Directory Manager

Oracle Directory Manager は、Java ベースの Graphical User Interface（GUI）を使用したツールで、次の方法で Oracle Directory Integration Platform を管理するために使用します。

- ディレクトリ統合プロファイルの作成、変更および削除
- 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 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 30 章「Oracle Directory Integration 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 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 Server のいずれかがインストールされている *ORACLE_HOME* で、Directory Integration 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 Server を起動します。この構成でも、Oracle Directory Manager を使用して Oracle Directory Integration Server の状態を調べることはできます。

関連項目：

- 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」
- 第 30 章「Oracle Directory Integration Server の管理」

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：

- 『Oracle Enterprise Manager 概説』
- 『Oracle Enterprise Manager 管理者ガイド』
- Oracle Enterprise Manager オンライン・ヘルプ

例 : Oracle Directory Integration 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 Platform によって統合されている配置例を示します。

この項では、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。
- 既存の iPlanet Directory Server。特定のアプリケーションで使用されています。
- Oracle9*i*AS 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 Internet File System リリース 9.2 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

この企業が持つ要件は、次のとおりです。

1. 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。
2. 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。
3. 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。
4. Oracle Human Resources でのユーザーの終了時には、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 27-4 は、様々なコンポーネントとそれらの相互関係を示しています。

図 27-4 MyCompany での Oracle Directory Integration Platform の配置例

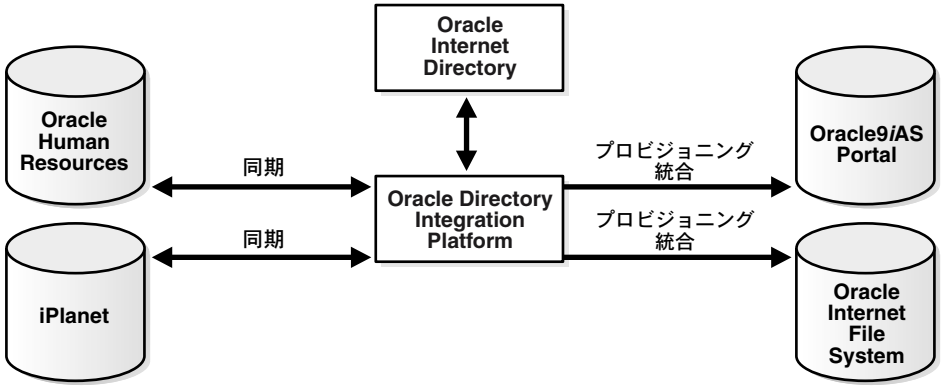


図 27-4 は、次のコンポーネントを示しています。

- Oracle Internet Directory は、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 は、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。
- iPlanet 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。
- Oracle9*i*AS 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 Internet File System。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。新規ユーザー・レコードを企業内の他のすべてのリポジトリに伝播するのは、Oracle Directory Integration Platform のタスクです。

図 27-5 は、Oracle Directory Integration Platform によるこのタスクの完了を補助する、様々な相互作用を示しています。

図 27-5 ユーザーの作成とプロビジョニング

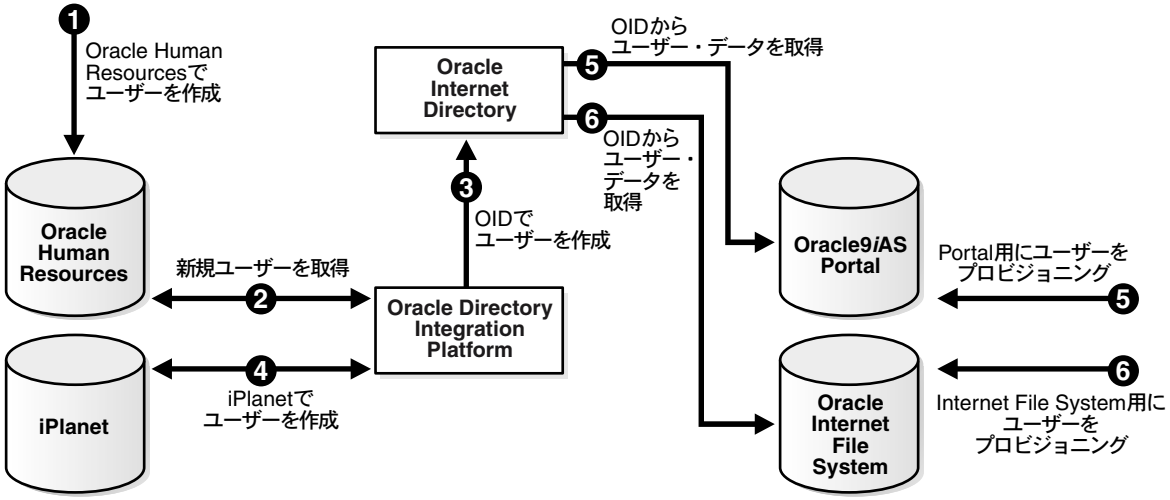


図 27-5 は、Oracle Human Resources での新規ユーザーの作成を示しています。この作成によって、そのユーザーに関するエントリが Oracle Internet Directory と iPlanet Directory Server に作成されます。また、企業内に配置されている 2 つのアプリケーション、つまり Oracle9*i*AS Portal および Oracle Internet File System にアクセスするユーザーのプロビジョニング・プロセスも示しています。ユーザーの作成とプロビジョニングは、次の方法で行われます。

1. Oracle Human Resources 管理者が、ユーザーを Oracle Human Resources データベースに作成します。
2. Oracle Directory Synchronization Service が、ユーザーの新規作成を検出します。
3. 次に、Oracle Directory Synchronization Service は、ユーザーのエントリを Oracle Internet Directory に作成します。
4. Oracle Directory Synchronization Service は、iPlanet 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、Oracle9*i*AS Portal の管理者は、Oracle9*i*AS 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、Oracle9*i*AS 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フェッチします。
6. Oracle Internet File System の管理者もまた、同様のプロセスを使用して、Oracle Internet File System 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 Platform は、新規ユーザーについて Oracle9*i*AS Portal または Oracle Internet File System 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限らないためです。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

この例では、MyCompany という企業では、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 27-6 は、この要件を満たすために Oracle Directory Integration Platform が実行するアクションを示しています。

図 27-6 ユーザー・プロパティの変更

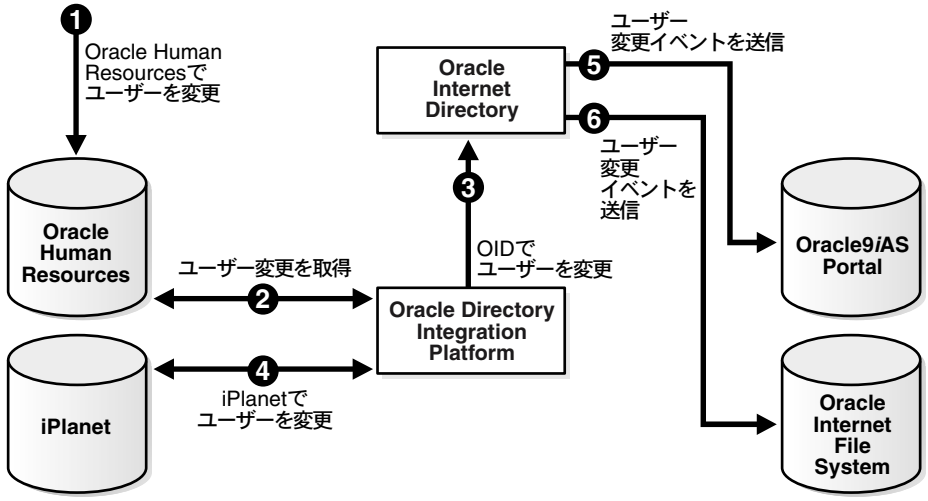


図 27-6 は、Oracle Directory Integration Platform がユーザー・プロパティの変更を企業内の全システムに通信するプロセスを示しています。このプロセスは、次のとおりです。

1. ユーザーは、最初に Oracle Human Resources で変更されます。
2. Oracle Directory Integration 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 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、iPlanet Directory Server 内でユーザーを変更します。
5. Oracle Directory Provisioning Integration Service は、ユーザー・プロパティの変更を Oracle9*i*AS Portal に通知します。
6. Oracle Directory Provisioning Integration Service は、ユーザー・プロパティに関する同じ変更を Oracle Internet File System 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 で削除または終了されたユーザーは、ディレクトリ・サービスに基づいた企業の全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 27-7 は、ユーザーが削除されたときのイベントの流れを示しています。

図 27-7 企業の Human Resources からのユーザーの削除

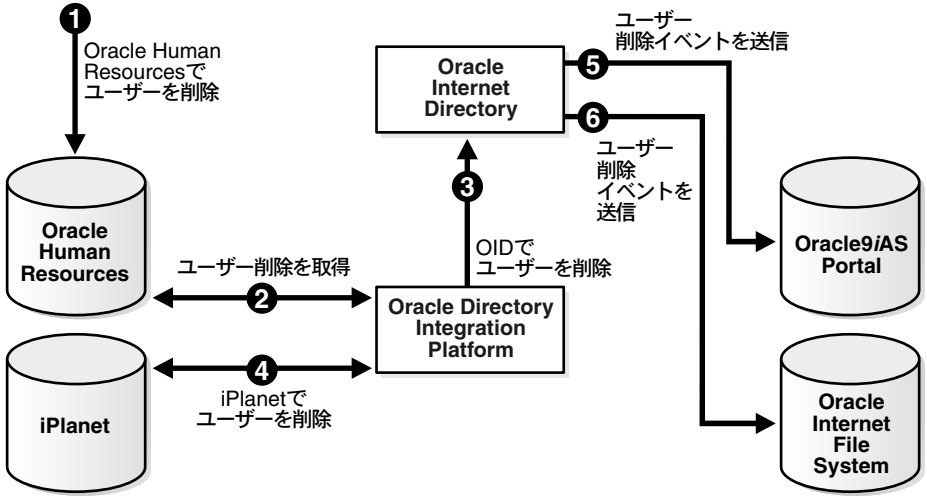


図 27-7 は、Oracle Directory Integration Platform がユーザーの削除を企業内の全システムに通信するプロセスを示しています。このプロセスは、次のとおりです。

1. ユーザーは、最初に Oracle Human Resources で削除されます。
2. Oracle Directory Integration 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 Platform は、Oracle Internet Directory 内の対応するユーザーを削除します。
4. Oracle Directory Synchronization Service は、iPlanet Directory Server 内でユーザーを削除します。
5. Oracle Directory Provisioning Integration Service は、ユーザーの削除を Oracle9*i*AS Portal に通知します。
6. Oracle Directory Provisioning Integration Service は、ユーザーの削除を Oracle Internet File System に通知します。

前述のすべてのステップが終了すると、Oracle Human Resources で削除されたユーザーは、Oracle9*i*AS Portal や Oracle Internet File System にアクセスできなくなります。

28

Oracle Directory Synchronization Service

この章では、同期について説明します。同期では、2 つのタイプの統合プロファイルのうち、ディレクトリ同期プロファイルを使用します。このプロファイルは、Oracle Internet Directory と接続ディレクトリ間での一貫性を維持するために必要な構成情報を提供します。

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
- 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

関連項目： 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と方法を識別します。詳細は、27-8 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。

- コネクタ
- 同期の使用例
- 一意の形式によるディレクトリ
- ディレクトリ同期プロファイル
- コネクタの Oracle Directory Integration Platform への登録
- 追加コネクタ構成情報
- マッピング・ルールとその形式
- ファイルの位置とネーミング

コネクタ

Oracle Directory Integration Platform でのコネクタは、あらかじめパッケージされた、Oracle Internet Directory と接続ディレクトリ間の接続ソリューションを表します。コネクタは、最小限の場合でも、**ディレクトリ統合プロファイル**と呼ばれるコネクタ・プロファイルで構成されます。このプロファイルには、Oracle Internet Directory と接続ディレクトリの同期に必要な構成情報がすべて含まれています。

コネクタとサポート対象インタフェースの使用

接続ディレクトリでデータ交換に Oracle Directory Integration Platform によってサポートされているインタフェースの 1 つを使用できる場合、同期を発生させるためにコネクタに必要となるのはディレクトリ統合プロファイルのみです。その一例が、Oracle Internet Directory に付属する iPlanet コネクタです。Oracle Internet Directory と iPlanet Directory は LDAP インタフェースを使用して同期できるため、iPlanet コネクタはあらかじめパッケージされたディレクトリ統合プロファイルのみで構成されています。

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 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 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。このエージェントは、Oracle Directory Integration Platform がサポートするタグ付きファイル形式を使用して Oracle Internet Directory と通信し、SQL（OCI インタフェースを介して）を使用して Oracle Human Resources システムと通信します。

同期の使用例

同期は、接続ディレクトリから Oracle Internet Directory へ、または Oracle Internet Directory から接続ディレクトリへ（あるいはその両方）の方向で発生する可能性があります。

Oracle Internet Directory から接続ディレクトリへの同期

Oracle Internet Directory に対する各変更では、番号付けされたエントリが変更ログ・コンテナに格納されます。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. 対応する接続ディレクトリの更新で最後に使用した変更ログ・エントリの番号を取得します。
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. プロファイルのフィルタ処理規則を使用して、対応する接続ディレクトリとの同期化が必要な変更を選択します。

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、PL/SQL、LDAP、タグ付きまたは LDIF の各フォーマット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コネクタが起動されます。）正常に使用された最終ログ番号がプロファイルに格納されます。

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、PL/SQL、LDAP、タグ付きまたは LDIF の各フォーマット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。それ以外の場合は、そのディレクトリの同期プロファイルに指定されているコネクタが、変更をエクスポート・ファイルにタグ付きフォーマットまたは LDIF フォーマットで書き込む必要があります。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。

一意の形式によるディレクトリ

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。エージェントと呼ばれるこのプログラムは、接続ディレクトリの特定形式と、同期データが含まれているタグ付きファイルまたは LDIF ファイルとの間で変換を行います。Oracle Directory Synchronization Service は、同期を実行するためにプロファイルに定義されているエージェントを起動します。

このタイプの接続ディレクトリへのインポートのために、Oracle Internet Directory から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 フォーマットで作成します。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。

Oracle Internet Directory へのインポートのために、このタイプの接続ディレクトリからデータをエクスポートする場合、エージェントは、必要なファイルをタグ付き形式または LDIF フォーマットで作成します。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

同期のためのディレクトリ統合プロファイルは、**ディレクトリ同期プロファイル**と呼ばれます。このプロファイルには、次のように、同期に必要な構成情報がすべて含まれています。

- 同期の方向

  構成情報の一部は、同期方向に関連があります。接続ディレクトリには、Oracle Internet Directory との間でデータの受信のみを行うもの、データの送信のみを行うものおよび送受信の両方を行うものがあります。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。

- インタフェース型

  構成情報の他の部分は、使用するインタフェースの型に関連があります。一部の接続ディレクトリは、Oracle Directory Integration 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。これらのインタフェースには、現在、PL/SQL、LDAP、タグ付きおよび LDIF が含まれます。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。

- その他の情報

  ディレクトリ同期プロファイルには、エージェントの名前とタイプ、エージェント起動の方法と時点、同期エントリや属性の同期に必要なマッピング情報などの情報も含まれています。

同期を必要とする変更は、Oracle Internet Directory または接続ディレクトリで発生する可能性があります。Oracle Directory Synchronization Service は、最後に成功した更新時刻と変更番号を変更ログと照合して比較し、各プロファイルを定期的にチェックします。未同期の変更が見つかると、Oracle Directory Synchronization Service は同期を開始します。Oracle Internet Directory に対するインポートとエクスポートは、Oracle Directory Integration Server によって直接処理されます。特定の接続ディレクトリとの同期にエージェントが必要な場合は、必要なエージェントがプロファイルに指定され、自動的に起動されます。

コネクタの Oracle Directory Integration Platform への登録

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。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 またはコマンドライン・ツールのいずれかを使用できます。

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、同期プロファイル・エントリの `orclOdipAgentConfigInfo` 属性に格納できます。

> **関連項目：** `orclOdipAgentConfigInfo` 属性の詳細は、28-9 ページの「追加コネクタ構成情報」を参照してください。

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。唯一の例外は `orcllastappliedchangenumber` 属性で、この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。28-5 ページの表 28-1 に、Oracle Directory Integration Platform のプロファイルのすべての属性を示します。

表 28-1 Oracle Directory Integration Platform の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`）	統合プロファイルの名前。
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。
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 ID に対しても行われます。

表 28-1 Oracle Directory Integration Platform のプロファイルの属性（続き）

属性	説明
同期モード (`orclOdipSynchronizationMode`)	次の 2 つのモードがあります。 ■ インポート。接続ディレクトリの変更が Oracle Internet Directory にインポートされます。 ■ エクスポート。Oracle Internet Directory の変更が抽出され、接続ディレクトリに提供されます。
スケジューリングの間隔 (`orclOdipSchedulingInterval`)	コネクタが同期化を行う間隔。
再試行回数 (`orclodipSyncRetryCount`)	失敗した場合にエージェントまたは同期が試行される最大回数。デフォルトで、Oracle Directory Integration Server は、最大 10 回まで同期を試行します。最初の再試行は最初の失敗の 1 分後に、2 回目の再試行は 2 回目の失敗の 2 分後に、後続の n 回目の再試行は n 回目の失敗の n 分後に行われます。
プロファイル・バージョン (`orclVersion`)	統合プロファイルのバージョンを示す識別子。値は 1.0 です。このフィールドが 1.0 以外の値の場合、プロファイルは処理されません。
実行情報	
エージェント実行コマンド (`orclodipAgentExeCommand`)	Directory Integration 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典型的な使用方法は、第 33 章「Oracle Human Resources との同期化」を参照してください。

表 28-1 Oracle Directory Integration Platform の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（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。たとえば、iPlanet 同期コネクタの場合のユーザー・アカウントは、iPlanet ディレクトリ内の有効なバインド識別名です。Hragent 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 ID 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典型的な使用方法は、第 33 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・アカウントのパスワード（orclOdipConDirAccessPassword）	接続ディレクトリへの接続で、「接続ディレクトリ・アカウント」属性に指定したユーザー ID が使用するパスワード。たとえば、iPlanet 同期コネクタの場合のパスワードは、iPlanet ディレクトリ内の有効なバインド・パスワードです。Hragent の場合は、Oracle Human Resources データベース・パスワードです。
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。iPlanet 同期の場合、このパラメータは `host:port` 形式でホスト名とポート番号を示します。データベースの場合も同様に、`Host:port:oraclesid` 形式でこのパラメータを使用できます。

