Oracle® Internet Directory

管理者ガイド

10*g*（10.1.4.0.1）

部品番号 : B31507-01

2006 年 9 月

ORACLE®

Oracle Internet Directory 管理者ガイド , 10*g*（10.1.4.0.1）

部品番号 : B31507-01

原本名 : Oracle Internet Directory Administrator's Guide, 10*g* (10.1.4.0.1)

原本部品番号 : B15991-01

原本著者 : Ellen Desmond

原本協力者 : Vasuki Ashok, Neelima Bawa, Tridip Bhattacharia, Jingjing Wei, Kamalendu Biswas, , Ramakrishna Bollu, Margaret Chou, Quan Dinh , Sriram Ganesan, Rajinder Gupta, Ajay Keni, Ashish Kolli, Buddhika Kottahachchi,, Karen Lee, Stephen Lee, David Lin, Andrew Maywah, Hari Sastry, Ramaprakash Sathyanarayan, Gurudatt Shakshikumar, Amit Sharma, Daniel Shih, Saurabh Shrivastava, Olaf Stullich, Dipankar Thakuria, Satishkumar Venkatasamy, Jingjing Wei, Quan Zhou

目次

2 LDAP および Oracle Internet Directory の概要

3 ディレクトリの概念およびアーキテクチャ

4 インストール後に実行するタスクと情報

5 ディレクトリ管理および監視ツール

6 Oracle Internet Directory のプロセス制御コンポーネント

第 II 部　基本的なディレクトリ管理

7 Oracle ディレクトリ・サーバーの管理

8 ディレクトリ・エントリの管理

9 バルク・ツールの使用方法

10 ディレクトリの属性一意性

11 ディレクトリ・スキーマの管理

12 参照整合性

13 Oracle Internet Directory の静的グループと動的グループ

14 ディレクトリのロギング、監査および監視

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

20 パスワード・ベリファイアのディレクトリ格納

21 Oracle テクノロジ配置のための権限の委任

第 IV 部　ディレクトリの配置

22 ディレクトリ配置の考慮事項

23 Oracle Identity Management レルムの配置

24 ディレクトリの容量計画

25 ディレクトリのチューニングに関する考慮事項

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

27 他のデータ・リポジトリからのデータの移行

28 サーバー・チェーン

第 V 部　ディレクトリ・レプリケーション

29　Oracle Internet Directory レプリケーションの概要

30 Oracle Internet Directory レプリケーションのインストールと構成

31 Oracle Internet Directory レプリケーションの監視および管理

第 VI 部　ディレクトリ・プラグイン

32　Oracle Internet Directory サーバー・プラグイン・フレームワーク

33　Oracle Internet Directory のパスワード・ポリシー・プラグイン

34　カスタマイズされた外部認証プラグインの設定

第 VII 部　付録

A　Oracle Directory Manager のウィンドウとフィールド

E　ユーザーおよびグループの作成ベースおよび検索ベースに対するアクセス制御の設定

F　マルチマスター・レプリケーション・プロセス

G　ディレクトリでのユーザー証明書の検索

H　LDAP のレプリカ状態

I　データベース・コピー・プロシージャを使用したディレクトリ・ノードの追加

J　Oracle Internet Directory を使用した UNIX 認証およびユーザー・プロビジョニング

K　Oracle Internet Directory でサポートされている RFC

L　Oracle Internet Directory に関するトラブルシューティング

図一覧

表一覧

はじめに

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

「はじめに」の項目は次のとおりです。

対象読者

『Oracle Internet Directory 管理者ガイド』は、Oracle Internet Directory の管理タスクを実行するすべての管理者を対象としています。管理者は、コマンドライン・モードのコマンドや例を理解するために、UNIX オペレーティング・システムまたは Microsoft Windows オペレーティング・システムのどちら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 をある程度理解している必要があります。**

ドキュメントのアクセシビリティについて

オラクル社は、障害のあるお客様にもオラクル社の製品、サービスおよびサポート・ドキュメントを簡単にご利用いただけることを目標としています。オラクル社のドキュメントには、ユーザーが障害支援技術を使用して情報を利用できる機能が組み込まれています。HTML 形式のドキュメントで用意されており、障害のあるお客様が簡単にアクセスできるようにマークアップされています。標準規格は改善されつつあります。オラクル社はドキュメントをすべてのお客様がご利用できるように、市場をリードする他の技術ベンダーと積極的に連携して技術的な問題に対応しています。オラクル社のアクセシビリティについての詳細情報は、Oracle Accessibility Program の Web サイト `http://www.oracle.com/accessibility/` を参照してください。

ドキュメント内のサンプル・コードのアクセシビリティについて

スクリーン・リーダーは、ドキュメント内のサンプル・コードを正確に読めない場合があります。コード表記規則では閉じ括弧だけを行に記述する必要があります。しかし JAWS は括弧だけの行を読まない場合があります。

外部 Web サイトのドキュメントのアクセシビリティについて

このドキュメントにはオラクル社およびその関連会社が所有または管理しない Web サイトへのリンクが含まれている場合があります。オラクル社およびその関連会社は、それらの Web サイトのアクセシビリティに関しての評価や言及は行っておりません。

Oracle サポート・サービスへの TTY アクセス

アメリカ国内では、Oracle サポート・サービスへ 24 時間年中無休でテキスト電話（TTY）アクセスが提供されています。TTY サポートについては、(800)446-2398 にお電話ください。

関連ドキュメント

詳細は、次の Oracle ドキュメントを参照してください。

- Oracle Directory Manager、Oracle Internet Directory の Single Sign-On コンソールおよび Oracle Enterprise Manager 10*g* を介して使用可能なオンライン・ヘルプ。
- Oracle Application Server および Oracle Database 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 Identity Management 概要および配置プランニング・ガイド』
  - 『Oracle Identity Management 統合ガイド』
  - 『Oracle Identity Management 委任管理ガイド』
  - 『Oracle Identity Management アプリケーション開発者ガイド』
  - 『Oracle Application Server Single Sign-On 管理者ガイド』
  - 『Oracle Application Server Certificate Authority 管理者ガイド』
  - 『Oracle Identity Management ユーザー・リファレンス』
  - 『Oracle Application Server 高可用性ガイド』
  - 『Oracle Application Server 管理者ガイド』
  - 『Oracle Database 管理者ガイド』
  - 『Oracle Database Net Services 管理者ガイド』
  - 『Oracle Database Oracle Clusterware および Oracle Real Application Clusters 管理およびデプロイメント・ガイド』
  - 『Oracle Database アドバンスト・レプリケーション』
  - 『Oracle Advanced Security 管理者ガイド』

詳しい情報は、次のドキュメントを参照してください。

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

表記規則

本文では、次の表記規則を使用します。

規則	意味
太字	太字は、操作に関連するグラフィカル・ユーザー・インタフェース要素、または本文中で定義されている用語および用語集に記載されている用語を示します。
イタリック	イタリックは、特定の値を指定するプレースホルダ変数を示します。
固定幅フォント	固定幅フォントは、パラグラフ内のコマンド、URL、例に記載されているコード、画面に表示されるテキスト、または入力するテキストを示します。

サポートおよびサービス

次の各項に、各サービスに接続するための URL を記載します。

Oracle サポート・サービス

オラクル製品サポートの購入方法、および Oracle サポート・サービスへの連絡方法の詳細は、次の URL を参照してください。

```
http://www.oracle.co.jp/support/
```

製品マニュアル

製品のマニュアルは、次の URL にあります。

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

研修およびトレーニング

研修に関する情報とスケジュールは、次の URL で入手できます。

```
http://www.oracle.co.jp/education/
```

その他の情報

オラクル製品やサービスに関するその他の情報については、次の URL から参照してください。

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

注意： ドキュメント内に記載されている URL や参照ドキュメントには、Oracle Corporation が提供する英語の情報も含まれています。日本語版の情報については、前述の URL を参照してください。

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。この章の項目は次のとおりです。

Oracle Internet Directory 10*g*（10.1.4.0.1）で導入された新機能

- **手順情報へのリンク :** このドキュメントには、重要なタスクへのリンクの表が含まれています。第 1 章「一般的タスクへのリンク」を参照してください。
- **Identity Management Grid Control Plug-in:** この新しいインタフェースにより、Oracle Enterprise Manager 10*g* Grid Control コンソールの機能を使用して、Oracle Internet Directory、Oracle Application Server Single Sign-On、Oracle Delegated Administration Services および Oracle Directory Integration Platform の監視と管理ができます。

  関連資料 :『Oracle Identity Management 概要および配置プランニング・ガイド』の「Identity Management Grid Control Plug-in」

- **改良されたバルク・ツール :** 次のバルク・ツールが、C 言語実行可能ファイルに変換されました。
  - `bulkload`
  - `bulkmodify`
  - `bulkdelete`
  - `catalog`
  - `ldifwrite`

  このマニュアルと『Oracle Identity Management ユーザー・リファレンス』の例や説明は、これらのツールの新機能を反映するために更新されました。

  関連資料 :

  第 9 章「バルク・ツールの使用方法」

  『Oracle Identity Management ユーザー・リファレンス』の Oracle Internet Directory サーバー管理ツールに関する章

- **アプリケーション固有のスキーマ・コンテナ :** Oracle Internet Directory にスキーマを追加する製品は、`cn=subSchemaSubentry` の下に独自の `subSchemaSubentry` を持つことができます。

  関連項目 : 第 11 章「ディレクトリ・スキーマの管理」の「ディレクトリ・スキーマの概要」

- **属性別名のサポート :** 属性名にわかりやすい別名を作成できます。

  関連項目 : 第 11 章「ディレクトリ・スキーマの管理」の「ディレクトリ内の属性別名」

- **動的グループのキャッシング :** 動的グループが追加されると、その動的グループのメンバーが計算され、動的グループを後で変更したときに、メンバー・リストの一貫性が維持されます。

  関連項目 : 第 13 章「Oracle Internet Directory の静的グループと動的グループ」の「動的グループ」

- **ラージ・グループ・エントリ検索の最適化 :** エントリ・キャッシュを無効にせず、エントリ・キャッシュのサイズを増やすことで、検索を最適化するテクニックが加わりました。

  関連項目 : 第 25 章「ディレクトリのチューニングに関する考慮事項」の「大きいグループ・エントリの検索の最適化」

- **参照整合性 :** 参照整合性を有効にした場合、ディレクトリ内のエントリを更新すると、そのエントリを参照する他のエントリもサーバーによって更新されます。

  関連項目 : 第 12 章「参照整合性」

- **サーバー管理を容易にするための新しい監視機能 :** 追加の健全性統計、ユーザー統計およびセキュリティ・イベント追跡を有効にできます。

  関連項目 : 第 14 章「ディレクトリのロギング、監査および監視」の「Oracle Internet Directory サーバーの監視」

- **新しいパスワード・ポリシー機能 :** 任意のサブツリー、または単一エントリにもパスワード・ポリシーを適用できます。選択対象のパスワード・ポリシー属性も増えました。

  関連項目 : 第 19 章「Oracle Internet Directory のパスワード・ポリシー」

- **サーバー・チェーン :** この機能により、サード・パーティの LDAP ディレクトリにあるエントリを、ディレクトリ・ツリーの一部にマップし、同期化やデータの移行なしに、Oracle Internet Directory を介してアクセスできます。

  関連項目 : 第 28 章「サーバー・チェーン」

- **LDAP 検索結果のページングおよびソート :** `ldapsearch` コマンドに、ソート用の `-T` オプションとページング用の `-j` オプションが使用できるようになりました。

  関連資料 :

  『Oracle Identity Management ユーザー・リファレンス』の `ldapsearch` コマンドラインのリファレンス

  『Oracle Identity Management アプリケーション開発者ガイド』の LDAP プロトコルに対する拡張機能に関する章

- **新しいレプリケーション機能 :** Oracle Internet Directory レプリケーションは、次の機能により強化されました。

  - **双方向 LDAP ベース・レプリケーション :** この機能により、ファンアウト・レプリケーション・グループを配置できます。このグループでは、レプリケーションが双方向に流れ、どのノードで更新が行われてもグループ全体にレプリケートされます。
  - **レプリケーション・フェイルオーバー :** あるサプライヤから別のサプライヤへの LDAP レプリカのフェイルオーバーが、管理者の操作によりサポートされます。
  - **Oracle Internet Directory 比較調整ツール :** 機能が改善された新しい `oidcmprec` コマンドが、従来の `oidreconcile` ツールに代わりました。

    関連資料 :

    第 29 章「Oracle Internet Directory レプリケーションの概要」

    第 30 章「Oracle Internet Directory レプリケーションのインストールと構成」

    第 31 章「Oracle Internet Directory レプリケーションの監視および管理」

    『Oracle Identity Management ユーザー・リファレンス』の `oidcmprec` コマンドライン・ツールのリファレンス

- **Java Server プラグイン :** Oracle Internet Directory Plug-in Framework では、Java と PL/SQL で書かれたプラグインをサポートするようになりました。

  関連項目 : 第 32 章「Oracle Internet Directory サーバー・プラグイン・フレームワーク」

Oracle Internet Directory 10*g* リリース 2（10.1.2）で導入された新機能

注意：

次の章は、『Oracle Application Server 高可用性ガイド』に移動しました。

- 「高可用性とフェイルオーバーに関する考慮事項」
- 「Oracle Application Server Cluster（Identity Management）構成」
- 「Oracle Application Server Cold Failover Cluster（Identity Management）」
- 「Oracle Real Application Clusters 環境でのディレクトリ」

次の付録は、『Oracle Identity Management ユーザー・リファレンス』に章として記載されています。

- 「LDIF およびコマンドライン・ツールの構文」
- 「Oracle Internet Directory のスキーマ要素」

- **他のコンポーネントとの改善された統合機能：**新機能では、Oracle Collaboration Suite などのコンポーネントとの統合性が向上しています。これらの機能には、サービスツーサービス認証、サービス・レジストリ、および動的パラメータを使用したベリファイアの生成があります。

  関連項目：

  - 3-24 ページの「サービス・レジストリとサービス・ツー・サービス認証」
  - 20-12 ページの「動的パラメータを使用したベリファイアの生成」

- **証明書の一致規則のサポート：**証明書を使用した外部認証では、完全一致と証明書ハッシュのどちらかの形式を選択できるようになりました。完全一致では、ユーザー認証を行うためにクライアント証明書のサブジェクト DN が使用されます。証明書ハッシュでは、クライアント証明書がハッシュされ、ディレクトリに格納されている証明書ハッシュと比較されます。

  関連項目： 16-4 ページの「直接認証」

- **レプリケーション配置の容易性：**レプリケーションのインストール、構成および管理が非常に簡単になりました。

  関連資料：

  第 30 章「Oracle Internet Directory レプリケーションのインストールと構成」

  Oracle Application Server のインストレーション・ガイド

- **クラスタ配置の容易性：**クラスタ構成のインストール、構成および管理が非常に簡単になりました。

  関連資料：

  『Oracle Application Server 高可用性ガイド』の「Oracle Application Server Cluster（Identity Management）構成」

  Oracle Application Server のインストレーション・ガイド

- Oracle Internet Directory スーパーユーザーに対するアクセス制御の適用：スーパーユーザーも他のユーザーと同様にアクセス制御ポリシーの適用対象になりました。新しい ACL キーワードを使用すると、権限グループを使用してスーパーユーザーのアクセスを制限できます。

関連項目： 第 18 章「ディレクトリ・アクセス制御」

- **Oracle Internet Directory サーバー診断ツール :** OID 診断ツールにより、Oracle Internet Directory で報告される優先順序決定の問題に役立つ診断情報を収集できます。

  関連資料 :『Oracle Identity Management ユーザー・リファレンス』の `oiddiag` コマンドライン・ツールのリファレンス

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

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

  関連資料 :『Oracle Identity Management 統合ガイド』の Microsoft Windows との統合に関する章

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

  関連資料 :

  - 第 34 章「カスタマイズされた外部認証プラグインの設定」
  - 『Oracle Identity Management 統合ガイド』のサード・パーティに接続されたディレクトリとの統合に関する考慮事項の章

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

  関連項目： 第 13 章「Oracle Internet Directory の静的グループと動的グループ」

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

  関連項目： 25-10 ページの「検索の最適化」

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

  関連項目： 第 26 章「Oracle Internet Directory におけるガベージ・コレクション」

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

  関連項目： 16-4 ページの「Oracle Internet Directory での認証」

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

    関連資料 : 第 14 章「ディレクトリのロギング、監査および監視」

- **OID 移行ツール（ldifmigrator）の拡張機能 :** このツールを使用して、データを既存のディレクトリにあるデータと一致させ、Oracle Internet Directory に直接ロードできます。

  関連資料 :
  - 27-9 ページの「ユーザー・データのアプリケーション固有リポジトリからの移行」
  - 『Oracle Identity Management ユーザー・リファレンス』の `ldifmigrator` コマンドライン・ツールのリファレンス

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

  関連資料 :
  - 8-13 ページの「クライアント側の参照キャッシング」
  - 『Oracle Identity Management アプリケーション開発者ガイド』の `ldap_set_option` および `ldap_get_option` に関する記述

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

    関連項目 :
    - 第 29 章「Oracle Internet Directory レプリケーションの概要」
    - 第 30 章「Oracle Internet Directory レプリケーションのインストールと構成」

- **パスワード・ポリシーの拡張機能 :** Oracle Internet Directory のパスワード・ポリシーには、次の新機能があります。
  - パスワード履歴
  - アカウントのロック解除
  - 初回ログイン時におけるパスワード変更の強制
  - アカウント・ロックアウトやパスワードを忘れた場合のパスワードの自己再設定
  - 再設定を要求するスーパーユーザー・アカウントのロックアウト
  - IP ベースのアカウント・ロックアウト

- パスワード・ポリシー・エントリで単一値属性を使用することによるパスワード・ポリシーの有効化または無効化

  関連項目： 第 19 章「Oracle Internet Directory のパスワード・ポリシー」

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

  関連項目： 第 20 章「パスワード・ベリファイアのディレクトリ格納」

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

  関連資料 :『Oracle Identity Management ユーザー・リファレンス』の `remtool` コマンドライン・ツールのリファレンス

- **DNS の使用によるサーバー検出 :** この機能により、分散環境にあるディレクトリ・サーバーの位置を、ドメイン・ネーム・システム（DNS）を使用して動的に検出できます。サーバーの位置情報を、クライアントの `ldap.ora` ファイルに静的に格納するのではなく、その情報を中央のドメイン・ネーム・サーバーに格納し、管理します。クライアントは、リクエストを処理するときに、ドメイン・ネーム・サーバーからこの情報を取得します。
- **バルク・ロード・ツールの拡張機能 :** bulkload を使用して、大量のエントリを空でないディレクトリに追加できるようになりました。たとえば、すでに 100 万件のエントリを持つディレクトリに 100 万件のエントリを追加できます。また、中規模数のエントリを大きなディレクトリに増分的に追加できます。たとえば、すでに 500 万件のエントリを持つディレクトリに、一度に 50,000 件ずつエントリを追加できます。

  関連資料 :『Oracle Identity Management ユーザー・リファレンス』の `bulkload` コマンドライン・ツールのリファレンス

- **Oracle Application Server Cluster（Identity Management）ディレクトリ・サーバー構成のサポート :** この構成は、異なるハードウェア・ノードで複数のディレクトリ・サーバー・インスタンスを実行することにより、ディレクトリ・サーバーの可用性を高めます。ディレクトリ・サーバーは、基礎となる同一のデータ・ストア、すなわち Oracle Database に接続されます。

  関連資料 :『Oracle Application Server 高可用性ガイド』の「Oracle Application Server Cluster（Identity Management）構成」

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

  関連資料 :『Oracle Identity Management 統合ガイド』のプロビジョニング・サービスの概要に関する章

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

  関連資料 :『Oracle Identity Management 統合ガイド』の Oracle E-Business Suite との統合に関する章

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

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

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

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

  関連資料 :『Oracle Identity Management 委任管理ガイド』の Oracle Internet Directory セルフ・サービス・コンソールに関する章

- **アップグレード手順**

  関連資料 : Oracle Internet Directory の以前のバージョンからアップグレードする方法の詳細は、Oracle Application Server のアップグレードおよび互換性ガイドを参照してください。

Oracle Internet Directory リリース 9.2 の概要

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

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

  関連資料 :『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

注意 :

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

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

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

- **サーバー側のエントリ・キャッシング :** この機能によって、LDAP クライアントのディレクトリ問合せ待機時間が短縮されます。Oracle Internet Directory では、ネーミング・コンテキスト、クライアントの識別情報またはその他の使用可能なパラメータに基づいてサーバー側のエントリ・キャッシュを構成することによって、以前に取得したエントリとその属性を共有メモリーに保存し、後続のデータ・リクエスト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。返されたこれらの 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、クライアントに返されます。

  関連資料 : 25-9 ページの「エントリ・キャッシング」

- **新しいディレクトリ統合機能 :** Oracle Internet Directory リリース 9.0.2 では、(Oracle および Oracle 以外で作成された）他のアプリケーションやリポジトリとの新しい種類の接続性が導入されました。新しい Oracle Directory Provisioning Integration Service および Oracle Directory Synchronization Service は、Oracle Directory Integration 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、人間のエンド・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・エンティティには、ローカル・リポジトリの同期を維持する

ために、Oracle Internet Directory での更新を知らされます。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。

  関連資料 :『Oracle Identity Management 統合ガイド』の概念とコンポーネントに関する章

- **エンタープライズ・パスワード・ポリシー管理の拡張機能 :** パスワード・ポリシーを構成して、次のものを確定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
  - 承認されるパスワード構文および再試行制限
  - ディレクトリ・サービスへの不正アクセスのロックアウト（指定した回数を超えてアクセスに失敗した場合）

  ハッシング・アルゴリズムとして salted SHA を使用できるようになりました。この結果、次の各種ハッシング・アルゴリズムを使用できます。
  - **MD4**: 128 ビットのハッシュを生成する一方向ハッシュ関数です。
  - MD5**:** MD4 が改善された、より複合的なバージョンです。
  - SHA**:** Secure Hash Algorithm。MD5 よりも長い 160 ビットのハッシュを生成します。このアルゴリズムは MD5 よりも若干速度が遅くなりますが、大きなメッセージ・ダイジェストによって、総当た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。salt 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、予測される辞書攻撃を回避します。
  - UNIX Crypt**:** UNIX 暗号化アルゴリズム。
  - ハッシングなし

  関連項目 :
  - 概念の説明は、16-7 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。
  - パスワード・ハッシングの設定方法は、第 19 章「Oracle Internet Directory のパスワード・ポリシー」を参照してください。

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

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

関連項目： 第 10 章「ディレクトリの属性一意性」

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

  関連項目： 第 20 章「パスワード・ベリファイアのディレクトリ格納」

- **拡張されたプロキシ・ユーザー機能 :** この新機能によって、開発者は中間層の能力をより有効に活用できます。ユーザーは、独立した、ディレクトリとは無関係なセッションを確立する必要はありません。中間層が Oracle Application Server などからプロキシ・ユーザーのバインド・メソッドを、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通じて変わらないときにも、Oracle Internet Directory では、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 16 章「ディレクトリ・セキュリティの概念」
  - 7-9 ページの「スーパーユーザー、ゲスト・ユーザーおよびプロキシ・ユーザーの管理」

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

  関連項目： 第 23 章「Oracle Identity Management レルムの配置」

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

  関連項目： 14-14 ページの Oracle Internet Directory サーバーの監視

- **Oracle Directory Manager の拡張機能 :** Oracle Internet Directory のスタンドアロンで 100% Java の管理コンソールである Oracle Directory Manager は、様々な面で進化しました。Oracle Directory Manager を使用すると、次の操作を行うことができます。

  – レルムの構成

  – パスワード・ポリシーの構成

  – Oracle Directory Synchronization Service および Oracle Internet Directory のコネクタとエージェントの構成

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

関連項目： 第 5 章「ディレクトリ管理および監視ツール」

- **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やカスケード削除、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 32 章「Oracle Internet Directory サーバー・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： 7-12 ページの「別名エントリの間接参照」

- **Delegated Administration Services**

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

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

  – 他の領域または部門の管理者の作成

  – 特定のリージョン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・コンソールは、Oracle Delegated Administration Services の新規コンポーネントで、これにより、中央のチームから、または分散化と委任によって、アプリケーション、レルムおよびエンド・ユーザーを柔軟に管理できます。このコンポーネントでは、次の機能が提供されます。

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

  – 許可されたエンド・ユーザーが、パーソナライズされたプリファレンスの表示および Oracle Application Server Single Sign-On パスワードの更新を行うための機能

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

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

  関連資料：『Oracle Identity Management 委任管理ガイド』の Oracle Internet Directory セルフ・サービス・コンソールに関する章

- **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 およびリリース 3.0.1 からアップグレードできます。

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

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

- **クラスタ構成でのフェイルオーバー**

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

  関連資料：『Oracle Application Server 高可用性ガイド』の「Oracle Application Server Cold Failover Cluster (Identity Management)」

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

  Oracle 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。

  関連資料：『Oracle Application Server 高可用性ガイド』の「Oracle Real Application Clusters 環境でのディレクトリ」

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

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

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

  関連資料：『Oracle Application Server 高可用性ガイド』の「Oracle Application Server Cold Failover Cluster (Identity Management)」

- **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したりできます。

  関連項目： 22-5 ページの「1 つのホストにおける複数の Oracle Internet Directory インストール」

- **Oracle Directory Integration and Provisioning**

  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。

  関連資料：『Oracle Identity Management 統合ガイド』

- **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実行が可能になります。

  関連項目：

  - 概念の説明は、「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。
  - 第 19 章「Oracle Internet Directory のパスワード・ポリシー」

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

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

- **UTF8 制限の削除**

  Oracle ディレクトリ・サーバーとデータベース・ツールの実行を UTF8 データベース上に限定する制限はなくなりました。ただし、クライアント・リクエストとディレクトリ・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、3-13 ページの「属性オプション」を参照してください。
  - 8-7 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」
  - 8-10 ページの「コマンドライン・ツールを使用した属性オプション付きエントリの管理」

- **変更ログの削除機能の拡張機能**

  これらの拡張機能によって、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、26-6 ページの「マルチマスター・レプリケーションの変更ログの削除」を参照してください。
- 31-4 ページの「Oracle Directory Manager を使用した特定のレプリカ・ノードのパラメータの表示と変更」

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

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

  関連資料：

  - 概念の説明は、3-11 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の例は、『Oracle Identity Management ユーザー・リファレンス』の `ldapsearch` コマンドライン・ツールのリファレンスを参照してください。

- **他の LDAP 準拠のディレクトリからの移行**

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

  関連項目： 第 27 章「他のデータ・リポジ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、11-4 ページの「オブジェクト・クラスの追加のガイドライン」を参照してください。

- **OID データベース統計収集ツール**

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

  関連資料：『Oracle Identity Management ユーザー・リファレンス』の `oidstats.sql` コマンドライン・ツールのリファレンス

- **パスワード保護の拡張機能**

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

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

関連項目：

- 概念の説明は、16-7 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。
- パスワード・ハッシングの設定方法は、第 19 章「Oracle Internet Directory のパスワード・ポリシー」を参照してください。

- **レプリケーション・ツール**

  次の新しいレプリケーション・ツールが追加されました。

  – **管理者操作キュー操作ツール**

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

  – **OID 調整ツール**

    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、5-8 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。
    - 30-38 ページの「管理者操作キュー操作ツールの概要」
    - 30-39 ページの「Oracle Internet Directory 比較調整ツールの概要」

- **レプリケーション・ノードの削除**

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

  ヒント： 30-19 ページの「マルチマスター・レプリケーション・グループからのノードの削除」

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

  メタディレクトリ環境で作業している場合は、この新機能を使用して、複数ディレクトリを Oracle Internet Directory と同期化できます。

  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。『Oracle Identity Management 統合ガイド』の概要とコンポーネントに関する章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）**

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

第I部

スタート・ガイド

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

- 第 1 章「一般的タスクへのリンク」
- 第 2 章「LDAP および Oracle Internet Directory の概要」
- 第 3 章「ディレクトリの概念およびアーキテクチャ」
- 第 4 章「インストール後に実行するタスクと情報」
- 第 5 章「ディレクトリ管理および監視ツール」
- 第 6 章「Oracle Internet Directory のプロセス制御コンポーネント」

1

一般的タスクへのリンク

Oracle Internet Directory ルーチン管理タスクについては、このマニュアル全体と、『Oracle Identity Management ユーザー・リファレンス』の各ツールに関する章で説明しています。この章では、一般的なタスクのいくつかについて必要な情報を説明します。この章の項目は次のとおりです。

- オブジェクト・クラスおよび属性
- レプリケーション
- セキュリティ、パスワード・ポリシーおよびユーザー・アカウント
- レルム
- サーバー・プロセス、インスタンスおよび構成設定エントリ
- システム操作属性
- ネーミング・コンテキスト
- バインド、接続、別名およびディレクトリ検出
- 参照整合性
- エントリ
- グループ
- ロギング、監査および監視
- チューニング
- ガベージ・コレクション
- サーバー・チェーンおよびデータの移行
- プラグイン

オブジェクト・クラスおよび属性

オブジェクト・クラスおよび属性に関連した Oracle Internet Directory のタスクは、次の表に示すとおりです。

表 1-1 オブジェクト・クラスおよび属性

タスク	参照箇所
オブジェクト・クラスを追加、変更または削除	11-8 ページの「コマンドライン・ツールを使用したオブジェクト・クラスの管理」 11-3 ページの「ディレクトリのオブジェクト・クラス」
属性を追加、変更または削除	11-15 ページの「コマンドライン・ツールを使用した属性の管理」 11-10 ページの「ディレクトリの属性」
属性一意性制約エントリを作成、変更および削除	10-6 ページの「Oracle Directory Manager を使用した属性一意性の管理」 10-7 ページの「コマンドライン・ツールを使用した属性一意性の管理」
コマンドライン・ツールを使用して属性を追加、変更または削除	11-23 ページの「コマンドライン・ツールを使用した属性別名の管理」

レプリケーション

レプリケーションに関連した Oracle Internet Directory のタスクは、次の表に示すとおりです。

表 1-2 レプリケーション

タスク	参照箇所
レプリケーションを設定	30-2 ページの「レプリケーション・グループをインストールし構成するための前提情報」 30-5 ページの「マルチマスター・レプリケーションのインストールと構成」 30-20 ページの「一方向または双方向 LDAP ベース・レプリケーションのインストールと構成」 付録 I「データベース・コピー・プロシージャを使用したディレクトリ・ノードの追加」
レプリケーション競合を解消	30-37 ページの「手動でのレプリケーション・グループ内の競合の解消」
レプリケーション・フェイルオーバーを構成	30-43 ページの「レプリケーション・フェイルオーバーの構成」
レプリケーション構成パラメータを変更	31-2 ページの「ディレクトリ・レプリケーション・サーバーの構成パラメータの表示および変更」 31-4 ページの「特定のレプリカ・ノードについてのパラメータの表示および変更」 31-6 ページの「レプリケーション承諾のパラメータの変更」
全ノードでレプリケーション管理者パスワードを変更	31-10 ページの「Oracle Database アドバンスト・レプリケーションを使用した、全ノードでのレプリケーション管理者パスワードの変更」
変更ログを管理	31-11 ページの「変更ログの管理」
レプリケーションの速度を変更	31-11 ページの「ディレクトリ・レプリケーションの速度変更」
トポロジを管理および監視	31-12 ページの「トポロジの管理および監視」

セキュリティ、パスワード・ポリシーおよびユーザー・アカウント

セキュリティ、パスワード・ポリシーおよびユーザー・アカウントに関連した Oracle Internet Directory のタスクは、次の表に示すとおりです。

表 1-3 セキュリティ、パスワード・ポリシーおよびユーザー・アカウント

タスク	参照箇所
SSL を設定	第 17 章「Secure Sockets Layer（SSL）とディレクトリ」
ACP 内でアクセス制御情報を表示および変更	18-14 ページの「Oracle Directory Manager を使用したアクセス制御の管理」 18-35 ページの「コマンドライン・ツールを使用したアクセス制御の管理」
パスワード保護を管理	20-4 ページの「Oracle Directory Manager を使用したパスワード保護の管理」 20-4 ページの「ldapmodify を使用したパスワード保護の管理」
Oracle コンポーネントのパスワード・ベリファイアを管理	20-11 ページの「Oracle Directory Manager を使用した Oracle コンポーネント用パスワード検証プロファイルの管理」 20-11 ページの「コマンドライン・ツールを使用した Oracle コンポーネント用パスワード検証プロファイルの管理」
パスワード・ポリシーを表示、リフレッシュおよび変更するために Oracle Directory Manager を使用	19-10 ページの「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・ツールを使用してパスワード・ポリシー、アカウントおよびパスワードを管理	19-11 ページの「コマンドライン・ツールを使用したパスワード・ポリシー、アカウントおよびパスワードの管理」
セルフサービス・コンソールを使用してアカウントおよびパスワードを管理	19-13 ページの「セルフ・サービス・コンソールを使用したアカウントおよびパスワードの管理」
スーパー・ユーザー、ゲスト・ユーザー、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	7-10 ページの「Oracle Directory Manager を使用したスーパーユーザー、ゲスト・ユーザーおよびプロキシ・ユーザーの管理」 7-10 ページの「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」

レルム

レルムに関連した Oracle Internet Directory のタスクは、次の表に示すとおりです。

表 1-4 レルム

タスク	参照箇所
デフォルト・レルムをカスタマイズ	23-12 ページの「デフォルトの ID 管理レルムのカスタマイズ」
追加レルムを作成	23-18 ページの「ホスティングされた配置での ID 管理レルムの追加作成」

サーバー・プロセス、インスタンスおよび構成設定エントリ

サーバー・プロセス、インスタンスおよび構成設定エントリに関連した Oracle Internet Directory のタスクは、次の表に示すとおりです。

表 1-5 サーバー・プロセス、インスタンスおよび構成設定エントリ

タスク	参照箇所
サーバー・インスタンス・パラメータを構成	7-6 ページの「コマンドライン・ツールを使用したサーバー構成設定エントリの管理」 7-3 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」
ディレクトリ・サーバー・プロセスを起動	6-3 ページの「Oracle Internet Directory を起動する OPMN のセマンティックス」
ディレクトリ・サーバー・プロセスを停止	6-3 ページの「Oracle Internet Directory を停止する OPMN のセマンティックス」
システム操作属性を表示	7-8 ページの「Oracle Directory Manager を使用したシステム操作属性の設定」
Oracle Directory Manager を使用してサーバー・プロセス数またはデータベース接続数を変更	6-5 ページの「OID LDAP サーバー・インスタンスのデフォルト構成の変更」
Oracle Directory Manager を使用して追加の Oracle Internet Directory LDAP インスタンス起動のための構成設定を追加	6-5 ページの「追加の Oracle Internet Directory LDAP サーバー・インスタンスの構成」
Oracle Directory Manager を使用してサーバー・インスタンスを表示	7-11 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」
`opmn.xml` の編集によりデフォルト Oracle Internet Directory LDAP サーバー・インスタンスを他のインスタンスに置換	6-6 ページの「デフォルトの Oracle Internet Directory LDAP サーバー・インスタンスの構成解除」
`oidctl start` コマンドを使用して OID レプリケーション・サーバーのインスタンスを構成	6-6 ページの「Oracle Internet Directory レプリケーション・サーバー・インスタンスの構成」
`oidctl start` コマンドを使用して Oracle Internet Directory サーバーのインスタンスを構成	6-6 ページの「Oracle Directory Integration Platform サーバー・インスタンスの構成」
Oracle Directory Manager を使用して構成設定エントリおよびそのパラメータを表示	7-4 ページの「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追加	7-4 ページの「Oracle Directory Manager を使用した構成設定エントリの追加」 7-6 ページの「ldapadd を使用した構成設定エントリの追加」および『Oracle Identity Management ユーザー・リファレンス』の `ldapadd` コマンドライン・ツールのリファレンス

表 1-5 サーバー・プロセス、インスタンスおよび構成設定エントリ（続き）

タスク	参照箇所
既存の構成設定エントリを変更または削除	7-7 ページの「ldapmodify を使用した構成設定エントリの変更と削除」および『Oracle Identity Management ユーザー・リファレンス』の `ldapmodify` コマンドライン・ツールのリファレンス 7-5 ページの「Oracle Directory Manager を使用した構成設定エントリの変更」 7-5 ページの「Oracle Directory Manager を使用した構成設定エントリの削除」

システム操作属性

システム操作属性に関連した Oracle Internet Directory のタスクは、次の表に示すとおりです。

表 1-6 システム操作属性

タスク	参照箇所
Oracle Directory Manager を使用して接続先の Oracle ディレクトリ・サーバーの操作属性を表示または設定	7-8 ページの「Oracle Directory Manager を使用したシステム操作属性の設定」
`ldapmodify` を使用してシステム操作属性を変更	『Oracle Identity Management ユーザー・リファレンス』の `ldapmodify` コマンドライン・ツールのリファレンス

ネーミング・コンテキスト

ネーミング・コンテキストに関連した Oracle Internet Directory のタスクは、次の表に示すとおりです。

表 1-7 ネーミング・コンテキスト

タスク	参照箇所
ユーザーによる特定のネーミング・コンテキストの検索を有効化	7-9 ページの「Oracle Directory Manager を使用したネーミング・コンテキストの公開」 7-9 ページの「ldapmodify を使用したネーミング・コンテキストの公開」
小さなディレクトリまたはネーミング・コンテキストをバックアップおよびリストア	15-2 ページの「小さいディレクトリまたはディレクトリ内の特定のネーミング・コンテキストのバックアップとリストア」

バインド、接続、別名およびディレクトリ検出

バインド、接続、別名およびディレクトリ検出に関連した Oracle Internet Directory のタスクは、次の表に示すとおりです。

表 1-8 バインド、接続、別名およびディレクトリ検出

タスク	参照箇所
匿名バインドを無効化または有効化	7-11 ページの「匿名ユーザーによるバインドの管理」
`ldapbind` を使用してディレクトリ・サーバーに対してユーザーまたはクライアントを認証	『Oracle Identity Management ユーザー・リファレンス』の `ldapbind` コマンドライン・ツールのリファレンス
`ldapbind` を使用してクライアントをサーバーに接続できることを確認	
アイドル状態の LDAP 接続をクローズ	7-12 ページの「アイドル状態の LDAP 接続のクローズ」
Oracle Internet Directory データベースへのパスワードを変更	『Oracle Identity Management ユーザー・リファレンス』の `oidpasswd` コマンドライン・ツールのリファレンス
コマンドライン・ツール `ldapadd` を使用して別名エントリを持つディレクトリを追加、変更または検索	7-12 ページの「別名エントリの概要」
ディレクトリを検出	7-17 ページの「ディレクトリ・サーバー構成ファイル（ldap.ora）を使用した静的ディレクトリ・サーバーの検出」 7-17 ページの「ドメイン・ネーム・システム（DNS）を使用した動的ディレクトリ・サーバーの検出」
ディレクトリ・サーバーを DNS に登録	7-19 ページの「ドメイン・ネーム・システムへのディレクトリ・サーバーの登録」

参照整合性

参照整合性に関連した Oracle Internet Directory のタスクは、次の表に示すとおりです。

表 1-9 参照整合性

タスク	参照箇所
参照整合性を構成および有効化	12-2 ページの「参照整合性の構成および有効化」
参照整合性を無効化	12-3 ページの「参照整合性の無効化」

エントリ

エントリに関連した Oracle Internet Directory のタスクは、次の表に示すとおりです。

表 1-10 エントリ

タスク	参照箇所
エントリを表示または検索	8-2 ページの「Oracle Directory Manager を使用したエントリの検索」 『Oracle Identity Management ユーザー・リファレンス』の ldapsearch コマンドライン・ツールのリファレンス
Oracle Directory Manager を使用してエントリの属性を表示	8-3 ページの「Oracle Directory Manager を使用した特定エントリの属性の表示」
Oracle Directory Manager を使用してエントリを追加	8-3 ページの「Oracle Directory Manager を使用したエントリの追加」
Oracle Directory Manager を使用してエントリを変更	8-6 ページの「Oracle Directory Manager を使用したエントリの変更」
Oracle Directory Manager を使用してエントリの属性オプションを追加、変更または削除	8-7 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」
コンテンツ・ルールを管理	11-20 ページの「コンテンツ規則の管理」
ldapadd を使用して一度に 1 つずつエントリを追加	『Oracle Identity Management ユーザー・リファレンス』の ldapadd コマンドライン・ツールのリファレンス
ldapadd を使用して入力ファイルでサーバーを構成	
ldapaddmt を使用して複数エントリを同時に追加	『Oracle Identity Management ユーザー・リファレンス』の ldapaddmt コマンドライン・ツールのリファレンス
ldapcompare を使用して指定する属性値をディレクトリ・エントリ内の属性値と比較	『Oracle Identity Management ユーザー・リファレンス』の ldapcompare コマンドライン・ツールのリファレンス
ldapdelete を使用してエントリを削除	『Oracle Identity Management ユーザー・リファレンス』の ldapdelete コマンドライン・ツールのリファレンス
ldapmoddn を使用してエントリの識別名または相対識別名を変更	『Oracle Identity Management ユーザー・リファレンス』の ldapmoddn コマンドライン・ツールのリファレンス
ldapmoddn を使用してエントリまたはサブツリーの名前を変更	
ldapmoddn を使用してエントリまたはサブツリーを新しい親の下に移動	
ldapmodify を使用してエントリの属性データを作成、更新および削除	『Oracle Identity Management ユーザー・リファレンス』の ldapmodify コマンドライン・ツールのリファレンス
ldapmodify を使用してエントリの識別名または相対識別名を変更	
ldapmodifymt を使用して複数エントリを同時に変更	『Oracle Identity Management ユーザー・リファレンス』の ldapmodifymt コマンドライン・ツールのリファレンス

表 1-10 エントリ（続き）

タスク	参照箇所
大量のデータ・ファイルをインポート	9-4 ページの「bulkload を使用した LDIF ファイルのインポート」 『Oracle Identity Management ユーザー・リファレンス』の bulkload コマンドライン・ツールのリファレンス 『Oracle Identity Management ユーザー・リファレンス』の LDIF ファイルの書式設定規則と例に関する項
ldifwrite を使用してディレクトリ・データを LDIF に変換	9-9 ページの「ldifwrite の使用例」 『Oracle Identity Management ユーザー・リファレンス』の ldifwrite コマンドライン・ツールのリファレンス
bulkmodify を使用して多数のエントリを変更	9-7 ページの「bulkmodify の使用例」 『Oracle Identity Management ユーザー・リファレンス』の bulkmodify コマンドライン・ツールのリファレンス
bulkdelete を使用して多数のエントリを削除	9-8 ページの「bulkdelete の使用例」 『Oracle Identity Management ユーザー・リファレンス』の bulkdelete コマンドライン・ツールのリファレンス
catalog を使用して属性を検索可能化または検索不可能化	9-10 ページの「catalog の使用例」 『Oracle Identity Management ユーザー・リファレンス』の catalog コマンドライン・ツールのリファレンス

グループ

グループに関連した Oracle Internet Directory のタスクは、次の表に示すとおりです。

表 1-11 グループ

タスク	参照箇所
Oracle Directory Manager を使用して静的グループ・エントリを管理	13-7 ページの Oracle Directory Manager を使用した静的グループ・エントリの管理
コマンドライン・ツールを使用して静的グループ・エントリを管理	13-8 ページの「コマンドライン・ツールを使用した静的グループ・エントリの管理」
Oracle Directory Manager を使用して動的グループ・エントリを管理	13-10 ページの「Oracle Directory Manager を使用した動的グループの管理」
コマンドライン・ツールを使用して動的グループ・エントリを管理	13-11 ページの「コマンドライン・ツールを使用した動的グループの管理」

ロギング、監査および監視

ロギング、監査および監視に関連した Oracle Internet Directory のタスクは、次の表に示すとおりです。

表 1-12 ロギング、監査および監視

タスク	参照箇所
デバッグ・ディメンションを指定してロギングを特定の操作に限定	14-7 ページの「操作デバッグ・ディメンションの設定」
デバッグ・メッセージをログ・ファイルに強制的にフラッシュ	14-8 ページの「ログ・ファイルへのトレース情報のフラッシュの強制」
監査レベルを設定	14-12 ページの「Oracle Directory Manager を使用した監査レベルの設定」 14-13 ページの「ldapmodify を使用した監査レベルの設定」
監査ログ・エントリの検索	14-13 ページの「監査ログ・エントリの検索」
Oracle Internet Directory サーバー管理機能フレームワークの構成	14-18 ページの「Oracle Internet Directory サーバー管理機能の構成」
Oracle Internet Directory サーバー管理機能情報を表示	14-21 ページの「Oracle Internet Directory サーバー管理機能情報の表示」
デバッグ・ロギング・レベルを設定	14-6 ページの「デバッグ・ロギング・レベルの設定」

チューニング

チューニングに関連した Oracle Internet Directory のタスクは、次の表に示すとおりです。

表 1-13 チューニング

タスク	参照箇所
検索を最適化	25-10 ページの「大きいグループ・エントリの検索の最適化」 25-11 ページの「偏りのある属性の検索の最適化」
時間制限モードを設定	25-12 ページの「Oracle Directory Manager を使用した制限時間モードの設定」 25-12 ページの「ldapmodify を使用した制限時間モードの設定」
タイムアウトを設定	25-13 ページの「クライアント / サーバー間の接続のタイムアウトの設定」 25-13 ページの「書込み操作のタイムアウトの設定」

ガベージ・コレクション

ガベージ・コレクションに関連した Oracle Internet Directory のタスクは、次の表に示すとおりです。

表 1-14 ガベージ・コレクション

タスク	参照箇所
ガベージ・コレクタを変更	26-8 ページの「Oracle Directory Manager を使用したガベージ・コレクタの変更」 26-8 ページの「コマンドライン・ツールを使用したガベージ・コレクタの変更」 26-9 ページの「Oracle Internet Directory 統計情報コレクタの変更」
ガベージ・コレクションのロギングを有効化、無効化または監視	26-9 ページの「Oracle Internet Directory ガベージ・コレクタのロギングの有効化」 26-10 ページの「Oracle Internet Directory ガベージ・コレクタのロギングの無効化」 26-10 ページの「ガベージ・コレクションのロギングの監視」

サーバー・チェーンおよびデータの移行

サーバー・チェーンおよびデータの移行に関連した Oracle Internet Directory のタスクは、次の表に示すとおりです。

表 1-15 サーバー・チェーンおよびデータの移行

タスク	参照箇所
LDAP に準拠したサード・パーティのディレクトリからデータを移行	27-7 ページの「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」
アプリケーション固有のリポジトリからユーザー・データを移行	27-10 ページの「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」
サーバー・チェーンを構成	28-4 ページの「コマンドラインからのサーバー・チェーンの構成」 28-5 ページの「Oracle Directory Manager を使用したサーバー・チェーンの構成」

プラグイン

プラグインに関連した Oracle Internet Directory のタスクは、次の表に示すとおりです。

表 1-16 プラグイン

タスク	参照箇所
プラグインを作成	32-4 ページの「プラグインの作成」
プラグインを登録および管理	32-5 ページの「プラグインの登録と管理」
パスワード・ポリシー・プラグインを設定	第 33 章「Oracle Internet Directory のパスワード・ポリシー・プラグイン」
外部認証プラグインを設定	第 34 章「カスタマイズされた外部認証プラグインの設定」

2

LDAP および Oracle Internet Directory の概要

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

この章の項目は次のとおりです。

ディレクトリとは

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

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

この項の項目は次のとおりです。

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。このような情報は、管理が必要なあらゆるリソースを意味します。つまり、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です。

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

- 会社の個人別電話帳情報を検索し、メール・クライアントでアドレス帳から電子メール・アドレスを調べる従業員
- ユーザーのメール・サーバーの位置を特定する、メッセージ転送エージェントなどのアプリケーション
- ユーザーのロール情報を識別するデータベース・アプリケーション

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

表 2-1 オンライン・ディレクトリとリレーショナル・データベースの比較

オンライン・ディレクトリ	リレーショナル・データベース
主に読取りを目的としています。一般的な使用例では、データの更新が比較的少なく、検索が多い傾向があります。	**主に書込みを目的としています。**一般的な使用例では、トランザクションが連続的に記録され、検索が比較的少ない傾向があります。
比較的小規模な単位のデータで比較的単純なトランザクションを処理するように設計されています。たとえば、アプリケーションがディレクトリを使用して、電子メール・アドレス、電話番号またはデジタル画像の格納および検索のみを行う場合があります。	**大規模な単位のデータで多数の操作を利用しながら、多様で大量のトランザクションを処理するように設計されています。**
ロケーションに依存しないように設計されています。ディレクトリ対応アプリケーションは、問合せ中のサーバーに関係なく、配置環境全体にわたって常に同じ情報を参照していると想定しています。問合せ先のサーバーにローカルの情報が格納されていない場合、そのサーバーはその情報を取り出すか、クライアント・アプリケーションにその情報を透過的に示す必要があります。	**一般的にはロケーション固有に設計されています。**リレーショナル・データベースは分散が可能ですが、通常は特定のデータベース・サーバーに常駐します。

表 2-1 オンライン・ディレクトリとリレーショナル・データベースの比較（続き）

オンライン・ディレクトリ	リレーショナル・データベース
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です。各エントリには、多数の属性が関連付けられます。それぞれの属性には 1 つ以上の値が割り当てられる場合があります。たとえば、person エントリの一般的な属性は、姓名、電子メール・アドレス、デフォルトのメール・サーバーのアドレス、パスワードまたは他のログイン資格証明、デジタル化された顔写真などです。	**リレーショナル表に行として情報を格納するように設計されています。**

問題点 : 特別な用途を指定されたディレクトリが多すぎる場合

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

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

- 高い管理費用 : 管理者は、複数の場所で基本的には同じ情報をメンテナンスする必要があります。たとえば、ある企業が新しい従業員を雇用するとき、管理者は新しいユーザー ID をネットワークに作成し、新しい電子メール・アカウントを作成し、そのユーザーを従業員データベースに追加し、そして従業員が必要とするすべてのアプリケーション（開発、テストおよび本番データベース・システムのユーザー・アカウントなど）を設定する必要があります。その従業員が退社した場合は、管理者はこれらのユーザー・アカウントをすべて無効にするために逆の処理を行う必要があります。
- 一貫性のないデータ : 大きな管理オーバーヘッドのため、複数のシステムに冗長な情報を入力している複数の管理者にとっては、この従業員の情報をすべてのシステムで同期化させることが困難な場合があります。結果として、企業内で一貫性のないデータが発生することになります。
- セキュリティの問題 : 各ディレクトリには、独自のパスワード・ポリシーがあります。つまり、ユーザーは、システムごとに異なる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ります。

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

Lightweight Directory Access Protocol（LDAP）とは

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

この項の項目は次のとおりです。

LDAP と単純化されたディレクトリ管理

LDAP は、国際標準化機構（ISO）のディレクトリ・サービスに関する X.500 規格の、インターネットに対応する軽量実装として考え出されました。クライアント側に必要なネットワーキング・ソフトウェアを最小限に抑えられるため、インターネット・ベースのシン・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 Version 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** によって、インターネット標準の案として承認されました。LDAP バージョン 3 では、次のいくつかの重要な領域において LDAP バージョン 2 の内容が改善されています。

- グローバリゼーション・サポート : LDAP バージョン 3 では、世界中の言語で使用されている文字を、サーバーとクライアントの両方でサポートできます。
- ナレッジ参照（参照とも呼ばれる）: LDAP バージョン 3 の参照機能によって、サーバーは、ディレクトリ問合せの結果として、参照を他のサーバーに返すことができます。これにより、**ディレクトリ情報ツリー**を複数の LDAP サーバーにわたってパーティション化して、ディレクトリをグローバルに分散できます。
- セキュリティ : LDAP バージョン 3 では、**Simple Authentication and Security Layer** をサポートするための標準機能が追加され、データ・セキュリティに関する総合的で拡張可能なフレームワークが提供されています。
- 拡張性 : LDAP バージョン 3 では、ベンダーは、制御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。これらは、既存の操作に付随する追加情報で、操作の動きを変更します。クライアント・アプリケーションから標準 LDAP コマンドとともに制御が渡されると、命令された操作の動きがそれに応じて変更されます。たとえば、クライアントからディレクトリ内の非表示メタ情報を変更するには、LDAP コマンドに加えて manageDSAIT 制御を送信します。
- 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。

関連資料：

- IETF の RFC（Requests for Comments）2251 ～ 2256。`http://www.ietf.org` で入手可能です。
- 付録 K「Oracle Internet Directory でサポートされている RFC」
- LDAP に関する参考資料の追加リストは、xxxiii ページの「関連ドキュメント」を参照してください。
- ディレクトリ情報ツリーおよびナレッジ参照の概念の説明は、第 3 章「ディレクトリの概念およびアーキテクチャ」を参照してください。
- Oracle Internet Directory でサポートしている制御のリストおよび説明は、『Oracle Identity Management ユーザー・リファレンス』の LDAP 制御に関する項を参照してください。

Oracle Identity Management

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

- Oracle Directory Integration Platform: このコンポーネントは、Oracle Internet Directory と次の機能を同期化します。
  - 他のディレクトリおよびユーザー・リポジトリ
  - Oracle コンポーネントおよびアプリケーションのための自動プロビジョニング・サービス
  - サード・パーティのアプリケーション
- Oracle Delegated Administration Services: ユーザーおよびアプリケーション管理者による、信頼できるプロキシ・ベースのディレクトリ情報管理を提供します。
- Oracle Application Server Single Sign-On: Oracle アプリケーションとサード・パーティのアプリケーションへのシングル・サインオン・アクセスを提供します。
- Oracle Application Server Certificate Authority: 強力な認証方式をサポートする X.509 V3 PKI 証明書を生成し、公開します。

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

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

関連資料：

- Oracle Identity Management インフラストラクチャの計画策定、配置および使用方法の詳細は、『Oracle Identity Management 概要および配置プランニング・ガイド』を参照してください。
- Oracle Identity Management に関連する Oracle Internet Directory の役割の詳細は、第 23 章「Oracle Identity Management レルムの配置」を参照してください。

Oracle Internet Directory とは

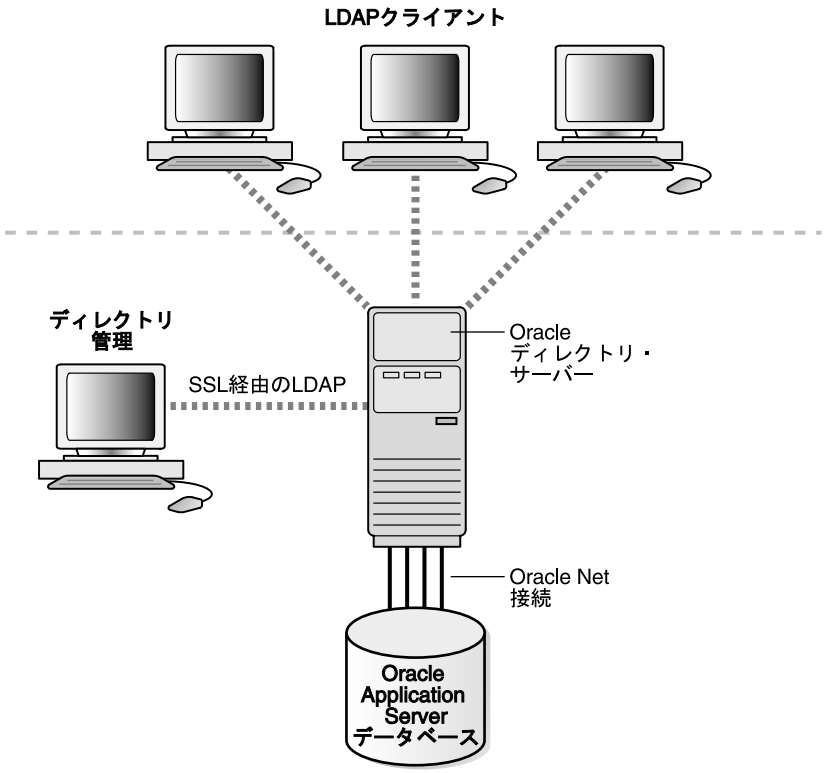
Oracle Internet Directory は、分散ユーザーやネットワーク・リソースに関する迅速な情報検索および情報の中央管理を可能にする、汎用ディレクトリ・サービスです。**Lightweight Directory Access Protocol** バージョン 3 と Oracle Database のすぐれたパフォーマンス、スケーラビリティ、堅牢性および可用性を組み合せたものです。

この項の項目は次のとおりです。

Oracle Internet Directory の概要

Oracle Internet Directory は、Oracle Database 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、データベースと通信します。データベースのホストが異なっていてもかまいません。図 2-1 に、この関係を示します。

図 2-1 Oracle Internet Directory の概要



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リクエストに応答します。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、次のものがあります。
  - Oracle Directory Manager。Java ベースの Graphical User Interface（GUI）を使用してディレクトリの管理を簡素化します。
  - 各種のコマンドライン管理ツールとデータ管理ツール。これらは LDAP クライアントから呼び出されます。
  - Oracle Enterprise Manager 10*g* Application Server Control コンソール内のディレクトリ・サーバー管理ツール。これらの管理ツールにより、次のことが可能になります。
    * 標準的なブラウザからのリアルタイム・イベントや統計の監視
    * これらのデータを新しいリポジトリに収集するプロセスの開始
- Oracle Internet Directory Software Developer's Kit

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

Oracle Internet Directory の利点

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

スケーラビリティ

Oracle Internet Directory は、Oracle Database の高機能を活用して、TB 単位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、わずかな検索レスポンス時間を実現します。

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、Oracle Database 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 **Oracle Database アドバンスト・レプリケーション**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、Oracle Database 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、Oracle Database 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、Oracle Database 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** バージョン 3 を使用した証明書ベースという 3 つのレベルのユーザー認証を実装し、認証アクセスおよびデータ・プライバシが保障されています。

Oracle 環境との統合

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

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

この項の項目は次のとおりです。

簡単で対費用効果の高いアプリケーション管理

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

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

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

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

セキュリティ・ポリシーの集中管理によるセキュリティの強化

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

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

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

- ユーザー認証資格証明の集中管理

  Oracle Advanced Security は、ユーザーのデータベース・パスワードを各データベースではなく 1 箇所に、つまりディレクトリに格納します。パスワードをそのユーザー・エントリの属性として格納します。

- 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、共有または所有にかかわらず指定のスキーマ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、あるユーザーを事務のエンタープライズ・ロールに割り当て、このロールに、人事のグローバル・ロールと人事管理データベースに対する付随権限、および分析のグローバル・ロール・ロールと給与管理データベースに対する付随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

  Oracle Database では、Oracle Advanced Security によって、エンタープライズ・ユーザーは、集中管理された単一のパスワードを使用して複数のデータベースに対する認証を実行できます。パスワードは、ユーザーのエントリの属性としてディレクトリに格納され、暗号化とアクセス制御リスト（ACL）によって保護されます。これによって、ユーザーは、クライアントでの Secure Sockets Layer（SSL）を設定し、複数のパスワードを記憶する必要がなくなります。

- エンタープライズ・ユーザー・セキュリティ

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

- PKI 資格証明の集中格納

  Oracle Database と Oracle Application Server では、ユーザー Wallet をユーザーのエントリの属性としてディレクトリに格納できます。これによって、モバイル・ユーザーは、エンタープライズ・ログイン・アシスタントを使用して Wallet を取得およびオープンできます。Wallet のオープン中は、認証は透過的に行われます。つまり、ユーザーは、スキーマを所有または共有しているデータベースに、再認証せずにアクセスできます。

複数ディレクトリの統合

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

- すべての Oracle コンポーネントでは、Oracle Internet Directory を使用することが事前に認証されています。
- サード・パーティの各ディレクトリを Oracle Internet Directory に統合することによって、Oracle 環境全体をサード・パーティ・ディレクトリに簡単に統合できます。したがって、各アプリケーションを各ディレクトリと統合する必要はありません。

3

ディレクトリの概念およびアーキテクチャ

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

この章の項目は次のとおりです。

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

Oracle Internet Directory のアーキテクチャ

この項の項目は次のとおりです。

Oracle Internet Directory のノード

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

3-3 ページの図 3-1 に、単一ノード上で稼働している様々なディレクトリ・サーバー・コンポーネントと、それらの関係を示します。

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

- **オブジェクト・クラス**
- Oracle ディレクトリ・サーバー・インスタンス 1 の非 SSL ポート 389
- Oracle ディレクトリ・サーバー・インスタンス 2 の SSL 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 3-1 一般的な Oracle Internet Directory のノード

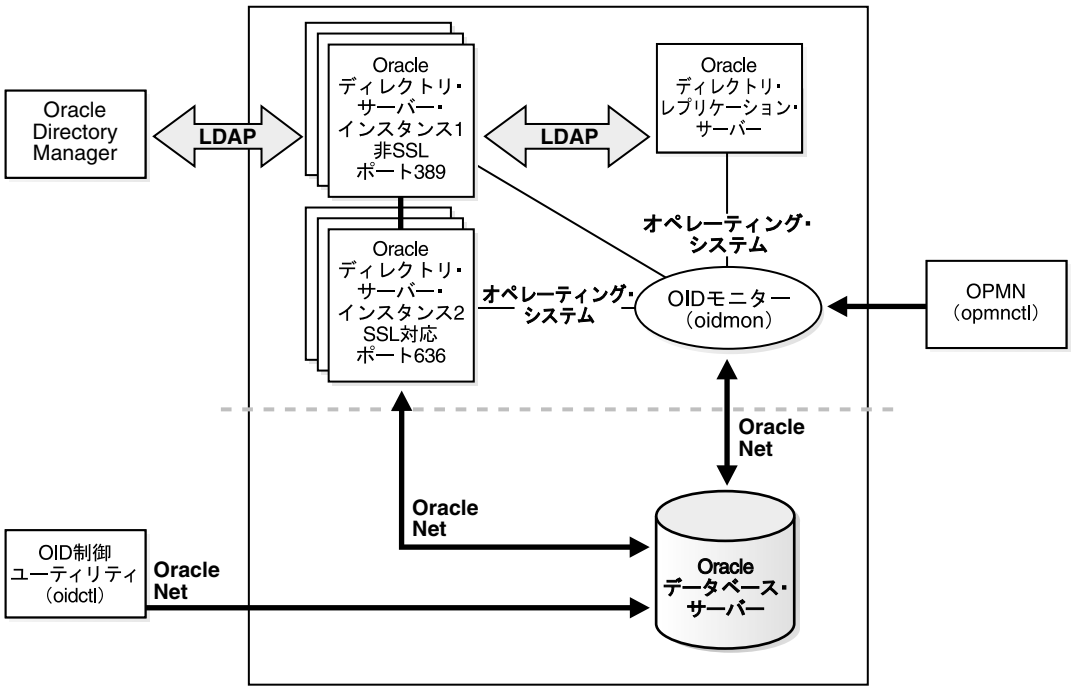


図 3-1 に示すとおり、Oracle Internet Directory のノードには、次の主なコンポーネントがあります。

表 3-1 Oracle Internet Directory のノードのコンポーネント

コンポーネント	説明
Oracle ディレクトリ・サーバー・インスタンス	LADP サーバー・インスタンスまたはディレクトリ・サーバー・インスタンスとも呼ばれ、特定の TCP/IP ポートでリスニングする単一の Oracle Internet Directory ディスパッチャ・プロセスを介して、ディレクトリ・リクエストに応答します。1 つのノードに、それぞれが異なるポートでリスニングする複数のディレクトリ・サーバー・インスタンスを設定できます。
Oracle ディレクトリ・レプリケーション・サーバー	レプリケーション・サーバーとも呼ばれ、他の Oracle Internet Directory システム内のレプリケーション・サーバーの変更を追跡し、その内容を送信します。1 つのノード上に設定できるレプリケーション・サーバーは 1 つのみです。レプリケーション・サーバーを構成するかどうかは選択できます。
Oracle データベース・サーバー	ディレクトリ・データを格納します。データベースをこのディレクトリ専用に使用することをお薦めします。データベースは、ディレクトリ・サーバー・インスタンスと同じノードに置くことができます。
Oracle Process Manager and Notification Server（OPMN）	Oracle Internet Directory を Oracle Application Server コンポーネントとして管理します。OPMN は `$ORACLE_HOME/opmn/conf/opmn.xml` の OID コンポーネント Snippet 内のディレクティブを使用し、必要に応じて OIDMON および OIDCTL を起動します。Oracle Internet Directory サーバー・インスタンスは認識しません。

表 3-1 Oracle Internet Directory のノードのコンポーネント（続き）

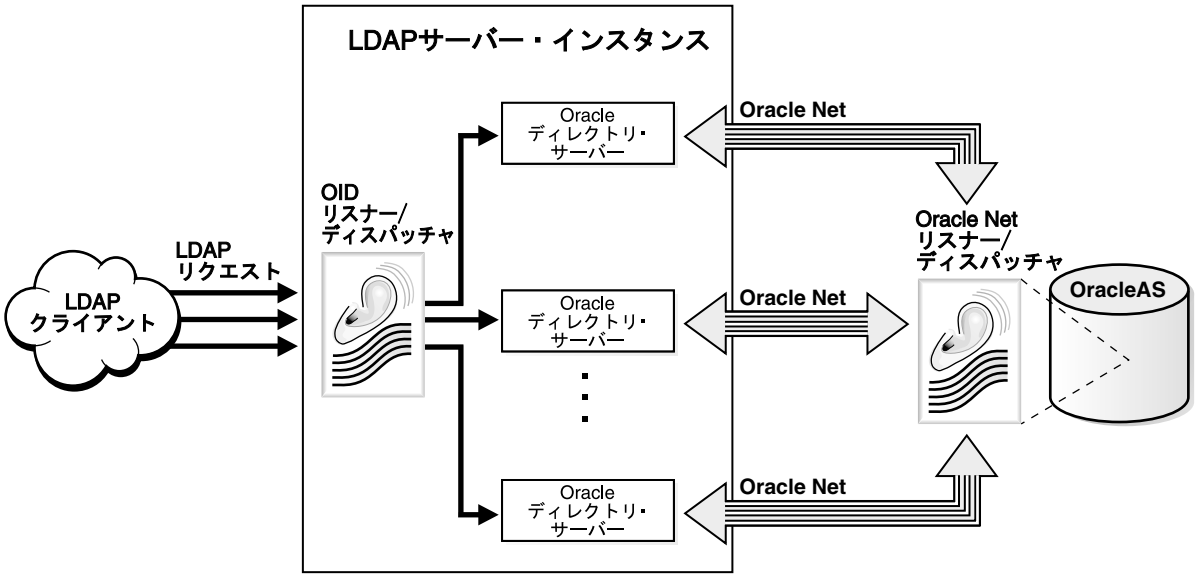
コンポーネント	説明
OID モニター（OIDMON）	LDAP のサーバー・プロセスを開始、監視および終了します。レプリケーション・サーバーをインストールするように選択した場合、レプリケーション・サーバーは OID モニターによって制御されます。ディレクトリ・サーバー・インスタンスを起動または停止するために OID 制御ユーティリティ（OIDCTL）を介してコマンドを発行すると、そのコマンドはこのプロセスによって解析されます。 OID モニターは、管理者が OID 制御ユーティリティで行う LDAP サーバー・インスタンスの起動と停止のリクエストを処理します。また、OID モニターはサーバーを監視し、異常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。また、プロセス表内で検出したすべてのサーバーも起動します。OID モニターは、ディレクトリ・サーバー・インスタンスを停止すると、プロセス表を更新します。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 3-2 のようになります。

図 3-2 Oracle ディレクトリ・サーバー・インスタンスのアーキテクチャ



1 つのインスタンスは、1 つのディスパッチャ・プロセスと 1 つ以上のサーバー・プロセスで構成されます。デフォルトでは、インスタンスごとに 1 つのサーバー・プロセスがありますが、これは増やすことができます。Oracle Internet Directory ディスパッチャとサーバー・プロセスは、複数のスレッドを使用して、負荷を分散できます。LDAP クライアントは LDAP リクエストを、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。

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

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

構成パラメータ ORCLMAXCC に設定された数値に応じて、各サーバー・プロセスとデータベースとの間に必要な数の接続が生成されます。各サーバーによって生成されたデータベース接続の数は、ORCLMAXCC + (ORCLMAXCC/2) + 1 と等しくなります。configset0 の ORCLMAXCC のデフォルト値は 2 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、Oracle Database にリクエストを中継します。

ディレクトリ・メタデータ

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

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

- ディレクトリ・スキーマ

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

- アクセス制御ポリシー・ポイント（ACP）

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

- ルート DSE エントリ

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

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

- 権限グループ

  アクセス制御ポリシーで使用できるグループ。

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

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

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

  関連項目：

  - 8-2 ページの「Oracle Directory Manager を使用したエントリの管理」
  - 8-5 ページの「例 : Oracle Directory Manager を使用したユーザー・エントリの追加」

- カタログ・エントリ

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

- 共通エントリ

  ホスティングされた企業に関する情報を入れる特別なエントリ。ホスティングされた企業とは、別の企業からサービスを提供される企業のことをいいます。このエントリのメタデータには、ホスティングされた企業の識別名、ユーザー検索ベース、ニックネームなどの属性が入っています。詳細は、第 23 章「Oracle Identity Management レルムの配置」を参照してください。

- プラグイン・エントリ

  プラグイン・イベントをトリガーする操作の種類と、操作のどの時点でそのプラグインをトリガーするかに関する情報を入れる特別なエントリ。詳細は、第 32 章「Oracle Internet Directory サーバー・プラグイン・フレームワーク」を参照してください。

- パスワード検証エントリ

  暗号タイプと検証属性タイプに関する情報を入れる特別なエントリ。詳細は、第 20 章「パスワード・ベリファイアのディレクトリ格納」を参照してください。

- パスワード・ポリシー・エントリ

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

構成設定エントリ

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

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

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

関連資料：

- 7-2 ページの「サーバーの構成設定エントリの管理」
- 構成設定エントリの属性リストは、『Oracle Identity Management ユーザー・リファレンス』の Oracle Internet Directory 構成のスキーマ要素に関する項を参照してください。

例 : Oracle Internet Directory の動作

この例では、Oracle Internet Directory がどのように検索リクエスト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リクエストを入力します。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、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、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へのアクセスを要求できます。
   - 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するものがあります。
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リクエストをディレクトリ・サーバー・インスタンスに送信します。
4. ディレクトリ・サーバーはユーザーを認証します。このプロセスはバインドと呼ばれます。ディレクトリ・サーバーは、アクセス制御リスト（ACL）もチェックして、そのユーザーが、リクエスト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 からの検索リクエストを Oracle Call Interface（OCI）および Oracle Net Services に変換し、Oracle Database に送信します。
6. Oracle Database は、情報を取得し、ディレクトリ・サーバー、C API、クライアントの順に返していきます。

エントリ

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

この項の項目は次のとおりです。

識別名（DN）とディレクトリ情報ツリー（DIT）

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

識別名とディレクトリ情報ツリーとの関係を理解するには、図 3-3 を参照してください。

図 3-3 ディレクトリ情報ツリー

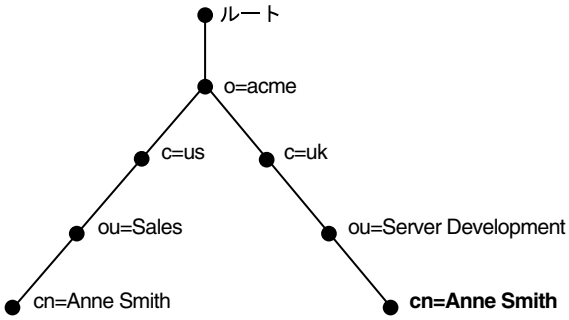


図 3-3 のディレクトリ情報ツリーは、Acme Corporation に所属する、Anne Smith という同名の 2 人の従業員のエントリを示しています。この図のディレクトリ情報ツリーは、地理的および組織的な系統に従って構造化されています。左のブランチの Anne Smith は米国の Sales 部門に勤務し、もう一方の Anne Smith は英国の Server Development 部門に勤務しています。

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

この Anne Smith エントリの識別名（DN）は次のとおりです。

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

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

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

ディレクトリ情報ツリー全体の中で特定エントリを検索するために、クライアントは、そのエントリの相対識別名のみではなく、完全な識別名を使用することによって、エントリを一意に識別します。たとえば、図 3-3 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します。同一組織単位内に同名の従業員が 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、補助的な方法を使用してください。

エントリ・キャッシング

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

注意： Oracle Internet Directory 10*g*（10.1.4.0.1）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。

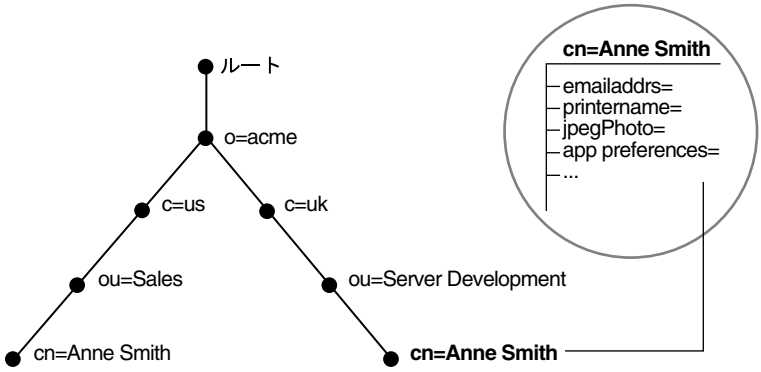
関連項目： 第 8 章「ディレクトリ・エントリの管理」

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 3-4 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示されています。`emailaddrs`、`printername`、`jpegPhoto` および `app preferences` などがあります。さらに、図 3-4 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 3-4 Anne Smith のエントリの属性



各属性は、属性タイプと 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です（例：`jobTitle`）。**属性値**は、そのエントリで表示さ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。

この項の項目は次のとおりです。

- 属性情報の種類
- 単一値と複数値の属性
- 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。

- アプリケーション属性

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

- 操作属性

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

エントリをディレクトリに追加すると、エントリの検索能力を強化するために、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。その属性は次のとおりです。

表 3-2 新規エントリごとに作成される属性

属性	説明
`creatorsName`	エントリ作成者の名前
`createTimestamp`	**UTC** でのエントリの作成時間
`modifiersName`	エントリ変更者の名前
`modifyTimestamp`	UTC での最後のエントリ変更時間

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

> **関連項目：** システム操作属性の構成方法は、7-7 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

属性は、単一値または複数値のいずれかです。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 3-3 に、Internet Engineering Task Force（IETF）の RFC 2798 に定義されている、一般的な LDAP 属性の一部を示します。

表 3-3 一般的な LDAP 属性

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

関連資料： Oracle Internet Directory で使用できる属性のリストは、『Oracle Identity Management ユーザー・リファレンス』で、Oracle Identity Management の LDAP の属性リファレンスに関する項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必要があります。しかし、別の属性の構文では、そのデータを日付書式で表すか、または数値のみで表すかの指定が必要な場合もあります。各属性の構文は必ず 1 つのみです。

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

関連資料：『Oracle Identity Management ユーザー・リファレンス』の LDAP の属性構文に関する項

属性の一致規則

ディレクトリ・サーバーは、クライアントのリクエストに応じて、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る。属性の作成時に、属性を一致規則と関連付けます。

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。

> **関連資料：**『Oracle Identity Management ユーザー・リファレンス』の LDAP の一致規則に関する項

属性オプション

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

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

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

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

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

関連項目：

- 8-7 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」
- 8-10 ページの「コマンドライン・ツールを使用した属性オプション付きエントリの管理」

オブジェクト・クラス

オブジェクト・クラスはエントリの構造を定義する属性のグループです。ディレクトリ・**エントリ**を定義するときは、そのエントリに 1 つ以上のオブジェクト・クラスを割り当てます。これらのオブジェクト・クラスの属性には、必須で値を指定する必要があるものもあれば、オプションで値を指定しなくてよいものもあります。