表 28-1 Oracle Directory Integration Platform のプロファイルの属性（続き）

属性	説明
インタフェース型 (`orclodipDataInterfaceType`)	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 フォーマットと同様に、Oracle Directory Integration Server がサポートする独自の形式です。 **関連項目：**付録 A「LDIF およびコマンドライン・ツールの構文」 ■ 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。
追加構成情報 (`orclOdipAgentConfigInfo`)	コネクタに渡す必要がある追加構成情報。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。
マッピング情報	
マッピング・ルールの属性 (`orclOdipAttributeMappingRules`)	接続ディレクトリから Oracle Internet Directory にデータを変換するためのマッピング・ルール。この情報はバイナリ属性として格納されます。 **関連項目：** ■ 28-10 ページ「マッピング・ルールとその形式」 ■ マッピング・ルールの例は、33-13 ページの「デフォルトの Oracle Human Resources コネクタのマッピング・ルール」を参照してください。
接続ディレクトリ照合フィルタ (`orclOdipConDirMatchingFilter`)	接続ディレクトリに適用するために、Oracle Internet Directory の変更を選択する属性。
OID 照合フィルタ (`orclOdipOIDMatchingFilter`)	Oracle Internet Directory に適用するために、接続ディレクトリの変更を選択する属性。

表 28-1 Oracle Directory Integration Platform のプロファイルの属性（続き）

属性	説明
ステータス情報	
前回実行日時（orclOdipLastExecutionTime）	同期が最後に実行された日時。書式は dd-mon-yyyy hh:mm:ss で、hh は 24 時間書式での時刻です。
前回成功実行日時（orclOdipLastSuccessfulExecutionTime）	同期が最後に正常終了した日時。書式は dd-mon-yyyy hh:mm:ss で、hh は 24 時間書式での時刻です。
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。
同期エラー（orclodipSynchronizationErrors）	前回の実行に失敗した場合のエラーの理由。
接続ディレクトリの前回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。
OID の前回適用された変更番号（orclOdipLastAppliedChgNum）	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。

追加コネクタ構成情報

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 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。この属性の使用はオプションです。コネクタで追加情報が不要な場合、同期プロファイル内の対応する属性は単に空の状態のままです。追加情報を使用する場合は、oidmuplf.sh という名前のスクリプトを使用して、追加情報をこの属性にロードできます。追加構成情報の属性に格納されるデータの型および形式は、各実行可能ファイルのニーズによって異なります。

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 Server は、この情報の読込みも変更も行いません。コネクタの起動時に、Oracle Directory Integration 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。

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 1.0。サイト：`http://sources.redhat.com/cygwin/`
- MKS Toolkit 5.1 または 6.0。
  サイト： `http://www.datafocus.com/products/`

関連項目： これらのファイルの名前については、28-18 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。

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するエンティティです。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 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 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。

マッピング・ルール属性の形式

マッピング・ルール属性は、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する手段を提供します。マッピング・ルールは、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 の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]
srcAttrName2: [ReqAttrSeq]:[SrcAttrType]:
[SrcObjectClass]:[dstAttrName2]:[DstAttrType]:
[DstObjectClass]:[AttrMappingRule2]
###
```

srcAttrName1 と *srcAttrName2* を拡張する場合、それぞれ改行のない長い 1 行に記述されます。

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 28-2 で説明されているコンポーネント（コロン区切り）で表現されます。

表 28-2 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 28-2 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 28-3 で説明されているコンポーネント（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 28-3 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 28-3 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。ソース属性の型と宛先属性の型が等しいかどうかが検証されます。 リリース 9.2 では、このフィールドは無視されます。
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 TableName 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、マッピング・ルールの妥当性をチェックします。ソース属性の型と宛先属性の型が等しいかどうかが検証されます。 リリース 9.2 では、このフィールドは無視されます。
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 TableName 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	演算子の「+」、ファンクションの「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。

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。

例 : マッピング・ファイル

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。このファイルの例は、インストール時に $*ORACLE_HOME*/ldap/odi/conf/oraclehragent.map.master に格納されます。

```
DomainRules
NONLDAP:dc=metaagt,dc=com:uid=%dc=metaagt,dc=com
AttributeRules
firstname: : : :cn: :person
email : : : :cn: :person: trunc(email,'@')
email : : : :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=metaagt,dc=com:cn=%,dc=metaagt,dc=com が含まれています。このルールは、ソース・ドメインがなく、ソース・ドメインが LDAP でないことを示しています。

宛先ドメイン（:dc=metaagt,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=metaagt,dc=com にあることを示しています。

DomainMappingRule（: uid=%,dc=metaagt,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 が単一値の属性であることも必要です。

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=metaagt,dc=com（cn は複数値属性）の識別名を持つエントリを構成する場合、DomainMappingRule は、rdn,l=%,dc=metaagt,dc=com の形式にできます。この場合の rdn は、NULL 以外の値を持つ宛先属性の 1 つです。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=metaagt,dc=com:rdn,l=%,dc=metaagt,dc=com
AttributeRules
firstname: : : :cn: :person
email : : : :cn: :person: trunc(email,'@')
email : : : :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: : : :l: :locality
Title: : : :title: :organizationalperson
#Sex: : : :sex: :person
###
```

この属性マッピング・ルール、firstname: : : :cn: : person には、次の説明が適用されます。

SrcAttrName: firstname （元の属性の名前）

ReqAttrSeq : empty（属性が見つからない場合も、マッピングを続行できます）

SrcAttrType: empty（不要）

SrcObjectClass: empty（不要）

DstAttrName : cn （Oracle Internet Directory で表示する属性の名前）

DstAttrType: empty（不要）

DstObjectClass : person 属性が属しているオブジェクト・クラスで、タグ付きファイル・インタフェースでインポートを使用する場合は必須です。

同様に、ルール `e-mail: : : :cn: : person: trunc(email,'@')` は、`e-mail` の文字をすべて切り捨て、残りの部分を `cn` として取得するマッピング・ルールの適用を示しています。

マッピング・ルールは、新規規則の追加、ファイルの変更による既存規則の変更または削除によって、カスタマイズすることができます。ファイルにマッピング・ルールがない場合は、A-20 ページの「ldapsearch の構文」で説明する ldapsearch を使用して属性値をファイルにダウンロードできます。検索対象エントリは、属性 `orclodipattributemappingrules` の `orclodipagentname=ProfileName,cn=subscriber profile,cn=changelog subscriber,cn=oracle internet directory` です。

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。

> **関連項目：** マッピング・ルールの例は、33-13 ページの「デフォルトの Oracle Human Resources コネクタのマッピング・ルール」を参照してください。

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。一般的に、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-20 ページの「ldapsearch の構文」に説明されている ldapsearch コマンドを使用してファイルの属性値を格納します。

`OrclodipAttributeMappingRules` は、ディレクトリ内の単一値属性で、固定形式に従う必要があります。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、ユーティリティ oidmuplf.sh 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。

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を識別します。
2. マップ先の Oracle Internet Directory で対応する属性名を識別します。
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. oidmuplf.sh ツールを使用して、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。

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。次に、oidmuplf.sh ツールを使用して、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。

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。次に、oidmuplf.sh ツールを使用して、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。

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 1.0。サイト：`http://sources.redhat.com/cygwin/`
- MKS Toolkit 5.1 または 6.0。
  サイト：`http://www.datafocus.com/products/`

ファイルの位置とネーミング

表 28-4 は、様々なファイルの位置と使用する名前を示しています。

表 28-4　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`
トレース・ファイル	`$ORACLE_HOME/ldap/odi/log/`*`Profile_Name`*`.trc`
追加構成情報	`$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 エージェントのデータ・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 を使用したプロファイルの管理
- 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 を使用したプロファイルの管理

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

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」>「*directory server instance*」>「サーバーの管理」の順に展開し、「Directory Integration Server」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。
2. ツールバーの「作成」ボタンをクリックします。「構成設定」ダイアログ・ボックスが表示されます。
3. 「構成設定」ダイアログ・ボックスで、「作成」をクリックします。「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。
   - 既存の統合プロファイルをコピーして統合プロファイルを作成する場合は、コピーする Oracle Directory Integration Platform プロファイルを選択し、「類似項目の作成」をクリックします。「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。
   - 既存の統合プロファイルをコピーせずに統合プロファイルを作成する場合は、「新たに作成」をクリックします。「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。
4. 「一般」タブ・ページで、表 28-5 の説明に従って各フィールドに情報を入力します。

表 28-5 Oracle Directory Manager の「一般」タブ・ページの各フィールドの説明

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、接続ディレクトリから Oracle Internet Directory に変更をプルします。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プッシュします。 このフィールドは必須です。デフォルトは `IMPORT` です。
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「使用可能」です。

表 28-5 Oracle Directory Manager の「一般」タブ・ページの各フィールドの説明（続き）

フィールド	説明
最大試行回数	Directory Integration 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 n 回目の再試行は n 回目の失敗の n 分後に行われます。
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。

5. 「実行」タブを選択し、表 28-6 の説明に従って各フィールドに情報を入力します。

表 28-6 Oracle Directory Manager の「実行」タブの各フィールドの説明

フィールド	説明

エージェント実行コマンド	Directory Integration 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。
	典型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。
	典型的な例は、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。

表 28-6 Oracle Directory Manager の「実行」タブの各フィールドの説明（続き）

フィールド	説明
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 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 ODM 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、oidmuplf.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。
接続されたディレクトリ URL	接続ディレクトリの URL（使用可能な場合）。
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。有効な値は `LDIF`、`DB`、`LDAP` または `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。

6. 「マッピング」タブを選択し、表 28-7 の説明に従って各フィールドに情報を入力します。

表 28-7 Oracle Directory Manager の「マッピング」タブの各フィールドの説明

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 `oidmuplf.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。
OID 一致フィルタ	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。
接続されたディレクトリ一致フィルタ	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。

7. 「ステータス」タブを選択し、表 28-8 の説明に従って各フィールドに情報を入力します。このタブ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。

表 28-8 Oracle Directory Manager の「ステータス」タブの各フィールドの説明

フィールド	説明
OID 前回適用された変更番号	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。
前回変更された適用番号	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。

8. 「統合プロファイル」ダイアログ・ボックスの各タブで、すべての編集を終了後、「OK」をクリックします。「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。

9. 「OK」をクリックして「構成設定」ダイアログ・ボックスを終了します。これで作成したエージェントが 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

コネクタを削除する手順は、次のとおりです。

1. ナビゲータ・ペインで「Oracle Internet Directory サーバー」>「*directory server instance*」>「サーバーの管理」>「Directory Integration Server」の順に展開します。

2. エージェントを削除する「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エージェントを選択し、「削除」をクリックします。

コマンドライン・ツールを使用した同期プロファイルの管理

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。次の項目について説明します。

- oidmcrep.sh を使用した同期プロファイルの作成
- oidmdelp.sh を使用した同期プロファイルの登録解除

oidmcrep.sh を使用した同期プロファイルの作成

コマンドライン・ツールの oidmcrep.sh を使用すると、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-49 ページ「oidmcrep.sh ツール」

oidmdelp.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・ツールの oidmdelp.sh を使用すると、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-51 ページ「oidmdelp.sh ツール」

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 1.0。サイト：`http://sources.redhat.com/cygwin/`
- MKS Toolkit 5.1 または 6.0。
  サイト：`http://www.datafocus.com/products/`

29

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 の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
- アプリケーションが、Oracle Directory Provisioning Integration Service を使用して、プロビジョニング情報を取得する方法

プロビジョニングの概要

プロビジョニングとは、Oracle Internet Directory のユーザー・データまたはグループ・データが変更された場合に、その変更をアプリケーションに通知するプロセスです。関連するユーザーまたはグループのステータスや情報に変更が発生した場合は、常にプロビジョニング・イベントが発生します。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、最初のインストール時に、プロビジョニングをサブスクライブします。サブスクリプションは、アプリケーションごとに発生します。

プロビジョニングは同期に関連がありますが、同期化と同じではありません。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。しかし、この場合、アプリケーションのプロビジョニングで受信できるのは、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通知のみです。

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のユーザーの作成
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。

ユーザーとグループの情報は、次のいずれからでも変更できます。

- Oracle Human Resources または Oracle Directory Integration 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 この例は、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。Oracle9*i*AS 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 アプリケーション固有の管理ツールを使用して、管理者が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 ID、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、ユーザーとグループ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、ユーザーまたはグループの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。たとえば、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。

Oracle Directory Provisioning Integration Service 環境でのコンポーネント間の関係は、図 29-1 を参照してください。

図 29-1 Oracle Directory Provisioning Integration Service 環境の典型的な配置

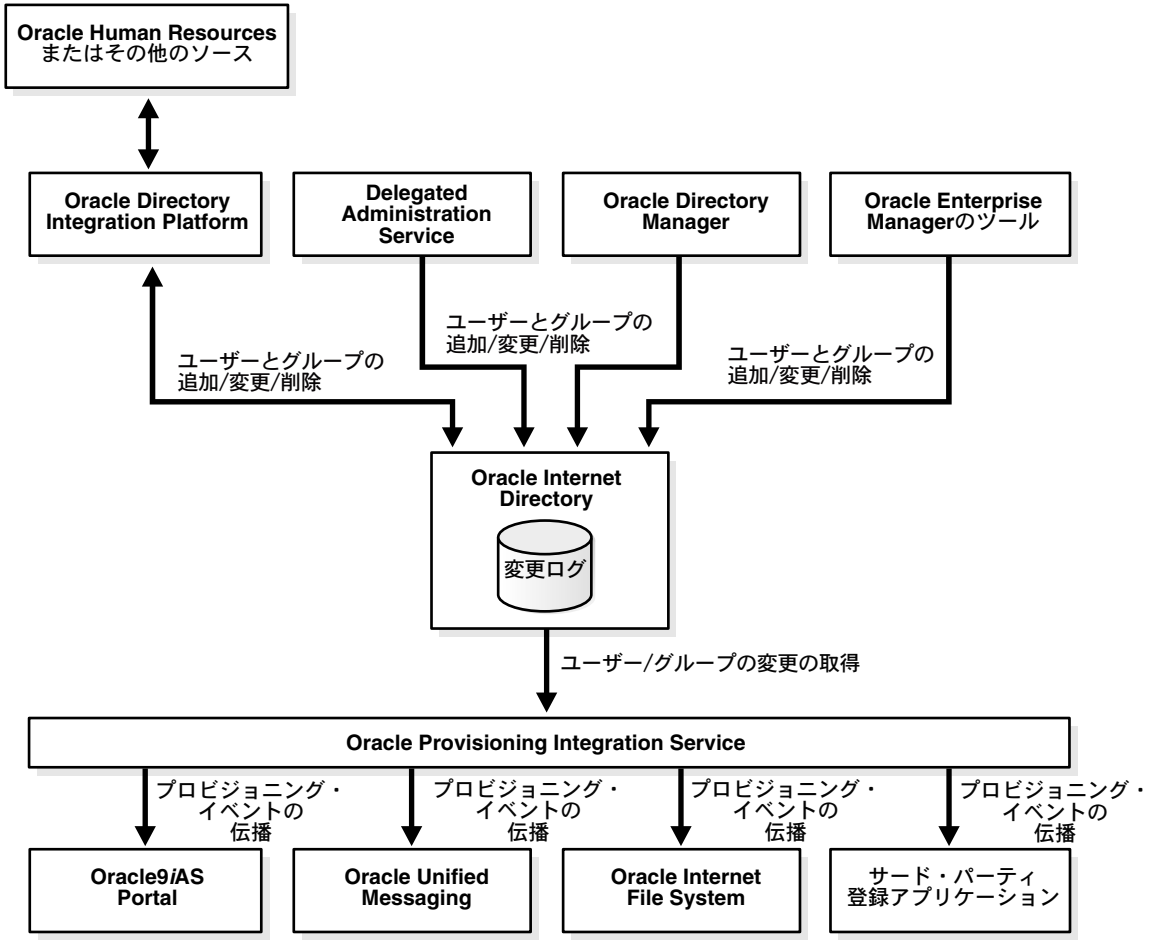


図 29-1 が示している内容は、次のとおりです。

- Oracle Internet Directory は、ユーザーとグループ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 内のユーザーとグループのエントリを追加、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 Platform
  - Delegated Administration Service
  - Oracle Directory Manager
  - Oracle Enterprise Manager のツール（Enterprise Security Manager など）

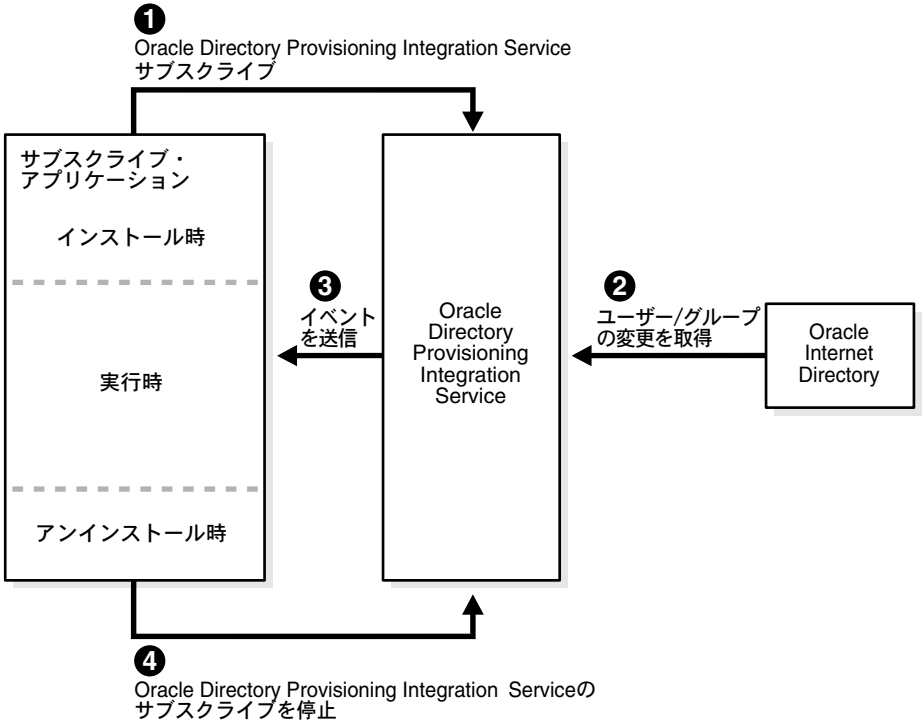
  Oracle Internet Directory の変更ログには、これらの変更が記録されます。
- Oracle Directory Provisioning Integration Service は、ユーザーとグループの情報への変更を Oracle Internet Directory から取得し、サブスクライブ・アプリケーションに送信します。この図にあるアプリケーションは、Oracle9*i*AS Portal、Oracle Unified Messaging、Oracle Internet File System およびサード・パーティ登録アプリケーションです。

アプリケーションが、Oracle Directory Provisioning Integration Service を使用して、プロビジョニング情報を取得する方法

Oracle Directory Provisioning Integration Service は、ユーザーまたはグループ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 29-2 は、プロビジョニング・イベントを取得するアプリケーションのライフ・サイクルを示しています。

図 29-2 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取得する方法



1. Oracle Directory Provisioning Integration Service のサブスクリプションは、次の 2 つのいずれかの方法で行われます。

   - 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サブスクライブする。
   - 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、手動でサブスクライブする。

   プロビジョニング・サブスクリプション・ツール `oidprovtool` は、いずれの *ORACLE_HOME*/`bin` からも起動されます。このツールを起動する一般的なパターンは、次のとおりです。

   ```
   oidprovtool param1=p1_value param2=p2_value param3=p3_value ...
   ```

   関連項目： プロビジョニング・サブスクリプション・ツールのパラメータと可能な値の詳細は、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。

2. 次に、このツールは、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次の情報を要求します。
   - 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）

   Oracle Internet Directory に必要な構成情報が揃うと、Oracle Directory Provisioning Integration Service は、変更をアプリケーションに対して定期的に送信します。送信する変更は、アプリケーション固有のデータベース接続情報に従います。
3. Oracle Directory Provisioning Integration Service からのアンインストールは、次の 2 つのいずれかの方法で行います。
   - アプリケーション自体が自動的にアンインストール
   - 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サブスクライブを停止

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 の管理

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 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. 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。
3. 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。

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 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 Server の管理

Oracle Directory Integration 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 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 Server の管理方法は、30-7 ページの「Oracle Directory Integration 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、使用可能な状態に設定されるため、Oracle Directory Integration Platform で処理することができます。
- 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・プロファイルの監視には、Oracle Enterprise Manager 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-53 ページ「プロビジョニング・サブスクリプション・ツール」
- 『Oracle Enterprise Manager 概説』
- 『Oracle Enterprise Manager 管理者ガイド』
- 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および様々な操作の完了に必要なディレクトリ権限に関係する主要なエンティティ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。アプリケーションをプロビジョニングできる担当者の数は制限してください。

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 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 ID 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 29-1 は、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ています。

表 29-1 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 Server	はい	いいえ	はい	Oracle Directory Integration 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 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 ID があります。リリース 9.2 の場合、この ID 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
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 29-2 にその属性を示します。

表 29-2 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 29-3 は、保護属性のアクセス制御を示しています。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 29-3 保護属性のアクセス制御

ユーザー・カテゴリ	読込み	書込み	検索	比較	説明
Oracle Directory Integration Server	はい	いいえ	はい	はい	Oracle Directory Integration 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 29-3 保護属性のアクセス制御（続き）

ユーザー・カテゴリ	読込み	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、必要な権限は読込み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 29-4 は、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ています。

表 29-4 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	読込み	書込み	検索	比較
Oracle Directory Integration 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 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 の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・メッセージをリストし、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 29-5 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 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・サーバーの接続に関する情報は、5-35 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 Server エントリを確認してください。`odisrvreg` を使用して Oracle Directory Integration Server を再登録します。 **関連項目：**30-2 ページ「Oracle Directory Integration Server の登録」
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。	$*ORACLE_HOME*/ldap/odi/log/PROFILE_NAME.trc のトレース・ファイルでスタック・トレースを調査してください。
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。	$*ORACLE_HOME*/ldap/odi/log/PROFILE_NAME.trc のトレース・ファイルでスタック・トレースを調査してください。
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。

30

Oracle Directory Integration Server の管理

この章では、Oracle Directory Integration Server について説明し、その構成方法と管理方法を示します。次の項目について説明します。

- Oracle Directory Integration Server の概要
- Oracle Directory Integration Server の登録
- Oracle Directory Integration Server の操作情報
- Oracle Directory Integration Server の管理
- Oracle Directory Integration Server の情報の表示
- レプリケート環境での Oracle Directory Integration Platform の管理

Oracle Directory Integration Server の概要

Oracle Directory Integration Server は、Oracle Directory Integration Platform の中心的なコンポーネントです。このコンポーネントは、次のことを行うサーバー・プロセスです。

- コネクタのスケジューリング

  Directory Integration 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、その実行時期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 Server は、変更の Oracle Internet Directory へのインポートおよび Oracle Internet Directory からのエクスポートを行います。LDIF、LDAP 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 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 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。

複数の Directory Integration Server のインスタンスをホスト上で実行できます。

Oracle Directory Integration Server の登録

Oracle Directory Integration Platform を実行するノードを認証するには、Directory Integration Server をインストールして、Oracle Internet Directory に登録します。この登録には、Oracle Directory Integration Server の登録ツール（`odisrvreg`）を使用します。異なるホストにインストールされている各 Directory Integration Server は、そのホストの `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、Oracle Internet Directory 管理者の権限が必要です。

このツールでは、登録処理の一部としてディレクトリにエントリが作成され、Directory Integration 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リセットできます。また、`odisrvreg` ツールは、`$ORACLE_HOME/ldap/odi/conf` に `odisrvwallet` と呼ばれるローカル・ファイルを作成します。このファイルは、Directory Integration Server のプライベート Wallet として機能し、Directory Integration 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 30-1 は、`odisrvreg` で使用するパラメータを示しています。`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 30-1 に示します。

Directory Integration Server を非 SSL モードで登録するには、次のコマンドを入力します。

```
odisrvreg -h hostname -p port -D binddn  -w bindpasswd
```

表 30-1 ODISRVREG の引数の説明

引数	説明
-h *hostname*	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。バインド識別名が、Directory Integration Server の登録エントリを作成するには認可が必要です。
-w *bindpasswd*	バインド・パスワード。
-U *ssl mode*	SSL モード。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*	SSL Wallet。SSL Wallet ファイルのフルパス名を入力します。この Wallet は、Oracle Wallet Manager の「Wallet のエクスポート」オプションを使用して作成するテキスト Wallet です。 UNIX の場合、パス名は次のようになります。 /home/my_dir/my_wallet.dat Windows NT の場合は、次のようになります。 C:¥my_dir¥my_wallet.dat **関連項目：**Oracle Wallet Manager の使用方法は、『Oracle Advanced Security 管理者ガイド』を参照してください。
-P *wallet_password*	SSL Wallet をオープンするためのパスワード。

Oracle Directory Integration Server を SSL モードで登録（つまり、登録ツールを SSL モードで実行）するには、次のコマンドを入力します。

```
odisrvreg -h hostname -p port -D binddn  -w bindpasswd
-U ssl_mode -W wallet -P wallet_password
```

この例にある -U、-W および -P パラメータは、わかりやすいように別の行に記述されていますが、実際には他のパラメータと同様に同じコマンドラインで使用します。

Oracle Directory Integration Server の操作情報

この項では、Directory Integration Server に関する構造上および操作上の情報を紹介します。次の項目について説明します。

- Oracle Directory Integration Server と構成設定エントリ
- Directory Integration Server イベントの標準の順序
- 構成設定エントリの管理

Oracle Directory Integration Server と構成設定エントリ

各 Directory Integration Server は、Oracle Internet Directory と接続ディレクトリの間の同期をサポートする一連の接続を実行できます。一連のコネクタによって、Directory Integration Server はこれらの接続をサポートできます。構成設定エントリには、この一連のコネクタがリストされ、コマンドライン引数の 1 つとしてサーバーに渡されます。

コネクタによる同期がスケジューリングされている場合は、常に Directory Integration Server によって別のスレッドが起動されます。このスレッドはディレクトリ・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。

サーバーには、プロセス中に実行する 3 つのタイプのスレッドがあります。

表 30-2 Oracle Directory Integration Server のスレッド

スレッド	説明
メイン・スレッド	Oracle Directory Integration 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リフレッシュ・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リフレッシュします。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	同期用のコネクタを、スケジューリング間隔に基づいてスケジューリングします。メイン・スレッドからリフレッシュ・シグナルを受信したスケジューラ・スレッドは、同期プロファイルを最新の値にリフレッシュします。
コネクタ・スレッド	各スケジューラのスケジューリング間隔によって起動されます。起動時に、コネクタ・スレッドは、プロファイルに指定されているコネクタ実行可能ファイルを起動し、属性のマッピングとフィルタ処理を実行します。同期サイクルが終了すると、コネクタ・スレッドも終了します。

統合プロファイルが構成設定にリストされていない場合、Oracle Directory Integration 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、構成設定に構成されている統合プロファイルが、すべて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された構成設定がディレクトリ内に存在しない場合、Oracle Directory Integration Server はこの情報をログ・ファイルに記録して終了します。

構成設定が未指定の場合は、構成設定 0（ゼロ）が使用され、すべてのプロビジョニング・プロファイルがスケジューリングの対象となります。

関連項目：

- 構成設定エントリの詳細は、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。
- ディレクトリ統合エージェントを使用可能および使用禁止にする方法は、第 28 章「Oracle Directory Synchronization Service」を参照してください。
- デバッグ・レベルの詳細は、30-13 ページの「デバッグ・レベルの設定」を参照してください。

Directory Integration Server イベントの標準の順序

Oracle Directory Integration Server の特定の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 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。

30-4 ページの表 30-2 で説明した 3 つのスレッドは相互に機能して、これらの典型的なプロセス・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
- 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。このメイン・スレッド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。インスタンスが未登録の場合（つまり、OID モニターでインスタンスが起動されない場合）は、構成設定番号とインスタンス番号の詳細の自己登録が Oracle Internet Directory 内で実行されます。

メイン・スレッドはリフレッシュ時期を定期的にチェックし、リフレッシュ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、構成設定を読み込み、スケジューリングを行う統合プロファイルを検索します。スケジューリング対象プロファイルのリストを作成し、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。

リフレッシュ・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リフレッシュします。

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。

コネクタ・スレッド・プロセスの順序

初期化の一部として、コネクタ・スレッドは Oracle Internet Directory と接続ディレクトリとの接続を確立します。データ・インタフェース型が LDIF または TAGGED の場合は、適切なファイルがオープンします。コネクタ・スレッドの動作順序は、次のとおりです。

- ソースから 1 つずつ変更を読み込みます。
- 適用可能な場合、変更をフィルタ処理します。
- マッピング・ルールの指定に従って変更をマップします。
- 宛先変更レコードを作成します。
- 変更を宛先に書き込みます。

すべての変更を適用した後、スケジューラに戻ります。

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。

構成設定では、Directory Integration Server が実行する統合プロファイルがすべてリストされるのみでなく、同期化のためにホストが統合プロファイルに関連付けられます。コネクタが登録されると、統合プロファイルが作成され、構成設定に追加されます。構成設定エントリは、Directory Integration Server の動作を決定します。

Directory Integration 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り、Directory Integration 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 Server のインスタンス 1 を `configset1` とともに起動し、ホスト H1 の Directory Integration Server のインスタンス 2 を `configset2` とともに起動することができます。Directory Integration Server のインスタンス 1 の動作は configset1 に依存し、インスタンス 1 の動作は configset2 に依存します。ホスト H1 の異なるエージェントを 2 つの構成設定エントリに分割することにより、エージェントを実行する負荷を 2 つの Directory Integration Server インスタンスに分割できます。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ことは、サーバー間の負荷の均衡化に役立ちます。

Oracle Directory Integration 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 Server の起動
- Oracle Directory Integration Server の停止
- restart コマンドの使用
- デバッグ・レベルの設定
- ログ・ファイルの検索
- 同期ステータス属性の変更

Oracle Directory Integration Server の起動

Oracle Directory Integration 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 Server の起動方法は、**OID モニター**および **OID 制御ユーティリティ**がインストールされているかどうかにより異なります。これらのツールは、他のサーバーやクライアントのコンポーネントとともに、標準的なサーバー・インストールの一部です。この場合は、これらのツールを使用して Directory Integration Server を起動します。

注意： Directory Integration 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。これにより、Directory Integration Server が突然終了した場合、OID モニターを使用して再起動できます。

クライアントのみのインストールの場合は、OID モニターと OID 制御ユーティリティはインストールされません。この場合は、コマンドラインから Directory Integration Server を起動します。

ディレクトリ・サーバーは、非 SSL モードでも、厳重なセキュリティの SSL モードでも起動できます。30-4 ページの表 30-3 は、各タイプで起動するためのパラメータを示しています。

注意： Oracle Directory Integration 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 モニターと制御ユーティリティを使用した Oracle Directory Integration Server の起動

Directory Integration 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、3-2 ページの「タスク 1: OID モニターの開始」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、OID 制御ユーティリティを使用して Directory Integration Server を起動します。

   ```
   oidctl [connect=net_service_name] server=odisrv [instance=instance_number]
   [config=configuration_set_number] [flags="[host=hostname] [port=port_number]
   [debug=debug_level] [refresh=interval_between_refresh]
   [maxprofiles=number_of_profiles] "] start
   ```

   表 30-3 は、このコマンドの引数の説明です。

表 30-3 Oracle Directory Integration Server を起動するための引数の説明

引数	説明
connect=*net_service_name*	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 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 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 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、30-13 ページの表 30-4 を参照してください。
refresh=*interval_between_refresh*	サーバーが統合プロファイルの変更をリフレッシュ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。
sslauth=*ssl_mode*	SSL モード（0: 認証なし、1: サーバー認証）

表 30-3 Oracle Directory Integration Server を起動するための引数の説明（続き）

引数	説明

`wloc=wallet`	SSL Wallet。SSL Wallet ファイルのフルパス名を入力します。この Wallet は、Oracle Wallet Manager の「Wallet のエクスポート」オプションを使用して作成するテキスト Wallet です。
	UNIX の場合、パス名は次のようになります。
	`/home/my_dir/my_wallet.dat`
	Windows NT の場合は、次のようになります。
	`C:¥my_dir¥my_wallet.dat`
	関連項目：Oracle Wallet Manager の使用方法は、『Oracle Advanced Security 管理者ガイド』を参照してください。

`wpass=wallet_password`	SSL Wallet をオープンするために使用されるパスワード。

ディレクトリ・サーバーを SSL モードで起動するには、次のコマンドを使用します。

```
oidctl [connect=net_service_name] server=odisrv [instance=instance_number]
[config=configuration_set_number] [flags="[host=hostname] [port=port_number]
[debug=debug_level] [refresh=interval_between_refresh] [maxprofiles=number_of_
profiles]
[ sslauth=ssl_mode ] [ wloc=wallet ] [ wpass=wallet_password] "] start
```

このように、唯一の違いは、次の SSL 関連フラグの使用にあります。

```
sslauth=ssl_mode, wloc=wallet, and wpass=wallet_password
```

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 Server の起動

ディレクトリ・サーバーは、非 SSL モードまたは厳重なセキュリティの SSL モードで、OID モニターまたは 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。各タイプで起動するためのパラメータは、表 30-3 に記載されているとおりです。

Directory Integration Server を非 SSL モードで起動するには、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]
```

Directory Integration Server を SSL モードで起動するには、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] [refresh=interval_between_refresh]
[maxprofiles=number_of_profiles] [sslauth=ssl_mode] [wloc=wallet] [wpass=wallet_
password]
```

ここでも、唯一の違いは、次の SSL 関連フラグの使用にあります。

```
[sslauth=ssl_mode] [wloc=wallet] [wpass=wallet_password]
```

Oracle Directory Integration Server の停止

Directory Integration Server は、起動時に使用した同じツールを使用して（つまり、OID モニターと OID 制御ユーティリティを使用するか、odisrv を使用して）停止します。

OID モニターと OID 制御ユーティリティを使用した Oracle Directory Integration 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 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 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、3-2 ページの「タスク 1: OID モニターの開始」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 Server を停止できます。

   ```
   oidctl [connect=net_service_name] 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 Directory Integration Server の停止

OID モニターと OID 制御ツールが利用できない、クライアントのみのインストールの場合は、OID 制御ツールなしで Oracle Directory Integration Server を起動できます。これらのツールなしで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 `stopodis.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 1.0。サイト：`http://sources.redhat.com/cygwin/`
- MKS Toolkit 5.1 または 6.0。
  サイト：`http://www.datafocus.com/products/`

関連項目： stopodis.sh ツールの使用方法は、A-51 ページの「stopodis.sh ツール」を参照してください。

注意： 前述以外の方法で Oracle Directory Integration Server を停止した場合、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/stopodis.sh [-host *directory_server_host*] [-port *directory_server_port*] [-binddn *super_user_dN*（デフォルトは cn=orcladmin）] [-bindpass *super_user_password*（デフォルトは welcome）] -instance *number_of_the_instance_to_stop* **-clean**

---

restart コマンドの使用

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 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。予定のリフレッシュ時刻を待たず、サーバーのキャッシュを即時にリフレッシュする場合は、この方法が便利です。Directory Integration Server が再起動するときは、停止前と同じパラメータが維持されます。

Directory Integration Server を再起動する手順は、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、3-2 ページの「タスク 1: OID モニターの開始」の説明に従って OID モニターを起動します。

2. コマンドラインで次のように入力します。

   ```
   oidctl [connect=net_service_name] server=odisrv instance=instance_number restart
   ```

デバッグ・レベルの設定

ログ・ファイルにリストするサーバーとプロファイルのイベントの種類を指定するには、debug フラグを使用します。

複数のタイプのデバッグを指定する手順は、次のとおりです。

1. 30-13 ページの表 30-4 に示される、個々のタイプの数値を加算します。
2. コマンドラインで、合計値を指定します。たとえば、次のコマンドでは、デバッグ・レベルが 484 に設定されます。

```
oidctl server=odisrv flags="debug=7" start
```