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

この項の項目は次のとおりです。

サブクラス、スーパークラスおよび継承

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

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

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

---

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

オブジェクト・クラスの型

オブジェクト・クラスには次の 3 つの型があります。

- 構造型
- 補助型
- 抽象型

構造型オブジェクト・クラス

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

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

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

補助型オブジェクト・クラス

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

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

抽象型オブジェクト・クラス

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

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

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

関連項目：

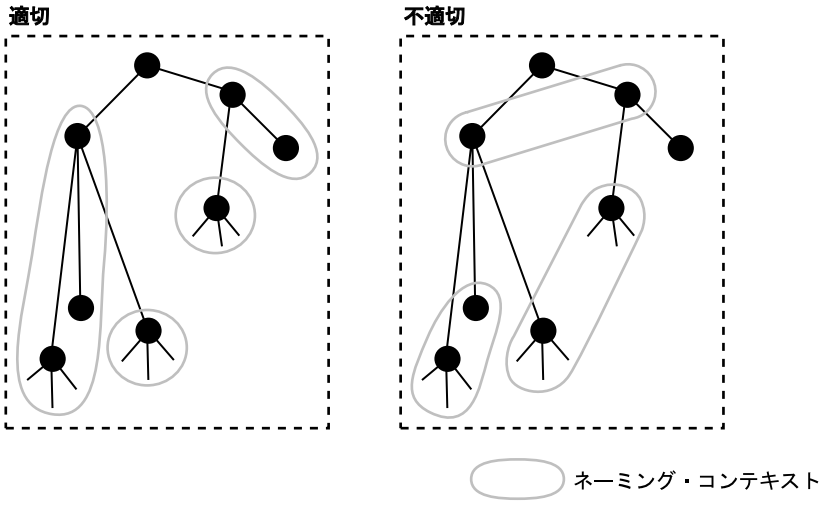
- アクセス制御ポリシーおよび ACL の詳細は、3-18 ページの「グローバリゼーション・サポート」を参照してください。
- エントリにコンテンツを追加する方法の詳細は、11-17 ページの「エントリと関連付けられた属性数の拡大方法」を参照してください。

ネーミング・コンテキスト

ディレクトリ・ネーミング・コンテキストは、全部が 1 つのサーバーに存在するサブツリーです。これは完全なサブツリーである必要があります。つまり、サブツリーの最上位の役割を果す**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へと伸びていく必要があります。単一のエントリから**ディレクトリ情報ツリー**全体まで、サイズは様々です。

図 3-5 に、適切なネーミング・コンテキストと不適切なネーミング・コンテキストを示します。左側の適切なコンテキストは連続しており、右側の不適切なコンテキストは連続していないことに注意してください。

図 3-5 適切なネーミング・コンテキストと不適切なネーミング・コンテキスト



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

関連項目： ネーミング・コンテキストの公開方法は、7-8 ページの「ネーミング・コンテキストの管理」を参照してください。

セキュリティ

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

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

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

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

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

関連資料 :

- Oracle Internet Directory のセキュリティ機能の詳細は、第 16 章「ディレクトリ・セキュリティの概念」を参照してください。
- Oracle Identity Management インフラストラクチャと Oracle Internet Directory の関係については、第 23 章「Oracle Identity Management レルムの配置」を参照してください。
- 大企業やホスティングされた環境でアプリケーションを保護する方法の詳細は、第 21 章「Oracle テクノロジ配置のための権限の委任」を参照してください。
- Oracle Directory Integration Platform 環境におけるセキュリティの詳細は、『Oracle Identity Management 統合ガイド』のセキュリティに関する章を参照してください。
- Oracle Identity Management インフラストラクチャの詳細は、『Oracle Identity Management 概要および配置プランニング・ガイド』を参照してください。

グローバリゼーション・サポート

Oracle Internet Directory は、LDAP バージョン 3 国際化（I18N）規格に準拠しています。この規格では、ディレクトリ・データを格納するデータベースで **UTF-8**（Unicode Transformation Format 8-bit）キャラクタ・セットを使用する必要があります。Oracle9*i* では、AL32UTF8 と呼ばれる新しい UTF-8 キャラクタ・セットを追加しました。このデータベース・キャラクタ・セットは、最新の補助文字を含む最新バージョンの Unicode（3.2）をサポートしています。この規格に従って、Oracle Internet Directory は、Oracle グローバリゼーション・サポートがサポートするほとんどすべての言語の文字データを格納できます。また、Oracle Internet Directory の実装では異なる Application Program Interface（API）がいくつか含まれていますが、Oracle Internet Directory では、各 API に正しい文字エンコーディングが使用されることを保証しています。

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

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

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

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

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

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

関連資料：

- Oracle Internet Directory の主なコンポーネントの詳細は、3-2 ページの「Oracle Internet Directory のアーキテクチャ」を参照してください。
- 付録 D「ディレクトリにおけるグローバリゼーション・サポート」
- グローバリゼーション・サポートの詳細は、Oracle Database ドキュメント・ライブラリの『Oracle 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。

分散ディレクトリ

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

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

この項の項目は次のとおりです。

- ディレクトリ・レプリケーション
- ディレクトリ・パーティション化

ディレクトリ・レプリケーション

レプリケーションは、複数のディレクトリ・サーバーに同じネーミング・コンテキストをコピーし、管理するプロセスです。レプリケーションには次のような機能があります。

- 問合せの処理に複数のサーバーで備えることによってパフォーマンスを向上させ、シングル・ポイント障害に伴うリスクを排除して信頼性を向上させます。
- レプリケーションには、完全レプリケーションと部分レプリケーションがあります。
- 完全レプリケーションでは、DIT 全体を別のノードに伝播します。
- 部分レプリケーションでは、DIT 全体ではなく 1 つ以上のサブツリーを別のノードに伝播します。

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

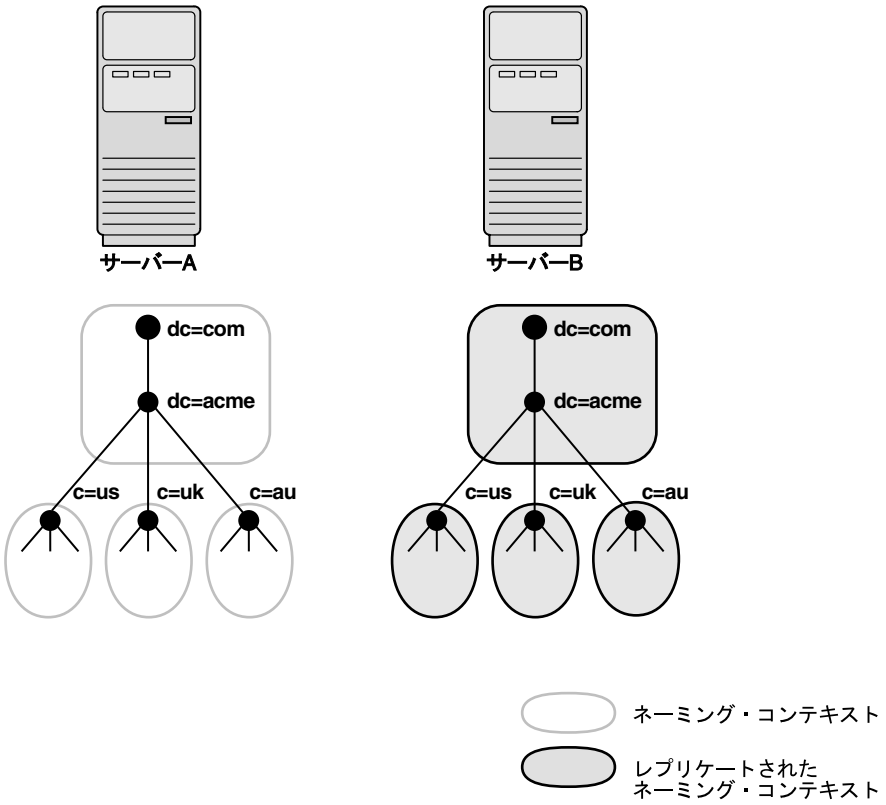
指定したネーミング・コンテキストのレプリケーションの対象となるディレクトリ・サーバーは、ディレクトリ・レプリケーション・グループ（DRG）と呼ばれるグループを形成します。DRG を構成するディレクトリ・サーバー間の関係は、各ノード上でレプリケーション承諾と呼ばれる特別なディレクトリ・エントリによって表されます。DRG の場合、ノード間でデータを転送するプロトコルは、Oracle Database アドバンスト・レプリケーションまたは LDAP のいずれかに基づきます。

DRG は、単一マスター、マルチマスター、ファンアウトのいずれかです。

- 単一マスター・レプリケーション・グループには、1 つ以上のコンシューマに変更をレプリケートするサプライヤが 1 つのみ存在します。更新できるのはサプライヤのみで、コンシューマは読取り専用です。
- マルチマスター・レプリケーションは、peer-to-peer レプリケーションまたは *n*-way レプリケーションとも呼ばれ、同等に機能する複数のサイトが、レプリケートされたデータのグループを管理できるようにします。マルチマスター・レプリケーション環境では、各ノードはサプライヤ・ノードであると同時にコンシューマ・ノードであり、各ノードでディレクトリ全体がレプリケートされます。
- ファンアウト・レプリケーション・グループは、point-to-point レプリケーション・グループとも呼ばれ、コンシューマに直接レプリケートするサプライヤを持っています。そのコンシューマは、1 つ以上の別のコンシューマにレプリケートできます。レプリケーションには、完全レプリケーションと部分レプリケーションがあります。

図 3-6 に、レプリケート・ディレクトリを示します。

図 3-6 レプリケート・ディレクトリ



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

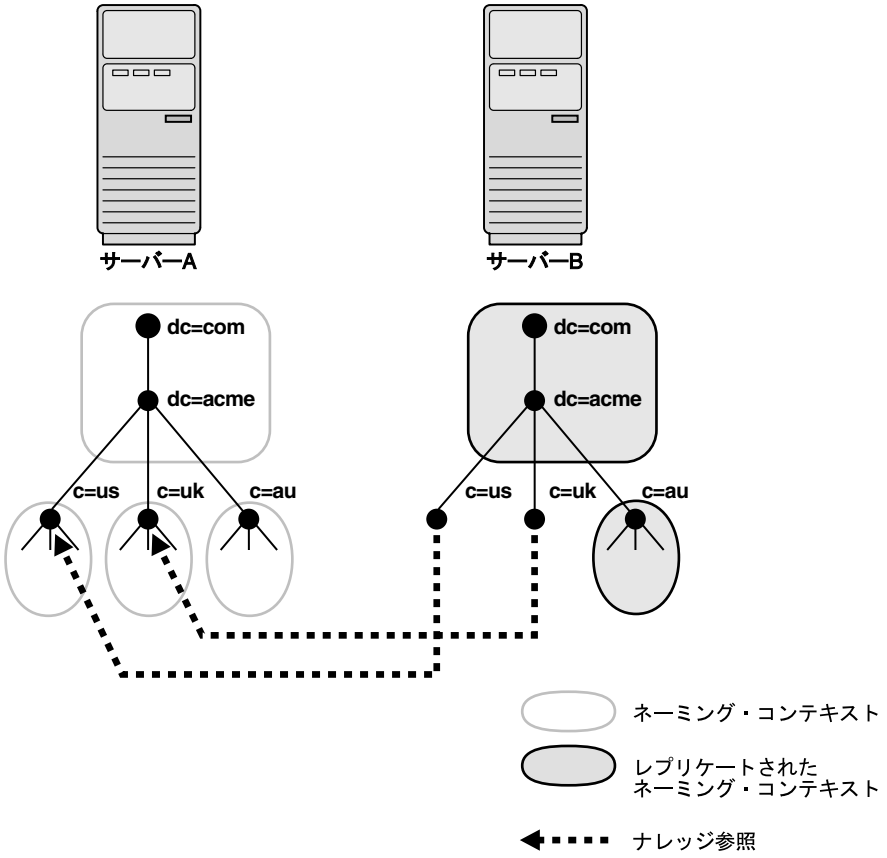
関連項目： レプリケーションの詳細は、第 29 章「Oracle Internet Directory レプリケーションの概要」を参照してください。これには、Oracle Database アドバンスト・レプリケーションのアーキテクチャ、LDAP ベースのレプリケーション、変更ログの削除、競合の解決、レプリケーションのプロセスが含まれています。

ディレクトリ・パーティション化

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

図 3-7 に、異なるサーバーにいくつかのネーミング・コンテキストが存在している、パーティション化されたディレクトリを示します。

図 3-7 パーティション化されたディレクトリ



3-21 ページの図 3-7 では、サーバー A に次の 4 つのネーミング・コンテキストが存在しています。

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

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

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

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

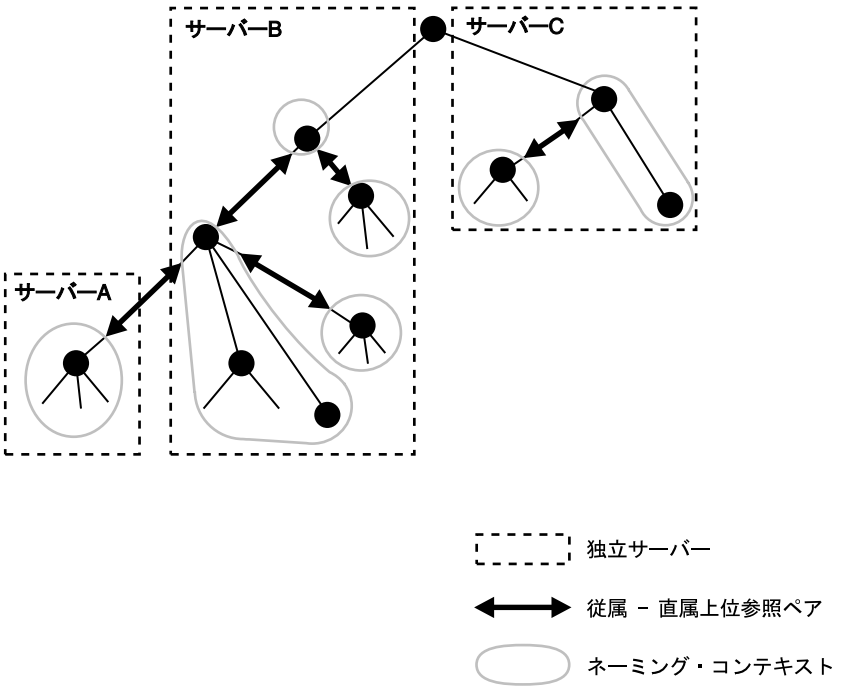
ナレッジ参照と参照

ナレッジ参照は、別のパーティションに保持されている様々なネーミング・コンテキストの名前とアドレスを提供します。たとえば、3-21 ページの図 3-7 で、サーバー B は、ナレッジ参照を使用して、サーバー A 上のネーミング・コンテキスト c=us と c=uk を指し示します。サーバー B がサーバー A に常駐している情報の要求を受けると、サーバー B は 1 つ以上のサーバー A への参照を返します。クライアントは、これらの参照を使用してサーバー A と通信できます。

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

たとえば、3-22 ページの図 3-8 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 3-8 ナレッジ参照を使用したネーミング・コンテキストへの指示



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

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

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

参照には次の 2 つの種類があります。

- スマート参照

  これらは、ナレッジ参照エントリが検索の有効範囲内にあるときにクライアントに返されます。スマート・ナレッジ参照は、リクエスト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` にある情報のリクエストを、クライアントがサーバー A に送信すると、サーバー A はサーバー B への参照をユーザーに提供します。

- デフォルト参照

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

  たとえば、サーバー A が次のものを保持するとします。

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

  クライアントが `c=uk,o=acme` にある情報をリクエストしたとします。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、リクエストしたネーミング・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： 8-11 ページの「ナレッジ参照と参照の管理」

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

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

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

関連資料：『Oracle Identity Management 委任管理ガイド』

サービス・レジストリとサービス・ツー・サービス認証

サービス・レジストリおよびサービス・ツー・サービス認証フレームワークとは Oracle Internet Directory の機能で、サービスを相互にリクエストする Oracle テクノロジ・コンポーネント間の統合を促進します。サービス・レジストリは、コンポーネントが互いに検出できるように情報の格納場所を提供します。サービス・ツー・サービス認証フレームワークは、一方のコンポーネントから他方のコンポーネントを認証できるようにして、互いの信頼関係を確立します。

サービス・レジストリとは Oracle Internet Directory で cn=Services、Cn=OracleContext の下にあるコンテナで、コンポーネントがプロトコルやサービス・タイプなどの接続情報を格納する場所です。インストールの際、それぞれの OCS コンポーネントがこのレジストリに情報を登録します。実行時には、このコンポーネントが他のコンポーネントの登録情報を検出します。サービス・レジストリ・オブジェクトは、Oracle Internet Directory のディレクトリ情報ツリーで、rootOracleContext のコンポーネント固有のサービス・コンテナに格納されます。

サービス・ツー・サービス認証は、一方のサービスから他方のサービスを認証できるようにして、サービス間の信頼関係を確立するフレームワークです。インストールの際、各クライアント・サービスには Oracle Internet Directory でのユーザー名とパスワードが提供されます。さらに、それぞれのターゲット・サービスが Oracle Internet Directory での権限ロールを定義して、どのコンポーネントを信頼すべきかを制御します。一方のコンポーネントが他方のコンポーネントのサービスをリクエストする場合、リクエスト側は独自の識別情報と資格証明を使用して、他のクライアントと同様にターゲット・サービスに対して認証する必要があります。またリクエスト・サービスは、ターゲット・サービスのトラステッド・アプリケーション・グループにリスト表示される必要があります（デフォルト・グループは対比アプリケーション、カウンターポイズ、cn=OracleContext です）。さらにリクエスト・サービスは、ターゲット・サービスがユーザーも認証できるように、ユーザーの識別情報を送信する必要があります。このデータは、Digest 認証もしくはターゲット・サービスに備わっているセキュア認証のいずれかにより、安全に送信されます。

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

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

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

関連資料：『Oracle Identity Management 統合ガイド』

Oracle Internet Directory と Oracle Identity Management

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

この項の項目は次のとおりです。

ID 管理の概要

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

ID 管理は、管理コストを削減すると同時にセキュリティを向上できるため、IT 配置にとって重要です。

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

- 企業規模の単一コンソールを使用したエンタープライズ ID の作成および ID の共有プロパティの管理。
- エンタープライズ ID のグループの作成。
- 企業で利用できる各種サービスでのこれらの ID のプロビジョニング。次のサービスが含まれます。
  - アカウント作成
  - アカウント一時停止
  - アカウント削除
- これらの ID に関連付けられたポリシーの管理。次のポリシーが含まれます。
  - 認可ポリシー
  - 認証ポリシー
  - 既存 ID に委任された権限

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

Oracle Identity Management は、分散セキュリティのために Oracle 製品が利用する統合インフラストラクチャです。これは、他の Oracle 製品同様、Oracle Application Server のインフラストラクチャの一部です。3-26 ページの図 3-9 は、Oracle Identity Management インフラストラクチャのコンポーネントと、各種 Oracle 製品およびサード・パーティ製品がこのインフラストラクチャにどのように依存しているかを示しています。

図 3-9 Oracle Identity Management インフラストラクチャおよび他のコンポーネント

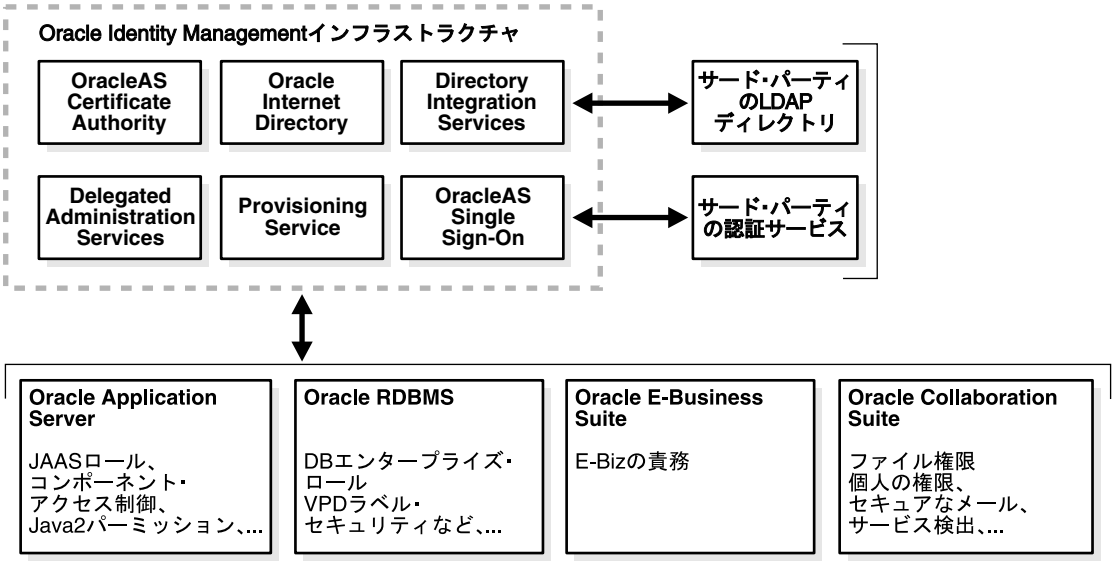


図 3-9 に示すとおり、Oracle Identity Management インフラストラクチャは次のコンポーネントと機能を含んでいます。

- Oracle Internet Directory: Oracle Database に実装されたスケーラブルで堅牢な LDAP V3 準拠のディレクトリ・サービスです。
- Oracle Directory Integration Platform: Oracle Internet Directory と、他のディレクトリ、ユーザー・リポジトリを同期させ、Oracle コンポーネントやアプリケーションに対して、また標準インタフェースを介してサード・パーティのアプリケーションに対して、自動プロビジョニング・サービスを可能にします。
- Oracle Delegated Administration Services: ユーザーおよびアプリケーション管理者による、信頼できるプロキシ・ベースのディレクトリ情報管理を提供します。
- Oracle Application Server Single Sign-On: Oracle アプリケーションとサード・パーティの Web アプリケーションへのシングル・サインオン・アクセスを提供します。
- Oracle Application Server Certificate Authority: 強力な認証方式をサポートする X.509 V3 PKI 証明書を生成し、公開します。

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

- Oracle Internet Directory は、C、Java および PL/SQL のための LDAP API を提供します。他の LDAP SDK と互換性があります。

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

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

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

ID 管理レルム

ID 管理レルムは、ある ID 管理ポリシーが配置により定義され、施行される企業内での有効範囲を定義します。次の要素で構成されます。

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

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

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

デフォルト ID 管理レルム

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

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

ID 管理ポリシー

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

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

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

リソース情報

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

- データの収集元となるリソースのタイプを指定する情報。たとえば、Oracle Database などです。これは、リソース・タイプ情報と呼ばれます。
- リソースに対するユーザーの接続および認証のための情報。これは、リソース・アクセス情報と呼ばれます。

この項の項目は次のとおりです。

- リソース・タイプ情報
- リソース・アクセス情報
- DIT 内のリソース情報の位置

リソース・タイプ情報

ユーザーのリクエストを処理するためにアプリケーションが使用するリソースの情報をリソース・タイプ情報と呼びます。リソース・タイプには、Oracle Database やプラッガブルな Java Database Connectivity データ・ソースなどがあります。リソース・タイプ情報には、ユーザーの認証に使用するクラス、ユーザー識別子、パスワードなどの項目が含まれます。

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

リソース・アクセス情報

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

たとえば、販売レポートに関するユーザーのリクエストを処理するために、Oracle Reports は複数のデータベースに問い合せます。データベースへの問合せでは、次の処理が実行されます。

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

この処理が終了すると、レポートがコンパイルされます。

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

DIT 内のリソース情報の位置

図 3-10 に、DIT 内のリソース情報の位置を示します。

図 3-10 DIT 内のリソース・アクセス情報およびリソース・タイプ情報の配置

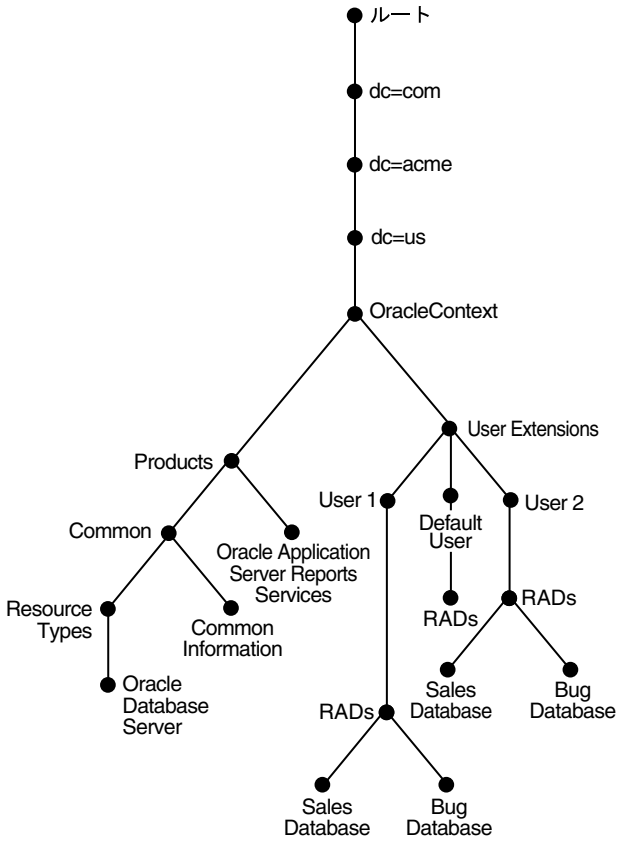


図 3-10 に示すとおり、リソース・アクセス情報およびリソース・タイプ情報は、Oracle コンテキストに格納されます。

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

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

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

関連資料：

- エンド・ユーザーによるリソース・アクセス情報の指定手順は、『Oracle Identity Management 委任管理ガイド』の独自のリソース情報の管理に関する項を参照してください。
- 管理者によるユーザー・エントリ作成時のリソース・アクセス情報の指定手順は、『Oracle Identity Management 委任管理ガイド』のセルフ・サービス・コンソールを使用したユーザー・エントリ作成に関する項を参照してください。
- すべてのユーザーが自動的に継承する一般的に使用されるリソースを管理者が定義する手順は、『Oracle Identity Management 委任管理ガイド』のデフォルトのリソース・アクセス情報の構成に関する項を参照してください。
- 管理者によるリソース・タイプの指定手順は、『Oracle Identity Management 委任管理ガイド』の新しいリソース・タイプの作成に関する項を参照してください。
- 『Oracle Identity Management ユーザー・リファレンス』のプラグインのスキーマ要素に関する項
- http://www.oracle.com/technology/documentation の Oracle Reports にある『Oracle Application Server Reports Services レポート Web 公開ガイド』

4

インストール後に実行するタスクと情報

インストールが正常に終了すると、OID モニター（oidmon）とディレクトリ・サーバーのインスタンス（oidldapd）が稼働している状態になります。

注意：

- ディレクトリ・サーバーが同じコンピュータ上にある場合は、複数のインスタンスを実行できます。たとえば、1 つのインスタンスを SSL モードで実行し、別のインスタンスを Non-SSL モードで実行できます。
- コンピュータを再起動する場合は、『Oracle Application Server 管理者ガイド』の OracleAS Infrastructure の起動に関する項で説明されている手順に従って、Oracle Application Server Infrastructure を再起動できます。
- Oracle Internet Directory サーバー（ディレクトリ・サーバー、ディレクトリ・レプリケーション・サーバーおよび Oracle Directory Integration and Provisioning Server の各デーモン）を起動できるのは、Oracle Internet Directory ソフトウェアをインストールしたオペレーティング・システム・ユーザーのみです。

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。

この項の項目は次のとおりです。

タスク 1: デフォルトのセキュリティ構成の再設定

使用環境でのニーズを満たすように、デフォルトのセキュリティ構成をカスタマイズする必要があります。表 4-1 に、カスタマイズで必要なタスクとその説明を示します。

表 4-1 デフォルトのセキュリティ構成を再設定するためのタスク

タスクの領域	説明
subSchemaSubEntry サブエントリとその子エントリの保護	ディレクトリに関する情報は、サブエントリ subSchemaSubEntry とその子エントリに格納されます。これらのオブジェクトへのアクセスを制御することをお薦めします。
エントリへのアクセスの確立	ディレクトリ・エントリをロードすると、ディレクトリ・エントリの階層が作成されます。このため、次の権限を設定する必要があります。 ■ この階層にエントリをロードするための権限 ■ ディレクトリ・エントリに対する読取り、変更および書込みのアクセス権限を必要とするクライアントのディレクトリ・アクセス権限
デフォルト・アクセス・ポリシーの変更	Oracle Internet Directory は、第 21 章「Oracle テクノロジ配置のための権限の委任」で説明する、デフォルトのセキュリティ構成でインストールされます。ディレクトリの使用を開始する前に、使用する環境に合せてこのデフォルトの構成を変更し、各ユーザーが適切な認可を確実に持つようにすることができます。
デフォルト・パスワード・ポリシーの変更	パスワード・ポリシーとは、パスワードの使用方法を管理する規則のセットです。Oracle Internet Directory は、デフォルト・パスワード・ポリシーとともにインストールされます。これは、環境に合せて変更できます。
スーパーユーザーのパスワードの変更	スーパーユーザーは、ディレクトリ情報に対するあらゆるアクセス権を持っています。スーパーユーザーのデフォルトのユーザー名は orcladmin で、デフォルトのパスワードはインストール時に指定した Oracle Application Server 管理者のパスワードです。このパスワードは、インストール後、ただちに変更してください。
機密の属性に対するプライバシ・モードの有効化	ユーザーが機密の属性をクリアテキストで取得できないようにするため、プライバシ・モードを有効にする必要があります。16-3 ページの「受信した機密の属性のプライバシ」を参照してください。

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 3 章「ディレクトリの概念およびアーキテクチャ」を参照してください。
- データの整合性、データのプライバシ、認証、認可およびパスワードの各ポリシーについては、第 16 章「ディレクトリ・セキュリティの概念」を参照してください。
- アクセス制御のオプションおよびセキュリティの設定方法の詳細は、第 18 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 23 章「Oracle Identity Management レルムの配置」を参照してください。
- デフォルト・パスワード・ポリシーの詳細は、第 19 章「Oracle Internet Directory のパスワード・ポリシー」を参照してください。

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

タスク 2: 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、指定された Oracle データベースへの接続時にパスワードを使用します。このパスワードのデフォルトは、インストール時に Oracle Application Server 管理者（ias_admin）に対して指定されたパスワードと同じです。このデフォルト・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変更します。

関連資料： 構文と使用方法は、『Oracle Identity Management ユーザー・リファレンス』の `oidpasswd` コマンドライン・ツールのリファレンスを参照してください。

タスク 3: 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`）以外の方法でデータをディレクトリにロードする場合は、ロード後に OID データベース統計収集ツール、`$ORACLE_HOME/ldap/admin/oidstats.sql` を実行する必要があります。その処理により、LDAP 操作に対応する問合せについて Oracle のオプティマイザが最適な実行計画を選択できるようになります。OID データベース統計収集ツールは、OID デーモンを停止せずに必要に応じて実行できます。

関連資料：『Oracle Identity Management ユーザー・リファレンス』の `oidstats.sql` コマンドライン・リファレンス

リリース 9.0.2 からのアップグレード後に実行するタスク

Oracle Internet Directory をリリース 9.0.2 からリリース 10.1.2 にアップグレードした場合は、次のタスクを実行します。

リリース 9.0.2 からのアップグレード後のグループ・コンテナへの ACL ポリシーの設定

Oracle Internet Directory をリリース 9.0.2 からリリース 10.1.2 にアップグレードする場合は、レルム内のグループ・コンテナに次の ACL ポリシーを設定する必要があります。ACL ポリシーでは、グループ `cn=Common Group Attributes,cn=groups,`*`Oracle_Context_DN`* のメンバーに、プライベートおよびパブリックのグループ（`orclIsVisible` が設定されていないか、`TRUE` または `FALSE` に設定されているグループ）への参照、検索および読取りアクセス権限が許可されている必要があります。この ACL については、『Oracle Internet Directory 管理者ガイド』の第 17 章の「共通グループ属性を読み取るためのデフォルトの権限」で説明されています。

共通グループ属性のグループは、OracleAS Portal で、プライベートおよびパブリックのグループの問合せに使用されます。グループ・コンテナには ACI を追加する必要があります。*`Realm DN`* をレルムの DN に変更し、*`DN of groups container in the realm`* を適切なグループ検索ベースに変更してください。

```
dn: DN of groups container in the realm
changetype: modify
add: orclaci
orclaci: access to entry filter=(!(orclisvisible=false)) by group="cn=Common Group
Attributes,cn=groups, cn=Oracle Context, Realm DN" (browse)
orclaci: access to attr=(*) filter=(!(orclisvisible=false)) by group="cn=Common Group
Attributes,cn=groups,cn=Oracle Context, Realm DN" (search, read)
```

```
orclaci: access to entry filter=(orclisvisible=false) by group="cn=Common Group
Attributes,cn=groups,cn=Oracle Context, Realm DN" (browse)
orclaci: access to attr=(*) filter=(orclisvisible=false) by group="cn=Common Group
Attributes,cn=groups, cn=Oracle Context, Realm DN" (search, read)
```

UNIX および Linux での LDAP ポート割当ての決定

Oracle Application Server またはサード・パーティ製品のインストール時に、Oracle Internet Directory または LDAP のポートの入力を求められる場合があります。インストール時に Oracle Internet Directory に割り当てられる特定のポート番号を調べるには、`$ORACLE_HOME/config/ias.properties` ファイルを参照します。エントリ、`OIDport` および `OIDsslport` を探してください。

Oracle Internet Directory のインストール時に LDAP を使用可能にするデフォルトのポートは 389 です。Oracle Universal Installer は、最初に必ずこのポートを選択しようとします。ただし、多くの UNIX コンピュータでは、`/etc/services` に LDAP でポート 389 を予約する行が含まれています。この行が存在する場合、インストーラはかわりに 3060 ～ 3129 のポート番号を選択します。

Oracle Internet Directory が実行されているポートを確認するには、`ldapbind` コマンドライン・ツールを実行します。引数には、ホスト名と、`portlist.ini` ファイルで指定されているポート番号または Oracle Internet Directory のインストール時に指定した代替ポートを指定します。

5

ディレクトリ管理および監視ツール

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。

この章の項目は次のとおりです。

- Oracle Identity Management Grid Control Plug-in の使用方法
- Oracle Directory Manager の使用方法
- Oracle Internet Directory サーバー管理機能の使用方法
- コマンドライン・ツールの使用方法

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

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

関連資料：『Oracle Identity Management 委任管理ガイド』

Oracle Identity Management Grid Control Plug-in の使用方法

Oracle Identity Management Grid Control Plug-in については、『Oracle Identity Management 概要および配置プランニング・ガイド』を参照してください。

Oracle 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。

この項の項目は次のとおりです。

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。インスタンスを実行していない場合は、6-3 ページの「Oracle Internet Directory を起動する OPMN のセマンティックス」の説明に従って起動してください。

> **関連項目：** ディレクトリ・サーバー・インスタンスの概念の説明は、3-2 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、表 5-1 で説明されているオペレーティング・システムの手順に従ってください。

表 5-1 オペレーティング・システム固有の Oracle Directory Manager の起動方法

オペレーティング・システム	参照先
Microsoft Windows	「**スタート**」メニューから「**プログラム**」を選択し、「**ORACLE_HOME**」、「**Integrated Management**」、「*Oracle Directory Manager*」の順に選択します。

UNIX	`$ORACLE_HOME/bin` を `$PATH` に追加している場合は、コマンド・プロンプトで、次のように入力します。
	`oidadmin`
	`$ORACLE_HOME/bin` を `$PATH` に追加していない場合は、`$ORACLE_HOME/bin` に移動して、コマンド・プロンプトで、次のように入力します。
	`./oidadmin`

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

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

ディレクトリ・サーバーへ接続する手順は、次のとおりです。

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

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

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

2. 「**資格証明**」タブ・ページの各フィールドに、このサーバー・インスタンス固有の情報を入力します。フィールドについては、A-2 ページの表 A-1 を参照してください。

   関連資料：

   - SSL を使用可能にする方法は、第 17 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、3-8 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、17-3 ページの「SSL パラメータの構成」を参照してください。
   - SSL の使用時に Oracle Wallet Manager を使用して Wallet を作成する手順は、『Oracle Advanced Security 管理者ガイド』を参照してください。

3. 「**資格証明**」タブ・ページの「**SSL 有効**」チェック・ボックスを選択した場合は、次に「**SSL**」タブを選択します。
4. 「SSL」タブ・ページの各フィールドに必要なデータを入力します。フィールドについては、A-3 ページの表 A-2 を参照してください。
5. 「**ログイン**」を選択します。Oracle Directory Manager が表示されます。

Oracle Directory Manager のナビゲート

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

Oracle Directory Manager の概要

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

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

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

Oracle Directory Manager のメニュー・バー

表 5-2 に、メニュー・バーからアクセスできるメニューを示します。各メニュー項目は、表示しているペインやタブ・ページによって、使用できる場合と使用できない場合があります。

表 5-2 Oracle Directory Manager のメニュー・バー

メニュー	メニュー項目
ファイル	**作成 :** オブジェクトを追加します。 **類似作成 :** ナビゲータ・ペインで選択したオブジェクトをテンプレートとして使用し、新規オブジェクトを追加します。 **接続 :** ナビゲータ・ペインで選択したディレクトリ・サーバーに接続します。 **切断 :** ナビゲータ・ペインで選択したディレクトリ・サーバーから切断します。 **終了 :** Oracle Directory Manager を終了します。
編集	**編集 :** オブジェクトを変更します。 **削除 :** 選択したオブジェクトを削除します。 **オブジェクト・クラスの検索**または**属性の検索 :** コンテキストに応じて、オブジェクト・クラスまたは属性を検索します。ナビゲータ・ペインで「**Oracle Internet Directory**」、「**< ディレクトリ・サーバー・インスタンス >**」、「**サーバー管理**」、「**オブジェクト・クラス**」の順に選択すると、このメニュー項目でオブジェクト・クラスを検索できます。「**Oracle Internet Directory**」、「**< ディレクトリ・サーバー・インスタンス >**」、「**サーバー管理**」、「**属性**」の順にナビゲートすると、属性を検索できます。
表示	**リフレッシュ :** メモリーに格納されているデータを更新し、データベースに変更内容を反映します。 **切離し :** Oracle Directory Manager の右側のペインに表示されているフィールドと値を含むセカンダリ・ダイアログを生成します。2 つの情報を比較する場合に便利です。
操作	**オブジェクト・クラスの作成 :** 新規オブジェクト・クラスの追加に使用する「新規オブジェクト・クラス」ウィンドウを表示します。 **属性の作成 :** エントリへの新規属性の追加に使用する「新規属性の型」ダイアログ・ボックスを表示します。 **アクセス制御ポイントの作成 :** 新規**アクセス制御ポリシー・ポイント**の追加に使用する「新規アクセス制御ポイント」ダイアログ・ボックスを表示します。 **エントリの作成 :** 新規ディレクトリ・エントリの追加に使用する「新規エントリ」ダイアログ・ボックスを表示します。 **エントリのリフレッシュ :** 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。 **検索フィルタの構成 :** 指定されたフィルタに応じてナビゲータ・ペインが表示するエントリの範囲を狭くします。 **索引の削除 :** 属性から索引を削除します。この項目を選択すると、削除の確認を要求するアラートが表示されます。 **検索 :** ACP 検索の構成を可能にします。 **ユーザー・プリファレンス :** 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

表 5-2 Oracle Directory Manager のメニュー・バー（続き）

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「ヘルプ検索」ダイアログ・ボックスを表示します。
	Oracle Internet Directory 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

表 5-3 に、Oracle Internet Directory ツールバーのボタンの説明を示します。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。

表 5-3 Oracle Directory Manager のツールバー

ボタン	目的
	**接続 / 切断 :** ナビゲータ・ペインで選択したディレクトリ・サーバーに対して接続または切断します。
	**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。
	**作成 :** 新規オブジェクトを追加します。
	**類似作成 :** 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。
	**編集 :** オブジェクトを変更します。
	**「オブジェクト・クラスの検索」または「属性の検索」:** コンテキストに応じて、オブジェクト・クラスまたは属性を検索します。ナビゲータ・ペインで「Oracle Internet Directory」→「< ディレクトリ・サーバー・インスタンス >」→「サーバー管理」→「オブジェクト・クラス」の順に移動すると、このボタンでオブジェクト・クラスを検索できます。「Oracle Internet Directory」→「< ディレクトリ・サーバー・インスタンス >」→「サーバー管理」→「属性」の順に移動すると、属性を検索できます。
	**削除 :** オブジェクトを削除します。
	**オブジェクト・クラスの追加 :** 既存エントリにオブジェクト・クラスを追加します。
	**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。
	**検索フィルタの構成 :** 指定されたフィルタに応じてナビゲータ・ペインが表示するエントリの範囲を狭くします。
	**索引の削除 :** 属性から索引を削除します。このボタンをクリックすると、削除の確認を要求するアラートが表示されます。
	**検索 :** ACP 検索の構成を可能にします。
	**ユーザー・プリファレンス :** 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。
	**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、ナビゲータ・ペインの「Oracle Internet Directory サーバー」の下に、各サーバーが表示されます。

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**」をクリックします。
3. 5-3 ページの「Oracle Directory Manager を使用したディレクトリ・サーバーへの接続」で説明している手順に従ってログインします。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

関連資料：

- 5-8 ページの「コマンドライン・ツールの使用方法」
- 『Oracle Identity Management ユーザー・リファレンス』の Oracle Identity Management のコマンドライン・ツールのリファレンス

表 5-4 に、Oracle Directory Manager を使用して管理できるタスクの領域、および各領域に関する説明の参照先を示します。

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

タスクの領域	参照先
アクセス制御管理	18-14 ページの「Oracle Directory Manager を使用したアクセス制御の管理」 18-35 ページのコマンドライン・ツールを使用したアクセス制御の管理
属性一意性管理	第 10 章「ディレクトリの属性一意性」
監査ログ管理	第 14 章「ディレクトリのロギング、監査および監視」
変更ログ管理	29-21 ページの「ディレクトリ・レプリケーションの変更ログ」 第 30 章「Oracle Internet Directory レプリケーションのインストールと構成」 『Oracle Identity Management 統合ガイド』の Oracle Directory Synchronization Service に関する章 『Oracle Identity Management 統合ガイド』の Oracle Directory Integration and Provisioning Server に関する章
エントリ管理	8-2 ページの「Oracle Directory Manager を使用したエントリの管理」
ガベージ・コレクション管理	第 26 章「Oracle Internet Directory におけるガベージ・コレクション」
パスワード・ポリシー管理	第 19 章「Oracle Internet Directory のパスワード・ポリシー」
パスワード検証管理	第 20 章「パスワード・ベリファイアのディレクトリ格納」
プラグイン管理	第 VI 部「ディレクトリ・プラグイン」
レプリケーション管理	第 30 章「Oracle Internet Directory レプリケーションのインストールと構成」

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

タスクの領域	参照先
スキーマ管理	11-3 ページの「ディレクトリのオブジェクト・クラス」
	11-10 ページの「ディレクトリの属性」
サーバー管理	第 7 章「Oracle ディレクトリ・サーバーの管理」

Oracle Internet Directory サーバー管理機能の使用方法

Oracle Internet Directory サーバー管理機能により、Oracle Internet Directory サーバーに関する様々なタイプの情報を監視できます。Oracle Internet Directory サーバー管理機能を使用して、ディレクトリ・サーバー・インスタンスの起動、停止または再起動も行えます。Oracle Internet Directory サーバー管理機能の機能を利用するには、Oracle Enterprise Manager 10*g* Application Server Control コンソールを使用します。

関連項目： Oracle Internet Directory サーバーの監視

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

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

注意： コマンドライン・ツールを使用するには、次の環境変数を設定します。

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

注意： Oracle Identity Management のドキュメントにおけるコマンドラインの例は、UNIX の ksh に基づいたものです。シェルからエスケープする必要のある引数は、二重引用符（"）で表示されています。使用するシェル環境に応じて適切な引用符を使用してください。

関連資料： LDIF ファイルのフォーマット方法は、『Oracle Identity Management ユーザー・リファレンス』の LDIF ファイルの形式化規則に関する項を参照してください。

この項の項目は次のとおりです。

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

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

表 5-5 に、Oracle Internet Directory サーバーを起動、停止および監視するための各種コマンドライン・ツールとその詳細情報の参照先を示します。

関連項目： 第 6 章「Oracle Internet Directory のプロセス制御コンポーネント」

表 5-5 Oracle Internet Directory サーバーの起動、停止、監視のためのツール

ツール	説明	詳細情報の参照先
Oracle Process Manager and Notification Server（OPMN）	Oracle Application Server コンポーネントとしての Oracle Internet Directory を停止または起動するには、OPMNCTL を使用します。	『Oracle Identity Management ユーザー・リファレンス』の opmnctl コマンドライン・ツールのリファレンス 『Oracle Process Manager and Notification Server 管理者ガイド』の「Oracle Internet Directory の構成」の章
OID 制御ユーティリティ（OIDCTL）	このツールは、サーバーの個別のインスタンスを起動および停止するときに使用します。コマンドは、OID モニター・プロセスによって解析され、実行されます。	概念の説明は、3-2 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 Identity Management ユーザー・リファレンス』の oidctl コマンドライン・ツールのリファレンス
OID モニター（OIDMON）	OIDMON を直接起動する必要はありません。OIDMON は、OPMN を使用して起動および停止します。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 OIDMON によって解析されます。	概念の説明は、3-2 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、『Oracle Identity Management ユーザー・リファレンス』の oidmon コマンドライン・ツールのリファレンスを参照してください。

エントリと属性の管理のためのコマンドライン・ツール

表 5-6 に、エントリと属性を管理するためのコマンドライン・ツールとその詳細情報の参照先を示します。

表 5-6 エントリの管理のためのツール

ツール	説明	詳細情報の参照先
カタログ管理ツール (catalog)	Oracle Internet Directory は、索引を使用して属性を検索できるようにしています。Oracle Internet Directory のインストール時に、エントリ cn=catalogs に、検索で使用できる属性がリストされます。等価の一致規則を持つ属性のみが索引付けできます。 その他の属性を検索フィルタで使用する場合は、使用する属性をカタログ・エントリに追加する必要があります。この操作は、Oracle Directory Manager を使用して属性を作成するときに実行できます。ただし、すでに存在している属性への索引付けに使用できるのは、カタログ管理ツールのみです。 索引の作成と削除に便利です。	構文と使用方法は、『Oracle Identity Management ユーザー・リファレンス』の `catalog` コマンドライン・ツールのリファレンスを参照してください。 11-14 ページの「Oracle Directory Manager を使用した属性の索引付け」 11-16 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」
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。	『Oracle Identity Management ユーザー・リファレンス』の ldapadd コマンドライン・ツールのリファレンス
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。	『Oracle Identity Management ユーザー・リファレンス』の `ldapaddmt` コマンドライン・ツールのリファレンス
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。	『Oracle Identity Management ユーザー・リファレンス』の `ldapbind` コマンドライン・ツールのリファレンス
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。	『Oracle Identity Management ユーザー・リファレンス』の `ldapcompare` コマンドライン・ツールのリファレンス
ldapdelete	このツールは、エントリを削除するときに使用します。	『Oracle Identity Management ユーザー・リファレンス』の `ldapdelete` コマンドライン・ツールのリファレンス
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の下への移動を行うときに使用します。	『Oracle Identity Management ユーザー・リファレンス』の `ldapmoddn` コマンドライン・ツールのリファレンス
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。	『Oracle Identity Management ユーザー・リファレンス』の `ldapmodify` コマンドライン・ツールのリファレンス
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。	『Oracle Identity Management ユーザー・リファレンス』の `ldapmodifymt` コマンドライン・ツールのリファレンス
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。	『Oracle Identity Management ユーザー・リファレンス』の `ldapsearch` コマンドライン・ツールのリファレンス

バルク操作を実行するためのコマンドライン・ツール

表 5-7 に、バルク操作を実行するためのコマンドライン・ツールとその詳細情報の参照先を示します。

表 5-7 バルク操作を実行するためのコマンドライン・ツール

ツール	説明	詳細情報の参照先
bulkdelete	このツールは、サブツリーを効率的に削除するときに使用します。	『Oracle Identity Management ユーザー・リファレンス』の `bulkdelete` コマンドライン・ツールのリファレンス
bulkload	このツールは、LDIF ファイルを使用して Oracle Internet Directory に大量のエントリをロードし、追加するときに使用します。	『Oracle Identity Management ユーザー・リファレンス』の `bulkload` コマンドライン・ツールのリファレンス
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。	『Oracle Identity Management ユーザー・リファレンス』の `bulkmodify` コマンドライン・ツールのリファレンス
ldifwrite	このツールは、ディレクトリ情報ベースのデータを、LDAP 準拠のディレクトリ・サーバーで読取り可能な LDIF ファイルにコピーするために使用します。ldifwrite は、bulkload と組み合せて使用できます。ldifwrite を使用して、ディレクトリの一部またはすべての情報をバックアップすることもできます。	『Oracle Identity Management ユーザー・リファレンス』の `ldifwrite` コマンドライン・ツールのリファレンス

レプリケーション管理のためのコマンドライン・ツール

5-12 ページの表 5-8 に、レプリケーションを管理するためのコマンドライン・ツールとその詳細情報の参照先を示します。

表 5-8 レプリケーション管理のためのコマンドライン・ツール

ツール	説明	詳細情報の参照先
レプリケーション環境管理ツール	このツールは、アドバンスト・レプリケーションがディレクトリ・レプリケーションのために正しく構成されることを保証します。ディレクトリ・レプリケーション障害が発生した場合、このツールは問題を調査し、修正方法を検証します。問題を解決できない場合は、問題の性質に関するレポートを作成し、考えられる解決方法を示します。	構文と例は、『Oracle Identity Management ユーザー・リファレンス』の `remtool` コマンドライン・ツールのリファレンスを参照してください。
Oracle Internet Directory 比較調整ツール	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、管理者によるアクションを待ちながら、そこから長い間隔で変更適用プロセスを繰り返します。 この時点で、次の操作を行う必要があります。 1. 管理者操作キューの変更を検証します。 2. Oracle Internet Directory 比較調整ツールを使用して、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整します。 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。	30-39 ページの「Oracle Internet Directory 比較調整ツールの概要」 『Oracle Identity Management ユーザー・リファレンス』の `oidcmprec` コマンドライン・ツールのリファレンス
管理者操作キュー操作ツール	Oracle Internet Directory 比較調整ツールを使用して、競合している変更を調製した後に、管理者操作キュー操作ツールを使用して、変更を管理者操作キューからリトライ・キューまたはパージ・キューに移動できます。パージ・キューへの変更の移動は、変更ログ・エントリの再適用を以降は試みないということを意味します。	30-38 ページの「管理者操作キュー操作ツールの概要」 比較および調整ツールの構文と動作の説明は、『Oracle Identity Management ユーザー・リファレンス』の `hiqretry` コマンドライン・ツールのリファレンスを参照してください。

OID 移行ツール（ldifmigrator）

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

関連資料： このツールの使用方法は、『Oracle Identity Management ユーザー・リファレンス』の `ldifmigrator` コマンドライン・ツールのリファレンスを参照してください。

OID データベース統計収集ツール（oidstats.sql）

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

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

関連資料：『Oracle Identity Management ユーザー・リファレンス』の `oidstats.sql` コマンドライン・ツールのリファレンス

OID データベース・パスワード・ユーティリティ（oidpasswd）

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

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

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

- Oracle Internet Directory データベース・パスワード用の `oidpwdlldap1` という Wallet、および Oracle ディレクトリ・レプリケーション・サーバー・パスワード用の `oidpwdr`*`sid`* という Wallet を作成します。

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

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

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

  注意： ODS データベース・ユーザー・パスワードを変更するには、oidpasswd ツールを使用する必要があります。ODS データベース・ユーザー・パスワードを他の方法で変更すると、Oracle Internet Directory インスタンスの起動に失敗します。

- スーパーユーザーのパスワードをリセットします。
- スーパーユーザーの制限付き ACP を管理します。

関連資料：『Oracle Identity Management ユーザー・リファレンス』の `oidpasswd` コマンドライン・ツールのリファレンス

6

Oracle Internet Directory のプロセス制御コンポーネント

この章では、Oracle Internet Directory におけるプロセス制御モデルの背後にある概念を説明します。プロセス制御モデルは、Oracle Internet Directory LDAP サーバー、レプリケーション・サーバーおよびディレクトリ統合サーバーに適用されます。

この項の項目は次のとおりです。

- Oracle Internet Directory プロセス制御で重要なツールとデーモン
- Oracle Internet Directory と OPMN の統合
- Oracle Internet Directory プロセス制御の最良実施例
- OIDMON および ODS_PROCESS 表
- OIDCTL のプロセス制御セマンティクス

Oracle Directory Integration Platform サーバーの起動と停止の詳細は、『Oracle Identity Management 統合ガイド』の Oracle Directory Integration Platform サーバー管理に関する章を参照してください。

Oracle Internet Directory プロセス制御で重要なツールとデーモン

Oracle Process Manager and Notification Server（OPMN）は、Oracle Application Server のインストールでコンポーネントを監視するデーモン・プロセスです。OPMN は、すべての中間層および Oracle Application Server Infrastructure にインストールおよび構成され、Oracle Application Server の実行に不可欠です。Oracle Internet Directory は Oracle Application Server Infrastructure の一部としてインストールされるため、OPMN は Oracle Application Server コンポーネントとしての Oracle Internet Directory を監視します。OPMN のコマンドライン・インタフェースは、`$ORACLE_HOME/opmn/bin/opmnctl` です。コンポーネントとしての Oracle Internet Directory を停止または起動するには、OPMNCTL を使用します。

> **関連資料：**『Oracle Process Manager and Notification Server 管理者ガイド』の「Oracle Internet Directory の構成」の章

OIDMON（`$ORACLE_HOME/bin/oidmon`）は、すべての Oracle Internet Directory サーバー・インスタンスのプロセス制御を行うデーモン・プロセスです。

OIDCTL（`$ORACLE_HOME/bin/oidctl`）は、追加の Oracle Internet Directory サーバー・インスタンスの構成や、インスタンス・レベルのプロセス制御の実行を可能にするコマンドライン・ツールです。

Oracle Internet Directory と OPMN の統合

この項では、Oracle Internet Directory と OPMN の相互作用について説明します。この項の項目は次のとおりです。

- Oracle Internet Directory を監視する OPMN のセマンティックス
- OPMN.XML 内の Oracle Internet Directory Snippet
- Oracle Internet Directory を起動する OPMN のセマンティックス
- Oracle Internet Directory を停止する OPMN のセマンティックス
- OIDMON を監視する OPMN のセマンティクス

Oracle Internet Directory を監視する OPMN のセマンティックス

監視ルールは次のとおりです。

- OPMN は Oracle Application Server コンポーネントとしての Oracle Internet Directory の監視を行います。
- OPMN と Oracle Internet Directory の統合とは、OPMN が OIDMON のみを認識し、Oracle Internet Directory サーバー・インスタンスは認識しないということです。
- OPMN は、直接的な OIDMON の起動、停止、再起動および監視のみを行います。OIDMON は、引き続きすべての Oracle Internet Directory サーバー・インスタンスの直接的な起動、停止、再起動および監視を行います。

OPMN.XML 内の Oracle Internet Directory Snippet

Oracle Internet Directory コンポーネント固有のディレクティブは、次の場所にあります。

- OPMN 用の Oracle Internet Directory コンポーネント固有のディレクティブは、`$ORACLE_HOME/opmn/conf/opmn.xml` の `<ias-component id="OID" status="enabled">` タグの下にあります。
- OPMN は `opmn.xml` の OID コンポーネント Snippet 内のディレクティブを使用し、必要に応じて OIDMON および OIDCTL を起動します。
- OIDCTL 関連の要件は `<category id="oidctl parameters">` タグの下にあります。
- OIDMON 関連の要件は `<category id="oidmon parameters">` タグの下にあります。このようなディレクティブは 1 つのみです。
- `opmn.xml` 内の OID Snippet のデフォルト値には、OIDMON 用のエントリおよび OIDCTL 用のエントリが 1 つずつあります。

> **関連資料：**『Oracle Process Manager and Notification Server 管理者ガイド』の「Oracle Internet Directory の構成」の章

Oracle Internet Directory を起動する OPMN のセマンティックス

OPMN による Oracle Internet Directory コンポーネントの起動は次の手順で行われます。

- 次のコマンドのいずれかを使用すると、Oracle Internet Directory コンポーネントを起動することを OPMN に示すことができます。

```
opmnctl startall

opmnctl startproc ias-component=OID
```

- OPMN は OIDMON に対し、`opmn.xml` 内の OID Snippet の oidmon parameters で指定されている適切な引数を付けた `oidmon start` コマンドを発行します。
- opmn.xml 内の OID Snippet に `oidctl start` コマンドを必要とするエントリがある場合、OPMN はこのコマンドを発行します。

`opmnctl startproc ias-component=OID` を使用する場合、opmn.xml パラメータは `opmnctl startall` を使用するときのようにリロードされません。

Oracle Internet Directory を停止する OPMN のセマンティックス

OPMN による Oracle Internet Directory コンポーネントの停止は次の手順で行われます。

- 次のコマンドのいずれかを使用すると、Oracle Internet Directory コンポーネントを停止することを OPMN に示せます。

```
opmnctl stopall

opmnctl stopproc ias-component=OID
```

- OPMN は `oidmon stop` コマンドを発行します。
- OPMN は `oidctl stop` コマンドを発行しません。かわりに、必要に応じて OIDMON の停止セマンティクスが Oracle Internet Directory サーバー・インスタンスの停止を確認します。詳細は、6-6 ページの「OIDMON および ODS_PROCESS 表」を参照してください。

`opmnctl stopproc ias-component=OID` を使用する場合、opmn.xml パラメータは `opmnctl stopall` を使用するときのようにリロードされません。

OIDMON を監視する OPMN のセマンティクス

OPMN は次の手順で OIDMON を監視します。

- OPMN を介して OIDMON を起動すると、OPMN は OIDMON が稼働中であることを確認します。なんらかの理由で OIDMON が停止した場合、OPMN は OIDMON を稼働状態に戻します。
- コマンドラインで `oidmon stop` を発行すると、OIDMON は停止しますが、OPMN はただちに OIDMON を稼働状態に戻します。

Oracle Internet Directory プロセス制御の最良実施例

OPMNCTL および OIDCTL を使用する場合には、次の方法をお薦めします。

- コンポーネントとしての Oracle Internet Directory を停止または起動するには、OPMNCTL を使用します。つまり、すべての Oracle Internet Directory の LDAP、レプリケーションおよび Oracle Directory Integration Platform サーバー・インスタンスの停止または起動にこれを使用します。
  - Oracle Internet Directory の停止に OPMNCTL を使用すると、OPMN は `oidmon stop` を発行します。これにより、OIDMON は構成された LDP、レプリケーションおよび Oracle Directory Integration Platform サーバー・インスタンスをすべて停止します。
  - Oracle Internet Directory の起動に OPMNCTL を使用すると、OPMN は `oidmon start` を発行します。これにより、OIDMON は構成された LDAP、レプリケーションおよび Oracle Directory Integration Platform サーバー・インスタンスをすべて起動します。
- 必要な追加の Oracle Internet Directory サーバー・インスタンスを構成するには、OIDCTL を使用します。
  - デフォルト構成にはない Oracle Internet Directory の LDAP、レプリケーションまたは Oracle Directory Integration Platform サーバーを構成するには、OIDCTL コマンドを使用してそのようなインスタンスを起動します。
  - 構成の配置中に、各インスタンスに対して 1 回のみ `oidctl start` コマンドを発行します。OIDMON の起動および停止セマンティクスが、構成済サーバーが適切に起動または停止しているかどうかを確認します。
- インスタンス・レベルでのみプロセス制御を実行する場合は、OIDCTL を使用します。
  - Oracle Internet Directory の LDAP、レプリケーションまたは Oracle Directory Integration Platform サーバーの特定のインスタンスを停止するには、`oidctl stop` を使用します。サーバーの構成済インスタンスをすべて停止する場合には使用しないでください。
  - まだ構成されていない Oracle Internet Directory の LDAP、レプリケーションまたは Oracle Directory Integration Platform サーバーの追加インスタンスを起動するには、`oidctl start` を使用します。
  - なんらかの理由で `oidctl stop` を使用してサーバー・インスタンスを停止した場合、そのインスタンスはプロセス表から削除され、OIDMON から認識されなくなります。このようにして停止されたインスタンスを再起動するには、`oidctl start` を使用します。

次の項では、お薦めする方法の例を示します。たとえば次のような方法です。

- OID LDAP サーバー・インスタンスのデフォルト構成の変更
- 追加の Oracle Internet Directory LDAP サーバー・インスタンスの構成
- デフォルトの Oracle Internet Directory LDAP サーバー・インスタンスの構成解除
- Oracle Internet Directory レプリケーション・サーバー・インスタンスの構成
- Oracle Directory Integration Platform サーバー・インスタンスの構成

関連資料： この例で使用するコマンド構文の詳細は、『Oracle Identity Management ユーザー・リファレンス』の Oracle Internet Directory Server の管理ツールに関する項を参照してください。

OID LDAP サーバー・インスタンスのデフォルト構成の変更

デフォルトの Oracle Internet Directory インストールでは、デフォルト構成設定（configset0）を使用します。この設定では、1 つのサーバー・プロセスおよび 2 つのデータベース接続のある単一のサーバー・インスタンスが構成されます。この構成では、ユーザー環境での本番の LDAP ロードを適切に処理できない場合があります。その場合、サーバー・プロセス数またはデータベース接続数、あるいはその両方を増やす必要があります。これらは、configset0 の `orclserverprocs` および `orclmaxcc` の属性値をそれぞれ変更することで変更できます。

Oracle Directory Manager を使用して、次の手順でデフォルトの configset を変更します。

1. Oracle Directory Manager を起動します。
2. `orcladmin` としてログインします。
3. 「**サーバー管理**」を展開します。
4. 「**デフォルト構成**」をクリックします。
5. 「**DB の最大接続数**」を必要な値に変更します。一般的には、10 をお薦めします。
6. 必要に応じて、「**要素のプロセスの数**」を変更します。一般的な値は、1 またはシステム上の CPU の数です。
7. 「**適用**」をクリックします。
8. 次のように入力して、Oracle Internet Directory サーバーを再起動します。

   ```
   opmnctl stopproc ias-component=OID
   opmnctl startproc ias-component=OID
   ```

   デフォルト構成設定のその他のパラメータは変更しないことをお薦めします。

追加の Oracle Internet Directory LDAP サーバー・インスタンスの構成

追加の Oracle Internet Directory LDAP サーバー・インスタンスを起動するには、必要な構成値を設定した追加構成設定を追加し、これらの追加構成設定を使用して追加のサーバー・インスタンスを起動します（デフォルト構成設定を使用してデフォルト値を上書きしないでください）。構成設定を追加し、この設定を使用して次の手順で Oracle Internet Directory LDAP サーバー・インスタンスを起動します。

1. Oracle Directory Manager を起動します。
2. 「**サーバー管理**」を展開します。
3. 「**ディレクトリ・サーバー**」を展開します。
4. 「**デフォルト構成設定**」を右クリックします。
5. 「**類似作成**」をクリックします。
6. 新規の構成設定の必要なパラメータを変更します。デフォルト構成設定またはその他の構成設定とポート番号が重複していないことを確認します。
7. 「**OK**」をクリックします。

`configset2` という新規の構成設定を使用して LDAP サーバー・インスタンスを起動するには、次を入力します。

```
oidctl connect=connStr server=oidldapd instance=2 configset=2 start
```

デフォルトの Oracle Internet Directory LDAP サーバー・インスタンスの構成解除

Oracle Internet Directory LDAP サーバー・インスタンスを 1 つ以上の Oracle Internet Directory LDAP サーバー・インスタンスに置き換えるには、opmn.xml を編集してデフォルトの LDAP インスタンスの構成を解除する必要があります。デフォルトでは、opmn.xml には opmnctl start の入力時にデフォルトの Oracle Internet Directory LDAP サーバー・インスタンスを起動しようとする XML Snippet が含まれています。デフォルトの Oracle Internet Directory LDAP サーバー・インスタンスの構成を解除するには、次の手順を実行します。

1. 次のように入力します。

```
oidctl connect=connStr server=oidldapd instance=1 stop
```

2. $ORACLE_HOME/opmn/conf/opmn.xml ファイルを編集し、次の行を削除します。

```
<category id="oidctl-parameters">
<data id="connect" value="iasdb"/>
<data id="startoidldapd" value="true"/>
</category>
```

Oracle Internet Directory レプリケーション・サーバー・インスタンスの構成

OID レプリケーション・サーバーのインスタンスを構成するには、oidctl start コマンドを使用します。次に例を示します。

```
oidctl connect=connStr server=oidrepld instance=1 \
 flags="-h LdapHost -p LdapPort" start
```

oidrepld のインスタンスは、複数起動しないでください。

Oracle Directory Integration Platform サーバー・インスタンスの構成

Oracle Directory Integration Platform サーバーのインスタンスを構成するには、oidctl start コマンドを使用します。次に例を示します。

```
oidctl connect=connStr server=odisrv instance=1 \
 flags="-h LdapHost -p LdapPort" start
```

OIDMON および ODS_PROCESS 表

OIDMON は、Oracle Internet Directory の LDAP、レプリケーションおよびディレクトリ・サーバー・インスタンスを含むすべての Oracle Internet Directory サーバー・インスタンスの起動、停止、再起動および監視を行います。

OIDMON は、ODS データベース・ユーザー・スキーマの ods_process 表の内容を定期的に読み取り、その内容により伝達される目的に基づいて動作します。周期は oidmon の起動時に使用されるコマンドライン引数 sleep の値によって制御されます。デフォルト値は 10 秒です。

表 6-1 で、ODS_PROCESS 表のプロセス制御に関する情報について説明します。

表 6-1 ODS_PROCESS 表のプロセス制御項目

項目	意味
Instance	指定されたホスト上の指定されたサーバー ID に対する一意のインスタンス番号
PID	稼働中のサーバーのプロセス ID
ServerID	サーバー ID（2=OIDLDAPD、3=OIDREPLD、7=ODISRV）
Flags	サーバー・インスタンスに渡す必要のあるコマンドライン引数
Hostname	このサーバーが存在している必要のあるホスト名
Configset	Configset の情報
State	サーバー・インスタンスの状態（0= 停止、1= 起動、2= 実行中、3= 再起動、4= シャットダウン）
RetryCount	サーバー・インスタンスが正常に起動するまでの起動試行回数

注意：

- （Instance、ServerID、Hostname には）一意性制約があります。
- ここでは、概念を示す目的のみで ods_process の詳細を説明しています。ユーザーが OIDCTL を使用せずに表を更新することは不適切であり、オラクル社ではこのような更新をサポートしていません。

OIDMON は Oracle Internet Directory サーバー・インスタンスに関して、次のアクションを実行します。

- OIDMON の停止時には、停止する前に次のタスクを実行します。
  - OIDMON はノード上のすべてのアクティブな（稼働中）サーバー・インスタンスを停止します。つまり、OIDMON と同一のホスト上にあるすべてのアクティブなインスタンスを停止します。
  - OIDMON は、ods_process 表内の合致するホスト名を持つ state 列の値を 4 に更新します。
- OIDMON の起動時には、ods_process 表の `state` 値が 1 または 4 であり、OIDMON がアクティブとなっているホストと `hostname` 値が合致するすべての Oracle Internet Directory サーバー・インスタンスが起動します。

OIDCTL のプロセス制御セマンティクス

この項では、OIDCTL を使用した Oracle Internet Directory サーバー・インスタンスの起動および停止のセマンティクスを説明します。

OIDCTL は、ODS データベース・ユーザー・スキーマの ods_process 表を更新することによって、特定の Oracle Internet Directory サーバー・インスタンスを起動、停止または再起動することを伝達します。

Oracle Internet Directory サーバー・インスタンスの起動時のプロセスは次のとおりです。

- OIDCTL コマンドライン・ユーティリティを使用して、特定の Oracle Internet Directory サーバー・インスタンスを起動する目的を伝達します。
- OIDCTL は OIDMON に目的を伝達するため、ods_process 表に行を挿入します。
- ods_process 表の一意性制約に違反する場合、OIDCTL は「*** インスタンス番号はすでに使用されています。***」というエラーを報告します。
- OIDMON はこの情報を読み取り、サーバー・インスタンスを起動し、適切な ods_process 表の state 列および PID 列を更新します。

OIDCTL を使用した Oracle Internet Directory サーバー・インスタンスの停止時のプロセスは次のとおりです。

- OIDCTL コマンドライン・ユーティリティを使用して、特定の Oracle Internet Directory サーバー・インスタンスを停止する目的を伝達します。
- OIDCTL は OIDMON に目的を伝達するため、ods_process 表の対応する行を更新します。
- 対応する行が見つからない（指定されたインスタンスが構成されていない）場合、OIDCTL は「*** 実行していないインスタンスは停止できません。」というエラーを報告します。
- OIDCTL は状態値を 0 に更新します。
- OIDMON はこの情報を読み取り、サーバー・インスタンスを停止し、このサーバー・インスタンスを示す行を ods_process 表から削除します。

第 II 部

基本的なディレクトリ管理

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

7

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。

この章の項目は次のとおりです。

> **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 4 章「インストール後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

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

この項の項目は次のとおりです。

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

> **関連項目：** 構成設定エントリの概要は、3-7 ページの「構成設定エントリ」を参照してください。

構成設定エントリ管理のための事前の考慮事項

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

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

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

図 7-1 に、それぞれ異なる値を持つ、3 つのディレクトリ・サーバー・インスタンスを示します。

図 7-1 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

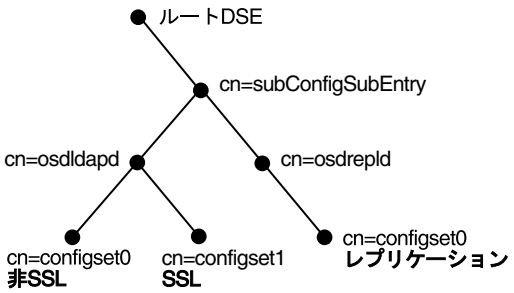


図 7-1 は、次のものを表しています。

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

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

関連資料：

- SSL の構成パラメータの詳細は、第 17 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 30 章「Oracle Internet Directory レプリケーションのインストールと構成」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、『Oracle Identity Management ユーザー・リファレンス』の OID 構成のスキーマ要素に関する項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。

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

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

ディレクトリ・サーバー・インスタンスを再起動する方法は、『Oracle Identity Management ユーザー・リファレンス』の Oracle Internet Directory サーバーの管理ツールに関する項を参照してください。

この項の項目は次のとおりです。

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

構成設定エントリを表示する手順は、次のとおりです。

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

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

   関連項目： 7-5 ページの「Oracle Directory Manager を使用した構成設定エントリの変更」

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

初めて構成設定エントリを追加するときには、次の操作が可能です。

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

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

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」、「**サーバー管理**」、「**ディレクトリ・サーバー**」の順に展開します。
2. 「**デフォルト構成設定**」を選択します。
3. ツールバーの「**類似作成**」ボタンを選択します。「構成設定」ダイアログ・ボックスに「**一般**」タブ・ページが表示されます。
4. 「**一般**」タブ・ページの各フィールドに情報を入力します。詳細は、A-25 ページの表 A-40 を参照してください。
5. 「**SSL 設定**」タブを選択し、各フィールドに情報を入力します。詳細は、A-25 ページの表 A-41 を参照してください。
6. 「**適用**」を選択します。
7. コマンドを有効にするために、サーバー・インスタンスを再起動します。

関連資料：

- 『Oracle Identity Management ユーザー・リファレンス』の `oidctl` コマンドライン・ツールのリファレンス
- 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。
- 14-6 ページの「デバッグ・ロギング・レベルの設定」

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

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「<ディレクトリ・サーバー・インスタンス>」、「**サーバー管理**」、「**ディレクトリ・サーバー**」の順に展開します。
2. 「**デフォルト構成設定**」を選択します。
3. ツールバーの「**作成**」ボタンを選択します。「構成設定」ダイアログ・ボックスに「**一般**」タブ・ページが表示されます。
4. 「**一般**」タブ・ページの各フィールドに情報を入力します。詳細は、A-25 ページの表 A-40 を参照してください。
5. 「**SSL 設定**」タブを選択し、各フィールドに情報を入力します。これらのフィールドについては、A-25 ページの表 A-41 を参照してください。
6. 「**OK**」を選択します。

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

構成設定エントリを変更する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「<ディレクトリ・サーバー・インスタンス>」、「**サーバー管理**」、「**ディレクトリ・サーバー**」の順に展開します。
2. 変更する構成設定を選択します。右側のペインのタブ・ページに、構成設定が表示されます。
3. 「**一般**」タブ・ページの各フィールドの情報を変更します。詳細は、A-25 ページの表 A-40 を参照してください。変更内容を保存するには、「**適用**」を選択します。
4. 「**SSL 設定**」タブを選択し、各フィールドの情報を変更します。詳細は、A-25 ページの表 A-41 を参照してください。変更内容を保存するには、「**適用**」を選択します。
5. コマンドを有効にするために、サーバー・インスタンスを再起動します。

関連資料 :

- 『Oracle Identity Management ユーザー・リファレンス』の `oidctl` コマンドライン・ツールのリファレンス
- Oracle Wallet Manager を使用して Oracle Wallet の位置と Oracle Wallet パスワードを設定する手順は、『Oracle Advanced Security 管理者ガイド』を参照してください。

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

構成設定エントリを削除する手順は、次のとおりです。

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

関連資料 : 『Oracle Identity Management ユーザー・リファレンス』の `oidctl` コマンドライン・ツールのリファレンス

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、**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。

> **関連資料：** LDIF の詳細は、『Oracle Identity Management ユーザー・リファレンス』の LDIF ファイルの形式化規則と例に関する項を参照してください。

この項の項目は次のとおりです。

- ldapadd を使用した構成設定エントリの追加
- ldapmodify を使用した構成設定エントリの変更と削除

ldapadd を使用した構成設定エントリの追加

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

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

1. テキスト・エディタで入力ファイルを作成します。

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

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

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

2. 入力ファイルを使用して ldapadd を実行します。

   コマンド・プロンプトで、入力ファイルを追加するコマンドを入力します。

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

   関連資料：

   - 『Oracle Identity Management ユーザー・リファレンス』の LDIF ファイルの形式化規則と例に関する項
   - このコマンドで使用できるオプションの詳細は、『Oracle Identity Management ユーザー・リファレンス』の `ldapadd` コマンドライン・ツールのリファレンスを参照してください。
   - 構成設定エントリの属性の説明は、『Oracle Identity Management ユーザー・リファレンス』の OID 構成のスキーマ要素に関する項を参照してください。

ldapmodify を使用した構成設定エントリの変更と削除

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

1. 入力ファイルを作成します。

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

   入力ファイルは LDIF フォーマットで作成する必要があります。

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

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

2. 入力ファイルを参照する ldapmodify を実行します。

   コマンド・プロンプトで、入力ファイルを参照するコマンドを入力します。

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

   関連資料：

   - 『Oracle Identity Management ユーザー・リファレンス』の LDIF ファイルの形式化規則と例に関する項
   - ldapmodify の詳細とそのオプションのリストは、『Oracle Identity Management ユーザー・リファレンス』の `ldapmodify` コマンドライン・ツールのリファレンスを参照してください。
   - 構成設定エントリの属性の説明は、『Oracle Identity Management ユーザー・リファレンス』の OID 構成のスキーマ要素に関する項を参照してください。

システム操作属性の設定

操作**属性**は、アプリケーション属性とは異なり、ディレクトリ自体の操作に関係します。一部の操作情報（エントリのタイムスタンプなど）は、サーバーを制御するためにディレクトリによって指定されます。アクセス情報などのその他の操作情報は、管理者が定義し、ディレクトリ・プログラムで処理時に使用されます。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。