様々なデバッグ・イベントのタイプを表 30-4 および表 30-5 にリストします。

表 30-4 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（サーバー・デバッグ）	数値
異なるスレッドの起動と停止	1
詳細レベル（リフレッシュの詳細を表示）	2

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・ファイルの各トレース文には、次の情報が格納されます。

- タイムスタンプ
- スレッドタイプ
- プロファイル名

トレース文には、次の種類があります。

- 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 30-5 プロファイル・デバッグ用デバッグ・タイプ

デバッグ・イベント・タイプ（プロファイル）	数値
スレッドの起動と停止	1
初期化、実行および終了の詳細	2
実行時の詳細	4
変更レコード	8
マッピングの詳細	16

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、前述の表のデバッグ・イベントは記録されません。ただし、エラーと例外は常に記録されます。

ログ・ファイルの検索

ログ・ファイルは、$*ORACLE_HOME*/ldap/log/odisrv_*instance_number*.log ディレクトリにあります。

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。

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。

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 を絶えず更新します。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 から手動で変更する手順は、次のとおりです。

1. Oracle Directory Manager を使用して、エージェントを使用禁止にします。
2. 属性変更を行います。
3. 変更後、エージェントを再度使用可能にします。

Oracle Directory Integration Server の情報の表示

Directory Integration 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 Server のインスタンス番号。
- 実行されているホスト。
- Directory Integration Server の起動に使用された構成設定。
- 構成設定リフレッシュ・フラグの状態。このフラグは、ディレクトリ統合プロファイルに変更がありリフレッシュが必要になるたびに、Directory Integration Server を示します。

この Directory Integration Server に関する情報は、Oracle Directory Manager または ldapsearch を使用して表示できます。

Oracle Directory Manager を使用した Oracle Directory Integration Server の実行時情報の表示

Oracle Directory Manager を使用して Directory Integration 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」>「*directory server instance*」>「サーバーの管理」の順に展開し、「Directory Integration Server」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。
2. 「プロパティの表示」をクリックします。「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 Server の実行時情報の表示

ldapsearch を使用して Directory Integration 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。次のようなコマンドを実行します。

```
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=subregistrysubentry
cn: instance1
orcldiaconfigdns: "orclDIAName=HR,cn=subscriber profile,cn=changelog subscriber,
cn=oracle internet directory"
orcldiaconfigrefreshflag: 0
orclhostname: my_host
orclconfigsetnumber: 1
objectclass: top
objectclass: orclDIA
```

レプリケート環境での Oracle Directory Integration Platform の管理

複数のノードを持つレプリケート環境で Oracle Directory Integration Platform を使用する場合は、DSE ルートの `orcldiprepository` 属性を 1 に設定します。この設定によって、ディレクトリ・サーバーは、他の Oracle Internet Directory ノードでの変更に関する変更ログ・エントリを生成します デフォルトでは、ディレクトリ・サーバーはこれらの変更ログ・エントリを生成しません。変更ログ・エントリは、ディレクトリ・データをサード・パーティのディレクトリやメタディレクトリと同期させるために必要です。

31

Oracle Directory Integration Platform におけるセキュリティ

この章では、Oracle Directory Integration Platform におけるセキュリティの最も重要な面について説明します。次の項目について説明します。

- 認証
- アクセス制御と認可
- データ整合性
- データ・プライバシ
- ツールのセキュリティ

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 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 Platform
- Oracle Directory Integration Server の認証
- プロファイルの認証

Secure Sockets Layer（SSL）と Oracle Directory Integration Platform

Oracle Directory Integration Platform は、**Secure Sockets Layer（SSL）**を使用してもしなくても配置できます。SSL の実装は、次のモードをサポートします。

- 認証なしーデータの SSL 暗号化を提供しますが、認証には SSL を使用しません。
- SSL サーバー認証ーデータの 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 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 Server です。

  サーバーは、信頼できる**認証局（CA）**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 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 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 Server の認証

Directory Integration 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 Server を装う、あるい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 Server が正しく識別されていることを確認する。
- Directory Integration 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 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 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 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 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。この Wallet の名前は `odisrvwallet` で、`$ORACLE_HOME/ldap/odi/conf` ディレクトリに格納されます。

Directory Integration 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 Server の登録方法は、30-2 ページの「Oracle Directory Integration Server の登録」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 Server の両方を SSL サーバー認証モードで起動します。ディレクトリ・サーバーは自身の証明書を Directory Integration Server に提供し、Directory Integration Server は Oracle Internet Directory のクライアントとして機能します。

Directory Integration 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。

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。この情報は、エージェントの統合プロファイルに格納されます。不正アクセスからプロファイルを保護するには、適切なアクセス制御ポリシー・ポイントをディレクトリに確立します。このポリシーによって、Oracle Internet Directory 管理者が指定した統合プラットフォームの管理者やユーザーのみが統合プロファイルを作成できるようにします。

Directory Integration Server が統合プロファイルに基づいてデータを Oracle Internet Directory にインポートする場合は、その統合プロファイルとしてディレクトリにバインドし、そのプロファイル名とパスワードを使用します。Oracle Directory Integration Platform は、このメカニズムを SSL モードと非 SSL モードの両方のエージェントの認証に使用します。

アクセス制御と認可

認可は、ユーザーが権限を持つ情報のみを読込みまたは更新する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 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 Server に対するアクセス制御
- エージェントに対するアクセス制御

Oracle Directory Integration Server に対するアクセス制御

Directory Integration 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ときは、Directory Integration 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 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。
- Directory Integration Server がエージェントのかわりに操作を行うときは、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 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 Server に付与されるアクセス権を設定し管理するため、Oracle Directory Integration 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 Server は、登録時にこのグループのメンバーになります。

Directory Integration 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・ポイントを設定します。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 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 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 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・ポイントを設定します。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：

- 7-8 ページ「Oracle Directory Manager を使用したグループ・エントリの追加」
- グループ・エントリのアクセス制御ポリシー・ポイントの設定方法は、12-3 ページの「アクセス制御グループ」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。クライアント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。

データ整合性

Oracle Directory Integration 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・プライバシ

Oracle Directory Integration 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 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。

ツールのセキュリティ

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 Server 登録ツール（odisrvreg）－ Directory Integration Server をディレクトリに登録するために使用します。
- ldapadd ツールおよび ldapmodify ツール － コマンドラインからエントリを追加または変更するために使用します。

32

Oracle Directory Integration 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、次の項目について説明します。

- 接続ディレクトリからの Oracle Internet Directory のブートストラップ
- Oracle Internet Directory からの接続ディレクトリのブートストラップ

注意： この章のブートストラップの手順では、接続ディレクトリと Oracle Internet Directory の間の同期化に、接続ディレクトリの統合プロファイルが使用できることを前提にしています。これらの手順は、あるディレクトリから他のディレクトリへの、データの初期同期または移植のためにのみ有効です。

接続ディレクトリからの Oracle Internet Directory のブートストラップ

接続ディレクトリが現実のソースである場合のブートストラップには、接続ディレクトリから Oracle Internet Directory へのデータの移行が含まれます。この場合のブートストラップは、次の方法のいずれかを使用して行います。

- 外部ツールを使用した Oracle Internet Directory へのデータ・インポート
- コネクタの設定による Oracle Internet Directory へのデータ・インポート

Oracle Internet Directory のブートストラップ元になるディレクトリも Oracle Directory Integration Platform 環境の一部になる場合は、この章の手順に従って初期ブートストラップを実行します。たとえば、Oracle HR の場合などがこれに該当します。

外部ツールを使用した Oracle Internet Directory へのデータ・インポート

1. 接続ディレクトリを読取り専用モードに設定し、すべての更新を禁止します。
2. LDIF ファイル形式または LDIF テンプレート形式で接続ディレクトリからデータをダンプします。
3. データが LDIF フォーマットの場合は、bulkload ツールを使用してデータを Oracle Internet Directory にアップロードします。
4. コピーの完了と検証後に、接続ディレクトリの設定を更新モードに戻します。

関連項目： コマンドライン・ツールの使用方法は、A-11 ページの「エントリ管理コマンドライン・ツール」を参照してください。

コネクタの設定による Oracle Internet Directory へのデータ・インポート

この方法では、コネクタは、接続ディレクトリがその変更を識別する方法に従って、タイムスタンプ（`orclOdipLastSuccessfulExecutionTime` 属性）または前回適用された変更番号（`orclOdipConDirLastAppliedChgNum`）に基づいて接続ディレクトリから変更をプルします。データは、次の順序で Oracle Internet Directory にブートストラップできます。

1. 接続ディレクトリを読取り専用モードに設定し、すべての更新を禁止します。
2. Oracle Directory Manager を使用して、接続ディレクトリのエージェントを Oracle Directory Integration Platform に登録します。

   関連項目： 30-2 ページ「Oracle Directory Integration Server の登録」

3. Directory Integration Server は、スケジューリングの間隔に基づいてインポート操作を開始します。同期の完了を待機します。
4. 同期の完了と検証後に、接続ディレクトリの設定を更新モードに戻します。

Oracle Internet Directory からの接続ディレクトリのブートストラップ

接続ディレクトリからの Oracle Internet Directory のブートストラップと同様に、Oracle Internet Directory からの接続ディレクトリのブートストラップも、次のいずれかの方法で行うことができます。

- 外部ツールを使用した Oracle Internet Directory からのデータ・エクスポート
- コネクタの設定による Oracle Internet Directory からのデータ・エクスポート

外部ツールを使用した Oracle Internet Directory からのデータ・エクスポート

1. Oracle Internet Directory を読取り専用モードに設定し、すべての更新を禁止します。
2. LDIFWrite ツールを使用して、データを Oracle Internet Directory から LDIF ファイルにダンプします。
3. LDIF ファイルを使用して、データを接続ディレクトリにロードします。

コネクタの設定による Oracle Internet Directory からのデータ・エクスポート

この方法で、Oracle Internet Directory からの変更は、OID の前回適用された変更番号（orclLastAppliedChangeNumber 属性）に基づいて接続ディレクトリにプッシュされます。データは、次の順序で接続ディレクトリにブートストラップできます。

1. Oracle Internet Directory を読取り専用モードに設定し、すべての更新を禁止します。
2. Oracle Directory Manager を使用して、接続ディレクトリのエージェントを Oracle Directory Integration Platform に登録します。
3. Directory Integration Server は、スケジューリングの間隔に基づいてエクスポート操作を開始します。エクスポートの完了を待機します。
4. 同期の完了と検証後に、接続ディレクトリの設定を更新モードに戻します。

33

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。この確認には、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。

- 概要
- Oracle Human Resources からインポートできるデータ
- Oracle Human Resources との同期の管理

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 Human Resources コネクタは、デフォルトの構成では、Oracle Internet Directory とともにインストールされます。インストール後はただちに実行できます。

Oracle Human Resources コネクタは、Oracle Human Resources システムから増分変更を毎秒 1 回の頻度で抽出するように構成することによって、いつでも実行できます。また、Oracle Human Resources と Oracle Internet Directory の間の属性マッピングを、設定および変更することもできます。

Oracle Human Resources コネクタの実行可能ファイル名は `odihragent` で、`$ORACLE_HOME/ldap/odi/bin` ディレクトリにあります。Oracle Human Resources コネクタは、Oracle Directory Manager を使用して管理できます。

Oracle Human Resources からインポートできるデータ

表 33-1 は、Oracle Human Resources のスキーマ内の表のリストです。これらの表のほとんどの属性は、Oracle Internet Directory にインポートできます。

表 33-1 Oracle Human Resources のスキーマ内の表

表名	「Connector Config Info」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 33-2 は、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ています。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 33-2 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
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 /E 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

表 33-2 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
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 との同期の管理

この項では、次の項目について説明します。

- 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 Internet Directory と同期化される属性のリストのカスタマイズ
- Oracle Human Resources コネクタに関するマッピング・ルールのカスタマイズ
- Oracle Human Resources から Oracle Internet Directory への同期の実行

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。これは、第 30 章「Oracle Directory Integration Server の管理」で説明している手順に従って行います。ただし、通常どおりサーバー・インストールを行った場合は、Oracle Universal Installer によってディレクトリ内に作成された、デフォルトの統合プロファイルを使用できます。クライアントのみのインストールの場合は、この統合プロファイルは作成されません。

この統合プロファイルには、いくつかの属性と属性値が含まれています。表 33-3 は、これらの属性のリストです。属性は、Oracle Directory Manager で使用するわかりやすい名前（`Profile Name` など）と、実際の名前（`orclodipAgentName` など）の両方で示されています。この表では各属性について説明し、適切な場合は、Oracle Human Resources コネクタの統合プロファイルのデフォルト値を示します。

表 33-3 Oracle Human Resources コネクタ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）	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。
プロファイル・ステータス（orclODIPAgentcontrol）	コネクタが使用可能か使用禁止かを示します。有効な値は「ENABLE」または「DISABLE」です。 デフォルトは「DISABLE」です。この属性は必須で、変更可能です。 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（orclODIPAgentPassword）	Directory Integration 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です。この属性は必須で、変更可能です。 この値は、Oracle Human Resources プロファイルで使用するパスワードに設定してください。
実行ホスト（orclODIPAgentHostName）	コネクタが実行されるホスト。この属性は必須で、変更可能です。リリース 9.2 では、この属性は無視されます。
同期（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 Human Resources に関して、Oracle Internet Directory リリース 9.2 がサポートしているのは、インポート操作のみです。
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の秒数。デフォルトは 600 です。 この属性は必須で、変更可能です。

表 33-3 Oracle Human Resources コネクタの統合プロファイルの属性（続き）

属性	説明
最大再試行回数（orclODIPSyncRetryCount）	Directory Integration Server が同期の断念までに行う、同期の最大試行回数。同期は、スケジュールされている次の機会に再試行されます。 デフォルトは 5 です。 この属性は必須で、変更可能です。
実行情報	

エージェント実行コマンド（orclODIPAgentExeCommand）	Directory Integration 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 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）	Oracle Human Resources システム内の変更にアクセスする、Oracle Human Resources システム内で有効なユーザー・アカウント。 この情報は、コネクタの起動時に、Directory Integration Server によってコマンドラインの中のコネクタに渡されます。 この属性はオプションで、変更可能です。
接続ディレクトリ・アカウント・パスワード（orclODIPConDirAccessPassword）	Oracle Human Resources システムにアクセスするユーザー・アカウントのためのパスワード。このパスワードは、コネクタの起動時に、Directory Integration Server によってコネクタに渡されます。 この属性はオプションで、変更可能です。

表 33-3 Oracle Human Resources コネクタの統合プロファイルの属性（続き）

属性	説明
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 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 Server はその内容を一切認識しません。 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：**33-8 ページ「Oracle Internet Directory と同期化される属性のリストのカスタマイズ」 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。
インタフェース型（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）	接続ディレクトリと Oracle Internet Directory 間でデータをマッピングするためのマッピング・ルール。 **関連項目：** この属性に格納される値については、28-5 ページの「コネクタの Oracle Directory Integration Platform への登録」を参照してください。 Oracle Human Resources の場合、この属性は必須で、変更可能です。
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 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。

表 33-3 Oracle Human Resources コネクタの統合プロファイルの属性（続き）

属性	説明
ステータス情報	
同期ステータス （orclODIPSynchronizationStatus）	同期を行っているプロファイルの実行ステータスを示します。 この属性は読取り専用です。
同期エラー （orclODIPSynchronizationErrors）	最後に発生した同期エラーに関するエラー・メッセージ。 この属性は読取り専用です。
前回実行日時（orclODIPLastExecutionTime）	プロファイルを実行した最新の日時。 通常、この属性は読取り専用です。異なる時点から再度同期化する場合は変更できます。
前回成功実行日時 （orlcODIPLastSuccessfulExecutionTime）	プロファイルの実行に成功した最新の日時。通常、この属性は読取り専用です。異なる時点から再度同期化する場合は変更できます。
接続ディレクトリの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。
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。

Oracle Internet Directory と同期化される属性のリストのカスタマイズ

Oracle Internet Directory と同期化される Oracle Human Resources の属性のリストは、カスタマイズできます。これに役立つように、Oracle Internet Directory には、Oracle Human Resources の同期化される属性のデフォルトのリストが含まれています。このリストは、属性を追加または除外することにより変更できます。

デフォルトの属性のリストは、統合プロファイルの一部として orclodipAgentConfigInfo 属性に格納されています。統合プロファイルは通常のインストールの一部として Oracle Internet Directory にロードされます。このリストは oraclehragent.cfg.master という名前のファイルにも含まれており、*$ORACLE_HOME*/ldap/odi/conf ディレクトリの下にあります。

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標識。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
```

Oracle Human Resources の同期化される属性の追加

Oracle Human Resources の同期化される属性を追加するには、次の手順に従います。

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 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. 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、33-2 ページの表 33-1 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、この属性を出力ファイル内で識別するための出力タグとして機能します。また、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も使用されます。

   `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。マッピング・ルールの作成方法は、33-14 ページの「Oracle Human Resources の属性マッピング・ルールの作成」を参照してください。

3. ldapmodify ツールを使用して、このファイルを `orclodipAgentConfigInfo` 属性にロードします。変更は次回コネクタを実行したときに有効になります。

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 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。
3. ldapmodify ツールを使用して、このファイルを `orclodipAgentConfigInfo` 属性にロードします。変更は次回コネクタを実行したときに有効になります。

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

サポートされている前述の属性の構成が、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 コネクタは、構成ファイル内にある事前構成の 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フェッチするサンプルの 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、増分変更をフェッチ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 文でフェッチす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 としてフェッチされます。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。

```
[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')
```

Oracle Human Resources コネクタに関するマッピング・ルールのカスタマイズ

属性マッピング・ルールは、Directory Integration 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 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。

これを容易にするために、Oracle Internet Directory には、Oracle Human Resources システム用の、Oracle Human Resources のマッピング・ルールのデフォルトのリストが含まれています。マッピング・ルールを構成、変更または削除するには、このリストを編集します。

マッピング・ルールのデフォルトのリストは、統合プロファイルの中の `orclodipAttributeMappingRules` 属性に格納されています。さらに、この規則は `oraclehragent.map.master` という名前のファイルにも含まれており、*$ORACLE_HOME*`/ldap/odi/conf` ディレクトリの下にあります。

注意： `oraclehragent.map.master` ファイルはバックアップとして機能するため、変更できません。

デフォルトの Oracle Human Resources コネクタのマッピング・ルール

oraclehragent.map.master ファイルの内容は、次のとおりです。

```
DomainRules
NONLDAP:dc=metaagt,dc=com:uid=%dc=metaagt,dc=com
AttributeRules
firstname: : : :cn: :person
email : : : :cn: :person: trunc(email,'@')
email : : : :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
```

このサンプル・マッピング・ファイルで、'dc=metaagt,dc=com' は同期ドメインとみなされます。このドメイン名は、配置要件に従って変更する必要があります。

```
AttributeRules
firstname: : : :cn: :person
lastname: : : :sn: :person
lastname: : : :cn: :person
 : : : :cn: :person: trunc(email,'@')
 : : : :cn: :person: firstname+","+lastname
 : : : :cn: :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: : : :l: :locality
```

```
Title: : : :title: :organizationalperson
Sex: : : :sex: :person
socialsecurity: : : :ssn: :person
country: : : :c: :country
BirthDate: : : :birthday: :organizationalperson
 : : : :userpassword: :person: "welcome"
changetype
###
```

orclodipAttributeMappingRules 属性内のデフォルトのマッピング・ルールは、orclodipAgentConfigInfo 属性内のデフォルトの Oracle Human Resources 属性リストに対応しています。Oracle Human Resources の属性と Oracle Internet Directory の属性の間のマッピングを確立するために、マッピング・ルールは Oracle Human Resources 属性リストの各レコードの ATTRNAME 列を使用します。

> **関連項目：** マッピング・ルールのレコードの書式は、28-10 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。

Oracle Human Resources の属性マッピング・ルールの作成

Oracle Human Resources の属性マッピング・ルールを作成するには、orclodipAttributeMappingRules 属性を変更します。この手順は、次のとおりです。

1. oraclehragent.map.master ファイルを *Agent_Name*.tmp にコピーします。
2. このファイルにレコードを追加することにより、新規規則を追加します。これには、次の情報が必要です。
   - Oracle Internet Directory にマップされる Oracle Human Resources の属性名
   - Oracle Human Resources の属性のマップ先になる、Oracle Internet Directory 内の対応する属性とそのオブジェクト・クラス
   - Oracle Human Resources の属性を Oracle Internet Directory の属性にマップする方法を決定するインポート・ルール
3. 次のスクリプトを使用して、このファイルを orclodipAttributeMappingRules 属性にロードします。

   ```
   $ORACLE_HOME/ldap/odi/admin/ldapUploadAgentFile.sh
   ```

   変更は次回プロファイルを実行したときに有効になります。

Oracle Human Resources の属性マッピング・ルールの変更

Oracle Human Resources の既存の属性マッピング・ルールを変更するには、orclodipAttributeMappingRules 属性を変更します。この手順は、次のとおりです。

1. oraclehragent.map.master ファイルを *Profile_Name*.map にコピーします。
2. このファイルを編集します。
3. ldapmodify ツールを使用して、このファイルを orclodipAttributeMappingRules 属性にロードします。変更は次回コネクタを実行したときに有効になります。

Oracle Human Resources の属性マッピング・ルールの削除

Oracle Human Resources の既存の属性マッピング・ルールを削除するには、orclodipAttributeMappingRules 属性を変更します。この手順は、次のとおりです。

1. oraclehragent.map.master ファイルをコピーし、*Agent_Name*.map 以外の名前を付けます。この名前は Directory Integration Server が使用するために予約されています。
2. 次のいずれか 1 つを行います。
   - 規則をファイルから削除する。
   - 前にハッシュ（#）符号を付けてコメント化する。
3. 次のスクリプトを使用して、このファイルを orclodipAttributeMappingRules 属性にロードします。

   ```
   $ORACLE_HOME/ldap/odi/admin/ldapUploadAgentFile.sh
   ```

   変更は次回プロファイルを実行したときに有効になります。

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 1.0。サイト：http://sources.redhat.com/cygwin/
- MKS Toolkit 5.1 または 6.0。
  サイト：http://www.datafocus.com/products/

Oracle Human Resources から Oracle Internet Directory への同期の実行

この項では、Oracle Human Resources から Oracle Internet Directory への同期のセットアップ方法を説明します。

同期時に、Oracle Directory Integration Platform はインポート・ファイルを使用します。このファイルには、Oracle Human Resources コネクタが Oracle Human Resources システムから抽出する、少数または多数の変更を含めることができます。

このファイルはタグ付き形式で、Oracle ディレクトリ・サーバーへの入力として機能します。ファイル名は *Oracle_HR_Agent_Name*.data で、$*ORACLE_HOME*/ldap/odi/import にあります。

このファイルは変更する必要はありませんが、その最新バージョンは、トラブルシューティングに役立つようにディレクトリ $*ORACLE_HOME*/ldap/odi/import/archive に格納されます。

次に示すのは、インポート・ファイル内の Oracle Human Resources の変更レコードの例です。

```
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
```

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 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 リリース 9.2 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. このホストの Directory Integration Server が Oracle Internet Directory に登録されていることを確認します。

   関連項目： " 登録方法は、30-2 ページの「Oracle Directory Integration Server の登録」を参照してください。

4. 33-4 ページの「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
5. すべてを適切に設定した後、プロファイル・ステータス属性を「使用可能」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できていることを示します。
6. 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。
7. すべての準備ができた後、まだこのホストで Directory Integration Server が実行されていなければ、これを起動します。

   関連項目： Directory Integration Server を起動および停止する方法は、30-7 ページの「Oracle Directory Integration Server の管理」を参照してください。

同期化プロセス

Oracle Human Resources システム、Oracle Internet Directory および Directory Integration Server が実行され、Oracle Human Resources コネクタが使用可能になると、Directory Integration 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 Server は、Oracle Human Resources コネクタを起動します。
2. Oracle Human Resources コネクタは、統合プロファイルの `orclodipLastSuccessfulExecutionTime` 属性に指定されている日時に従って、Oracle Human Resources システムから変更をすべて抽出します。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。Oracle Human Resources コネクタが抽出するのは、統合プロファイルの `orclodipAgentConfigInfo` 属性に指定されている属性のみです。

3. エージェントが実行を完了すると、Directory Integration Server は次の操作を実行して、変更を Oracle Internet Directory にインポートします。
   - インポート・ファイルからの各変更レコードの読込み。
   - 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。
4. 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（`$ORACLE_HOME/ldap/odi/import/archive`）に移動します。ステータスの属性である前回実行日時（`orclodipLastExecutionTime`）と前回成功実行日時（`orclodipLastSuccessfulExecutionTime`）を現行の日時に更新します。
5. インポート操作に失敗した場合は、前回実行日時のみが更新され、コネクタは、前回成功実行日時に基づいて Oracle Human Resources システムからの変更の抽出を再試行します。失敗の理由は、`$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、`orclodipConDirLastAppliedChgTime` 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。

関連項目： 初期ブートストラップの方法の詳細は、第 32 章「Oracle Directory Integration 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。

34

iPlanet Directory Server との同期化

この章では、Oracle Directory Integration Platform で iPlanet コネクタを使用して、Oracle Internet Directory と iPlanet Directory Server を同期化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。

- iPlanet コネクタの概要
- iPlanet コネクタの構成
- Oracle Internet Directory と iPlanet Directory Server 間の同期
- トラブルシューティング
- 今回のリリースでの制限事項

iPlanet コネクタの概要

iPlanet コネクタ環境では、次のことが可能になります。

- iPlanet Directory Server から Oracle Internet Directory へのデータのインポート
- Oracle Internet Directory から iPlanet Directory Server へのデータのエクスポート

各操作ごとに個別のプロファイルを構成する必要があります。

同期は、iPlanet Directory Server リリース 4.13 および 5.0 でサポートされます。

iPlanet コネクタの構成

この項では、iPlanet 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: 同期化する双方のディレクトリの準備
- タスク 2: iPlanet コネクタの統合プロファイルの構成
- タスク 3: マッピング・ルールの構成
- タスク 4: アクセス制御の構成
- タスク 5: パスワード保護の構成

タスク 1: 同期化する双方のディレクトリの準備

1. 2 つのディレクトリを同期化する前に、両方のディレクトリのサブスクライブ・ドメインに等しいユーザー・データがあることを確認します。データが等しくない場合は、最新のデータをもう一方のディレクトリに移行します。

   関連項目：

   - データの移行方法は、付録 E「他のディレクトリからのデータの移行」を参照してください。
   - iPlanet Directory Server へのデータの移行方法は、iPlanet Directory Server のドキュメントを参照してください。

2. 移行の終了時には、Oracle ディレクトリ・サーバーの変更ログ記録オプションがデフォルト（つまり、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。

   関連項目： OID 制御ユーティリティの詳細は、A-6 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。

   同様に、iPlanet 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。

3. 変更ログがすでに使用可能な場合は、各ディレクトリに対して次のコマンドを使用し、Oracle Internet Directory と iPlanet Directory Server の `lastChangeNumber` 属性の値を書き留めてください。

```
ldapsearch  -D SuperUserDn  -w SuperUserPass -b "" -s base "objectclass=*"
lastchangenumber
```

   次に、両方のディレクトリの `lastChangeNumber` 属性の値を使用して、統合プロファイルに次の属性を構成します。

   - `orclLastAppliedChangeNumber`: Oracle Internet Directory から iPlanet Directory Server へのエクスポート用
   - `orclodipConDirLastAppliedChgNum`: iPlanet Directory Server から Oracle Internet Directory へのインポート用

タスク 2: iPlanet コネクタの統合プロファイルの構成

iPlanet 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 Internet Directory サーバーに作成されています。同期を使用可能にする前に、その配置で固有のパラメータをプロファイルに設定します。この設定には、Oracle Directory Manager を使用します。

関連項目：

- 必要な手順、および設定が必要な各属性の一般的な説明は、28-5 ページの「コネクタの Oracle Directory Integration Platform への登録」を参照してください。
- 表 34-1 は、iPlanet Directory Server の統合プロファイルに固有な属性情報のリストと説明です。

表 34-1 iPlanet Directory Server の統合プロファイルの属性（インポート / エクスポート）

属性	説明
一般情報	
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。
プロファイル・ステータス（orclodipAgentControl）	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）	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。
同期モード（orclodipSynchronizationMode）	Oracle Internet Directory と iPlanet コネクタ間での同期の方向。 ■ IMPORT は iPlanet Directory Server 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 iPlanet Directory Server への変更のエクスポートを示します。 この属性は、各統合プロファイルにすでに構成されています。
スケジューリングの間隔（orclodipSchedulingInterval）	デフォルトは 600 秒です。この属性は、必要に応じて異なるスケジューリング間隔に変更できます。
最大再試行回数（orclodipSyncRetryCount）	失敗した場合に Oracle Directory Integration Server が iPlanet 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。

表 34-1 iPlanet Directory Server の統合プロファイルの属性（インポート / エクスポート）（続き）

属性	説明
実行情報	
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。
接続ディレクトリ・アカウント（`orclodipConDirAccessAccount`）	iPlanet コネクタが iPlanet Directory Server へのアクセスに使用する iPlanet Directory Server の有効なユーザー・アカウント。 ■ 変更が iPlanet 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 iPlanet 変更ログ・コンテナでの読込み権限が必要です。 ■ Oracle Internet Directory での変更が iPlanet 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 / 変更権限が必要です。 ■ **注意 :** iPlanet コネクタに対して、排他的に iPlanet のユーザー・アカウントを作成して、同期を行なってください。
接続ディレクトリ・アカウント・パスワード（`orclodipConDirAccessPassword`）	iPlanet Directory Server へのアクセスのために、以前に指定したユーザー・アカウントのパスワード。
追加構成情報（`orclodipAgentConfigInfo`）	iPlanet コネクタの場合、この属性には iPlanet コネクタの詳細が格納され、その LDAP インタフェースを使用して、iPlanet Directory Server と同期を行います。この情報は、統合プロファイルにすでにロードされています。 ファイルは、`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。
インタフェース型（`orclodipInterfaceType`）	この属性は、LDAP に設定されています。

表 34-1 iPlanet Directory Server の統合プロファイルの属性（インポート / エクスポート）（続き）

属性	説明
マッピング情報	
マッピング・ルールの属性（orclodipAttributeMappingRules）	マッピング・ルールは、ldapuploadagentfile.sh ツールを使用してファイルに格納してください。 **関連項目：**マッピング・ファイルのエントリの詳細は、34-7 ページの「タスク 3: マッピング・ルールの構成」を参照してください。
接続ディレクトリの照合フィルタ（orclodipConDirMatchingFilter）	この属性は、iPlanet Directory 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。フィルタは、インポート（iPlanetImport）とエクスポート（iPlanetExport）の統合プロファイルの両方が使用可能な場合に、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。
OID の照合フィルタ	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。フィルタは、インポート（iPlanetImport）とエクスポート（iPlanetExport）の統合プロファイルの両方が使用可能な場合に、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。

表 34-1 iPlanet Directory Server の統合プロファイルの属性（インポート / エクスポート）（続き）

属性	説明
ステータス情報	
同期ステータス（orclodipSynchronizationStatus）	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）	エラー・メッセージ。前回の実行で同期化に失敗した場合に表示されます。このパラメータは Oracle Directory Integration Server によって更新されます。この属性は読取り専用です。
接続ディレクトリの前回適用された変更番号（orclodipConDirLastAppliedChgNum）	デフォルト値は 0（ゼロ）です。この属性の lastchangenumber 値への設定については、34-2 ページの「タスク 1: 同期化する双方のディレクトリの準備」を参照してください。
OID の前回適用された変更番号（orclLastAppliedChangeNumber）	デフォルト値は 0（ゼロ）です。この属性の lastchangenumber 値への設定については、34-2 ページの「タスク 1: 同期化する双方のディレクトリの準備」を参照してください。
最終実行時間（orclodipLastExecutionTime）	この属性は、「次に実行される時間」に設定する必要があります。
前回成功実行日時（orclodipLastSuccessfulExecution Time）	この属性はステータスの属性で、Directory Integration 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ます。

タスク 3: マッピング・ルールの構成

iPlanet Directory Server と Oracle Internet Directory 間で同期化されるエントリの属性をカスタマイズできます。マッピング・ルールを使用すると、ディレクトリに属性値を格納する方法も決定できます。

要件にあわせてカスタマイズできるように、サンプル・マッピング・ファイルが $*ORACLE_HOME*/ldap/odi/conf/iPlanet.map.master に用意されています。

このファイルのロードには、ldapuploadagentfile.sh ツールを使用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 1.0。サイト：`http://sources.redhat.com/cygwin/`
- MKS Toolkit 5.1 または 6.0。
  サイト：`http://www.datafocus.com/products/`

関連項目：

- 詳細は、28-10 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。
- ldapuploadagentfile.sh ツールの使用方法は、A-48 ページの「oidmuplf.sh ツール」を参照してください。

タスク 4: アクセス制御の構成

サブスクライブ・ドメインで読込み、追加または変更を行うためのアクセス権限を許可する適切な ACL を設定します。

インポート操作では、次のアクセス制御が必要です。

1. Oracle Internet Directory のサブスクライブ・ドメインを更新するための権限を Oracle Internet Directory のユーザー `orclodipagentname=iPlanetImport, cn=subscriber profile,cn=changelog subscriber, cn=oracle internet directory` に付与します。
2. 統合プロファイルの接続ディレクトリ・アカウントの属性に指定されているユーザーには、iPlanet Directory Server の変更ログ・コンテナに対する読込みアクセス権限が必要です。

   たとえば、関係のあるドメインに適用する ACL がない（つまり、`Synchronization domain in OID`）と仮定すると、次の LDIF サンプルを使用できます。

```
ACL in OID:
    dn: <Synchronization domain in OID>
    changetype: modify
    replace: 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)"
```

エクスポート操作では、統合プロファイルの接続ディレクトリ・アカウントの属性に指定されているユーザーには、iPlanet Directory Server に含まれる変更ログに対する読込みアクセス権限が必要です。

関連項目： iPlanet 変更ログ・コンテナと iPlanet サブスクライブ・ドメインへの ACL の適用方法は、iPlanet Server のドキュメントを参照してください。

タスク 5: パスワード保護の構成

保護されている複数のパスワード属性（たとえば、`userPassword`）の同期化を可能にするには、両方のディレクトリに同一のパスワード・ハッシング・アルゴリズムを構成します。

Oracle Internet Directory のパスワードにハッシング・アルゴリズムを設定するには、次のコマンドを使用します。