この項の項目は次のとおりです。

関連項目： 3-11 ページの「属性情報の種類」

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

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

Oracle Directory Manager に表示されるシステム操作属性フィールドの説明は、A-26 ページの表 A-42 を参照してください。

ldapmodify を使用したシステム操作属性の設定

システム操作属性を変更するには、ldapmodify を使用します。変更可能なシステム操作属性は、『Oracle Identity Management ユーザー・リファレンス』で、Oracle Identity Management の LDAP の属性リファレンスに関する項を参照してください。

> **関連資料：** ldapmodify の詳細とそのオプションのリストは、『Oracle Identity Management ユーザー・リファレンス』の `ldapmodify` コマンドライン・ツールのリファレンスを参照してください。

ネーミング・コンテキストの管理

ユーザーが特定のネーミング・コンテキストを検索できるように、それらのネーミング・コンテキストを公開できます。この項の項目は次のとおりです。

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

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

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

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

ネーミング・コンテキストを公開する前に、次のことを確認してください。

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

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

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

ldapmodify を使用したネーミング・コンテキストの公開

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

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

スーパーユーザー、ゲスト・ユーザーおよびプロキシ・ユーザーの管理

この項の項目は次のとおりです。

- スーパーユーザー、ゲスト・ユーザーおよびプロキシ・ユーザーの説明
- 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

スーパーユーザー、ゲスト・ユーザーおよびプロキシ・ユーザーの説明

7-9 ページの表 7-1 は、スーパーユーザー、ゲスト・ユーザーおよびプロキシ・ユーザーを定義したものです。

Oracle Directory Manager または ldapmodify のどちらかを使用して、ユーザーごとにユーザー名とパスワードを管理できます。

表 7-1 スーパーユーザー、ゲスト・ユーザーおよびプロキシ・ユーザーの定義

ユーザーのタイプ	定義
スーパーユーザー	ディレクトリ情報への完全なアクセス権限を持つ特別なディレクトリ管理者。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。 **注意：**このパスワードは、インストール後にすぐに変更することをお薦めします。
ゲスト・ユーザー	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。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。
プロキシ・ユーザー	通常、ファイアウォール、Oracle Delegated Administration Services のようなアプリケーション、RADIUS サーバーなどの中間層を備えた環境でのユーザー。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。 **関連項目：**プロキシ・ユーザーの詳細は、16-6 ページの「間接認証」を参照してください。

関連項目： アクセス権限の設定方法は、第 18 章「ディレクトリ・アクセス制御」を参照してください。

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

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

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

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

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」を展開して、ディレクトリ・サーバーを選択します。そのサーバーに対応するタブ・ページが右側のペインに表示されます。
2. 「**システム・パスワード**」タブを選択します。このページに、各タイプのユーザーに対するカレント・ユーザー名とパスワードが表示されます。各パスワードは、パスワードのフィールドには表示されないことに注意してください。
3. A-29 ページの表 A-43 で説明されているとおり、「**システム・パスワード**」タブ・ページ内の該当するフィールドを編集します。変更内容を保存するには、「**適用**」を選択します。

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

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

表 7-2 スーパーユーザー、ゲスト・ユーザーおよびプロキシ・ユーザーのユーザー名、パスワードおよび属性

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

たとえば、スーパーユーザーのパスワードを superuserpassword に変更するには、ldapmodify で、次のように記述した LDIF ファイルを使用して DSE を変更します。

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

関連資料： ldapmodify の構文と使用方法は、『Oracle Identity Management ユーザー・リファレンス』の ldapmodify コマンドライン・ツールのリファレンスを参照してください。

匿名ユーザーによるバインドの管理

Oracle ディレクトリ・サーバーは、匿名ユーザーによるバインドを許可するようにも禁止するようにも構成できます。この動作は、ルート DSE エントリの orclAnonymousBindsFlag 属性で制御します。表 7-3 に、orclAnonymousBindsFlag に指定可能な値と、ディレクトリ・サーバーの動作を示します。

表 7-3 orclanonymousbindflag の値とディレクトリ・サーバーの動作

orclAnonymousBindsFlag の値	ディレクトリ・サーバーの動作
0	匿名ユーザーによるバインドを禁止。
1	匿名ユーザーによるバインドを許可（デフォルト）。
2	匿名ユーザーによるバインドを許可。ただし、許可されるのは、ルート DSE エントリに対する匿名ユーザーの検索操作のみ。

ディレクトリ・サーバーでは、デフォルトで匿名ユーザーによるバインドが許可されます。つまり、orclAnonymousBindsFlag 属性は 1 に設定されています。

次の例は、ldapmodify コマンドライン・ツールを使用して匿名ユーザーによるバインドを無効にする方法を示しています。

```
ldapmodify -h hostname -p port -D cn=orcladmin -w super_user_pwd <<EOF
dn:
changetype: modify
replace: orclanonymousbindsflag
orclanonymousbindsflag: 0
EOF
```

関連項目：

- 7-7 ページの「システム操作属性の設定」
- A-26 ページの表 A-42「Oracle Directory Manager に表示されるシステム操作属性」

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。これは、次の手順に従って行います。

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

   関連項目： 構成設定エントリの変更方法は、7-3 ページの「Oracle Directory Manager を使用したサーバーの構成設定エントリの管理」を参照してください。

アイドル状態の LDAP 接続のクローズ

アイドル状態の LDAP 接続がクローズするまでのアイドル時間を分単位で指定できます。この処理を行うには、`orclLDAPconnTimeout` 属性に値を設定します。この属性の詳細は、『Oracle Identity Management ユーザー・リファレンス』で、Oracle Identity Management の LDAP の属性リファレンスに関する項を参照してください。

10*g*（10.1.4.0.1）では、14-15 ページの「Oracle Internet Directory サーバー管理機能の機能」で説明しているように、操作統計追跡のために構成されていないユーザーに対してのみこれを設定できます。

注意： Oracle Internet Directory サーバーでは、構成された接続タイムアウトの値と同じ間隔で、アイドル接続タイムアウトを処理します。これによりパフォーマンスのオーバーヘッドが最小限に抑えられます。その結果、接続の削除に、事前に構成された接続タイムアウトの値より長くかかる場合があります。しかし、この値の 2 倍以上の時間はかかりません。

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

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

関連資料：『Oracle Identity Management ユーザー・リファレンス』の `oidpasswd` コマンドライン・ツールのリファレンス

別名エントリの間接参照

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

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

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

別名エントリの概要

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

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

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

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

図 7-2 およびその後に続く説明では、別名エントリの間接参照の例を示します。

図 7-2 別名エントリの例

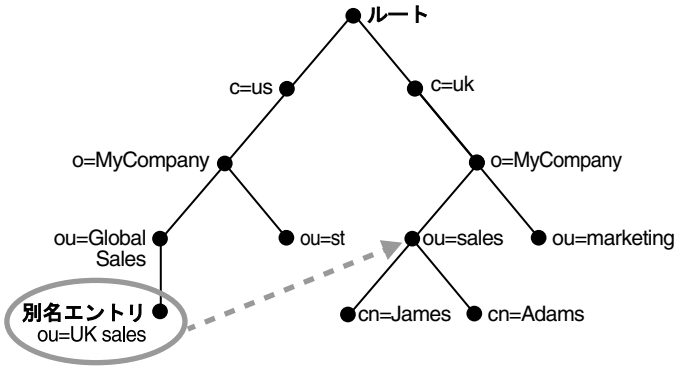


図 7-2 で、ou=uk sales,ou=global sales,o=myCompany,c=us は、ou=sales,o=myCompany,c=uk エントリを指し示す別名エントリです。

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

例 : 別名エントリ間接参照の使用方法

この項では、次の例について説明します。

- 例 : 別名エントリの追加
- 例 : 別名エントリによるディレクトリの検索
- 例 : 別名エントリの変更

例 : 別名エントリの追加

別名エントリを追加するには、LDIF の通常のエントリ、および実際のエントリを指し示す別名エントリを作成します。この例の手順を実行すると、7-14 ページの図 7-3 に示すツリーが生成されます。

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

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

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

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

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

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

2. 次のコマンドを使用して、これらのエントリをディレクトリに追加します。

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

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

関連項目： エラー・メッセージは、7-16 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 7-3 My_file.ldif の作成結果を示すツリー

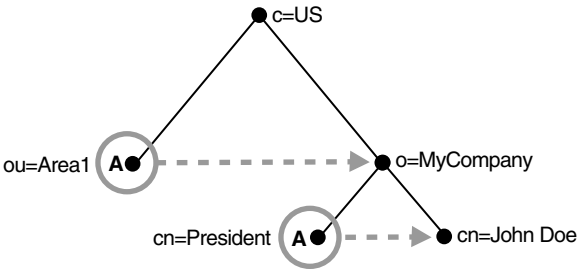


図 7-3 の文字 A は、別名エントリを表します。

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

例 : 別名エントリによるディレクトリの検索

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

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

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

注意： 10*g*（10.1.4.0.1）では、Oracle Internet Directory は次のオプションをサポートしていません。

- `ldapsearch` のオプション `-a search` と `-a always`
- RFC2251 で説明されている `extensibleMatch` 機能

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

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

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

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

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

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

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

ディレクトリ・サーバーは、2 つの手順で検索を実行します。

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

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

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

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

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

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

ディレクトリ・サーバーは、2 つの手順で検索を実行します。

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

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

したがって、この検索では次の情報が返されます。

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

例 : 別名エントリの変更

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

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

次のコマンドを使用して、別名エントリを変更します。

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

成功メッセージとエラー・メッセージ

表 7-4 は、間接参照の別名エントリに関するメッセージと、各メッセージの意味を示しています。

表 7-4 エントリ別名間接参照メッセージ

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

分散環境でのディレクトリ・サーバーの位置の特定

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

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

この項では、サーバー情報の位置を特定する 2 通りの方法について説明します。この項の項目は次のとおりです。

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

関連資料：

- `http://www.ietf.org` の Michael P. Armijo 他による「Discovering LDAP Services with DNS」
- `http://www.ietf.org` の Internet RFC 2782 の「A DNS RR for specifying the location of services (DNS SRV)」

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

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

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

ファイル ldap.ora は LDAP クライアントのファイル・システムに存在しています。クライアントは、このファイルを次のファイル・システム・ディレクトリから優先順位に従って検索します。

1. LDAP_ADMIN 環境変数が指し示すディレクトリ
2. *ORACLE_HOME*/ldap/admin のディレクトリ（または Microsoft Windows の場合、*ORACLE_HOME*¥ldap¥admin）
3. TNS_ADMIN 環境変数が指し示すディレクトリ
4. *ORACLE_HOME*/network/admin のディレクトリ（または Microsoft Windows の場合、*ORACLE_HOME*¥network¥admin）

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

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

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

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

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

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

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

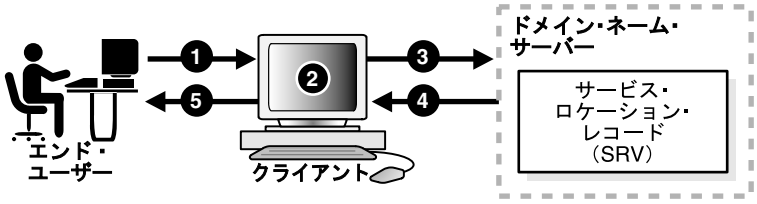
クライアントが DNS を使用してディレクトリ・サーバーの位置を特定する方法

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

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

図 7-4 とその後の説明で、クライアントの視点からディレクトリ・サーバーの位置を特定するプロセスを示します。

図 7-4 DNS を使用してディレクトリ・サーバーの位置を特定するクライアント



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

関連資料：

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

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

ドメイン・ネーム・システムへのディレクトリ・サーバーの登録

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

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

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

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

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

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

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

表 7-5 に引数を示します。次に、Oracle Internet Directory 固有の形式を使用した SRV レコードの例を示します。

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

SRV レコード用の標準形式

標準形式は、次のとおりです。

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

表 7-5 に引数を示します。次に、非 SSL ベースのディレクトリ・サーバー用の標準形式を使用した SRV レコードの例を示します。

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

表 7-5 サービス・ロケーション・レコード（SRV）の引数

引数	説明
Service	非 SSL ベースのサーバーの場合、この引数の値は `ldap` です。SSL ベースのサーバーの場合は、`ldaps` です。
Proto	常に、値は `tcp` です。
Product	常に、値は `oid` です。
Domain	ドメイン名。通常は、ディレクトリ・サーバーによって作成されたネーミング・コンテキストの DN をドメイン名に変換して取得されます。 **関連項目：**7-18 ページの「クライアントが DNS を使用してディレクトリ・サーバーの位置を特定する方法」を参照してください。
TTL	有効期間。この引数は標準 DNS の意味を持っています。情報のソースを再度問い合せるまでリソース・レコードをキャッシュしておくことができる時間を指定します。
Class	この引数は標準 DNS の意味を持っています。SRV レコードは IN クラスで発生します。
Type	すべての SRV レコードで、この引数の値は SRV です。
Priority	ディレクトリ・サーバーの優先順位。クライアントは、優先順位番号が一番小さいターゲット・ホストと通信する必要があります。

表 7-5 サービス・ロケーション・レコード（SRV）の引数（続き）

引数	説明
Weight	サーバー選択メカニズム。この引数は、同じ優先順位を持つエントリに対して相対的な重みを指定します。複数の SRV が同じ優先順位を持っている場合は、次のプロトコルに従って順位付けされます。 **1.** 次に通信するターゲットを選択するために、順位付けされていないすべての SRV リソース・レコードを任意の順序で並べます。ただし、重み 0 のレコードはすべてリストの先頭に置きます。 **2.** これらのリソース・レコードの重みの合計を計算します。また、各リソース・レコードには、選択した順序での重みの累計を関連付けます。 **3.** 0 から計算した合計までの間の一様乱数を選択し、選択した順序で、重みの累計値が初めて選択した乱数以上となるリソース・レコードを選択します。選択した SRV リソース・レコードに指定されているターゲット・ホストが、クライアントによって次に通信されるホストです。 **4.** 順位付けされていない SRV リソース・レコードのセットから、この SRV リソース・レコードを削除します。 **5.** 順序付けされていない SRV リソース・レコードに前述のアルゴリズムを適用して、次のターゲット・ホストを選択します。 **6.** 順位付けされていない SRV リソース・レコードがなくなるまで、この順位付けプロセスを続けます。 **7.** このプロセスを各優先順位に対して繰り返します。
Port	ディレクトリ・サービス用のターゲット・ホストのポート。
Target	ディレクトリ・サーバーが稼働しているホストのドメイン名。

注意： ディレクトリ・サーバーが別のホストに移動された場合、または別のポートで稼働している場合は、対応する SRV リソース・レコードをそれに応じて更新する必要があります。

8

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。この章の項目は次のとおりです。

- 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
- 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 3 章「ディレクトリの概念およびアーキテクチャ」を参照してください。

バルク・ツールについては、第 9 章「バルク・ツールの使用方法」で説明しています。

Oracle Directory Manager を使用したエントリの管理

この項の項目は次のとおりです。

Oracle Directory Manager を使用したエントリの検索

すべてのエントリの表示にはナビゲータ・ペインを、1 つ以上の特定のエントリの検索には Oracle Directory Manager の検索機能を使用できます。

エントリを表示するには、ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」、「**エントリ管理**」の順に展開します。

ツリーのルートが最初にリストされ、次に第 2 レベル、第 3 レベルというように、左から右へ移動してリストされます。サブツリーには、各エントリの **RDN** が階層順にリストされます。サブツリー内の下位レベルのエントリを表示するには、親エントリの横のプラス記号（+）をクリックします。

ディレクトリ・エントリを検索する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」、「**エントリ管理**」の順に展開します。右側のペインに「**検索**」フィールドが表示されます。
2. 「**検索のルート**」フィールドに、検索のルートの **DN** を入力します。

   たとえば、Americas にある IMC 組織の Manufacturing 部門に勤務する従業員を検索するとします。検索のルートの識別名は、次のようになります。

   ```
   ou=Manufacturing,ou=Americas,o=IMC,c=US
   ```

   この識別名を「**検索のルート**」テキスト・ボックスに入力します。

   ディレクトリ情報ツリー（DIT）を参照して検索のルートを選択することもできます。この手順は、次のとおりです。

   a. 「**検索のルート**」フィールドの右側の「**参照**」をクリックします。「識別名 (DN) パスの選択 : ツリー表示」ダイアログ・ボックスが表示されます。
   b. ツリー・ビューの横のプラス記号（+）をクリックして、そのエントリを表示します。
   c. 検索のルートのレベルを表すエントリまで、ナビゲートします。
   d. そのエントリを選択して、「**OK**」をクリックします。検索のルートの識別名が、右側のペインの「**検索のルート**」テキスト・ボックスに表示されます。
3. 「**最大結果件数**」ボックスに、検索で取り出すエントリの最大数を入力します。デフォルトは 200 です。ここで設定できるディレクトリ・サーバーのエントリ数は、最大 1000 です。
4. 「**最長検索時間**」ボックスに、検索の最大時間を秒数で入力します。ここで入力する値は、少なくともデフォルト値の 25 以上にする必要があります。ここで指定できるディレクトリ・サーバーの最大検索時間は、1 時間です。
5. 「**検索の深さ**」のリストで、検索するディレクトリ情報ツリーのレベルを選択します。

   オプションは次のとおりです。

   - **ベース :** 特定のディレクトリ・エントリを取り出します。この検索レベルの場合は、検索基準バーを使用して、属性 `objectClass` とフィルタ「存在」を選択します。
   - **1 レベル :** 検索のルートの 1 レベル下から始まるすべてのエントリに検索を制限します。
   - **サブツリー :** 検索のルートを含め、サブツリー全体のエントリを検索します。

6. 「**検索基準**」ボックスで、検索基準バーのリストとテキスト・フィールドを使用して、検索基準をさらに詳細に指定します。

   a. 検索基準バーの一番左のリストから、検索するエントリの属性を選択します。各エントリですべての属性が使用されているわけではないため、指定した属性が、検索しているエントリの属性に実際に一致していることを確認する必要があります。一致する属性がない場合は、検索に失敗します。

   b. 検索基準バーの中央のリストから、フィルタを選択します。オプションの説明は、A-31 ページの表 A-45 を参照してください。

   c. 検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。たとえば、選択した属性が cn の場合は、検索する個々の一般名を入力します。

7. 検索をさらに詳細に指定するには、「**検索基準**」ボックスのボタンを使用して検索基準バーを拡張します。これらのフィールドの説明は、A-32 ページの表 A-46 を参照してください。

8. 「**検索**」をクリックします。検索結果は「**識別名**」ボックスに表示されます。

関連項目： 検索で表示するエントリ数と検索の制限時間の設定方法は、7-11 ページの「アクティブ・サーバー・インスタンスの情報の表示」を参照してください。

Oracle Directory Manager を使用した特定エントリの属性の表示

検索結果の表示後、属性を参照するエントリをクリックします。「エントリ」ダイアログ・ボックスに、そのエントリの属性が表示されます。

一部の属性は、識別名である可能性もあります。たとえば、指定した従業員の 1 つの属性がその従業員のマネージャで、そのマネージャに識別名がある場合があります。この場合、従業員の「エントリ」ダイアログ・ボックスを表示すると、「**マネージャ**」テキスト・ボックスの横に「**参照**」ボタンが表示されます。そのマネージャの情報を検索するには、「**参照**」をクリックして「ディレクトリ : エントリ管理」ダイアログ・ボックスを表示し、8-2 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、11-11 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、ユーザーのエントリおよびグループ・エントリを追加する方法を説明します。

注意： エントリを追加または削除する場合、Oracle ディレクトリ・サーバーではエントリ属性値の構文検証は行われません。

Oracle Directory Manager を使用した新規エントリの追加

Oracle Directory Manager でエントリを追加または削除するには、親エントリに対する書込みアクセス権限があり、新規エントリの識別名を認識している必要があります。

新規エントリを追加する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」の順に展開します。

2. 「**エントリ管理**」を選択します。

3. ツールバーの「**作成**」ボタンをクリックします。「新規エントリ」ダイアログ・ボックスが表示されます。

4. 「**識別名**」フィールドに、完全な識別名を入力します。「**参照**」をクリックして、追加するエントリの親の識別名を見つけ、選択することもできます。選択したエントリが「**識別名**」

フィールドに表示されます。その親の識別名の左に新規エントリの相対識別名を入力し、その後にカンマを付けます。

5. 新規エントリのオブジェクト・クラスを指定するには、「**オブジェクト・クラス**」ボックスの横の「**追加**」をクリックします。「スーパー・クラス・セレクタ」ダイアログ・ボックスが表示されます。

> **注意：** Oracle Internet Directory セルフ・サービス・コンソールにユーザー・エントリを表示するには、エントリを `inetOrgPerson` オブジェクト・クラスに割り当てる必要があります。

6. 「スーパー・クラス・セレクタ」ダイアログ・ボックスでオブジェクト・クラスを選択して、「**選択**」をクリックします。オブジェクト・クラス・リストからオブジェクト・クラスを選択すると、「新規エントリ」ダイアログ・ボックスの下半分のタブ・ページにあるウィンドウに、必須属性とオプション属性が表示されます。必須属性のフィールドには、値を入力する必要があります。オプション属性のフィールドには、値を必ずしも入力する必要はありません。
7. オブジェクト・クラスを選択して、対応する属性に値を入力した後、「**OK**」をクリックします。

Oracle Directory Manager の既存エントリを利用したエントリの追加

Oracle Directory Manager では、既存エントリをコピーしてその識別名を変更する方法で、新規エントリを作成できます。この操作を行う場合は、名前やアドレスなどの属性も、新規識別名に対応するように変更してください。エントリを追加するには、その親に対する書込みアクセス権限が必要です。

> **ヒント：** 検索ペインで他の類似エントリを参照して、新規識別名用のテンプレートを検索できます。

既存エントリを利用してエントリを追加する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「<ディレクトリ・サーバー・インスタンス>」の順に展開します。
2. 「**エントリ管理**」を選択します。
3. 右側のペインに「検索」インタフェースが表示されます。このペインで、テンプレートとして使用するエントリを検索します。
4. 取り出したエントリから、テンプレートとして使用するエントリをダブルクリックします。そのエントリに対応する「エントリ」ダイアログ・ボックスが表示されます。
5. 「エントリ」ダイアログ・ボックスで、「**類似作成**」をクリックします。「新規エントリ：類似作成」ダイアログ・ボックスが表示されます。
6. このエントリを作成するエントリに調整するために、重要なフィールドを変更します。この操作で、識別名と一般名は必ず変更する必要があります。変更しないと、新規エントリのデータは保存されません。たとえば、Henri Latour のエントリをテンプレートとして使用して Henri Latrobe のエントリを作成する場合は、識別名の `cn=Henri Latour` を `cn=Henri Latrobe` に変更する必要があります。また、この他にも従業員番号や電話番号など、一意であることが必要な属性をすべて変更する必要があります。
7. 「**OK**」をクリックして、変更内容を保存します。

> **関連資料：** フィールドに情報を追加する方法は、このダイアログ・ボックスのオンライン・ヘルプを参照してください。

例 : Oracle Directory Manager を使用したユーザー・エントリの追加

この例では、Anne Smith というユーザーを作成し、パスワードを割り当てます。

1. administrator でログインします。
2. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」の順に展開します。
3. 「**エントリ管理**」を選択します。
4. ツールバーの「**作成**」ボタンをクリックします。「新規エントリ」ダイアログ・ボックスが表示されます。
5. 「**識別名**」フィールドに、完全な識別名を入力します。「**参照**」ボタンをクリックして、このエントリの親の識別名を探し、親の識別名の左に相対識別名、つまり `cn=Anne Smith` を入力して、その後にカンマを付けることもできます。

   注意 : ユーザー名にチルダ（~）は使用できません。

6. 「オブジェクト・クラス」ボックスの右の「**追加**」をクリックします。「スーパー・クラス・セレクタ」ダイアログ・ボックスが表示されます。
7. 「スーパー・クラス・セレクタ」ダイアログ・ボックスで `person` オブジェクト・クラスを選択して、「**選択**」をクリックします。「新規エントリ」ダイアログ・ボックスに戻ります。
8. 「新規エントリ」ダイアログ・ボックスで「**オプション・プロパティ**」タブをクリックし、「ユーザー・パスワード」ウィンドウまでスクロールします。
9. Anne Smith 用のパスワードを入力します。

関連項目 :

- 8-2 ページの「Oracle Directory Manager を使用したエントリの検索」
- 13-6 ページの「グループ・エントリの管理」
- 18-3 ページの「セキュリティ・グループ」
- アクセス権限の詳細は、3-18 ページの「グローバリゼーション・サポート」および第 18 章「ディレクトリ・アクセス制御」を参照してください。

Oracle Directory Manager を使用したエントリの変更

既存エントリに補助型オブジェクト・クラスを追加できます。

すでにエントリで使用されているオブジェクト・クラスには、オプション属性は追加できますが、必須属性は追加できません。すでに使用されているオブジェクト・クラスにオプション属性を追加する場合、特別な規則は適用されません。オプション属性は、空の属性としてこれらのエントリに追加されます。

注意： エントリを追加または削除する場合、Oracle ディレクトリ・サーバーではエントリ属性値の構文検証は行われません。

エントリを変更する手順は、次のとおりです。

1. 8-2 ページの「Oracle Directory Manager を使用したエントリの検索」の説明に従って、変更するエントリの検索を実行します。
2. 右側のペインの「**識別名**」ボックスで、変更するエントリを選択します。
3. 「**編集**」をクリックします。「エントリ」ダイアログ・ボックスが表示されます。
4. 該当するフィールドを変更し、「**プロパティの選択**」タブ・ページを選択します。追加または変更する属性が表示されない場合は、タブ・ページの一番上にある「**プロパティの表示：すべて**」を選択します。
5. 「**プロパティ**」タブ・ページで、編集可能な属性の値を変更します。
6. 「**適用**」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、8-5 ページの「例 : Oracle Directory Manager を使用したユーザー・エントリの追加」の項で Anne Smith 用に作成したエントリ用のパスワードを変更します。

1. Anne Smith エントリの検索を実行します。
2. 右側のペインの「**識別名**」ボックスで、Anne Smith のエントリを選択します。
3. 「**編集**」をクリックします。
4. 「エントリ」ダイアログ・ボックスで、「ユーザー・パスワード」ウィンドウまでスクロールしてその値を変更します。
5. 「**OK**」をクリックします。

Oracle Directory Manager を使用した属性オプション付きエントリの管理

この項では、属性オプションを追加、変更および削除する方法を説明します。

> **関連項目：** 属性オプション付きエントリの検索方法は、8-2 ページの「Oracle Directory Manager を使用したエントリの検索」を参照してください。

Oracle Directory Manager を使用した、既存エントリへの属性オプションの追加

> **注意：** Oracle Internet Directory 10*g*（10.1.4.0.1）の Oracle Directory Manager では、エントリを作成した時点で、そのエントリに属性オプションを追加することはできません。すでに存在しているエントリに対してのみ、Oracle Directory Manager を使用して属性オプションを追加できます。

既存のエントリに属性オプションを追加する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」、「**エントリ管理**」の順に展開します。
2. 属性オプションを追加するエントリを選択します。対応するタブ・ページが、右側のペインに表示されます。
3. 右側のペインにある「**プロパティ**」タブ・ページの「**プロパティの表示**」フィールドで、「**拡張**」を選択します。この操作に伴って、「**プロパティ**」タブ・ページが変わります。
4. 「**属性**」フィールドで、オプションを追加する属性（たとえば、`ou`）を選択します。
5. 「**属性オプション**」フィールドで、属性オプション（たとえば、`lang-en`）を入力します。
6. 「**属性値**」フィールドで、指定する属性オプションの値（たとえば、`Server Technologies`）を入力します。指定した属性オプションに複数の値を追加するには、各値をセミコロンで区切ります。
7. 「**適用**」をクリックします。

Oracle Directory Manager を使用した属性オプションの変更

属性オプションを変更する手順は次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」、「**エントリ管理**」の順に展開します。
2. 変更する属性オプションのエントリを選択します。対応するタブ・ページが、右側のペインに表示されます。
3. 「**プロパティ**」タブ・ページの「**プロパティの表示**」フィールドで、「**NULL 以外の値のみ**」または「**すべて**」を選択します。
4. 変更する属性オプションを含むフィールドまでスクロールします。
5. フィールドの値を変更します。
6. 「**適用**」をクリックします。

Oracle Directory Manager を使用した属性オプションの削除

属性オプションを削除する手順は次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「<ディレクトリ・サーバー・インスタンス>」、「**エントリ管理**」の順に展開します。
2. 属性オプションを削除するエントリを選択します。対応するタブ・ページが、右側のペインに表示されます。
3. 「**プロパティ**」タブ・ページの「**プロパティの表示**」フィールドで、「**NULL 以外の値のみ**」または「**すべて**」を選択します。
4. 削除する属性オプションを含むフィールドまでスクロールします。
5. フィールドの値を削除します。
6. 「**適用**」をクリックします。

コマンドライン・ツールを使用したエントリの管理

この項では、エントリの管理に使用できるコマンドライン・ツールについて説明します。また、コマンドライン・ツールを使用したエントリ管理の例もいくつか紹介します。この項の項目は次のとおりです。

- エントリ管理のためのコマンドライン・ツール
- 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

バルク・ツールについては、第 9 章「バルク・ツールの使用方法」で説明しています。

エントリ管理のためのコマンドライン・ツール

表 8-1 に、エントリ管理のための各コマンドライン・ツールと、それぞれのツールの構文および使用方法の参照先を示します。

表 8-1 エントリ管理のためのコマンドライン・ツール

ツール	タスク	構文と使用方法
ldapadd	エントリを一度に 1 つずつ追加します。 新規構成設定エントリを追加します。 入力ファイルを使用してサーバーを構成します。	『Oracle Identity Management ユーザー・リファレンス』の ldapadd コマンドライン・ツールのリファレンス
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。	『Oracle Identity Management ユーザー・リファレンス』の ldapaddmt コマンドライン・ツールのリファレンス
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。	『Oracle Identity Management ユーザー・リファレンス』の ldapbind コマンドライン・ツールのリファレンス
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。	『Oracle Identity Management ユーザー・リファレンス』の ldapcompare コマンドライン・ツールのリファレンス
ldapdelete	エントリを削除します。	『Oracle Identity Management ユーザー・リファレンス』の ldapdelete コマンドライン・ツールのリファレンス
ldapmoddn	エントリの識別名または相対識別名を変更します。 エントリまたはサブツリーの名前を変更します。 エントリまたはサブツリーを新しい親の下に移動します。	『Oracle Identity Management ユーザー・リファレンス』の ldapmoddn コマンドライン・ツールのリファレンス

表 8-1 エントリ管理のためのコマンドライン・ツール（続き）

ツール	タスク	構文と使用方法
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。	『Oracle Identity Management ユーザー・リファレンス』の ldapmodify コマンドライン・ツールのリファレンス
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。	『Oracle Identity Management ユーザー・リファレンス』の ldapmodifymt コマンドライン・ツールのリファレンス
ldapsearch	ディレクトリ・エントリを検索します。	『Oracle Identity Management ユーザー・リファレンス』の ldapsearch コマンドライン・ツールのリファレンス

例 : ldapadd を使用したユーザー・エントリの追加

次の例では、John という従業員のエントリを追加するための、entry.ldif という名前の LDIF ファイルを示します。

```
dn: cn=john, c=us
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
cn: john
cn;lang-fr:Jean
cn;lang-en-us:John
sn: Doe
jpegPhoto: /photo/john.jpg
userpassword: welcome
```

このファイルには、cn、sn、jpegPhoto および userpassword の各属性が含まれています。

cn 属性には、2 つのオプションを指定します。cn;lang-fr と cn;lang-en-us です。これらのオプションは、French（フランス語）または American English（米語）での一般名を返します。

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。
- ユーザー名にチルダ（~）は挿入できません。

例 : ldapmodify を使用したユーザー・エントリの変更

次の例では、Audrey というユーザーのパスワードを、welcome から audreyspassword に変更します。前述の例と同様に、このユーザー・エントリ用のデータは entry.ldif ファイルに記述されています。このファイルの内容は次のとおりです。

```
dn: cn=audrey,c=us
changetype: modify
replace: userpassword
userpassword: audreyspassword
```

ファイルを変更するには、次のコマンドを発行します。

```
ldapmodify -p 389 -v -f entry.ldif
```

-v は冗長モードを指定します。

注意 : エントリを追加または削除する場合、Oracle ディレクトリ・サーバーではエントリ属性値の構文検証は行われません。

コマンドライン・ツールを使用した属性オプション付きエントリの管理

この項では、属性オプションを追加する例と削除する例、および属性オプション付きエントリを検索する例を紹介します。

例 : ldapmodify を使用した属性オプションの追加

John のエントリのスペイン語属性を追加するとします。また、このユーザー・エントリ用のデータは entry.ldif ファイルに記述されているとします。このファイルの内容は次のとおりです。

```
dn: cn=john,c=us
changeType: modify
add: cn;lang-sp
cn;lang-sp: Juan
```

ファイルを変更するには、次のコマンドを発行します。

```
ldapmodify -p 389 -v -f entry.ldif
```

例 : ldapmodify を使用した属性オプションの削除

次の例では、John のエントリから cn;lang-fr 属性オプションを削除します。前述の例と同様に、このユーザー・エントリ用のデータは entry.ldif ファイルに記述されています。このファイルの内容は次のとおりです。

```
dn: cn=john, c=us
changetype: modify
delete: cn;lang-fr
cn;lang-fr: Jean
```

ファイルを変更するには、次のコマンドを発行します。

```
ldapmodify -p 389 -v -f entry.ldif
```

例 : ldapsearch を使用した属性オプション付きエントリの検索

次の例では、言語コード属性オプションを指定するオプションのある一般名（cn）属性を使用して、エントリを取り出します。この例の場合には、一般名がフランス語で、R で始まるエントリを取り出します。

```
ldapsearch -p 389 -h myhost -b "c=US" -s sub "cn;lang-fr=R*"
```

John のエントリで、cn;lang-it 言語コード属性オプションに値が設定されていないと想定します。この場合、次の例は失敗します。

```
ldapsearch -p 389 -h myhost -b "c=us" -s sub "cn;lang-it=Giovanni"
```

関連項目： 3-13 ページの「属性オプション」

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関連付けます。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、3-21 ページの「ディレクトリ・パーティション化」を参照してください。

この項の項目は次のとおりです。

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返します。

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 は参照を返します。

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 は参照を返します。

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**ディレクトリ・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、デフォルト参照は返されません。

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、3-22 ページの「ナレッジ参照と参照」を参照してください。

クライアント側の参照キャッシング

参照キャッシングとは、参照情報へのアクセスを簡単に繰り返すことができるように、その情報を格納するプロセスです。クライアントがサーバー A に問い合せ、サーバー A がサーバー B に参照を返すとします。クライアントはこの参照を追跡して、操作を実行し、クライアントに結果を返すサーバー B と通信します。参照キャッシングが行われていない場合、クライアントが次回同じ問合せをサーバー A に対して行うと、手順全体が繰り返され、時間とシステム・リソースを必要以上に消費することになります。

参照情報をキャッシュできる場合は、以降の各問合せで、参照情報をキャッシュから取り出し、サーバー B と直接通信できます。これによって、操作にかかる時間を短縮できます。

クライアント側の参照キャッシングによって、各クライアントは、参照情報をキャッシュして使用し、参照処理にかかる時間を短縮できます。

クライアント側の参照キャッシングの動作

参照エントリは、クライアントの構成ファイルに格納されます。クライアントは、セッション確立時に、この構成ファイルから参照情報を読み取ってキャッシュに格納します。このキャッシュは静的状態を保持し、セッション中に更新の追加は行われません。これ以降、クライアントは、操作を行うたびにキャッシュ内の参照情報を検索します。

クライアントが使用するこの構成ファイルは、ディレクトリ管理者が準備します。

注意： 構成ファイルは、クライアントにとってはオプションです。ファイルが存在しない場合でも、参照に関係するクライアント操作は正常に行われます。したがって、このファイルの準備は、管理者の必須作業ではありません。構成ファイルを使用する利点は、参照に関係するクライアント / サーバーの操作時間を短縮できることです。

構成ファイルは、1 つ以上の参照セットで構成されます。それぞれの参照セットは、次の要素で構成されます。

- 特定のディレクトリ・サーバーが稼働しているホスト名
- そのサーバーに存在する 1 つ以上のエントリ

各参照エントリは一連の行で構成され、それぞれの行は 1 つの参照 URL に対応します。行セパレータは、CR LF または LF です。

```
ref_file=ref_file_content
ref_file_content=1*(referral_set)
referral_set=hostname       SEP      ref_entry_set   SEP
ref_entry_set=ref_entry     *(SEP    ref_entry)
ref_entry=1*(referralurl    SEP)
SEP=CR LF / LF
CR=0x0D
LF=0x0A
```

たとえば、ホスト・サーバー X で稼働しているディレクトリ・サーバーに次の 2 つの参照エントリがあるとします。

```
dn: dc=acme, dc=com
ref: ldap://serverA:389/dc=acme, dc=com
ref: ldap://serverB:389/dc=acme, dc=com

dn: dc=oracle, dc=com
ref: ldap://serverC:389/dc=oracle, dc=com
ref: ldap://serverD:389/dc=oracle, dc=com
```

ホスト・サーバー Y で稼働しているディレクトリ・サーバーには、次の参照エントリがあるとします。

```
dn: dc=fiction, dc=com
ref: ldap://serverE:389/dc=fiction, dc=com
```

対応する referral.ora ファイルは、次のようになります。

```
ServerX
ldap://serverA:389/dc=acme, dc=com
ldap://serverB:389/dc=acme, dc=com

ldap://serverC:389/dc=oracle, dc=com
ldap://serverD:389/dc=oracle, dc=com

ServerY
ldap://serverE:389/dc=fiction, dc=com
```

9

バルク・ツールの使用方法

10*g*（10.1.4.0.1）では、バルク・ツールはC言語の実行可能ファイルとして書き換えられました。新しいバージョンのツールには、いくつかの新機能があります。

- バルク・ツールは、他のOracle Internet Directoryコマンドライン・ツールと同じ`$ORACLE_HOME/ldap/bin`ディレクトリにあります。
- バルク・ツールには一貫したインタフェースがあります。
- バルク・ツールは、Windowsコマンドライン・インタフェースから直接起動できます。CygwinまたはMKS Toolkitをインストールする必要はなくなりました。
- エラーおよび進捗状況の報告が強化されました。
- 各ツールには、`$ORACLE_HOME/ldap/log`にそれぞれ独自のログ・ファイルがあります。

バルク・ツールについては、この章の他に、次の項でも説明しています。

- 11-16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」
- 14-2ページの「ログ・ファイルの位置」
- 15-2ページの「小さいディレクトリまたはディレクトリ内の特定のネーミング・コンテキストのバックアップとリストア」
- 27-2ページの「LDAP準拠のディレクトリからのデータの移行」
- 30-5ページの「マルチマスター・レプリケーションのインストールと構成」
- 30-20ページの「一方向または双方向LDAPベース・レプリケーションのインストールと構成」

関連資料：『Oracle Identity Management ユーザー・リファレンス』のOracle Internet Directory サーバー管理ツールに関する章

注意： `bulkload`を使用する前に、すべてのOracle Internet Directoryインスタンスを停止してください。他のバルク・ツールを使用する前には、すべてのOracle Internet Directoryインスタンスを停止するか、エントリ・キャッシュを無効にしてください。

この章の項目は次のとおりです。

bulkload

バルク・ローダー bulkload は、バルク管理ツールです。このツールは、LDIF または SQL*Loader 形式の入力データを取得し、このデータをメタデータ・リポジトリにある Oracle Internet Directory のスキーマに直接ロードします。これには、check、generate および load の 3 つの主要フェーズがあります。

check フェーズでは、bulkload が LDIF 入力データをスキーマのために解析および検証します。

generate フェーズでは、bulkload が SQL*Loader 形式で中間ファイルを生成します。

load フェーズでは、bulkload は、バルク・モード・ロードまたは増分モード・ロードのいずれかの方法でロードできます。

- バルク・モード・ロードを使用する場合、bulkload は生成された中間ファイルをデータベースにロードします。その際、古い索引を削除し、新しい索引を生成します。
- 増分モード・ロードを使用する場合、bulkload は中間ファイルを挿入モードでデータベースの表にロードします。データをロードする際に、bulkload は索引を更新します。

バルク・モード・ロードは、増分モード・ロードより高速です。

バルク・ローダーでは、次の機能もサポートしています。

- 生成フェーズとロード・フェーズの間に並列処理ができるように、スレッド数を指定できます。
- データを他の言語で使用できるようにするエンコード・オプションがあります。
- LDIF ファイルで指定した操作属性を保持できる restore オプションがあります。
- 索引作成用の index オプションがあります。
- bulkload の失敗からのリカバリに役立つ recover オプションがあります。
- 既存のディレクトリにデータを追加するとき、bulkload では、バルク・モードと増分モードの両方のロードをサポートします。
- append オプションを使用すると、LDAP サーバーの稼働中にデータをロードできます。

generate フェーズの初めに、サーバーの orclServerMode が、read-write から read-modify に変わります。generate フェーズの終わりには、read-modify 状態のままであるため、generate フェーズと load フェーズの間にエントリを Oracle Internet Directory に追加することはできません。これは内部の順序番号を保持するために必要です。load フェーズは、generate フェーズの直後に実行します。load フェーズの終わりに、サーバーの orclServerMode は、read-write の設定に戻されます。bulkload を recover オプションとともに使用しても、orclServerMode は read-write に戻ります。

bulkload ツールは、次の出力ファイルを $ORACLE_HOME/ldap/log ディレクトリに生成します。

- 出力ログ、bulkload.log
- 重複識別名のリスト、duplicateDN.log
- SQL*Loader によって生成された中間ログ・ファイル、bsl_*.log

bulkload ツールは、次の出力ファイルを $ORACLE_HOME/ldap/load ディレクトリに生成します。

- 不正な LDIF エントリのリスト、badentry.ldif
- ldapadd、dynGrp.ldif を使用して追加できるすべての動的グループ・エントリのリスト
- 中間ファイル、*.ctl および *.dat

注意： 適用されるパスワード・ポリシーで pwdmustchange 属性が TRUE に設定されている場合、bulkload によってロードされるすべての新規エントリでは、pwdreset 属性がデフォルトで 1 に設定されます。詳細は、第 19 章「Oracle Internet Directory のパスワード・ポリシー」を参照してください。

注意： ディレクトリへのデータの移入に bulkload ユーティリティを使用しない場合は、oidstats.sql ツールを実行して、検索パフォーマンスの大幅低下を回避する必要があります。

関連資料：

- oidstats.sql ツールの説明と構文は、『Oracle Identity Management ユーザー・リファレンス』の oidstats.sql コマンドライン・ツールのリファレンスを参照してください。
- これらのツールの概要は、5-8 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 コマンドライン・パラメータ

bulkload ツールでは、key=value 形式のパラメータが使用されます。

```
bulkload connect=connect_string
{[check="TRUE"|"FALSE" [restore="TRUE"|"FALSE"] [threads=num_of_threads]
[file=ldif_file]][generate="TRUE"|"FALSE" [append="TRUE"|"FALSE"]
[restore="TRUE"|"FALSE"] [threads=num_of_threads] file=ldif_file]
[load="TRUE"|"FALSE" [append="TRUE"|"FALSE"] [threads=num_of_threads]]
[index="TRUE"|"FALSE"] [recover="TRUE"|"FALSE"]}
[encode=character_set] [debug="TRUE"|"FALSE"] [verbose="TRUE"|"FALSE"]
```

パラメータの組合せには、有効なものもあれば、無効なものもあります。

bulkload の起動時には、check、generate、load、append、recover または index のアクションのうち少なくとも 1 つを指定する必要があります。

check が TRUE の場合、bulkload はスキーマ・チェックを実行します。

generate が TRUE の場合、bulkload は中間ファイルを生成します。

check または generate アクションを使用する場合、LDIF データ・ファイルへのパス名を指定する必要があります。

load が TRUE の場合、bulkload は中間ファイルをロードします。

append が TRUE の場合、bulkload はサーバーの稼働中にアクションを実行できます。

restore フラグは、LDIF ファイルに orclguid や creatorsname などの操作属性が含まれる場合にのみ使用します。

recover を他のオプションとともに指定しないでください。

check index のオプションの組合せは、既存の索引を検証します。

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。

> **関連資料：**『Oracle Identity Management ユーザー・リファレンス』の bulkload コマンドライン・ツールのリファレンス

この項の項目は次のとおりです。

タスク 1: Oracle データベース・サーバーのバックアップ

ファイルをインポートする前に、安全対策として Oracle データベース・サーバーをバックアップします。

> **関連資料：** Oracle Database ドキュメント・ライブラリの『Oracle Database バックアップおよびリカバリ基礎』

タスク 2: Oracle Internet Directory のパスワードの準備

bulkload を使用するには、Oracle Internet Directory パスワードを指定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。

> **関連資料：**『Oracle Identity Management ユーザー・リファレンス』の oidpasswd コマンドライン・ツールのリファレンス

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チェックと SQL*Loader 用の入力ファイルの生成

UNIX では、bulkload ツールは通常は次の場所にあります。
`$ORACLE_HOME/ldap/bin`

Microsoft Windows では、このツー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し、SQL*Loader 用のファイルを生成するには、次のように入力します。

```
bulkload connect="connect_string" check="TRUE" generate="TRUE" \
   file="path_to_ldif-file_name"
```

すべてのスキーマ違反が、$ORACLE_HOME/ldap/log/bulkload.log に記録されます。すべての不正エントリは、$ORACLE_HOME/ldap/load/badentry.ldif に記録されます。テキスト・エディタを使用してすべての不正エントリを修正し、check オプションと generate オプションを指定して bulkload を再実行します。

エントリが重複している場合、その識別名は $ORACLE_HOME/ldap/log/duplicateDN.log に記録されます。これは単に参考のためです。bulkload ツールは、重複するエントリに対して重複データは生成しません。重複エントリは無視されます。

bulkload が正常に終了すると、*.ctl ファイルと *.dat ファイルが $ORACLE_HOME/ldap/load ディレクトリに生成され、load モードで SQL*Loader によって使用されます。このファイルは変更できません。

タスク 4: 入力ファイルのロード

入力ファイルの生成後、load オプションを指定して bulkload を再実行します。この手順で、Oracle SQL*Loader 固有の形式の *.dat ファイルがデータベースにロードされ、属性の索引が作成されます。構文は次のとおりです。

```
bulkload connect="connect_string" load="TRUE"
```

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 ディレクトリに報告されます。エラーは bulkload.log、および SQL*Loader で生成された *.bad ファイルと bsl_*.log ファイルに記録されます。bulk 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になる可能性があります。この状態が発生した場合、データベースを bulkload 操作の前の状態にリストアする必要があります。bulkload を recover オプションを指定して使用するか、bulkload を起動する前に取ったバックアップから Oracle Internet Directory ディレクトリをリストアすることにより、データベースを元の状態に戻せます。

bulkload の例

次の例は、bulkload のいくつかの使用例を示しています。

例 1. バルク・モードでのロード

通常、データは Oracle Internet Directory インストール直後に直接ロードします。これには 3 つのアクションが必要です。

- LDIF ファイルにスキーマ・エラーがないかチェックし、中間ファイルを生成します。
- Oracle Internet Directory メタデータ・リポジトリにデータをロードします。

これらのアクションは、次のようなコマンドラインで実行します。

```
bulkload connect="conn_str" check="TRUE" generate="TRUE" file="LDIF_file"
bulkload connect="conn_str" load="TRUE"
```

LDIF データが別の Oracle Internet Directory ノードのものである場合、check フェーズは省略してもかまいません。

例 2. 増分または追加モードでのロード

すでにデータが格納されている Oracle Internet Directory サーバーにエントリを追加し、同時にそのサーバーを稼働させておく場合、増分または追加モードを使用する必要があります。このモードは通常、ダイレクトリにエントリを追加する他の方法より高速です。ただし、Oracle Internet Directory LDAP インスタンスが読取り / 更新モードであり、bulkload でデータを追加できることを確認する必要があります。次のようなコマンドにより、bulkload を増分または追加モードで起動します。

```
bulkload connect="conn_str" check="TRUE" generate="TRUE" append="TRUE" \
  file="LDIF_file"
bulkload connect="conn_str" load="TRUE" append ="TRUE"
```

例 3. 索引検証

bulkload 操作は、索引の更新または索引の作成ができます。しかし、bulkload で索引を正しく更新あるいは作成できないことがあります。これは通常、不適切なサイズ設定などの問題が原因です。このような問題が発生した場合は、bulkload を使用してすべての索引を検証し、再作成できます。

次の構文を使用して、索引の検証のために bulkload を起動します。

```
bulkload connect="conn_str" check="TRUE" index="TRUE"
```

例 4. 索引の再作成

索引を再作成するには、次の構文を使用します。

```
bulkload connect="conn_str"  index="TRUE"
```

例 5. データのリカバリ

ディスクの不適切なサイズ設定などの問題が原因で、bulkload の load フェーズが失敗する可能性があります。そのような失敗の後には、ディレクトリ・データの一貫性がなくなる可能性があります。recover オプションを使用すれば、ディレクトリ・データを bulkload 前の状態に戻せます。構文は次のとおりです。

```
bulkload connect="conn_str" recover="TRUE"
```

bulkmodify

bulkmodify ツールは、既存のディレクトリ内にある多数のエントリの属性を変更する場合に役立ちます。このツールは、属性値に対して追加操作と置換操作を実行できます。ネーミング・コンテキストに対する操作もできます。フィルタを使用すれば、指定したネーミング・コンテキストの下のいくつかのエントリに対して選択的に操作を行うこともできます。

bulkmodify ツールは、次の属性に対しては add または replace 操作を行えません。

- dn
- cn
- userpassword
- orclpassword
- orclentrylevelaci
- orclaci
- orclcertificatehash
- orclcertificatematch
- すべてのバイナリ属性

objectclass 属性に対しては replace 操作ができません。

単一値属性については add 操作ができません。bulkmodify の出力は、$ORACLE_HOME/ldap/log/bulkmodify.log に記録されます。

> **関連資料 :**『Oracle Identity Management ユーザー・リファレンス』の bulkmodify コマンドライン・ツールのリファレンス

bulkmodify コマンドライン・パラメータ

bulkmodify では、key=value 形式のパラメータが使用されます。

```
bulkmodify connect=connect_string basedn=Base_DN
{[add="TRUE"|"FALSE"]|[replace="TRUE"|"FALSE"]} attribute=attribute_name
value=attribute_value [filter=filter_string] [size=transaction_size]
[threads=num_of_threads] [debug="TRUE"|"FALSE"] [encode=character_set]
[verbose="TRUE"|"FALSE"]
```

CPU 数の 1 ～ 6 倍のスレッド数が必要です。

add または replace オプションのいずれかを選択します。デフォルトでは、どちらも FALSE に設定されています。

bulkmodify の使用例

次の例は、bulkmodify のいくつかの使用例を示しています。

例 1. 指定ネーミング・コンテキストの下の全エントリに説明を追加

この例では、"c=us" の下のすべてのエントリに説明を追加します。

```
bulkmodify connect="connect_str"  basedn="c=us" add="TRUE" \
    attribute="description"  value="US citizen" filter="objectclass=*"
```

例 2. 同じマネージャを持つ指定ネーミング・コンテキストの下の全エントリに telephonenumbe を追加

この例では、Anne Smith がマネージャである "c=us" の下のすべてのエントリに telephonenumber を追加します。

```
bulkmodify connect="connect_str" basedn="c=us" add="TRUE" \
  attribute="telephoneNumber" value="408-123-4567" filter="manager=Anne Smith"
```

例 3. 指定ネーミング・コンテキストの下の全エントリの属性を置換

この例では、"c=us" の下のすべてのエントリで pwdreset を置換します。

```
bulkmodify connect="connect_str"  basedn="c=us" replace="TRUE" \
  attribute="pwdreset" value="1" filter="objectclass=*"
```

bulkdelete

bulkdelete ツールは、既存のディレクトリ内にある多数のエントリの属性を削除する場合に役立ちます。bulkdelete は、ネーミング・コンテキストの下で指定したエントリを削除できます。デフォルトでは、エントリを完全に削除します。データベースからエントリのすべての痕跡を削除します。オプション cleandb=FALSE を使用すると、bulkdelete はすべてのエントリを、完全に削除するかわりに、ツームストン・エントリに変えます。

bulkdelete の出力は、$ORACLE_HOME/ldap/log/bulkdelete.log に記録されます。

> **関連資料：**『Oracle Identity Management ユーザー・リファレンス』の bulkdelete コマンドライン・ツールのリファレンス

bulkdelete コマンドライン・パラメータ

bulkdelete ツールでは、key=value 形式のパラメータが使用されます。

```
bulkdelete connect=connect_string { [basedn=Base_DN] | [file=file_name] }
[cleandb="TRUE"|"FALSE"] [size=transaction_size] [encode=character_set]
[debug="TRUE"|"FALSE"] [threads=num_of_threads] [verbose="TRUE"|"FALSE"]
```

basedn または file オプションのいずれかを選択します。cleandb が TRUE ならば、bulkdelete はエントリをデータベースから完全に削除します。デフォルトでは、cleandb は TRUE に設定されています。CPU 数の 1 ～ 6 倍のスレッド数が必要です。

bulkdelete の使用例

次の例は、bulkdelete の使用方法を説明しています。

例 1. 指定ネーミング・コンテキストの下の全エントリをデータベースから削除

この例では、"c=us" の下のすべてのエントリを削除します。

```
bulkdelete connect="connect_str" basedn="c=us" cleandb="TRUE"
```

例 2. ネーミング・コンテキスト下のエントリを削除し、ツームストン・エントリ化

この例では、"c=us" の下のすべてのエントリを削除し、それらをツームストン・エントリとして残します。

```
bulkdelete connect="connect_str" basedn="c=us" cleandb=FALSE
```

例 3. 指定ネーミング・コンテキストの下のエントリを削除し、ツームストン・エントリ化

この例では、ファイルで指定された特定の basedn の下のすべてのエントリを削除し、それらをツームストン・エントリとして残します。

```
bulkdelete connect="connect_str" file="file" cleandb=FALSE
```

ldifwrite

ldifwrite ツールは、Oracle Internet Directory ストアから 1 つのファイルにデータをダンプするために使用します。データを 1 ファイルにまとめると、レプリケーションまたはバックアップ・ストレージ用に別のノードへデータをロードすることが容易になります。出力ファイルへの書込みの際に、ldifwrite ツールは、指定した識別名はもとより、その下のすべてのエントリを含むサブツリーの検索を実行します。ツールはデータを LDIF 形式でダンプします。指定したレプリケーション承諾識別名の下のエントリもダンプできます。

ldifwrite ツールは、指定したフィルタを使用して見つけたエントリをダンプできます。ldifwrite の出力は、$ORACLE_HOME/ldap/log/ldifwrite.log に記録されます。

> **関連資料 :**『Oracle Identity Management ユーザー・リファレンス』の ldifwrite コマンドライン・ツールのリファレンス

ldifwrite コマンドライン・パラメータ

ldifwrite ツールでは、keyword=value 形式のパラメータが使用されます。

```
ldifwrite connect=connect_string basedn=Base_DN ldiffile=LDIF_Filename
[filter=LDAP_Filter] [threads=num_of_threads] [debug="TRUE"|"FALSE"]
[encode=character_set] [verbose="TRUE"|"FALSE"]
```

basedn オプションを使用して、ベース識別名またはレプリケーション承諾識別名を指定します。

CPU 数の 1 ～ 6 倍のスレッド数が必要です。

ldifwrite の使用例

次の例は、ldifwrite のいくつかの使用例を示しています。

例 1. 指定ネーミング・コンテキストの下の全エントリを LDIF ファイルにダンプ

この例では、"ou=Europe, o=imc, c=us" の下のすべてのエントリを output.ldif ファイルに書き込みます。

```
ldifwrite connect="connect_str" basedn="ou=Europe, o=imc, c=us" \
  ldiffile=output.ldif
```

ldifwrite ツールには、createtimestamp、creatorsname、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。

例 2. 指定ネーミング・コンテキストの一部を LDIF ファイルにダンプ

この例では、部分レプリケーションで定義した次のネーミング・コンテキスト・オブジェクトを使用します。

```
dn: cn=includednamingcontext000001, cn=replication namecontext,
 orclagreementid=000001, orclreplicaid=node replica identifier,
 cn=replication configuration
orclincludednamingcontexts: c=us
orclexcludednamingcontexts: ou=Americas, c=us
orclexcludedattributes: userpassword
objectclass: top
objectclass: orclreplnamectxconfig
```

この例では、c=us の下のエントリは、ou=Americas,c=us を除いてすべてバックアップが取られます。userpassword 属性も除外されます。コマンドは次のとおりです。

```
ldifwrite connect="conn_str" \
  basedn="cn=includednamingcontext000001, cn=replication namecontext, \
  orclagreementid=000001,orclreplicaid=node replica identifier,\
  cn=replication configuration" ldiffile="ldif_file_name"
```

例 3. 指定ネーミング・コンテキストの下のエントリを LDIF ファイルにダンプ

この例では、"ou=Europe, o=imc, c=us" の下で LDAP 検索フィルタ基準を満たすエントリをすべて output.ldif ファイルに書き込みます。

```
ldifwrite connect="connect_str" basedn="ou=Europe, o=imc, c=us" filter="uid=abc" \
  ldiffile="output.ldif"
```

catalog

catalog ツールは、既存の属性の索引を作成する場合や、既存の属性からの索引を削除する場合に役立ちます。catalog ツールは、属性を検索可能にします。catalog の出力は、$ORACLE_HOME/ldap/log/catalog.log に記録されます。

catalog コマンドライン・パラメータ

catalog では、key=value 形式のパラメータが使用されます。

```
catalog connect=connect_string {[add="TRUE"|"FALSE"]|[delete="TRUE"|"FALSE"]}
{[attribute=attribute_name]|[file=file_name]} [logging="TRUE"|"FALSE"]
[threads=num_of_threads] [debug="TRUE"|"FALSE"] [verbose="TRUE"|"FALSE"]
```

add または delete オプションのいずれかを選択します。デフォルトでは、どちらも FALSE に設定されています。

CPU 数の 1 ～ 6 倍のスレッド数が必要です。

ロギングが TRUE の場合、catalog により REDO ログが生成されます。

コマンドラインでは、一度に 1 つしか attribute 引数を指定できません。1 つのコマンドの起動で複数の属性の add または delete を行うには、file オプションを使用し、ファイル内の属性のリストを指定します。次のように、属性を 1 行ずつ指定します。

```
description
sn
title
```

catalog の使用例

次の例は、catalog のいくつかの使用例を示しています。

例 1. 検索可能属性を検索不可能属性に変更

この例では、title 属性から索引を削除します。

```
catalog connect="connect_str" delete="TRUE"  attribute="title"
```

例 2. 検索不可能属性を検索可能属性に変更

この例では、title 属性に索引を追加します。

```
catalog connect="connect_str" add="TRUE" attribute="title"
```

関連項目： 11-16 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」

10

ディレクトリの属性一意性

この章では、Oracle Internet Directory の属性一意性について説明します。この章の項目は次のとおりです。

属性一意性の概要

属性一意性機能は、属性値の追加時および変更時に属性値が重複しないようにします。たとえば、すでに別の従業員に割り当てられている識別子を新しい従業員に割り当てることを防止します。かわりに、ディレクトリ・サーバーは操作を中止し、エラー・メッセージを返します。

次の対象に属性一意性を定義できます。

- ディレクトリ全体

  たとえば、mail 属性を持つディレクトリ内のすべてのエントリが、その属性に対して一意の値を持つようにするには、mail と関連付けられた属性一意性のインスタンスを作成します。

- 属性ごとの 1 つのサブツリー全体

  たとえば、MyCompany が SubscriberCompany1 と SubscriberCompany2 用のディレクトリをホスティングしている場合は、SubscriberCompany1 のみに属性一意性を適用することを選択できます。

- 1 つのオブジェクト・クラス全体

  たとえば、ID が、machine オブジェクト・クラスと person オブジェクト・クラスの両方で属性になっているとします。属性一意性を有効にすると、ディレクトリ・サーバーは、同じ ID を持つ 2 台のマシンまたは 2 人のユーザーの追加を防止します。ただし、machine の ID 属性に、person の ID 属性と同じ値を指定することは可能です。

属性一意性を実装するには、10-2 ページの表 10-1 に示す属性の値を指定する属性一意性制約エントリを作成します。

表 10-1 属性一意性制約エントリ

属性名	必須	有効値	デフォルト値	デフォルト有効範囲
orcluniqueattrname	○	任意の文字列	該当なし	該当なし
orcluniquescope	×	次のいずれかの値 ■ base: ルート・エントリのみを検索 ■ onelevel: 1 レベルのみを検索 ■ sub: ディレクトリ全体を検索	sub	ディレクトリ全体を検索
orcluniqueenable	×	0（無効）または 1（有効）	0	属性一意性を無効化
orcluniquesubtree	×	任意の文字列	" "	ディレクトリ全体を検索
orcluniqueobjectclass	×	任意の文字列	" "	すべてのオブジェクト・クラスを検索

エントリを作成し、属性を指定した場合、ディレクトリ・サーバーは、エントリに対する操作を実行する前に次のことを行います。

- 属性一意性制約を使用したすべての更新操作のチェック
- 監視対象の属性、サブツリーまたはオブジェクト・クラスに操作を適用するかどうかの決定

監視対象の属性、接尾辞またはオブジェクト・クラスに操作を適用して、2 つのエントリに同じ属性値が含まれた場合、ディレクトリ・サーバーは操作を中止し、制約違反エラー・メッセージをクライアントに返します。

注意： 属性一意性機能は、索引付き属性でのみ機能します。

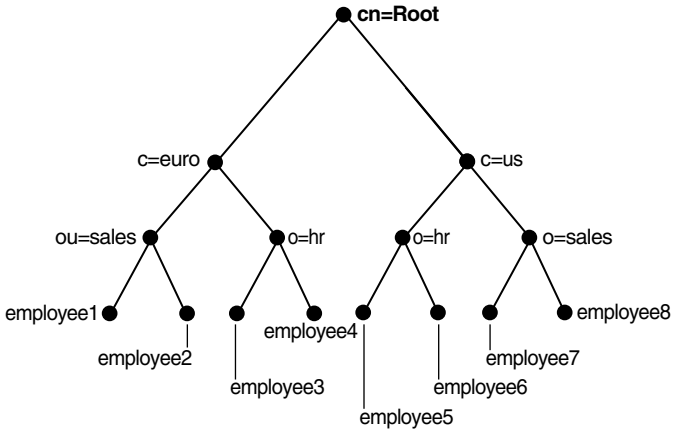
属性一意性作成の規則

この項では、属性一意性制約の作成時に適用される規則について、例を使用して説明します。この項の項目は次のとおりです。

- 属性一意性制約での複数の属性名の指定
- 属性一意性制約での複数のサブツリーの指定
- 属性一意性制約での複数の有効範囲の指定
- 属性一意性制約での複数のオブジェクト・クラスの指定
- 属性一意性制約での複数のサブツリー、有効範囲およびオブジェクト・クラスの指定

この項の例を理解するには、図 10-1 を参照してください。

図 10-1 ディレクトリ情報ツリーの例



属性一意性制約での複数の属性名の指定

複数の属性一意性制約で `orcluniqueattrname` の値が異なる場合、その影響は互いに無関係です。

たとえば、ユーザーが、次のような 2 つの属性一意性制約を定義するとします。

制約 1:

```
orcluniqueattrname: employee_id
```

制約 2:

```
orcluniqueattrname: email_id
```

この例で、制約 1 と制約 2 は、それぞれの属性一意性の有効範囲内で指定された属性に対して一意性を適用します。制約 1 と制約 2 は、互いに無関係です。

属性一意性制約での複数のサブツリーの指定

複数の属性一意性制約で、orcluniqueattrname、orcluniquescope および orcluniqueobjectclass の値が同一で、orcluniquesubtree の値が異なる場合は、それらの属性一意性制約で指定されたサブツリーの有効範囲を結合したものがチェックされます。

例として、10-3 ページの図 10-1 を参照してください。ユーザーが、次のような 2 つの属性一意性制約を定義するとします。

制約 1:

```
orcluniqueattrname: employee_id
orcluniquesubtree: o=sales, c=us, cn=root
orcluniquescope: onelevel
```

制約 2:

```
orcluniqueattrname: employee_id
orcluniquesubtree: o=hr, c=euro, cn=root
orcluniquescope: onelevel
```

この例で、employee_id の属性一意性は、サブツリー o=sales,c=us,cn=root および o=hr,c=euro,cn=root の下にあるすべてのエントリに対して適用されます。ディレクトリ・サーバーは、employee_id 属性の一意の値を employee3、employee4、employee7 および employee8 に対して適用します。

属性一意性制約での複数の有効範囲の指定

複数の属性一意性制約で、orcluniqueattrname、orcluniquesubtree および orcluniqueobjectclass の値が同一で、orcluniquescope の値が異なる場合は、最大の検索有効範囲を持つ属性一意性制約が有効となります。

たとえば、10-3 ページの図 10-1 で、ユーザーが、次のような 2 つの属性一意性制約を定義するとします。

制約 1:

```
orcluniqueattrname: employee_id
orcluniquesubtree: c=us, cn=root
orcluniquescope: onelevel
```

制約 2:

```
orcluniqueattrname: employee_id
orcluniquesubtree: c=us, cn=root
orcluniquescope: sub
```

この例で、employee_id の属性一意性は、サブツリー c=us,cn=root の下にあるすべてのエントリおよびエントリ c=us,cn=root 自体に対して適用されます。これは、ユーザーが制約 2 のみを定義した場合と同じです。

属性一意性制約での複数のオブジェクト・クラスの指定

複数の属性一意性制約で、orcluniqueattrname、orcluniquesubtree および orcluniquescope の値が同一で、orcluniqueobjectclass の値が異なる場合は、それらのオブジェクト・クラスに属する属性を結合したものがチェックされます。

例として、10-3 ページの図 10-1 を参照してください。ユーザーが、次のような 2 つの属性一意性制約を定義するとします。

制約 1:

```
orcluniqueattrname: employee_id
orcluniquesubtree: c=us, cn=root
orcluniqueobjectclass: person
```

制約 2:

```
orcluniqueattrname: employee_id
orcluniquesubtree: c=us, cn=root
```

この例で、employee_id の属性一意性は、エントリが属するオブジェクト・クラスに関係なく、サブツリー c=us,cn=root の下にあるすべてのエントリと、エントリ c=us,cn=root 自体に対して適用されます。制約 2 は orcluniqueobjectclass 属性を指定していません。これはすべてのオブジェクト・クラスを指定した場合と同じです。

属性一意性制約での複数のサブツリー、有効範囲およびオブジェクト・クラスの指定

複数の属性一意性制約で、orcluniqueattrname の値が同一で、orcluniquesubtree、orcluniquescope および orcluniqueobjectclass の値が異なる場合は、異なる制約の属性一意性の有効範囲に属するエントリを結合したものがチェックされます。

たとえば、10-3 ページの図 10-1 で、ユーザーが、次のような 2 つの属性一意性制約を定義するとします。

制約 1:

```
orcluniqueattrname: employee_id
orcluniquesubtree: o=sales, c=us, cn=root
orcluniquescope: onelevel
orcluniqueobjectclass: person
```

制約 2:

```
orcluniqueattrname: employee_id
orcluniquesubtree: c=euro, cn=root
orcluniquescope: sub
orcluniqueobjectclass: organization
```

この例で、employee_id の属性一意性は次のエントリに対して適用されます。

- オブジェクト・クラスが person に属しているサブツリー o=sales,c=us,cn=root の下のすべてのエントリ
- オブジェクト・クラスが organization に属しているサブツリー c=euro,cn=root の下のすべてのエントリおよびエントリ c=euro,cn=root 自体

属性一意性の管理

この項の項目は次のとおりです。

属性一意性エントリの位置

属性一意性制約エントリは、`cn=unique,cn=Common,cn=Products,cn=OracleContext` の下に格納されます。

Oracle Directory Manager を使用した属性一意性の管理

Oracle Directory Manager を使用して、属性一意性制約エントリの作成、変更および削除を実行できます。

属性一意性制約エントリの作成

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「<ディレクトリ・サーバー・インスタンス>」、「**属性一意性管理**」の順に展開します。「属性一意性管理」ウィンドウが表示され、右側のペインに既存の属性一意性制約エントリのリストが表示されます。
2. ツールバーの「**作成**」ボタンを選択します。「新規制約」ウィンドウが表示されます。

   「新規制約」ウィンドウの各フィールドに値を入力します。詳細は、A-5 ページの表 A-8 を参照してください。
3. 「**OK**」を選択します。「属性一意性管理」ウィンドウに戻ります。作成したエントリが、属性一意性制約エントリのリストに表示されます。
4. 「**適用**」を選択します。

Oracle Directory Manager を使用した属性一意性制約エントリの変更

属性一意性制約エントリを変更する手順は次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「<ディレクトリ・サーバー・インスタンス>」、「**属性一意性管理**」の順に展開します。「属性一意性管理」ウィンドウが表示され、右側のペインに既存の属性一意性制約エントリのリストが表示されます。
2. 「属性一意性管理」ウィンドウで、変更する属性一意性制約エントリを選択した後、「**編集**」を選択します。その属性の「属性一意性制約」ウィンドウが表示されます。
3. 「属性一意性制約」ウィンドウで、該当するフィールドに変更する値を入力した後、「**OK**」を選択します。「属性一意性管理」ウィンドウに戻ります。
4. 「**適用**」を選択します。

Oracle Directory Manager を使用した属性一意性制約ポリシーの削除

属性一意性制約ポリシーを削除する手順は次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「<ディレクトリ・サーバー・インスタンス>」、「**属性一意性管理**」の順に展開します。「属性一意性管理」ウィンドウが表示され、右側のペインに既存の属性一意性制約エントリのリストが表示されます。
2. 「属性一意性管理」ウィンドウで、削除する属性一意性制約エントリを選択した後、「**編集**」を選択します。この属性の「属性一意性制約」ウィンドウが表示されます。
3. 「**削除**」を選択し、確認を求めるプロンプトで削除を確認します。「属性一意性制約」ウィンドウに戻ります。削除したエントリは、属性一意性制約エントリのリストに表示されなくなります。

コマンドライン・ツールを使用した属性一意性の管理

この項の項目は次のとおりです。

コマンドライン・ツールを使用した属性一意性の有効化および無効化

既存の属性一意性制約エントリに対する属性一意性を有効または無効にできます。

既存の属性一意性制約エントリに対する属性一意性を有効にする手順は、次のとおりです。

1. ldapmodify を使用して、`orcluniqueenable` 属性を `1` に設定します。
2. ディレクトリ・サーバーを再起動して、ポリシーを有効にします。

属性一意性を無効化する手順は、次のとおりです。

1. ldapmodify を使用して、`orcluniqueenable` 属性を `0` に設定します。
2. ディレクトリ・サーバーを再起動して、ポリシーを無効にします。

コマンドライン・ツールを使用した属性一意性制約エントリの作成

属性一意性を有効にするには、10-2 ページの表 10-1 に示した属性を持つ属性一意性制約エントリを指定します。

コマンドライン・ツールを使用したディレクトリ全体を対象とする属性一意性の作成 ディレクトリ全体を対象とする属性一意性のインスタンスを作成するには、値の一意性を適用する属性名を指定します。

たとえば、MyCompany の米国の全従業員に対して一意の従業員識別子を作成する手順は、次のとおりです。

1. 次のように、属性一意性制約エントリを（LDIF フォーマットで）作成します。

```
dn: cn=constraint1, cn=unique, cn=common, cn=products, cn=oraclecontext
objectclass: orclUniqueConfig
orcluniqueattrname: employeenumber
orcluniquesubtree: o=MyCompany, c=US
orcleuniqueobjectclass: person
```

2. 次のような属性一意性制約エントリをロードして、属性一意性機能を適用します。

```
ldapadd -h host -p port -D DN -w password -f constraint1.dat
```

3. ディレクトリ・サーバーを再起動します。

注意： `orclcommonusernickname` 属性に一意性制約を指定するには、次の LDIF テンプレート・ファイルを使用します。

```
$ORACLE_HOME/ldap/schema/oid/uniquenessConstraint.ldif
```

コマンドライン・ツールを使用した 1 つのサブツリーを対象とする属性一意性の作成 1 つ以上のサブツリーを対象とする属性一意性のインスタンスを作成するには、次の項目を指定します。

- 値の一意性を適用する属性名
- 一意性制約を適用するサブツリーの位置

たとえば、MyCompany が SubscriberCompany1 と SubscriberCompany2 をホスティングしていて、SubscriberCompany1 のみに従業員識別子属性の一意性を適用するとします。`uid=dlin,ou=people,o=SubscriberCompany1,dc=MyCompany,dc=com` などのエントリを追加する場合は、`o=SubscriberCompany1,dc=MyCompany,dc=com` サブツリーでのみ一意性を適用する必要があります。これを行うには、属性一意性制約の構成で、サブツリーの識別名を明示的に列挙します。

この場合、LDIF ファイルは次のようになります。

```
dn: cn=constraint1, cn=unique, cn=common, cn=products, cn=oraclecontext
objectclass: orclUniqueConfig
orcluniqueattrname: employeenumber
orcluniquesubtree: o=SubscriberCompany1,dc=MyCompany,dc=com
```

コマンドライン・ツールを使用した 1 つのオブジェクト・クラスを対象とする属性一意性の作成 1 つのオブジェクト・クラスを対象とする属性一意性のインスタンスを作成するには、次の項目を指定します。

- 値の一意性を適用する属性名
- オブジェクト・クラス名

この場合、LDIF ファイルは次のようになります。

```
dn: cn=constraint1, cn=unique, cn=common, cn=products, cn=oraclecontext
objectclass: orclUniqueConfig
orcluniqueattrname: employeenumber
orcleuniqueobjectclass: person
```

コマンドライン・ツールを使用した属性一意性制約エントリの変更

属性一意性エントリを変更するには、エントリの LDIF ファイルを作成し、その後 ldapmodify を使用してそのファイルをディレクトリにアップロードします。

たとえば、次のような既存の属性一意性制約エントリがあるとします。

```
dn: cn=constraint1, cn=unique, cn=common, cn=products, cn=oraclecontext
objectclass: orclUniqueConfig
orcluniqueattrname: employeenumber
orcluniquesubtree: o=MyCompany, c=US
orcleuniqueobjectclass: person
```

この制約を `o=MyCompany` ではなく `c=US` に適用する手順は、次のとおりです。

1. LDIF エントリを作成して、`orcluniquenesssubtree` エントリを次のように変更します。

   ```
   dn: cn=constraint1, cn=unique, cn=common, cn=products, cn=oraclecontext
   changetype: modify
   replace: orcluniquesubtree
   orcluniquesubtree: o=Oracle Corporation, c=US
   ```

2. ldapmodify を使用して、この変更をディレクトリ・サーバーに適用します。

   ```
   ldapmodify -p port -D user -w password -f file_name
   ```

3. ディレクトリ・サーバーを再起動して、この変更を有効にします。

コマンドライン・ツールを使用した属性一意性制約エントリの削除

属性一意性制約ポリシーを削除するには、ldapdelete コマンドライン・ツールを使用します。

1. ldapdelete を使用して、ディレクトリから属性一意性制約エントリを削除します。

```
ldapdelete -p port -D bind_DN -w password \
"cn=constraint1,cn=unique,cn=common,cn=products,cn=oraclecontext"
```

2. ディレクトリ・サーバーを再起動して、この変更を有効にします。

Oracle Internet Directory 10*g*（10.1.4.0.1）での属性一意性の制限事項

属性一意性制約が Oracle Internet Directory レプリケーション環境にある場合は、各サーバーでの属性一意性制約の構成は慎重に行ってください。この項の項目は次のとおりです。