```
ldapmodify  -D SuperUserDn  -w SuperUserPass  << EOF
dn:
changetype: modify
replace: orclcryptoscheme
orclcryptoscheme: your_hashing_algorithm
```

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、10-7 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。
- iPlanet 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、iPlanet Directory Server のドキュメントを参照してください。

Oracle Internet Directory と iPlanet Directory Server 間の同期

この項では、次の項目について説明します。

- 同期の準備
- 同期化プロセス

同期の準備

Oracle Internet Directory と iPlanet Directory Server 間の同期を正しく準備するには、次のことを確認します。

- Oracle Directory Integration Server と iPlanet Directory Server がインストール済みで、実行されていること
- 構成の詳細が、34-2 ページの「iPlanet コネクタの構成」の説明に正しく従っていること
- このホストの Oracle Directory Integration Server が Oracle Internet Directory に登録済みで、実行されていること

同期化プロセス

同期化プロセスは、次の順序で実行されます。

1. インポート操作では、iPlanet コネクタが `orclodipConDirLastAppliedChgNum` 属性に指定されている値に基づいて、すべての変更をソース・ディレクトリ（つまり、iPlanet Directory Server）から抽出し、Oracle Internet Directory に適用します。同様に、エクスポート操作では、iPlanet コネクタが `orclodipLastChangeNumber` 属性に基づいて、すべての変更を Oracle Internet Directory から抽出し、iPlanet Directory Server に適用します。
2. 変更がすべて読み込まれて適用されると、適切な属性（`orclodipConDirLastAppliedChgNum` または `orclodipLastAppliedChangeNumber`）が更新されます。
3. 実行が完了すると、Oracle Directory Integration Server は実行ステータスの属性を更新します。

トラブルシューティング

Oracle Directory Integration Server は、エラー・メッセージを 30-13 ページの表 30-5 に説明されている適切なファイルに格納します。

今回のリリースでの制限事項

Oracle Internet Directory リリース 9.2 では、スキーマおよび ACL の同期はサポートされません。ACL またはスキーマを変更する場合は、手動で変更を適用する必要があります。

スキーマを同期化するツール（つまり、SchemaSync）は、Oracle Internet Directory リリース 9.2 で使用できます。

> **関連項目：** SchemaSync ツールの詳細は、A-52 ページの「schemasync ツール」を参照してください。

Oracle Internet Directory リリース 9.2 では、Oracle Directory Integration Server と Oracle Internet Directory の間の SSL 認証はサポートされますが、Oracle Internet Directory と iPlanet Directory Server の間の SSL 認証はサポートされません。

> **関連項目：** Oracle Directory Integration Server と Oracle Internet Directory の間で安全な通信を行うために SSL パラメータを設定する方法については、第 30 章「Oracle Directory Integration Server の管理」を参照してください。

35

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 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 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
- 同期化プロセス
- 変更サブスクリプション・オブジェクトの無効化と削除

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 全体を読み込み、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、28-2 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: 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 Oracle Internet Directory での作成

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には、次の手順を実行します。

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-41 ページの「ldifwrite の構文」を参照してください。

タスク 2: 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 Oracle Internet Directory での作成

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やすべて削除する方法については、35-6 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。

同期化プロセス

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、35-3 ページの「タスク 2: 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 Oracle Internet Directory での作成」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、適用済み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、21-6 ページの「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 IX 部

付録

第 IX 部は次の各付録で構成されています。

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
- エントリ管理コマンドライン・ツール
- 属性管理コマンドライン・ツール
- バルク操作コマンドライン・ツール
- レプリケーション管理コマンドライン・ツール
- ディレクトリの同期とプロビジョニングのコマンドライン・ツール
- OID データベース・パスワード・ユーティリティ
- OID データベース統計収集ツール
- OID 移行ツール

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
email: 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。6-9 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、xxxv ページの「関連文書」の各種資料を参照してください。
  - 8-4 ページ「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
- OID 制御ユーティリティ
- 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

OID モニター

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 モニターの開始

OID モニターを開始する手順は、次のとおりです。

1. 次の環境変数を適切な言語設定に設定します。インストール時のデフォルトの言語設定は、AMERICAN_AMERICA です。

   ```
   NLS_LANG=APPROPRIATE_LANGUAGE.AL32UTF8
   ```

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=net_service_name] [sleep=seconds] start
   ```

引数	説明
`connect=net_service_name`	接続するデータベースのネット・サービス名を指定します。`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。
`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。

次のようなコマンドを実行します。

```
oidmon connect=dbs1 sleep=10 start
```

OID モニターの停止

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=net_service_name] stop
```

引数	説明
connect=*net_service_name*	接続するデータベースのネット・サービス名を指定します。tnsnames.ora ファイルに設定されているネット・サービス名です。
stop	OID モニターのプロセスを停止します。

次のようなコマンドを実行します。

```
oidmon connect=dbs1 stop
```

OID 制御ユーティリティ

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。

> **注意：** ディレクトリ・サーバー・インスタンスを起動、停止または再起動するときは、常に OID モニターが実行中であることが必要です。

この項では、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
- 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
- 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・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=net_service_name server=oidldapd instance=server_instance_number
[configset=configset_number] [flags='-p port_number -work maximum_number_of_worker_
threads_per_server -server number_of_server_processes -debug debug_level -l
change-logging -server n'] start
```

引数	説明
connect=*net_service_name*	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=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。
instance=*server_instance_number*	起動するサーバーのインスタンス番号。0 ～ 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。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。
-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。未設定の場合、デフォルト・ポートは 389 です。
-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。
-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。記録しない場合は -l を入力し、記録する場合はこのフラグを省略します。デフォルトは TRUE（値は TRUE と FALSE）です。（ディレクトリ・サーバーのみ）
-server *n*	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。
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 Oracle 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、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=net_service_name server=oidldapd instance=server_instance_number stop
```

次のようなコマンドを実行します。

```
oidctl connect=dbs1 server=oidldapd instance=3 stop
```

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=net_service_name server=oidrepld instance=server_instance_number
[configset=configset_number] flags='-h hostname -p port_number
-d debug_level -z transaction_size' start
```

引数	説明
connect	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	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	起動するサーバーのインスタンス番号。0 ～ 1000 の間の数値を設定してください。
configset	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。
-p	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。未設定の場合、デフォルト・ポートは 389 です。
-d	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	サーバーを実行するホスト名を指定します。（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。デフォルトは TRUE（値は TRUE と FALSE）です。（レプリケーション・サーバーのみ）
-z	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=net_service_name server=oidrepld instance=server_instance_number stop
```

次のようなコマンドを実行します。

```
oidctl connect=dbs1 server=oidrepld instance=1 stop
```

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=net_service_name server={oidldapd|oidrepld}
instance=server_instance_number  restart
```

ディレクトリ・サーバー・インスタンスを起動、停止または再起動するときは、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。

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=net_service_name flags='-p port_number -f'
```

フラグ内に `-f` オプションを指定すると、定義済みの構成設定が `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。

エントリ管理コマンドライン・ツール

この項では、次のツールの使用方法を説明します。

- ldapadd の構文
- ldapaddmt の構文
- ldapbind の構文
- ldapdelete の構文
- ldapmoddn の構文
- ldapsearch の構文

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-28 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、5-11 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 filename
```

filename は、A-2 ページの「LDAP Data Interchange Format（LDIF）の構文」で説明されている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
```

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。）

オプションの引数	説明
-D "*binddn*"	ディレクトリに対して認証するときに、*binddn* に指定されているエントリ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。第 8 章「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 *filename*	LDIF フォーマットのインポート・データ・ファイルの入力名を指定します。LDIF ファイルのフォーマット方法の詳細は、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。
-K	-k と同様ですが、Kerberos バインドの最初のステップのみ実行します。
-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、定義済みの 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* 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。

オプションの引数	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*	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 UNIX では、このパラメータは次のように設定します。
	`-W "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。
	`-W "file:C:¥my_dir¥my_wallet"`

ldapaddmt の構文

ldapaddmt は ldapadd と似ています。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 filename
```

filename は、A-2 ページの「LDAP Data Interchange Format（LDIF）の構文」で説明されている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。

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するときに、*binddn* に指定されているエントリ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。第 8 章「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。
-K	-k と同様ですが、Kerberos バインドの最初のステップのみ実行します。
-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、定義済みの 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。

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`	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 UNIX では、このパラメータは次のように設定します。
	`-W "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。
	`-W "file:C:¥my_dir¥my_wallet"`

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]
```

オプションの引数	説明
`-D "binddn"`	ディレクトリに対して認証するときに、*binddn* に指定されているエントリ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。第 8 章「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。

オプションの引数	説明
-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。
-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 UNIX では、このパラメータは次のように設定します。
	`-W "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。
	`-W "file:C:¥my_dir¥my_wallet"`

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_filename]
```

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"
```

オプションの引数	説明
-D "*binddn*"	ディレクトリに対して認証するときに、*binddn* パラメータに完全識別名を使用します。通常、-w *password* オプションとともに使用されます。
-d *debug level*	デバッグ・レベルを設定します。5-26 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。第 8 章「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_filename*	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、定義済みの 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。

オプションの引数	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`	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 UNIX では、このパラメータは次のように設定します。
	`-W "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。
	`-W "file:C:¥my_dir¥my_wallet"`

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"
```

必須の引数	説明
`-b "basedn"`	変更されるエントリの識別名を指定します。

オプションの引数	説明
-D "*binddn*"	ディレクトリに対して認証するときは、そのエントリが *binddn* に指定されている場合に認証します。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。第 8 章「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 *filename*	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。
-N *newparent*	相対識別名の新しい親を指定します。
-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。
-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。
-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。

オプションの引数	説明

`-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 UNIX では、このパラメータは次のように設定します。
	`-W "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。
	`-W "file:C:¥my_dir¥my_wallet"`

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 の書式は RFC-2254 に準拠している必要があります。

> **関連項目：** フィルタの書式の規格の詳細は、`http://www.ietf.org/rfc/rfc2254.txt` 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。

必須の引数	説明
`-b "basedn"`	検索のためのベース識別名を指定します。
`-s scope`	検索有効範囲を指定します。base、one または sub。

オプションの引数	説明
`-A`	属性名のみ取り出します（値は取り出しません）。
`-a deref`	別名参照解除を指定します。never、always、search または find。
`-B`	非 ASCII 値を出力します。

オプションの引数	説明
-D "*binddn*"	ディレクトリに対して認証するときに、*binddn* に指定されているエントリ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（5-27 ページの表 5-1 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。第 8 章「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 フォーマットで出力します（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。
-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。

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	冗長モードを指定します。
-w *bindpassword*	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 UNIX では、このパラメータは次のように設定します。
	`-W "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。
	`-W "file:C:¥my_dir¥my_wallet"`

-z *sizelimit*	エントリの最大検索数を指定します。

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"
```

属性管理コマンドライン・ツール

この項では、次の項目について説明します。

- カタログ管理ツール
- ldapcompare の構文
- ldapmodify の構文
- ldapmodifymt の構文

カタログ管理ツール

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
- 属性名が 27 文字以下

> **関連項目：** Oracle Internet Directory でサポートする一致規則については、C-9 ページの「一致規則」を参照してください。

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。

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 1.0。サイト：`http://sources.redhat.com/cygwin/`
- MKS Toolkit 5.1 または 6.0。
  サイト：`http://www.datafocus.com/products/`

カタログ管理ツールは次の構文を使用します。

```
catalog.sh -connect net_service_name {add|delete} {-attr attr_name|-file filename}
```

必須の引数	説明
-connect *net_service_name*	ディレクトリ・データベースに接続するためのネット・サービス名を指定します。 **関連項目：**『Oracle9*i* Net Services 管理者ガイド』

オプションの引数	説明
- 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 *filename*	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 *filename*	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-5 ページの「OID 制御ユーティリティ」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」を参照してください。

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
```

必須の引数	説明
-a *attribute name*	比較を実行する属性を指定します。
-b *"basedn"*	比較を実行するエントリの識別名を指定します。
-v *attribute value*	比較する属性値を指定します。

オプションの引数	説明
-D *binddn*	ディレクトリに対して認証するときに、*binddn* に指定されているエントリ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。5-26 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。第 8 章「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 *filename*	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。

オプションの引数	説明
`-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 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 UNIX では、このパラメータは次のように設定します。
	`-W "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。
	`-W "file:C:¥my_dir¥my_wallet"`

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 filename
```

filename は、A-2 ページの「LDAP Data Interchange Format（LDIF）の構文」で説明されている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。

オプションの引数	説明
-a	エントリが追加対象で、入力ファイルが LDIF フォーマット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するときに、*binddn* に指定されているエントリ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。第 8 章「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。
-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。

オプションの引数	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 UNIX では、このパラメータは次のように設定します。
	`-W "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。
	`-W "file:C:¥my_dir¥my_wallet"`

`-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」を参照してください）。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。次のようなコマンドを実行します。

```
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。たとえば、次のように記述します。

```
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。たとえば、次のように記述します。

```
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フォーマットします。

- `changetype:add`

  LDIF フォーマットを使用します（A-2 ページの「LDAP Data Interchange Format（LDIF）の構文」を参照してください）。

- `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...
    ```

    次のようなコマンドを実行します。

    ```
    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]
    ```

    次のようなコマンドを実行します。

    ```
    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。

次のようなコマンドを実行します。

```
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。

  次のようなコマンドを実行します。

  ```
  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
  ```

  次のようなコマンドを実行します。

  ```
  dn: cn=Barbara Fritchy,ou=Sales,o=Oracle,c=US
  changetype: modrdn
  newrdn: cn=Barbara Fritchy-Blomberg
  ```

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書式を示します。

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、この例のような書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 filename
```

filename は、A-2 ページの「LDAP Data Interchange Format（LDIF）の構文」で説明されている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-28 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。

オプションの引数	説明
`-a`	エントリが追加対象で、入力ファイルが LDIF フォーマット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。
`-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するときに、binddn に指定されているエントリ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。第 8 章「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。

オプションの引数	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	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。
-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 UNIX では、このパラメータは次のように設定します。
	`-W "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。
	`-W "file:C:¥my_dir¥my_wallet"`

バルク操作コマンドライン・ツール

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 1.0。サイト：`http://sources.redhat.com/cygwin/`
- MKS Toolkit 5.1 または 6.0。
  サイト：`http://www.datafocus.com/products/`

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。

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 net_service_name -base "base_dn" -size number_of_entries
-encode "character_set"
```

必須の引数	説明
-connect *net_service_name*	ディレクトリ・データベースに接続するためのネット・サービス名を指定します。 **関連項目：**『Oracle9*i* Net Services 管理者ガイド』
- 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。

オプションの引数	説明
-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：** 第 8 章「ディレクトリにおける グローバリゼーション・サポート」

bulkload の構文

bulkload コマンドライン・ツールは、Oracle SQL*Loader を使用して、他のアプリケーションに常駐しているデータまたは他のアプリケーションで作成されたデータからディレクトリ・エントリを作成します。bulkload を使用するときは、オプションと入力ファイル名を指定します。bulkload は空のディレクトリを想定しているため、既存のエントリがある場合は失敗するか、既存のエントリを上書きします。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「LDAP Data Interchange Format（LDIF）の構文」

bulkload ツールは次の構文を使用します。

```
bulkload.sh -connect net_service_name [-check] [-encode] [-generate] [-load]
[-numthread n] [-parallel] [-restore] absolute_path_to_ldif.file
```

必須の引数	説明
connect *net_service_name*	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。 **関連項目：**『Oracle9*i* Net Services 管理者ガイド』

オプションの引数	説明
`-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。
`-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：** 第 8 章「ディレクトリにおける グローバリゼーション・サポート」
`-generate`	Oracle Internet Directory へのロードに適したファイルを作成します。
`-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。
`numthread n`	`-generate` モードで使用するスレッドの数を指定します。デフォルトは 1 です。
`-parallel`	ロードをパラレルで実行するように指定します。
`-restore`	`orclguid`、`creatorsname` および `createtimestamp` などの操作属性を、新たに生成するかわりに LDIF ファイルから取得します。この引数は、LDIF ファイルに操作属性が含まれている場合にのみ使用してください。また、`generate` および `check` 引数と組み合せて使用してください。

バルク・ロードは、ディレクトリ・サーバー・インスタンスを実行していないときに実行する必要があります。

> **関連項目：** ディレクトリ・サーバー・インスタンスの停止方法は、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。

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。

> **注意：** ディレクトリへの移入に bulkload.sh を使用しない場合は、$ORACLE_HOME/ldap/admin/oidstats.sh を実行して、検索パフォーマンスに著しい低下がないことを確認する必要があります。

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：** 22-1 ページ「Oracle ディレクトリ・レプリケーション・サーバーの管理」

bulkload の現行バージョンでは、すべてのノードに対する接続情報を 1 つのコマンドで指定できません。

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。

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 net_service_name -b "base_dn" {-a|-r} attr_name -v att_value [-f
filter] [-s size]
```

必須の引数	説明
`-c net_service_name`	ディレクトリ・データベースのネット・サービス名を指定します。 **関連項目：**『Oracle9*i* Net Services 管理者ガイド』
`-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。
`-a attr_name`	追加する場合に属性名を指定します。
`-r attr_name`	置換する場合に属性名を指定します。
`-v attr_value`	追加または置換する場合に属性値を指定します。

オプションの引数	説明
`-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。第 8 章「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 フォーマット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 net_service_name -b "base_DN" -f filename
```

必須の引数	説明
-c *net_service_name*	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。 **関連項目：**『Oracle9*i* Net Services 管理者ガイド』
-b "*base_dn*"	LDIF フォーマットで書き出すサブツリーのベース識別名を指定します。
-f *filename*	作成する LDIF ファイルの名前を指定します。

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。 **関連項目：**8-10 ページ「ldifwrite でのグローバリゼーション・サポートの使用方法」

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。

OID 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。

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の索引を削除しないでください。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。

レプリケーション管理コマンドライン・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。

この項では、次の項目について説明します。

- 管理者操作キュー操作ツール
- OID 調停ツール

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 1.0。サイト：`http://sources.redhat.com/cygwin/`
- MKS Toolkit 5.1 または 6.0。
  サイト：`http://www.datafocus.com/products/`

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 net_service_name [-start change_number]
[-end change_number] [-equal change_number] -supplier supplier_node
```

引数は、次のとおりです。

引数	説明
`-connect` *`net_service_name`*	`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 net_service_name [-start change_number] [-end change_number]
[-equal change_number] -supplier supplier_node
```

引数は、次のとおりです。

引数	説明
-connect *net_service_name*	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_rep1
```

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 1.0。サイト : `http://sources.redhat.com/cygwin/`
- MKS Toolkit 5.1 または 6.0。
  サイト : `http://www.datafocus.com/products/`

OID 調停ツールを使用した一貫性のないデータの調停

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]
```

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。
`-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 `cn=orcladmin` のパスワード。
`-w` *`consumer_password`*	コンシューマ・ノードの `cn=orcladmin` のパスワード。
`-T` *`thread`*	ワーカー・スレッド。

OID 調停ツールの動作

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
```

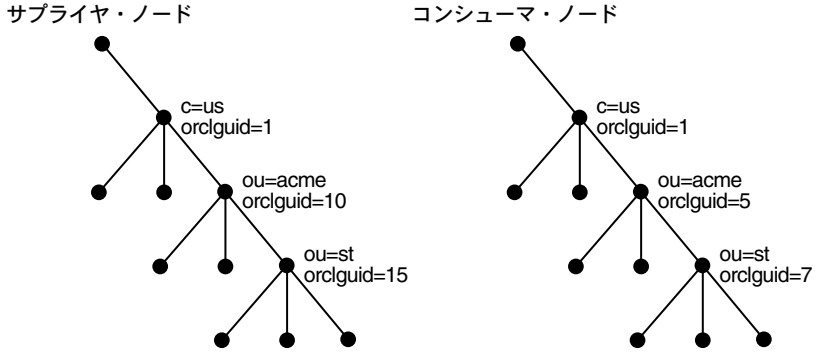
両方の親（"o=acme,c=us"）のグローバル識別子（orclGuid）が一致し、-s subtree が設定されていない場合、OID 調停ツールはコンシューマ・ノードのエントリ自身のみをサプライヤ・ノードからの指定されたエントリと置換します。