単純なレプリケーション使用例

クライアント・アプリケーションによる変更はすべてサプライヤ・サーバーで実行されます。したがって、サプライヤ・サーバーの属性一意性制約を使用可能に設定してください。コンシューマ・サーバーで属性一意性制約を使用可能にする必要はありません。コンシューマ・サーバーの属性一意性制約を使用可能にしても、ディレクトリ・サーバーの正しい動作を妨害することはありませんが、パフォーマンスが低下する可能性があります。

マルチマスター・レプリケーション使用例

マルチマスター・レプリケーション使用例では、ノードが同じレプリカのサプライヤとコンシューマの両方として機能します。マルチマスター・レプリケーションでは、ゆるやかな一貫性を持つレプリケーション・モデルを使用します。

1 台のサーバーの属性一意性制約を使用可能にしても、指定された時間に両方のマスターで属性値が一意であることは保証されません。1 台のサーバーのみで属性一意性制約を使用可能にすると、各レプリカに保持されているデータに不整合が発生する可能性があります。

属性一意性制約は、両方のマスターで使用可能にする必要があります。ただし、それでも不整合な状態になる可能性があります。たとえば、両方のマスターで、それぞれのエントリを同じ属性値に変更することができます。ただし、後で変更が別のノードにレプリケートされる際、競合が明白になります。この種の競合解消も考慮する必要があります。競合解消がレプリケーション・サーバー側の問題によるものであるかどうかを調査してください。

11

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。

この章の項目は次のとおりです。

ディレクトリ・スキーマの概要

ディレクトリ・スキーマには、次の機能があります。

- ディレクトリに格納できるオブジェクトの種類に関する規則を含んでいます。
- 検索などの処理時にディレクトリ・サーバーとクライアントが情報を扱う方法の規則を含んでいます。
- ディレクトリに格納されているデータの整合性と品質をメンテナンスするのに役立ちます。
- データの重複を削減します。
- ディレクトリに対応したアプリケーションがディレクトリ・オブジェクトにアクセスしたり変更したりするための、予測可能な方法を提供します。

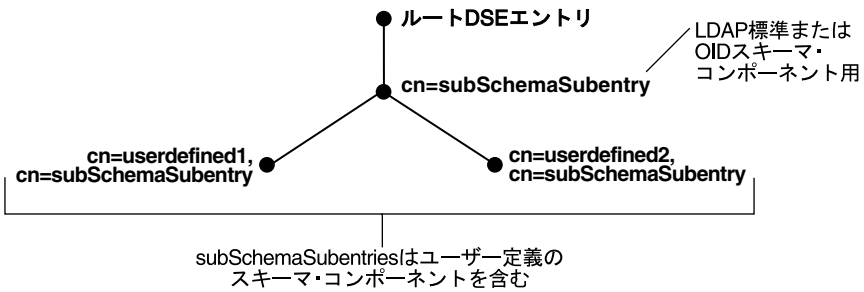
ディレクトリ・スキーマには、ディレクトリ情報ツリー内のデータを編成する方法に関するすべての情報（オブジェクト・クラス、属性、一致規則、構文などのメタデータ）が含まれています。この情報は、**サブエントリ**と呼ばれる特別なクラスのエントリに格納されます。Oracle Internet Directory は、LDAP バージョン 3 の規格に従って、`subSchemaSubentry` と呼ばれるサブエントリにこの情報を格納します。

`subSchemaSubentry` タイプのサブエントリに新規のオブジェクト・クラスと属性タイプを追加できます。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。

10*g*（10.1.4.0.1）以前は、ルート DSE エントリの直下に `cn=subSchemaSubentry` という `subSchemaSubentry` が 1 つしかなく、常にオブジェクト・クラスや属性タイプをそこに直接追加していました。10*g*（10.1.4.0.1）では、エントリ `cn=subSchemaSubentry` に下位エントリを設定できるようになりました。スキーマ・コンポーネントを追加する必要のある Oracle Internet Directory 使用アプリケーションは、`cn=subSchemaSubentry` の下に独自の `subSchemaSubentry` を作成し、そこにスキーマ・コンポーネントを追加できます。図 11-1 は、アプリケーションによって定義された `subSchemaSubentry` エントリ、`cn=userdefined1,cn=subschemasubentry` と `cn=userdefined2,cn=subschemasubentry` を示しています。

スキーマ・エントリはすべて、ルート DSE 属性 `subschemasubentry` に示されています。

図 11-1 subSchemaSubentry タイプのエントリでのスキーマ・コンポーネントの位置



`subSchemaSubentry` エントリの追加には、`bulkload` を使用できません。`ldapadd` を使用する必要があります。

ディレクトリのオブジェクト・クラス

この項の項目は次のとおりです。

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。

エントリを追加する場合は、そのエントリを 1 つ以上のオブジェクト・クラスと関連付けます。各オブジェクト・クラスには、新規エントリと関連付ける属性が含まれています。たとえば、従業員に関するエントリを作成する場合は、そのエントリを person オブジェクト・クラスと関連付けることができます。このオブジェクト・クラスには、その従業員エントリと関連付ける多くの属性（名前、住所、電話番号など）が含まれています。

継承

各オブジェクト・クラスは、スーパークラスの階層から派生し、これらのスーパークラスからの属性を継承します。デフォルトでは、すべてのオブジェクト・クラスは top オブジェクト・クラスから継承します。オブジェクト・クラスをエントリに割り当てると、エントリは、そのオブジェクト・クラスとそのオブジェクト・クラスのスーパークラスの両方の属性をすべて継承します。

オブジェクト・クラスの必須属性とオプション属性

エントリがスーパークラスから**継承**する属性は、必須またはオプションのいずれかです。オプション属性の値は、ディレクトリ・エントリに存在している必要はありません。

オブジェクト・クラスに対して、属性が必須であるか、オプションであるかを指定できます。ただし、この指定は、そのオブジェクト・クラスにのみバインドされます。同じ属性を別のオブジェクト・クラスに割り当てる場合は、そのオブジェクト・クラスに対して必須であるか、オプションであるかを指定しなおすことができます。次の操作が可能です。

- 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
- 既存の標準オブジェクト・クラスからの選択
- 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

関連資料：

- 11-10 ページの「属性管理の概要」
- オブジェクト・クラスの概要は、3-14 ページの「オブジェクト・クラス」を参照してください。
- Oracle Internet Directory とともにインストールされるスキーマ要素のリストは、『Oracle Identity Management ユーザー・リファレンス』の LDAP スキーマの概要に関する項を参照してください。

上位から下位の順序でのエントリの追加

エントリは上位から下位の順序で追加する必要があります。エントリを追加する場合は、そのすべての親エントリがディレクトリに存在している必要があります。同様に、オブジェクト・クラスと属性を参照するエントリを追加するときは、参照先のオブジェクト・クラスと属性が、ディレクトリ・スキーマにすでに存在している必要があります。ディレクトリ・サーバーには標準のディレクトリ・オブジェクトの完全なセットが用意されているため、通常、問題は発生しません。

オブジェクト・クラスの増加

エントリに操作を追加または実行する場合、そのエントリに関連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。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、情報モデル制約を適用します。たとえば、`inetOrgPerson` オブジェクト・クラスは、そのスーパークラスとして、`top`、`person` および `organizationalPerson` を持っています。ある人物を表すエントリを作成する場合、オブジェクト・クラスとして指定する必要があるのは `inetOrgPerson` のみです。Oracle Internet Directory は、各スーパークラス `top`、`person` および `organizationalPerson` によって定義されたスキーマ制約を適用します。

オブジェクト・クラスの追加、変更、削除のガイドライン

この項では、オブジェクト・クラスを追加、変更または削除する際の留意点について説明します。

注意： Oracle Internet Directory は、これら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。

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・クラスを追加するときは、次の点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。実際の属性名と属性名の別名は、すべての属性名と属性別名を通して一意であることが必要です。オブジェクト識別子は一意の識別子、2.16.840.1.113894 で始まり、その後ろに Oracle 指定の接頭辞 .9999 か、サイト固有の接頭辞が続いている必要があります。
- オブジェクト・クラスで参照されるスキーマ・コンポーネント（スーパークラスなど）は、すでに存在している必要があります。
- 抽象型オブジェクト・クラスの場合は、スーパークラスも抽象型であることが必要です。
- スーパークラスの必須属性は、新規オブジェクト・クラスでオプション属性に再定義することが可能です。同様に、スーパークラスのオプション属性は、新規オブジェクト・クラスで必須属性に再定義できます。

注意： Oracle Internet Directory のスキーマ・オブジェクトには、それぞれ特定の制限があります。たとえば、一部のオブジェクトは変更できません。これらの制限事項は、ここでは制約や規則として説明しています。

関連項目： これらの用語の概念については、3-14 ページの「サブクラス、スーパークラスおよび継承」を参照してください。

オブジェクト・クラスの変更のガイドライン

この項では、既存のオブジェクト・クラスに対して実行できる変更のタイプについて説明します。変更は、Oracle Directory Manager およびコマンドライン・ツールを使用して実行できます。

オブジェクト・クラスに対しては、次の変更を実行できます。

- 必須属性からオプション属性への変更
- オプション属性の追加
- スーパークラスの追加
- 抽象型オブジェクト・クラスから構造型または補助型オブジェクト・クラスへの変換（その抽象型オブジェクト・クラスが、別の抽象型オブジェクト・クラスのスーパークラスではない場合）

オブジェクト・クラスを変更するときは、次のガイドラインに注意してください。

- 標準の LDAP スキーマの一部であるオブジェクト・クラスは変更できません。ユーザー定義のオブジェクト・クラスは変更できます。
- 必要な属性が既存のオブジェクト・クラスに設定されていない場合は、補助型オブジェクト・クラスを作成して、必要な属性をそのオブジェクト・クラスに関連付けることができます。
- 既存のオブジェクト・クラスに、必須属性を追加できません。
- ベース・スキーマのオブジェクト・クラスは変更できません。
- 既存のオブジェクト・クラスから属性またはスーパークラスを削除できません。
- 構造型オブジェクト・クラスは、他の型のオブジェクト・クラスに変換できません。
- エントリがすでに関連付けられているオブジェクト・クラスは変更しないでください。

関連項目：

- 11-3 ページの「ディレクトリのオブジェクト・クラス」
- 11-8 ページの「コマンドライン・ツールを使用したオブジェクト・クラスの管理」

オブジェクト・クラスの削除のガイドライン

オブジェクト・クラスの削除に関しても、いくつかの制限事項があります。

- ベース・スキーマからオブジェクト・クラスを削除できません。
- ベース・スキーマ内にないオブジェクト・クラスは、他のスキーマ・コンポーネントから直接または間接的に参照されていないかぎり削除できます。たとえば、このようなオブジェクト・クラスを参照するディレクトリ・エントリがいくつか存在するとします。このオブジェクト・クラスを削除すると、これらのエントリにはアクセスできなくなります。

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

この項では、Oracle Directory Manager を使用して、オブジェクト・クラスの検索、そのプロパティの表示、オブジェクト・クラスの追加、変更および削除を行う方法を説明します。

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

次の方法でオブジェクト・クラスを検索できます。

- オブジェクト・クラスのプロパティを選択する方法。たとえば、名前やオブジェクト識別子を選択します。
- 選択したプロパティの値を入力する方法。
- 選択したオブジェクト・クラスのプロパティと入力値との関連を指定する検索フィルタを選択する方法。「次の文字で始まる」または「完全に一致する」などのフィルタがあります。

この項では、オブジェクト・クラスの検索の入力方法を説明します。

オブジェクト・クラスを検索する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」の順に展開します。
2. 「**スキーマ管理**」を選択します。「スキーマ管理」タブ・ページが、右側のペインに表示されます。
3. 右側のペインの「**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。
4. 検索基準バーから、検索するオブジェクト・クラスのプロパティを選択します。オプションのリストと説明は、A-18 ページの表 A-28 を参照してください。

   注意 : 各オブジェクト・クラスでは、すべての属性が使用されているわけではありません。指定する属性が、探しているオブジェクト・クラス内の属性と実際に一致していることを確認してください。一致する属性がない場合は、検索に失敗します。

5. 検索基準バーの中央のメニューから、検索に使用するフィルタを選択します。オプションのリストと説明は、A-19 ページの表 A-29 を参照してください。
6. 検索基準バーの一番右のテキスト・ボックスに、検索するオブジェクト・クラスのプロパティの値を入力します。たとえば、名前が `orcl` で始まるすべてのオブジェクト・クラスを検索するには、検索基準バーの一番右のテキスト・ボックスに orcl と入力します。
7. 「**基準**」フィールドの下に、次の表で説明する 5 つのボタンがあります。これらのボタンを使用すると、検索基準をさらに詳細に指定できます。
8. 「**検索**」を選択します。検索結果が、「検索 : オブジェクト・クラス」ダイアログ・ボックスの下部のウィンドウに表示されます。

Oracle Directory Manager を使用したオブジェクト・クラスのプロパティの表示

スキーマ内のすべてのオブジェクト・クラスを表示する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」の順に展開します。
2. 「**スキーマ管理**」を選択します。
3. 右側のペインで、「**オブジェクト・クラス**」タブ・ページを選択します。

   個々のオブジェクト・クラスとその属性を調べるには、「**オブジェクト・クラス**」タブ・ページでオブジェクト・クラスを選択します。選択したオブジェクト・クラスのプロパティが、「オブジェクト・クラス」ダイアログ・ボックスに表示されます。

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

Oracle Directory Manager を使用してオブジェクト・クラスを追加する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」の順に展開します。
2. 「**スキーマ管理**」を選択します。
3. 右側のペインで「**オブジェクト・クラス**」タブを選択し、ツールバーの「**作成**」をクリックします。「新規オブジェクト・クラス」ダイアログ・ボックスが表示されます。

   または、「**オブジェクト・クラス**」タブ・ページで、作成するオブジェクト・クラスに類似しているオブジェクト・クラスを選択した後、「**類似作成**」を選択する方法もあります。「新規オブジェクト・クラス」ダイアログ・ボックスに選択したオブジェクト・クラスの属性が表示されます。このオブジェクト・クラスをテンプレートとして使用して、新規のオブジェクト・クラスを作成できます。
4. 「新規オブジェクト・クラス」ダイアログ・ボックスで、フィールドに情報を入力します。詳細は、A-20 ページの表 A-31 を参照してください。
5. 「**OK**」を選択します。

関連資料 :

- 3-15 ページの「オブジェクト・クラスの型」
- 3-14 ページの「サブクラス、スーパークラスおよび継承」
- オブジェクト・クラスを追加する方法の詳細は、Oracle Directory Manager のオンライン・ヘルプを参照してください。

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

オブジェクト・クラスを変更する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」の順に展開します。
2. 「**スキーマ管理**」を選択します。
3. 右側のペインで「**オブジェクト・クラス**」タブを選択した後、変更するオブジェクト・クラスを選択します。「オブジェクト・クラス」ダイアログ・ボックスが表示されます。
4. 「オブジェクト・クラス」ダイアログ・ボックスのフィールドで、情報を変更または追加します。詳細は、A-20 ページの表 A-31 を参照してください。
5. 「**OK**」を選択します。

関連項目：

- 3-15 ページの「オブジェクト・クラスの型」
- 3-14 ページの「サブクラス、スーパークラスおよび継承」

注意： 属性は、補助型オブジェクト・クラスまたはユーザー定義の構造型オブジェクト・クラスに追加できます。

関連項目：補助型オブジェクト・クラスへの属性の追加例は、11-9 ページの「例：補助型またはユーザー定義のオブジェクト・クラスへの新規属性の追加」を参照してください。

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

注意： ベース・スキーマからはオブジェクト・クラスを削除しないことをお薦めします。エントリの参照先であるオブジェクト・クラスを削除すると、そのエントリにアクセスできなくなります。

ベース・スキーマからオブジェクト・クラスを削除する場合は、使用中または将来使用する可能性があるオブジェクト・クラスを削除しないように注意してください。

Oracle Directory Manager を使用してオブジェクト・クラスを削除する手順は、次のとおりです。

1. ナビゲータ・ペインで「**スキーマ管理**」を選択します。
2. 右側のペインで「**オブジェクト・クラス**」タブ・ページを選択し、削除するオブジェクト・クラスを選択します。
3. 「**削除**」を選択します。

コマンドライン・ツールを使用したオブジェクト・クラスの管理

ディレクトリ・スキーマへのオブジェクト・クラスの追加や、既存のオブジェクト・クラスの変更にコマンドライン・ツールを使用できます。コマンドライン・ツールでは、入力ファイルが使用できます。さらに、いくつかのコマンドをスクリプトにまとめて、バッチ処理することもできます。

スキーマ・コンポーネントを追加または変更するには、ldapmodify を使用します。

関連資料：『Oracle Identity Management ユーザー・リファレンス』の `ldapmodify` コマンドライン・ツールのリファレンス

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: ( 2.16.840.1.113894.9999.12345 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
```

この例では、次の操作を行います。

- myobjclass という名前の構造型オブジェクト・クラスを追加します。
- オブジェクト識別子に 2.16.840.1.113894.9999.12345 を指定します。
- スーパークラスとして top を指定します。
- 必須属性として cn と sn を指定します。
- オプション属性として telephonenumber、givenname および myattr を許可します。

記述されている属性すべてが、コマンドの実行前に存在している必要があることに注意してください。

抽象型オブジェクト・クラスを作成する場合は、前述の例の STRUCTURAL を ABSTRACT に置き換えてください。

例 : 補助型またはユーザー定義のオブジェクト・クラスへの新規属性の追加

補助型オブジェクト・クラスまたはユーザー定義の構造型オブジェクト・クラスに新規属性を追加するには、ldapmodify を使用します。この例では、複合変更操作で、古いオブジェクト・クラス定義を削除して新規の定義を追加します。変更はディレクトリ・サーバーによって 1 回のトランザクションでコミットされます。既存のデータは影響されません。入力ファイルには次のように指定します。

```
dn: cn=subschemasubentry
changetype: modify
delete: objectclasses
objectclasses: old value
-
add: objectclasses
objectclasses: new value
```

たとえば、既存のオブジェクト・クラス country に属性 changes を追加する場合、入力ファイルは次のようになります。

```
dn: cn=subschemasubentry
changetype: modify
delete: objectclasses
objectclasses:
 ( 2.16.840.1.113894.9999.12345 NAME 'country' SUP top STRUCTURAL MUST c MAY
 ( searchGuide $ description  )  )
-
add: objectclasses
objectclasses:
 ( 2.16.840.1.113894.9999.12345 NAME 'country' SUP top STRUCTURAL MUST c MAY
 ( searchGuide $ description  $ changes )  )
```

ディレクトリの属性

この項の項目は次のとおりです。

関連資料：

- 属性オプションの詳細は、3-13 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、8-7 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 8-10 ページの「コマンドライン・ツールを使用した属性オプション付きエントリの管理」を参照してください。
- 属性値のサイズを指定する構文の使用方法の詳細は、『Oracle Identity Management ユーザー・リファレンス』の、LDAP の属性構文に関する項を参照してください。

属性管理の概要

属性を扱う操作を実行する前に、概念的な観点から属性を理解する必要があります。

多くの場合、ベース・スキーマにある属性で、ユーザーの組織のニーズを満たすことができます。ベース・スキーマにない属性を使用する場合は、新規属性の追加または既存属性の変更が可能です。

デフォルトでは、属性は複数値です。Oracle Directory Manager またはコマンドライン・ツールを使用して、属性を単一値に指定できます。

関連項目： 属性の概念については、3-10 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。
- 属性名の長さは 127 文字までです。

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、変更または削除できません。

属性の削除に関する規則

属性の削除に関しては、次の規則があります。

- 削除できるのはユーザー定義属性のみです。ベース・スキーマの属性は削除しないでください。
- 他のスキーマ・コンポーネントから直接または間接的に参照されていない属性は、削除することができます。

  エントリの参照先である属性を削除すると、そのエントリはディレクトリ操作に使用できなくなります。

  関連資料： 属性値のサイズを指定する構文の使用方法の詳細は、『Oracle Identity Management ユーザー・リファレンス』の、LDAP の属性構文に関する項を参照してください。

Oracle Directory Manager を使用した属性の管理

この項では、Oracle Directory Manager を使用して、属性の検索、表示、追加、変更、削除および索引付けを行う方法を説明します。

Oracle Directory Manager を使用したすべてのディレクトリ属性の表示

Oracle Directory Manager を使用して属性を表示する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」の順に展開します。
2. 「**スキーマ管理**」を選択します。
3. 右側のペインで、「**属性**」タブ・ページを選択します。このタブ・ページには、属性プロパティを含む表が表示されます。この表の列の説明は、A-20 ページの表 A-32 を参照してください。

   関連項目： 特定のエントリの属性を表示する方法は、8-3 ページの「Oracle Directory Manager を使用した特定エントリの属性の表示」を参照してください。

Oracle Directory Manager を使用した属性の検索

Oracle Directory Manager を使用して属性を検索する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」の順に展開します。
2. 「**スキーマ管理**」を選択します。対応するタブ・ページが、右側のペインに表示されます。
3. 「**属性**」タブ・ページを選択します。
4. 右下隅の「**属性の検索**」ボタンをクリックします。「属性の検索」ダイアログ・ボックスが表示されます。
5. 検索基準バーの一番左のメニューから、検索する属性のプロパティを選択します。オプションの説明は、A-20 ページの表 A-32 を参照してください。
6. 検索基準バーの中央のメニューから、検索に使用するフィルタを選択します。オプションの説明は、A-21 ページの表 A-33 を参照してください。
7. 検索基準バーの一番右のテキスト・ボックスに、検索する属性の値または値の一部を入力します。たとえば、名前が `orcl` で始まる属性をすべて検索するには、検索基準バーの一番右のテキスト・ボックスにこの文字を入力して、「名前」「次の文字で始まる」「`orcl`」という句を作成します。
8. 検索をさらに詳細に指定するには、「**検索基準**」ボックスのボタンを使用して検索基準バーを拡張します。詳細は、A-21 ページの表 A-34 を参照してください。

9. 「**検索**」を選択します。検索結果が、「属性の検索」ダイアログ・ボックスの下部のウィンドウに表示されます。

Oracle Directory Manager を使用した属性の追加

新しい属性の作成や既存の属性からのコピーが可能です。

> **ヒント：** 等価、構文および一致規則は数が多く複雑であるため、これらの特性は、類似の既存属性からコピーすると作業が簡単になります。11-12 ページの「Oracle Directory Manager を使用した既存の属性からの新規属性の作成」を参照してください。

Oracle Directory Manager を使用した新規属性の追加 新規属性を追加する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」の順に展開します。
2. 「**スキーマ管理**」を選択します。
3. 右側のペインで「**属性**」タブを選択し、ツールバーの「**作成**」ボタンをクリックします。「新規属性の型」ダイアログ・ボックスが表示されます。そこには、「**一般**」と「**拡張**」の 2 つのタブ・ページがあります。これらの各フィールドでは、値を入力するかまたはメニューから選択します。
4. 「**一般**」タブの各フィールドに値を入力します。詳細は、A-22 ページの表 A-35 を参照してください。
5. 「**拡張**」タブを選択し、各フィールドに値を入力します。詳細は、A-22 ページの表 A-36 を参照してください。
6. 「**OK**」を選択します。

> **注意：** この属性を使用するには、オブジェクト・クラスに対する属性セットの一部であることを必ず宣言してください。宣言は、ナビゲータ・ペインで「スキーマ管理」を選択した後、右側のペインで「オブジェクト・クラス」タブ・ページを選択して行います。詳細は、11-5 ページの「オブジェクト・クラスの変更のガイドライン」を参照してください。

Oracle Directory Manager を使用した既存の属性からの新規属性の作成 既存属性を利用して属性を追加する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」の順に展開します。
2. 「**スキーマ管理**」を選択します。
3. 右側のペインで「**属性**」タブを選択します。
4. 「**属性**」タブ・ページで、コピーする属性を選択します。
5. 「**類似作成**」を選択します。その属性の「新規属性の型」ダイアログ・ボックスが表示されます。このダイアログ・ボックスには、「**一般**」と「**拡張**」の 2 つのタブ・ページがあります。
6. 「**一般**」タブを選択し、各フィールドに値を入力します。詳細は、A-22 ページの表 A-35 を参照してください。識別名は、新規属性の識別名に必ず変更する必要があります。
7. 「**拡張**」タブを選択し、各フィールドに値を入力します。詳細は、A-22 ページの表 A-36 を参照してください。
8. 「**OK**」を選択します。

注意： この属性を使用するには、オブジェクト・クラスに対する属性セットの一部であることを必ず宣言してください。宣言は、ナビゲータ・ペインで「スキーマ管理」を選択した後、右側のペインで「オブジェクト・クラス」タブ・ページを選択して行います。詳細は、11-5 ページの「オブジェクト・クラスの変更のガイドライン」を参照してください。

Oracle Directory Manager を使用した属性の変更

Oracle Directory Manager を使用して属性を変更する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」の順に展開します。
2. 「**スキーマ管理**」を選択します。
3. 右側のペインで「**属性**」タブを選択して、リストの中から編集可能な属性を選択します。
4. 「**編集**」を選択します。「属性」ダイアログ・ボックスには、「**一般**」と「**拡張**」の 2 つのタブ・ページが表示されます。これらの各フィールドには値を直接入力するか、メニューから値を選択します。
5. 「**一般**」タブを選択し、各フィールドに値を入力します。詳細は、A-22 ページの表 A-35 を参照してください。
6. 「**拡張**」タブを選択し、各フィールドに値を入力します。詳細は、A-22 ページの表 A-36 を参照してください。
7. 「**OK**」を選択します。

Oracle Directory Manager を使用した属性の削除

注意： 削除できるのはユーザー定義属性のみです。ベース・スキーマの属性は削除しないでください。

属性を削除する方法は次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」の順に展開します。
2. 「**スキーマ管理**」を選択します。
3. 右側のペインで「**属性**」タブを選択して、リストの中から編集可能な属性を選択します。
4. 「**削除**」を選択します。

Oracle Directory Manager を使用した属性の索引付け

Oracle Internet Directory は、索引を使用して属性を検索できるようにしています。Oracle Internet Directory のインストール時に、特定の属性はすでに索引付けされています。その他の属性を検索フィルタで使用する場合は、使用する属性に索引を付ける必要があります。

注意： Oracle Directory Manager では、属性の作成時にのみ索引を付けることができます。Oracle Directory Manager を使用して、既存の属性に索引を付けることはできません。既存の属性に索引を付けるには、11-16 ページの「コマンドライン・ツールを使用した属性の索引付け」で説明するカタログ管理ツールを使用します。

次の条件を満たす属性のみ索引を付けることができます。

- 等価の一致規則
- Oracle Internet Directory でサポートされる一致規則（『Oracle Identity Management ユーザー・リファレンス』の、LDAP 属性の一致規則に関する項を参照）
- 属性名が 127 文字以下

Oracle Directory Manager を使用した索引付き属性の表示 索引付き属性を表示する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」の順に展開します。
2. 「**スキーマ管理**」を選択します。
3. 右側のペインで「**属性**」タブ・ページを選択します。このタブ・ページに、スキーマ内のすべての属性が表示されます。「索引付け」列のチェック・ボックスが選択されている場合は、索引付き属性であることを示しています。

Oracle Directory Manager を使用した属性への索引の追加 属性に索引を追加する手順は、次のとおりです。

1. 属性を作成します（11-12 ページの「Oracle Directory Manager を使用した属性の追加」を参照）。
2. 「新規属性の型」ダイアログ・ボックスの「**拡張**」タブ・ページで、「**索引付け**」チェック・ボックスを選択します。

Oracle Directory Manager を使用した属性からの索引の削除 属性から索引を削除する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」の順に展開します。
2. 「**スキーマ管理**」を選択します。
3. 右側のペインで「**属性**」タブを選択します。
4. 索引付き属性を選択します。選択する属性は編集可能である必要があります。編集可能かどうかは、属性名の左にアイコンで示されています。
5. 「**索引の削除**」を選択します。

コマンドライン・ツールを使用した属性の管理

この項では、コマンドライン・ツールを使用した属性の追加、変更および索引付けについて説明します。

ldapmodify を使用した属性の追加と変更

ldapmodify コマンドを使用して新規属性をスキーマに追加するには、コマンド・プロンプトで次のようなコマンドを入力します。

```
ldapmodify -h host -p port -f ldif_file_name
```

LDIF ファイルには、次のようなデータが含まれています。

```
dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: ( 1.2.3.4.5 NAME 'myattr' SYNTAX
                '1.3.6.1.4.1.1466.115.121.1.38' )
```

属性を単一値として指定するには、LDIF ファイルの属性定義エントリに、空白で囲んだキーワード SINGLE-VALUE を含めます。

Oracle Directory Manager または ldapsearch コマンドライン・ツールを使用して、指定した構文のオブジェクト ID を検索できます。

関連資料：

- ldapmodify とそのオプションの詳細は、『Oracle Identity Management ユーザー・リファレンス』の `ldapmodify` コマンドライン・ツールのリファレンス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、11-27 ページの「ディレクトリの構文」を参照してください。

ldapmodify を使用した属性の削除

注意： 削除できるのはユーザー定義属性のみです。ベース・スキーマの属性は削除しないでください。

ldapmodify を使用して属性を削除するには、コマンド・プロンプトで次のようなコマンドを入力します。

```
ldapmodify -h host -p port -f ldif_file_name
```

LDIF ファイルには、次のようなデータが含まれています。

```
dn: cn=subschemasubentry
changetype: modify
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。

関連資料：

- ldapmodify とそのオプションの詳細は、『Oracle Identity Management ユーザー・リファレンス』の `ldapmodify` コマンドライン・ツールのリファレンス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、11-27 ページの「ディレクトリの構文」を参照してください。

コマンドライン・ツールを使用した属性の索引付け

Oracle Internet Directory は、索引を使用して属性を検索できるようにしています。Oracle Internet Directory のインストール時に、エントリ cn=catalogs に、検索で使用できる属性のリストが表示されます。

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
- Oracle Internet Directory でサポートされる一致規則（『Oracle Identity Management ユーザー・リファレンス』の、LDAP 属性の一致規則に関する項を参照）
- 属性の名前が 128 文字以下

新しい属性（ディレクトリにデータが存在していない属性）に、ldapmodify を使用して索引を付けることができます。ディレクトリにデータがすでに存在している属性に索引を付けるには、カタログ管理ツールを使用します。属性から索引を削除するには、ldapmodify を使用することもできますが、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、次のようにします。

```
dn: cn=catalogs
changetype: modify
delete: orclindexedattribute
orclindexedattribute: foo
```

> **関連資料：**『Oracle Identity Management ユーザー・リファレンス』の ldapmodify コマンドライン・ツールのリファレンス

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。

> **関連資料：**『Oracle Identity Management ユーザー・リファレンス』の catalog コマンドライン・ツールのリファレンス

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 delete=T オプションを使用して属性から索引を削除しないように注意してください。ベース・スキーマ属性から索引を削除すると、Oracle Internet Directory の操作に悪影響を及ぼす場合があります。

エントリと関連付けられた属性数の拡大方法

エントリの属性数を拡大できます。使用する方法は、エントリがすでに存在するかどうかによって異なります。

既存エントリの場合、関連付ける属性数の拡大方法には 2 通りあります。1 つは、各エントリの `objectclass` 属性のリストにオブジェクト・クラスの名前を追加する方法です。ディレクトリが比較的小さい場合は、属性に基づいてエントリを検索できるため、この方法が適しています。一方、ディレクトリが大きい場合は、`objectclass` 属性へのオブジェクト・クラスの名前の入力が、非常に複雑な作業になる場合があります。この場合、もう 1 つの方法として、コンテンツ規則を使用する方法で、より効率的にエントリのコンテンツを拡大できます。

この項の項目は次のとおりです。

- ディレクトリでエントリを作成する前の属性数の拡大
- 補助型オブジェクト・クラスの作成による既存エントリの属性数の拡大
- コンテンツ規則の作成による既存エントリの属性数の拡大

ディレクトリでエントリを作成する前の属性数の拡大

Oracle Internet Directory は、インストール時に、標準的な LDAP オブジェクト・クラスといくつかの専用オブジェクト・クラスを用意します。この事前に定義されたオブジェクト・クラスに属している属性のセットには、必須属性を追加できません。エントリに必要なすべての属性が所定のオブジェクト・クラスに含まれていない場合には、次のうちのいずれかを行います。

- 新規の（ベース）オブジェクト・クラスの定義
- オブジェクト・サブクラスの定義

関連項目：

- Oracle Internet Directory とともにインストールされるスキーマに含まれるオブジェクト・クラスのリストは、『Oracle Identity Management ユーザー・リファレンス』の Oracle Identity Management の LDAP オブジェクト・クラスに関する項を参照してください。
- 新規のオブジェクト・クラスまたはオブジェクト・サブクラスを定義する方法については、11-3 ページの「オブジェクト・クラス管理」を参照してください。

補助型オブジェクト・クラスの作成による既存エントリの属性数の拡大

エントリに必要な追加属性を含む補助型オブジェクト・クラスを作成し、その補助型オブジェクト・クラスをエントリと関連付けることができます。補助型オブジェクト・クラスをエントリと関連付けるには、エントリの `objectclass` 属性でそれを指定します。

関連項目：

- 補助型オブジェクト・クラスの作成方法の詳細は、11-3 ページの「オブジェクト・クラス管理」を参照してください。
- オブジェクト・クラスをエントリと関連付ける方法の詳細は、第 8 章「ディレクトリ・エントリの管理」を参照してください。

コンテンツ規則の作成による既存エントリの属性数の拡大

コンテンツ規則は、仕様に従って、特定の構造型オブジェクト・クラスと関連付けられたエントリで使用されるコンテンツの種類を決定します。たとえば、person オブジェクト・クラスと関連付けられたエントリは、そのオブジェクト・クラスの属性だけでなく、他の属性も持つ必要があることを指定できます。追加属性は、補助型オブジェクト・クラスの必須またはオプションの属性にできます。

エントリには補助型クラスをリストする必要があります（これはかなりの管理負荷になることがあります）が、コンテンツ規則をリストする必要はありません。

コンテンツ規則には、コンテンツ規則が適用される構造型オブジェクト・クラスだけでなく、次のものも含めることができます。

- 規則によって制御されるエントリで使用可能な補助型オブジェクト・クラス
- 構造型および補助型オブジェクト・クラスに必要な属性に加え、ディレクトリ情報ツリー・コンテンツ規則によって制御されるエントリで必要な必須属性
- 構造型および補助型オブジェクト・クラスに必要な属性に加え、ディレクトリ情報ツリーのコンテンツ規則によって制御されるエントリで使用可能なオプション属性

コンテンツ規則を作成および変更するための規則

コンテンツ規則は、サブスキーマ・サブエントリ（cn=subschemasubentry）の DITContentRule 属性の値として定義されます。コンテンツ規則は、次の規則に準拠する必要があります。

- エントリの構造型オブジェクト・クラスは、エントリに適用可能なコンテンツ規則を識別します。構造型オブジェクト・クラスに対するコンテンツ規則が存在しない場合、そのオブジェクト・クラスと関連付けられたエントリには、構造型オブジェクト・クラス定義によって許可された属性のみが含まれます。
- コンテンツ規則は構造型オブジェクト・クラスと関連付けられるため、同じ構造型オブジェクト・クラスのすべてのエントリが、ディレクトリ情報ツリーでの位置に関係なく、同じコンテンツ規則を持ちます。
- エントリのコンテンツは、そのエントリの objectClass 属性にリストされたオブジェクト・クラスの一貫性を維持している必要があります。具体的には、次の条件を満たしている必要があります。
  - objectClass 属性にリストされたオブジェクト・クラスの必須属性は、常にエントリ内に存在する必要があります。
  - コンテンツ規則で指定された補助型オブジェクト・クラスのオプション属性は、objectClass 属性にそれらの補助型オブジェクト・クラスがリストされていない場合でも存在できます。

関連項目： コンテンツ規則の作成と管理の詳細は、11-20 ページの「コンテンツ規則の管理」を参照してください。

コンテンツ規則使用時のスキーマ制約

スキーマ整合性についてオブジェクトを検証する場合、ディレクトリ・サーバーはエントリの構造型オブジェクト・クラスのコンテンツ規則を使用します。またエントリにリストされた他のすべてのオブジェクト・クラスも使用します。

オブジェクト・クラスに複数のコンテンツ規則が存在する場合は、エントリの追加または変更時、あるいはデータのバルク・ロード時に、次の規則が適用されます。

- エントリには、各種コンテンツ規則にリストされたすべての補助型オブジェクト・クラスからの属性を含めることができます。コンテンツ規則にオブジェクト・クラスが指定されていない場合、クライアントは、制限なくディレクトリ・エントリの補助型オブジェクト・クラスを明示的に追加できます。
- エントリには、次のものにリストされたすべての必須属性の値を含める必要があります。
  - コンテンツ規則
  - エントリと関連付けられたオブジェクト・クラス
  - エントリに適用可能なコンテンツ規則にリストされた補助型オブジェクト・クラス
- オプションで、次のものにリストされたオプション属性の一部またはすべての値をエントリに含めることができます。
  - コンテンツ規則
  - エントリにリストされたオブジェクト・クラス
  - エントリに適用可能なコンテンツ規則にリストされた補助型オブジェクト・クラス
- 必須と指定された属性は、その属性をオプションと定義する他のすべての定義をオーバーライドします。

コンテンツ規則にリストされたオブジェクト・クラスの検索

コンテンツ規則にリストされた補助型オブジェクト・クラスは、エントリの `objectclass` 属性にリストされないため、それらのオブジェクト・クラスをエントリ検索時にフィルタとしてリストすることはできません。かわりに、関連する構造型オブジェクト・クラスに基づいて検索します。補助型オブジェクト・クラスに基づいて検索する必要がある場合は、その補助型オブジェクト・クラスをユーザー・オブジェクトの `objectclass` 属性に明示的に追加します。

たとえば、構造型オブジェクト・クラス `inetOrgPerson` のコンテンツ規則は、補助型オブジェクト・クラス `orclUser` を指定できます。ただし、これは、ディレクトリ内のすべての `inetOrgPerson` エントリに `orclUser` が `objectclass` 属性の値として含まれることを意味しません。したがって、フィルタ `objectclass=orclUser` を使用した検索は失敗します。コンテンツ規則に含まれる補助型オブジェクト・クラスを問い合せるかわりに、`objectclass=inetOrgPerson` などの構造型オブジェクト・クラスを問い合せる必要があります。

`objectclass=orcluser` に基づいて検索するには、各エントリの `objectclass` 属性の値の 1 つとして `orclUser` を追加します。

この注意事項は、アクセス制御ポリシーで使用するフィルタにも適用されます。追加の補助型オブジェクト・クラスと関連付けられたコンテンツ規則を使用している場合、検索フィルタでは構造型オブジェクト・クラスのみを使用します。

コンテンツ規則の管理

この項では、Oracle Directory Manager およびコマンドライン・ツールを使用してコンテンツ規則を管理する方法を説明します。

Oracle Directory Manager を使用したコンテンツ規則の管理 この項では、Oracle Directory Manager を使用してコンテンツ規則の作成と変更を行う方法を説明します。

Oracle Directory Manager を使用したコンテンツ規則の作成

コンテンツ規則を作成する手順は次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」の順に展開します。
2. 「**スキーマ管理**」を選択します。
3. 右側のペインで「**コンテンツ・ルール**」タブを選択します。
4. 「**作成**」を選択します。「新規コンテンツ・ルール」ダイアログ・ボックスが表示されます。
5. 「新規コンテンツ・ルール」ダイアログ・ボックスの適切なフィールドに値を入力します。フィールドについては、A-23 ページの表 A-38 を参照してください。
6. 「**OK**」を選択します。

Oracle Directory Manager を使用したコンテンツ規則の変更

コンテンツ規則を変更する手順は次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」の順に展開します。
2. 「**スキーマ管理**」を選択します。
3. 右側のペインで「**コンテンツ・ルール**」タブを選択します。
4. 変更するコンテンツ規則を選択し、「**編集**」をクリックします。「コンテンツ・ルール」ダイアログ・ボックスが表示されます。
5. 「コンテンツ・ルール」ダイアログ・ボックスの適切なフィールドに値を入力します。このダイアログ・ボックスのフィールドの説明は、A-24 ページの表 A-39 を参照してください。
6. 「**OK**」を選択します。

コマンドライン・ツールを使用したコンテンツ規則の管理 コンテンツ規則の形式は次のとおりです。

```
DITContentRule  ::=  SEQUENCE  {
oids                              ALPHA-NUMERIC-OID,
structuralObjectClass             OBJECT-CLASS,
LABEL                             CONTENT-LABEL OPTIONAL,
auxiliaries                       SET (1..MAX) OF OBJECT-CLASS OPTIONAL,
mandatory                         SET (1..MAX) OF ATTRIBUTE OPTIONAL,
optional                          SET (1..MAX) OF ATTRIBUTE OPTIONAL,
precluded                         SET (1..MAX) OF ATTRIBUTE OPTIONAL
}
```

表 11-1 に、パラメータを示します。属性およびオブジェクト・クラスの名前では、大文字と小文字が区別されることに注意してください。

表 11-1 コンテンツ規則のパラメータ

パラメータ	説明
oids	コンテンツ規則の一意のオブジェクト識別子（oid）。オブジェクト・クラスまたは属性定義のオブジェクト識別子と同様です。`2.16.840.1.113894` で始まり、その後ろに `.9999` またはサイト固有の接頭辞が続く、一意の数字である必要があります。
LABEL	ディレクトリで適用されるコンテンツ規則のコンテンツ・ラベル。
structuralObjectClass	コンテンツ規則が適用される構造型オブジェクト・クラス。
auxiliaries	コンテンツ規則が適用されるエントリで使用可能な補助型オブジェクト・クラス。
mandatory	コンテンツ規則が適用されるエントリに含まれるユーザー属性タイプ。これは、指定された構造型および補助型オブジェクト・クラスとの関連付けの結果としてエントリに含まれる必須属性に対する追加の属性です。
optional	コンテンツ規則が適用されるエントリに含めることができるユーザー属性タイプ。これは、指定された構造型および補助型オブジェクト・クラスとの関連付けの結果としてエントリに含めることができる属性に対する追加の属性です。

新しいコンテンツ規則の定義中に、ディレクトリ・サーバーは構文を検証し、コンテンツ規則にリストされた属性およびオブジェクト・クラスがディレクトリで定義済であることを確認します。

コンテンツ規則は、構造型オブジェクト・クラスに対してのみ指定できます。オブジェクト・クラスの名前では、大文字と小文字が区別されます。

各構造型オブジェクト・クラスに複数のコンテンツ規則を指定できます。ただし、コンテンツ規則は、オブジェクト・クラスごとに異なるラベルで関連付ける必要があります。

コンテンツ規則の既存の定義を変更する場合、クライアントは既存の定義を削除した後で、新しい定義を追加する必要があります。`replace` コマンドを使用してコンテンツ規則を単純に置き換えることはできません。

コンテンツ規則を削除する場合、クライアントは構造型オブジェクト・クラスおよびコンテンツ規則の英数字のオブジェクト識別子のみを指定する必要があります。オプションで、削除するコンテンツ規則の関連バージョンを指定することもできます。

ディレクトリ内の属性別名

この項の項目は次のとおりです。

属性別名の機能

10*g*（10.1.4.0.1）では、属性名の別名を作成できます。たとえば、属性 sn に対して、わかりやすい別名 surname を作成できます。属性名に別名を作成すると、ユーザーは LDAP 操作で属性名のかわりに別名を指定できます。

属性の LDAP スキーマ定義で、属性に対して別名を定義します。ディレクトリ・スキーマの操作属性 attributeTypes が強化され、属性名リストに別名を含めることができるようになりました。これまでのリリースでは、属性名リストの形式は、次のようなものでした。

```
attributeTypes=( ObjectIdentifier NAME 'AttributeName'  ... )
```

10*g*（10.1.4.0.1）では、オプションで次のように指定できます。

```
attributeTypes=( ObjectIdentifier NAME ( 'AttributeName' 'Alias1' 'Alias2' ...) ... )
```

これは、RFC 2251 および RFC 2252 で指定されているように、LDAP プロトコルと一致します。属性名リストでは、最初の項目は属性の名前として認識され、リストの残りの項目は属性別名として認識されます。たとえば、属性 sn に別名 surname を指定するには、sn の次のスキーマ定義から変更します。

```
attributeTypes=( 2.5.4.4 NAME 'sn' SUP name )
```

から次のように変更します。

```
attributeTypes=( 2.5.4.4 NAME ( 'sn' 'surname' ) SUP name )
```

属性別名規則

次の規則が属性別名に適用されます。

- 属性別名は、すべてのスキーマ・コンポーネントにわたり、実際の属性名すべてとその他の属性別名全体を通して一意であることが必要です。
- 属性名を定義するとき、attributeTypes 定義の最初の値の NAME フィールドは、実際の属性名を指定する必要があります。NAME フィールドで、実際の属性名の後に、属性別名を定義します。
- 属性別名は、属性名と同じ構文規則に従います。
- 別名のない属性を再定義することにより、属性別名を削除します。

注意： 識別名は属性ではありません。スキーマ内では dn を定義できません。したがって、dn の別名を作成できません。

コマンドライン・ツールを使用した属性別名の管理

10*g*（10.1.4.0.1）では、Oracle Directory Manager を使用して属性別名を管理できません。LDIF ファイルを作成し、`ldapmodify` を次の構文で使用することにより、属性別名の追加、変更または削除を行います。

```
ldapmodify -h host -p port -f ldif_file_name
```

次の例は、次のタスクを実行するために使用する LDIF ファイル形式を示しています。

- 複数の属性別名を持つ新規属性の追加
- 既存の属性での属性別名の追加または変更
- 属性別名の削除

複数の属性別名を持つ新規属性の追加

次の LDIF ファイルでは、複数の属性別名 `myalias1` と `myalias2` を持つ属性 `myattr` を追加します。

```
dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: ( 1.2.3.4.5 NAME ( 'myattr' 'myalias1' 'myalias2' ) SYNTAX
                  '1.3.6.1.4.1.1466.115.121.1.38' )
```

既存の属性での属性別名の追加または変更

次の LDIF ファイルでは、属性別名 `surname` と `mysurName` を、既存の属性 `sn` に追加します。

```
dn: cn=subschemasubentry
changetype: modify
delete: attributeTypes
attributeTypes: ( 2.5.4.4 NAME 'sn' SUP name )
-
add: attributeTypes
attributeTypes: ( 2.5.4.4 NAME ( 'sn' 'surname' 'mysurName' ) SUP name )
```

属性別名の削除

次の LDIF ファイルでは、属性 `sn` から属性別名 `mysurName` は削除しますが、属性属性別名 `surName` は削除しません。

```
dn: cn=subschemasubentry
changetype: modify
delete: attributeTypes
attributeTypes: ( 2.5.4.4 NAME ( 'sn' 'surname' 'mysurName' ) SUP name )
-
add: attributeTypes
attributeTypes: ( 2.5.4.4 NAME ( 'sn' 'surname' ) SUP name )
```

次の LDIF ファイルでは、属性別名の `surname` と `mysurName` の両方を属性 `sn` から削除します。

```
dn: cn=subschemasubentry
changetype: modify
delete: attributeTypes
attributeTypes: ( 2.5.4.4 NAME ( 'sn' 'surname' 'mysurName' ) SUP name )
-
add: attributeTypes
attributeTypes: ( 2.5.4.4 NAME 'sn' SUP name )
```

属性別名の使用方法

LDAP スキーマで属性別名を定義すると、ユーザーは LDAP 操作で属性名に別名を代入できます。次の例は、使用するコマンドと予想される結果を示します。

- 属性別名と ldapsearch の使用方法
- 属性別名と ldapadd の使用方法
- 属性別名と ldapmodify の使用方法
- 属性別名と ldapdelet の使用方法
- 属性別名と ldapmoddn の使用方法

表 11-2 は、例で使用されている別名と、それらが表す属性名を示しています。

表 11-2 例で使用されている属性別名

別名	属性名
userid	uid
organizationalunit	ou
country	c
organization	o
surname	sn
commonname	cn
phone	telephonenumber

属性別名と ldapsearch の使用方法

LDAP サーバーは、ldapsearch 操作で、検索フィルタ文字列、ベース識別名、必須属性リスト内の属性別名を認識します。ユーザーが必須属性リストを使用して別名を明示的に要求しなければ、検索結果には実際の属性名が含まれます。たとえば、ユーザーが、ベース識別名で別名 organizationalUnit、country および organization を、フィルタ文字列で別名 surname を使用して、次の検索を指定するとします。

```
ldapsearch -p 389 -h myhost \
   -b "organizationalUnit=dev,country=us,organization=myorg" \
   -s sub "surname=brown"
```

検索は次のような結果を返します。

```
uid=mbrown,ou=dev,c=us,o=myorg
uid=mbrown
sn=Brown
cn=Mark Brown
telephonenumber;office=444006
telephonenumber;mobile=555006
objectclass=organizationalPerson
objectclass=top
objectclass=person
```

次に、ユーザーが、別名 surname、commonname および userid を次のように必須属性リストに含めることにより、明確に別名を要求するとします。

```
ldapsearch -p 389 -h myhost \
   -b "organizationalUnit=dev,country=us,organization=myorg" \
   -s sub "surname=brown" surname commonname userid phone
```

ユーザーが別名を明確に含めたので、検索は次のような結果を返します。

```
uid=mbrown,ou=dev,c=us,o=myorg
surname=Brown
commonname=Mark Brown
userid=mbrown
phone;office=444006
phone;mobile=555006
```

属性別名と ldapadd の使用方法

LDAP サーバーは、追加操作中に、属性名のかわりに属性別名を認識します。LDAP サーバーはエントリを保存する際、別名を実際の属性名に置換します。

コマンドラインの書式は、次のとおりです。

```
ldapadd -h host -p port -f ldif_file_name
```

ユーザーは LDIF ファイルを次のように指定できます。

```
dn: userid=mbrown,organizationalUnit=dev,country=us,organization=myorg
objectclass: account
objectclass: organizationalPerson
userID: mbrown
surname: Brown
commonName: Mark Brown
userpassword: welcome
phone;office: 444006
phone;mobile: 555006
```

エントリは、ファイルに別名のかわりに属性名が含まれてかのように保存されます。ただし、後続の LDAP 検索では、追加または変更時に識別名が入力されたので、識別名が返されます。

```
dn: userid=mbrown,organizationalUnit=dev,country=us,organization=myorg
```

これは LDAP 検索結果を得るための標準動作です。識別名は常に、エントリの作成時に使用されたものと同じ書式で返されます。

属性別名と ldapmodify の使用方法

LDAP サーバーは、変更操作中に、属性名のかわりに属性別名を認識します。

コマンドラインの書式は、次のとおりです。

```
ldapmodify -h host -p port -f ldif_file_name
```

ユーザーは LDIF ファイルを次のように指定できます。

```
dn:
userid=mbrown,organizationalUnit=dev,country=us,organization=myorg
changetype: modify
replace: surname
surname: davis
```

エントリは、ファイルに別名のかわりに属性名が含まれてかのように保存されます。ただし、後続の LDAP 検索では、追加または変更時に識別名が入力されたので、識別名が返されます。

```
dn: userid=mbrown,organizationalUnit=dev,country=us,organization=myorg
```

これは LDAP 検索結果を得るための標準動作です。識別名は常に、エントリの作成時に使用されたものと同じ書式で返されます。

属性別名と ldapdelet の使用方法

LDAP サーバーは、削除操作に指定された識別名で属性別名を認識します。たとえば、ユーザーが次のように検索フィルタで別名 userid、organizationalUnit、country および organization を指定してリクエストをするとします。

```
ldapdelelete -p 389 \
   -h myhost  "userid=mbrown,organizationalUnit=dev,country=us,organization=myorg"
```

サーバーは、ユーザーが次のように入力したものとしてエントリを削除します。

```
ldapdelelete -p 389 \
   -h myhost  "uid=mbrown,ou=dev,c=us,o=myorg"
```

属性別名と ldapmoddn の使用方法

LDAP サーバーは、識別名、新規相対識別名および新規親識別名のオプションで、属性別名を認識します。たとえば、ユーザーが次のコマンドラインを入力するとします。

```
ldapmoddn -b "userid=mbrown,organizationalUnit=dev,country=us,organization=myorg"\
   -R "userid=mdavis"
```

LDAP サーバーは、コマンドラインをユーザーが次のように入力しものとして解釈します。

```
ldapmoddn -b "uid=mbrown,ou=dev,c=us,o=myorg"\
   -R "uid=mdavis"
```

エントリは、ファイルに別名のかわりに属性名が含まれてかのように保存されます。ただし、後続の LDAP 検索では、追加または変更時に識別名が入力されたので、識別名が返されます。

```
dn: userid=mbrown,organizationalUnit=dev,country=us,organization=myorg
```

これは LDAP 検索結果を得るための標準動作です。識別名は常に、エントリの作成時に使用されたものと同じ書式で返されます。

LDAP 操作でのオブジェクト識別子のサポート

ユーザーは、属性別名と同じように、属性名のかわりにオブジェクト識別子を使用できます。

ディレクトリの一致規則

この項の項目は次のとおりです。

- Oracle Directory Manager を使用した一致規則の表示
- ldapsearch を使用した一致規則の表示

注意： 一致規則は変更できません。

Oracle Directory Manager を使用した一致規則の表示

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」の順に展開します。
2. 「**スキーマ管理**」を選択します。
3. 右側のペインで「**一致ルール**」タブを選択します。このタブ・ページのフィールドは列見出しとして表示されます。詳細は、A-23 ページの表 A-37 を参照してください。

ldapsearch を使用した一致規則の表示

サブエントリ cn=subSchemaSubentry で ldapsearch を使用します。

関連資料 :『Oracle Identity Management ユーザー・リファレンス』の ldapsearch コマンドライン・ツールのリファレンス

ディレクトリの構文

この項の項目は次のとおりです。

- Oracle Directory Manager を使用した構文の表示
- ldapsearch を使用した構文の表示

注意 : 構文は変更できません。

Oracle Directory Manager を使用した構文の表示

Oracle Directory Manager を使用して構文を表示する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」の順に展開します。
2. 「**スキーマ管理**」を選択します。
3. 右側のペインで「**構文**」タブを選択します。このタブ・ページのフィールドは列見出しとして表示されます。これには次のようなものがあります。
   - **詳細 :** 属性構文の名前
   - **オブジェクト ID:** この構文の一意の識別子

ldapsearch を使用した構文の表示

サブエントリ cn=subSchemaSubentry で ldapsearch を使用します。

関連資料 :『Oracle Identity Management ユーザー・リファレンス』の ldapsearch コマンドライン・ツールのリファレンス

12

参照整合性

参照整合性は、Oracle Internet Directory の新機能です。参照整合性を有効にした場合、ディレクトリ内のエントリを更新すると、そのエントリを参照する他のエントリもサーバーによって更新されます。たとえば、ユーザーのエントリをディレクトリから削除し、そのユーザーがあるグループのメンバーだとすると、サーバーはユーザーをグループからも削除します。参照整合性が無効の場合、ユーザーは手動で削除されるまでそのグループのメンバーであり続けます。

参照整合性は、次の 2 つの状況で効力を生じます。

- 削除 : エントリが削除されると、このエントリ識別名を参照するすべての識別名属性が削除されます。
- 変更 : エントリの識別名が変更（名前変更）されると、このエントリ識別名を参照するすべての属性が変更されます。

この章の項目は次のとおりです。

参照整合性の構成および有効化

参照整合性を構成し、有効にするには、次の手順を実行します。

1. $ORACLE_HOME/ldap/server/plugin/rimoddn.java ファイルを次のように編集します。

   a. ファイルの 107 行目に移動します。この行は次のようになっています。

   ```
   conn = DriverManager.getConnection(
          "jdbc:oracle:thin:ods/ODSPWD@OHOST:OPORT:OSID");
   ```

   b. ODSPWD を自身の Oracle Internet Directory ODS パスワードに置き換えます。

   c. OHOST を自身の Oracle Internet Directory バックエンド・データベース・ホスト名に置き換えます。

   d. OPORT を自身の Oracle Internet Directory バックエンド・データベース・ポート番号に置き換えます。

   e. OSID を自身の Oracle Internet Directory バックエンド・データベース ORACLE_SID に置き換えます。

2. $ORACLE_HOME/ldap/server/plugin/rimoddn.java ファイルを次のようにコンパイルします。

   ```
   % $ORACLE_HOME/jdk/bin/javac -classpath \
       $ORACLE_HOME/jdbc/lib/classes12.zip:$ORACLE_HOME/ldap/jlib/ospf.jar \
       rimoddn.java
   ```

3. これで rimoddn.java ファイルには、ODS パスワードがクリアテキストで含まれるようになりました。ファイルからパスワードを削除するか、そのファイルに対する権限を変更するかのいずれかで、不正なアクセスを防ぎます。

4. プラグインを登録します。

   ```
   % ldapadd -h hostname -p port -D cn=orcladmin -w orcladmin_pwd -v -f \
     $ORACLE_HOME/ldap/admin/oidriplg.dat
   ```

   これ以降、識別名参照属性に対する ldapmoddn と ldapdelete のすべての操作は記録されます。

   関連項目： 第 32 章「Oracle Internet Directory サーバー・プラグイン・フレームワーク」

5. $ORACLE_HOME/ldap/admin/oidrimdx.pls を次のように編集します。

   a. ファイルの 42 行目に移動します。この行は次のようになっています。

   ```
   v_attrlist := ODS.MODDELREF.t_attrlist('uniquemember', 'owner');
   ```

   この行は、デフォルト値の uniquemember と owner を指定します。

   b. 変更する識別名属性参照がさらにある場合は、行にその他の属性を追加します。たとえば、識別名属性 manager が変更されるように指定するには、行を次のように変更します。

   ```
   v_attrlist := ODS.MODDELREF.t_attrlist('uniquemember', 'owner', 'manager');
   ```

   注意：

   - 属性を指定するときは、すべて小文字を使用します。
   - 追加する各属性は、検索可能であることが必要です。必要な場合は、catalog コマンドを実行して、属性に索引を付けます。

関連項目：

- 9-9 ページの「catalog」
- 11-16 ページの「コマンドライン・ツールを使用した属性の索引付け」

6. `$ORACLE_HOME/ldap/admin/oidrimdx.pls` を頻繁に実行します。正確な頻度はサイト固有のニーズによって異なりますが、15 分から 24 時間ごとが適当な範囲です。

   `$ORACLE_HOME/ldap/admin/oidrimdx.pls` スクリプトは参照整合性記憶域表のレコードを使用し、関連のすべての表で識別名参照を削除または変更します。

   スクリプトを実行するコマンドは次のとおりです。

   ```
   % sqlplus ods/odspassword@connect_string @$ORACLE_HOME/ldap/admin/oidrimdx.pls
   ```

   このコマンドを実行するには、データベース管理者または Oracle Internet Directory 管理者のいずれかであることが必要です。UNIX または Linux システムでは、cron ジョブを設定して、いずれかのシステムのユーザーとしてプログラムを実行できます。コマンドラインをスクリプトまたは crontab ファイルに組み込む場合、ファイル権限が不正ユーザーによる ODS パスワードの表示を防止することを確認してください。

7. エントリ・キャッシュが有効な場合、$ORACLE_HOME/ldap/admin/oidrimdx.pls を実行するたびに無効にしてください。oidrimdx.pls プログラムは、データベース・ディレクトリ内の表を変更するため、キャッシュ内のエントリが不正確になります。`oidrimdx.pls` を実行するたびに、エントリ・キャッシュを次のようにすぐに無効してから有効にします。

   ```
   % ldapmodify -h host -p port -D cn=orcladmin -w orcladmin_pwd <<EOF
   dn:
   changetype: modify
   replace: orclecacheenabled
   orclecacheenabled: 0
   EOF

   % ldapmodify -h host -p port -D cn=orcladmin -w orcladmin_pwd <<EOF
   dn:
   changetype: modify
   replace: orclecacheenabled
   orclecacheenabled: 1
   EOF
   ```

   cron ジョブから `oidrimdx.pls` を実行していて、エントリ・キャッシュが有効になっている場合、キャッシュを無効にするためのコマンドを含める必要があります。

参照整合性の無効化

参照整合性を無効にするには、次の手順を実行します。

1. プラグインを次のように削除します。

   ```
   % ldapdelete -h hostname -p port -D cn=orcladmin -w orcladmin_pwd \
   "cn=ri_postdelete,cn=plugin,cn=subconfigsubentry"
   % ldapdelete -h hostname -p port -D cn=orcladmin -w orcladmin_pwd \
   "cn=ri_postmoddn,cn=plugin,cn=subconfigsubentry
   ```

2. 実行中の `$ORACLE_HOME/ldap/admin/oidrimdx.pls` を停止します。cron ジョブを使用している場合は、それを削除するか無効にします。

13

Oracle Internet Directory の静的グループと動的グループ

この章では、Oracle Internet Directory で静的グループと動的グループの両方を管理する方法について説明します。この章の項目は次のとおりです。

グループの概要

Oracle Internet Directory では、静的グループと動的グループでメンバーシップの割当ておよび管理を実行できます。各タイプのグループは、それぞれ異なる目的に適しています。

この項の項目は次のとおりです。

静的グループ

静的グループは、明示的に管理するメンバーのリストを含むエントリで構成されるグループです。

静的グループに対しては、管理者がそのメンバーシップを明示的に管理する必要があります。たとえば、メンバーが名前を変更した場合、管理者はそのメンバーが属する各グループでそのユーザーの識別名を変更する必要があります。このため、静的グループは、メンバーシップの変更が頻繁に行われないグループに適しています。また、静的グループにはメンバーの識別名のリストが含まれているため、ディレクトリ内でのフットプリントがそのメンバーシップ・リストによって増加します。このため、静的グループは、エントリがディレクトリの領域を取らないグループに適しています。

静的グループ作成のためのスキーマ要素

この種のグループのエントリを作成する場合は、エントリを `groupOfNames` オブジェクト・クラスまたは `groupOfUniqueNames` オブジェクト・クラスのいずれかと関連付けます。

いずれのオブジェクト・クラスにも、グループ・メンバーの名前を格納するための複数値属性があります。ユーザーをグループのメンバーとして割り当てるには、各メンバーの識別名を対応する複数値属性に追加します。逆に、グループからメンバーを削除するには、そのメンバーの識別名を対応する属性から削除します。この複数値属性は、`groupOfNames` オブジェクト・クラスでは `member` で、`groupOfUniqueNames` オブジェクト・クラスでは `uniqueMember` です。

動的グループ

動的グループは、そのメンバーシップがリストで管理されるのではなく、指定した規則およびアサーションに基づいて計算されるグループです。Oracle Internet Directory 10*g*（10.1.4.0.1）では、`labeleduri` 属性に基づく動的グループはキャッシュされます。

キャッシュされることで、動的グループが追加されると、その動的グループのメンバーが計算され、動的グループを後で変更したときに、メンバー・リストの一貫性が維持されます。エントリが追加、変更、削除されたり、名前の変更が行われたりすると、すべての動的グループのメンバー・リストの一貫性が維持されます。たとえば、`c=us` の下にすべての `person` エントリを含む動的グループがある場合、`cn=user1,c=us` を追加すると、そのエントリは動的グループのメンバー・リストに自動的に追加されます。同様に、`cn=user1,c=us` を削除すると、エントリは動的グループのメンバー・リストから削除されます。この機能により、動的グループの検索が実行された場合はいつでも、メンバー・リストを追加の計算なしで返すことができます。動的グループの検索のパフォーマンスは、静的グループの場合と同じになりました。

動的グループは、動的メンバーばかりでなく静的メンバーも持つことができます。静的メンバーは、`member` または `uniquemember` 属性の値として表示されます。

注意： `labeleduri` 属性に基づく動的グループのみがキャッシュされます。`CONNECT_BY` アサーションに基づく動的グループはキャッシュされません。

注意： 有効範囲が base の labeledURI 属性に基づく動的グループは追加できません。有効範囲 sub と one のみがサポートされています。

注意： 動的グループのメンバーシップをリフレッシュするには、DSA 構成エントリの orclrefreshdgrmems 属性を 1 に設定します。Oracle Internet Directory は、すべての動的グループのメンバー・リストを再計算し、orclrefreshdgrmems の値を 0 に再設定します。

注意： 10*g*（10.1.4.0.1）では、あるユーザーが属するグループを問い合せると、動的グループは自動的にその結果に含まれます。

旧リリースでは、静的グループの他に動的グループの問合せを指示する制御を渡す必要がありました。10*g*（10.1.4.0.1）より前のリリースでは、この制御が渡されなかった場合、静的グループの問合せのみが行われました。

Oracle Internet Directory で使用される制御の詳細は、『Oracle Identity Management ユーザー・リファレンス』の LDAP 制御に関する項を参照してください。

関連資料：

- 『Oracle Identity Management アプリケーション開発者ガイド』の C API に関する章
- 『Oracle Identity Management アプリケーション開発者ガイド』の階層検索の実行に関する項

Oracle Internet Directory 10*g*（10.1.4.0.1）での動的グループの拡張機能および制限事項

Oracle Internet Directory 10*g*（10.1.4.0.1）では、動的グループを静的グループと同様に使用できます。たとえば、動的グループは次のもので使用できます。

- アクセス制御リスト。グループを orclACPgroup または orclPrivilegeGroup オブジェクト・クラスのいずれかと関連付けます。
- メンバーの必須属性の検索。動的グループの場合は -G または -C 制御を使用して検索を行い、静的グループの場合は -C 制御を使用します。
- 階層グループ解決の問合せ。

動的グループには Oracle Internet Directory 10*g*（10.1.4.0.1）で次の制限事項があります。

- labelеduri 属性に基づく動的グループのみがキャッシュされます。CONNECT_BY アサーションに基づく動的グループはキャッシュされません。
- 階層問合せと、メンバーの特定の属性関連の問合せは、キャッシュされた動的グループに対してのみ行うことができます。
- 動的グループを追加できるのは、ldapadd を使用した場合のみです。bulkload を使用して追加することはできません。
- catalog ツールを使用して ct_member または ct_uniquemember カタログ表を削除し、再作成する場合、動的グループ・メンバー・リストは、ldapmodify を使用して、DSA 構成エントリの orclrefreshdgrmems 属性を 1 に設定することにより再計算する必要があります。

動的グループ作成のためのスキーマ要素

動的グループを作成する場合も、静的グループの作成と同様に、まず、エントリを groupOfNames オブジェクト・クラスまたは groupOfUniqueNames オブジェクト・クラスのいずれかと関連付けます。次に、そのオブジェクト・クラスを補助型オブジェクト・クラス orclDynamicGroup と関連付けます。この補助型オブジェクト・クラスには、グループのメンバーシップを動的に計算するための 2 つの方法のいずれかを指定する各種属性があります。

この 2 つの方法は、次のとおりです。

- labeledURI 属性を使用する方法

  この方法を使用する場合、ディレクトリ・サーバーはディレクトリ情報ツリーの階層構造に基づいて通常の検索を実行します。この検索を実行するには、orclDynamicGroup オブジェクト・クラスの属性の 1 つ labeledURI に対して値を設定する必要があります。この属性には、問合せのベース、フィルタ、その他の必要なすべての属性を指定します。たとえば、labeledURI 属性に次のような値を入力したとします。

  ```
  labeledURI:ldap://host:port/ou=NewUnit,o=MyCompany,c=US??sub? (objectclass=person)
  ```

  この方法を使用した場合、エントリの検索では、グループの全メンバーのエントリが返されます。

  labeledURI 属性の方法を使用する場合は、orclConnectByAttribute や orclConnectByStartingValue を設定しないでください。

  > **関連資料：**『The LDAP URL Format』（RFC 2255）（T. Howes、M. Smith 著、1997 年 12 月）を参照してください。この RFC では、labeledURI 属性などで LDAP URL を表示する方法について説明しています。Web サイト http://www.ietf.org で入手可能です。

- CONNECT BY アサーションを使用する方法

  この方法は、前述の方法と異なり、ディレクトリ情報ツリーの階層構造ではなく、エントリを暗黙的に相互に結び付ける属性を、ディレクトリ情報ツリー内での位置に関係なく利用します。たとえば、manager 属性は、従業員のエントリをその上司のエントリと結び付けます。この結び付きは、ディレクトリ情報ツリー内での従業員の位置に関係なく適用されます。この方法では、CONNECT BY 句を使用して、階層を作成するために使用する属性（manager など）およびそのような階層の開始値（cn=Anne Smith など）を指定します。

  > **関連資料：**『Oracle Identity Management アプリケーション開発者ガイド』の階層検索の実行に関する項

  この方法を使用するには、表 13-1 に示す各単一値属性の値を orclDynamicGroup オブジェクト・クラスに指定します。

表 13-1 Connect By アサーションのための orclDynamicGroup 属性

属性	説明
orclConnectByAttribute	問合せのフィルタとして使用する属性。例 : manager
orclConnectByStartingValue	orclConnectByAttribute 属性に指定した属性の識別名。例 : Anne Smith

  CONNECT BY アサーションの方法を使用する場合は、labeledURI を設定しないでください。

  たとえば、米国の MyOrganizational Unit の Anne Smith の部下であるすべての従業員のエントリを取得するには、前述の属性に対して次のような値を設定します。

  ```
  orclConnectByAttribute=manager
  orclConnectByStartingValue=
  "cn=Anne Smith,ou=MyOrganizationalUnit,o=MyCompany,c=US"
  ```

また、すべてのメンバーの特定の属性（email 属性など）の値を取得することを指定するアプリケーションを開発することもできます。

> **関連資料：** 特定の属性の値を取得するアプリケーションを開発する方法の詳細は、『Oracle Identity Management アプリケーション開発者ガイド』を参照してください。

階層

階層は、明示的または暗黙的のいずれかにできます。

明示的階層では、ディレクトリ情報ツリーのエントリの位置によって関係が決まります。たとえば、グループ A はディレクトリ情報ツリーでグループ B より上位にあります。

暗黙的階層では、エントリ間の関係は、ディレクトリ情報ツリー内の位置によってではなく、特定の属性の値によって決まります。たとえば、John Doe のエントリが Anne Smith と同じレベルの階層にあるディレクトリ情報ツリーがあるとします。ただし、John Doe のエントリでは、manager 属性に Anne Smith が彼の上司として指定されているとします。この場合、ディレクトリ情報ツリーでの両方の位置は同レベルですが、Anne Smith は John Doe の上司として指定されているため、階層のランクは同一ではありません。

注意： 階層グループを作成する場合は、正しい階層となるように注意してください。たとえば、正しい階層では、グループ A はグループ B のメンバーとなることができますが、グループ B が同時にグループ A のメンバーとなることはできません。後者の関係は循環的であるため、グループ A のメンバーの検索は失敗します。

暗黙的階層に基づく問合せでは、クライアントは検索リクエストに制御 2.16.840.1.113894.1.8.3 を指定できます。この問合せのフィルタは、暗黙的階層の作成に使用する属性を指定します。たとえば、(manager=cn=john doe, o=foo) と指定すると、John Doe が直接または間接的に管理するすべての人が問い合されます。暗黙的階層は、manager 属性に基づいたものとなります。このような問合せでは、検索のベースは無視されます。

Oracle Internet Directory で使用される制御の詳細は、『Oracle Identity Management ユーザー・リファレンス』の LDAP 制御に関する項を参照してください。

> **関連資料：**『Oracle Identity Management アプリケーション開発者ガイド』の C API に関する章

グループ・エントリの問合せ

アプリケーションは、いずれかのグループに問い合せて、次の操作を実行できます。

- グループのすべてのメンバーをリスト
- あるユーザーがメンバーであるすべてのグループをリスト
- あるユーザーが特定のグループのメンバーであるかどうかをチェック

また、指定するメンバー属性について、動的グループに問合せできますが、静的グループには問合せできません。

静的または動的グループを使用すべき場合

使用するグループについて検討する場合は、管理の容易性とパフォーマンスの効率を比較検討する必要があります。たとえば、動的グループは管理が簡単ですが、パフォーマンスが低下します。表 13-2 に、静的グループまたは動的グループの使用を検討する場合の考慮事項を示します。

表 13-2 静的グループと動的グループについての考慮事項

考慮事項	静的グループ	動的グループ
管理の容易性	グループのメンバーシップが大きく、頻繁に変更がある場合は管理が困難	特に、グループのメンバーシップが大きく、頻繁に変更がある場合に有効
パフォーマンス	メンバーシップ・リストを明示的に管理するため、パフォーマンスが向上	メンバーシップはその場で検索されるため、パフォーマンスが低下
ディレクトリ内でのフットプリントのサイズ	グループ・メンバーシップのサイズによっては、フットプリントが拡大	グループ・メンバーシップのサイズに関係なく、小さなフットプリント

グループ・エントリの管理

この項の項目は次のとおりです。

- Oracle Directory Manager を使用した静的グループ・エントリの管理
- コマンドライン・ツールを使用した静的グループ・エントリの管理
- 動的グループ・エントリの例
- Oracle Directory Manager を使用した動的グループの管理
- コマンドライン・ツールを使用した動的グループの管理

注意： グループの階層を作成する場合は、13-5 ページの「階層」で説明したとおり、必ず正しい階層にしてください。

関連項目：

- グループ・エントリのアクセス制御ポリシーの設定方法の詳細は、18-3 ページの「セキュリティ・グループ」を参照してください。
- アクセス権限の詳細は、3-18 ページのグローバリゼーション・サポートおよび第 18 章「ディレクトリ・アクセス制御」を参照してください。

Oracle Directory Manager を使用した静的グループ・エントリの管理

Oracle Directory Manager を使用して、静的グループ・エントリの作成と変更の両方を実行できます。

Oracle Directory Manager を使用した静的グループ・エントリの作成

エントリが groupOfNames オブジェクト・クラスに属する場合は、複数値属性 member に識別名を追加してグループのメンバーシップを決定します。エントリが groupOfUniqueNames オブジェクト・クラスに属する場合は、複数値属性 uniqueMember に識別名を追加してグループのメンバーシップを決定します。

静的グループ・エントリを追加する手順は、次のとおりです。

1. 「**Oracle Internet Directory サーバー**」、「<ディレクトリ・サーバー・インスタンス>」の順に展開します。
2. 「**エントリ管理**」を選択します。
3. ツールバーの「**作成**」ボタンを選択します。「新規エントリ」ダイアログ・ボックスが表示されます。
4. 「**識別名**」フィールドに、完全な識別名を入力します。「**参照**」を使用して、追加するエントリの親の識別名を検索し、親の識別名の左側にカンマで区切って新規エントリの相対識別名を入力することもできます。
5. 新規エントリに使用するオブジェクト・クラスを指定するには、「**オブジェクト・クラス**」ボックスの右の「**追加**」を選択します。「スーパー・クラス・セレクタ」ダイアログ・ボックスが表示されます。
   a. 「スーパー・クラス・セレクタ」ダイアログ・ボックスで、次のオブジェクト・クラスを選択します。
      * top
      * groupOfNames または groupOfUniqueNames
   b. 「**選択**」を選択します。「新規エントリ」ダイアログ・ボックスの「**オブジェクト・クラス**」ウィンドウに、選択したオブジェクト・クラスが表示されます。
6. グループ・エントリの必須属性とオプション属性を入力します。

   groupOfNames オブジェクト・クラスを選択した場合は、いくつかのフィールド、たとえば「**必須プロパティ**」タブ・ページのメンバー・フィールドの横に、「**参照**」ボタンが表示されます。参照によって必須プロパティを入力する手順は、次のとおりです。
   a. 「**参照**」を選択します。「ディレクトリ : エントリ管理」ダイアログ・ボックスが表示されます。
   b. このダイアログ・ボックスを使用して、リストに追加する特定のエントリを検索します。
   c. 「ディレクトリ : エントリ管理」ダイアログ・ボックスの「**識別名**」ウィンドウで、エントリを選択した後、「**OK**」を選択します。「新規エントリ」ダイアログ・ボックスに戻ります。選択したエントリが、メンバー・ウィンドウのリストに追加されています。
7. 「**OK**」を選択します。

Oracle Directory Manager を使用した静的グループ・エントリの変更

グループ・エントリのメンバー・リストを変更する手順は、次のとおりです。

1. 変更するグループ・エントリを検索します。
2. 右側のペインの「**識別名**」ボックスで、変更するグループ・エントリを選択します。
3. 「**編集**」を選択します。
4. 「エントリ」ダイアログ・ボックスで、member 属性のテキスト領域までスクロールして、その値を変更します。
5. 「**OK**」を選択します。

コマンドライン・ツールを使用した静的グループ・エントリの管理

この項では、静的グループ・エントリを作成および変更する方法の例を示します。

ldapadd を使用した静的グループ・エントリの作成

LDIF ファイルの構文は、次のとおりです。

```
dn: DN_of_group_entry
objectclass: top
objectclass: [groupOfNames] [groupOfUniqueNames]
member: DN of member 1
member: DN of member 2
.
.
.
member: DN of member N
```

次のコマンドは、この LDIF ファイルをディレクトリに追加します。

```
ldapadd -p port_number -h host -f file_name.ldif
```

例 : ldapadd を使用した静的グループ・エントリの作成　次の例は、MyStaticGroup というグループのエントリ用の mystaticGroup.ldif という LDIF ファイルを示しています。

```
dn: cn=myStaticGroup,c=us
objectclass: top
objectclass: groupOfNames
member: cn=John Doe
member: cn=Anne Smith
```

次のコマンドは、この LDIF ファイルをディレクトリに追加します。

```
ldapadd -p 389 -h myhost -f myStaticGroup.ldif
```

ldapmodify を使用した静的グループの変更

グループにメンバーを追加する場合、LDIF ファイルの構文は次のようになります。

```
dn: DN_of_group_entry
changetype: modify
add:member
member:DN of member entry
```

グループからメンバーを削除する場合、LDIF ファイルの構文は次のようになります。

```
dn: DN of group entry
changetype: modify
delete:member
member:DN of member entry
```

ファイルを変更するには、次のコマンドを発行します。

```
ldapmodify -p 389 -v  -f file_name.ldif
```

-v は冗長モードを指定します。

例 : ldapmodify を使用した静的グループの変更　次の例は、John Doe を MyStaticGroup というグループに追加します。前述の例と同様に、このユーザー・エントリに関するデータは myStaticGroup.ldif ファイルに記述されています。このファイルの内容は次のとおりです。

```
dn: cn=myStaticGroup,c=us
changetype: modify
add:member
member: cn=John Doe
```

ファイルを変更するには、次のコマンドを発行します。

```
ldapmodify -p 389 -v  -f  myStaticGroup.ldif
```

-v は冗長モードを指定します。

> **注意 :** エントリを追加または変更する場合、Oracle ディレクトリ・サーバーではエントリの存在は検証されません。ただし、属性値に識別名を含める必要がある場合、ディレクトリ・サーバーは識別名が指定されていることを検証します。

動的グループ・エントリの例

この項では、次の 2 種類の動的グループ・エントリの例を示します。

例 : labeledURI 属性を使用した動的グループ・エントリ

次の例は、labeledURI 属性を使用した動的グループ・エントリを示しています。

```
dn: cn=dgroup1
cn: dgroup1
description: this is an example of a dynamic group
labelеduri:ldap://hostname:7777/ou=oid,l=amer,dc=oracle,
 dc=dgrptest??sub?objectclass=person
objectclass: orcldynamicgroup
objectclass: groupOfUniqueNames
objectclass: top
```

このグループには、サブツリー ou=oid,l=amer,dc=oracle,dc=dgrptest 内のオブジェクト・クラス person に関連付けられている、すべてのエントリの識別名となる uniquemember 値が指定されます。

例 : CONNECTBY アサーションを使用した動的グループ・エントリ

次の例は、CONNECTBY アサーションを使用した動的グループ・エントリを示しています。

```
dn: cn=dgroup2
cn: dgroup21
description: this is connect by manager assertion dynamic group
orclconnectbyassertionbase: l=amer,dc=oracle,dc=dgrptest
orclconnectbyattribute: manager
orclconnectbystartingvalue: cn=john doe sr.
objectclass: orcldynamicgroup
objectclass: groupOfUniqueNames
objectclass: top
```

この動的グループには、その manager 属性が直接または間接的に cn=john doe sr. である、すべてのエントリの識別名となる値を持つ固有のメンバーがあります。cn=john doe JR. が複数の従業員の上司として指定されており、さらにその上司として cn=john doe SR. が指定されている場合、cn=john doe SR. より下位のすべての部下が返されます。

Oracle Directory Manager を使用した動的グループの管理

Oracle Directory Manager を使用して、動的グループ・エントリの作成と変更の両方を実行できます。

Oracle Directory Manager を使用した動的グループ・エントリの作成

エントリが groupOfNames オブジェクト・クラスに属する場合は、複数値属性 member に識別名を追加してグループのメンバーシップを決定します。エントリが groupOfUniqueNames オブジェクト・クラスに属する場合は、複数値属性 uniqueMember に識別名を追加してグループのメンバーシップを決定します。

動的グループ・エントリを追加する手順は、次のとおりです。

1. 「**Oracle Internet Directory サーバー**」、「<ディレクトリ・サーバー・インスタンス>」の順に展開します。
2. 「**エントリ管理**」を選択します。
3. ツールバーの「**作成**」ボタンを選択します。「新規エントリ」ダイアログ・ボックスが表示されます。
4. 「**識別名**」フィールドに、完全な識別名を入力します。「**参照**」を使用して、追加するエントリの親の識別名を検索し、親の識別名の左側にカンマで区切って新規エントリの相対識別名を入力することもできます。
5. 新規エントリに使用するオブジェクト・クラスを指定するには、「**オブジェクト・クラス**」ボックスの右の「**追加**」を選択します。「スーパー・クラス・セレクタ」ダイアログ・ボックスが表示されます。
   a. 「スーパー・クラス・セレクタ」ダイアログ・ボックスで、次のオブジェクト・クラスを選択します。
      * top
      * orcldynamicgroup
      * groupOfNames または groupOfUniqueNames
   b. 「**選択**」を選択します。「新規エントリ」ダイアログ・ボックスの「**オブジェクト・クラス**」ウィンドウに、選択したオブジェクト・クラスが表示されます。
6. グループ・エントリの必須属性とオプション属性を入力します。

   グループ内のメンバーシップの動的な計算に labeledURI メソッドを使用する場合は、labeledURI 属性を設定する必要がありますが、orclConnectByAttribute 属性と orclConnectByStartingValue 属性を設定する必要はありません。「**オプション・プロパティ**」タブ・ページの「labeledURI」フィールドで、次のように指定します。

   ldap:*ldap_URL*

   たとえば、次のようになります。

   ```
   ldap://my_host/ou=MyNeworganizationalUnit,
    o=MyCompany,c=US??sub?(objectclass=person)
   ```

   グループ内のメンバーシップの動的な計算に CONNECT BY の方法を使用する場合は、orclConnectByAttribute および orclConnectByStartingValue 属性を設定する必要がありますが、labeledURI 属性を設定する必要はありません。
   「orclConnectByAttribute」フィールドで、問合せのフィルタとして使用する属性（manager など）を指定します。「orclConnectByStartingValue」フィールドで、orclConnectByAttribute 属性で指定した属性の識別名（cn=Anne Smith など）を指定します。

   「**オプション・プロパティ**」タブ・ページに表示される他の属性の指定は、『Oracle Identity Management ユーザー・リファレンス』の、ユーザーおよびグループのスキーマ要素に関する項を参照してください。

   groupOfNames オブジェクト・クラスを選択した場合は、いくつかのフィールド、たとえば「**必須プロパティ**」タブ・ページのメンバー・フィールドの横に、「**参照**」ボタンが表示

されます。「参照」を選択すると、「ディレクトリ:エントリ管理」ダイアログ・ボックスが表示されます。このダイアログ・ボックスを使用して、リストに追加する特定のエントリを検索します。次に、「ディレクトリ:エントリ管理」ダイアログ・ボックスの「**識別名**」ウィンドウで、エントリを選択した後、「**OK**」を選択します。「新規エントリ」ダイアログ・ボックスに戻ります。選択したエントリが、メンバー・ウィンドウのリストに追加されています。

7. 「**OK**」を選択します。

Oracle Directory Manager を使用した動的グループ・エントリの変更

動的グループ・エントリのメンバー・リストを変更する手順は、次のとおりです。

1. 変更するグループ・エントリを検索します。
2. 右側のペインの「**識別名**」ボックスで、変更するグループ・エントリを選択します。
3. 「**編集**」を選択します。
4. 「エントリ」ダイアログ・ボックスで、member 属性のテキスト領域までスクロールして、その値を変更します。
5. 「**OK**」を選択します。

コマンドライン・ツールを使用した動的グループの管理

この項では、コマンドライン・ツールを使用して動的グループを作成および変更する方法について説明します。

ldapadd を使用した動的グループ・エントリの作成

labeledURI 属性を使用する場合、LDIF ファイルの構文は次のようになります。

```
dn: DN_of_group_entry
objectclass: top
objectclass: [groupOfNames] [groupOfUniqueNames]
objectclass: orcldynamicgroup
labeledURI:ldap:ldap_URL
member: DN of member 1
member: DN of member 2
.
.
.
member: DN of member N
```

次のコマンドは、この LDIF ファイルをディレクトリに追加します。

```
ldapadd -p port_number -h host -f file_name.ldif
```

CONNECT BY 文字列を使用する場合、LDIF ファイルの構文は次のようになります。

```
dn: DN_of_group_entry
objectclass: top
objectclass: [groupOfNames] [groupOfUniqueNames]
objectclass: orclDynamicGroup
orclConnectByAttribute:attribute_name
orclConnectByStartingValue:DN_of_attribute
member: DN of member 1
```

この構文でエントリを指定する場合は、識別名を二重引用符で囲まないでください。

例 : ldapadd を使用した動的グループ・エントリの作成

次の例は、動的グループのエントリ用の LDIF ファイルを示しています。

```
dn: cn=myDynamicGroup,c=us
objectclass: top
objectclass: groupOfNames
objectclass: orcldynamicgroup
labeledURI:ldap://my_host/ou=MyNeworganizationalUnit,
 o=MyCompany,c=US??sub?(objectclass=person)
member: cn=John Doe
member: cn=Anne Smith
```

次のコマンドは、この LDIF ファイルをディレクトリに追加します。

```
ldapadd -p 389 -h myhost -f myDynamicGroup.ldif
```

例 : ldapmodify を使用した動的グループの変更

前述の例で作成したグループの組織単位を変更する場合、LDIF ファイルの構文は次のようになります。

```
dn: DN_of_group_entry
changetype: modify
replace:labeledURI
labeledURI:ldap://my_host/
 ou=MyNeworganizationalUnit,o=MyCompany,c=US??sub?(objectclass=person)
```

注意 : エントリを追加または削除する場合、Oracle ディレクトリ・サーバーではエントリ属性値の構文検証は行われません。

14

ディレクトリのロギング、監査および監視

Oracle Internet Directory には、ディレクトリのデバッグ、監査および監視を行うための包括的フレームワークが用意されています。この章の項目は次のとおりです。

- ログ・ファイルの位置
- デバッグ・ロギングの使用
- 監査ログの使用方法
- Oracle Internet Directory サーバーの監視

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 14-1 に、各コンポーネントと対応するログ・ファイルの位置を示します。

表 14-1 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）	`$ORACLE_HOME/ldap/log/bulkload.log`
バルク・モディファイア（bulkmodify）	`$ORACLE_HOME/ldap/log/bulkmodify.log`
バルク削除ツール（bulkdelete）	`$ORACLE_HOME/ldap/log/bulkdelete.log`
カタログ管理ツール（catalog）	`$ORACLE_HOME/ldap/log/catalog.log`
データ・エクスポート・ツール（ldifwrite）	`$ORACLE_HOME/ldap/log/ldifwrite.log`
ディレクトリ統合エージェント	`$ORACLE_HOME/ldap/odi/log/`*`AgentName`*`.err`（*AgentName* にはエージェント名が入ります。）
ディレクトリ統合サーバー（odisrv）	`$ORACLE_HOME/ldap/log/odisrv`*`XX`*`.log`（*XX* には Oracle Directory Integration and Provisioning Server インスタンス番号が入ります。）
ディレクトリ・レプリケーション・サーバー（oidrepld）	`$ORACLE_HOME/ldap/log/oidrepld00.log`
ディレクトリ・サーバー（oidldapd）	`$ORACLE_HOME/ldap/log/oidldapdXXs`*`pid.log`*（pid にはサーバー・プロセス識別子が入ります。） `$ORACLE_HOME/ldap/log/oidstack` *`instance_identifier dispatcher	server PID.log`* **注意：**`oidstack.log` ファイルは、SIGSEGV/SIGBUS 追跡に関係します。また、ディレクトリ・インスタンスの起動時に空ファイルがこの名前で作成されますが、無視できます。
LDAP ディスパッチャ（oidldapd）	`$ORACLE_HOME/ldap/log/oidldapd`*`XX`*`.log`（*XX* にはサーバー・インスタンス番号が入ります。）
OID モニター（oidmon）	`$ORACLE_HOME/ldap/log/oidmon.log`

OPMN	`$ORACLE_HOME/opmn/logs/opmn.log`
	`$ORACLE_HOME/opmn/logs/OID`
	`$ORACLE_HOME/opmn/logs/OIDCTL`
	OPMN によって起動されたその他の Oracle Application Server コンポーネントのログ・ファイルは `$ORACLE_HOME/logs/opmn/` に格納されます。

レプリケーション設定（ldaprepl.sh）	`$ORACLE_HOME/ldap/admin/LOGS/ldaprepl.log`

デバッグ・ロギングの使用

この項の項目は次のとおりです。

Oracle Internet Directory デバッグ・ロギングの概要

Oracle Internet Directory では、次のことが可能になります。

- ディレクトリ・サーバー、ディレクトリ・レプリケーション・サーバー、Directory Integration Server に関するロギング情報の表示
- ロギング・レベルの設定
- ロギングする操作の指定
- 致命的エラーおよび重大エラーに対する対処方法を判断するための標準形式のメッセージの検索
- 重大度と重要性の度合いによるトレース・メッセージの表示
- エントリの識別名、ACP 評価、操作のコンテキストなどに関する関連情報の入ったトレース・メッセージを調べることによる Oracle Internet Directory コンポーネントの診断

ログ・メッセージの概要

この項では、特定の LDAP 操作と関連付けられたログ・メッセージおよび関連付けられていないログ・メッセージについて説明します。トレース・ログの例と、その解釈方法を示します。

特定の LDAP 操作に関するログ・メッセージ

特定の操作に関するログ・メッセージは、トレース・オブジェクトとして格納されます。このオブジェクトは、各種の Oracle Internet Directory モジュールにわたって、操作の開始から終了までを追跡します。これは、次のいずれかの状態が発生した場合に記録されます。

- LDAP 操作が完了したとき
- 優先度の高いメッセージが記録されたとき
- トレース・メッセージ・バッファが一杯になったとき

各スレッドは、操作ごとに連続的な情報ブロックを 1 つ持ち、そのブロックは明確に区切られます。したがって、共有サーバー環境でも、異なるスレッド、操作、接続に関するメッセージの追跡が容易です。

内部メッセージ・バッファ・オーバーフローのため、1 つのトレース・オブジェクトに 1 つの操作に関する情報をすべて格納できない場合、情報は複数のトレース・オブジェクトに分散されます。分散された情報の各部分は明確に区切られており、共通のヘッダーが付けられます。操作の進行を追跡するには、トレース・オブジェクトとその共通ヘッダーを最後までたどります。最後は、「操作が完了しました。」というトレース・メッセージで識別できます。

特定の LDAP 操作と関連付けられていないログ・メッセージ

どの LDAP 操作とも関連付けられていないメッセージは、オブジェクト・ベースではない単純な形式で表示されます。これは、操作が完了したとき、または優先度の高いメッセージが発生したときにログ・ファイルに記録されます。

例 : Oracle Internet Directory サーバー・ログ・ファイル内のトレース・メッセージ

```
2003/01/28:13:44:27 * Main:1 * Starting up the OiD Server, on node dthakuri-sun

2003/01/28:13:44:27 * Main:1 * Oid Server Connected to DB store via inst1 connect
string.
2003/01/28:13:44:27 * Main:1 * OiD LDAP server started.

2003/01/28:13:44:31 * ServerController:1 * INFO * slsfctSpawnDispatcher * Entry
2003/01/28:13:44:31 * ServerController:1 * INFO * gslsfctSpawnDispatcher * Spawned
server dispatcher thread successfully. Thread id : 1
2003/01/28:13:44:31 * ServerController:1 * INFO * gslsfctSpawnDispatcher * Exit


2003/01/28:13:44:31 * ServerWorker:6 * INFO : ServerWorker : Entry
2003/01/28:13:44:31 * ServerWorker:6 * INFO : gslsfccRegisterThread : Entry
2003/01/28:13:44:31 * ServerWorker:6 * INFO : gslsfccRegisterThread : Exit
2003/01/28:13:44:31 * ServerWorker:6 * INFO * gslfsfAStr2Filter *
Filter="(|(objectclass=referral))"
2003/01/28:13:44:31 * ServerWorker:6 * INFO * gslfsfAStr2Filter *
Filter="(objectclass=referral)"
2003/01/28:13:44:31 * ServerWorker:6 * INFO * gslfsfCStr2Simple *
Filter="objectclass=referral"
2003/01/28:13:44:31 * ServerWorker:6 * INFO * gslsbnrNormalizeString() String to
Normalize: "objectclass"
2003/01/28:13:44:31 * ServerWorker:6 * INFO * gslsbnrNormalizeString() Normalized
value: "objectclass"


BEGIN
2003/01/28:13:45:49 * ServerWorker:6 * ConnID:0 * OpId:0 * OpName:bind
13:45:49 * INFO * gslfbiADoBind * Entry
13:45:49 * INFO * gslfbiGetControlInfo * Entry
13:45:49 * INFO * gslfbiGetControlInfo * Exit
13:45:49 * INFO * gslfbiADoBind * connID=0 opID=0 Version=3 BIND dn="" method=128
13:45:49 * INFO * gslfrsBSendLdapResult * Entry
13:45:49 * INFO * gslfrsASendLdapResult2 * Entry
13:45:49 * INFO * sgslunwWrite * Entry
13:45:49 * INFO * sgslunwWrite * Exit
13:45:49 * INFO * gslfrsASendLdapResult2 * Exit
13:45:49 * INFO * gslfrsBSendLdapResult * Exit
13:45:49 * INFO * gslfbiADoBind * Exit
13:45:49 * INFO * Total Bind operation time for dn=2588  micro sec and Total Worker
time=3434  micro sec
END

2003/01/28:13:45:49 * ServerWorker:6 * INFO * ServerWorker * Operation Complete

2003/01/28:13:44:31 * ServerWorker:7 * INFO * ServerWorker : Entry
2003/01/28:13:44:31 * ServerWorker:7 * INFO * gslsfccRegisterThread : Entry
2003/01/28:13:44:31 * ServerWorker:7 * INFO * gslsfccRegisterThread : Exit


BEGIN
2003/01/28:13:48:53 * ServerWorker:13 * ConnID:0 * OpId:0 * OpName:bind
13:48:14 * INFO * gslfbiADoBind * Entry
13:48:53 * INFO * gslfbiGetControlInfo * Entry
13:48:53 * INFO * gslfbiGetControlInfo * Exit
```

```
13:48:53 * INFO * gslfbiADoBind * conn=0 op=0 Version=3 BIND dn="cn=proxy" method=128
13:48:53 * INFO * gslsbbBind * Entry
13:48:53 * INFO * gslsbnrNormalizeString * String to Normalize: "proxy"
13:48:53 * INFO * gslsbnrNormalizeString * Normalized value: "proxy"
13:48:53 * INFO * gslfrsBSendLdapResult * Entry
13:48:53 * INFO * gslfrsASendLdapResult2 * Entry
13:48:53 * INFO * sgslunwWrite * Entry
13:48:53 * INFO * sgslunwWrite * Exit
13:48:53 * INFO * gslfrsASendLdapResult2 * Exit
13:48:53 * INFO * gslfrsBSendLdapResult * Exit
13:48:53 * INFO * gslsbbBind * Exit
13:48:53 * INFO * gslfbiADoBind:Exit
13:48:53 * INFO * Total Bind operation time for dn = cn=proxy is  3710  micro sec
 Total Worker time = 4767  micro sec
END

2003/01/28:13:48:53 * ServerWorker:13 * INFO * ServerWorker * Operation Complete


2003/01/28:14:05:56 * ServerWorker:6 * FATAL * ServerWorker * Processing shutdown
notification
2003/01/28:14:05:56 * ServerWorker:6 * WARNING * ServerWorker * Shutting down worker ID
:  6
```

ログ・ファイル内のトレース・メッセージの解釈方法

前述のメッセージ例に示したとおり、ログ情報は、操作を実行するスレッド、または操作を実行しないスレッドのいずれかと関連付けることができます。操作を実行するスレッドのログのヘッダーには、次の項目が格納されます。

- 日時
- 特定の接続のスレッド名と識別子
- 接続識別子
- 関連付けられた操作の名前と識別子

操作を実行しないスレッドでは、通常のトレース・メッセージが記録されます。そのヘッダーには、日時とスレッド識別子が格納されます。接続および操作に関係する情報は含まれません。

トレース・オブジェクトは、キーワード BEGIN で始まり、キーワード END で終わります。

表 14-2 に、トレース・メッセージ内の各フィールドを示します。

表 14-2 トレース・メッセージ内のフィールド

フィールド 1	フィールド 2	フィールド 3	フィールド 4	フィールド 5	フィールド 6
オブジェクトに基づかないメッセージの場合 : 日時 オブジェクトに基づくメッセージの場合 : 時刻のみ	非オブジェクト・ベースのトレース・メッセージのみの場合、スレッド識別子	トレース・メッセージの重大性。次の 4 つの値があります。 ■ FATAL ■ ERROR ■ WARN（警告） ■ INFO（通知）	機能名	実行された操作に関する情報。この情報は、問題の診断のために使用できます。	エラー・コード（該当する場合）。エラー・コードには、オペレーティング・システム、Oracle データベースまたは LDAP に関するものがあります。

デバッグ・ロギング・レベルの設定

Oracle Directory Manager または **OID 制御ユーティリティ**を使用して、デバッグ・ロギング・レベルを設定できます。

Oracle Directory Manager を使用したデバッグ・ロギング・レベルの設定

デバッグ・ロギング・レベルを設定する手順は、次のとおりです。

1. **ナビゲータ**・ペインで、「Oracle Internet Directory サーバー」を展開して、サーバー・インスタンスを選択します。そのサーバーに対応するタブ・ページが右側のペインに表示されます。
2. 「**デバッグ・フラグ**」タブを選択します。
3. 「**デバッグ・フラグ**」を選択します。
4. 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。それ以外の場合は、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。

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。14-6 ページの表 14-3 に基づいて、デバッグ・レベルの数値を設定します。

デバッグ・レベルは加算方式であるため、アクティブ化する機能を表す数値を加算し、その合計値をコマンドライン・オプションに使用する必要があります。

デフォルトでは、デバッグ・ログは記録されません。デバッグ・ログを記録するには、**ディレクトリ固有のエントリ**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・ファイルを表示するには、*$ORACLE_HOME*`/ldap/log` にナビゲートします。

表 14-3 に、デバッグ・ロギング・レベルの完全なリストを示します。

表 14-3 デバッグ・ロギング・レベル

ロギング・レベルの値	提供される情報
1	大容量トレースのデバッグ
128	パケット・ハンドリングのデバッグ
256	接続管理（ネットワーク・アクティビティ関連）
512	検索フィルタの処理
1024	エントリの解析
2048	構成ファイルの処理
8192	アクセス制御リストの処理
491520	バックエンド（つまり、データベース）との通信のログ
524288	スキーマ関連の操作
4194304	レプリケーション固有の操作
8388608	各接続に関するエントリ、操作および結果のログ
16777216	ファンクション・コール引数のトレース
67108864	このサーバーに接続しているクライアントの数と識別情報
117440511	潜在的なすべての操作 / データ

表 14-3 デバッグ・ロギング・レベル（続き）

ロギング・レベルの値	提供される情報
134217728	Java プラグイン・フレームワーク関連のすべての Java プラグイン・デバッグ・メッセージと内部サーバー・メッセージ
268435456	`ServerLog` オブジェクトを使用して Java プラグインによって渡されるすべてのメッセージ
402653184	上の両方

たとえば、検索フィルタ処理（512）とアクティブな接続管理（256）をトレースするには、次のようにデバッグ・レベルとして 768（512 + 256 = 768）を入力します。

```
oidctl server=oidldapd instance=1 flags='-debug 768' restart
oidctl server=oidrepld instance=1 flags='-h my_host -p 389 -d 768' restart
```

この例では、デバッグ・フラグを付けて、Oracle ディレクトリ・サーバーと Oracle ディレクトリ・レプリケーション・サーバーを再起動しています。

操作デバッグ・ディメンションの設定

ロギングの対象を絞り込むには、デバッグ・レベルと組み合せてデバッグ・ディメンションを使用します。たとえば、ロギングを特定のディレクトリ・サーバー操作に限定するには、それらの操作に対してデバッグ・ディメンションを指定します。

表 14-4 に、これらのディメンションを示します。

表 14-4 LDAP 操作に関するデバッグ・ディメンション値

操作デバッグ・ディメンション値	提供される情報
1	ldapbind
2	ldapunbind
4	ldapadd
8	ldapdelete
16	ldapmodify
32	ldapmodrdn
64	ldapcompare
128	ldapsearch
256	ldapabandon
511	すべての LDAP 操作

デバッグ・ディメンションの設定には、Oracle Directory Manager または ldapmodify のいずれかを使用できます。

Oracle Directory Manager を使用した操作デバッグ・ディメンションの設定

操作デバッグ・ディメンションを設定する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」を展開して、サーバー・インスタンスを選択します。そのサーバーに対応するタブ・ページが右側のペインに表示されます。
2. 「**デバッグ・フラグ**」タブを選択します。
3. 「**デバッグ操作のフラグ**」を選択します。

デフォルトでは、すべての操作が選択されます。特定の操作に関するログを生成するには、対応する操作を選択します。複数の操作を選択できます。

ldapmodify を使用した操作デバッグ・ディメンションの設定

複数の操作を記録するには、そのディメンションの値を加算します。たとえば、ldapbind（1）、ldapadd（4）および ldapmodify（16）の操作をトレースする場合、`orcldebugop` 属性を 21（1 + 4 + 16 = 21）に設定した LDIF ファイルを作成します。この LDIF ファイルは、次のようになります。

```
dn:
changetype:modify
replace:orcldebugop
orcldebugop:21
```

このファイルをロードするには、次のように入力します。

```
ldapmodify -h host_name -p port_number -f file_name
```

ログ・ファイルへのトレース情報のフラッシュの強制

I/O 操作のパフォーマンス・オーバーヘッドを最小限にするため、デバッグ・メッセージは、メッセージがディレクトリ・サーバーに記録されるたびにではなく、定期的にログ・ファイルにフラッシュされます。ログ・ファイルへの書込みは、次のいずれかの状態が発生した場合に実行されます。

- LDAP 操作が完了したとき
- 優先度の高いメッセージが記録されたとき
- トレース・メッセージ・バッファが一杯になったとき

ただし、定期的なフラッシュを待たずに、トレース・メッセージが記録されたときにログ・ファイルでそれを検証することもできます。これを行うには、DSA 構成属性 `orcldebugforceflush` を `1` に設定します。次の例に示すとおり、ldapmodify を使用して、これを行います。

例 14-1 強制フラッシュの有効化

ldapmodify を使用して強制フラッシュを使用可能にする手順は、次のとおりです。

1. 次のような LDIF ファイルを作成します。

```
dn: cn=dsaconfig,cn=configsets,cn=oracle internet directory
changetype: modify
replace: orcldebugforceflush
orcldebugforceflush: 1
```

2. 次のように入力して、このファイルをロードします。

```
ldapmodify -h host_name -p port_number -f file_name
```

注意：

- 強制フラッシュが使用可能な場合、各操作のトレース・メッセージ・オブジェクトの形式は断片化されたものになります。
- デフォルトでは、強制フラッシュは使用禁止です。必要な情報をログ・ファイルにフラッシュした後は、強制フラッシュを無効にしてください。

関連資料： `orcldebugforceflush` 属性の詳細は、『Oracle Identity Management ユーザー・リファレンス』の Oracle Identity Management の LDAP の属性リファレンスに関する項を参照してください。

監査ログの使用方法

監査ログには、Oracle ディレクトリ・サーバーに関するセキュリティ上および操作上のクリティカル・イベントが記録されています。ログはディレクトリ・サーバーのイベントによって生成されるため、管理者による監査ログ・エントリの作成はできません。監査ログ・エントリを作成できるのはディレクトリ・サーバー自体のみです。

監査ログは、通常のディレクトリ・エントリで構成されています。イベントごとに 1 つのエントリがあります。監査ログは ldapsearch を使用して問い合せることができ、監査ログ・エントリは Oracle Directory Manager を使用して表示できます。

デフォルトでは、監査ログは無効です。監査ログを有効にするには、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。

この項の項目は次のとおりです。

関連資料：

- 監査レベルのリストは、14-11 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、14-12 ページの「監査レベルの設定」を参照してください。
- 14-13 ページの「Oracle Directory Manager を使用した監査ログ・エントリの検索」
- 14-14 ページの「ldapsearch を使用した監査ログ・エントリの検索」
- 『Oracle Identity Management ユーザー・リファレンス』の `ldapdelete` コマンドライン・ツールのリファレンス

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。表 14-5 に、orclAuditoc オブジェクト・クラスの属性およびその説明を示します。

表 14-5 オブジェクト・クラスの属性

属性	説明
orclsequence	エントリ名の作成に使用されます。名前は、データベース順序を使用して生成されます。
orcleventtype	発生したイベントのタイプを指定します。この属性はカタログ化されています。
orcleventtime	イベントを発生させる時刻を指定します。時刻は、**UTC** 形式です。UTC 形式であることは、値の最後の z によって示されます。 例 : orcleventtime: 199811281010z
orcluserdn	操作を実行するために Oracle ディレクトリ・サーバーにログインしたユーザーの識別子を指定します。これはカタログ化属性です。
orclopresult	操作の結果を指定します。操作が無事終了した場合は「SUCCESS」、失敗の場合はその理由を示します。
orclauditmessage	テキスト・メッセージを指定します。この属性はカタログ化されていません。
objectclass	値は top と orclauditoc に事前設定されています。

検索フィルタが問合せ基準を満たしている場合でも、通常の検索の結果セットには監査ログ・エントリは含まれません。たとえば、検索条件が objectclass=top の場合、監査ログ・エントリは結果として返されません。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。
11-14 ページの「Oracle Directory Manager を使用した属性の索引付け」を参照してください。

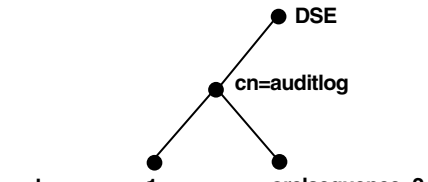
関連資料 :

- カタログ化属性の詳細は、『Oracle Identity Management ユーザー・リファレンス』の catalog コマンドライン・ツールのリファレンスを参照してください。
- top の詳細は、3-15 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。図 14-1 に示すとおり、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 14-1 DSE 下のサンプル監査ログ



orclsequence: 1
orcleventtime: 199811281010z
orclauditmessage: Adding Attribute: (1.2.32.43.3.NAME 'myattr' SYNTAX '1.2.3.4.5.6.7')
orcleopresult: Invalid syntax.
orcluserdn: cn=orcladmin
objectclass: top
objectclass: orclauditoc

監査可能なイベント

表 14-6 に、監査可能なイベントとその監査レベルを示します。3 列目の「監査レベル」は 16 進の値です。複数のイベントを監査するには、この列のそれぞれのイベントに対応する値を加算します。

表 14-6 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	バインドの失敗	0x0008
アクセス違反	アクセス制御ポリシー・ポイントで否認されたアクセス	0x0010
ディレクトリ固有のエントリの変更	DSE に対する変更（成功または失敗）	0x0020
レプリケーション・ログイン	レプリケーション・サーバーの認証（成功または失敗）	0x0040
ACI 変更	アクセス制御リストの変更	0x0080
ユーザー・パスワードの変更	ユーザー・パスワード属性の変更	0x0100
追加	ldapadd 操作（成功または失敗）	0x0200
削除	ldapdelete 操作（成功または失敗）	0x0400
変更	ldapmodify 操作（成功または失敗）	0x0800
識別名の変更	ldapModifyDN 操作（成功または失敗）	0x1000
バインド	ユーザーのバインドの成功	0x2000

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。前の項で説明したイベントを有効または無効にできます。属性の値が 0（ゼロ）の場合（これがデフォルト）、監査は無効です。

監査レベルの設定には、Oracle Directory Manager または ldapmodify のいずれかを使用します。この項では、両方の方法について説明します。

Oracle Directory Manager を使用した監査レベルの設定

Oracle Directory Manager を使用して監査レベルを設定する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」を展開して、ディレクトリ・サーバー・インスタンスを選択します。
2. 右側のペインで、「**監査マスク・レベル**」タブ・ページを選択します。このタブ・ページには、表 14-7 で説明する監査可能イベントのリストが表示されます。

表 14-7 監査マスク・レベル

監査レベル	説明
スーパーユーザー・ログイン	スーパーユーザーのサーバーへのバインド（成功または失敗）
スキーマ要素の追加 / 置換	新規スキーマ要素の追加（成功または失敗）
スキーマ要素の削除	スキーマの削除（成功または失敗）
バインド	バインドの失敗
アクセス違反	ACP で否認されたアクセス
DSE の変更	DSE エントリに対する変更（成功または失敗）
レプリケーション・ログイン	レプリケーション・サーバーの認証（成功または失敗）
ACL の変更	ACP に対する変更
ユーザー・パスワードの変更	ユーザー・パスワード属性の変更
追加	ldapadd 操作（成功または失敗）
削除	ldapdelete 操作（成功または失敗）
変更	ldapmodify 操作（成功または失敗）
識別名の変更	ldapModifyDN 操作（成功または失敗）

3. 使用する監査レベルを選択します。

   成功したイベントと失敗したイベントが選択されている場合は、次の場合を除き、両方が監査ログに記録されます。

   - バインド : バインドに失敗した例のみをログに記録します。
   - アクセス違反 : ACP によってアクセスが拒否されたイベントのみをログに記録します。

4. 「**適用**」を選択します。
5. 変更を有効にするために、ディレクトリ・サーバー・インスタンスを再起動します。

   関連資料 : ディレクトリ・サーバーを再起動する方法は、『Oracle Identity Management ユーザー・リファレンス』の oidctl コマンドライン・ツールのリファレンス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、表 14-8 のイベントを監査するとします。

表 14-8 例 : 監査レベルの設定

イベント	監査レベル	値
スキーマ要素の削除	0x0004	4
DSE の変更	0x0020	32
追加	0x0200	512

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。

> **関連資料 :** ディレクトリ・サーバーを再起動する方法は、『Oracle Identity Management ユーザー・リファレンス』の `oidctl` コマンドライン・ツールのリファレンスを参照してください。

監査ログ・エントリの検索

Oracle Directory Manager または ldapsearch を使用して、監査ログ・エントリを検索できます。

Oracle Directory Manager を使用した監査ログ・エントリの検索

Oracle Directory Manager を使用して監査ログ・エントリを表示する手順は次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」の順に展開します。
2. 「**監査ログ管理**」を選択します。対応する右側のペインが表示されます。
3. 「**最大結果件数**」フィールドに、検索で取得する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。
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. 「**検索基準**」ボックスで、検索基準バーのリストとテキスト・フィールドを使用して、検索基準をさらに詳細に指定します。
   a. 検索基準バーの一番左のリストから、検索するエントリの属性を選択します。各エントリですべての属性が使用されているわけではないため、指定した属性が、検索しているエントリの属性に実際に一致していることを確認する必要があります。一致する属性がない場合は、検索に失敗します。
   b. 検索基準バーの中央のリストから、フィルタを選択します。詳細は、A-31 ページの表 A-45 を参照してください。
   c. 検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。たとえば、選択した属性が cn の場合は、検索する個々の一般名を入力します。
6. 検索をさらに詳細に指定するには、「**検索基準**」ボックスのボタンを使用して検索基準バーを拡張します。詳細は、A-32 ページの表 A-46 を参照してください。

7. 「**検索**」を選択します。検索結果は「識別名」ボックスに表示されます。
8. 特定の監査ログ・エントリのプロパティを表示するには、そのプロパティを「**識別名**」ボックスで選択し、Oracle Internet Directory サーバー管理機能の機能を使用するように選択します。「監査ログ・エントリ」ダイアログ・ボックスに、選択した監査ログのプロパティが表示されます。

> **関連項目：** 検索で表示するエントリ数と検索の制限時間の設定方法は、5-6 ページの「Oracle Directory Manager での検索の表示と期間の構成」を参照してください。

ldapsearch を使用した監査ログ・エントリの検索

監査ログのコンテナの DN は、`cn=auditlog` です。監査ログ・エントリを検索するには、検索のベースとしてコンテナ・オブジェクト `cn=auditlog` を指定し、サブツリー検索または 1 レベルの検索を実行します。

> **関連資料：**『Oracle Identity Management ユーザー・リファレンス』の `ldapsearch` コマンドライン・ツールのリファレンス

監査ログの消去

bulkdelete を使用して、コンテナ `cn=auditlog` の下の監査ログ・オブジェクトを消去できます。次のコマンドを実行します。

```
bulkdelete connect="connect_string" basedn="cn=auditlog"
```

Oracle Internet Directory サーバーの監視

Oracle Internet Directory サーバー管理機能により、Oracle Internet Directory サーバーに関する様々なタイプの情報を監視できます。この項の項目は次のとおりです。

- Oracle Internet Directory サーバー管理機能の機能
- Oracle Internet Directory サーバー管理機能のアーキテクチャとコンポーネント
- Oracle Internet Directory サーバー管理機能の構成情報の位置
- サーバー管理機能情報にアクセスするために使用されるアカウント
- Oracle Internet Directory サーバー管理機能の構成
- 監査および統計エントリの消去
- Oracle Internet Directory サーバー管理機能情報の表示

Oracle Internet Directory サーバー管理機能の機能

Oracle Internet Directory サーバー管理機能フレームワークにより、次のディレクトリ・サーバー統計を監視できます。

- LDAP リクエスト・キュー、メモリー、LDAP セッションおよびデータベース・セッションに関するサーバー健全性統計。たとえば、ある期間のアクティブなデータベース・セッションの数を表示できます。ある期間に Oracle Internet Directory サーバーに対してオープンされた接続の合計数も表示できます。
- パフォーマンス統計。ある期間にわたり、バインド、比較、メッセージング検索およびすべての検索の操作に平均待機時間（ミリ秒）が指定されます。
- 特定のサーバー操作（追加、変更、削除などの操作）に関する一般統計。たとえば、ある期間のディレクトリ・サーバー操作の数を表示できます。
- ディレクトリおよび各操作を実行するユーザーに対する、成功および失敗した操作を含むユーザー統計。すべての LDAP 操作は、構成されたユーザーについて追跡されます。また、統計収集期間の最後の時点でユーザーが保持している接続が追跡されます。
- システム・リソースとセキュリティに関するクリティカル・イベント（ユーザーがパスワードを間違えた場合や、操作の実行に十分なアクセス権限を持っていない場合など）。その他のクリティカル・イベントには、予想されるエラー（1、100 または 1403 など）以外の ORA エラーと LDAP サーバーの異常終了が含まれます。
- ユーザーの成功したバインド操作とユーザーパスワード比較操作、およびユーザーパスワード比較の失敗を追跡するセキュリティ・イベント
- ディレクトリ・サーバーとディレクトリ・レプリケーション・サーバーのステータス情報（ディレクトリ・レプリケーション・サーバーが呼び出された日時など）
- Oracle Directory Integration and Provisioning Server と統合プロファイルのステータス情報（Directory Integration Server が失敗した回数や、統合プロファイルが使用可能かどうかなど）

関連資料：『Oracle Identity Management 統合ガイド』の Oracle Directory Integration Platform の概念とコンポーネントに関する章

Oracle Internet Directory サーバー管理機能のアーキテクチャとコンポーネント

ディレクトリ・サーバー管理機能の各種コンポーネント間の関係については、図 14-2 とその後の表 14-9 で説明します。

図 14-2 Oracle Internet Directory サーバー管理機能のアーキテクチャ

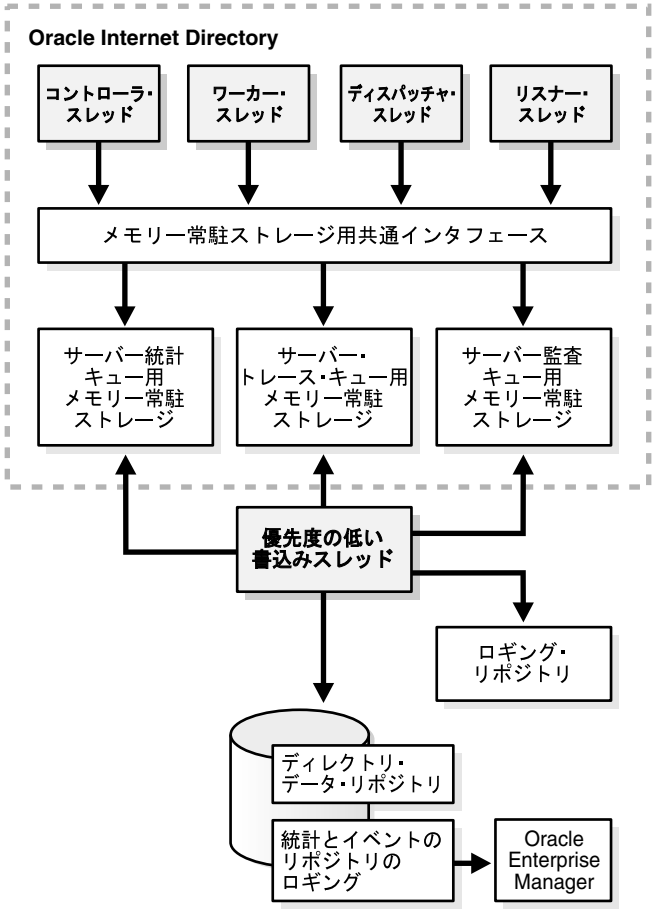


表 14-9 Oracle Internet Directory サーバー管理機能のコンポーネント

コンポーネント	説明
Oracle Internet Directory	ディレクトリ・サーバーは、クライアントからのディレクトリ・リクエストに応答します。コントローラ、ワーカー、ディスパッチャ、リスナーの 4 種類の機能スレッドがあります。ディレクトリ・サーバーは、クライアントからの LDAP リクエストを受信し、処理した後、LDAP レスポンスをクライアントに返信します。 Oracle Internet Directory サーバー管理機能フレームワークを使用して実行時監視機能を設定すると、サーバーの 4 種類の機能スレッドが、指定された情報を記録し、それをローカル・メモリーに格納します。 **関連項目：**ディレクトリ・サーバーの詳細は、3-5 ページの「Oracle ディレクトリ・サーバー・インスタンス」を参照してください。
メモリー常駐ストレージ	これは、ローカル・プロセス・メモリーです。Oracle Internet Directory サーバー管理機能フレームワークは、統計、トレース、監査にそれぞれ 1 つのストレージを割り当てます。それぞれのストレージは、ローカル・メモリー・ストレージで管理される独自のデータ構造を持ちます。
優先度の低い書込みスレッド	これらの書込み専用スレッドは、サーバー統計、監査ロギングおよびトレース情報をリポジトリに書き込むサーバー機能スレッドとは異なります。システム・オーバーヘッドを少なくするため、その優先度は低く保たれます。

表 14-9 Oracle Internet Directory サーバー管理機能のコンポーネント（続き）

コンポーネント	説明
外部監視アプリケーション	このモジュールは独自のもので、サーバー管理機能フレームワークの外部にあります。これは、集められた統計をディレクトリ・サーバーの標準 LDAP インタフェースを通じて収集し、それを専用のリポジトリに格納します。
サーバー管理情報のための外部リポジトリ	これは、収集されたディレクトリ・サーバー統計を格納するために監視エージェントが使用するリポジトリです。監視エージェントがこのリポジトリの実装方法を決定します。
Oracle Enterprise Manager 10*g* Application Server Control コンソール	Application Server Control コンソールは、統計とイベントのリポジトリから、監視されたデータを抽出し、それを Web ベースの Graphical User Interface（GUI）で表示します。ユーザーは通常のブラウザでデータを表示できます。リポジトリは、収集されたデータを一般問合せとカスタム問合せのために格納できます。
ロギング・リポジトリ（ファイル・システム）	このリポジトリは、ファイル・システムを使用して、ディレクトリ・サーバーの各種モジュールでトレースされた情報を格納します。この目的のためにファイル・システムを使用することにより、Oracle Internet Directory サーバー管理機能フレームワークはオペレーティング・システムの機能とセキュリティを使用できます。
ディレクトリ・データ・リポジトリ	このリポジトリには、ユーザーが入力したすべてのデータ（ユーザー・エントリやグループ・エントリなど）が格納されます。
統計とイベントのリポジトリ	このリポジトリは、ファイル・システムにではなく、ディレクトリ・データ・リポジトリと同じデータベースに情報を格納する点を除き、トレース・リポジトリと同じです。この方法で、Oracle Internet Directory サーバー管理機能フレームワークは次の機能を使用できます。 ■ 通常の LDAP 操作による情報の格納と取得 ■ 既存のアクセス制御ポリシーによる収集済情報のセキュリティの管理 ディレクトリ管理機能フレームワークは、この 2 つを別々に格納することにより、収集された情報をディレクトリ・データから分離します。

Oracle Internet Directory サーバー管理機能の構成情報の位置

Oracle Internet Directory サーバー管理機能フレームワークは、サーバー統計、サーバー・トレース、サーバー監査のための 3 つのモジュールすべてに関する構成パラメータを、ディレクトリの DSE ルートに格納します。収集する情報の周期、量、レベルを指定するには、これらのパラメータに対して適切な値を設定する必要があります。

サーバー管理機能情報にアクセスするために使用されるアカウント

Oracle Internet Directory データベース・アカウント `ODSSM` が、データベースからサーバー管理機能情報にアクセスするために使用されます。

インストール時に、このアカウントには無作為に生成されたパスワードが指定されます。

このアカウントの資格証明（無作為に選択されたパスワードなど）は、Enterprise Manager ファイルの `targets.xml` の Oracle Internet Directory スニペットに格納されます。

このアカウントのパスワードは、SQLPLUS を使用しなければ変更できません。`oidpasswd` ツールでは、このパスワードの変更はサポートされていません。また、そのパスワードは Wallet に格納されません。データベースでこのパスワードを変更すると、`targets.xml` ファイルでも変更する必要があります。これは `user` フィールドと `password` フィールドで新規の値を設定するか、`oidemdpasswd` ツールを実行するかのいずれかで行います。

Oracle Internet Directory サーバー管理機能の構成

Oracle Internet Directory サーバー管理機能フレームワークを構成するには、ldapmodify を使用して、ルート DSE の各種属性に対して正の整数値を設定します。

- 健全性統計、一般統計およびパフォーマンス統計を使用可能にするには、`orclStatsFlag` 属性と `orclStatsPeriodicity` 属性を設定します。
- セキュリティ・イベント追跡を構成するには、14-19 ページの「セキュリティ・イベント追跡の構成」を参照してください。
- ユーザー統計を使用するには、次の設定を行います。
  - `orclstatslevel` 属性を 1 に設定します。
  - `orclStatsPeriodicity` 属性を設定します。

  注意： Grid Control の統計を収集している場合は、orclStatsPeriodicity を Enterprise Manager エージェントの収集周期と同じ値（デフォルトでは 10 分）に設定します。

  ユーザーを統計収集のために構成するには、14-20 ページの「接続および操作統計収集のためのユーザーの構成」を参照してください。
- クリティカル・イベントを使用可能にするには、`OrclEventLevel` 属性を設定します。クリティカル・イベントを構成するには、14-20 ページの「クリティカル・イベントの構成」を参照してください。
- スーパーユーザー、プロキシ・ユーザーおよびレプリケーション管理者以外のログインのイベントを使用可能にするには、次のように設定します。
  - `OrclEventLevel` 属性を適切な値に設定します。
  - `orclStatsFlag` を 1 に設定します。

  関連資料： Oracle Internet Directory サーバー管理機能を使用する場合に設定する各属性の詳細は、『Oracle Identity Management ユーザー・リファレンス』の Oracle Identity Management の LDAP の属性リファレンスに関する項を参照してください。

  たとえば、Oracle Internet Directory サーバー管理機能フレームワークを使用可能にするには、次のような LDIF ファイルを作成します。

```
dn:
changetype: modify
replace: orclstatsflag
orclstatsflag:1
```

  このファイルをアップロードするには、次のコマンドを入力します。

```
ldapmodify -h host -p port_number -D bind_DN -w bind_DN_password -f file_name
```

  ここで、サーバー管理機能構成を実行する権限を持つバインド識別名は、`cn=emd admin,cn=oracle internet directory` です。

  関連資料： Oracle Internet Directory サーバー管理機能を使用した Oracle Internet Directory サーバーの監視と管理の詳細は、Oracle Enterprise Manager 10*g* Application Server Control コンソールのオンライン・ヘルプを参照してください。

セキュリティ・イベント追跡の構成

セキュリティ・イベント追跡を構成するには、DSA 構成属性 orcloptracklevel をコマンドラインまたは Oracle Directory Manager を使用して設定します。この属性は、cn=dsaconfig,cn=configsets,cn=oracle internet directory にあります。表 14-10 には、様々なレベルのバインドおよび比較情報収集を構成する DSA 構成属性 orcloptracklevel の値を示しています。

表 14-10 DSA 構成属性 orcloptracklevel の値

orcloptracklevelvalue	構成
1	バインド識別名のみ
2	バインド識別名と IP アドレス
4	比較識別名のみ
8	比較識別名と IP アドレス
16	比較識別名、IP アドレスおよび失敗の詳細

各 orcloptracklevel 値により記録されるメトリックは、次の表に示すとおりです。

表 14-11 各 orcloptracklevel 値により記録されるメトリック

構成	記録されるメトリック
識別名のみ	日時スタンプ 操作を実行する識別名の EID 成功回数 失敗回数
識別名と IP アドレス	識別名の下にのみ示されたすべてのメトリック ソース IP アドレス
識別名、IP アドレスおよび失敗の詳細	識別名と IP アドレスの下に示されたすべてのメトリック 個別の成功回数 個別の失敗回数 IP アドレスからパスワードの比較を実行する各識別名の失敗の詳細 ■ 日時スタンプ ■ ソース IP アドレス ■ パスワードが比較される識別名の EID ■ 失敗回数

2 つの属性、orcloptracknumelemcontainers と orcloptrackmaxtotalsize により、セキュリティ・イベントの追跡に使用されるメモリーをチューニングできます。25-6 ページの「セキュリティ・イベント追跡のチューニング」を参照してください。

接続および操作統計収集のためのユーザーの構成

接続統計収集のためにユーザーを構成するには、ldapmodify コマンドライン・ツールを使用して、ユーザーの識別名を DSA 構成セット・エントリの複数値属性 `orclstatsdn`（DN: cn=dsaconfig, cn=configsets, cn=oracle internet directory）に追加します。これは、Oracle Directory Manager またはコマンドラインを使用して行うことができます。Oracle Directory Manager を使用してユーザーを構成するには、次のようにします。

1. ナビゲータ・ペインで、「Oracle Internet Directory サーバー」を展開して、ディレクトリ・サーバー・インスタンスを選択します。
2. 右側のペインで「問合せの最適化」タブを選択します。
3. ユーザーの識別名を、「問合せの最適化」タブ・ページの「監視中のユーザーの DN」フィールドに追加します。

コマンドラインを使用してユーザーを構成するには、`ldapmodify` コマンドライン・ツールを使用して、ユーザーの識別名を DSA 構成セット・エントリの複数値属性 `orclstatsdn`（DN: cn=dsaconfig,cn=configsets,cn=oracle internet directory）に追加します。たとえば、次のようになります。

```
ldapmodify -h host -p port <<EOF
dn: cn=dsaconfig,cn=configsets,cn=oracle internet directory
changetype:modify
add: orclstatsdn
orclstatsdn: userDN
EOF
```

クリティカル・イベントの構成

クリティカル・イベントを構成するには、ldapmodify を使用し、`OrclEventLevel` 属性に表 14-12 に示すイベント・レベルを 1 つ以上設定します。

表 14-12 クリティカル・イベントのレベル

レベル値	クリティカル・イベント	提供される情報
1	スーパーユーザー・ログイン	スーパーユーザーのバインド（成功または失敗）
2	プロキシ・ユーザー・ログイン	プロキシ・ユーザーのバインド（失敗）
4	レプリケーション・ログイン	レプリケーションのバインド（失敗）
8	追加アクセス	追加アクセス違反
16	削除アクセス	削除アクセス違反
32	書込みアクセス	書込みアクセス違反
64	ORA 3113 エラー	ORA 3113 エラー
128	ORA 3114 エラー	ORA 3114 エラー
256	ORA 28 エラー	ORA-28 エラー
512	ORA エラー	予想される 1、100 または 1403 以外の ORA エラー
1024	Oracle Internet Directory サーバーの終了回数	
2047	すべてのクリティカル・イベント	

監査および統計エントリの消去

不要な監査および統計エントリは、第 26 章「Oracle Internet Directory におけるガベージ・コレクション」で説明されている Oracle Internet Directory 消去ツールにより Oracle Internet Directory から削除されます。

Oracle Internet Directory サーバー管理機能情報の表示

この項の項目は次のとおりです。

- oiddiag ツールによる情報の表示
- Oracle Identity ManagementGrid Control プラグインによる情報の表示
- Oracle Enterprise Manager 10g Application Server Control コンソールによる情報の表示

oiddiag ツールによる情報の表示

すべての統計のレポートは、`oiddiag` ツールを次のように使用すれば表示できます。

```
oiddiag audit_report=true outfile=file_name
```

関連資料：

- 『Oracle Identity Management ユーザー・リファレンス』の `oiddiag` コマンド・ツールのリファレンス
- 『Oracle Application Server 管理者ガイド』の管理ツールに関する章

Oracle Identity ManagementGrid Control プラグインによる情報の表示

10*g*（10.1.4.0.1）の新機能のいくつかは、Oracle Identity Management Grid Control プラグインを使用して表示できます。この新しい Oracle Enterprise Manager インタフェースについては、『Oracle Identity Management 概要および配置プランニング・ガイド』で説明されています。

関連資料：

- 『Oracle Identity Management 概要および配置プランニング・ガイド』の Oracle Identity Management Grid Control プラグインに関する章
- Oracle Enterprise Manager 10*g* Application Server Control コンソールのオンライン・ヘルプ
- Oracle Identity Management Grid Control プラグインのオンライン・ヘルプ

Oracle Enterprise Manager 10*g* Application Server Control コンソールによる情報の表示

Oracle Internet Directory サーバー管理機能の機能の多くを表示するには、Oracle Enterprise Manager 10*g* Application Server Control コンソールを、この項で説明するように使用します。

注意：

Application Server Control コンソールは、SSL モードのみで実行される Oracle ディレクトリ・サーバーのポートのステータス情報を表示しません。

関連資料： Oracle Enterprise Manager 10*g* Application Server Control コンソールの停止と起動については、『Oracle Application Server 管理者ガイド』を参照してください。

Oracle Enterprise Manager 10*g* Application Server Control コンソールを使用した情報収集の有効化
Oracle Enterprise Manager 10*g* Application Server Control コンソールを使用して情報収集を可能にする手順は、次のとおりです。

1. 「Oracle Internet Directory」メイン・ウィンドウで、「**LDAP メトリック**」を選択します。「LDAP 診断の収集構成」ページが表示されます。
2. 「**メトリックの収集**」をチェックします。
3. 「**間隔**」を選択します。
4. 必要なパスワードを入力します。
5. 「**適用**」を選択します。

注意： クリティカル・イベントを使用可能にするには、ldapmodify を使用して `orclEventLevel` 属性を適切な値に設定します。

Oracle Enterprise Manager 10*g* Application Server Control コンソールを使用した新規ディレクトリ・サーバー・インスタンスの起動 サーバーを起動する手順は、次のとおりです。

1. 「Oracle Internet Directory」メイン・ウィンドウで、「**新規インスタンスの起動**」を選択します。「新規 LDAP サーバー・インスタンスの開始」ウィンドウに、表 14-13 のフィールドが表示されます。

表 14-13 Application Server Control コンソールの「新規 LDAP サーバー・インスタンスの開始」ウィンドウのフィールド

列	説明
セット番号	ディレクトリ・サーバー・インスタンスの構成設定番号
デフォルト・ポート	ディレクトリ・サーバー・インスタンスのデフォルト・ポート番号
使用可能なポート	デフォルト・ポートが使用可能かどうかのインジケータ
最大データベース接続数	このディレクトリ・インスタンスで使用可能なデータベース接続の数
サーバー・プロセス	サーバー・プロセスの数
ポート番号	デフォルト・ポート番号を使用しない場合にディレクトリ・サーバー・インスタンスに割り当てるポート番号

2. 「**設定番号**」列で、使用する構成設定を選択します。

   デフォルト・ポートを使用できない場合は、「**ポート番号**」列にポート番号を指定します。
3. 「**起動**」を選択します。

Oracle Enterprise Manager 10*g* Application Server Control コンソールを使用したディレクトリ・サーバー・インスタンスの停止 ディレクトリ・サーバー・インスタンスを停止する手順は、次のとおりです。

1. 「Oracle Internet Directory」メイン・ウィンドウの「**LDAP インスタンス**」セクションで、停止するディレクトリ・サーバー・インスタンスを選択します。
2. 「**停止**」を選択します。

Oracle Enterprise Manager 10*g* Application Server Control コンソールを使用したディレクトリ・サーバー・インスタンスの再起動 ディレクトリ・サーバー・インスタンスを再起動する手順は、次のとおりです。

1. 「Oracle Internet Directory」メイン・ウィンドウの「**LDAP インスタンス**」セクションで、再起動するサーバーを選択します。
2. 「**再起動**」を選択します。「LDAP サーバー・インスタンスの再起動」ウィンドウに、表 14-14 に記載されているフィールドが表示されます。

表 14-14 Application Server Control コンソールの「LDAP サーバー・インスタンスの再起動」ウィンドウのフィールド

列	説明
セット番号	ディレクトリ・サーバー・インスタンスの構成設定番号
デフォルト・ポート	ディレクトリ・サーバー・インスタンスのデフォルト・ポート番号
使用可能なポート	デフォルト・ポートが使用可能かどうかのインジケータ
最大データベース接続数	このディレクトリ・インスタンスで使用可能なデータベース接続の数
サーバー・プロセス	サーバー・プロセスの数
ポート番号	デフォルト・ポート番号を使用しない場合にディレクトリ・サーバー・インスタンスに割り当てるポート番号

3. 構成を選択します。デフォルト・ポートを使用できない場合は、「**ポート番号**」列にポート番号を入力します。
4. 「**起動**」を選択します。

Oracle Enterprise Manager 10*g* Application Server Control コンソールを使用したディレクトリ・サーバー・アクティビティの表示 ディレクトリ・サーバー・アクティビティ情報を表示する手順は、次のとおりです。

1. 「ディレクトリ・サーバー」メイン・ウィンドウで、情報を表示するディレクトリ・サーバー・インスタンスを選択します。
2. 「**ロードの表示**」を選択します。「LDAP ロード」ウィンドウが表示されます。
3. 「**ロード特性の選択**」のリストから、このインスタンスについて表示する情報を選択します。オプションは次のとおりです。
   - **LDAP リポジトリ・データベース・セッション:** このオプションを選択すると、2 つのグラフが表示されます。最初のグラフは、統計収集の指定期間終了時にオープン中のデータベース・セッション、もう 1 つはアクティブなデータベース・セッションに関する情報を示します。
   - **レスポンス時間と LDAP 操作:** このオプションを選択すると、2 つのグラフが表示されます。最初のグラフは、統計収集の指定期間の平均 LDAP 操作レスポンス時間を示します。もう 1 つのグラフは、その期間終了時に進行中であった操作の数を示します。
   - **アクティブ LDAP セッションと新規 LDAP セッション:** このオプションを選択すると、2 つのグラフが表示されます。最初のグラフは、アクティブな LDAP セッション（統計収集の指定期間終了時にオープンしていたセッション）の数を表示します。2 番目のグラフは、新規 LDAP セッション（統計収集の指定期間中にオープンされたセッション）の数を表示します。
4. 選択した後、「**実行**」をクリックします。

Oracle Enterprise Manager 10*g* Application Server Control コンソールを使用したディレクトリ・サーバー操作の表示 Application Server Control コンソールを使用して、統計収集の指定期間中のディレクトリ・サーバー操作を表示できます。この手順は、次のとおりです。

1. 「ディレクトリ・サーバー」メイン・ウィンドウで、情報を表示するディレクトリ・サーバー・インスタンスを選択します。
2. 「**操作の表示**」を選択します。すべての LDAP 操作に関するチャートが表示されます。チャートをクリックすると、チャートが拡大表示されます。

15

ディレクトリのバックアップとリストア

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

- 小さいディレクトリまたはディレクトリ内の特定のネーミング・コンテキストのバックアップとリストア
- 大きいディレクトリのバックアップとリストア

小さいディレクトリまたはディレクトリ内の特定のネーミング・コンテキストのバックアップとリストア

小さいディレクトリまたはディレクトリ内の特定のネーミング・コンテキストのバックアップとリストアを行う手順は、次のとおりです。

1. ldifwrite ユーティリティを使用してノードをバックアップします。次のコマンドを入力します。

   ```
   ldifwrite connect="connect_string"  basedn="naming_context" file="backup.ldif"
   ```

2. 次のコマンドを入力して、新規ノードでディレクトリ・サーバーを起動します。

   ```
   oidctl connect= connect_string  server=oidldapd instance=1 \
         flags= '-p port_number' start
   ```

3. ldapaddmt ユーティリティを使用して、新規ノードにデータをロードします。次のコマンドを入力します。

   ```
   bulkload connect="connect_string" check="TRUE" generate="TRUE" \
     load="TRUE" restore="TRUE" append=TRUE" file="/complete_path/backup.ldif"
   ```

注意： Oracle Internet Directory の旧リリース（10*g* リリース 2（10.1.2.0.2）など）のデータのバックアップを取り、それを 10*g*（10.1.4.0.1）が稼働中のノードでリストアする場合、パスワード・ポリシー・エントリを、30-32 ページの「パスワード・ポリシーとファンアウト・レプリケーション」で説明しているように更新する必要があります。

大きいディレクトリのバックアップとリストア

大きいディレクトリのバックアップとリストアの方法は、『Oracle Application Server 管理者ガイド』を参照してください。

第 III 部

ディレクトリのセキュリティ

第Ⅲ部では、次の内容について説明します。

- ディレクトリ内のデータの保護
- 企業およびホスティングされた環境内のアプリケーションを管理するアクセス制御の確立
- パスワードの管理ポリシーの設定および管理
- 他の Oracle コンポーネントへのユーザーの認証に使用するパスワード・ベリファイアの管理
- ユーザー、グループおよびサービスに関するデータの 1 つのリポジトリへの格納、およびそのデータ管理の様々な管理者への委任

第Ⅲ部は次の各章で構成されています。

16

ディレクトリ・セキュリティの概念

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

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

この章では、Oracle Internet Directory セキュリティ機能の概念上の概要を示します。この章の項目は次のとおりです。

データの整合性と Oracle Internet Directory

Oracle Internet Directory は、Secure Sockets Layer（SSL）を使用して、送信時にデータの変更、削除または再現が行われないことを保証します。SSL は、暗号方式の保護メッセージ・ダイジェストを、**MD5** アルゴリズムまたは **Secure Hash Algorithm** 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 17 章「Secure Sockets Layer（SSL）とディレクトリ」を参照してください。

データのプライバシと Oracle Internet Directory

データ・プライバシは、データの送信時と受信後の両方で重要な問題です。この項では、Oracle Internet Directory がこれら 2 つの状況でデータをどのように保護するかについて説明します。この項の項目は次のとおりです。

データ送信時のプライバシ

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宛先に対して、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エクスポート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 17 章「Secure Sockets Layer（SSL）とディレクトリ」を参照してください。

受信した機密の属性のプライバシ

Oracle Internet Directory は、機密の属性を暗号化形式で格納します。機密の属性の例としては、orclpasswordattribute、orclrevpwd、プラグイン属性 orclpluginsecuredflexfield およびサーバー・チェーン属性 orclOIDSCExtPassword があります。

orcldataprivacymode 属性は、データの受信時にこれらの属性を暗号化するかどうかを制御します。orcldataprivacymode が有効な場合、機密の属性は暗号化されます。プライバシ・モードが無効の場合、機密のデータはクリアテキストで返されます。

プライバシ・モードはデフォルトでは無効です。つまり、orcldataprivacymode の値は 0 です。セキュリティ保護を提供するには、orcldataprivacymode の値を 0 から 1 に変更することで、プライバシ・モードを有効にする必要があります。

orcldataprivacymode の値を決定するには、次の検索を実行します。

```
$ORACLE_HOME/bin/ldapsearch -h host -p port -D cn=orcladmin -w password \
   -b "cn=dsaconfig,cn=configsets,cn=oracle internet directory" -s base \
   "objectclass=*" orcldataprivacymode
```

プライバシ・モードを有効にするには、次のエントリが含まれる LDIF ファイルを使用します。

```
dn: cn=dsaconfig,cn=configsets,cn=oracle internet directory
changetype: modify
replace: orcldataprivacymode
orcldataprivacymode: 1
```

LDIF ファイルを次のようなコマンドラインによりロードします。

```
$ORACLE_HOME/bin/ldapmodify -h host -p port -D cn=orcladmin -w password -v \
   -f LDIF_file_name
```

Oracle Internet Directory での認可

認可とは、オブジェクトまたはオブジェクトのセットへのアクセスのためにユーザー、プログラムまたはプロセスに与えられる権限です。ディレクトリ・セッション中にディレクトリ操作が試行されると、ディレクトリ・サーバーによって、ユーザーにこれらの操作を実行するための権限があるかどうかが確認されます。ユーザーに権限がない場合、ディレクトリ・サーバーはこれらの操作を許可しません。ディレクトリ・サーバーはアクセス制御情報を使用して、ディレクトリ・ユーザーによる不正操作からディレクトリ・データを保護します。

アクセス制御情報アイテム（ACI）は、アクセス制御に関連する管理ポリシーを記録したディレクトリ・メタデータです。この情報は、ユーザーによる変更が可能な操作属性として、Oracle Internet Directory に格納されています。各属性は、**アクセス制御情報項目**と呼ばれます。

通常、**アクセス制御リスト**と呼ばれるこの ACI 属性値のリストは、ディレクトリ・オブジェクトと関連付けられています。このリストの属性値は、様々なディレクトリ・ユーザー・エンティティ（対象）が各オブジェクトに対して所有している権限を表しています。

ACI は次のコンポーネントで構成されています。

- アクセス権限を付与するオブジェクト
- アクセス権限を付与するエンティティ（サブジェクト）
- 付与するアクセス権限の種類

アクセス制御ポリシーは規定的です。つまり、そのセキュリティ・ディレクティブは、**ディレクトリ情報ツリー**内のすべての下位エントリに適用されるように設定できます。アクセス制御ポリシーが適用される開始点は、**アクセス制御ポリシー・ポイント**と呼ばれます。

ACI は、ディレクトリ内にテキスト文字列として記述され、格納されています。この文字列は、ACI ディレクティブ書式と呼ばれる、明確に定義された書式に従う必要があります。ACI 属性の各有効値は、個別のアクセス制御ポリシーを表します。

ホスティングされた環境で実行されているアプリケーションでは、ディレクトリ・アクセス制御の次の機能が使用できます。

- 規定のアクセス制御

  サービス・プロバイダは、ディレクトリ・オブジェクトの集合に対してアクセス制御リスト（ACL）を指定できます。個々のオブジェクトごとにポリシーを設定する必要はありません。この機能によって、アクセス制御の管理が簡素化されます。特に同じポリシーまたは同等のポリシーで管理されるオブジェクトが多数含まれる大きなディレクトリで有効です。

- 階層的なアクセス制御管理のモデル

  サービス・プロバイダは、ホスティングされた企業にディレクトリ管理を委任できます。必要に応じて、レルムからさらに委任することもできます。

- 委任ドメインに対する管理無効制御

  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、サブジェクトとオブジェクトの双方を、そのネームスペースおよびディレクトリのその他のオブジェクトとの関連の点で識別できます。たとえば、あるレルムの管理者は、ユーザーの上司のみに、そのユーザーの給与属性の更新を認めることができます。他のレルムの管理者は、給与属性に関して、これと異なるポリシーを確立して適用できます。

Oracle Internet Directory での認証

認証は、ディレクトリ・サーバーが、そのディレクトリに接続しているユーザーの正体を確定するプロセスです。認証は、LDAP セッションが ldapbind 操作によって確立されたときに発生します。このようにして、すべてのセッションにユーザー ID が関連付けられます。

ユーザー、ホストおよびクライアントの識別情報を検証するために、Oracle Internet Directory では、3 種類の一般的な認証を使用できます。それらについて、次の項目で説明します。

- 直接認証
- 間接認証
- 外部認証

直接認証

この項では、Oracle Internet Directory 内で使用可能な 3 種類の直接認証と、SASL 対応クライアントがディレクトリ・サーバーに対して認証を行う方法について説明します。直接認証オプションには、次の 3 種類があります。

- 匿名認証

  匿名で認証する場合、ユーザーは、ユーザー名とパスワードのフィールドを空白のままにしてログインします。各匿名ユーザーは、匿名ユーザーに付与されている権限すべてを使用できます。

- 簡易認証

  簡易認証を使用する場合、クライアントは、ネットワーク上を暗号化されずに送信される識別名とパスワードによって、サーバーに対して自己認証を行います。

- Simple Authentication and Security Layer（SASL）を使用した認証

  これは、接続ベースのプロトコルに認証サポートを追加する方法です。SASL を使用するために、プロトコルには、ユーザーを識別してサーバーに対して認証を行うコマンドが含まれます。また、オプションで、以降のプロトコル対話の保護を規定するコマンドも含まれます。SASL の使用が正常に規定されると、プロトコルと接続の間にセキュリティ・レイヤーが挿入されます。

Oracle Internet Directory は、SASL を使用する 2 種類の認証メカニズムをサポートします。

– ダイジェスト MD5: LDAP バージョン 3 内では必須の認証メカニズムです（RFC 2829）。MD5 ハッシュ関数を使用して、任意の長さのメッセージを、クライアント / サーバー認証のベリファイアとして使用できる 128 ビットのメッセージ・ダイジェストに変換します。

– 外部認証 : SSL 相互認証を使用するメカニズム。この場合、クライアントは、ユーザー名とパスワードを使用するかわりに、証明書、トークンまたは他のデバイスによって、サーバーに対して認証します。証明書による認証には、次の形式があります。

  * 完全一致 : クライアント証明書内のサブジェクト DN が、ディレクトリ内のユーザー DN と比較されます。この 2 つの値が一致すると、バインドが行われます。

  * 証明書ハッシュ : クライアント証明書がハッシュ処理され、ディレクトリ内に保管されている証明書のハッシュ値と比較されます。この 2 つの値が一致し、かつこのペアに関連付けられている DN が 1 つのみの場合は、バインドが行われます。複数の DN が関連付けられている場合は、証明書ハッシュとユーザー DN の関係は n 対 1 の対応であり 1 対 n の対応ではないので、エラーが返されます。つまり、1 つの DN には複数の証明書を関連付けることができますが、1 つの証明書には 1 つの DN しか関連付けられません。

  * 完全一致 / 証明書ハッシュ : まず、完全一致検索が行われます。一致するものがない場合は、証明書ハッシュが実行されます。

  これらの方法のいずれかを選択するには、『Oracle Identity Management ユーザー・リファレンス』における Oracle Identity Management の LDAP の属性リファレンスに関する項で指示されている DSA 構成パラメータ `orclpkimatchingrule` を編集します。（認証の場合、`orclpkimatchingrule` の値 3 または 4 が値 2 に等しくなります）。

注意 :

- 10*g*（10.1.4.0.1）に証明書のハッシュ値を導入する場合は、ユーザー証明書を旧リリースからアップグレードする必要があります。証明書をアップグレードする方法については、『Oracle Identity Management ユーザー・リファレンス』の `upgradecert.pl` コマンドライン・ツールのリファレンスを参照してください。
- バイナリ属性 `usercertificate` を検索できます。検索方法については、付録 G「ディレクトリでのユーザー証明書の検索」を参照してください。

関連資料 :

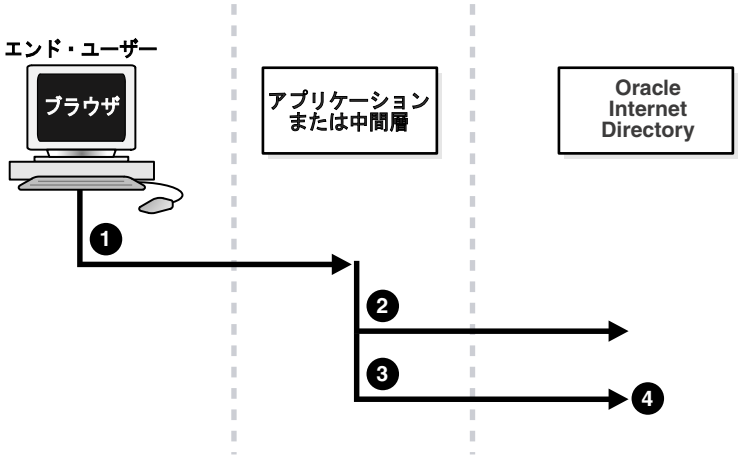
- 16-8 ページの Simple Authentication and Security Layer（SASL）を使用した認証
- `http://www.ietf.org` にある Internet Engineering Task Force（IETF）の Web サイトで、RFC 2829（LDAP バージョン 3 サーバーで必要な認証メカニズムとしての SASL MD5 ダイジェストを指定）、RFC 2831（MD5 ダイジェストメカニズムの説明）、RFC 2617（SASL MD5 ダイジェストがベースとしている HTTP Digest 認証メカニズムの説明）の各 RFC を参照してください。

間接認証

間接認証は、ディレクトリに資格証明を保持するエンティティ（Oracle Internet Directory セルフ・サービス・コンソールのようなアプリケーション、ファイアウォールや RADIUS サーバーのような中間層など）を介して発生します。アプリケーションや中間層は、**プロキシ・ユーザー**となります。プロキシ・ユーザーは、エンド・ユーザーの代理となる権限を持ち、そのユーザーが権限を持つ操作をユーザーにかわって実行します。

次の図 16-1 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 16-1 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. ディレクトリ・サーバーは、アプリケーションまたは中間層がエンド・ユーザーの ID に切り替えようとしているものとして、この 2 回目のバインドを認識します。ディレクトリ・サーバーは、アプリケーションまたは中間層によってエンド・ユーザーに付与された認証を受け入れます。ただし、アプリケーションまたは中間層に、このユーザーのプロキシとなる権限があるかどうかを検証する必要があります。ディレクトリ・サーバーは、エンド・ユーザーのエントリを管理する ACP によって、このエンド・ユーザーに対するプロキシ権限がこのアプリケーションまたは中間層に付与されているかどうかをチェックします。
   - エンド・ユーザーのエントリにより、アプリケーションまたは中間層に必要なプロキシ権限が提供された場合、ディレクトリ・サーバーは、認可識別情報をエンド・ユーザーの認可識別情報に変更します。後続するすべての操作は、そのエンド・ユーザーがサーバーに直接接続して直接認証された場合と同様に行われます。
   - エンド・ユーザーのエントリが、アプリケーションまたは中間層に必要なプロキシ権限を提供しない場合、ディレクトリ・サーバーは、「アクセス権限が不十分です。」というエラー・メッセージを返します。