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 であることを示す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。

ディレクトリの同期とプロビジョニングのコマンドライン・ツール

この項では、次の項目について説明します。

- oidmuplf.sh ツール
- oidmcrep.sh ツール
- oidmdelp.sh ツール
- stopodis.sh ツール
- schemasync ツール
- プロビジョニング・サブスクリプション・ツール

oidmuplf.sh ツール

ディレクトリを同期化するときに、oidmuplf.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。

```
oidmuplf.sh -name  Profile_Name
    -config which_configset_the_profile_is_associated_with
    -host  <LDAP Server host
    -port  <LDAP server port
    -binddn  < Dn that can modify the profile  ( default  = cn=orcladmin)
    -bindpass <  password to the binddn ( default = welcome)
    -attrtype  <  "MAP" / "ATTR"
    -filename < Complete path name of the file to be uploaded
```

表 A-1 oidmuplf.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。
host	ディレクトリ・サーバーのホスト。
port	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。
Bindpass	バインド識別名に対応するパスワード。
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。

関連項目： oidmuplf.sh を使用する場合については、第 28 章「Oracle Directory Synchronization Service」を参照してください。

oidmcrep.sh ツール

コマンドライン・ツールの oidmcrep.sh を使用すると、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。このツールの構文は次のとおりです。表 A-2 は、このツールの引数を示しています。

```
oidmcrep.sh -name profile_name \
[ -type [IMPORT | EXPORT ] [ -agentpwd connector_password ] \
[ -config configset_to_associate_with_this_profile ] \
[ -host directory_server_host ] \
[ -port directory_server_port ] \
[ -binddn super_user_dn (default cn=orcladmin ) ] \
[ -bindpass   bind_password (default=welcome) ] \
[ -retry   max_retry_count_on_synchronization_errors > ]\
[ -poll polling_interval_for_synchronization ] \
[ -conndirurl  connected_directory_url] \
[ -conndiracct connected_directory_acct_info > ]\
[ -conndirpwd connected_directory_account_password ] \
[ -execmd command_line_for_connector ]\
[ -iftype interface_type]      \
[ -condirfilter connected_directory_matching_filter ]\
[ -oidfilter oid_matching_filter ] \
[ -U ssl_authentication_mode> ]\
[ -W wallet_location ]   [ -P wallet_password ]
```

表 A-2 oidmcrep.sh 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。
host	ディレクトリ・サーバー・ホスト。デフォルトは現行のホストです。
port	ディレクトリ・サーバー・ポート。デフォルト・ポートは 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。
Poll	プロファイルのスケジューリング間隔（秒単位）。デフォルトは 60 です。
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	コネクタを実行するためのオペレーティング・システム・コマンド。
Iftype	インタフェース型。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	Oracle Internet Directory の照合フィルタ。

統合サーバーが、このコマンドライン引数の構成設定 2 を使用して起動されると、このコネクタが実行されます。詳細は、-help 引数で oidmcrep.sh を起動してください。

oidmdelp.sh ツール

同期プロファイルは、コマンドライン・ツール oidmdelp.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。

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。

```
oidmdelp.sh name HRMS config 2
```

stopodis.sh ツール

OID モニターおよび OID 制御ユーティリティが使用できないクライアントのみのインストールでは、oidctl ツールを使用せずに Directory Integration Server を起動できます。サーバーを停止するには、stopodis.sh ツールを使用します。

このツールのパス名は、*$ORACLE_HOME*/ldap/admin/stopodis.sh です。

使用方法は次のとおりです。

```
$ORACLE_HOME/ldap/admin/stopodis.sh
        [ -host directory_server_host ]
        [ -port LDAP_server_port ]
        [ -binddn super_user_dn (default cn=orcladmin ) ]
        [ -bindpass   bind_password (default=welcome) ]
        -instance instance_number_to_stop
```

表 A-3 stopodis.sh の引数

引数	説明
host	LDAP サーバー・ホスト。デフォルトは現行のホストです。
port	LDAP 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。
instance	停止する DIP サーバー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 1.0。サイト：`http://sources.redhat.com/cygwin/`
- MKS Toolkit 5.1 または 6.0。
  サイト：`http://www.datafocus.com/products/`

---

schemasync ツール

schemasync 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

プロビジョニング・サブスクリプション・ツール

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、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、使用可能な状態に設定されるため、Oracle Directory Integration Platform で処理することができます。
- 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 1.0。サイト：http://sources.redhat.com/cygwin/
- MKS Toolkit 5.1 または 6.0。
  サイト：http://www.datafocus.com/products/

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-4 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	操作	必須 / オプション	説明
operation	すべて	必須	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。
ldap_host	すべて	オプション	サブスクリプション操作を実行する LDAP 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。
ldap_port	すべて	オプション	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。
ldap_user_dn	すべて	必須	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。
ldap_user_password	すべて	必須	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。
application_dn	すべて	必須	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。
organization_dn	すべて	必須	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。

表 A-4 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	操作	必須 / オプション	説明
interface_name	作成のみ	必須	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。
interface_type	作成のみ	オプション	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）。
interface_connect_info	作成のみ	必須	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。
interface_version	作成のみ	オプション	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。
interface_additional_info	作成のみ	オプション	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。
schedule	作成のみ	オプション	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。
max_retries	作成のみ	オプション	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。
event_subscription	作成のみ	オプション	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。

OID データベース・パスワード・ユーティリティ

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=net_service_name]
```

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=net_service_name` オプションを使用する必要があります。

次のようなコマンドを実行します。

```
$ oidpasswd
current password: ods
new password: newsupersecret
confirm password: newsupersecret
password set.
$
```

注意： ユーザーの入力値は画面に表示されません。

OID データベース統計収集ツール

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。

bulkload 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。

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 1.0。サイト : `http://sources.redhat.com/cygwin/`
- MKS Toolkit 5.1 または 6.0。
  サイト : `http://www.datafocus.com/products/`

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 net_service_name ]
            [ -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` *`net_service_name`*	DB 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方法

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ります。

```
oidstats.sh -cat all -pct 40
```

OID 移行ツール

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 Input_file=my_users.dat" "Output_file=my_users.ldif"
        [-lookup "Host=directoryName"
        ["Port=portnumber"]
        "DN=bindDn"
        ["Password=password"]
        ["Subscriber=subscribername"]]
        {"s_SubVar1=val1" ..."s_SubVarN=valN"  }
```

表 A-5 では、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説明します。

表 A-5 ldifmigrator のパラメータ

パラメータ	必須 / オプション	説明
Input_file	必須	置換変数が含まれるファイル。
Output_file	必須	このツールで生成されるファイルの名前。
-lookup	オプション	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。変数の名前については、次の表を参照してください。ディレクトリ・サーバーの名前は、host パラメータを使用して指定します。-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	オプション	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	オプション	バインド・パスワード。
Subscriber	オプション	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・サブスクライバが使用されます。
s_SubsVar1..N	オプション	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-6 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、サブスクライバ固有の 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、サブスクライバ固有の 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%	サブスクライバのユーザー・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、サブスクライバ固有の 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%	サブスクライバに対応する 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、orclSubscriberSearchBase 属性と orclSubscriberNickName 属性を使用し、ルート Oracle コンテキストにある cn=Common,cn=Products のエントリから、そのサブスクライバ名を識別名に解決します。
%s_SubscriberOracleContextDN%	サブスクライバ固有の Oracle コンテキストの識別名。	最初にサブスクライバ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。

表 A-6 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_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。
%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

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
```

参照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。

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
```

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。

メッセージ	原因	対処方法
環境変数 *ORACLE_HOME* が設定されていません	*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のエラー。再確認してください。	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` 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` 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` 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。
入力ファイルをチェックしてください。入力ファイルは 0 バイトです。	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。出力ファイルは既に存在します。	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ホスト・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。

メッセージ	原因	対処方法
バインド DN パラメータが指定されていません。-lookup オプションを使用するときは 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（ホスト、ポート、DN、パスワード）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。入力パラメータを指定してください。	指定されたサブスクライバがディレクトリに存在しません。	subscriber 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。	サブスクライバ・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。	ディレクトリ内のサブスクライバ・エントリをチェックしてください。
LDIF データの OID へ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

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。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 をバッカス正規形で記述すると、次のようになります。

```
<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> ::= | BindMode = Simple
               | BindMode = SSLNoauth
               | BindMode = SSLOneway
               | BindMode = SSLTwoway

<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> )]+
```

C

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のスキーマ要素を簡単に説明します。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）
- `http://www.ietf.org/html.charters/ldapext-charter.html`（ldapext の Charter と LDAP Draft）
- `http://www.ietf.org/html.charters/ldup-charter.html`（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 で施行されている IETF Draft
- Oracle Internet Directory 独自のスキーマ要素
- LDAP 構文
- 一致規則
- ユーザーを表現するスキーマ

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）が施行されています。

RFC	タイトル	URL
1777	Lightweight Directory Access Protocol	`http://www.ietf.org/rfc/rfc1777.txt`
1778	The String Representation of Standard Attribute Syntaxes	`http://www.ietf.org/rfc/rfc1778.txt`
1779	A String Representation of Distinguished Names	`http://www.ietf.org/rfc/rfc1779.txt`
1960	A String Representation of LDAP Search Filters	`http://www.ietf.org/rfc/rfc1960`
2079	Definition of an X.500 Attribute Type and an Object Class to Hold Uniform Resource Identifiers (URIs)	`http://www.ietf.org/rfc/rfc2079.txt`
2247	Using Domains in LDAP/X.500 Distinguished Names	`http://www.ietf.org/rfc/rfc2247.txt`
2251	Lightweight Directory Access Protocol (v3)	`http://www.ietf.org/rfc/rfc2251.txt`
2252	Lightweight Directory Access Protocol (v3):Attribute Syntax Definitions	`http://www.ietf.org/rfc/rfc2252.txt`
2253	Lightweight Directory Access Protocol (v3):UTF-8 String Representation of Distinguished Names	`http://www.ietf.org/rfc/rfc2253.txt`
2254	The String Representation of LDAP Search Filters	`http://www.ietf.org/rfc/rfc2254.txt`
2255	The LDAP URL Format	`http://www.ietf.org/rfc/rfc2255.txt`
2256	A Summary of the X.500(96) User Schema for use with LDAP v3	`http://www.ietf.org/rfc/rfc2256.txt`

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 が施行されています。

Draft: "Definition of the inetOrgPerson LDAP Object Class"

URL: `http://ietf.org/rfc/rfc2798.txt`

Draft: "Referrals and Knowledge References in LDAP Directories"

URL: `http://www.ietf.org/proceedings/99nov/I-D/draft-ietf-ldapext-knowledge-00.txt`

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
- レプリケーション
- Oracle Internet Directory の構成
- SSL
- 監査ログ
- 構成設定エントリの属性

この他に、Oracle Internet Directory のインストレーションには、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

属性	`orclEntryLevelACI`、`orclACI`
オブジェクト・クラス	`orclPrivilegeGroup`

レプリケーション

属性	`orclGUID`、`changeNumber changeType`、`changes`、`orclParentGUID`、`server`、`supplier`、`consumer`、`orclReplBindDN`、`orclReplBindPassword`、`changeLog`、`changeStatus`、`orclChangeRetryCount`、`orclPurgeSchedule`、`orclDirReplGroupAgreement`、`orclAgreementId`、`orclSupplierReference`、`orclConsumerReference`、`orclReplicationProtocol`、`orclUpdateSchedule`、`targetDN`、`orclExcludedNamingcontexts`、`orclDirReplGroupDSAs`
オブジェクト・クラス	changeLogEntry、changeStatusEntry、orclReplAgreementEntry

Oracle Internet Directory の構成

属性	orcldebugflag、orclMaxCC、orclDBType、orclSuffix、orclDITRoot、orclSuName、orclSuPassword、orclSizeLimit、orclTimeLimit、orclGuName、orclGuPassword、orclServerProcs、orclconfigsetnumber、orclhostname、orclIndexedAttribute、orclCatalogEntryDN、orclServerMode、orclPrName、orclPrPassword、orclUseEncrypt、orclDirectoryVersion
オブジェクト・クラス	subconfig、orclConfigSet、orclLDAPSubConfig、orclREPLSubConfig、orclcontainerOC、subregistry、orclLDAPInstance、orclREPLInstance、orclIndexOC、orcleventLog、orclEvents

SSL

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。

属性	orclsslAuthentication、orclsslEnable、'orclsslWalletURL、orclsslWalletPasswd、orclsslPort、orclsslVersion

監査ログ

属性	orclServerEvent、orcleventtype、orclauditattribute、orclauditmessage、orcleventtime、orcluserdn、orclSequence、orclAuditLevel、orclOpResult
オブジェクト・クラス	OrclAuditOC

構成設定エントリの属性

次の表は、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をリストし、その説明を示しています。

パラメータ	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 ～ 65535 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 を使用可能にするかどうかを切り替えるフラグ。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、このフラグを切り替えることができます。次の 2 つの値のいずれかを使用できます。 ■ 0 = SSL 使用禁止（構成設定 0 のデフォルト） ■ 1 = SSL 使用可能 デフォルトは 0（ゼロ）です。
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 = SSL 認証なし ■ 32 = SSL サーバー認証（サーバーがクライアントに証明書を送信します） ■ 64 = 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、証明書を交換します）

パラメータ	説明

orclsslwalleturl	Oracle Wallet の位置を設定します。この値は、Wallet の作成時に設定済みです。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 Solaris では、このパラメータは次のように設定します。
	`orclsslwalleturl=file:///Home/my_dir/`
	Windows NT では、このパラメータは次のように設定します。
	`file:Home¥my_dir¥`

orclsslwalletpasswd	Wallet をオープンするためにサーバーが使用するパスワード。この値は、Wallet の作成時に設定済みです。Wallet のパスワードを変更する場合は、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 のパスワードを設定する必要があります。
orclsslversion	SSL のバージョン。デフォルトは 3 です。

関連項目：

- デバッグ・レベルの詳細は、5-26 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に関する情報は、『Oracle Advanced Security 管理者ガイド』を参照してください。

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 が認識する、一般的に使用されている LDAP 構文
- Oracle Internet Directory が認識する、その他の LDAP 構文
- 属性値のサイズ

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、一般的に使用されている 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
Boolean
Certificate
Directory String
DN
Facsimile Telephone Number
INTEGER
JPEG
Name And Optional UID
Numeric String
Object Class Description
Octet String
OID
Presentation Address
Printable String
Telephone Number
UTC Time

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
ACI Item
Audio
Binary
Bit String
Certificate List
LDAP Schema Description
LDAP Syntax Description
Mail Preference
Master And Shadow Access Points
Matching Rule
Matching Rule Use Description

Certificate Pair
Country String
Data Quality Syntax
Delivery Method
DIT Content Rule Description
DIT Structure Rule Description
DL Submit Permission
DSA Quality Syntax
DSE Type
Enhanced Guide
Fax
Generalized Time
Guide
IA5 String
LDAP Schema Definition
MHS OR Address
Modify Rights
Name Form Description
Object Class Description
Octet String
Other Mailbox
Postal Address
Protocol Information
Substring Assertion
Subtree Specification
Supplier And Consumer
Supplier Information
Supplier Or Consumer
Supported Algorithm
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。この RFC は、URL: `http://www.ietf.org/rfc/rfc2251.txt` にあります。

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
bitStringMatch
caseExactMatch
caseExactIA5Match
caseIgnoreIA5Match
caseIgnoreListMatch
caseIgnoreMatch
caseIgnoreOrderingMatch
distinguishedNameMatch
generalizedTimeMatch
generalizedTimeOrderingMatch
IntegerMatch
numericStringMatch
objectIdentifierFirstComponentMatch
ObjectIdentifierMatch
OctetStringMatch
presentationAddressMatch
protocolInformationMatch
telephoneNumberMatch
uniqueMemberMatch

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 C-1 では、属性名を説明します。

表 C-1 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。
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。

表 C-1 ユーザー属性（続き）

属性名	必須またはオプション	説明
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。
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。

表 C-1 ユーザー属性（続き）

属性名	必須またはオプション	説明
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。
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。

D

Oracle Internet Directory のアップグレード

この付録では、Oracle Internet Directory リリース 2.1.1.x または 3.0.1.x から Oracle Internet Directory リリース 9.2.1.0 へのアップグレード方法について説明します。

この付録では、次の項目について説明します。

- 推奨アップグレード手順
- 代替手順 : スタンドアロンの Oracle Internet Directory ノードのアップグレード

推奨アップグレード手順

Oracle Internet Directory をアップグレードするには、Oracle9*i* データベース・サーバー リリース 2（9.2）のオペレーティング・システム固有のインストレーション・ガイドの指示に従ってください。

代替手順 : スタンドアロンの Oracle Internet Directory ノードのアップグレード

次の状況では、スタンドアロンの Oracle Internet Directory ノードのアップグレードは適していません。

- 以前のバージョンの Oracle Internet Directory が存在するマシンに、Oracle Internet Directory リリース 9.2 のインストールとアップグレードに十分なディスク領域がない場合。
- 以前のバージョンの Oracle Internet Directory に大量のデータが存在し、データベースの移行よりも、データをエクスポートまたはインポートする方が適切な場合。

注意 : Oracle Internet Directory ノードがレプリケーションの一部である場合、またはレプリケーション用に構成されている場合は、この手順でノードをアップグレードしないでください。

前述の状況でディレクトリをアップグレードするには、次の各項で説明する手順に従ってください。

- タスク 1: 以前のバージョンのノード上にある Oracle ディレクトリ・サーバーの停止
- タスク 2: エクスポート・ユーティリティを使用したスポンサ・ノードのバックアップ
- タスク 3: インポート・ユーティリティを使用した新規ノードへのデータのロード
- タスク 4: Oracle Internet Directory スキーマのアップグレードの実行

タスク 1: 以前のバージョンのノード上にある Oracle ディレクトリ・サーバーの停止

Oracle ディレクトリ・サーバーを停止するには、ノード上で `$ORACLE_HOME/bin/` から次のコマンドを実行します。

```
oidctl connect=<db_connect_string> server=oidldapd instance=1 stop
```

タスク 2: エクスポート・ユーティリティを使用したスポンサ・ノードのバックアップ

1. `oidexp.dat` という新規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。

```
FILE=oid.data
OWNER=ods, odscommon
GRANTS=y
ROWS=y
```