     関連項目： 18-9 ページの「操作 : 付与するアクセス権の種類」

ディレクトリ・サーバーは同一セッションで、その他のエンド・ユーザーを認証および許可できます。また、セッションをエンド・ユーザーから、そのセッションをオープンしたアプリケーションまたは中間層に切り替えることもできます。

セッションをクローズするには、アプリケーションまたは中間層がバインド解除リクエストをディレクトリ・サーバーに送信します。

たとえば、次の場合を想定します。

- `cn=User1` でディレクトリにバインドする中間層には、ディレクトリ全体に対するプロキシ・アクセス権限があります。
- `cn=User2` でディレクトリにバインドできるエンド・ユーザーがいます。

このエンド・ユーザーが、ディレクトリに対する問合せが含まれている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。ディレクトリ・サーバーは、`cn=user1` にプロキシ・アクセス権限があることを確認した後、この 2 回目のバインドの実行を許可します。パスワードなど、エンド・ユーザー識別名の妥当性をさらに要求することはありません。このセッションでは、これ以降すべての LDAP 操作は、`cn=User2` が実行しているかのようにアクセス制御されます。

あるユーザーがアプリケーションからサービスを受け、続いて別のユーザーが同じアプリケーションのサービスを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、まだサービスを受けている先行ユーザーがいない場合は、新しい接続を確立することなく、既存の確立済接続を何度も使用できます。

外部認証

多くの企業では、ユーザー・セキュリティ資格証明を Oracle Internet Directory 以外のリポジトリ（データベースや他の LDAP ディレクトリなど）に格納しています。Oracle Internet Directory の外部認証プラグインとパスワード変更プラグインにより、ユーザー認証用のこれらの資格証明を Oracle コンポーネントに対して使用できます。資格証明を Oracle Internet Directory に格納する必要はなく、常に同期化させる必要はありません。

関連項目： 第 34 章「カスタマイズされた外部認証プラグインの設定」

ディレクトリ認証用ユーザー・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： 第 20 章「パスワード・ベリファイアのディレクトリ格納」

Oracle Internet Directory のパスワード・ポリシー

パスワード・ポリシーとは、パスワードの使用方法を定めた一連の規則のことです。ユーザーがディレクトリへのバインドを試みると、ディレクトリ・サーバーは、ユーザーのパスワードがパスワード・ポリシーの様々な要件に適合するかを確認します。

パスワード・ポリシーを確立する際は、次のような規則を設定します。なお、この規則はほんの一部です。

- 指定されたパスワードの有効期限
- パスワードの最小必須文字数
- パスワードに必要な数字の文字数

> **関連項目：** パスワード・ポリシーの確立で設定する規則の詳細は、第 19 章「Oracle Internet Directory のパスワード・ポリシー」を参照してください。

Simple Authentication and Security Layer（SASL）を使用した認証

16-4 ページの「直接認証」の項では、Oracle Internet Directory 環境での SASL の使用について説明しました。この項では、SASL の動作について詳細に説明します。この項の項目は次のとおりです。

- SASL 対応クライアントが MD5 ダイジェストを使用してディレクトリ・サーバーに対して認証する方法
- SASL 対応クライアントが外部認証を使用してディレクトリ・サーバーに対して認証する方法

SASL 対応クライアントが MD5 ダイジェストを使用してディレクトリ・サーバーに対して認証する方法

SASL 対応クライアントがサーバーに対して MD5 ダイジェスト認証を求める場合、その認証プロセスは次のとおりです。

1. ディレクトリ・サーバーは、サポートする各種 MD5 ダイジェスト認証オプションと特別なトークンを含むダイジェスト・チャレンジを LDAP クライアントに送信します。
2. クライアントは、認証オプションを選択し、選択したオプションを示すダイジェスト・レスポンスをサーバーに送信します。このレスポンスには、セキュアなトークンとクライアント資格証明が暗号化されて含まれます。このようして、サーバーに対するクライアントの認証を実行できます。
3. ディレクトリ・サーバーは、レスポンスのクライアント資格証明を復号化し、検証します。

SASL 対応クライアントが外部認証を使用してディレクトリ・サーバーに対して認証する方法

Oracle Internet Directory では、クライアントおよびサーバーの両方が相互に証明書を提供して認証する SSL 接続を介して SASL 外部認証を提供します。識別名は、SSL ネットワーク・ネゴシエーションで使用されたクライアント証明書から作成されます。

クライアントが、SSL のような外部認証メカニズムを使用してディレクトリ・サーバーに認証を求める場合、その認証プロセスは次のとおりです。

1. クライアントは、認可識別情報の入った初期メッセージを送信します。
2. ディレクトリ・サーバーは、SASL の外部にある情報を使用して、クライアントが認可識別情報として正当に認証できるかどうかを判断します。クライアントを確実に認証できた場合、ディレクトリ・サーバーは認証情報の交換が無事完了したことを示します。そうでない場合、ディレクトリ・サーバーは失敗を示します。

外部情報は、IPsec や SSL/TLS などのシステムにより提供されます。認可識別情報は、次のようにして得られます。

- 完全一致の場合は、外部認証を提供するシステムのクライアント認証資格証明（クライアント SSL 証明書など）から認可識別情報が作成されます。
- クライアントが認可識別情報として空の文字列を送信した場合、認可識別情報は外部認証を提供するシステムのクライアント認証資格証明（SSL 証明書など）から作成されます。

17

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。

この章の項目は次のとおりです。

> **関連項目：** Oracle Internet Directory に関連する SSL の概念の概要は、3-17 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暗号スイート

暗号スイートは、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 つのノード間で通信条件の情報交換を行い、メッセージを送受信するときに使用する暗号スイートを確認します。

表 17-1 に、Oracle Internet Directory でサポートされる SSL 暗号スイートと、各暗号スイートに対応する認証、暗号化およびデータ整合性のアルゴリズムを示します。

表 17-1 Oracle Internet Directory でサポートされている SSL 暗号スイート

暗号スイート	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。

10*g*（10.1.4.0.1）での SSL の使用制限事項

Oracle Internet Directory 10*g*（10.1.4.0.1）の場合、Oracle ディレクトリ・レプリケーション・サーバーは、双方向（相互）認証をサポートする SSL 対応の LDAP サーバーと直接通信できません。LDAP サーバーが SSL 相互認証用に構成されていると、レプリケーション・サーバーの起動は失敗し、停止します。

関連項目： サーバー・インスタンスの構成方法は、第 7 章「Oracle ディレクトリ・サーバーの管理」を参照してください。

SSL を使用した Oracle Internet Directory の構成とテスト

Oracle Wallet Manager を使用して、SSL 対応の Oracle Internet Directory を構成します。接続をテストするには、コマンドラインまたは Oracle Directory Manager を使用します。

注意： デフォルトでは、構成設定 0 に定義されている SSL ポートが、認証モード 1（暗号化のみ）に設定されます。1 以外の認証モードで構成設定 0 の SSL ポートを構成しないでください。1 以外の認証モードで構成すると、暗号化された SSL ポートで Oracle Internet Directory と通信することを想定している Oracle Delegated Administration Services とその他のアプリケーションに障害が発生します。

この項の項目は次のとおりです。

- SSL パラメータの構成
- SSL 対応の Oracle Internet Directory の構成
- コマンドラインによる SSL 接続のテスト
- Oracle Directory Manager を使用した SSL のテスト

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 パラメータを確認し、場合によっては再構成する必要があります。

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 有効化」パラメータを 1（デフォルトの保護ポートは 3031）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 有効化」を 2（デフォルトの非保護ポートは 3060）に設定します。

管理者は、異なる値を持つ複数の構成パラメータのセットを作成および変更し、Oracle Internet Directory のインスタンスごとに異なる構成設定エントリを使用できます。これは、セキュリティ要件の異なるクライアントを制御する便利な方法です。

SSL の値を変更するときは、デフォルトの構成設定にある SSL の値を変更するのではなく、別の構成設定を作成して、その SSL の値を変更する方法をお薦めします。デフォルトの構成設定は、技術的な問題を診断するときに Oracle サポート・サービスから要求される場合があります。

この項の項目は次のとおりです。

- Oracle Directory Manager を使用した SSL パラメータの構成
- コマンドライン・ツールを使用した SSL パラメータの構成

関連資料：

- これらのパラメータの設定方法は、7-2 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。
- Oracle Internet Directory これらのパラメータの説明は、『Oracle Identity Management ユーザー・リファレンス』の、OID 構成のスキーマ要素に関する項を参照してください。

Oracle Directory Manager を使用した SSL パラメータの構成

作成した各構成設定エントリおよび現在実行中の各サーバー・インスタンスの SSL 構成パラメータの値を、確認および変更できます。

> **注意：** アクティブ・インスタンスのパラメータを直接変更することはできません。アクティブ・インスタンスのパラメータを変更する場合は、構成設定エントリ内のパラメータを変更して、それを保存してください。保存後は、現行のインスタンスを停止して、サーバーの起動メッセージ内にある新しく変更された構成設定を参照できます。

SSL 構成パラメータの表示と変更 SSL 構成パラメータを表示および変更する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「**< ディレクトリ・サーバー・インスタンス >**」、「**サーバー管理**」の順に展開します。
2. 必要に応じて「**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のタブ・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、各フィールドを修正して変更内容を保存します。フィールドについては、A-33 ページの表 A-47 を参照してください。

> **関連資料：** 構成設定エントリのパラメータの変更方法は、7-3 ページの「Oracle Directory Manager を使用したサーバーの構成設定エントリの管理」を参照してください。

コマンドライン・ツールを使用した SSL パラメータの構成

コマンドラインから SSL パラメータを構成する方法は、次の項目を参照してください。

- 7-6 ページの「コマンドライン・ツールを使用したサーバー構成設定エントリの管理」
- `ldapadd` や関連コマンドで、`-p` フラグ、`-U` フラグおよび `-W` フラグを使用して SSL を構成する方法の詳細は、『Oracle Identity Management ユーザー・リファレンス』の Oracle Internet Directory サーバー管理ツールに関する項を参照してください。

SSL 対応の Oracle Internet Directory の構成

SSL 対応のサーバー側 LDAP サーバーを構成するには、次の手順を実行します。

1. Oracle Wallet Manager を起動します。

   UNIX では、DISPLAY 環境変数を設定して次のように入力します。

   ```
   owm
   ```

   Windows では、次のいずれかの方法でプログラムを起動します。

   - 「**スタート**」→「**プログラム**」→「**ORACLE_HOME**」→「**Network Administration**」→「**Wallet Manager**」を選択します。
   - 「**スタート**」→「**プログラム**」→「**ORACLE_HOME**」→「**Integrated Management Tools**」→「**Wallet Manager**」を選択します。
2. 上部メニュー・バーの「**ウォレット**」を選択し、「**新規**」を選択します。

   パスワードを選択および確認します。
3. 空の Wallet が新規作成されます。

   「**はい**」を選択して証明書リクエストを作成します。
4. 必要な情報を入力します。

関連資料： 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。

5. 「**OK**」を選択します。

   Oracle Wallet Manager のダイアログ・ボックスに、証明書リクエストが正常に作成されたことが表示されます。このダイアログ・パネルの内容から証明書リクエストのテキストをコピーして電子メール・メッセージに貼り付け、認証局に送付できます。または、証明書リクエストをファイルにエクスポートできます。

6. メニュー・バーで「**操作**」→「**証明書リクエストのエクスポート**」を選択します。

   「証明書リクエストのエクスポート」ダイアログ・ボックスが表示されます。

7. 証明書リクエストのファイル名（`usercert.req` など）を入力します。

8. Wallet を保存します。

   注意： Windows 2000 で Wallet を保存する場合、スペースを含まないディレクトリ・パスを選択してください。Wallet は、デフォルト位置である *Documents and Settings¥oracle¥wallets* に格納しないでください。

9. 新規作成した証明書リクエストを認証局に送信します。

   関連資料：

   - 『Oracle Application Server Certificate Authority 管理者ガイド』
   - Oracle MetaLink（`http://metalink.oracle.com`）の MetaLink ノート : 178806.1: 「How to get SSL certificates from a Microsoft Certification Services CA」

   Microsoft 証明サービス認証局の証明書の詳細は、これらの資料を参照してください。

10. 認証局からユーザー証明書と（必要に応じて）信頼できる証明書を入手する必要があります。認証局が Oracle Wallet Manager のデフォルトのリストにない場合は、ユーザー証明書をインポートする前に、認証局の信頼できる証明書をインポートする必要があります。

    a. 信頼できる証明書をインポートするには、メニュー・バーで「**操作**」→「**信頼できる証明書のインポート**」を選択します。「**信頼できる証明書のインポート**」ダイアログ・パネルが表示されます。BASE64 形式の証明書を貼り付けるか、信頼できる証明書を含むファイルを選択するかを決定します。新規の認証局が、「信頼できる証明書」のリストに表示されます。

    b. ユーザー証明書をインポートするには、メニュー・バーで「**操作**」→「**信頼できる証明書のインポート**」を選択します。「**証明書のインポート**」ダイアログ・ボックスが表示されます。BASE64 形式の証明書を貼り付けるか、信頼できる証明書を含むファイルを選択するかを決定します。

11. 「**ウォレット**」を選択し、「**ウォレット**」→「**保存**」を選択して Wallet を保存します。メニュー・バーの「**ウォレット**」を選択し、「**自動ログイン**」メニュー項目の横のチェック・ボックスを選択して、自動ログインを有効にします。ウィンドウの下部に、**「自動ログインは使用可能」**というメッセージが表示されます。Wallet ディレクトリに、cwallet.sso というファイルが格納されます。

    注意： Oracle Internet Directory リリース 9.0.2 の時点では、cwallet.sso などの暗号化形式の Wallet のみがサポートされます。そのため、SSL インスタンスを起動する前に、Oracle Wallet Manager を使用して Wallet を開き、自動ログインを有効にする必要があります。

12. Oracle Directory Manager を開き、「**構成設定**」の新規追加を選択します。「**デフォルト構成設定**」は変更しないでください。

    「**SSL 設定**」タブを選択し、Wallet の位置を入力します。UNIX の場合、URL の書式は次のとおりです。

    `file://path/directory_of_wallet`

    たとえば、次のようになります。

    `file://etc/ORACLE/WALLET`

    Windows の場合、URL の書式は次のとおりです。

    `file:¥device:¥path¥wallet_directory`

    たとえば、次のようになります。

    `file:d:¥wallet`

    SSL 認証方式を選択し、SSL ポートを構成します。認証方式は、次のとおりです。

SSL 認証方式	認証動作
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。SSL 暗号化および復号化のみが使用されます。
SSL サーバー認証	ディレクトリ・サーバーが、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 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、それぞれ相手側に証明書を送信します。

    該当するリリースの SSL インスタンス用ポートを選択します。

    関連項目： 第 6 章「Oracle Internet Directory のプロセス制御コンポーネント」

13. この段階で、デフォルトの SSL ポートとデフォルトの非 SSL ポートを使用する `DefaultConfigset`、デフォルトの `Configset1`、および一意の SSL ポートと一意の非 SSL ポートを使用する新規の `Configset2` という 3 つの構成設定が存在します。

    Windows システムでは、追加の構成手順を実行する必要があります。Oracle Directory Service のログイン・アカウントを、ローカル・システム・アカウントから Wallet を所有するユーザーのアカウントに変更します。このユーザーは、`Administrator Group` のメンバーである必要があります。次の手順に従ってアカウントを変更します。

    a. Windows で、「**スタート**」→「**設定**」→「**コントロール パネル**」→「**管理ツール**」→「**サービス**」を選択します。

    b. 「**プロパティ**」→「**ログオン**」をクリックします。

    c. ローカル・システム・アカウントから、Wallet 作成時に使用したログイン・アカウントに変更します。サービスを停止して、再起動します。

14. 暗号化モードの SSL を必要とする Oracle Delegated Administration Services とその他のアプリケーションが正常に稼働するように、Oracle Internet Directory インスタンスを開始します。

    a. ブラウザを開いて Oracle Enterprise Manager の Web サイトに移動し、Oracle Internet Directory プロセスまでドリルダウンします。このページには、稼働中のプロセスが表示されます。

    b. 「**新規インスタンスの起動**」ボタンをクリックします。新規構成設定がリストに表示されます。

    c. 開始する「**設定番号**」を選択し、「**起動**」をクリックします。

d. インスタンスが開始されたら、「**OK**」をクリックします。Oracle Internet Directory インスタンスのページが表示されます。新規インスタンスが起動済としてリストに表示されます。

この時点から

```
opmnctl startall
opmnctl stopall
```

という標準コマンドを使用して、Oracle Internet Directory インスタンスを自動的に管理できます。

15. これで、Oracle Internet Directory が実行され、4 つのポートでのリスニングが開始されました。

UNIX システムでは、`$ORACLE_HOME/ldap/bin/ldapcheck` コマンドを実行することで、`oidldapd` ディスパッチャとサーバー・プロセスを追加表示できます。SSL インスタンスのデバッグ・ログは、それぞれ `oidldapd02.log` と `oidldapd02s`*`XXXXX`*`.log` です。

コマンドラインによる SSL 接続のテスト

`ldapbind` コマンドを使用して、SSL 接続をテストできます。UNIX での構文は、次のとおりです。

```
ldapbind -D cn=orcladmin -w welcome -U authentication_mode -h host -p SSL_port \
-W "file://DIRECTORY_CONTAINING_WALLET" -P wallet_password
```

Windows での構文は、次のとおりです。

```
ldapbind -D cn=orcladmin -w welcome -U authentication_mode -h host -p SSL_port ¥
-W "file:device:¥DIRECTORY_CONTAINING_WALLET" -P wallet_password
```

ここで、*authentication_mode* は、次のいずれかです。

数値	認証
1	SSL 認証を必要としません。
2	一方向（サーバーのみ）の SSL 認証を必要とします。
3	双方向（クライアントとサーバー）の SSL 認証を必要とします。

関連資料：『Oracle Identity Management ユーザー・リファレンス』の `ldapbind` コマンドライン・ツールのリファレンス

暗号化のみの SSL のテスト

SSL 認証を必要としない SSL 構成をテストするには、この方法を使用します。構文は次のとおりです。

```
ldapbind -D cn=orcladmin -w password -U 1 -h host -p SSL_Port
```

サーバー認証を必要とする SSL のテスト

SSL サーバー認証の設定された SSL 構成をテストするには、この方法を使用します。クライアントがサーバー認証をリクエストするかどうかは、任意に選択できます。

サーバー認証を使用した匿名バインド用の構文は、次のとおりです。

```
ldapbind -U 2 -h host -p port -W "file:DIRECTORY_CONTAINING_WALLET" \
-P wallet_password
```

ユーザー `cn=orcladmin` とサーバー認証を使用したバインド用の構文は、次のとおりです。

```
ldapbind -D cn=orcladmin -w password -U 2 -h host -p port \
-W "file:DIRECTORY_CONTAINING_WALLET" -P wallet_password
```

SSL 認証を使用しないバインド用の構文は、次のとおりです。

```
ldapbind -D cn=orcladmin -w password -U 1 -h host -p SSL_Port
```

クライアントおよびサーバー認証を必要とする SSL のテスト

SSL クライアントおよびサーバー認証の設定された SSL 構成をテストするには、この方法を使用します。

Oracle Internet Directory 10*g*（10.1.4.0.1）の時点で、Oracle Internet Directory では、証明書の一致規則がサポートされます。`ldapbind` コマンドラインで渡される識別名とパスワードは、無視されます。認証に使用されるのは、証明書または証明書ハッシュの識別名のみです。

関連項目： 16-4 ページの「直接認証」

ユーザー `cn=orcladmin` を使用したバインド用の構文は、次のとおりです。

```
ldapbind -D cn=orcladmin -w password> -U 3 -p port \
-W "file:DIRECTORY_CONTAINING_WALLET" -P wallet_password
```

または

```
ldapbind -D cn=orcladmin -w password -U 2 -h host -p port \
-W "file:DIRECTORY_CONTAINING_WALLET" -P wallet_password
```

クライアント証明書のバインド識別名（DN）を使用するための構文は、次のとおりです。

```
ldapbind -U 3 -h host -p port -W "file:DIRECTORY_CONTAINING_WALLET" \
-P wallet_password
```

または

```
ldapbind -U 2 -h host -p port -W "file:DIRECTORY_CONTAINING_WALLET" \
-P wallet_password
```

Oracle Directory Manager を使用した SSL のテスト

Oracle Directory Manager との SSL 接続をテストするには、次の手順を実行します。

1. Oracle Directory Manager を起動します。

   ログイン画面で、ネットワーク・アイコンをクリックし、新規 SSL インスタンスを追加します。

   構成した SSL インスタンスのホスト名とポート番号を選択します。

2. 「**使用可能**」という表示を確認します。インスタンスをハイライトして「**選択**」をクリックします。

3. 「**SSL**」タブをクリックし、ユーザーおよびパスワードの Wallet 位置を入力します。Windows では、SSL 位置を次のように指定します。

   ```
   file:device:¥wallet_directory_path
   ```

   UNIX では、SSL 位置を次のように指定します。

   ```
   file://wallet_directory_path
   ```

   「**SSL パスワード**」に、Wallet パスワードを指定します。

   「**SSL 認証レベル**」に、構成した認証レベルを指定します。

4. 「**資格証明**」タブをクリックします。「SSL」チェック・ボックスが選択されていることを確認します。この手順を省略すると、Oracle Directory Manager が停止する可能性があります。

5. 「**ユーザー**」および「**パスワード**」の値を指定します。

その他のコンポーネントと SSL

インストールでは、Oracle Internet Directory は configset0 で起動され、デュアル・モードが指定されます。つまり、非 SSL 接続を使用して Oracle Internet Directory にアクセス可能なコンポーネントもあれば、SSL を使用してディレクトリに接続するコンポーネントもあります。デフォルトでは、Oracle Application Server コンポーネントは、Oracle Internet Directory との通信をこのデュアル・モード環境で実行するように構成されます。必要であれば、非 SSL モードを取り除き、中間層のすべてのインスタンスで SSL を使用するように変更できます。詳細は、『Oracle Application Server 管理者ガイド』の、Oracle Internet Directory でのデュアル・モードから SSL モードへの変更に関する項を参照してください。

エンタープライズ・ユーザー・セキュリティやカスタマ・アプリケーションでは、configset0 での構成とは異なる SSL チャネルが必要な場合があります。たとえば、SSL サーバー認証モードや SSL 相互認証モードが必要な場合などです。その場合は、追加の SSL モード・ポートを別の構成設定に構成し、追加の Oracle Internet Directory LDAP インスタンスがそのポートでリスニングできるようにする必要があります。

注意： configset0 の SSL モードは絶対に変更しないでください。変更すると、一部の Oracle Application Server コンポーネントのデフォルト構成と競合する恐れがあります。新しい SSL 設定を作成するには、別の構成設定を使用してください。

エンタープライズ・ユーザー・セキュリティの SSL 構成の詳細は、『Oracle Database エンタープライズ・ユーザー管理者ガイド』のエンタープライズ・ユーザー・セキュリティの構成に関する項を参照してください。

例 :

1. SSL サーバー認証モードの構成設定

```
cn=configset2, cn=osdldapd, cn=subconfigsubentry
cn=configset2
objectclass=top
objectclass=orclConfigSet
objectclass=orclLDAPSubConfig
orclsslauthentication=32
orclsslenable=2
orclsslwalleturl=file:/ade/qdinh_newld/oracle/work/ldap/lrgsrg
orclsslport=6060
orclnonsslport=8019
orclserverprocs=1
```

2. SSL 相互認証モードの構成設定

```
cn=configset3, cn=osdldapd, cn=subconfigsubentry
cn=configset3
objectclass=top
objectclass=orclConfigSet
objectclass=orclLDAPSubConfig
orclsslauthentication=64
orclsslenable=2
orclsslwalleturl=file:/ade/qdinh_newld/oracle/work/ldap/lrgsrg
orclsslport=7001
orclnonsslport=8029
orclserverprocs=1
```

18

ディレクトリ・アクセス制御

この章では、アクセス制御ポリシーの概要、および Oracle Directory Manager またはコマンドライン・ツール ldapmodify を使用してディレクトリのアクセス制御を管理する方法について説明します。

注意： Oracle Internet Directory 10*g*（10.1.4.0.1）では、スーパーユーザーも他のユーザーと同様にアクセス制御ポリシーの適用対象になりました。スーパーユーザーを制限するための新しい ACL 構文の変更は、Oracle Directory Manager からは管理できません。

この章で説明するアクセス制御ポリシーを使用すると、レルム全体を対象に大まかな権限の委任が可能です。より細かい委任が必要な場合は、Oracle Access Manager を使用する必要があります。

関連資料：『Oracle Access Manager アクセス管理ガイド』

この章の項目は次のとおりです。

関連項目：

- アクセス制御ポリシーの実装と管理を開始する前に理解しておく必要がある概要については、3-17 ページの「セキュリティ」および第 16 章「ディレクトリ・セキュリティの概念」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 C「アクセス制御ディレクティブ書式」を参照してください。

アクセス制御ポリシーの管理の概要

アクセス制御ポリシーは、対応するエントリ内の **ACI** 属性の値を構成して管理します。そのためには、Oracle Directory Manager または ldapmodify のいずれかを使用します。

この項の項目は次のとおりです。

- 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： 18-10 ページの「ACL 評価の動作」

規定のアクセス制御のための orclACI 属性

`orclACI` 属性には、規定の**アクセス制御リスト**・ディレクティブが含まれています。つまりこのディレクティブは、この属性が定義されている ACP より下位のサブツリー内にあるすべてのエントリに適用されます。ディレクトリ内のあらゆるエントリに、この属性の値を含めることができます。この属性自体へのアクセスは、他の属性に対するアクセスと同様に制御されます。

注意： 単一のエントリ固有の ACL ディレクティブを `orclACI` 属性で示すことができます。ただし、その場合には、「エントリ・レベルのアクセス制御のための orclEntryLevelACI 属性」で説明する、管理が容易でパフォーマンス上のメリットもある `orclEntryLevelACI` の使用をお薦めします。これは、`orclACI` を介して示されるディレクティブの数によって LDAP 操作のオーバーヘッドが増加するためです。エントリ固有のディレクティブを `orclACI` から `orclEntryLevelACI` に移動すると、このオーバーヘッドを削減できます。

エントリ・レベルのアクセス制御のための orclEntryLevelACI 属性

あるポリシーが特定のエンティティ（例 : 特別のユーザー）のみに関係するとき、そのエンティティのエントリ内で ACL ディレクティブをメンテナンスできます。これは、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実行できます。この属性には、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 が抽象型オブジェクト・クラス top を拡張し、オプション属性として orclEntryLevelACI を組み込むためです。

orclEntryLevelACI 属性は複数値の属性で、構造は orclACI と類似しています。

> **関連項目：** orclEntryLevelACI 属性の構造の定義については、18-6 ページの「オブジェクト : アクセス権を付与するオブジェクト」を参照してください。

セキュリティ・グループ

Oracle Internet Directory 内のグループ・エントリは、groupOfNames オブジェクト・クラスまたは groupOfUniqueNames オブジェクト・クラスのいずれかと関連付けられます。グループ内のメンバーシップは、それぞれ member 属性または uniqueMember 属性の値として指定されます。

個人またはエンティティのグループにアクセス権を指定するには、セキュリティ・グループでそのグループを識別します。セキュリティ・グループには、ACP グループと権限グループの 2 つのタイプがあります。

ACP グループ 個人が ACP グループのメンバーである場合、ディレクトリ・サーバーは、その ACP グループに関連付けられている権限をその個人に単純に付与します。

ACP グループを使用して、ACP のレベルでアクセス権を解決します。たとえば、エントリを参照できるアクセス権を数百ものユーザーに付与すると仮定します。参照権限を各エントリに個別に付与することもできますが、この作業には相当な管理オーバーヘッドが必要となります。さらに、後日その権限の変更が決定した場合は、各エントリを個々に修正する必要があります。より効率的な解決策は、権限を集合的に割り当てることです。そのためには、グループ・エントリを作成して ACP グループとして指定し、必要な権限をそのグループに割り当てた後、ユーザーをそのグループのメンバーに割り当てます。その後、アクセス権を変更する場合は、個々のユーザーに対してではなく、グループに対して 1 箇所で変更を行います。同様に、権限を削除する場合は、多数の各エントリにアクセスするのではなく、グループから権限を削除することによって、複数のユーザーから権限を削除できます。

ACP グループは、orclacpgroup オブジェクト・クラスに関連付けられています。

権限グループ 権限グループは、上位レベルのアクセス・グループです。同様の権限を持つユーザーを管理する点では、ACP グループと類似しています。ただし、権限グループは、単一の ACP 以外に追加チェックを提供します。たとえば、ある ACP によってアクセスが制限される場合、ディレクトリ・サーバーは、アクセスを制限されるユーザーがいずれかの権限グループに属しているかどうかをユーザー・エントリの属性によって判断します。権限グループに属している場合、このユーザーには上位管理レベルで別途の権限があるため、ディレクトリ情報ツリーで上位管理レベルすべてがチェックされます。リクエスト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。ただし、下位 ACP の orclACI または orclEntryLevelACI 属性に、キーワード DenyGroupOverride が含まれている場合、上位レベルの ACP は下位 ACP を無視しません。DenyGroupOverride を使用すると、権限グループを使用してスーパーユーザーのアクセスを制限できます。

通常は、ACP グループのみを実装します。権限グループが提供する追加チェックは、パフォーマンスを低下させる可能性があります。下位レベルの標準的な制御よりも上位レベルのアクセス制御を優先させる権限が必要な場合にのみ、権限グループを使用します。

権限グループを使用して、ディレクトリ情報ツリーの下位 ACP では認識されない管理者に対して、アクセス権を付与します。たとえば、ホスティングされた環境のグローバル管理者が、レルムで操作を行う必要があると仮定します。グローバル管理者の識別情報はホスティングされ

た企業のレルムでは認識されないため、ディレクトリ・サーバーは、そのレルムの ACP のみに依存している場合、必要なアクセスを拒否します。ただし、グローバル管理者が権限グループのメンバーである場合、ディレクトリ・サーバーは、ディレクトリ情報ツリーの上位で、そのサブツリーへのアクセス権をこの権限グループに付与している ACP を検索します。アクセス権を付与している ACP が見つかった場合、ディレクトリ・サーバーは、ホスティングされた企業のレルムにある ACP による制限を無視します。

DenyGroupOverride キーワードを ACI に追加すると、権限が付与されたグループのメンバーに対してアクセスを拒否できます。

権限グループは、orclPrivilegeGroup オブジェクト・クラスに関連付けられています。

両方のタイプのグループに属するユーザー ユーザーが ACP グループと権限グループの両方のメンバーの場合、ディレクトリ・サーバーは、各タイプのグループについて評価を行います。ディレクトリ・サーバーは、ディレクトリ情報ツリーで上位の ACP に注目して、権限グループのアクセス権を解決します。

概要 : グループへのアクセス権の付与 アクセス権をユーザーのグループに付与する手順は、次のとおりです。

1. 通常の方法でグループ・エントリを作成します。
2. グループ・エントリを orclPrivilegeGroup オブジェクト・クラスまたは orclACPgroup オブジェクト・クラスに関連付けます。
3. そのグループのアクセス・ポリシーを指定します。
4. メンバーをグループに割り当てます。

ディレクトリ・サーバーによるセキュリティ・グループ・メンバーシップの算出方法 エントリは、グループの直接のメンバーとなるか、またはグループをネストして権限グループの一群を形成し、他の ACP または権限グループの間接のメンバーとなることができます。与えられたレベルで指定されているアクセス・ポリシーは、そのレベル以下のすべてのメンバーに直接的または間接的に適用されます。

Oracle Internet Directory は、セキュリティ・グループのみをアクセス制御目的で評価するため、その他のタイプのグループに対してアクセス・ポリシーを設定できません。ユーザーが特定の識別名とバインドされると、Oracle Internet Directory は、セキュリティ・グループ内でそのユーザーの直接のメンバーシップを算出します。指定した識別名の第 1 レベルのグループを認識すると、Oracle Internet Directory は、この第 1 レベルのグループすべての、他のセキュリティ・グループへのネストを算出します。この処理は、評価対象のネストされたグループがなくなるまで行われます。

各セキュリティ・グループ（ネストされているかどうかに関係なく）は、セキュリティ・グループのオブジェクト・クラス（orclACPgroup または orclPrivilegeGroup）に関連付けられている必要があります。グループがセキュリティ・グループのメンバーの場合でも、セキュリティ・グループのオブジェクト・クラスに関連付けられていないかぎり、ディレクトリ・サーバーではアクセス制御目的のグループとはみなされません。セキュリティ・グループ内でユーザーのメンバーシップが判断された場合、ディレクトリ・サーバーでは、セッションの存続期間にわたってその情報を使用します。

例 : セキュリティ・グループ・メンバーシップの算出 たとえば、表 18-1 のエントリのサンプル・グループを仮定します。group 4 以外は、それぞれ権限グループ（objectclass:orclprivilegegroup）として指定されています。管理者は、group1、group2 および group3 のメンバーに適用されるアクセス制御ポリシーを設定できます。

表 18-1 サンプル・セキュリティ・グループ

グループ	entry
group 1	dn: cn=group1,c=us cn: group1 objectclass: top objectclass: groupofUniqueNames objectclass: orclPrivilegeGroup uniquemember: cn=mary smith,c=us uniquemember: cn=bill smith,c=us uniquemember: cn=john 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 uniquemember: cn=john smith,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 には、次のネストされたグループが含まれています。

- cn=group2,c=us
- cn=group1,c=us
- cn=group4,c=us

group3 のアクセス制御ポリシーは、group3、group1 および group2 のメンバーに適用されます。これは、各グループが権限グループとして指定されているためです。この同じアクセス制御ポリシーは、group4 のメンバーには適用されません。これは、group4 は権限グループとして指定されていないためです。

たとえば、ユーザーが識別名 cn=john smith,c=uk で group4 のメンバーとして Oracle Internet Directory にバインドされている場合を考えてみます。group3 のメンバーに適用されるアクセス・ポリシーがこのユーザーに適用されることはありません。これは、このユーザーの唯一の直接メンバーシップが非権限グループに対するものであるためです。これに対して、ユーザーが cn=john smith,c=us、つまり、group1 と group2 のメンバーとしてバインドされている場合、そのアクセス権は group1、group2 および group3（group1 と group2 がネストされているため）のメンバーに対して設定されているアクセス・ポリシーで管理されます。こ

れは、この 3 つのグループすべてがオブジェクト・クラス orclPrivilegeGroup と関連付けられているためです。

> **関連項目：** グループ・エントリを変更して、orclPrivilegeGroup または orclACPgroup オブジェクト・クラスに対して関連付けまたは関連付け解除を行う方法については、8-6 ページの「Oracle Directory Manager を使用したエントリの変更」または 8-5 ページの「例 : Oracle Directory Manager を使用したユーザー・エントリの追加」を参照してください。

アクセス制御情報アイテム（ACI）のコンポーネント

ACI とは、様々なエンティティまたはサブジェクト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（サブジェクト）
- 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)
```

アクセス制御ディレクティブのオブジェクト部分には、特別なキーワードが含まれている場合があります。これらのツールは、次のとおりです。

- DenyGroupOverride（上位レベルの ACP によるアクセス権の無視を防止）
- AppendToAll（評価時に ACI のサブジェクトをその ACP 内の他のすべての ACI に追加）

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 C「アクセス制御ディレクティブ書式」を参照してください。

サブジェクト : アクセス権を付与する対象

この項では、次の項目について説明します。

- アクセス権が付与されるエンティティ
- バインド・モード（そのエンティティ識別情報の検証に使用される認証モード）
- オブジェクト追加制約（アクセス権を付与されたユーザーが、親の下に追加できるオブジェクトの種類の制限）

エンティティ アクセス権は、エントリではなくエンティティに対して付与されます。エンティティ・コンポーネントは、アクセス権が付与されているエンティティを指定します。

直接または間接的にエンティティを指定できます。

エンティティの直接指定 : この方法は、実際のエンティティ値の入力（たとえば、group=managers）を必要とします。次の要素を使用して値を入力します。

- 任意のエントリと一致するワイルド・カード文字（*）
- アクセス権によって保護されているエントリと一致するキーワード SELF
- ディレクトリで指定されている SuperUser 識別名と一致するキーワード SuperUser
- 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。

1. Anne の manager 属性の値を参照し、John Doe であることを確認します。
2. バインド識別名と manager 属性が一致することを確認します。
3. 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、サブジェクトが使用する認証と暗号化の方法を指定します。

認証には、次の 4 つのモードがあります。

- MD5 ダイジェスト
- PKCS12
- プロキシ
- 簡易 : パスワードベースの簡易認証

暗号化には、次の 3 つのオプションがあります。

- SASL
- SSL 認証なし
- SSL 一方向

暗号化モードの指定はオプションです。未指定の場合は、選択した認証モードが PKCS12 でないかぎり暗号化は使用されません。PKCS12 を使用して送信したデータは、すべて暗号化されます。

認証の選択肢には次のような優先順位規則があります。

匿名 < プロキシ < 簡易 <MD5 ダイジェスト <PKCS12

この規則は次のことを意味します。

- プロキシ認証は、匿名アクセスをブロックします。
- 簡易認証は、プロキシおよび匿名アクセスの両方をブロックします。
- MD5 ダイジェスト認証は、簡易、プロキシおよび匿名アクセスをブロックします。
- PKCS12 認証は、MD5 ダイジェスト、簡易、プロキシおよび匿名アクセスをブロックします。

バインド・モードの構文は次のとおりです。

```
BINDMODE =(LDAP_AUTHENTICATION_CHOICE + [ LDAP_ENCRYPTION_CHOICE ] )
LDAP_AUTHENTICATION_CHOICE = Proxy | Simple | MD5Digest | PKCS12
LDAP_ENCRYPTION_CHOICE = SSLNoAuth | SSLOneway | SASL
```

LDAP_ENCRYPTION_CHOICE パラメータはオプションです。未指定の場合、ディレクトリ・サーバーでは、暗号化は使用されないとみなされます。

オブジェクト追加制約 親エントリに追加アクセス権がある場合、階層内の下位エントリとしてオブジェクトを追加できます。オブジェクト追加制約は、*ldapfilter* を指定することによって、追加アクセス権を制限するために使用できます。

> **関連項目：** 付録 C「アクセス制御ディレクティブ書式」および
> 付録 B「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。

- None
- Compare/nocompare
- Search/nosearch
- Read/noread
- Selfwrite/noselfwrite
- Write/nowrite
- Add/noadd
- Proxy/noproxy
- Browse/nobrowse
- 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も注意してください。

表 18-2 アクセスのタイプ

アクセス・レベル	説明	オブジェクトのタイプ
Compare	属性値で比較操作を実行する権限。	属性
Read	属性値を読み取る権限。属性に対して読取り権限が与えられている場合でも、エントリ自体に参照権限がないかぎり値は返されません。	属性
Search	検索フィルタで属性を使用する権限。	属性
Selfwrite	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の変更を行う権限。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
Write	エントリの属性を変更 / 追加 / 削除する権限。	属性
None	アクセス権なし。サブジェクト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、サブジェクト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
Add	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
Proxy	別のユーザーの代理となる許可。	エントリ
Browse	検索結果で識別名を返すための権限。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
Delete	ターゲットのエントリを削除する権限。	エントリ

エントリ・レベルのアクセス・ディレクティブは、オブジェクト・コンポーネント内のキーワード `ENTRY` で識別されます。

注意： デフォルトのアクセス制御ポリシーでは、エントリおよび属性の両方を対象に、すべての人に、エントリ内のすべての属性の読取り、検索、書込みおよび比較の各アクセス権が付与されており、自己書込み権限は未指定です。エントリが未指定の場合、アクセス権は、そのアクセス権が指定されている直近の上位レベルで判断されます。

LDAP 操作のアクセス・レベル要件

表 18-3 に、LDAP 操作と、各操作の実行に必要なアクセス権を示します。

表 18-3 LDAP 操作および各操作の実行に必要なアクセス権

操作	必要なアクセス権
オブジェクトの作成	親エントリに対する追加アクセス権
変更	変更対象の属性に対する書込みアクセス権
識別名の変更	現行の親に対する削除アクセス権と新しい親に対する追加アクセス権
相対識別名の変更	ネーミング属性すなわち相対識別名属性に対する書込みアクセス権
オブジェクトの削除	削除対象のオブジェクトに対する削除アクセス権
比較	属性に対する比較アクセス権とエントリに対する参照アクセス権
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返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返される必要があるすべての属性について）

ACL 評価の動作

ユーザーが指定されたオブジェクトで操作を実行しようとすると、ディレクトリ・サーバーは、そのオブジェクト上で操作を実行するための適切なアクセス権がユーザーにあるかどうかを判断します。オブジェクトがエントリの場合、ディレクトリ・サーバーは、エントリおよびその各属性に対するアクセス権を系統的に評価します。

オブジェクト（エントリの属性も含む）へのアクセス権の評価は、そのオブジェクトの ACI ディレクティブすべての検証を必要とする場合があります。これは、ACP に階層的な特性があり、上位 ACP から従属 ACP にポリシーが継承されるためです。

ディレクトリ・サーバーは、最初にエントリ・レベル ACI（`orclEntryLevelACI`）の ACI ディレクティブを検証します。検証は最も近い ACP に進み、評価が完了するまで各上位 ACP を次々に検討します。

ACL の評価時には、属性は表 18-4 に示すいずれかの状態になります。

表 18-4 ACL 評価時の属性の状態

状態	説明
Resolved with permission	属性に対して要求されたアクセスは、ACI で付与されています。
否認による解決	属性に対して要求されたアクセスは、ACI で明示的に否認されています。
Unresolved	対象の属性に対して、適用可能な ACI がまだ見つかりません。

検索を除き、次の場合にはすべての操作の評価が停止します。

- エントリ自体に対するアクセス権が否認される
- 属性のいずれかが「否認による解決」の状態になる

この場合、操作は失敗し、ディレクトリ・サーバーはエラーをクライアントに返します。

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」の属性は返されません。

この項の項目は次のとおりです。

ACL の評価に使用される優先順位規則

LDAP の操作では、LDAP セッションの BindDN（つまりサブジェクト）に、そのオブジェクト（エントリ自体およびエントリの個々の属性を含む）で操作を実行するための特定の権限が必要です。

通常は、アクセス制御の管理認可レベルの階層があります。ネーミング・コンテキストのルートから、継承する管理ポイント（または ACP）までが 1 つの階層です。ACP は、`orclACI` 属性の定義済の値を持つあらゆるエントリです。また、単一のエントリ固有のアクセス情報をそのエントリ（`orclEntryLevelACI`）内で示すこともできます。

ACL の評価には、LDAP 操作の実行に必要な権限がサブジェクトにあるかどうかを判別する処理が含まれています。通常、`orclentryLevelACI` または `orclACI` には、ACL の評価に必要な情報がすべて含まれているわけではありません。したがって、評価が完全に解決されるまで、使用可能なすべての ACL 情報が、一定の順序で処理されます。

処理の順序は次の規則に従います。

- エントリ・レベルの ACI が最初に検証されます。`orclACI` の ACI は、そのターゲット・エントリに一番近い ACP から順に上位方向に検証されます。
- 必要な権限が判別された時点で、評価は停止します。それ以外は評価が継続されます。
- 単一の ACI 内では、セッションの識別名と関連付けられているエンティティが、by 句で識別される複数の項目と一致している場合、有効なアクセス権が次のように評価されます。
  - 一致する by 句の項目内で付与された全権限の UNION

    次の場合の AND 検索
  - 一致する by 句の項目内で否認された全権限の UNION

エントリ・レベルにおける優先順位

エントリ・レベルにおける ACI は、次の順序で評価されます。

1. フィルタを使用している場合。たとえば、次のようになります。

```
access to entry filter=(cn=p*)
by group1 (browse, add, delete)
```

2. フィルタを使用していない場合。たとえば、次のようになります。

```
access to entry
by group1 (browse, add, delete)
```

属性レベルにおける優先順位

属性レベルにおいては、属性が指定されている ACI が未指定の ACI よりも優先されます。

1. 属性が指定されている ACI は、次の順序で評価されます。
   a. フィルタを使用しているもの。たとえば、次のようになります。

      ```
      access to attr=(salary) filter=(salary > 10000)
      by group1 (read)
      ```

   b. フィルタを使用していないもの。たとえば、次のようになります。

      ```
      access to attr=(salary)
      by group1 (search, read)
      ```

2. 属性が未指定の ACI は、次の順序で評価されます。
   a. フィルタを使用している場合。たとえば、次のようになります。

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

   b. フィルタを使用していない場合。たとえば、次のようになります。

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

同一オブジェクトに対する複数 ACI の使用

Oracle Internet Directory では、オブジェクトの ACP 内に複数の ACI を定義できます。オブジェクトに関連付けられている各 ACI を処理して、内部 ACP キャッシュ内に単一 ACI として格納します。その後、ACP 内に指定された複数の ACI のすべての関連ポリシーを適用します。

この動作については、次の ACP の例を参照してください。

```
Access to entry by dn="cn=john" (browse,noadd,nodelete)
Access to entry by group="cn=admingroup" (browse,add,nodelete)
Access to entry by dn=".*,c=us" (browse,noadd,nodelete)
```

この ACP には、オブジェクト・エントリに対する 3 つの ACI があります。この ACP をロードする場合、Oracle Internet Directory は、内部 ACP キャッシュ内でこの 3 つの ACI を 1 つの ACI としてマージします。

ACI の構文は次のとおりです。

```
Access to OBJECT> by SUBJECT ACCESSLIST
OBJECT = [ entry | attr [EQ-OR-NEQ] ( * | ATTRLIST ) ]
[ filter = ( LDAFILTER ) ]
```

この構文は、次のオブジェクトのタイプを可能にします。

- entry
- entry + filter = （*LDAPFILTER*）
- attr =（*ATTRLIST*）
- attr =（*ATTRLIST*）+ filter =（*LDAPFILTER*）
- attr !=（*ATTRLIST*）
- attr !=（*ATTRLIST*）+ filter =（*LDAPFILTER*）
- attr =
- attr =（*）+ filter =（*LDAPFILTER*）

前述のすべてのオブジェクトのタイプに対して、複数の ACI を定義できます。ACP の初期ロード時に、ディレクトリ・サーバーは、定義されたオブジェクト・タイプに基づいて ACI をマージします。ACI 内のオブジェクト文字列が完全一致の文字列かどうかを比較することが、一致基準となります。

1 つの ACI で ATTR=(ATTRLIST) が指定され、別の ATTR!=(ATTRLIST) が指定されている場合、ATTR=(*) はエントリ内で ACI としては指定できません。また、ACI で ATTR=(ATTRLIST) が指定されている場合に、ATTRLIST にはない属性に対するアクセス権限を指定するには、ATTR!=(ATTRLIST) ではなく、ATTR=(*) を指定する必要があります。ATTR=(*) は、ATTRLIST で指定されている属性以外のすべての属性を示します。

注意： 同じ属性に対して同じフィルタを使用して複数の ACI を定義する場合、Oracle Internet Directory はそれらをマージし、実行時の構造として単一の ACI を作成します。

同じ属性に対して異なるフィルタを使用して複数の ACI を定義する場合、Oracle Internet Directory ではそれらを個別の ACI として処理します。このような場合、優先順位は決定的ではありません。

あいまいな動作を防ぐには、同じ属性に対して異なるフィルタを使用して複数の ACI を定義する場合、フィルタにより重複する結果が生じないようにしてください。

ディレクトリ・オブジェクトに対する排他的アクセス権

指定したオブジェクトに ACI が存在している場合は、そのオブジェクト以外のすべてのオブジェクトに対してアクセス権を指定できます。そのためには、アクセス権をすべてのオブジェクトに付与するか、または 1 つのオブジェクトに対するアクセス権を否認します。

次の例は、アクセス権をすべての属性に付与します。

```
access to attr=(*)
by group2 (read)
```

次の例は、userpassword 属性に対するアクセス権を否認します。

```
access to attr!=(userpassword)
by group2 (read)
```

グループの場合の ACL 評価

属性またはエントリ自体の操作が、ディレクトリ情報ツリー内の下位の ACP で明示的に否認されている場合、通常、ACL によるそのオブジェクトの評価は、否認による解決とみなされます。しかし、そのセッションのユーザー（bindDN）がグループ・オブジェクトのメンバーの場合、評価はまだ解決されていないかのように継続されます。グループのサブジェクト・セレクタを介して、ツリー内の上位の ACP でセッションのユーザーに権限が付与されている場合、この権限付与はディレクトリ情報ツリー内の下位での否認よりも優先されます。

この例は、上位レベルの ACP の ACL ポリシーが、ディレクトリ情報ツリー内の下位の ACP ポリシーよりも優先される唯一のケースです。

Oracle Directory Manager を使用したアクセス制御の管理

ACP 内のアクセス制御情報アイテム（ACI）は、Oracle Directory Manager またはコマンドライン・ツールを使用して表示および変更できます。この項では、Oracle Directory Manager でこれらのタスクを実行する方法について説明します。

注意： Oracle Internet Directory のインストール直後に、4-2 ページの「タスク 1: デフォルトのセキュリティ構成の再設定」の説明に従ってデフォルトのセキュリティ構成を必ずリセットしてください。

注意： Oracle Internet Directory 10*g*（10.1.4.0.1）では、スーパーユーザーも他のユーザーと同様にアクセス制御ポリシーの適用対象になりました。スーパーユーザーを制限するための新しい ACL 構文の変更は、Oracle Directory Manager からは管理できません。

この項の項目は次のとおりです。

- 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

関連資料： コマンドライン・ツールの説明は、『Oracle Identity Management ユーザー・リファレンス』の、Oracle Identity Management コマンドライン・ツールのリファレンスに関する項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・プリファレンス**」をクリックします。「ユーザー・プリファレンス」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」**
   - **「検索リクエストに基づく ACP のみ表示」**
5. 「**OK**」を選択します。
6. 変更内容を反映するには、Oracle Directory Manager を再起動します。

Oracle Directory Manager を使用する場合の ACP の検索の構成

Oracle Directory Manager では、ACP の検索に次の項目が指定できます。

- 検索のルート
- 取り出されるエントリの最大数
- 検索の制限時間
- 検索の深さ

ACP エントリの検索を構成する手順は、次のとおりです。

1. ナビゲータ・ペインで、「Oracle Internet Directory サーバー」を展開して、ディレクトリ・サーバー・インスタンスを選択します。
2. ツールバーの「**ユーザー・プリファレンス**」を選択します。「ユーザー・プリファレンス」ダイアログ・ボックスが表示されます。
3. 「**エントリ管理の構成**」タブを選択します。
4. 「**1 レベルのサブツリー・エントリの最大数**」のラベルが付いているフィールドに、ACP 検索で取得するエントリ数を入力します。
5. 「**最大の検索時間**」フィールドに、検索の最大時間を秒単位で入力します。
6. 「**OK**」を選択します。「注意」ウィンドウには、「ACP 管理の変更を表示するには、Oracle Directory Manager を再起動する必要があります。」というメッセージが表示されます。
7. 「注意」ウィンドウの「**OK**」を選択します。
8. 最新のアクセス制御管理のエントリを表示するには、Oracle Directory Manager を切断し、すぐに再接続します。

Oracle Directory Manager を使用した ACP の表示

18-14 ページの「Oracle Directory Manager の ACP の表示の構成」の説明に従って常に ACP を表示するように Oracle Directory Manager を構成した場合、ACP の位置を特定および表示する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」、「**アクセス制御管理**」の順に展開します。定義したすべての ACP は、いずれもナビゲータ・ペインの「アクセス制御管理」ノードの下に表示されます。
2. ナビゲータ・ペインで「**アクセス制御管理**」の下の ACP を選択すると、その情報が右側のペインに表示されます。「アクセス制御管理」ペインのフィールドの説明は、A-4 ページの表 A-3 を参照してください。

18-14 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 を見つけて表示する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」の順に展開し、「**エントリ管理**」を選択します。
2. ACP として指定したエントリの検索を実行します。検索結果が右側ペインの下半分の「**識別名**」ボックスに表示されます。
3. 「**識別名**」ボックスで、エントリをダブルクリックします。対応する「エントリ」ダイアログ・ボックスが表示されます。
4. この ACP のサブツリーのアクセス制御を表示するには、「**サブツリー・アクセス**」タブを選択します。

   この ACP のエントリ・レベルのアクセス制御を表示するには、「**ローカル・アクセス**」タブを選択します。

Oracle Directory Manager を使用した ACP の追加

ACP は、規定の、すなわち継承可能なアクセス制御情報アイテム（ACI）を含んだエントリです。この情報は、エントリ自体とその下位エントリすべてに影響を与えます。一般的に、サブツリー全体にわたる規模の大きいアクセス制御をブロードキャストする ACP を作成します。

Oracle Directory Manager を使用して ACP を追加するには、次の 3 つのタスクが必要です。

- タスク 1: ACP にするエントリの指定
- タスク 2: 構造型アクセス項目の構成（エントリに関係する ACI）
- タスク 3: コンテンツ・アクセス項目の構成（属性に関係する ACI）

タスク 1: ACP にするエントリの指定

1. 18-14 ページの「Oracle Directory Manager の ACP の表示の構成」の説明に従って常に ACP を表示するように Oracle Directory Manager を構成した場合は、次のように開始します。

   a. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」の順に展開します。

   b. 「**アクセス制御管理**」を選択し、手順 2 に進みます。

   18-14 ページの「Oracle Directory Manager の ACP の表示の構成」の説明に従って検索の結果としてのみ ACP を表示するように Oracle Directory Manager を構成した場合は、次のように開始します。

   a. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」、「**アクセス制御管理**」の順に展開します。

   b. ACP を常駐させるノードを選択します。構成された ACP が存在しない場合は、「DSE ルート」の下の ACP を選択できます。

2. ツールバーの「**作成**」ボタンを選択します。「新規アクセス制御ポイント」ダイアログ・ボックスが表示されます。

3. 「**エントリへのパス**」フィールドで、ACP に指定するエントリの識別名を入力します。また、識別名は、「**エントリへのパス**」フィールドの右側の「**参照**」を選択して検索することもできます。

タスク 2: 構造型アクセス項目の構成

1. 構造型アクセス項目（エントリに関係する ACI）を定義するには、「**構造型アクセス項目**」ウィンドウの下の「**作成**」を選択します。「構造型アクセス項目」ダイアログ・ボックスが表示されます。このダイアログ・ボックスには、「**エントリ・フィルタ**」、「**追加されたオブジェクト・フィルタ**」、「**責任者**」および「**アクセス権限**」の 4 つのタブがあります。

2. ACP では、定義されたアクセス権は、他のフィルタによりアクセスがそれ以上制限されないかぎり、このエントリおよびそのエントリのすべてのサブエントリに適用されます。

   ACP のすべての下位エントリを ACP で管理する場合は、「**エントリ・フィルタ**」タブ・ページには何も入力せず、次の手順に進みます。それ以外の場合は、この手順を実行します。

   適切な場合、「**エントリ・フィルタ**」タブ・ページを使用して、アクセスを指定するエントリを識別します。

   エントリへのアクセスを、このエントリの 1 つ以上の属性に基づいて制限できます。たとえば、役職名がマネージャで組織単位がアメリカであるすべてのエントリへのアクセスを制限できます。

   アクセスを指定するエントリを識別する手順は、次のとおりです。

   a. 検索基準バーの一番左のメニューから、属性タイプを選択します。

   b. バーの中央のメニューから、フィルタ・オプションのいずれかを選択します。これらのオプションの説明は、A-31 ページの表 A-45 を参照してください。

c. 検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。

3. 「**追加されたオブジェクト・フィルタ**」タブ・ページを選択します。

   ACI を指定して、ユーザーが追加できるエントリの種類を制限できます。たとえば、ユーザーが `objectclass=country` を持つエントリのみを追加できるように、DSE ルート・エントリで ACI を指定できます。その後、ディレクトリ・サーバーによって、新規エントリがこのフィルタの制限に適合するかどうかが検証されます。

   ユーザーが追加できるエントリの種類を制限する手順は、次のとおりです。

   a. 検索基準バーの一番左のメニューから、属性タイプを選択します。

   b. バーの中央のメニューから、フィルタ・オプションのいずれかを選択します。これらのオプションの説明は、A-31 ページの表 A-45 を参照してください。

   c. 検索基準バーの右のテキスト・ボックスに、選択した属性の値を入力します。

4. 「**責任者**」タブ・ページを選択します。

   a. 「**認証の選択**」リストから、サブジェクト（アクセス権を要求しているエンティティ）が使用する認証のタイプを選択します。オプションの説明は、A-4 ページの表 A-4 を参照してください。

      認証方式を選択しない場合は、どの種類の認証も受け入れられます。あるノードで指定されている認証方式は、通信先のノードで指定されている認証方式と一致している必要があります。

      「**暗号化の選択**」リストで、使用される暗号化のタイプを選択します。オプションの説明は、A-4 ページの表 A-5 を参照してください。

   b. アクセス権を付与するエンティティを指定します。オプションの説明は、A-4 ページの表 A-6 を参照してください。

5. 「**アクセス権限**」タブ・ページを選択します。

   付与する権限の種類を指定します。

   - **参照 :** サブジェクトにエントリの表示を許可します。
   - **追加 :** サブジェクトに、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 :** サブジェクトにエントリの削除を許可します。
   - **プロキシ :** サブジェクトに、別のユーザーの代理となることを許可します。

6. 「OK」をクリックします。

タスク 3: コンテンツ・アクセス項目の構成

1. コンテンツ・アクセス項目（属性に関係する ACI）を定義するには、「**コンテンツ・アクセス項目**」ウィンドウの下の「**作成**」を選択します。「コンテンツ・アクセス項目」ダイアログ・ボックスが表示されます。各タブ・ページには、変更可能な項目が含まれています。

2. ACP のすべての下位エントリを ACP で管理する場合は、「**エントリ・フィルタ**」タブ・ページには何も入力せず、手順 3 に進みます。それ以外の場合は、この手順を実行します。

   ACP では、アクセス権は、他のフィルタによりアクセスがそれ以上制限されないかぎり、このエントリおよびそのエントリのすべてのサブエントリに適用されます。適切な場合、「**エントリ・フィルタ**」タブ・ページを使用して、アクセスを指定するエントリを識別します。

   エントリへのアクセスを、このエントリの 1 つ以上の属性に基づいて制限できます。たとえば、役職名がマネージャで組織単位がアメリカであるすべてのエントリへのアクセスを制限できます。

アクセスを指定するエントリを識別する手順は、次のとおりです。

a. 検索基準バーの一番左のメニューから、属性タイプを選択します。

b. バーの中央のメニューから、フィルタ・オプションのいずれかを選択します。詳細は、A-31 ページの表 A-45 を参照してください。

c. 検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。

3. 「**責任者**」タブ・ページを選択します。

a. 「**認証の選択**」リストから、サブジェクト（アクセス権を要求しているエンティティ）が使用する認証のタイプを選択します。オプションの説明は、A-4 ページの表 A-4 を参照してください。

認証方式を選択しない場合は、どの種類の認証も受け入れられます。あるノードで指定されている認証方式は、通信先のノードで指定されている認証方式と一致している必要があります。

「**暗号化の選択**」リストで、使用される暗号化のタイプを選択します。オプションの説明は、A-4 ページの表 A-5 を参照してください。

b. アクセス権を付与するエンティティを指定します。オプションの説明は、A-4 ページの表 A-6 を参照してください。

4. 「**属性**」タブ・ページを選択します。

a. 右のメニューから、アクセス権を付与または否認する属性を選択します。

b. 左のメニューから、属性に対して実行する一致操作を選択します。選択肢は「EQ」（=）と「NEQ」（!=）です。

たとえば、「EQ」と「cn」を選択した場合は、付与したアクセス権が cn 属性に適用されます。「NEQ」と「cn」を選択した場合は、付与したアクセス権が cn 属性に適用されません。

5. 「**アクセス権限**」タブ・ページを選択して、権限を指定します。詳細は、A-5 ページの表 A-7 を参照してください。

6. 「**OK**」をクリックしてこのダイアログ・ボックスを閉じ、Oracle Directory Manager のメイン・ダイアログ・ボックスに戻ります。

Oracle Directory Manager の ACP 作成ウィザードを使用した ACP の追加

ACP 作成ウィザードを使用すると、ACP を追加するために必要なタスクを順に実行できます。次のタスクがあります。

- タスク 1: ACP にするエントリの指定
- 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
- タスク 3: ACP 作成ウィザードを使用したコンテンツ・アクセス項目の構成

タスク 1: ACP にするエントリの指定

1. 18-14 ページの「Oracle Directory Manager の ACP の表示の構成」の説明に従って常に ACP を表示するように Oracle Directory Manager を構成した場合は、次のように開始します。

   a. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」の順に展開します。

   b. ナビゲータ・ペインで「**アクセス制御管理**」を選択し、手順 2 に進みます。

   18-14 ページの「Oracle Directory Manager の ACP の表示の構成」の説明に従って検索の結果としてのみ ACP を表示するように Oracle Directory Manager を構成した場合は、次のように開始します。

   a. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」、「**アクセス制御管理**」の順に展開します。

   b. ナビゲータ・ペインで ACP を常駐させるノードを選択します。構成された ACP が存在しない場合は、「DSE ルート」の下の ACP を選択できます。

2. ツールバーの「**作成**」ボタンをクリックします。「新規アクセス制御ポイント」ダイアログ・ボックスが表示されます。

3. 「**エントリへのパス**」フィールドで、ACP に指定するエントリの識別名を入力します。「エントリ管理」の下のナビゲータ・ペインを探すか、または「参照」をクリックして、識別名を検索することもできます。

ACP では、アクセス権は、このエントリおよびそのエントリのすべてのサブエントリに適用されるか、または特定のエントリのみに適用されます。次に、両オプションでの ACP の構成方法を説明します。

タスク 2: ACP 作成ウィザードを使用した構造型アクセス項目の構成

1. 構造型アクセス項目（エントリに関係する ACI）を定義するには、「構造型アクセス項目」ウィンドウの下の「**ウィザードで作成**」をクリックします。最初の「構造型アクセス項目」ダイアログ・ボックスが表示されます。

2. 規範的な構造型アクセス項目を指定した場合は、ACP のすべての下位エントリをこの ACP が管理します。規範的な構造型アクセス項目を希望する場合は、この最初の「構造型アクセス項目」ダイアログ・ボックスには何も入力する必要がありません。

   ただし、特定のエントリに対してアクセス権を付与する場合には、この最初の「構造的アクセス項目」ダイアログ・ボックスで、次の手順を実行します。

   a. 検索基準バーの左のメニューから、属性タイプを選択します。

   b. バーの中央のメニューから、フィルタ・オプションのいずれかを選択します。詳細は、A-31 ページの表 A-45 を参照してください。

   c. 検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。

   d. 「**次へ**」をクリックします。ユーザーが追加できるエントリの種類を制限するための ACI の指定を要求する、2 番目の「構造型アクセス項目」ダイアログ・ボックスが表示されます。

3. ACI を指定して、ユーザーが追加できるエントリの種類を制限できます。たとえば、ユーザーが `objectclass=country` を持つエントリのみを追加できるように、DSE ルート・エントリで ACI を指定できます。その後、ディレクトリ・サーバーによって、新規エントリがこのフィルタの制限に適合するかどうかが検証されます。

   ユーザーが追加できるエントリの種類を制限する手順は、次のとおりです。

   a. 検索基準バーの一番左のメニューから、属性タイプを選択します。

   b. バーの中央のメニューから、フィルタ・オプションのいずれかを選択します。詳細は、A-31 ページの表 A-45 を参照してください。

   c. 検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。

d. 「**次へ**」を選択します。ウィザードによって、認証方式と暗号化方式、およびアクセス権を付与するサブジェクトの指定が要求されます。

4. 認証方式の指定はオプションです。認証方式を設定しない場合は、どの種類の認証も受け入れられます。あるノードで指定されている認証方式は、通信先のノードで指定されているバインド・モードと一致している必要があります。

   a. 認証のタイプを指定するには、「**認証の選択**」リストから、サブジェクト（アクセス権を要求しているエンティティ）が使用する認証のタイプを選択します。オプションの説明は、A-4 ページの表 A-4 を参照してください。

   b. 暗号化のタイプを指定するには、「**暗号化の選択**」リストから暗号化方式を選択します。オプションの説明は、A-4 ページの表 A-5 を参照してください。

   c. アクセス権を付与するエンティティを指定します。オプションの説明は、A-4 ページの表 A-6 を参照してください。

   d. 「**次へ**」をクリックします。アクセス権情報の入力を要求する「構造型アクセス項目」ダイアログ・ボックスが表示されます。

5. 付与する権限の種類を指定します。

   - **参照 :** サブジェクトにエントリの表示を許可します。
   - **追加 :** サブジェクトに、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 :** サブジェクトにエントリの削除を許可します。
   - **プロキシ :** パスワードを指定せずに、エンティティの代理となることを許可します。

6. 「**終了**」をクリックします。

タスク 3: ACP 作成ウィザードを使用したコンテンツ・アクセス項目の構成

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

2. 規範的なコンテンツ・アクセス項目を指定した場合は、ACP のすべての下位エントリをこの ACP が管理します。規範的なコンテンツ・アクセス項目を希望する場合は、この最初の「コンテンツ・アクセス項目」ダイアログ・ボックスには何も入力する必要がありません。

   ただし、アクセスを指定する属性を識別する手順は、次のとおりです。

   a. 検索基準バーの一番左のメニューから、属性タイプを選択します。

   b. バーの中央のメニューから、フィルタ・オプションのいずれかを選択します。詳細は、A-21 ページの表 A-33 を参照してください。

   c. 検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。

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

   e. 「**次へ**」を選択します。ウィザードによって、認証方式と暗号化方式、およびアクセス権を付与するサブジェクトの指定が要求されます。

3. 認証方式の指定はオプションです。認証方式を設定しない場合は、どの種類の認証も受け入れられます。あるノードで指定されている認証方式は、通信先のノードで指定されているバインド・モードと一致している必要があります。

   a. 認証のタイプを指定するには、「**認証の選択**」リストから、サブジェクト（アクセス権を要求しているエンティティ）が使用する認証のタイプを選択します。オプションの説明は、A-4 ページの表 A-4 を参照してください。

   b. 暗号化のタイプを指定するには、「**暗号化の選択**」リストから暗号化方式を選択します。オプションの説明は、A-4 ページの表 A-5 を参照してください。

   c. アクセス権を付与するエンティティを指定します。オプションの説明は、A-4 ページの表 A-6 を参照してください。

d. 「**次へ**」をクリックします。属性およびこの属性に対して実行する一致操作の選択を要求する、「コンテンツ・アクセス項目」ダイアログ・ボックスが表示されます。

4. 属性およびこの属性に対して実行する一致操作を選択する手順は、次のとおりです。

   a. 「コンテンツ・アクセス項目」ダイアログ・ボックスの「属性」フィールドで、アクセス権を付与または制限する属性を右のリストから選択します。

   b. 左のリストから、属性に対して実行する一致操作を選択します。選択肢は「EQ」(=)と「NEQ」(!=)です。

   c. 「**次へ**」をクリックします。アクセス権の指定を要求する「コンテンツ・アクセス項目」ダイアログ・ボックスが表示されます。

5. 付与する権限の種類を指定します。詳細は、A-5 ページの表 A-7 を参照してください。

6. 「**終了**」をクリックします。

Oracle Directory Manager を使用した ACP の変更

Oracle Directory Manager を使用して ACP を変更するには、次の 3 つのタスクが必要です。

- タスク 1: 変更するエントリの指定 .
- タスク 2: 構造型アクセス項目の変更（エントリに関係する ACI）
- タスク 3: コンテンツ・アクセス項目の変更（属性に関係する ACI）

タスク 1: 変更するエントリの指定

18-14 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。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」、「**アクセス制御管理**」の順に展開します。

2. 「**アクセス制御管理**」を選択します。ナビゲータ・ペインの「**アクセス制御管理**」の下のリストに、定義済のすべての ACP が表示されます。同じ内容のリストが、右側のペインにも表示されます。

3. ナビゲータ・ペインの「**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。

18-14 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。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「**< ディレクトリ・サーバー・インスタンス >**」、「**アクセス制御管理**」の順に展開します。

2. 変更する ACP を選択します。その ACP の情報が右側のペインに表示されます。

タスク 2: 構造型アクセス項目の変更

新規構造型アクセス項目を追加、または既存の構造型アクセス項目を変更できます。

> **関連項目：** 構造型アクセス項目の追加の詳細は、18-16 ページの「タスク 2: 構造型アクセス項目の構成」を参照してください。

構造型アクセス項目を変更する手順は、次のとおりです。

1. 「**構造型アクセス項目**」ウィンドウで変更する項目を選択し、「**構造型アクセス項目**」ウィンドウの下の「**編集**」をクリックします。「構造型アクセス項目」ダイアログ・ボックスが表示されます。
2. 「**エントリ・フィルタ**」タブ・ページを使用して、アクセス権を付与するエントリのセットを絞り込みます。ACP のすべての下位エントリを ACP で管理する場合は、次の手順に進んでください。

   1 つ以上の属性に基づいてエントリを選択する場合があります。たとえば、title が secretary の個人をすべて検索することや、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。これは、次の手順に従って行います。

   a. 検索基準バーの一番左のメニューから、属性を選択します。

   b. バーの中央のメニューから、フィルタ・オプションのいずれかを選択します。詳細は、A-21 ページの表 A-33 を参照してください。

   c. 検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。
3. 「**追加されたオブジェクト・フィルタ**」タブ・ページを使用して、ユーザーが追加できるエントリの種類を制限する ACI を指定できます。たとえば、ユーザーが `objectclass=country` を持つエントリのみを追加できるように、DSE ルート・エントリで ACI を指定できます。その後、ディレクトリ・サーバーによって、新規エントリがこのフィルタの制限に適合するかどうかが検証されます。

   ユーザーが追加できるエントリの種類を制限する手順は、次のとおりです。

   a. 検索基準バーの一番左のメニューから、属性タイプを選択します。

   b. バーの中央のメニューから、フィルタ・オプションのいずれかを選択します。詳細は、A-31 ページの表 A-45 を参照してください。

   c. 検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。
4. 「**責任者**」タブ・ページを使用して、認証方式と暗号化方式、および ACI のサブジェクト（アクセス権を要求しているエンティティ）を指定します。

   認証方式の指定はオプションです。認証方式を設定しない場合は、どの種類の認証も受け入れられます。あるノードで指定されている認証方式は、通信先のノードで指定されているバインド・モードと一致している必要があります。

   a. 認証のタイプを指定するには、「**認証の選択**」リストから、サブジェクト（アクセス権を要求しているエンティティ）が使用する認証のタイプを選択します。オプションの説明は、A-4 ページの表 A-4 を参照してください。

   b. 暗号化のタイプを指定するには、「**暗号化の選択**」リストから暗号化方式を選択します。オプションの説明は、A-4 ページの表 A-5 を参照してください。

   c. アクセス権を付与するエンティティを指定します。オプションの説明は、A-4 ページの表 A-6 を参照してください。

5. 「**アクセス権限**」タブ・ページを選択します。

   a. 付与する権限の種類を決定します。

   - **参照 :** サブジェクトにエントリの表示を許可します。
   - **追加 :** サブジェクトに、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 :** サブジェクトにエントリの削除を許可します。
   - **プロキシ :** パスワードを指定せずに、エンティティの代理となることを許可します。

     エントリが未指定の場合、アクセス権は、そのアクセス権が指定されている次の上位レベルで判断されます。

6. 「**OK**」をクリックします。

タスク 3: コンテンツ・アクセス項目の変更

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

> **関連項目 :** 新規のコンテンツ・アクセス項目を追加する方法は、18-17 ページの「タスク 3: コンテンツ・アクセス項目の構成」を参照してください。

コンテンツ・アクセス項目を変更する手順は、次のとおりです。

1. 「**コンテンツ・アクセス項目**」ボックスで変更するコンテンツ・アクセス項目を選択し、「**コンテンツ・アクセス項目**」ボックスの下の「**編集**」をクリックします。「コンテンツ・アクセス項目」ダイアログ・ボックスが表示されます。各タブ・ページには、変更可能な項目が含まれています。

2. ACP のすべての下位エントリを ACP で管理する場合は、「**エントリ・フィルタ**」タブ・ページには何も入力せず、次の手順に進みます。

   ACP では、定義されたアクセス権は、他のフィルタによりアクセスがそれ以上制限されないかぎり、このエントリおよびそのエントリのすべてのサブエントリに適用されます。適切な場合、「**エントリ・フィルタ**」タブ・ページを使用して、アクセスを指定するエントリを識別します。

   エントリへのアクセスを、このエントリの 1 つ以上の属性に基づいて制限できます。たとえば、役職名がマネージャで組織単位がアメリカであるすべてのエントリへのアクセスを制限できます。

   アクセスを指定するエントリを識別する手順は、次のとおりです。

   a. 検索基準バーの一番左のメニューから、属性タイプを選択します。

   b. バーの中央のメニューから、フィルタ・オプションのいずれかを選択します。詳細は、A-31 ページの表 A-45 を参照してください。

   c. 検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。

3. 「**責任者**」タブ・ページを使用して、認証方式と暗号化方式、および ACI のサブジェクト（アクセス権を要求しているエンティティ）を指定します。

   認証方式の指定はオプションです。認証方式を設定しない場合は、どの種類の認証も受け入れられます。あるノードで指定されている認証方式は、通信先のノードで指定されているバインド・モードと一致している必要があります。

   a. 認証のタイプを指定するには、「**認証の選択**」リストから、サブジェクト（アクセス権を要求しているエンティティ）が使用する認証のタイプを選択します。オプションの説明は、A-4 ページの表 A-4 を参照してください。

   b. 暗号化のタイプを指定するには、「**暗号化の選択**」リストから暗号化方式を選択します。オプションの説明は、A-4 ページの表 A-5 を参照してください。

c. アクセス権を付与するエンティティを指定します。オプションの説明は、A-4 ページの表 A-6 を参照してください。

4. 「**属性**」タブ・ページを選択します。

   a. 右のメニューから、アクセス権を付与または否認する属性を選択します。

   b. 左のメニューから、属性に対して実行する一致操作を選択します。選択肢は「EQ」（=）と「NEQ」（!=）です。

      たとえば、「EQ」と「cn」を選択した場合は、付与したアクセス権が cn 属性に適用されます。「NEQ」と「cn」を選択した場合は、付与したアクセス権が cn 属性に適用されません。

5. 「**アクセス権限**」タブ・ページを選択して、権限を指定します。詳細は、A-5 ページの表 A-7 を参照してください。

6. 「**OK**」をクリックします。

Oracle Directory Manager を使用したエントリ・レベルのアクセス権の付与

Oracle Directory Manager を使用してエントリ・レベルのアクセス権を付与する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「<ディレクトリ・サーバー・インスタンス>」、「**エントリ管理**」の順に展開します。
2. ナビゲータ・ペインで、エントリを選択して右側のペインにそのプロパティを表示します。
3. 「**ローカル・アクセス**」タブ・ページを選択して、18-21 ページの「Oracle Directory Manager を使用した ACP の変更」に示すように、「**構造型アクセス項目**」ボックスと「**コンテンツ・アクセス項目**」ボックスで、ローカル ACI を作成および編集します。
4. 変更後、「**適用**」をクリックします。

注意： 入力した情報をディレクトリ・サーバーに送信するには、「**適用**」をクリックする必要があります。「適用」をクリックしないと、情報は Oracle Directory Manager のキャッシュに保持されるだけです。

例 : Oracle Directory Manager を使用した ACP の管理

この例では、Oracle Directory Manager を使用して、ACI を含めた新規 ACP を作成する方法を紹介します。大企業の管理者が、ユーザー・パスワードに対するアクセス権を制限して、比較はすべての人が可能に、読取りと変更は各パスワードの所有者（ユーザー）のみ可能に設定する場合の例です。

この例では、新しい ACP を作成し、その ACP に次の各権限を設定する 4 つの ACI を移入します。

- すべての人による `userpassword` 属性に対する制限付きアクセス権
- ユーザー本人による同一 `userpassword` 属性への開かれたアクセス権
- すべての属性に対する開かれたアクセス権（すべての人による `userpassword` に対するアクセス権を除く）
- すべての人へのすべての属性に対する開かれたアクセス権

新規 ACP の作成

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」の順に展開します。
2. 「**アクセス制御管理**」を選択します。ACP のリストが右側のペインに表示されます。
3. 右側のペインの下の「**作成**」ボタンをクリックします。「新規アクセス制御ポイント」ダイアログ・ボックスが表示されます。
4. 「**エントリへのパス**」フィールドで、ACP に指定する識別名を入力します。ACP 内の ACI は、すべての下位エントリ（その識別名も含めて）に適用されます。

構造型アクセス項目の構成 エントリに対するアクセス権を設定する手順は、次のとおりです。

1. 「**構造型アクセス項目**」ボックスの下の「**作成**」をクリックします。+「構造型アクセス項目」ダイアログ・ボックスが表示されます。このダイアログ・ボックスには、「**エントリ・フィルタ**」、「**追加されたオブジェクト・フィルタ**」、「**責任者**」および「**アクセス権限**」のタブがあります。

   ACP のすべての下位エントリに ACI を適用するため、「**エントリ・フィルタ**」タブ・ページは使用しません。

2. 「**追加されたオブジェクト・フィルタ**」タブ・ページを選択します。

   ACI を指定して、ユーザーが追加できるエントリの種類を制限できます。たとえば、ユーザーが `objectclass=country` を持つエントリのみを追加できるように、DSE ルート・エントリで ACI を指定できます。その後、ディレクトリ・サーバーによって、新規エントリがこのフィルタの制限に適合するかどうかが検証されます。

   ユーザーが追加できるエントリの種類を制限する手順は、次のとおりです。

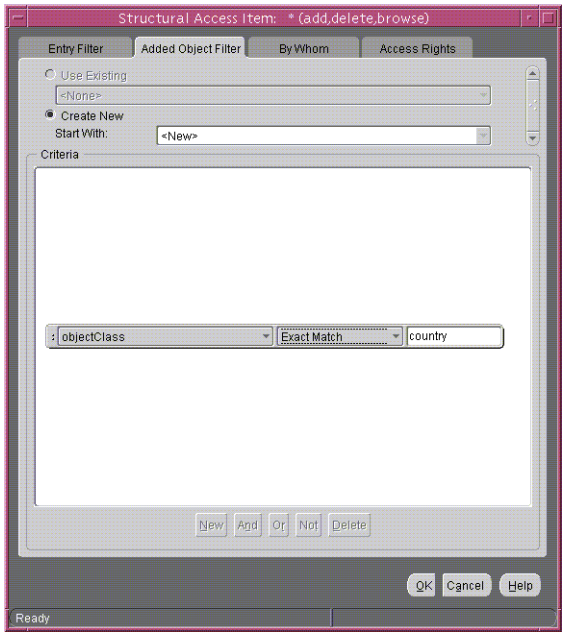
   a. 検索基準バーの一番左のメニューから、`objectclass` 属性タイプを選択します。

   b. バーの中央のメニューから「**完全一致**」を選択します。

   c. 検索基準バーの右のテキスト・ボックスに、`country` を入力します。

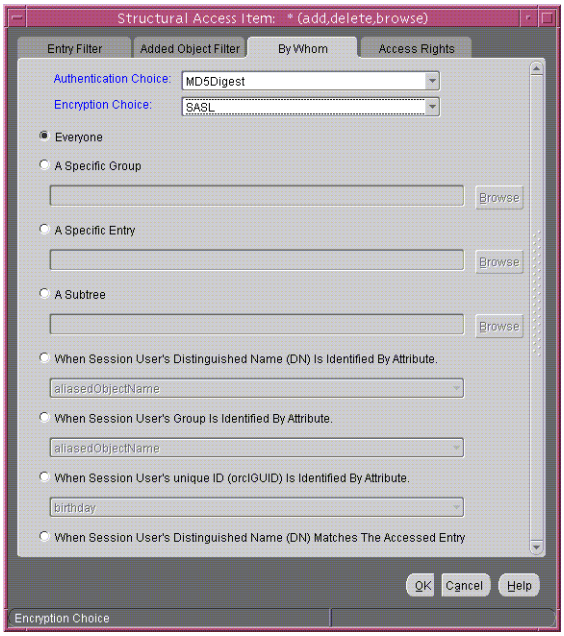
   ここで、「**追加されたオブジェクト・フィルタ**」タブ・ページは、図 18-1 のようになります。

図 18-1 構造型アクセス項目：「追加されたオブジェクト・フィルタ」タブ・ページ



3. 「**責任者**」タブ・ページを選択します。
   a. 「**認証の選択**」リストから、「**MD5 ダイジェスト**」を選択します。
   b. 「**暗号化の選択**」リストから、「**SASL**」を選択します。
   c. すべての人に対するアクセス権を作成するには、「**すべての人**」を選択します。「**責任者**」タブ・ページは、図 18-2 のようになります。

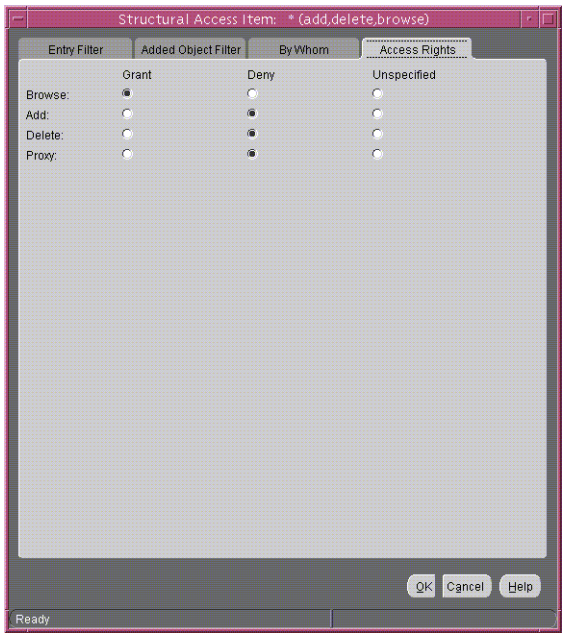
図 18-2 構造型アクセス項目：「責任者」タブ・ページ



4. 「**アクセス権限**」タブ・ページを選択します。デフォルトでは、すべての権限（「参照」、「追加」および「削除」）が付与されています。「プロキシ」は指定されません。

   a. すべての人が全エントリを参照でき、追加や削除はできないようにアクセス権を変更します。「**アクセス権限**」タブ・ページは、図 18-3 のようになります。

図 18-3 例 : 構造型アクセス項目 :「アクセス権限」タブ・ページ



   b. 「**OK**」をクリックします。

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

コンテンツ・アクセス項目を定義する手順は、次のとおりです。

1. 「**コンテンツ・アクセス項目**」ボックスの下の「**作成**」をクリックします。「コンテンツ・アクセス項目」ダイアログ・ボックスが表示されます。

   ACP のすべての下位エントリにこの ACI を適用するため、「**エントリ・フィルタ**」タブ・ページは使用しません。

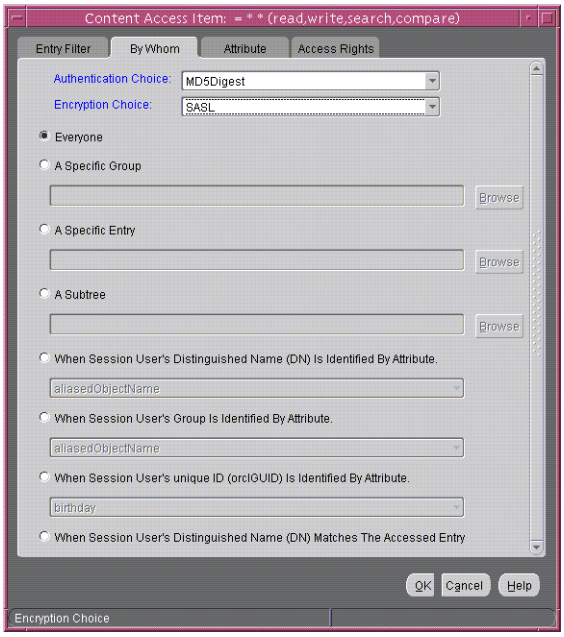
2. 「**責任者**」タブ・ページを選択します。

   a. 「**認証の選択**」リストから、「**MD5 ダイジェスト**」を選択します。

   b. 「**暗号化の選択**」リストから、「**SASL**」を選択します。

c. すべての人に対するアクセス権を作成するには、「**すべての人**」を選択します。「**責任者**」タブ・ページは、図 18-4 のようになります。

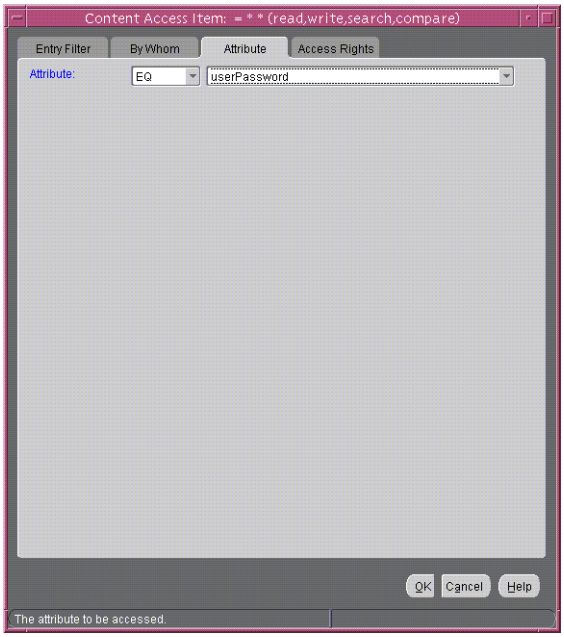
図 18-4 コンテンツ・アクセス項目：「責任者」タブ・ページ



3. 「**属性**」タブ・ページを選択します。このページには 2 つのフィールドがあります。最初のフィールドの選択肢は、「**EQ**」（等価）と「**NEQ**」（非等価）です。2 番目には、属性を設定します。

   「**EQ**」を選択して、「**`userPassword`**」を選択します。「**属性**」タブ・ページは、図 18-5 のようになります。

図 18-5 コンテンツ・アクセス項目：「属性」タブ・ページ



4. 「**アクセス権限**」タブ・ページを選択します。デフォルトでは、すべての権限が付与されています。読取り、検索、書込みおよび比較を否認するように権限を変更します。「**アクセス権限**」タブ・ページは、図 18-6 のようになります。

図 18-6 コンテンツ・アクセス項目：「アクセス権限」タブ・ページ

5. 「**OK**」をクリックします。

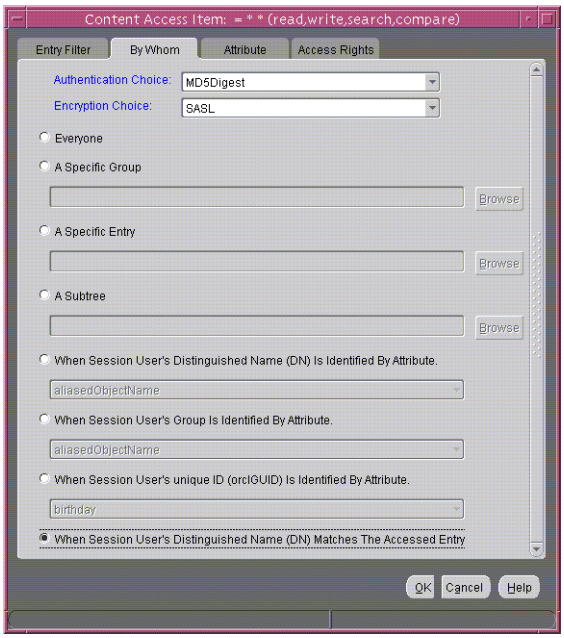
   これで 1 番目の ACI の設定は完了です。

2 番目の ACI の作成 ユーザーに、本人のパスワードの読取り、書込み、検索および比較を許可する 2 番目の ACI を作成します。

1. 「**コンテンツ・アクセス項目**」ボックスの下の「**作成**」をクリックします。「コンテンツ・アクセス項目」ダイアログ・ボックスが表示されます。
2. 「**責任者**」タブ・ページを選択します。
   a. 「**認証の選択**」リストから、「**MD5 ダイジェスト**」を選択します。
   b. 「**暗号化の選択**」リストから、「**SASL**」を選択します。

c. すべての人のアクセス権限を作成するには、「**セッション・ユーザーの識別名 (DN) がアクセス・エントリと一致する場合。**」を選択します。「責任者」タブ・ページは、図 18-7 のようになります。

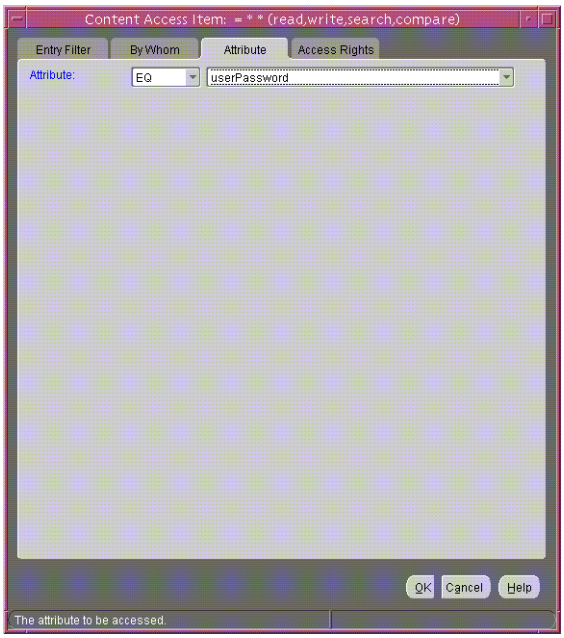
図 18-7 コンテンツ・アクセス項目：「責任者」タブ・ページ



3. 「**属性**」タブ・ページを選択します。このタブ・ページには、2 つのリストがあります。最初のリストの選択肢は、「**EQ**」（等価）と「**NEQ**」（非等価）です。2 番目には、属性を設定します。

   「**EQ**」と「**userPassword**」を選択します。「**属性**」タブ・ページは、図 18-8 のようになります。

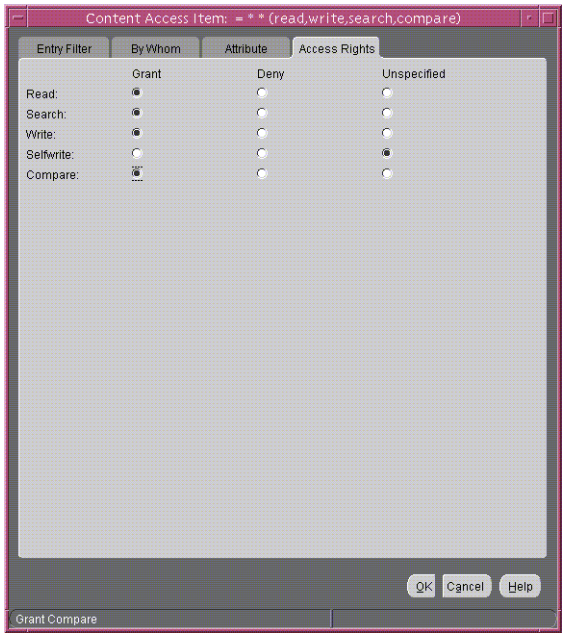
図 18-8 コンテンツ・アクセス項目：「属性」タブ・ページ



4. 「**アクセス権限**」タブ・ページを選択します。

   読取り、検索、書込みおよび比較の各アクセス権を付与します。「自己書込み」は未指定のままにします。「**アクセス権限**」タブ・ページは、図 18-9 のようになります。

図 18-9 コンテンツ・アクセス項目：「アクセス権限」タブ・ページ



5. 「**OK**」をクリックします。

これで 2 つの ACI が作成されました。1 番目の ACI は、`userPassword` 属性の読取り、検索、書込みおよび比較の各アクセス権をすべての人に対して否認しています。2 番目の ACI は、パスワードの所有者に対して、その属性の読取り、検索、書込みおよび比較を許可しています。

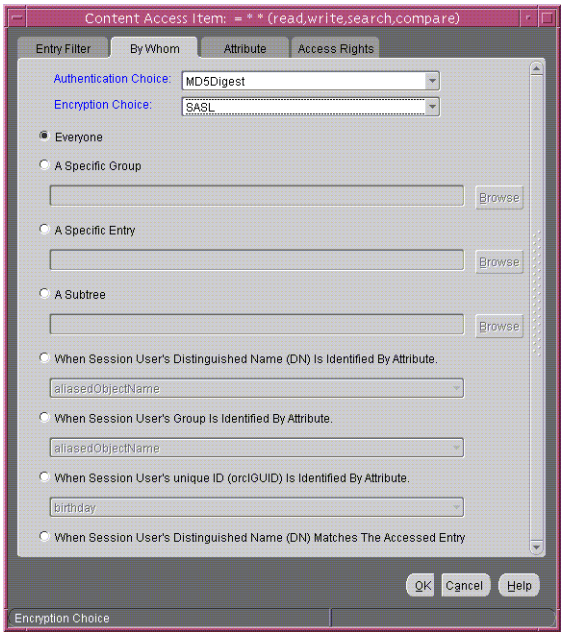
3 番目の ACI の作成

次の ACI は、`userPassword` を除くすべての属性の読取り、検索および比較の各アクセス権を、すべての人に付与します。書込みアクセス権は否認します。

1. 「**コンテンツ・アクセス項目**」ボックスの下の「**作成**」をクリックして、「コンテンツ・アクセス項目」ダイアログ・ボックスを表示します。
2. 「**責任者**」タブ・ページを選択します。
   a. 「**認証の選択**」リストから、「**MD5 ダイジェスト**」を選択します。
   b. 「**暗号化の選択**」リストから、「**SASL**」を選択します。

c. すべての人に対するアクセス権を作成するには、「**すべての人**」を選択します。「**責任者**」タブ・ページは、図 18-10 のようになります。

図 18-10 コンテンツ・アクセス項目：「責任者」タブ・ページ

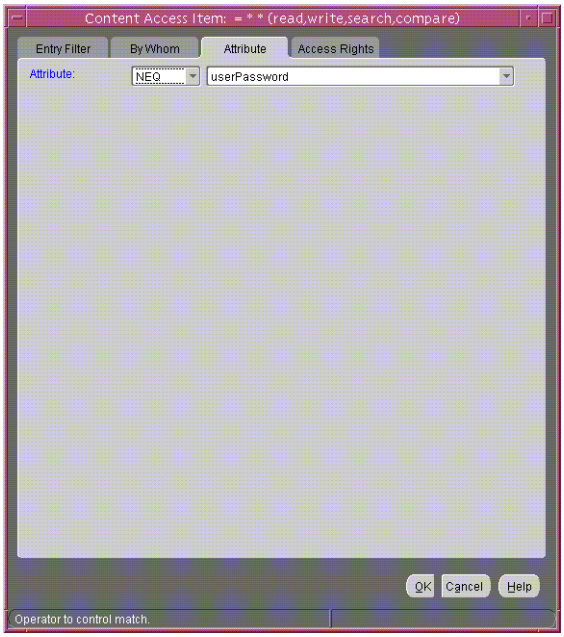


3. 「**属性**」タブ・ページを選択します。

「**NEQ**」と「**userPassword**」を選択します。

この組合せは、userpassword と等しくないあらゆる属性が、この ACI の権限の対象オブジェクトであることを示しています。「**属性**」タブ・ページは、図 18-11 のようになります。

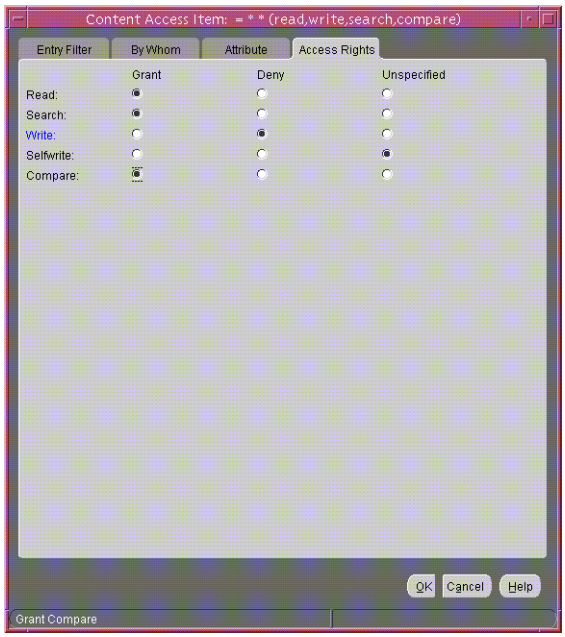
図 18-11 コンテンツ・アクセス項目：「属性」タブ・ページ



4. 「**アクセス権限**」タブ・ページを選択します。

   読取り、検索および比較の各アクセス権を付与します。「書込み」アクセス権は否認します。「自己書込み」は未指定のままにします。「**アクセス権限**」タブ・ページは、図 18-12 のようになります。

図 18-12 コンテンツ・アクセス項目：「アクセス権限」タブ・ページ



5. 「**OK**」をクリックしてこれらの権限を適用し、ダイアログ・ボックスを閉じます。

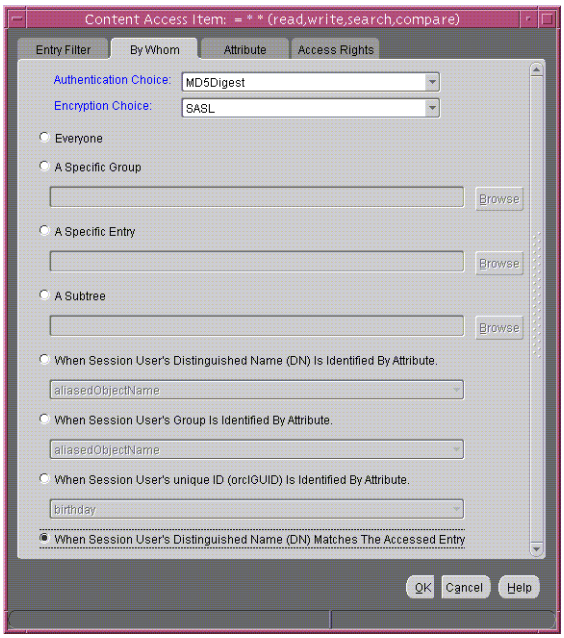
4 番目の ACI の作成

次の ACI は、`userpassword` を除くすべての属性の読取り、参照および書込みの各アクセス権を、その属性の所有者に付与します。この ACI を組み込むことによって、`userPassword` 以外の属性に対するアクセス権がその属性の所有者と他の人とで同じになるというあいまいさを排除できます。

1. 「**コンテンツ・アクセス項目**」ボックスの下の「**作成**」をクリックして、「コンテンツ・アクセス項目」ダイアログ・ボックスを表示します。
2. 「**責任者**」タブ・ページを選択します。
   a. 「**認証の選択**」リストから、「**MD5 ダイジェスト**」を選択します。
   b. 「**暗号化の選択**」リストから、「**SASL**」を選択します。

c. すべての人のアクセス権限を作成するには、「**セッション・ユーザーの識別名 (DN) がアクセス・エントリと一致する場合。**」を選択します。「責任者」タブ・ページは、図 18-13 のようになります。

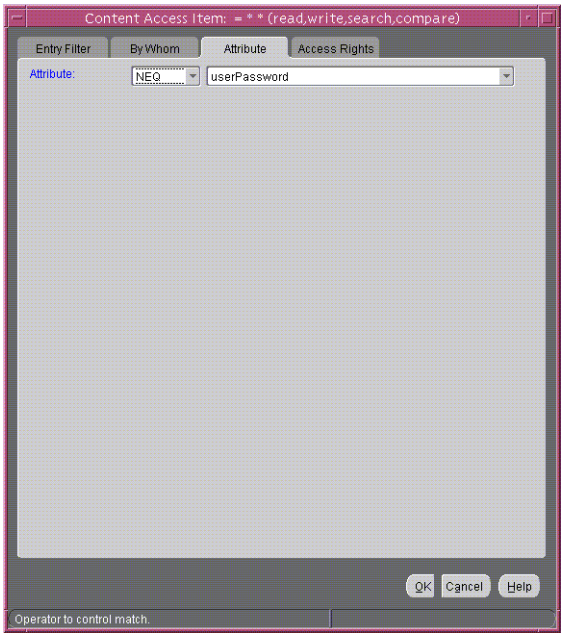
図 18-13 コンテンツ・アクセス項目：「責任者」タブ・ページ



3. 「**属性**」タブ・ページを選択します。

   リストから、「**NEQ**」と「**userPassword**」を選択します。この組合せは、userPassword 以外のすべての属性が、この ACI の権限の対象オブジェクトであることを示しています。「**属性**」タブ・ページは、図 18-14 のようになります。

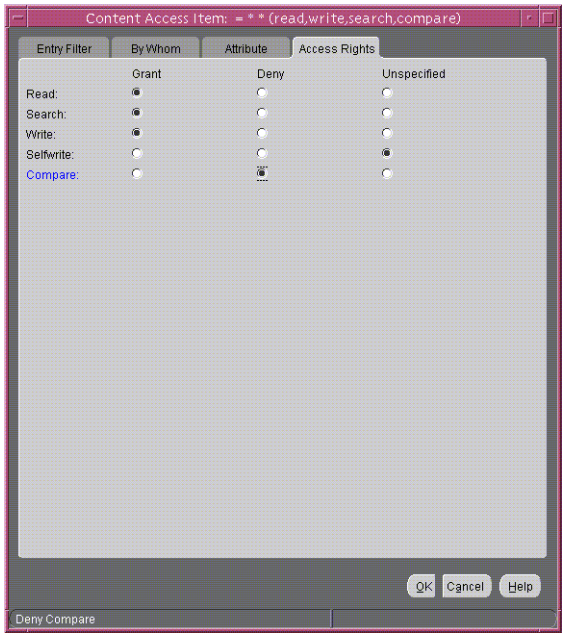
図 18-14 コンテンツ・アクセス項目：「属性」タブ・ページ



4. 「**アクセス権限**」タブ・ページを選択します。

   読取り、検索および書込みの各アクセス権を付与します。「自己書込み」は未指定のままにします。「**アクセス権限**」タブ・ページは、図 18-15 のようになります。

図 18-15 コンテンツ・アクセス項目：「アクセス権限」タブ・ページ



5. 「**OK**」をクリックしてこれらの権限を適用し、ダイアログ・ボックスを閉じます。

コマンドライン・ツールを使用したアクセス制御の管理

18-2 ページの「アクセス制御ポリシーの管理の概要」で説明したように、ディレクトリのアクセス制御ポリシーの情報は、ユーザーが変更可能な操作属性で表されます。これらの属性の値の設定および変更にコマンドライン・ツール（ldapmodify や ldapmodifymt を含む）を使用することで、ディレクトリのアクセス制御を管理できます。

付録 C「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。

この項の項目は次のとおりです。

- 例 : ユーザーが追加できるエントリの種類の制限
- 例 : ldapmodify を使用した継承可能な ACP の設定
- 例 : ldapmodify を使用したエントリ・レベルの ACI の設定
- 例 : ワイルド・カードの使用方法
- 例 : 識別名によるエントリの選択
- 例 : 属性セレクタとサブジェクト・セレクタの使用方法
- 例 : 読取り専用アクセス権の付与
- 例 : グループ・エントリへの自己書込みアクセス権の付与
- 例 : ポリシーの無視を禁止する完全な自律型ポリシーの定義

関連資料：

- 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、**LDIF** を使用した入力ファイルのフォーマット方法は、『Oracle Identity Management ユーザー・リファレンス』の、LDIF ファイルの形式化規則と例に関する項を参照してください。
- ldapmodify の実行方法は、『Oracle Identity Management ユーザー・リファレンス』の `ldapmodify` コマンドライン・ツールのリファレンスを参照してください。
- ACI の書式（構文）の詳細は、付録 C「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。

- サブジェクト `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。
- サブジェクト `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。
- その他はすべて、`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、それが存在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、オブジェクトとサブジェクトの指定子にワイルド・カード（*）を使用しています。acme.com ドメイン内のすべてのエントリに対して、すべてのユーザーが、すべての属性の読取り権限と検索権限およびすべてのエントリの参照権限を持つことになります。

dc=com の ACP 内の orclACI 属性は、次のように指定されています。

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

属性の読取りを許可するには、エントリの参照権限を付与する必要があります。

例 : 識別名によるエントリの選択

この例では、2 つのアクセス・ディレクティブで識別名を使用してエントリを選択する際の正規表現の使用方法を示します。この例では、dc=acme, dc=com アクセス権より下位の address book 属性の読取り専用アクセス権を、すべての人に付与します。

dc=acme,dc=com の orclACI 属性は、次のように指定されています。

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

dc=us, dc=acme,dc=com の orclACI 属性は、次のように指定されています。

```
access to entry by * (browse)
access to attr=(*) by dn=".*,dc=us,dc=acme,dc=com" (search, read)
```

例 : 属性セレクタとサブジェクト・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、および様々なサブジェクト・セレクタの使用方法を示します。この例は、dc=us,dc=acme,dc=com サブツリー内のエントリに適用されます。この ACI によって施行されるポリシーは次のとおりです。

- 管理者はサブツリー内のすべてのエントリに対する追加、削除および参照権限を所有しています。dc=us サブツリー内のその他のユーザーは、サブツリーの参照が可能ですが、サブツリー外部のユーザーはそのサブツリーにアクセスできません。
- salary 属性は、そのマネージャによる変更が可能で、本人は参照できます。その他のユーザーは salary 属性にアクセスできません。
- userPassword 属性は、パスワードの所有者と管理者による表示および変更が可能です。その他のユーザーは、この属性の比較のみ可能です。
- homePhone 属性は、本人による読取りおよび書込みが可能で、すべてのユーザーが参照できます。
- その他のすべての属性は、管理者のみ値の変更が可能です。その他のすべてのユーザーは、比較、検索、読取りは可能ですが、属性値の更新はできません。

dc=us,dc=acme,dc=com の orclACI 属性は、次のように指定されています。

```
access to entry
by dn="cn=admin, dc=us,dc=acme,dc=com" (browse, add, delete)
by dn=".*, dc=us,dc=acme,dc=com" (browse)
by * (none)


access to attr=(salary)
by dnattr=(manager) (read, write)
by self (read)
by * (none)


access to attr=(userPassword)
by self (search, read, write)
by dn="cn=admin, dc=us,dc=acme,dc=com" (search, read, write)
by * (compare)


access to attr=(homePhone)
by self (search, read, write)
by * (read)


access to attr != (salary, userPassword, homePhone)
by dn="cn=admin, dc=us,dc=acme,dc=com" (compare, search, read, write)
by * (compare, search, read)
```

例 : 読取り専用アクセス権の付与

この例では、dc=acme, dc=com より下位の address book 属性の読取り専用アクセス権を、すべての人に付与します。さらに、dc=us,dc=acme,dc=com サブツリー内のみのすべての属性に対する読取りアクセス権をすべての人に付与します。

dc=acme,dc=com の orclACI 属性は、次のように指定されています。

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

dc=us,dc=acme,dc=com の orclACI 属性は、次のように指定されています。

```
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。

グループ・エントリの orclEntryLevelACI 属性は、次のように指定されています。

```
access to attr=(member)
by dn=".*, dc=us,dc=acme,dc=com" (selfwrite)
```

例 : ポリシーの無視を禁止する完全な自律型ポリシーの定義

この例では、グループの無視を否認します。次の識別名を使用します。

表 18-5 例で使用される識別名

コンテナ	DN
グループ無視ポリシーを適用できないネーミング・コンテキスト	c=us
ユーザー・コンテナ	cn=users,c=us
重要なデータ	cn=appdata
このネーミング・コンテキストのユーザー管理グループ	cn= user admin group, cn=users,c=us
セキュリティ管理グループまたはこのネーミング・コンテキスト	cn= security admin group, cn=users,c=us
パスワードをリセットするすべてのネーミング・コンテキストのグローバル・パスワード管理グループ	cn=password admin group

c=us のポリシー要件は次のとおりです。

- ユーザーはその情報を参照および読取りできる。
- ユーザー・セキュリティ管理は、パスワードと ACP を除く、c=us の下の情報を変更できる。
- セキュリティ管理グループは、c=us の下のポリシーを変更できる。
- グローバル・パスワード管理とユーザーは、パスワードをリセットできる。
- 他のすべてのユーザーに権限は付与されない。
- このポリシーは無視できない。

必要な ACP は次のとおりです。

```
Access to entry DenyGroupOverride
by dn=".*,c=us" (browse,noadd,nodelete)
by group="cn=User admin group,cn=users,c=us" (browse,add,delete)

Access to attr=(orclaci) DenyGroupOverride
by group="cn=security admin group,cn=users,c=us" (search,read,write,compare)
by * (none)

Access to attr=(userpassword) DenyGroupOverride
by self (search,read,write,compare)
by group="cn=password admin group" (search,read,write,compare)
by * (none)

Access to attr=(*) DenyGroupOverride
by self (search,read,nowrite,compare)
by group="cn= User admin group,cn=users,c=us" (search,read,write,compare)
by * (none)
```

19

Oracle Internet Directory のパスワード・ポリシー

パスワード・ポリシーとは、パスワードの使用方法を管理する規則のセットです。この章の項目は次のとおりです。

パスワード・ポリシーの概要

この項の項目は次のとおりです。

パスワード・ポリシーとは

パスワード・ポリシーとは、パスワードの構文および使用方法を管理する規則のセットです。Oracle Internet Directory によって適用されるパスワード・ポリシーには、次のようなものがあります。

- 指定されたパスワードの有効期限
- パスワードの最小必須文字数
- パスワードに必要な数字の最小数
- アルファベット文字の最小数
- 繰返し文字の最小数
- 大文字および小文字の使用
- 英数字以外の文字（特殊文字）の最小数
- ユーザーによる定期的なパスワードの変更
- パスワード変更の最小および最大間隔
- パスワードの期限切れ（時間またはログイン回数による）後のログインの猶予期間
- 以前使用したパスワードのユーザーによる再利用禁止

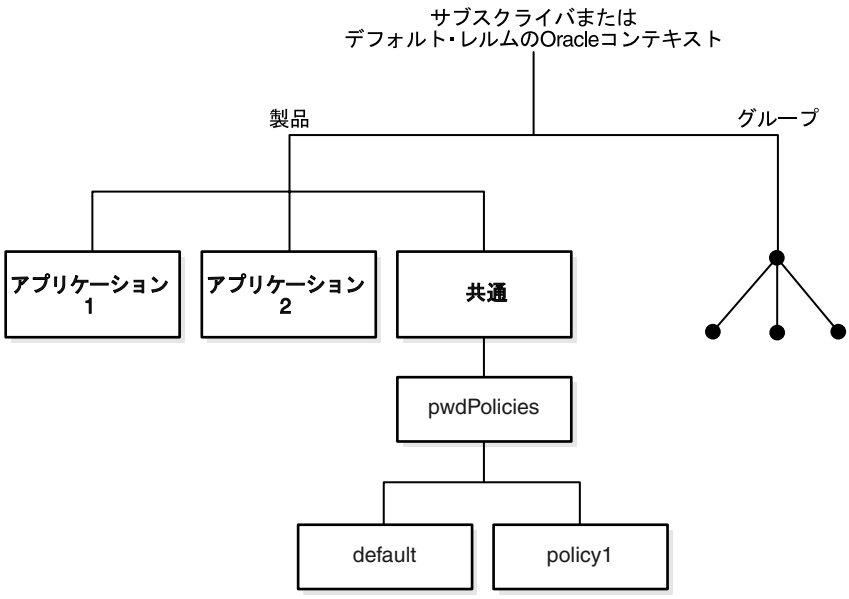
細かなパスワード・ポリシー

旧リリースでは、Oracle Internet Directory は、各レルムで 1 つのパスワード・ポリシーしかサポートしていませんでした。Oracle Internet Directory 10*g*（10.1.4.0.1）では、Oracle Internet Directory は、各レルムで複数のパスワード・ポシーをサポートするようになりました。10*g*（10.1.4.0.1）でのもう 1 つの変更は、これらのポリシーが、そのレルム内のどのサブツリーにも適用できることです。つまり、エントリ固有のパスワード・ポリシーを使用できるようになりました。

パスワード・ポリシーは、レルム固有または有効範囲がディレクトリ全体のものとして指定できます。希望する有効範囲を実現するには、適切なコンテナにパスワード・ポリシー・エントリを作成する必要があります。Oracle Internet Directory 10*g*（10.1.4.0.1）では、パスワード・ポリシーは、各レルムの `cn=common` エントリの下に作成された `cn=pwdPolicies` コンテナの下に移入されます。デフォルトでは、これらのコンテナに、相対識別名 `cn=default` のパスワード・ポリシーが入っています。たとえば、ディレクトリ固有のデフォルトのパスワード・ポリシーの識別名は、`cn=default,cn=pwdPolicies,cn=Common,cn=Products,cn=OracleContext` になります。

その他のポリシーは、別の相対識別名を持つ pwdPolicies コンテナの下に作成できます。図 19-1 は、この例を説明しています。

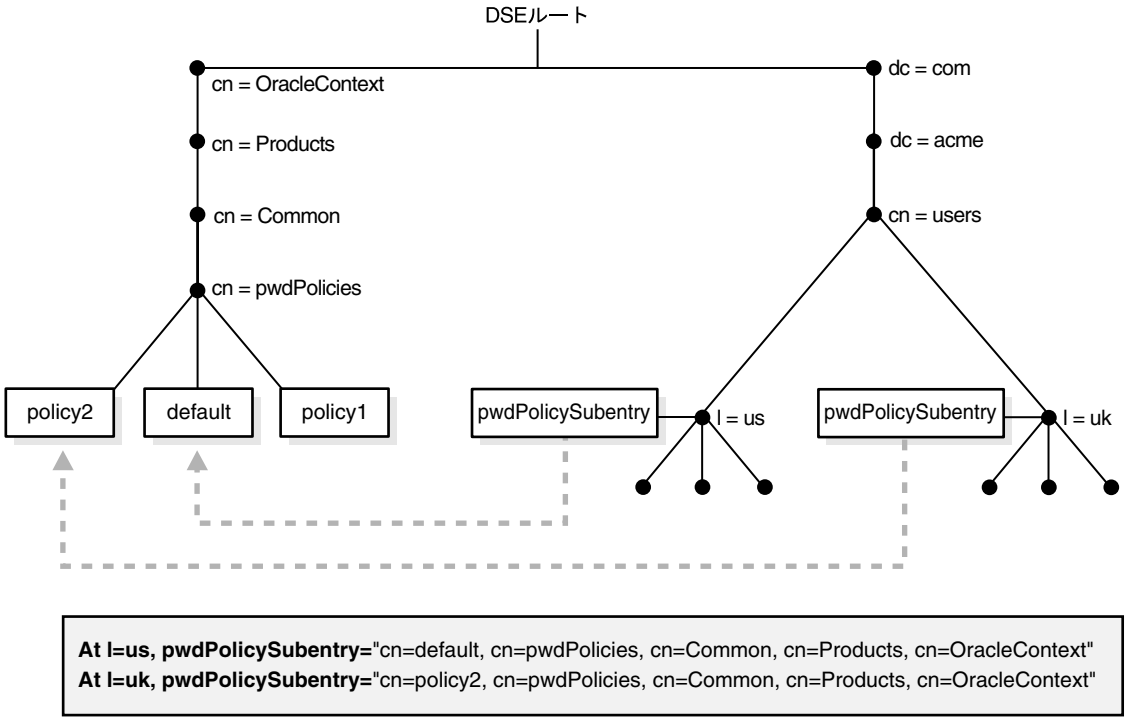
図 19-1 パスワード・ポリシー・エントリの位置



10*g*（10.1.4.0.1）では、旧リリースと異なり、パスワード・ポリシーは、レルム固有の共通エントリにある orclcommonusersearchbase 属性から完全に切り離されています。旧リリースからアップグレードした場合、アップグレード時に既存のパスワード・ポリシーが新規アーキテクチャに移行されています。ただし、識別名を単純に orclcommonusersearchbase に追加すると、レルムのデフォルトのパスワード・ポリシーが、その識別名をルートとするサブツリーに適用されることが保証されなくなります。

Oracle Internet Directory 10*g*（10.1.4.0.1）では、パスワード・ポリシーを定義すると、そのパスワード・ポリシーをそのディレクトリのサブツリーに適用するために、もう 1 つの手順を実行する必要があります。pwdPolicysubentry 属性に希望するパスワード・ポリシーの識別名を指定して、管理者としてそのポリシーの適用対象にしようと考えているサブツリーのルートであるエントリに移入します。図 19-2 では、これを説明しています。l=us にある pwdPolicysubentry には、デフォルト・ポリシー "cn=default,cn=pwdPolicies, cn=Common,cn=Products, cn=OracleContext" の識別名が含まれているため、デフォルト・ポリシーが米国内のユーザーに適用されます。l=uk にある pwdPolicysubentry には、ポリシー "cn=policy2,cn=pwdPolicies,cn=Common,cn=Products, cn=OracleContext" の識別名が含まれているため、policy2 が英国のユーザーに適用されます。

図 19-2 パスワード・ポリシーの識別名で移入された pwdPolicysubentry 属性



実行時に、Oracle Internet Directory は、エントリに移入された pwdPolicysubentry 属性を探し、その値で示されたポリシーを適用することにより、エントリで適用可能なパスワードを解決します。移入された pwdPolicysubentry 属性が存在しない場合、Oracle Internet Directory は、pwdPolicysubentry が移入されている一番近い上位エントリが見つかるまで、ディレクトリ・ツリーを遡っていき、属性で示されたパスワード・ポリシーを適用します。

注意： パスワード・ポリシーは、orclpwdpolicyenable を 0 に設定することで無効にできます。無効にすると、ディレクトリのその部分は適用できるパスワード・ポリシーのない状態のままになります。Oracle Internet Directory は、適用できる有効なポリシーを見つけるためにディレクトリ情報ツリーを遡らなくなります。これにより、ディレクトリの一部を必要に応じてパスワード・ポリシーなしにしておくことができます。ただし、このような変更を行う意味について実行する前に知っておく必要があります。

パスワード・ポリシーを設定する手順は、次のとおりです。

1. 該当するコンテナにパスワード・ポリシー・エントリを作成し、それを pwdpolicy オブジェクトと関連付けます。
2. 手順 1 で作成したエントリの pwdPolicy オブジェクト・クラスの下で定義された属性の値を設定して、希望するポリシーを作成します。
3. orclpwdpolicyenable 属性が 1 に設定されていることを確認します。これが 1 に設定されていない場合、Oracle Internet Directory はポリシーを無視します。
4. ポリシーの識別名を指定した pwdPolicysubentry 属性を追加し、そのポリシーによって管理されるサブツリーのルートに移入します。

関連資料： pwdPolicy オブジェクト・クラス、およびパスワード・ポリシーに関連する top オブジェクト・クラスの属性のリストおよび説明は、『Oracle Identity Management ユーザー・リファレンス』のオブジェクト・クラスのリファレンスに関する項を参照してください。

注意： サブツリーおよびユーザーのパスワード・ポリシー・エントリはレプリケートされています。10*g*（10.1.4.0.1）のポリシーを 10*g*（10.1.4.0.1）より前のノードにレプリケートしても、そのノードの機能には悪影響はありません。ただし、10*g*（10.1.4.0.1）より前のノードでは、10*g*（10.1.4.0.1）のパスワード・ポリシーを意味があるように解釈できません。ノードでは、そのパスワード・ポリシーを Oracle コンテキスト・レルムで適用し続けます。

注意： パスワード・ポリシー・エントリは、第 18 章「ディレクトリ・アクセス制御」で説明している Oracle Internet Directory の ACI インフラストラクチャを使用して、匿名アクセスから保護する必要があります。これは、パスワード・ポリシーが脆弱な場合、その情報が攻撃する者の助けとなって、ディレクトリを危険にさらす恐れがあるため、特に重要です。

デフォルトのパスワード・ポリシー

Oracle Internet Directory のデフォルトのパスワード・ポリシーは次のとおりです。

- パスワードの有効期限は 120 日です。
- 10 回ログインに失敗すると、アカウントがロックアウトされます。スーパーユーザー・アカウントを除き、すべてのアカウントは、ディレクトリ管理者がパスワードを再設定するまで、24 時間ロックされたままになります。アカウント・ロックアウト継続時間が経過しても、正しいパスワードでバインドするまでユーザー・アカウントはロックされたままになります。

  スーパーユーザー・アカウントである `cn=orcladmin` がロックされると、OID データベース・パスワード・ユーティリティを使用してロックを解除するまで、ロックされたままになります。このユーティリティでは、ODS ユーザー・パスワードの入力が要求されます。ODS パスワードを入力すると、アカウントのロックが解除されます。

  関連資料：

  スーパーユーザー・アカウントのロック解除の詳細は、『Oracle Identity Management ユーザー・リファレンス』の `oidpasswd` コマンドライン・ツールのリファレンスを参照してください。

  L-8 ページの「**パスワード・ポリシーに関するトラブルシューティング**」

- パスワードの最小文字数は 5 で、1 つ以上の数字を含める必要があります。
- パスワードの期限切れの警告は、期限終了前 7 日に出ます。
- パスワードの期限切れ後、5 回の猶予期間ログインが許されます。

Oracle Internet Directory リリース 9.0.4 からは、ルート Oracle コンテキストのパスワード・ポリシー・エントリがスーパーユーザーに適用されますが、アカウントのロックアウトを管理するパスワード・ポリシーのみがそのアカウントに適用されます。

注意： Oracle Identity Management には、2 つのタイプの特権ユーザーが存在します。どちらの特権ユーザー・アカウントも、特定のパスワード・ポリシーがアクティブになるとロックできます。

一方のタイプの特権ユーザーは、識別名が cn=orcladmin のスーパーユーザーで、デフォルトの ID 管理レルム内で特別なユーザー・エントリとして表されます。これによって、ディレクトリ管理者はディレクトリ情報ツリーを任意に修正し、Oracle Internet Directory サーバーの構成を任意に変更できます。このスーパーユーザー（orcladmin）アカウントが、誤ったパスワードでのバインドを何度も試行したなどの理由でロックされた場合は、**Oracle Internet Directory** リポジトリに対する DBA 権限を持った管理者が oidpasswd ツールを使用してロックを解除できます。orcladmin アカウントのロックを解除するには、次のコマンドを実行します。

```
oidpasswd unlock_su_acct=TRUE
```

もう一方の特権ユーザーは、レルム固有の特権ユーザーで、レルム内のユーザーやグループの作成と削除などの機能、および Oracle Delegated Administration Services に関連するすべての機能を制御します。このアカウントは、識別名 cn=orcladmin,cn=users,*realm DN* のエントリにより表されます。単一のスーパーユーザー・アカウントの場合と比較すると、各レルムにレルム固有の独自の特権ユーザーが存在することになります。レルム固有の特権アカウントのロックを解除する場合は、もう一方のタイプの特権ユーザーである cn=orcladmin が、Oracle Directory Manager を使用して該当するアカウントのパスワードを変更します。

Oracle Internet Directory のパスワード・ポリシーは、シンプルなバインド（userpassword 属性に基づく）、userpassword 属性に対する比較操作および SASL バインドに適用され、SSL バインドおよびプロキシ・バインドには適用されません。

パスワード・ポリシーの属性

次の属性は、パスワード・ポリシーに影響を与えます。

表 19-1 パスワード・ポリシーの属性

名前	機能
pwdMinAge	ユーザーによるパスワードへの変更から変更までに必要な経過時間（秒）。デフォルトは 0 です。
pwdMaxAge	パスワードが有効である最大時間（秒）。この時間に達すると同時に、パスワードは期限切れになったとみなされます。デフォルトは 10368000 秒（120 日）です。
pwdLockout	これに該当する場合、サーバーでは、無効なログインを何回か連続して試行したユーザーをロックアウトします。この回数は pwdMaxFailure で指定します。pwdLockout のデフォルト値は 1（TRUE）です。
orclpwdIPLockout	これに該当する場合、サーバーでは、同じ IP アドレスから無効なログインを何回か連続して試行したユーザーをロックアウトします。回数は orclpwdIPMaxFailure で指定します。デフォルトは FALSE です。
pwdLockoutDuration	無効なログイン試行回数がしきい値に達したユーザー・アカウントをロックアウトする期間（秒）。デフォルトは 186400 秒（24 時間）です。
orclpwdIPLockoutDuration	同じ IP アドレスからの無効なログイン試行回数がしきい値に達したユーザー・アカウントをロックアウトする期間（秒）。デフォルトは 0 です。

表 19-1 パスワード・ポリシーの属性（続き）

名前	機能
pwdMaxFailure	ユーザー・アカウントをロックアウトする前に、サーバーが許可する無効なログインの最大試行回数。デフォルト値は 10 です。
orclpwdIPMaxFailure	ユーザー・アカウントをロックアウトする前に、サーバーが許可する特定の IP アドレスからの無効なログインの最大試行回数。デフォルトは 0 です。
pwdFailureCountInterval	認証に成功しなくても、失敗カウンタからパスワードの失敗が消去されるまでの時間（秒）。デフォルトは 0 です。
pwdExpireWarning	パスワードが期限切れになるまでの最大時間（秒）で、期限切れ警告メッセージが認証ユーザーに返されます。デフォルトは 604800 秒（7 日）です。
pwdCheckSyntax	パスワードの構文チェックを有効または無効にします。 0: すべての構文チェックを無効にします。 1: パスワード構文値チェックを暗号化されたパスワードを除き有効にします（デフォルト）。
pwdMinLength	このポリシーで管理されるパスワードの最小文字数。デフォルトは 5 文字です。
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。デフォルトは 5 です。
orclpwdGraceLoginTimeLimit	パスワードの期限切れ後に猶予期間ログインを許可する最大時間（秒）。orclpwdGraceLoginTimeLimit が 0 以外の場合、pwdGraceloginLimit は 0 にします。pwdGraceloginLimit が 0 以外の場合、orclpwdGraceLoginTimeLimit は 0 にします。
pwdMustChange	ユーザーは、アカウント作成後、または管理者によるパスワードの再設定後の最初のログイン時に、パスワードを再設定する必要があります。デフォルトは 0（FALSE）です。
orclpwdIllegalValues	パスワードとして許可されない値のリストです。
orclpwdAlphaNumeric	パスワードに必要な数字の最小数。デフォルトは 1 です。
orclpwdMinAlphaChars	パスワードに必要なアルファベット文字の最小数。デフォルトは 0 です。
orclpwdMinSpecialChars	パスワードに必要な英数字以外の文字（特殊文字）の最小数。デフォルトは 0 です。
orclpwdMinUppercase	パスワードに必要な大文字の最小数。デフォルトは 0 です。
orclpwdMinLowercase	パスワードに必要な小文字の最小数。デフォルトは 0 です。
orclpwdMaxRptChars	パスワードで許可される繰返し文字の最小数。デフォルトは 0 です。
pwdInHistory	指定エントリの pwdHistory 属性に格納される使用済パスワードの最大数。pwdHistory に格納されたパスワードは、そこから消去されるまで、新規パスワードとして使用できません。デフォルトは 0 です。
pwdAllowUserChange	現在は使用されていません。
orclpwdPolicyEnable	これが TRUE の場合、サーバーはこのポリシーを評価します。TRUE でない場合、ポリシーは無視され、適用されません。デフォルトは 1（TRUE）です。
orclpwdEncryptionEnable	TRUE に設定すると、パスワードの暗号化が有効になります。デフォルトは 1（TRUE）です。

表 19-1 パスワード・ポリシーの属性（続き）

名前	機能
orclpwdAllowHashCompare	ハッシュ・パスワード値を使用するログインを有効または無効にします。0 = 無効（デフォルト）。1 = 有効。
orclpwdAllowHashCompare	ハッシュ・パスワード値を使用するログインを有効または無効にします。0 = 無効（デフォルト）。1 = 有効。

パスワード・ポリシー情報のディレクトリ・サーバー検証

19-2 ページの「細かなパスワード・ポリシー」で説明しているように、Oracle Internet Directory は、移入された適切な pwdPolicysubentry を見つけることで、エントリに適用可能なポリシーを判断します。ユーザー・パスワードが指定のポリシーの要件を満たしていることを確認する場合、ディレクトリ・サーバーは、次のことを検証します。

- パスワード・ポリシーが使用可能になっているかどうかの確認。この確認では、パスワード・ポリシー・エントリの orclpwdpolicyenable 属性の値がチェックされます。値 1 は、パスワード・ポリシーが使用可能になっていることを示します。値 0 は、パスワード・ポリシーが使用禁止になっていることを示します。
- パスワード・ポリシー構文情報（英数字の数、パスワード長など）の正確さ。ディレクトリ・サーバーは、ldapadd および ldapmodify が userpassword 属性上で実行中に構文チェックを行います。
- パスワード・ポリシー状態情報。次に、その例を示します。
  - ユーザー・パスワードが作成または変更されたときのタイムスタンプ。
  - 最小パスワード有効期限は、現在の時刻からパスワード作成時刻を引いた値より大きくなります。
  - ユーザーが連続してログインに失敗したときのタイムスタンプ。
  - ユーザーのアカウントがロックされた日時。
  - パスワードが再設定されたため、最初の認証でユーザーがパスワードを変更する必要があることを示すインジケータ。
  - ユーザーが以前に使用したパスワードの履歴。
  - 猶予期間ログインのタイムスタンプ。

  猶予期間ログインが時間で設定されている場合、サーバーは現在の時刻と期限切れ時刻の差異をチェックします。

  ディレクトリ・サーバーは、ldapbind および ldapcompare の実行中に、状態情報をチェックしますが、このチェックは、orclpwdpolicyenable 属性が 1 に設定されている場合にのみ実行されます。

  パスワード値の構文チェックを使用可能にするには、パスワード・ポリシー・エントリの orclpwdpolicyenable および pwdchecksyntax 属性を TRUE に設定します。

パスワード・ポリシー、アカウントおよびパスワードの管理

この項の項目は次のとおりです。

- Oracle Directory Manager を使用したパスワード・ポリシーの管理
- コマンドライン・ツールを使用したパスワード・ポリシー、アカウントおよびパスワードの管理
- セルフ・サービス・コンソールを使用したアカウントおよびパスワードの管理

表 19-2 に、パスワード・ポリシーに関連する管理タスク、各タスクの実行に使用するツールおよび対応する情報の参照先を示します。

表 19-2 パスワード・ポリシー管理のためのタスクおよびツール

タスク	ツール	参照先
アカウントの有効化と無効化	Oracle Internet Directory セルフ・サービス・コンソール ldapmodify	19-13 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用したアカウントの有効化と無効化」 19-12 ページの「例 : コマンドライン・ツールを使用したアカウントの有効化と無効化」
パスワードの強制変更	ldapmodify	19-13 ページの「例 : コマンドライン・ツールを使用したパスワードの強制変更」
ID 管理レルムのパスワード・ポリシーの変更	Oracle Directory Manager ldapmodify	19-11 ページの「Oracle Directory Manager を使用したパスワード・ポリシーの作成」 19-12 ページの「例 : コマンドライン・ツールを使用したパスワード・ポリシーの変更」
パスワード・ポリシーの設定	ldapmodify	19-11 ページの「例 : コマンドライン・ツールを使用したパスワード・ポリシーの設定」
アカウントのロック解除	Oracle Internet Directory セルフ・サービス・コンソール ldapmodify	19-14 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用したアカウントのロック解除」 19-13 ページの「例 : コマンドライン・ツールを使用したアカウントのロック解除」
ID 管理レルムのパスワード・ポリシーの表示	Oracle Directory Manager ldapsearch	19-10 ページの「Oracle Directory Manager を使用したパスワード・ポリシーの表示」 19-12 ページの「例 : コマンドライン・ツールを使用したパスワード・ポリシーの表示」

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

Oracle Directory Manager を使用して、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。

この項の項目は次のとおりです。

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

パスワード・ポリシーを表示するには、ナビゲータ・ペインで「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」、「パスワード・ポリシー管理」の順に展開します。ナビゲータ・ペインにはパスワード・ポリシー・エントリが表示されます。右側のペインには 2 つのタブがあります。「**一般**」タブには、パスワード・ポリシー・グループ・エントリへのパスが表示されます。「**パスワード・ポリシー有効サブツリー**」タブには、次の 2 つの列のある表が表示されます。

- 「**パスワード・ポリシー**」列は、各パスワードのポリシー・エントリを示します。
- 「**有効サブツリー**」列は、各ポリシーを適用するサブツリーを示します。

パスワード・ポリシーを最新の内容に更新するには、「**リフレッシュ**」を選択します。

特定のパスワード・ポリシーを取得するには、ナビゲータ・ペインで、表示するパスワード・ポリシーを選択します。右側のペインにポリシーが表示されます。

> **関連項目：** Oracle Directory Manager で表示される各パスワード・ポリシーの説明は、A-7 ページの「Oracle Directory Manager のパスワード・ポリシーに関するフィールド」を参照してください。

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

パスワード・ポリシーを変更する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」、「**パスワード・ポリシー管理**」の順に展開します。
2. ナビゲータ・ペインで、変更するパスワード・ポリシーを選択します。対応するタブ・ページが、右側のペインに表示されます。
3. 必要に応じて、「**一般**」タブ・ページの編集可能な属性フィールドを変更します。フィールドについては、A-7 ページの表 A-10 を参照してください。
4. 「**アカウントのロックアウト**」タブ・ページを選択した後、フィールドを変更する場合は「**グローバル・ロックアウト**」を選択します。必要に応じて、編集可能な属性フィールドを変更します。フィールドについては、A-8 ページの表 A-11 を参照してください。
5. 「**IP のロックアウト**」タブ・ページを選択した後、フィールドを変更する場合は「**IP のロックアウト**」を選択します。必要に応じて、編集可能な属性フィールドを変更します。フィールドについては、A-8 ページの表 A-12 を参照してください。
6. 「**パスワード構文**」タブ・ページを選択した後、フィールドを変更する場合は「**パスワード構文のチェック**」を選択します。必要に応じて、編集可能な属性フィールドを変更します。フィールドについては、A-8 ページの表 A-13 を参照してください。
7. ポリシーを適用するサブツリーを変更するには、「有効サブツリー」タブ・ページを選択します。
8. 変更終了後、「**適用**」を選択します。

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

新規のパスワード・ポリシーを作成する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「<ディレクトリ・サーバー・インスタンス>」、「**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、既存のパスワード・ポリシーの 1 つを選択します。対応するタブ・ページが、右側のペインに表示されます。
3. 右側のペインで、ポリシーの名前を選択して、「**編集**」を選択します。
4. 新規ポリシーを作成するには、「**作成**」または「**類似作成**」を選択します。
5. 必要に応じて、「**一般**」タブ・ページの編集可能な属性フィールドを設定または変更します。フィールドについては、A-7 ページの表 A-10 を参照してください。
6. 「**アカウントのロックアウト**」タブ・ページを選択した後、フィールドを変更する場合は「**グローバル・ロックアウト**」を選択します。必要に応じて、編集可能な属性フィールドを変更します。フィールドについては、A-8 ページの表 A-11 を参照してください。
7. 「**IP のロックアウト**」タブ・ページを選択した後、フィールドを変更する場合は「**IP のロックアウト**」を選択します。必要に応じて、編集可能な属性フィールドを変更します。フィールドについては、A-8 ページの表 A-12 を参照してください。
8. 「**パスワード構文**」タブ・ページを選択した後、フィールドを変更する場合は「**パスワード構文のチェック**」を選択します。必要に応じて、編集可能な属性フィールドを変更します。フィールドについては、A-8 ページの表 A-13 を参照してください。
9. 「**有効サブツリー**」タブ・ページを選択して、「**追加**」を選択します。識別名を入力するか、「**参照**」を選択し、「**識別名 (DN) パスの選択**」ウィンドウを使用して、ポリシーを適用するサブツリーにナビゲートします。
10. 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、アカウントおよびパスワードの管理

この項の項目は次のとおりです。

- 例 : コマンドライン・ツールを使用したパスワード・ポリシーの設定
- 例 : コマンドライン・ツールを使用したパスワード・ポリシーの管理
- 例 : コマンドライン・ツールを使用したアカウントの有効化と無効化
- 例 : コマンドライン・ツールを使用したアカウントのロック解除
- 例 : コマンドライン・ツールを使用したパスワードの強制変更

例 : コマンドライン・ツールを使用したパスワード・ポリシーの設定

次の例は、`pwdLockout` 属性を無効にして、その値をデフォルト設定（`1`）から変更します。

ファイル `my_file.ldif` の内容は、次のとおりです。

```
dn: cn=default,cn=pwdPolicies,cn=common,cn=products,cn=OracleContext,
 o=my_company,dc=com
changetype:modify
replace: pwdlockout
pwdlockout: 0
```

次のコマンドでこのファイルをディレクトリにロードします。

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

例 : コマンドライン・ツールを使用したパスワード・ポリシーの管理

次に、コマンドライン・ツールを使用してレルムのパスワード・ポリシーを表示および変更する方法を示します。

例 : コマンドライン・ツールを使用したパスワード・ポリシーの表示 次の例では、特定のパスワード・ポリシー・エントリを取得します。

```
ldapsearch -p port -h host \
           -b "cn=pwdPolicies,cn=common,cn=products,cn=OracleContext, \
               o=my_company,dc=com" \
           -s sub "(objectclass=pwdpolicy)"
```

次の例では、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 port -h host -b " " -s sub "(objectclass=pwdpolicy)"
```

例 : コマンドライン・ツールを使用したパスワード・ポリシーの変更 次の例では、パスワード・ポリシー・エントリを変更します。

```
ldapmodify -p port -h host -w <<EOF
dn: cn=default,cn=pwdPolicies,cn=common,cn=products,cn=OracleContext,
 o=my_company,dc=com
changetype: modify
replace: pwdMaxAge
pwdMaxAge: 10000
EOF
```

例 : コマンドライン・ツールを使用したアカウントの有効化と無効化

コマンドライン・ツールを使用して、ユーザー・アカウントを一時的に無効にし、その後再び有効にすることができます。

アカウントを永続的に無効にするには、orclisenabled 属性を DISABLED に設定します。この属性に他の値を設定すると、アカウントは有効になります。

アカウントを無効にした後、有効にするには、この属性をエントリから削除します。

特定の期間、アカウントを有効にするには、ユーザー・エントリ内の orclActiveStartDate および orclActiveEndDate 属性を、**UTC** 書式による適切な値に設定します。たとえば、次のようにします。

```
cn=John Doe,cn=users,o=my_company,dc=com
orclactivestartdate:20030101000000z
orclactiveenddate: 20031231000000z
```

この例で、John Doe は、2003 年 1 月 1 日から 2003 年 12 月 31 日までの期間ログインできます。2003 年 1 月 1 日より前、または 2003 年 12 月 31 日より後はログインできません。特定の期間 John Doe のアカウントを無効にする場合は、orclisenabled 属性を FALSE に設定する必要があります。

例 : コマンドライン・ツールを使用したアカウントのロック解除

セキュリティ管理者グループのメンバーの場合、ユーザーのパスワードを再設定せずに、アカウントのロックを解除できます。これによって、ユーザーに新規パスワードを明示的に知らせる必要がなくなります。ユーザーは、旧パスワードを使用してログインできます。

アカウントのロックを解除するには、orclpwdaccountunlock 属性を 1 に設定します。

次の例では、John Doe というユーザーのアカウントのロックを解除します。

```
ldapmodify -p port -h host -D cn=orcladmin -w welcome -v <<EOF
dn: cn=John Doe,cn=users,o=my_company,dc=com
changetype: modify
add: orclpwdaccountunlock
orclpwdaccountunlock: 1
EOF
```

例 : コマンドライン・ツールを使用したパスワードの強制変更

ユーザーが初めてログインする場合、ユーザーに対してパスワードの変更を強制できます。これを行うには、pwdpolicy エントリ内の pwdMustChange 属性を TRUE に設定し、パスワードを再設定します。この場合、ユーザーがログインしてパスワードを変更できるように、ユーザーに新しいパスワードを明示的に通知する必要があります。

> **関連項目 :** パスワードを再設定する方法については、19-14 ページの「Oracle Internet Directory セルフ・サービス・コンソールを使用したパスワードの再設定」を参照してください。

セルフ・サービス・コンソールを使用したアカウントおよびパスワードの管理

この項では、次の操作を行うための Oracle Internet Directory セルフ・サービス・コンソールの使用方法を説明します。

- アカウントの有効化および無効化
- アカウントのロック解除
- パスワードの再設定

Oracle Internet Directory セルフ・サービス・コンソールを使用したアカウントの有効化と無効化

Oracle Internet Directory セルフ・サービス・コンソールを使用して、ユーザー・アカウントを一時的に無効にし、その後再び有効にできます。

> **関連資料 :** Oracle Internet Directory セルフ・サービス・コンソールを使用したアカウントの有効化および無効化の方法は、『Oracle Identity Management 委任管理ガイド』のアカウントの管理に関する項を参照してください。

Oracle Internet Directory セルフ・サービス・コンソールを使用したアカウントのロック解除

セキュリティ管理者グループのメンバーの場合、アカウントがロックされると、ユーザーのパスワードを再設定せずに、アカウントのロックを解除できます。これによって、ユーザーに新規パスワードを明示的に知らせる必要がなくなります。ユーザーは、旧パスワードを使用してログインできます。

> **関連資料：** Oracle Internet Directory セルフ・サービス・コンソールを使用したアカウントのロック解除方法は、『Oracle Identity Management 委任管理ガイド』のアカウントの管理に関する項を参照してください。

Oracle Internet Directory セルフ・サービス・コンソールを使用したパスワードの再設定

パスワードを忘れた場合や、アカウントがロックアウトされた場合は、パスワードを再設定できます。この場合、パスワード検証属性セットに値を入力して、サーバーに対して本人確認を行う必要があります。この操作は、以前回答を指定したパスワードのヒントの質問に答えるという形をとります。

> **関連資料：** Oracle Internet Directory セルフ・サービス・コンソールを使用したパスワードの再設定方法は、『Oracle Identity Management 委任管理ガイド』のパスワードを忘れた場合の再設定に関する項を参照してください。

パスワード・ポリシーのエラー・メッセージ

パスワード・ポリシー違反が発生すると、ディレクトリ・サーバーはクライアントに様々なエラーおよび警告メッセージを送信します。Oracle Internet Directory 10*g*（10.1.4.0.1）では、クライアントが ldapbind または ldapcompare 操作の一部としてパスワード・ポリシー・リクエスト制御を送信する場合にのみ、ディレクトリ・サーバーはこれらのメッセージを LDAP 制御として送信できます。クライアントがリクエスト制御を送信しない場合、ディレクトリ・サーバーは、レスポンス制御を送信しません。かわりに、追加情報の一部としてエラーおよび警告を送信します。

> **関連項目：** エラー・メッセージのリストおよびそれらのエラーを解決する方法は、L-8 ページの「パスワード・ポリシーに関するトラブルシューティング」を参照してください。

20

パスワード・ベリファイアのディレクトリ格納

パスワード・ベリファイアは、Oracle Internet Directory 以外の Oracle コンポーネントに対してユーザーを認証するために使用するセキュリティ資格証明です。この章では、Oracle Internet Directory でこれらのパスワード・ベリファイアを集中的に格納する方法について説明します。

この章の項目は次のとおりです。

ユーザー認証資格証明の集中格納の概要

退職または役職が変わったユーザーの権限は、その当日に変更して、古くなった未使用のアカウントや権限が誤使用されないようにする必要があります。ユーザー・アカウントとパスワードが複数のデータベースに分散される大企業では、パスワードが集中管理されていないと、管理者が万全なセキュリティに必要な速度で変更を実行できない可能性があります。

Oracle Internet Directory では、セキュリティ資格証明を集中的に格納して、エンド・ユーザーと管理者が簡単に管理できるようにします。このコンポーネントで格納される情報は、次のとおりです。

- ディレクトリ自体に対する認証ユーザーのパスワード
- その他の Oracle コンポーネントに対する認証ユーザーのパスワード・ベリファイア

Oracle 以外のアプリケーションがディレクトリ対応の場合、ユーザーは非 Oracle の認証資格証明を格納できます。これらのアプリケーションは、製品エントリの下に独自のコンテナを作成する必要があります。

Oracle Internet Directory に対する認証用パスワード・ベリファイアの格納および管理

Oracle Internet Directory では、ユーザーのディレクトリ・パスワードを `userPassword` 属性に格納します。Oracle Internet Directory でサポートされるハッシング・アルゴリズムの 1 つを使用して、パスワードを一方向ハッシュ値の BASE64 エンコーディング文字列で格納することで、このパスワードを保護できます。パスワードを暗号値ではなく一方向ハッシュ値として格納することによって、パスワードのセキュリティが向上します。これは、悪意のあるユーザーにはこれらの値を読むことも復号化することもできないためです。

Oracle Internet Directory のデフォルトの userPassword ハッシング・アルゴリズムは、MD4 から SHA-1 に変更されました。このデフォルト・スキームは、新規のインストールに対してのみ有効です。新規のインストール後に作成されたすべての `userPassword` 属性は、SHA-1 を使用した一方向ハッシュであり、Oracle Internet Directory に格納されます。アップグレードを実行する場合、アップグレードを行う前のデフォルトのハッシング・スキームは保持されます。たとえば、アップグレード前のデフォルト・スキームが MD4 であった場合、アップグレード後のデフォルト・スキームも MD4 になります。`userPassword` のセキュリティを強化するには、アップグレード後、ただちにデフォルト・スキームを SHA-1 に変更します。デフォルト・スキームを SHA-1 に変更しても、ユーザー・ログインには影響しません。セキュリティを強化するため、ユーザーは SHA-1 値のハッシュ値が Oracle Internet Directory に格納されるように、パスワードをリセットする必要があります。

Oracle Internet Directory では、ユーザー・パスワードを `orclrevpwd` という操作属性に可逆暗号化形式で格納します。この属性は、パスワード・ポリシー・エントリの属性 `orclpwdencryptionenable` が `1` に設定されている場合にのみ生成されます。`orclrevpwd` 属性は、SSL サーバー認証メカニズムおよび SSL クライアントとサーバー認証メカニズムでのみ問合せが可能です。非 SSL セッションでは、この属性の問合せはできません。

この項の項目は次のとおりです。

- パスワード・ベリファイアおよびディレクトリに対する認証
- パスワード・ベリファイアを作成するためのハッシング・スキーム
- Oracle Directory Manager を使用したパスワード保護の管理
- ldapmodify を使用したパスワード保護の管理

パスワード・ベリファイアおよびディレクトリに対する認証

ディレクトリ・サーバーへの認証時、クライアントはパスワードをクリアテキストでディレクトリ・サーバーに提供します。ディレクトリ・サーバーは、**DSE** 属性の `userpassword` に指定されているハッシング・アルゴリズムを使用して、このパスワードをハッシュします。次に、このハッシュされたパスワードをバインド・エントリの `userPassword` 属性に保存されているハッシュ済パスワードと照合します。ハッシュされたパスワードの値が一致した場合、サーバーはユーザーを認証します。ハッシュされたパスワードの値が一致しない場合、サーバーは「無効な資格証明」のエラー・メッセージをユーザーに送信します。

外部ユーザーに対しては、Oracle Internet Directory は認証中に属性 `orclrevpwd` を生成します。特に、クライアントがクリアテキスト形式のユーザー・パスワードで `ldapcompare` を使用して認証を行う場合に、この属性が生成されます。属性 `orclrevpwd` が存在しない場合、Oracle Internet Directory サーバーは、認証用に提供されたクリアテキスト形式のパスワードを使用してこの属性を生成します。ただし、外部ユーザーが `ldapbind` を使用して Oracle Internet Directory に対して認証される場合、この属性は生成されません。

パスワード・ベリファイアを作成するためのハッシング・スキーム

インストール時に Oracle Universal Installer によって、ディレクトリに対するユーザーのパスワードを保護する一方向ハッシング・スキームの設定をユーザーに求めるプロンプトが表示されます。次のオプションがあります。

- **MD4**: 128 ビットのハッシュまたはメッセージ・ダイジェスト値を生成する一方向ハッシュ関数です。
- **MD5**: MD4 が改善された、より複合的なバージョンです。
- **SHA**: Secure Hash Algorithm。MD5 よりも長い 160 ビットのハッシュを生成します。このアルゴリズムは MD5 よりも若干速度が遅くなりますが、大きなメッセージ・ダイジェストによって、総当たり攻撃や反転攻撃に対処できます。
- SSHA: Salted セキュア・ハッシュ・アルゴリズム。SHA と類似していますが、パスワードにランダムな salt 文字を使用して生成します。
- SMD5: Salted MD5。MD5 と類似していますが、パスワードにランダムな salt 文字を使用して生成します。
- **UNIX Crypt**: UNIX ハッシング・アルゴリズムです。

インストール時に指定するハッシング・アルゴリズムの値は、**ルート DSE** の `orclCryptoScheme` 属性に格納されます。その値を変更するには、Oracle Directory Manager または ldapmodify のいずれかを使用します。

Oracle Directory Manager を使用したパスワード保護の管理

Oracle Directory Manager を使用してパスワード保護を管理するには、スーパーユーザーである必要があります。

Oracle Directory Manager を使用してパスワード保護のタイプを変更する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」を展開して、パスワード・ハッシングをリセットするディレクトリ・サーバー・インスタンスを選択します。そのディレクトリ・サーバーに対応するタブ・ページが右側のペインに表示されます。
2. 「**システム操作属性**」タブ・ページの「**暗号化パスワード**」フィールドで、使用するパスワード保護のタイプを選択します。オプションは次のとおりです。
   - MD4
   - MD5
   - 暗号化なし
   - SHA
   - UNIX Crypt
   - SSHA
   - SMD5
3. 「**適用**」を選択します。

注意：「暗号化なし」オプションを選択すると、ユーザー・パスワードがクリアテキストで保存されます。

---

ldapmodify を使用したパスワード保護の管理

次の例は、`my_ldif_file` という名前の LDIF ファイルを使用してパスワード・ハッシング・アルゴリズムを SHA に変更します。

```
ldapmodify -D cn=orcladmin -w welcome -h myhost -p 389 -v -f my_ldif_file
```

LDIF ファイル `my_ldif_file` の内容は、次のとおりです。