2. 識別されたスポンサ・ノードに対して、$ORACLE_HOME/bin/ から次のコマンドを実行します。

```
exp system/manager PARFILE=oidexp.dat
```

注意 : OID のスキーマとデータは、oid.data ファイルにバックアップされます。次のタスクを実行する前に、このファイルを新しいノードに移動してください。

タスク 3: インポート・ユーティリティを使用した新規ノードへのデータのロード

1. 次の SQL スクリプトを実行します。

```
cd $ORACLE_HOME/ldap/admin/
sqlplus system/manager @ldapdrop.sql
sqlplus system/manager @ldapxact.sql
sqlplus system/manager @ldapxsec.sql
```

2. `oidimp1.dat` という新規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。

```
FILE=oid.data
FROMUSER=ods
TOUSER=ods
```

3. 新規ノードに対して、次のコマンドを実行します。

```
imp system/manager PARFILE=oidimp1.dat
```

注意 : バックアップ・ファイルの `oid.data` が、現行のディレクトリに格納されていることを確認してください。

---

4. oidimp2.dat という新規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。

```
FILE=oid.data
FROMUSER=odscommon
TOUSER=odscommon
```

5. 新規ノードに対して、次のコマンドを実行します。

```
imp system/manager PARFILE=oidimp2.dat
```

注意 : バックアップ・ファイルの `oid.data` が、現行のディレクトリに格納されていることを確認してください。

タスク 4: Oracle Internet Directory スキーマのアップグレードの実行

1. `$ORACLE_HOME/bin/oidca` を実行して、OID Configuration Assistant を起動します。
2. 「ようこそ」画面で「次」をクリックします。
3. 「既存の OiD のアップグレード」オプションを選択し、「次」をクリックします。
4. 「データベースの移行」画面が表示されます。この画面では、Oracle Internet Directory データがインポートされたデータベースに関する情報の入力を要求されます（新規バージョンの OID)。次の情報を入力します。
   a. データベース SID
   b. データベース・ユーザーに関する SYSTEM パスワードと ODS パスワード
   c. Oracle ホーム
   d. INIT.ORA ファイルの位置
   e. OID データベース用のリスナー・ポート
   f. OID データベース用の接続文字列
5. 「次」をクリックします。（この操作が完了すると、Oracle Internet Directory ベース・スキーマは Oracle Internet Directory リリース 9.0.2.1.0 にアップグレードされます。）
6. 次の画面で、Oracle ディレクトリ・サーバーに関する次の情報を入力します。
   a. ディレクトリ・サーバーを起動する非 SSL ポート。デフォルト値は 389 です。
   b. ディレクトリ・サーバーを起動する SSL ポート。デフォルト値は 636 です。
   c. スーパー・ユーザーの識別名。
   d. 対応するスーパー・ユーザーのパスワード。
7. 「次」をクリックします。次の手順では、Oracle コンテキストと Oracle Directory Integration Platform の関連情報がアップグレードされます。

8. 「Upgrading Subscriber」画面が表示されます。この画面で、組織のルートを識別する識別名を入力する必要があります。たとえば、`o=acme, dc=com` のように入力します。これによって、このドメインがアップグレードされ、デフォルト・サブスクライバになります。
9. 「次」をクリックします。「User Data Migration」画面が表示されます。ディレクトリが大きい場合、この手順は時間がかかる場合があります。ディレクトリが大きい場合（つまり、ユーザー数が 10,000 を超える場合）、データの移行は、インストール後に行うことをお薦めします。
10. ユーザー・データの移行を、この OID Configuration Assistant 操作の一部として行う場合は、「はい」を選択して「次」をクリックします。これで、ユーザー・データの移行が完了しました。

アップグレードの最後に、ディレクトリ・サーバーを実行して、指定の非 SSL ポートと SSL ポートをリスニングします。

アップグレード後のタスク : ユーザー・データの移行

ディレクトリが大きい場合、つまり、エントリが 10,000 を超える場合、ユーザー・データの移行はアップグレード後に行うことをお薦めします。

1. ldapsearch を使用して、暗号化されたユーザー・パスワードをすべてファイルに出力します。

```
ldapsearch -L -h OID_host_name -p OID_Non-SSL_port -D OID_Super_User_DN -w OID_
Super_User_Password  -b "" -s sub "objectclass=*" dn userpassword
    $ORACLE_HOME/ldap/install/pwdin.ldif
```

2. passwordconvert ツールを使用して、ファイル `$ORACLE_HOME/ldap/install/pwdin.ldif` 内のユーザー・パスワードを、16 進数から BASE64 に変換します。

```
passwordconvert -m hex2base64 -f modify
$ORACLE_HOME/ldap/install/pwdin.ldif
$ORACLE_HOME/ldap/install/pwdout.ldif
```

3. ldapmodify を使用して、ファイル `$ORACLE_HOME/ldap/install/pwdout.ldif` 内の BASE64 でエンコードされたユーザー・パスワードを、ディレクトリ・サーバーにアップロードします。

```
ldapmodify -h OID_host_name  -p ID_Non-SSL_port -D ID_Super_User_DN  -w ID_
Super_User_Password -f $ORACLE_HOME/ldap/install/pwdout.ldif.
```

E

他のディレクトリからのデータの移行

この付録では、LDAP バージョン 3 互換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。

この付録では、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

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
- 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

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：** LDIF の技術的な仕様は、`http://www.ietf.org/rfc/rfc2849.txt` からダウンロードできます。

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
- E-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-52 ページの「schemasync ツール」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 リリース 9.2 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。

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 1.0。サイト：`http://sources.redhat.com/cygwin/`
- MKS Toolkit 5.1 または 6.0。
  サイト：`http://www.datafocus.com/products/`

関連項目： bulkload のチェック・モードの使用方法は、A-37 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。

この移行を実行するため、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します。これは、純粋な LDIF ファイルではありません。このテンプレート・ファイルのレコードは LDIF のフォーマットですが、置換変数を伴います。この置換変数はディレクトリ管理者が後の処理で定義する変数で、アプリケーション自体では未定義のままです。この変数は、情報を最終的に格納するディレクトリの場所などに関連があります。

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. （LDIF）テンプレート・ファイルを作成します。
2. ディレクトリ管理者は、OID 移行ツールを使用して、不完全な LDIF エントリをテンプレート・ファイルから読み込み、配置の選択に基づいて実際の LDIF エントリに変換します。
3. ディレクトリ管理者は、この 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。

アプリケーション固有のリポジトリからデータを移行するためのタスク

OID 移行ツールは、次のいずれかのモードで実行できます。

- 簡易モード。このモードでは、置換変数のすべての値を指定します。
- 参照モード。このモードでは、OID 移行ツールがディレクトリを検索して特定の置換変数の値を判別します。

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。

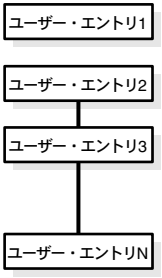
タスク 1: 中間テンプレート・ファイルの作成

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/rfc/rfc2849.txt` で、IETF の RFC 2849「The LDAP Data Interchange Format (LDIF) - Technical Specification（LDAP Data Interchange Format（LDIF）－ 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・セパレータで、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 移行ツールは、デフォルト・サブスクライバ（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 E-1 は、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ています。

図 E-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、$*SRCHOME*/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 E-1 は、ユーザー・エントリの必須属性のリストと説明です。

表 E-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は、必ず cn になります。
sn	ユーザーの姓。
objectclass	エントリが最低限、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。

inetOrgPerson 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。

orclGuid
userPassword
telephoneNumber
seeAlso
description
title
x121Address
registeredAddress
destinationIndicator
preferredDeliveryMethod
telexNumber
teletexTerminalIdentifier
internationaliSDNNumber
facsimileTelephoneNumber
street
postOfficeBox
postalCode
postalAddress
physicalDeliveryOfficeNameou
st
l
audio
businessCategory
carLicense
departmentNumber
displayName
employeeNumber
employeeType
givenName
homePhone
homePostalAddress
initials
jpegPhoto
labeledURI
mail
manager
mobile
pager
photo
preferredLanguage
roomNumber
secretary
uid
userCertificate
x500UniqueIdentifier
userSMIMECertificate
userPKCS12

関連項目： このオブジェクト・クラスの各属性については、http://www.ietf.org/rfc/rfc2798.txt?number=2798 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。

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 E-2 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 と同じような、カスタム認証スキームに対する Oracle 固有のパスワード識別子です。
OrclHireDate	従業員が企業またはサブスクライバ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。
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。

表 E-2 orclUserV2 オブジェクト・クラスの属性（続き）

属性	説明
`orclActiveStartDate`	ユーザーが Oracle9*i*AS Single Sign-On Server に対して正常に認証を開始できる日付。値は、協定世界時の書式で表します。
`orclEnddate`	ユーザーが Oracle9*i*AS Single Sign-On Server に対して認証が不可能になる日付。値は、協定世界時の書式で表します。

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。同期化は、Oracle Directory Synchronization Service または Oracle Directory Provisioning Integration Service のいずれかを使用して実行します。

> **関連項目：** OID 移行ツールの使用方法は、A-58 ページの「OID 移行ツール」を参照してください。

F

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）の許可を得て転載されています。この文書は、次の URL で閲覧できます。

`http://www.ietf.org/rfc/rfc2254.txt`

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
RFC:2254　　Netscape 社
種類 : 標準化過程　　1997 年 12 月

LDAP 検索フィルタの文字列表現

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、読込み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、十分な認証方法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. 読込み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

必要な認証方法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

ただし、インターネット標準化過程に定義されている著作権の手続きに従って、インターネット標準を開発するために必要な場合、または RFC を英語以外の言語に翻訳する必要がある場合はその限りではありません。

この制限付き許可は永続的なものであり、インターネット・ソサエティまたはその継承者や譲渡者によって取り消されることはありません。

この文書とこの文書に含まれている情報は現状のままで提供され、インターネット・ソサエティおよび IETF による、いかなる明示的または暗黙的な保証も行われせん。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。

G

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・サーバーをインストールおよび構成するときには、キャラクタ・セット UTF-8 を選択する必要があります。他のキャラクタ・セットを選択すると、ディレクトリ・サーバーが正しく機能しません。

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・メッセージをリストします。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。

この項では、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

次にリストされているメッセージは、標準のエラー・メッセージです。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、G-6 ページの「その他のエラー・メッセージ」にリストされています。

00: 成功しました

原因 : 操作が正常に完了しました。

01: 操作エラー

原因 : 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。

02: プロトコル・エラー

原因 : 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 資格証明の読込み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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : サーバーから参照が戻されました。

10: LDAP 参照エラー

原因 : サーバーから参照が戻されました。

11: LDAP 管理制限エラー

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 指定した属性の型が、スキーマ内で定義されていません。

18: 一致しません。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 現在、Oracle Internet Directory はこのメッセージを戻しません。

65: オブジェクト・クラス違反です。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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

原因 : 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。

原因 : 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

原因 : 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

原因 : 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

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : メモリー不足です。

その他のエラー・メッセージ

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。(*string* には文字列が入ります)

***string* 属性が見つかりません。**

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 削除操作に指定した識別名が見つかりません。

変更対象のエントリが見つかりません。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

一致規則 < パラメータ > が定義されていません。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 親エントリが存在していません。(ldapadd および ldapmodifydn)

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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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。

原因 : 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

表 G-1 は、パスワード・ポリシー違反が生じた結果、クライアントに送信されるエラー・メッセージを示しています。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 G-1 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。
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。

表 G-1 パスワード・ポリシー違反のエラー・メッセージ（続き）

エラー番号	例外	コメントまたは解消方法
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。

用語集

ACI

「アクセス制御情報アイテム（Access Control Information Item: ACI）」を参照。

ACL

「アクセス制御リスト（Access Control List: ACL）」を参照。

ACP

「アクセス制御ポリシー・ポイント（Access Control Policy Point: ACP）」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（configuration set entry）」を参照。

Delegated Administration Service

Delegated Administration Service ユニットと呼ばれる個々の事前定義済み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。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る。

DES

データ暗号化規格。1970 年代に IBM 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（directory information base: DIB）**」を参照。

Directory Integration Server

Oracle Directory Integration Platform 環境で、Oracle Internet Directory と**接続ディレクトリ（connected directory）**との間でデータの同期化を実行するサーバー。

DIS

「**Directory Integration Server**」を参照。

DIT

「**ディレクトリ情報ツリー（directory information tree: DIT）**」を参照。

DN

「**識別名（distinguished name: DN）**」を参照。

DRG

「**ディレクトリ・レプリケーション・グループ（directory replication group: DRG）**」を参照。

DSA

「**ディレクトリ・システム・エージェント（directory system agent: DSA）**」を参照。

DSE

「**ディレクトリ固有のエントリ（directory-specific entry: DSE）**」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）

マルチマスター・レプリケーション環境では、複数のノードでレプリケートされるエントリは、各ノードで同じ識別名を持つ。ただし、識別名が同じでも、各ノードで異なる GUID が割り当てられる。たとえば、同じ識別名を node1 と node2 の両方でレプリケートできるが、node1 に常駐しているときのその識別名に対する GUID は、node2 におけるその識別名に対する GUID とは異なる。

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 クライアントとサーバーが通信で使用する共通言語。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（master definition site: MDS）**」を参照。

MTS

「**共有サーバー（shared server）**」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（OID Monitor）**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 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 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 Integration Server（DIS）

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（directory integration profile）**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 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、共通のサービスおよびツールを組み合せ、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 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、拡張性、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（Oracle PKI certificate usages）

証明書（certificate）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における公開鍵の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* レプリケーション（Oracle9*i* 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。

PKCS #12

公開鍵暗号（public-key encryption）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。

RDN

「**相対識別名（relative distinguished name: RDN）**」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 よりも若干遅いが、メッセージ・ダイジェスト値が大きくなることで、総当り攻撃や反転攻撃に対してより強力に保護できる。

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（System Global Area: SGA）**」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、後続のプロトコル対話に使用するセキュリティ・レイヤーを取り決め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（subentry）**。

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。

Trustpoint

「**信頼できる証明書（trusted certificate）**」を参照。

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。

アクセス制御情報アイテム（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（directory information tree: DIT）**内の下位エントリすべてに適用される。

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 レプリケーション（Oracle9i Replication）**」を参照。

アドバンスト・レプリケーション（ASR）

「**Oracle9i レプリケーション（Oracle9i Replication）**」を参照。

暗号化（cryptography）

データのエンコーディングとデコーディングを行い、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）に変換するプロセス。

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。

一方向関数（one-way function）

一方向への計算は容易だが、逆の計算、すなわち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（one-way function）**。

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、他の複数の企業による Oracle コンポーネントの使用を可能にして、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、特定のサブスクライバ・ドメインで、または特定のアプリケーションについてのロールを持つ。

インスタンス（instance）

「**ディレクトリ・サーバー・インスタンス（directory server instance）**」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（import agent）**によってインポートされたデータを格納するファイル。

エージェント（agent）

「**ディレクトリ統合エージェント（directory integration agent）**」を参照。

エージェント・プロファイル（agent profile）

Oracle Directory Integration Platform 環境で、次の内容を指定する Oracle Internet Directory のエントリ。

- 統合エージェントの構成パラメータ
- 接続ディレクトリと Oracle Internet Directory との間の同期化に適用するマッピング・ルール

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（export agent）**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（export data file）**」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（authentication）**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 Server に依存しないディレクトリ統合エージェント。Oracle Directory Integration 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（public key）とそれに対応する**秘密鍵（private key）**のペア。

「**公開鍵と秘密鍵のペア（public/private key pair）**」を参照。

拡張性（scalability）

限定された使用可能なハードウェア・リソースに比例したスループットを提供するシステム機能。

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。

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、他の複数の企業による Oracle コンポーネントの使用を可能にして、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）

公開鍵暗号における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（directory information base: DIB）**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（naming context）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（superclass）**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（supertype）**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（consumer）**・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で、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情報。

「**ナレッジ参照（knowledge reference）**」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 Server** の制御下で実行される**エージェント（agent）**。

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で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（certificate authority: CA）**）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（subclass）**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（subtype）**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体。

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供給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（knowledge reference）**。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（consumer）**」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（object class）**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 Platform 環境では、Oracle Internet Directory が**中央ディレクトリ（central directory）**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（certificate）**とその関連する**秘密鍵（private key）**が含まれる **PKCS #12** 形式の **Wallet**。**公開鍵（public key）**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 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）

エントリの識別名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（directory information tree: DIT）**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（directory integration profile）**。

ディレクトリ統合エージェント（directory integration agent）

Oracle Directory Integration Platform 環境で、接続ディレクトリと Oracle Internet Directory との間の変更を同期化するために、接続ディレクトリとの対話を行うプログラム。

ディレクトリ統合プロファイル（directory integration profile）

Oracle Directory Integration Platform 環境で、Oracle Directory Integration Platform が外部システムとどのように通信し、何を通信するかを示す 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（naming context）**」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 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（directory integration profile）**。

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・サーバーの集まり。

デフォルト・サブスクライバ（default subscriber）

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、他の複数の企業による Oracle コンポーネントの使用を可能にして、その情報を格納する。このようにホスティングされた環境では、ホスティングを行う企業はデフォルト・サブスクライバと呼ばれ、ホスティングされる企業はサブスクライバと呼ばれる。

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（knowledge reference）**。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。

統合エージェント（integration agent）

「**エージェント（agent）**」を参照。

同時クライアント（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。

同時操作（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。

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。

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（knowledge reference）**（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）

異なるタイプの **RDN** の値を保持する特別な属性。ネーミング属性は、そのニーモニック・ラベル（通常 cn、sn、ou、o、c など）で識別できる。たとえば、ネーミング属性 c は、ネーミング属性 country（国）のニーモニックで、特定の国の値に対応する相対識別名が保持されている。

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 または 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）

障害の認識とリカバリのプロセス。

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（directory integration profile）」を参照。

並行性（concurrency）

複数の要求を同時に処理できる機能。並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。

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（connected directory）**の属性との間のマッピングを指定するファイル。

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。

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（master definition site: MDS）**以外のサイトで、Oracle9*i* レプリケーション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（root directory specific entry）**」を参照。

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（directory server instance）**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（directory replication group: DRG）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。

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

み

め

ゆ

よ

り

る

れ

ろ

わ