```
dn:
changetype: modify
replace: orclcryptoscheme
orclcryptoscheme: SHA
```

関連項目： 16-7 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」

Oracle コンポーネントに対する認証用パスワード・ベリファイアの格納および管理

Oracle コンポーネントは、パスワードとパスワード・ベリファイアの両方を Oracle Internet Directory に格納します。この項の項目は次のとおりです。

Oracle コンポーネント用のパスワード・ベリファイアの概要

Oracle コンポーネントは、それぞれのコンポーネントのパスワード値をパスワード・ベリファイアとして Oracle Internet Directory に格納できます。パスワード・ベリファイアとは、クリアテキストのパスワードをハッシュしたバージョンで、このバージョンは BASE64 エンコーディング文字列としてエンコードされます。

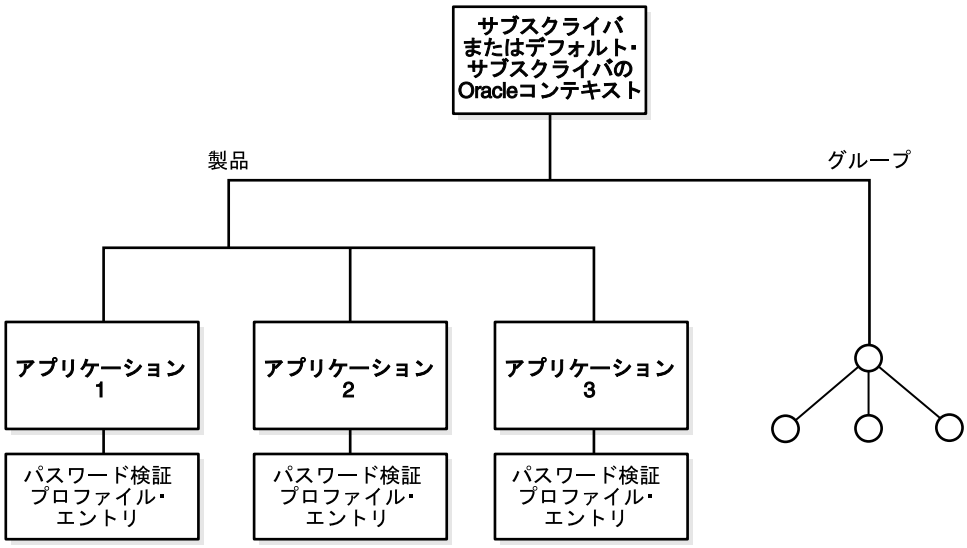
次のいずれかのハッシング・アルゴリズムを使用して、パスワード・ベリファイアを導出できます。

- **MD5**: MD4 が改善された、より複合的なバージョンです。
- **SHA**: Secure Hash Algorithm。**MD5** よりも長い 160 ビットのハッシュを生成します。このアルゴリズムは MD5 よりも若干速度が遅くなりますが、大きなメッセージ・ダイジェストによって、総当たり攻撃や反転攻撃に対処できます。
- SSHA および SMD5。
- **UNIX Crypt**: UNIX ハッシング・アルゴリズムです。
- SASL/MD5: Simple Authentication and Security Layer/MD5。接続ベースのプロトコルに認証サポートを追加し、チャレンジ / レスポンス・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。チャレンジ / レスポンス・プロトコルを使用する点で SASL/MD5 と似ています。
- ORCLWEBDAV: SASL/MD5 と同じ専用アルゴリズムで、`username@realm` の形式でユーザー名を取得します。
- ORCLLM: SMBLM アルゴリズムの Oracle 表現です。SMBLM アルゴリズムは、SMB/CIFS チャレンジ / レスポンス認証アルゴリズムの LM 改良型 Oracle 表現です。
- ORCLLM: SMBLM アルゴリズムの Oracle 表現です。SMBNT アルゴリズムは、SMB/CIFS チャレンジ / レスポンス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 20-1 に示すように、このエントリは、レルム固有の Oracle コンテキストの下にある製品エントリ下のアプリケーション・エントリの直下に配置されます。

このベリファイア・プロファイル・エントリは、指定されたレルム内のユーザーのみに適用されます。ベリファイアの生成を適切に行うには、レルム固有の Oracle コンテキストの共通エントリの `orclcommonusersearchbase` 属性に適切な値を設定する必要があります。

図 20-1 パスワード検証プロファイル・エントリの位置



パスワード・ベリファイアを格納するための属性

ディレクトリと Oracle コンポーネントの両方とも、ユーザー・パスワードをユーザー・エントリに格納しますが、格納する属性は異なります。ディレクトリは、userPassword 属性にユーザー・パスワードを格納しますが、Oracle コンポーネントは、ユーザー・パスワード・ベリファイアを authPassword、orclPasswordVerifier または orclpassword 属性に格納します。Oracle コンポーネントで使用する各属性の説明は、表 20-1 を参照してください。

表 20-1 ユーザー・エントリにパスワード・ベリファイアを格納するための属性

属性	説明
authPassword	パスワードが、ディレクトリに対してユーザー認証を行うために使用するパスワード userpassword と同じ場合に、パスワードを Oracle コンポーネントに格納するための属性。この属性の値は、userpassword 属性の値と同期します。 複数の異なるアプリケーションで、ディレクトリに使用したクリアテキスト・パスワードと同じパスワードの入力をユーザーに要求できます。ただし、各アプリケーションでは、異なるアルゴリズムを使用してそのパスワードがハッシュされる場合があります。この場合は、同じクリアテキスト・パスワードが、複数の異なるパスワード・ベリファイアのソースとなります。 この属性は複数値の属性であるため、異なるアプリケーションがこのユーザーのクリアテキスト・パスワードに対して使用する他のすべてのベリファイアを格納できます。userpassword 属性を変更すると、すべてのアプリケーションの authpasswords が再生成されます。
orclPasswordVerifier	パスワードが、ディレクトリに対してユーザー認証を行うために使用するパスワード userpassword と異なる場合に、パスワードを Oracle コンポーネントに格納するための属性。この属性の値は、userpassword 属性の値とは同期しません。 authPassword と同様に、この属性は複数値の属性であるため、異なるアプリケーションがこのユーザーのクリアテキスト・パスワードに対して使用する他のすべてのベリファイアを格納できます。

表 20-1 ユーザー・エントリにパスワード・ベリファイアを格納するための属性（続き）

属性	説明
orclPassword	エンタープライズ・ユーザー用の 03LOGON ベリファイアのみを格納するための属性。03LOGON ベリファイアは、userpassword 属性と同期し、デフォルトでは、orcluserv2 オブジェクト・クラスに関連付けられたすべてのユーザー・エントリに対して生成されます。 Oracle Internet Directory をインストールすると、デフォルトではルート Oracle コンテキストにデータベース・セキュリティ・プロファイルのエントリが作成されます。このエントリの存在によって、orcluserv2 オブジェクト・クラスに関連付けられたユーザー・エントリを対象とする 03LOGON ベリファイアが生成されます。

これらの属性の型には、属性サブタイプとして appID があります。この属性サブタイプで特定のアプリケーションを一意に識別します。たとえば、appID はアプリケーション・エントリの ORCLGUID にできます。この属性サブタイプは、アプリケーションのインストール時に生成されます。

20-8 ページの図 20-2 では、様々な Oracle コンポーネントがそれぞれのパスワード・ベリファイアを Oracle Internet Directory に格納しています。Oracle Application Server Single Sign-On では、ディレクトリに対するパスワードと同じパスワードを使用するため、パスワードは authPassword 属性に格納されます。その他のアプリケーションでは、ディレクトリに対するパスワードとは異なるパスワードを使用するため、それぞれのベリファイアが orclPasswordVerifier 属性に格納されます。

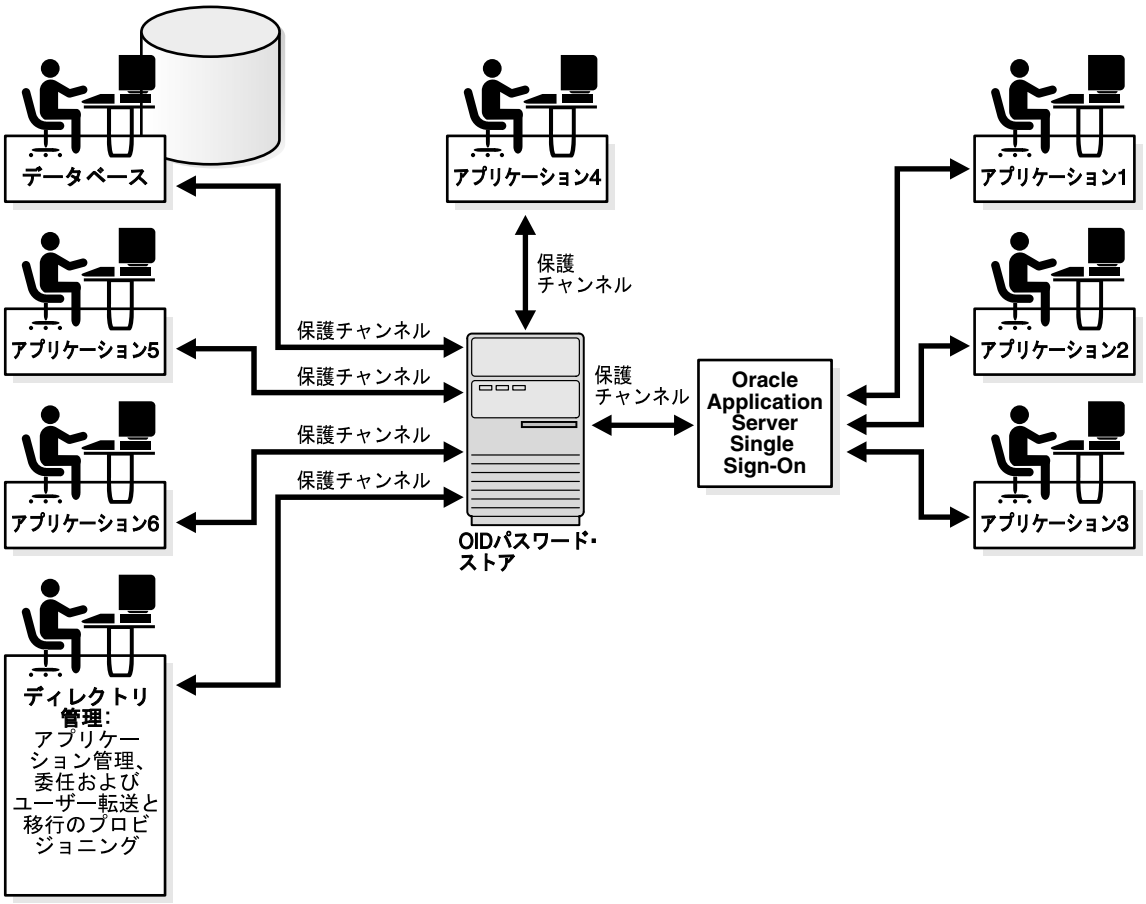
次の記述は、アプリケーション固有のベリファイア・プロファイルの例です。共通のベリファイア・フレームワークを使用しないことを選択したアプリケーションでは、次の例のように、固有のベリファイア・プロファイル・エントリを作成する必要があります。orclappid はアプリケーション・コンテナの GUID に設定され、ベリファイア属性 authpassword および orclpasswordverifier のサブタイプとしても使用されます。

```
dn: cn=IFSVerifierProfileEntry,cn=IFS,cn=Products,cn=OracleContext,o=Oracle,dc=com
objectclass:top
objectclass:orclpwdverifierprofile
cn:IFSVerifierProfileEntry
orclappid:8FF2DFD8203519C0E034080020C34C50
orclpwdverifierparams;authpassword: crypto:SASL/MDS $ realm:dc=com
orclpwdverifierparams;orclpasswordverifier: crypto:ORCLLM
orclpwdverifierparams;authpassword: crypto:ORCLWEBDAV $ realm:dc=com
$ usernameattribute: mail
$ usernamecase: lower
$ nodomain: TRUE
```

SASL/MD5 および ORCLWEBDAV ベリファイアは、ユーザー名、レルムおよびパスワードを使用して生成されます。使用するユーザー名属性は、ベリファイア・プロファイル・エントリで指定できます。ユーザー名は大文字でも小文字でも指定できます。ORLWEBDAV ベリファイアは、ユーザー名に ID 管理レルムの名前を追加して生成されます。レルムの名前を追加して生成する必要がない場合、ベリファイア・プロファイル・エントリでは nodomain: TRUE を指定する必要があります。

前述の例では、ORCLWEBDAV ベリファイアは、レルムの名前を追加せずに mail 属性の値を使用して生成されます。また、ユーザー名はベリファイアが生成される前に小文字に変換されます。

図 20-2 認証モデル



Oracle コンポーネントのデフォルトのベリファイア

各 Oracle コンポーネントのプロファイルを作成する必要をなくし、すべてのコンポーネントでパスワード・ベリファイアを共有できるようにするために、Oracle Internet Directory にはパスワード・ベリファイアのデフォルト・セットが用意されています。デフォルトのベリファイアには、MD5、MD5-IFS（ユーザー名がニックネーム属性の値に設定され、レルムが Authorized_Users に設定された SASL/MD5）、WEBDAV、ORCLLM および ORCLNT のタイプがあります。

2 つのプロファイル・エントリが必要です。1 つは数値のみを使用する個人識別番号（PIN）を使用するアプリケーション用、もう 1 つは英数字のパスワードを使用するアプリケーション用です。

PIN ベースのアプリケーション用ベリファイア（たとえば、OracleAS Unified Messaging のボイス・メール）は、`orclpasswordverifier;orclcommonpin` 属性に格納されます。サブタイプ `orclcommonpin` は、数値の PIN と英数字のパスワードを区別するために使用されます。数値の PIN を使用するアプリケーションでは、`orclpasswordverifier;orclcommonpin` 属性に対して直接に問合せや比較ができます。

英数字パスワード・ベースのアプリケーション用ベリファイア（たとえば、Oracle Internet File System）は、次のいずれかに格納されます。

- `authpassword;orclcommonpwd` 属性 : アプリケーションがそのベリファイアと `userpassword` 属性を同期する必要がある場合
- `orclpasswordverifier;orclcommonpwd` 属性 : `userpassword` 属性との同期が必要ない場合

サブタイプ orclcommonpwd は、数値の PIN と英数字のパスワードを区別するために使用されます。サブタイプが付いたベリファイア属性は、問合せが可能です。

これらのプロファイル・エントリには、サブスクライブ・アプリケーションのリストも含まれ、これらのアプリケーションは、プロファイル・エントリ内で uniquemember 属性の値として指定されます。デフォルトでは、Oracle Application Server Single Sign-On 識別情報の DN がサブスクライブ・アプリケーションの 1 つになっています。これは、Oracle Application Server Single Sign-On が、すべてのパートナ・アプリケーションのプロキシ・メンバーであることを示しています。Oracle Application Server Single Sign-On に基づいていないすべてのアプリケーションで、適切なプロファイル・エントリ内の uniquemember 属性に識別子（DN）を追加する必要があります。

次に、プロファイル・エントリの例を示します。

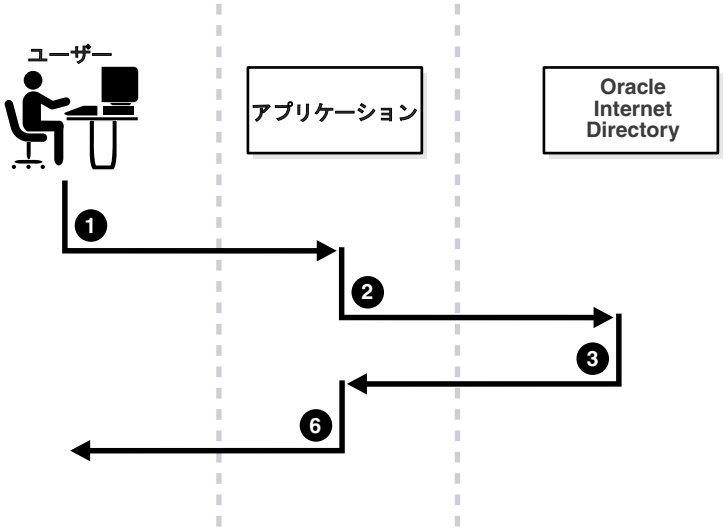
```
Cn=defaultSharedPwdProfileEntry, cn=common, cn=products, cn=oraclecontext
Objectclass: orclpwdverifierprofile
Cn: orclcommonpwdprofileentry
Orclappid: orclcommonpwd
Orclpwdverifierparams;authpassword: crypto:SASL/MD5 $ realm:Authorized_Users
Orclpwdverifierparams;authpassword: crypto:ORCLWEBDAV $ realm:Authorized_Users
Orclpwdverifierparams;authpassword: crypto:ORCLLM
Orclpwdverifierparams;authpassword: crypto:ORCLNT
Orclpwdverifierparams;orclpasswordverifier: crypto:SSHA
Uniquemember: cn=SSO,cn=Products,cn=OracleContext
Uniquemember: cn=IFS,cn=Products,cn=OracleContext

Cn=defaultSharedPINProfileEntry, cn=common, cn=products, cn=oraclecontext
Objectclass: orclpwdverifierprofile
Cn: orclcommonpinprofileentry
Orclappid: orclcommonpin
Orclpwdverifierparams;orclpasswordverifier: crypto:MD5
Orclpwdverifierparams;orclpasswordverifier: crypto:SSHA
Uniquemember: cn=SSO,cn=Products,cn=OracleContext
Uniquemember: cn=Unified Messaging,cn=Products,cn=OracleContext
```

PIN ベースのアプリケーションでは、authpassword はオプションではありません。orclpasswordverifier 属性が使用されます。

例 : Oracle コンポーネントに対するパスワード検証の動作

図 20-3 に、Oracle コンポーネントに対するパスワード検証の例を示します。この例の Oracle コンポーネントは、パスワード・ベリファイアをディレクトリに格納します。

図 20-3 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リクエストします。
3. ディレクトリ・サーバーは、次のように動作します。
   a. 特定のアプリケーションに指定されているハッシング・アルゴリズムを使用して、パスワード・ベリファイアを生成します。
   b. 次に、生成したパスワード・ベリファイアをディレクトリ内の対応するパスワード・ベリファイアと比較します。比較操作が成功した場合、アプリケーションは、ベリファイア属性のサブタイプとしてその `appID` を指定する必要があります。たとえば、次のようにします。

      ```
      ldapcompare -p389 -D "DN_of_the_appplication_entity" -w "password" \
                  -b "DN_of_the_user" -a orclpasswordverifier; appID \
                  -v password_of_the_user
      ```

   c. 比較操作の結果をアプリケーションに通知します。
4. アプリケーションは、ディレクトリ・サーバーからのメッセージに従って、ユーザーを認証または否認します。

アプリケーションは、比較操作を使用しない場合、次のように動作します。

1. ユーザーが入力したクリアテキスト・パスワードをハッシュします。
2. ユーザーが入力したクリアテキスト・パスワードのハッシュ値をディレクトリから取り出します。
3. クライアントが応答するユーザーへのチャレンジを開始します。レスポンスが適切な場合、アプリケーションはユーザーを認証します。

Oracle Directory Manager を使用した Oracle コンポーネント用パスワード検証プロファイルの管理

Oracle Directory Manager を使用して、パスワード検証プロファイル・エントリを表示および変更できます。

Oracle Directory Manager を使用した Oracle コンポーネント用パスワード検証プロファイルの表示と変更

アプリケーションのパスワード・ベリファイアを表示する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」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. 「**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表示されます。
   - 「**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表示されます。
3. 表示するパスワード・ベリファイアを選択します。選択したパスワード・ベリファイアが「パスワード検証プロファイル」ダイアログ・ボックスに表示されます。このダイアログ・ボックスのフィールドの説明は、A-9 ページの表 A-14 を参照してください。
4. パスワード・ベリファイアの生成に使用するハッシング・アルゴリズムを「パスワード検証プロファイル」ダイアログ・ボックスで変更するには、「**Oracle パスワード・パラメータ**」フィールドに新しい値を入力します。

コマンドライン・ツールを使用した Oracle コンポーネント用パスワード検証プロファイルの管理

コマンドライン・ツールを使用して、パスワード・ベリファイア・プロファイルを表示および変更できます。

コマンドライン・ツールを使用したパスワード検証プロファイルの表示

アプリケーションのパスワード・ベリファイアを表示するには、パスワード検証プロファイルの識別名を指定して検索を実行します。

例 : コマンドライン・ツールを使用したパスワード検証プロファイルの変更

この例では、アプリケーションのパスワード検証プロファイル・エントリのハッシング・アルゴリズムを変更します。このパスワード・ベリファイアは、ユーザーのディレクトリ・パスワードと同期しています。

```
ldapmodify -p 389 -h my_host -v <<EOF
dn: cn=MyAppVerifierProfileEntry,cn=MyApp,cn=Products,cn=OracleContext,
 o=my_company,dc=com
changetype: modify
replace: orclPwdVerifierParams
orclPwdVerifierParams;authPassword: crypto:SASL/MD5 $ realm:dc=com
EOF
```

動的パラメータを使用したベリファイアの生成

前述のパスワード・ベリファイアは、静的パスワード・ベリファイアです。つまり、通常アプリケーションのインストール中に、事前構成されたパラメータから生成されたベリファイアです。一部のアプリケーション（Oracle Calendar、Oracle Email および Oracle Wireless and Voice など）では、Oracle Internet Directory が動的パスワード・ベリファイアを生成する必要があります。

この項の項目は次のとおりです。

動的パスワード・ベリファイアの生成

Oracle Internet Directory は、アプリケーションが動的パスワード・ベリファイアをリクエストした場合に、これを生成します。動的ベリファイアは、アプリケーションの実行時に使用可能になるアプリケーション・パラメータに基づいています。

Oracle Internet Directory が動的パスワード・ベリファイアを生成するには、以前に可逆暗号化形式で格納されたユーザー・パスワードが必要です。Oracle Internet Directory では、これらの値を操作属性 `orclrevpwd` および `orclunsyncrevpwd` に格納します。`userpassword` に基づいて暗号化された値は、`orclrevpwd` パラメータに格納されます。Oracle Calendar で使用される数値の PIN など、`userpassword` 以外のパスワードに基づいて暗号化された値は、パラメータ `orclunsyncrevpwd` に格納されます。

動的パスワード・ベリファイアを生成するための Oracle Internet Directory の構成

`userpassword` を使用し、動的パスワード・ベリファイアを必要とするアプリケーションを配置する場合、Oracle Internet Directory が `orclrevpwd` パラメータを生成することを確認する必要があります。レルムのパスワード・ポリシー・エントリの属性 `orclpwdencryptionenable` が `1` に設定されている場合、ユーザーをプロビジョニングすると、Oracle Internet Directory は属性 `orclrevpwd` を生成します。したがって、ユーザーをプロビジョニングする前に、`orclpwdencryptionenable` を `1` に設定する必要があります。`orclpwdencryptionenable` を設定する前にユーザーをプロビジョニングした場合には、かわりにすべてのユーザーのユーザー・パスワードをリセットし、暗号化された値を生成する必要があります。

数値の PIN を使用し、動的パスワード・ベリファイアを必要とするアプリケーションを配置する場合、`orclunsyncrevpwd` に格納される値を生成するために、Oracle Internet Directory が暗号タイプ `3DES` を使用可能であることを確認する必要があります。`3DES` を、ルート Oracle コンテキスト下の共通ベリファイア・プロファイル・エントリの属性 `orclpwdverifierparams;orclpasswordverifier` の値として指定する必要があります。このエントリのデフォルトの識別名は `cn=DefaultSharedPINProfileEntry,cn=Common,cn=Products, cn=OracleContext` です。値を設定するには、次を指定します。

```
dn: cn=DefaultSharedPinProfileEntry, cn=Common,
    cn=Products, cn=Oraclecontext
cn: DefaultSharedPinProfileEntry
orclappid: orclcommonpin
orclpwdverifierparams;orclpasswordverifier: crypto:MD5
orclpwdverifierparams;orclpasswordverifier: crypto:3DES
```

21

Oracle テクノロジ配置のための権限の委任

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

この章の項目は次のとおりです。

Oracle Identity Management モデルでの委任

Oracle Identity Management を使用すると、ユーザー、グループおよびサービスのすべてのデータを 1 つのリポジトリに格納し、各データ・セットに特定の管理者を割り当てることができます。Oracle Identity Management は、集中型のリポジトリとカスタマイズされた委任アクセスの両方を提供するため、安全でスケーラブルです。

この項の項目は次のとおりです。

委任の機能

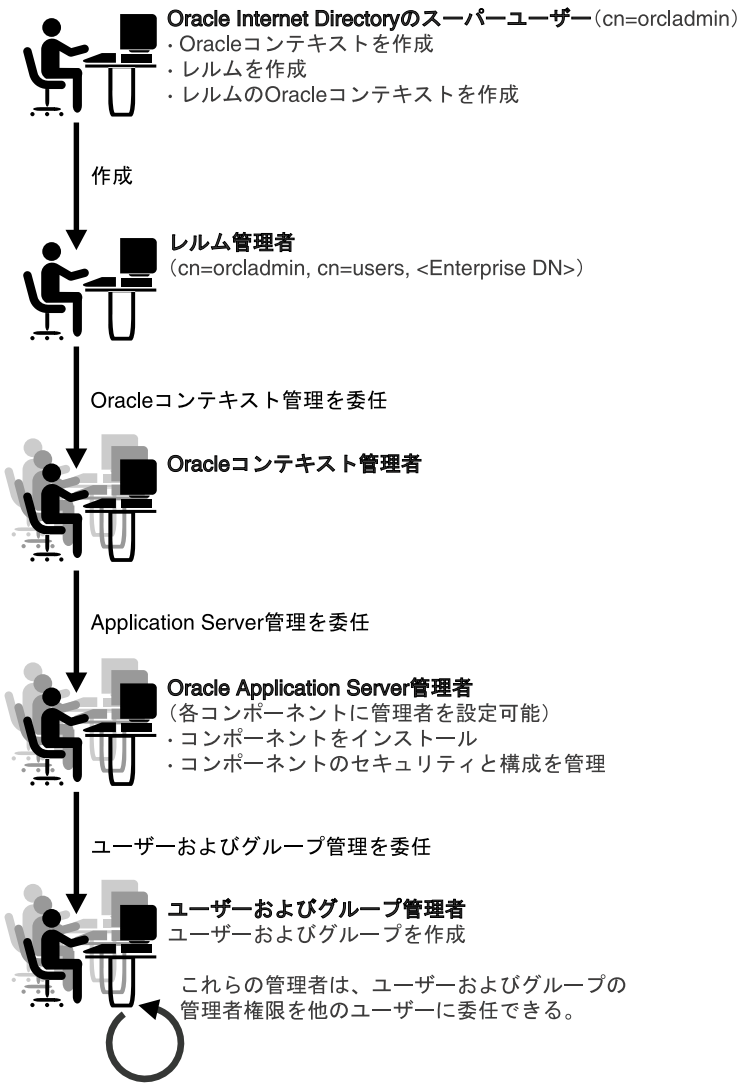
委任モデルを使用すると、グローバル管理者は、ホスティングされた企業の ID 管理レルムを作成し、管理する権限をレルム管理者に委任できます。一方、レルム管理者は、アプリケーション用パスワード、個人データおよび作業環境を変更する権限をエンド・ユーザーおよびグループに委任できます。このようにして、各タイプのユーザーに、適切なレベルの権限を与えることができます。

必要な権限を委任するには、ユーザーを適切な管理グループに割り当てます。たとえば、エンタープライズ・ユーザーと電子メール・サービスに関するデータの両方をディレクトリに格納し、それぞれのデータ・セットに一意の管理者を割り当てる必要があるとします。ユーザーをエンタープライズ・ユーザーの管理者として指定するには、そのユーザーをエンタープライズ・ユーザー管理者グループなどに割り当てます。ユーザーを電子メール・サービスの管理者として指定するには、そのユーザーを電子メール・サービス管理者グループなどに割り当てます。

Oracle Application Server 環境での委任

図 21-1 に、Oracle Application Server 環境での委任の流れを示します。

図 21-1 Oracle Application Server 環境での委任の流れ



21-3 ページの図 21-1 に示すように、Oracle Application Server 環境では、ディレクトリのスーパーユーザー（`cn=orcadmin`）は次の項目を作成します。

- Oracle コンテキスト
- レルム
- レルム固有の Oracle コンテキスト
- レルム管理者用のエントリ（`cn=orcladmin`、`cn=users`、*`Enterprise DN`*）

一方、レルム管理者は、Oracle コンテキスト管理者グループにユーザーを割り当てることで、Oracle コンテキストの管理を特定のユーザーに委任します。その後、Oracle コンテキスト管理者は、Oracle Application Server 管理者グループにユーザーを割り当てることで、Oracle Application Server の管理を 1 人以上のユーザーに委任します。Oracle Application Server の管理者は、Oracle Application Server コンポーネントをインストールおよび管理し、ユーザーやグループのデータ管理をユーザーおよびグループの管理者グループに委任します。ユーザーお

よびグループの管理者は、ユーザーおよびグループを作成します。他のユーザーにユーザーおよびグループの管理者権限を付与することもできます。

デフォルトの構成について

Oracle Internet Directory を初めてインストールすると、デフォルトの構成により、ディレクトリ情報ツリー（DIT）内の様々なポイントでアクセス制御ポリシーが確立されます。デフォルトのアクセス制御は、この章の後半で説明するとおり、「ユーザー」および「グループ」のコンテナに配置されます。同様に、特定のディレクトリ・エンティティのデフォルトの権限についても、この章の後半で説明します。また、表 21-2 に示すように、特定のデフォルトの権限はすべての人および各ユーザーに付与されます。

表 21-1 すべての人および各ユーザーに付与されるデフォルトの権限

対象	デフォルトの権限
すべての人	ルート DSE での権限は次のとおりです。 ■ ユーザー・エントリを参照する権限 ■ userpkcs12、orcluserpkcs12hint、userpassword、orclpassword および orclpasswordverifier 以外のすべてのユーザー属性に対する検索、読取りおよび比較権限
各ユーザー	`userpassword`、`orclpassword` および `orclpasswordverifier` 属性を含む各ユーザー独自の属性に対する完全なアクセス権

企業のセキュリティ要件を満たすように、このデフォルト構成をカスタマイズできます。

概要 : Oracle テクノロジ・スタックの管理権限

表 21-2 に、Oracle テクノロジ・スタックの管理に必要な権限を示します。

表 21-2 Oracle テクノロジ・スタックの管理権限

権限のタイプ	説明	詳細情報の参照先
ユーザーおよびグループの管理権限	これらの権限は、ID 管理インフラストラクチャを使用する Oracle コンポーネントまたはエンド・ユーザー自身のいずれかに委任されます。	21-5 ページの「ユーザーおよびグループの管理権限の委任」
配置時権限	この権限は、Oracle コンポーネントを配置するために必要です。ディレクトリ内部で適切なエントリを作成する権限や、共通リポジトリにメタデータを格納する権限を含む場合もあります。そのような権限は、OracleAS Portal 管理者などに与える必要があります。	21-10 ページの「Oracle コンポーネントの配置権限の委任」
実行時権限	この権限は、ID 管理インフラストラクチャ内の Oracle コンポーネントの実行時の対話を円滑にするために必要な権限です。ユーザー属性の表示、新規ユーザーの追加、グループ・メンバーシップの変更のための権限が含まれます。そのような権限は、各 Oracle コンポーネントに固有な管理ツールが Oracle Internet Directory 内部でエントリにアクセス、またはエントリを作成できるように、その管理ツールに対し与える必要があります。	21-12 ページの「コンポーネントの実行時権限の委任」

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

関連項目： 既存のディレクトリ構造から Oracle Application Server 環境への移行を検討している場合は、27-2 ページの「Oracle Internet Directory のデフォルトのディレクトリ構造」を参照してください。

ユーザーおよびグループの管理権限の委任

管理権限は、ID 管理インフラストラクチャを使用する Oracle コンポーネントまたはエンド・ユーザー自身のいずれかに委任されます。権限は、識別情報（ユーザーやアプリケーションなど）、またはロールやグループに対して委任できます。

この項の項目は次のとおりです。

ユーザーおよびグループのデータ管理権限の委任方法

管理権限を委任するには、Oracle Internet Directory スーパーユーザーは、次の作業を行います。

1. ID 管理レルムを作成します。
2. そのレルムでレルム管理者と呼ばれる特別なユーザーを識別します。
3. そのレルム管理者にすべての権限を委任します。

このレルム管理者は、Oracle 定義済ロール（Oracle Application Server 管理者など）に、Oracle コンポーネントが必要とする特定の権限を委任します。Oracle コンポーネントは、配置時にこれらのロールを受け取ります。

レルム管理者は、Oracle コンポーネント固有のロールに権限を委任する他に、配置に固有のロール（たとえば、ヘルプ・デスク管理者用のロール）を定義し、権限をこれらのロールに付与できます。委任された管理者は、これらのロールをさらにエンド・ユーザーに付与することができます。実際、ユーザー管理タスクの大部分はセルフ・サービス（電話番号の変更やアプリケーション固有の作業環境の指定など）に関係しているため、レルム管理者と Oracle コンポーネント管理者は、これらの権限をエンド・ユーザーに委任できます。

グループの場合、1 人以上の所有者（通常、エンド・ユーザー）を指定できます。これらの所有者に必要な管理権限が付与された場合、所有者は Oracle Internet Directory セルフ・サービス・コンソール、Oracle Directory Manager またはコマンドライン・ツールを使用してグループを管理できます。

ユーザー・データを管理するためのデフォルトの権限

ユーザーの管理には、次の権限が含まれます。

- ユーザー・エントリを作成および削除する権限
- ユーザー属性を変更する権限
- ユーザー管理を他のユーザーに委任する権限

ユーザーを作成するための**アクセス制御ポリシー・ポイント**（ACP）は、ID 管理レルムの「ユーザー」コンテナにあります。

この項では、これらの権限について説明します。

レルムに対するユーザーの作成

レルムに対してユーザーを作成するには、管理者はサブスクライバ DAS ユーザー作成グループのメンバーである必要があります。表 21-3 に、このグループの特性を示します。

表 21-3 サブスクライバ DAS ユーザー作成グループの特性

特性	説明
デフォルト ACP	デフォルトのレルムの「ユーザー」コンテナにある ACL により、レルムの Oracle コンテキストのサブスクライバ DAS ユーザー作成グループは、「ユーザー」コンテナの下でユーザーを作成できます。
管理者	Oracle Internet Directory スーパーユーザー。 Oracle コンテキスト管理者グループのメンバー。 ユーザー権限割当てグループのメンバー。 DAS 管理者グループのメンバー。 このグループの所有者。
DN	`cn=oracleDASCreateUser,cn=groups,`*`Oracle_Context_DN`*。

ユーザー属性の変更

ユーザー属性を変更するには、管理者はサブスクライバ DAS ユーザー編集グループのメンバーである必要があります。表 21-4 に、このグループの特性を示します。

表 21-4 サブスクライバ DAS ユーザー編集グループの特性

特性	説明
デフォルト ACP	デフォルトの ID 管理レルムの「ユーザー」コンテナにある ACL により、レルムの Oracle コンテキストのサブスクライバ DAS ユーザー編集グループは、ユーザーの各種属性を変更できます。
管理者	Oracle Internet Directory スーパーユーザー。 Oracle コンテキスト管理者グループのメンバー。 ユーザー権限割当てグループのメンバー。 DAS 管理者グループのメンバー。 このグループの所有者。
DN	`cn=oracleDASEditUser,cn=groups,`*`Oracle_Context_DN`*。

ユーザーの削除

レルムでユーザーを削除するには、管理者は DAS ユーザー削除グループのメンバーである必要があります。表 21-5 に、このグループの特性を示します。

表 21-5 DAS ユーザー削除グループの特性

特性	説明
デフォルト ACP	デフォルトの ID 管理レルムの「ユーザー」コンテナにある ACL により、レルムの Oracle コンテキストの DAS ユーザー削除グループは、レルムからユーザーを削除できます。
管理者	Oracle Internet Directory スーパーユーザー。 Oracle コンテキスト管理者グループのメンバー。 ユーザー権限割当てグループのメンバー。 DAS 管理者グループのメンバー。 このグループの所有者。
DN	`cn=oracleDASDeleteUser,cn=groups,`*`Oracle_Context_DN`*。

ユーザー管理の委任

委任管理者は、ディレクトリで指定された操作を実行できます。また、前述のユーザー作成、ユーザー編集、ユーザー削除の各グループにユーザーを追加する権限を必要とします。

委任管理者にユーザー管理権限を付与するには、付与する管理者がユーザー権限割当てグループのメンバーである必要があります。表 21-6 に、このグループの特性を示します。

表 21-6 ユーザー権限割当てグループの特性

特性	説明
デフォルト ACP	前述の各グループの ACL ポリシーにより、ユーザー権限割当てグループのメンバーは、これらのグループでユーザーを追加または削除することができます。
管理者	Oracle Internet Directory スーパーユーザー。 Oracle コンテキスト管理者グループ このグループの所有者。これらの所有者の識別名は、グループの `owner` 属性の値として表示されます。
DN	`cn=oracleDASUserPriv,cn=groups,`*`Oracle_Context_DN`*。

グループ・データを管理するためのデフォルトの権限

ユーザーとグループの管理には、次の権限が含まれます。

- グループ・エントリを作成および削除する権限
- グループ属性を変更する権限
- グループ管理を他のユーザーに委任する権限

グループを作成するための ACP は、ID 管理レルムの「グループ」コンテナにあります。

グループの作成

Oracle Internet Directory でグループを作成するには、管理者はグループ作成グループのメンバーである必要があります。表 21-7 に、このグループの特性を示します。

表 21-7 グループ作成グループの特性

特性	説明
デフォルト ACP	レルムの「グループ」コンテナにある ACL により、グループ作成グループは、レルムで新規グループを追加できます。
管理者	Oracle Internet Directory スーパーユーザー。 Oracle コンテキスト管理者グループのメンバー。 Oracle Application Server 管理者グループのメンバー。 グループ権限割当てグループのメンバー。 DAS 管理者グループのメンバー。 このグループの所有者。
DN	`cn=oracleDASCreateGroup,cn=groups,`*`Oracle_Context_DN`*。

グループ属性の変更

レルムの「グループ」コンテナの下のグループ属性を変更するには、管理者はグループ変更グループのメンバーである必要があります。表 21-8 に、このグループの特性を示します。

表 21-8 グループ編集グループの特性

特性	説明
デフォルト ACP	レルムの「グループ」コンテナにある ACL により、グループ編集グループは、レルムでグループの各種属性を変更できます。
管理者	Oracle Internet Directory スーパーユーザー。 Oracle コンテキスト管理者グループのメンバー。 Oracle Application Server 管理者グループのメンバー。 グループ権限割当てグループのメンバー。 DAS 管理者グループのメンバー。 このグループの所有者。
DN	`cn=oracleDASEditGroup,cn=groups,`*`Oracle_Context_DN`*。

グループの削除

グループを削除するには、管理者はグループ削除グループのメンバーであることが必要です。表 21-9 に、このグループの特性を示します。

表 21-9 グループ削除グループの特性

特性	説明
デフォルト ACP	レルムの「グループ」コンテナにある ACL により、グループ削除グループは、レルムでグループを削除できます。
管理者	Oracle Internet Directory スーパーユーザー。 Oracle コンテキスト管理者グループのメンバー。 グループ権限割当てグループのメンバー。 DAS 管理者グループのメンバー。 このグループの所有者。
DN	`cn=oracleDASDeleteGroup,cn=groups,`*Oracle_Context_DN*。

グループ管理の委任

グループの管理を他のユーザーに委任する（つまり、前述のグループ作成、グループ編集またはグループ委任の各グループでユーザーを追加または削除する）には、管理者はグループ権限割当てグループのメンバーである必要があります。表 21-10 に、このグループの特性を示します。

表 21-10 グループ権限割当てグループのメンバーの特性

特性	説明
デフォルト ACP	グループ作成、グループ編集、グループ削除の各グループの ACL ポリシーにより、グループ権限割当てグループのメンバーは、これらのグループでユーザーを追加または削除することができます。
管理者	Oracle Internet Directory スーパーユーザー。 Oracle コンテキスト管理者グループのメンバー。 グループの所有者。これらの所有者の識別名は、グループの `owner` 属性の値として表示されます。
DN	`cn=oracleDASUserPriv,cn=groups,`*Oracle_Context_DN*。

Oracle コンポーネントの配置権限の委任

この項では、Oracle コンポーネントを配置するグループについて説明します。また、これらの管理者が実行するタスクと、付与できる権限についても説明します。この項の項目は次のとおりです。

注意： Oracle Internet Directory のスーパーユーザーは、Oracle Application Server 管理者およびトラステッド・アプリケーション管理者のすべての権限を所有しています。また、Oracle Application Server 管理者グループのメンバーである必要があります。スーパーユーザーは、次の割当てを実行できます。

- ユーザーに対する Oracle Application Server 管理者ロールの割当て
- ユーザーに対するトラステッド・アプリケーション・ロールの割当て
- ユーザーに対するユーザー管理アプリケーション管理者ロールの割当て

配置権限の付与方法

管理者が Oracle コンポーネントを配置するには、スーパーユーザーは次の手順を実行します。

1. 特定の配置権限を Oracle Application Server 管理者グループなどの様々なグループに付与します。
2. 管理者をこれらの権限グループに追加します。

一方、委任管理者は、権限を他の管理者に委任できます。

Oracle Application Server 管理者

表 21-11 に、Oracle Application Server 管理者グループの特性を示します。

表 21-11 Oracle Application Server 管理者グループの特性

特性	説明
タスク	ディレクトリでリポジトリ・データベース登録エントリを作成する、リポジトリ・データベースのインストールの実行。 中間層インストールの実行。中間層をリポジトリと関連付けるには、ユーザーは特定のリポジトリ・データベースでの適切な権限が必要です。 Oracle Internet Directory でアプリケーション・エンティティを作成する、Oracle Application Server コンポーネントのインストールと構成。 この項で後述するリストに示す実行時権限のコンポーネント・エンティティへの付与。 コンポーネントが更新通知を受信できるようにするための、コンポーネントに対するプロビジョニング・プロファイルの構成。
このグループがコンポーネントに委任できる権限	パスワード、証明書および類似のセキュリティ資格証明以外の一般ユーザー属性を読み取る権限。 一般グループ属性を読み取る権限。 グループを作成、編集および削除する権限。 ユーザーを認証する権限。 アプリケーション・ベリファイアを読み取る権限。

表 21-11 Oracle Application Server 管理者グループの特性（続き）

特性	説明
管理者	Oracle Internet Directory スーパーユーザー（super user）。 Oracle コンテキスト管理者。 このグループの所有者。
DN	`cn=IASAdmins,cn=groups,`*`Oracle_Context_DN`*。

ユーザー管理アプリケーション管理者

ユーザー管理アプリケーション管理者は、Oracle Application Server 管理者グループのメンバーである必要があります。

表 21-12 に、ユーザー管理アプリケーション管理者グループの特性を示します。

表 21-12 ユーザー管理アプリケーション管理者グループの特性

特性	説明
タスク	ユーザー管理アプリケーション管理者は、ユーザー管理操作を実行するためのインタフェースを持つ特定のアプリケーションをインストールします。たとえば、OracleAS Portal や Oracle Application Server Wireless などです。
このグループがコンポーネントに委任できる権限	ユーザー属性を作成、編集および削除する権限。
管理者	Oracle Internet Directory スーパーユーザー（super user）。 Oracle コンテキスト管理者。 このグループの所有者。
DN	`cn=IAS & User Mgmt Admins,cn=groups,`*`Oracle_Context_DN`*。

トラステッド・アプリケーション管理者

トラステッド・アプリケーション管理者は、Oracle Application Server 管理者グループのメンバーである必要があります。

表 21-13 に、トラステッド・アプリケーション管理者グループの特性を示します。

表 21-13 トラステッド・アプリケーション管理者グループの特性

特性	説明
タスク	特定の ID 管理コンポーネントをインストールします。たとえば、Oracle Application Server Single Sign-On、Oracle Delegated Administration Services、Oracle Application Server Certificate Authority などです。
このグループがコンポーネントに委任できる権限	ユーザー・パスワードの読取り、比較、再設定を行う権限。 エンド・ユーザーのプロキシとなる権限。 ユーザーの証明書と SMIME 証明書の読取り、比較、変更を行う権限。
管理者	Oracle Internet Directory スーパーユーザー（super user）。 Oracle コンテキスト管理者。 このグループの所有者。
DN	`cn=Trusted Application Admins,cn=groups,` *`Oracle_Context_DN`*。

コンポーネントの実行時権限の委任

多くの Oracle コンポーネントでは、Oracle Internet Directory でユーザー・エントリが管理されているため、それに対応する権限が必要です。たとえば、次の場合を考えてみます。

- Oracle Application Server Single Sign-On Server がユーザーを認証する場合、そのサーバーには次の権限が必要です。
  - 独自の識別情報を使用して Oracle Internet Directory に接続する権限
  - ユーザーの入力したパスワードが、ディレクトリに格納されているそのユーザーのパスワードと一致するかどうかを検証する権限

  このためには、Oracle Application Server Single Sign-On Server はユーザー・パスワードを比較する権限を必要とします。Oracle Application Server Single Sign-On の Cookie を設定するには、ユーザー属性を読み取る権限が必要です。
- ユーザーにアクセス権を付与するには、OracleAS Portal はそのユーザーの属性を取得する必要があります。そのためには、アクセス権を必要とするユーザーにかわって、プロキシ・ユーザーとして Oracle Internet Directory にログインします。したがって、プロキシ・ユーザー権限が必要です。

通常、Oracle コンポーネントでは、次の権限が必要となる場合があります。

- ユーザー・パスワードの読取りと変更を行う権限
- ユーザー・パスワードの比較を行う権限
- アプリケーションにアクセスするユーザーのプロキシとなる権限
- すべての Oracle コンポーネントのメタデータが格納される Oracle コンテキストを管理する権限

ほとんどの Oracle コンポーネントには、事前定義された権限のセットが付属しています。これらの権限は、個々のビジネス要件を満たすように変更できます。たとえば、要件を満たすために、ユーザー・エントリを作成および削除するための権限を削除できます。

> **関連資料：** コンポーネント委任モデルの詳細は、『Oracle Application Server セキュリティ・ガイド』を参照してください。

この項では、Oracle コンポーネントが必要とするセキュリティ権限を説明します。この項の項目は次のとおりです。

ユーザー・パスワードの読取りおよび変更を行うためのデフォルトの権限

ユーザー・パスワードの読取りと変更は、ディレクトリにあるセキュリティ関係の属性（userPassword 属性など）に対する管理権限を必要とします。表 21-14 に示すユーザー・セキュリティ管理者グループでのメンバーである必要があります。

表 21-14 ユーザー・セキュリティ管理者グループの特性

特性	説明
デフォルト ACP	ルート（DSE エントリ）でのデフォルトの ACL ポリシーにより、ユーザー・セキュリティ管理者グループのメンバーは、ルート Oracle コンテキストで userpkcs12、orclpkcs12hint、userpassword、orclpassword および orclpasswordverifier の各属性の読取り、書込み、比較および検索を行えます。ただし、ディレクトリ管理者は、レルムの Oracle コンテキストのユーザー・セキュリティ管理者グループに同様の管理権限を付与することができます。
管理者	Oracle Internet Directory スーパーユーザー。 Oracle コンテキスト管理者グループのメンバー。 トラステッド・アプリケーション管理者グループのメンバー。
DN	cn=oracleUserSecurityAdmins,cn=groups,*Oracle_Context_DN*。

ユーザー・パスワードを比較するためのデフォルトの権限

ユーザー・パスワードの比較には、ユーザーの userPassword 属性を比較する権限が必要です。この操作は、Oracle Internet Directory に格納されたパスワードを使用してエンド・ユーザーを認証する Oracle Unified Messaging のようなコンポーネントにより実行されます。

ユーザー・パスワードを比較するには、表 21-15 に示す認証サービス・グループのメンバーである必要があります。

表 21-15 認証サービス・グループの特性

特性	説明
デフォルト ACP	デフォルトの ID 管理レルムの「ユーザー」コンテナにある ACL ポリシーにより、認証サービス・グループは、ユーザーの userPassword 属性に対する比較操作を実行できます。
管理者	Oracle Internet Directory スーパーユーザー。 Oracle コンテキスト管理者グループのメンバー。 アプリケーション・サーバー管理者グループのメンバー。 このグループの所有者。
DN	cn=authenticationServices,cn=groups,*Oracle_Context_DN*。

パスワード・ベリファイアを比較するためのデフォルトの権限

パスワード・ベリファイアを比較するには、userpassword 属性を比較する権限が必要です。パスワード・ベリファイアを比較するには、表 21-16 に示すベリファイア・サービス・グループのメンバーである必要があります。

表 21-16 ベリファイア・サービス・グループの特性

特性	説明
管理者	Oracle Internet Directory スーパーユーザー。 Oracle コンテキスト管理者グループのメンバー。 アプリケーション・サーバー管理者グループのメンバー。 このグループの所有者。
DN	cn=verifierServices,cn=groups,*Oracle_Context_DN*。

エンド・ユーザーのプロキシとなるためのデフォルトの権限

プロキシ・ユーザーは、エンド・ユーザーの代理となる権限を持ち、そのユーザーが権限を持つ操作をユーザーにかわって実行します。Oracle Application Server 環境では、Oracle Delegated Administration Services がエンド・ユーザーのプロキシとなり、Oracle Internet Directory セルフ・サービス・コンソールを通じて、そのユーザーのかわりに操作を実行します。そのような場合、ディレクトリ・サーバーに対するアクセス制御がユーザーの実行できる操作を実質的に制御します。

エンド・ユーザーのプロキシには、表 21-17 に示すユーザー・プロキシ権限グループのメンバーである必要があります。

表 21-17 ユーザー・プロキシ権限グループの特性

特性	説明
デフォルト ACP	デフォルトの ID 管理レルムの「ユーザー」コンテナでの ACL ポリシーにより、ユーザー・プロキシ権限グループは、エンド・ユーザーのプロキシとなることができます。
管理者	Oracle Internet Directory スーパーユーザー。 Oracle コンテキスト管理者グループのメンバー。 グループの所有者。これらの所有者の識別名は、Oracle Application Server 管理者グループのグループまたはメンバーの owner 属性の値として表示されます。 トラステッド・アプリケーション管理者グループのメンバー。
DN	cn=userProxyPrivilege,cn=groups,*OracleContextDN*。

Oracle コンテキストを管理するためのデフォルトの権限

特定の Oracle コンテキストを管理するには、そのコンテキストへの完全なアクセス権が必要です。Oracle コンテキストを管理するには、表 21-18 に示す Oracle コンテキスト管理者グループのメンバーである必要があります。Oracle コンテキスト管理者グループは、Oracle コンテキストごとに存在し、特定の Oracle コンテキストでの管理権限を持ちます。

表 21-18 Oracle コンテキスト管理者グループの特性

特性	説明
デフォルト ACP	Oracle コンテキストのルート・ノードにある ACL ポリシーにより、Oracle コンテキスト管理者グループは、Oracle コンテキスト内ですべての管理操作を実行できます。そのようなポリシーは、ディレクトリで新しい Oracle コンテキストが作成されるときに設定されます。
管理者	Oracle Internet Directory スーパーユーザー。 Oracle コンテキスト管理者グループのメンバー。
DN	`cn=oracleContextAdmins,cn=groups,`*`Oracle_Context_DN`*。

共通ユーザー属性を読み取るためのデフォルトの権限

共通ユーザー属性には、`mail`、`orclguid`、`displayname`、`preferredlanguage`、`orcltime`、`gender`、`dateofbirth`、`telephonenumber` および `wirelessaccountnumber` があります。これらの属性を読み取るには、表 21-19 に示す共通ユーザー属性グループのメンバーである必要があります。

表 21-19 共通ユーザー属性グループの特性

特性	説明
デフォルト ACP	デフォルト ACL は、レルム内の「ユーザー」コンテナ上にあり、共通ユーザー属性を読み取る権限を付与します。
管理者	Oracle Internet Directory スーパーユーザー。 アプリケーション・サーバー管理者グループのメンバー。 このグループの所有者。
DN	`cn=commonuserattributes,cn=users,`*`Oracle_Context_DN`*。

共通グループ属性を読み取るためのデフォルトの権限

共通グループ属性には、`cn`、`uniquemember`、`displayname` および `description` があります。これらの属性を読み取るには、21-15 ページの表 21-20 に示す共通グループ属性グループのメンバーである必要があります。

表 21-20 共通グループ属性グループの特性

特性	説明
デフォルト ACP	デフォルト ACL は、レルム内の「グループ」コンテナ上にあり、`cn`、`uniquemember`、`displayname` および `description` 属性を読み取る権限を付与します。
管理者	Oracle Internet Directory スーパーユーザー。 アプリケーション・サーバー管理者グループのメンバー。 このグループの所有者。
DN	`cn=commongroupattributes,cn=groups,`*`Oracle_Context_DN`*。

サービス・レジストリを読み取るためのデフォルトの権限

サービス・レジストリのコンテンツを表示するには、21-16 ページの表 21-21 に示すサービス・レジストリのビューア・グループのメンバーである必要があります。

表 21-21 サービス・レジストリのビューア・グループの特性

特性	説明
デフォルト ACP	デフォルトの ACL は、ルート Oracle コンテキストの「サービス」コンテナにあります。
管理者	Oracle Internet Directory スーパーユーザー。 アプリケーション・サーバー管理者グループのメンバー。 このグループの所有者。
DN	`cn=service registry viewers,cn=services,cn=rootoraclecontext,`

サービス・レジストリを管理するためのデフォルトの権限

サービス・レジストリを管理するには、21-16 ページの表 21-22 に示すサービス・レジストリの管理グループのメンバーである必要があります。

表 21-22 共通グループ属性グループの特性

特性	説明
デフォルト ACP	デフォルトの ACL は、ルート Oracle コンテキストの「サービス」コンテナにあります。
管理者	Oracle Internet Directory スーパーユーザー。 アプリケーション・サーバー管理者グループのメンバー。 このグループの所有者。
DN	`cn=service registry admins,cn=services,cn=rootoraclecontext,`

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。

22

ディレクトリ配置の考慮事項

この章では、Oracle Internet Directory を配置するときに考慮する必要がある問題について説明します。企業のディレクトリの要件を評価し、効果的な配置を選択するのに役立ちます。この章の推奨事項は、主に中規模および大規模の企業やインターネット・サービス・プロバイダ（ISP）のディレクトリに対するものですが、基本的な考え方は他の環境でも同様に適用できます。

この章の項目は次のとおりです。

関連資料 :

- 容量計画の詳細は、第 24 章「ディレクトリの容量計画」を参照してください。
- 高可用性の詳細は、『Oracle Application Server 高可用性ガイド』の「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 25 章「ディレクトリのチューニングに関する考慮事項」を参照してください。
- クラスタ化された環境でのフェイルオーバーの詳細は、『Oracle Application Server 高可用性ガイド』を参照してください。

拡大するディレクトリの役割

現在、ほとんどの企業では、集中化および整理統合された LDAP 準拠のディレクトリを配置する傾向にあります。一部の企業では、非 LDAP 準拠のディレクトリ（例 : NDS または ISO X.500）を使用していましたが、現在は対応する LDAP 対応のバージョンに変換しています。これは、LDAP に依存するインターネット・クライアント（Web ブラウザに埋め込まれているものなど）に対応するため、あるいは増え続けるディレクトリ対応のプラットフォームやサービスを整理統合するためです。

LDAP 対応のアプリケーションの増加により、LDAP 準拠のディレクトリに対する可用性とパフォーマンスの要件が重要視されています。ほとんどの環境で配置を更新する必要があります。

企業は、次のような状況に対応するために、堅牢で柔軟な配置を計画する必要があります。

- ディレクトリ内の情報量の増加
- ディレクトリに依存するアプリケーションの数
- 同時アクセスやスループットなどのロード特性

ディレクトリがネットワークとそのサービスの運用の中心となるので、配置の選択が重要となります。

ディレクトリ情報の論理編成

Oracle Internet Directory は、Oracle Identity Management インフラストラクチャ全体の共有リポジトリとして機能します。ディレクトリの論理構造を慎重に計画することによって、次のことが可能になります。

- 配置の要件を満たすセキュリティ・ポリシーの適用
- ディレクトリ・サービスの効率的な物理的配置
- サード・パーティのディレクトリを Oracle Internet Directory と同期化させる場合の簡単な構成

関連項目： 23-2 ページの「ID 管理を行うためのディレクトリ情報ツリーの計画」

物理的な分散 : パーティション、レプリカおよび高可用性

ディレクトリ・データを分散するには、次の 2 つの方法があります。

- 1 つのサーバーでのディレクトリ全体のメンテナンス
- 異なるサーバーでの異なるネーミング・コンテキストのホスティングとナレッジ参照によるネーミング・コンテキストの接続

関連項目： 3-19 ページの「分散ディレクトリ」

この項の項目は次のとおりです。

理想的な配置

中央の 1 つのディレクトリにすべてのネーミング・コンテキストを格納すると、より単純かつ安全であると考えられますが、この中央のディレクトリはシングル・ポイント障害の発生箇所になります。

1 つの解決策は、冗長な LDAP サーバーとそれに関連付けられたデータベースを実装することです。しかし、冗長性を持たせても、ほとんどのグローバルな組織がその地域やサイトすべてで必要とする接続性、アクセス可能性およびパフォーマンスが提供されない場合があります。これらの要件を満たすには、企業の地理的な広がりに応じて、様々な地域にレプリカを物理的に配置する必要があります。

Oracle Internet Directory が単一のマスターによる構成しかサポートしない場合、ディレクトリの論理的な統合は困難なものとなります。各地域またはグループは、信頼できるネーミング・コンテキストのマスター・レプリカを格納することが必要となります。この方法では、管理者はパーティションごとに異なるデータ管理手順を使用する必要があるため、パーティションにわたる管理ポリシーに一貫性を欠くことになります。

マルチマスター・レプリケーションでは、どこでも更新可能な構成ができるため、ディレクトリの統合は、複数のパーティションをメンテナンスするより効率的で費用がかかりません。

堅牢で集中化された企業ディレクトリにするための、単純で実用的な推奨事項は次のとおりです。

- それぞれがすべてのネーミング・コンテキストを保持した、2 つ以上のディレクトリ・ノードを持つネットワークを確立します。これらのノードはマルチマスター構成で設定します。
- これらのノードをそれぞれ各地域に 1 つずつ、企業のデータ・ネットワーク接続に合うように配置します。たとえば、ある地域が遅いリンク方法でネットワークの他の地域と接続されている場合、その地域のクライアントが使用するための専用のディレクトリ・サーバーを設置する必要があります。
- フェイルオーバーとリカバリのために、各地域のサーバーを個々に構成します。

すべてのネーミング・コンテキストは整理統合されていますが、今までどおり様々な論理ネーミング・コンテキストに対して管理の自律性を実現できます。そのためには、適切なアクセス制御ポリシーを各ネーミング・コンテキストのルートで設定してください。

> **関連資料 :** 冗長性の詳細は、22-5 ページの「高可用性に関する考慮事項」を参照してください。

パーティション化に関する考慮事項

パーティションが多すぎるディレクトリは、一般的に利点よりも管理上のオーバーヘッドの方が大きくなります。これは、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、独立したままの方が、より管理の境界およびデータ所有権の境界に対応している。
- 企業ネットワークに、費用がかかる、あるいはスピードが遅いリンクと接続されている地域があり、多くのパーティションがローカル・アクセスのみを必要としている。
- パーティションの可用性の欠如が大きな影響を及ぼさない。
- 1 つの地域での企業全体のディレクトリのメンテナンスに、費用がかかりすぎる。

パーティション化する場合は、**ナレッジ参照**を使用して 1 つのパーティションを他のパーティションに接続します。

注意 : LDAP では、LDAP サーバーによるナレッジ参照の自動連鎖をサポートしません。クライアント側の LDAP API のほとんどは、クライアント主導のナレッジ参照の追跡をサポートします。しかし、ナレッジ参照がすべての LDAP ツールでサポートされるという保証はありません。使用可能なツール全体で、一貫したナレッジ参照のサポートが欠如しているということは、パーティションの使用を決定する前の考慮事項です。

レプリケーションに関する考慮事項

LDAP ディレクトリ・レプリケーション・アーキテクチャは、緩和された一貫性モデルに基づいています。**レプリケーション承諾**内の 2 つのレプリケート・ノードが、リアルタイムで一貫しているという保証はありません。そのため、ディレクトリ・ネットワークの柔軟性と可用性が全般的に増加します。クライアントは相互接続されたすべてのノードが使用可能でなくても、データを変更できるためです。たとえば、1 つのノードが使用不可であるか、または負荷が高いとします。マルチマスター・レプリケーションでは、操作は代替のノードで実行され、後に相互接続されたすべてのノードが同期化します。

レプリケート・ネットワークを実装する理由の多くは、次のようなものです。

- ローカルなアクセス可能性とパフォーマンス要件

  多くの企業は世界中の様々な地域で活動しており、それらの活動には共通ディレクトリが必要です。複数の中継ルーターを含む、低帯域幅のリンクで各地域が相互接続されているとします。地域の外部からディレクトリ・サーバーにアクセスしているクライアントは、長い**待機時間**や不十分な**スループット**を体験する可能性があります。

  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 **Oracle Database アドバンスト・レプリケーション**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方が、費用がかからない場合があります。ロード・バランシングに加えて、そのような構成も、システムの可用性を高めることに貢献します。

- 障害許容度とシステム全体の高可用性

  ディレクトリ・レプリケーションを実装する最も重要な理由の 1 つは、システム全体の可用性を増すことです。1 つのサーバーが使用できない場合、通信量は他の使用可能なサーバーに送られます。これはクライアントには透過的です。

  関連資料 : レプリケート・ディレクトリ構成の詳細は、『Oracle Identity Management 概要および配置プランニング・ガイド』の Oracle Internet Directory の物理的配置計画に関する項を参照してください。

高可用性に関する考慮事項

ディレクトリ・サービスは企業内で重要な機能を持っているので、配置する際に障害リカバリと高可用性を考慮する必要があります。各ノードのバックアップおよびリカバリ計画を作成することが必要です。

マルチマスター・レプリケーションに加えて、Oracle Internet Directory のインストール時に可能な配置について、次のフェイルオーバーおよび高可用性オプションを考慮します。

- インテリジェント・クライアントのフェイルオーバー

  Oracle Internet Directory に接続しているすべての LDAP クライアントは、指定したサーバー・インスタンスとの接続が突然切断された場合に接続する、Oracle Internet Directory の代替サーバー・インスタンスのリストをメンテナンスできます。

- インテリジェント・ネットワーク・レベルのフェイルオーバー

  Oracle Internet Directory を稼働させるシステムの障害を検出できる、ハードウェアおよびソフトウェアのソリューションがいくつかあります。これらのソリューションでは、以降の接続リクエスト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、受信した接続リクエストの負荷を代替サーバーと調整するソリューションもあります。

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

  単一のホストで複数の Oracle Internet Directory のインストールを実行して、それらの間でレプリケートすることが可能です。自動バックアップにより、同一マシン上で最新のディレクトリ・データを提供する上で、この方法は便利です。使用するノードを 2 つのみにすると、フェイルオーバーも可能になります。いずれかのノードに障害が発生しても、両方の Oracle Internet Directory のインスタンスは、もう一方のノード上で実行できます。

Oracle Internet Directory は Oracle Database のクライアントであるため、Oracle 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。

関連資料：

- 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、『Oracle Application Server 高可用性ガイド』の「高可用性とフェイルオーバーに関する考慮事項」を参照してください。
- ディレクトリの高可用性の詳細は、『Oracle Identity Management 概要および配置プランニング・ガイド』の Oracle Internet Directory の物理的配置計画に関する項を参照してください。

Oracle Directory Integration Platform

サード・パーティの LDAP ディレクトリを含め、ディレクトリおよびアプリケーションを Oracle Internet Directory に統合することにより、管理作業に必要な時間とコストを削減できます。これは、Oracle Identity Management のコンポーネントである Oracle Directory Integration Platform によって実現します。たとえば、企業には次のようなニーズがあります。

- Oracle Human Resources と Oracle Internet Directory で従業員レコードの整合性を維持すること。Oracle Directory Integration Platform は Oracle Directory Synchronization Service によって、この同期化を行います。
- 変更が Oracle Internet Directory に適用されるたびに、OracleAS Portal などの LDAP 対応アプリケーションに通知されること。Oracle Directory Integration Platform は Oracle Directory Provisioning Integration Service によって、この通知を行います。

統合処理全体を通して、Oracle Directory Integration Platform は、アプリケーションとその他のディレクトリが確実な方法で必要な情報を授受することを保証します。

Oracle Directory Integration and Provisioning プラットフォームは、Microsoft Active Directory や SunONE Directory Server など、様々なディレクトリに統合することができます。たとえば、Oracle Application Server 環境では、Oracle コンポーネントへのアクセスは、Oracle Internet Directory に格納されているデータに基づいて行います。この環境では、企業の中央ディレクト

リとして Microsoft Active Directory も使用できます。これらのディレクトリのユーザーが Oracle コンポーネントにアクセスできるのは、Oracle Directory Integration Platform が、Microsoft Active Directory 内のデータを、Oracle Internet Directory 内のデータと同期化できるためです。

関連資料：『Oracle Identity Management 統合ガイド』

容量計画、サイズ設定およびチューニング

ディレクトリの使用に際し、企業全体および地域の要件を見積もるときは、将来の必要性を計画します。レプリケーションとフェイルオーバーは他の構成の選択に依存するため、それぞれ独自の負荷と容量の要件を持つ複数のディレクトリ・ノードを必要とする場合があります。この場合、各ディレクトリ・ノードに対し個々にサイズを決める必要があります。

企業ではディレクトリの使用が増加しているので、Oracle Internet Directory を使用してリクエスト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。

この項の項目は次のとおりです。

容量計画

容量計画は、パフォーマンスと容量の要件を決定するプロセスです。企業のディレクトリ使用の一般的なモデルに基づいて行われます。

Oracle Internet Directory のインストールに必要な容量を見積もる場合の考慮事項は、次のとおりです。

- LDAP クライアント・アプリケーションのタイプ
- アプリケーションにアクセスするユーザー数
- アプリケーションが実行する LDAP 処理の特性
- ディレクトリ情報ツリー内のエントリ数
- Oracle ディレクトリ・サーバーに対して実行される操作のタイプ
- Oracle ディレクトリ・サーバーへの同時接続数
- Oracle ディレクトリ・サーバーで実行する必要がある、ピーク時の操作の実行率
- ピーク時の負荷条件で必要となる、操作の平均待機時間

これらの考慮事項を詳しく見積もる場合は、ディレクトリの使用が将来増加した場合に備えて余裕を持って見積もってください。

サイズ設定に関する考慮事項

基本となる容量とパフォーマンスの要件を確立した後、それをシステム要件に変換します。これはシステム・サイズ設定と呼ばれます。このフェーズでの考慮事項の詳細は次のとおりです。

- Oracle Internet Directory サーバー・コンピュータの CPU のタイプと数
- Oracle Internet Directory サーバー・コンピュータのディスク・サブシステムのタイプとサイズ
- Oracle Internet Directory サーバー・コンピュータに必要なメモリーの量
- クライアントからの LDAP メッセージに使用されるネットワークのタイプ

表 22-1 に、Oracle Internet Directory の様々な配置例に必要な CPU 能力の概算レベルを、現在の経験に基づいて示します。

表 22-1 様々な配置例に必要な CPU 能力

使用方法	アクティブな接続数	CPU の数	SPECint_rate95 ベースライン	システム
部門単位	0-500	2	60 ～ 200	Compaq AlphaServer 8400 5/300 (300MHz × 2)
組織単位	500-2000	4	200 ～ 350	IBM RS/6000 J50 (200MHz × 4)
会社単位	2000+	4+	350+	Sun Ultra 450 (296MHz × 4)

Oracle Internet Directory のインストールに必要なディスク領域の量は、ディレクトリ情報ツリーに格納されるエントリ数に正比例します。表 22-2 に、様々なサイズのディレクトリ情報ツリーに必要なディスク領域要件の概算を示します。

表 22-2 様々なサイズのディレクトリ情報ツリーに必要なディスク領域要件の概算

ディレクトリ情報ツリー内のエントリ数	ディスク要件
100,000	450MB ～ 650MB
200,000	850MB ～ 1.5GB
500,000	2.5GB ～ 3.5GB
1,000,000	4.5GB ～ 6.5GB
1,500,000	6.5GB ～ 10GB
2,000,000	9GB ～ 13GB

この表のデータから、次のことが仮定されます。

- カタログ化属性が約 20 個であること
- 各エントリの属性が約 25 個であること
- 属性の平均サイズが約 30 バイトであること

Oracle Internet Directory に必要なメモリーの量は、配置サイトが要求するデータベース・バッファ・キャッシュの量によってほぼ決定されます。多くの場合、データベース・バッファ・キャッシュのサイズは、ディレクトリ情報ツリー内のエントリ数に比例します。22-8 ページの表 22-3 に、様々なサイズのディレクトリ情報ツリーのメモリー要件の概算を示します。

表 22-3 様々なサイズのディレクトリ情報ツリーのメモリー要件の概算

ディレクトリのタイプ	エントリ数	最小メモリー
小	600,000 未満	512MB
標準	600,000 ～ 2,000,000	1GB
大	2,000,001 以上	2GB

関連項目： 第 24 章「ディレクトリの容量計画」

チューニングに関する考慮事項

本番環境で使用する前に、Oracle Internet Directory を正しくチューニングすることをお薦めします。チューニングする前に、実際の使用手順をシミュレートするための、十分なテスト手段とサンプル・データがディレクトリにあることを確認してください。テスト用のディレクトリに依存するアプリケーションを使用できます。

Oracle Internet Directory のパフォーマンスをテストするツールは、次のものの表示が可能である必要があります。

- 調べている包括的なスループット
- 操作の平均待機時間

このように、チューニング効果を確認し、チューニング作業全般に指示を与えるため、ツールではフィードバック・メカニズムを提供します。

Oracle Internet Directory のインストールで、一般的にチューニングされるプロパティには、次のようなものがあります。

- CPU 使用量

  次のものによって、ほぼ決定されます。

  - Oracle ディレクトリ・サーバーの数
  - 各サーバーによって開かれるデータベース接続の数

  Oracle ディレクトリ・サーバーとデータベース接続の数が多すぎると、使用可能な CPU リソースの競合が頻繁に発生します。また、Oracle ディレクトリ・サーバーとデータベース接続の数が少なすぎると、CPU の能力の大部分が十分に活用されないままとなります。使用可能な CPU リソースと想定されるピーク時の負荷に基づいて、これらの数を適正なレベルに調整することを考慮してください。

- メモリー使用量

  Oracle Internet Directory のインストールで主にメモリーを使用するのは、**SGA** の一部であるデータベース・バッファ・キャッシュです。大規模なデータベース・バッファ・キャッシュを割り当てることで、Oracle データ・ファイルのディスク I/O の多くを削減できる場合もあります。しかし、パフォーマンスに悪影響を及ぼすページングを発生させることにもなります。逆にデータベース・バッファ・キャッシュを小さくすると、ディスク I/O が多く発生して、パフォーマンスに悪影響を及ぼします。システム内のメモリーのコンシューマすべてが、ページングの使用を必要とせずに物理メモリーを取得できるように、システムのメモリー使用量をチューニングします。

- ディスク使用量

  Oracle Internet Directory によって処理されるデータはすべてデータベースの表領域に常駐しているので、I/O スループットを増加させるようなチューニングには注意してください。一般的なディスクのチューニング方法は、次のとおりです。

  – 異なる論理ドライブおよび物理ドライブにある表領域の均衡化
  – 論理ボリュームの複数の物理ボリュームへのストライプ化
  – ディスク・ボリュームの複数の I/O 制御装置への分散

  関連項目： 様々なチューニングのヒントと方法の詳細は、第 25 章「ディレクトリのチューニングに関する考慮事項」を参照してください。

23

Oracle Identity Management レルムの配置

この章では、ID 管理レルムについて、企業内配置およびホスティングされた配置用に計画および構成する方法を説明します。

この章の項目は次のとおりです。

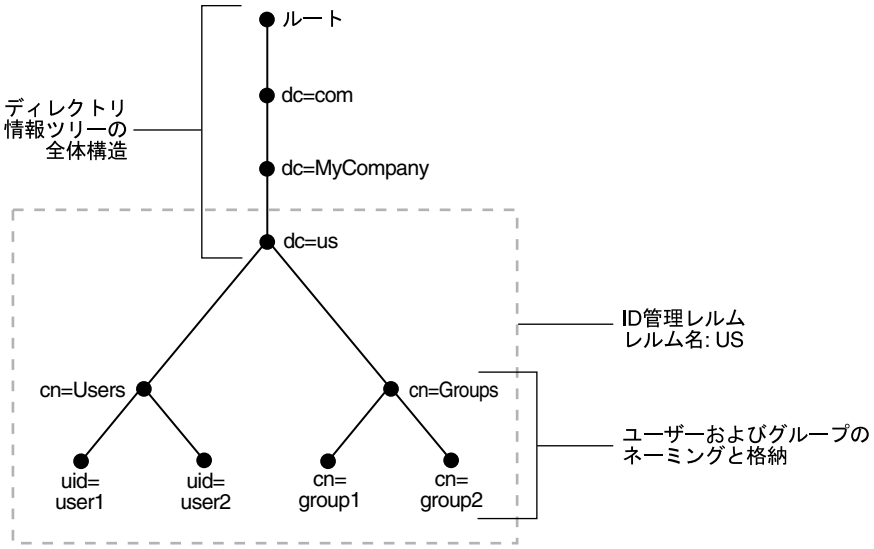
ID 管理を行うためのディレクトリ情報ツリーの計画

Oracle Internet Directory は、Oracle Identity Management インフラストラクチャ全体の共有リポジトリとして機能します。ディレクトリの論理構造を慎重に計画することによって、次のことが可能になります。

- 配置の要件を満たすセキュリティ・ポリシーの適用
- ディレクトリ・サービスの効率的な物理的配置
- サード・パーティのディレクトリを Oracle Internet Directory と同期化させる場合の簡単な構成

図 23-1 に、ID 管理を配置している MyCompany という架空の会社のディレクトリ情報ツリーを示します。

図 23-1 ディレクトリ情報ツリーの計画



MyCompany は、米国内での配置におけるディレクトリの論理編成に関して次の事項を決定しています。

- ドメイン名ベースのスキームは、ディレクトリ情報ツリー階層全体を表す。ID 管理インフラストラクチャが `us` ドメイン内で展開されるため、`dc=us,dc=mycompany,dc=com` がディレクトリ情報ツリーのルートとなる。
- 選択したネーミング・コンテキスト内部では、すべてのユーザーが `cn=users` というコンテナの下に表示される。このコンテナ内部では、すべてのユーザーが同一レベルで表示される。組織ベースの階層は存在しない。また、すべてのユーザーの一意の識別子として `uid` 属性を選択する。
- 選択したネーミング・コンテキスト内部では、すべての企業グループが `cn=groups` というコンテナの下に表示される。このコンテナ内部では、すべての企業グループが同一レベルで表示される。すべてのグループ・エントリのネーミング属性を `cn` とする。
- コンテナ `dc=us` を、ID 管理レルムのルートとして選択する。この場合、レルムの名前は `us` とする。配置では、`us` レルムの範囲に該当するすべてのユーザーに対して、同様のセキュリティ・ポリシーを施行することを想定する。

Oracle Identity Management のディレクトリの論理編成の計画には、次のものが含まれます。

- ディレクトリ情報ツリー構造全体の計画
- ユーザーおよびグループのディレクトリ格納とネーミングの計画
- ID 管理レルムの計画

この項では、ディレクトリ情報の論理編成を設計する場合の考慮事項の詳細を説明します。この項の項目は次のとおりです。

ディレクトリ構造全体の計画

このタスクでは、企業内のすべての ID 管理統合アプリケーションで使用される基本的なディレクトリ情報ツリーを設計します。この設計を行う場合は、次の考慮事項に注意してください。

- ディレクトリ編成によって、明確で効果的なアクセス制御が簡単に実行できるようになる必要があります。完全レプリケーションまたは部分レプリケーションのいずれかのレプリケーションを計画した場合、レプリケーションに対して適切な境界およびポリシーを施行できるのは、ディレクトリ情報ツリーが分離するように設計された場合のみです。
- サード・パーティのディレクトリ・サーバーとの統合を行う企業では、Oracle Internet Directory のディレクトリ情報ツリーの設計と既存のディレクトリ情報ツリーを一致させることをお薦めします。この考慮事項は、現在 Oracle Internet Directory を展開し、後で別のディレクトリ（マイクロソフト社のソフトウェアの操作に必要な Microsoft Active Directory など）を展開する配置にも該当します。いずれの場合でも、サード・パーティのディレクトリ情報ツリーの設計とより一貫性のある Oracle Internet Directory のディレクトリ情報ツリーの設計を採用すると、Oracle Delegated Administration Services および他の中間層アプリケーションを使用した、ユーザー・オブジェクトおよびグループ・オブジェクトの管理をより簡単にできます。
- 単一企業の使用例では、企業の DNS ドメイン名と一致するディレクトリ情報ツリー設計を選択すると、十分な結果が得られます。たとえば、`mycompany.com` というドメイン名を持つ企業で Oracle Internet Directory を設定する場合は、`dc=mycompany,dc=com` というルートを持つディレクトリ構造を使用することをお薦めします。部門または組織レベルのドメイン・コンポーネント（`engineering.mycompany.com` の `engineering` など）は使用しないことをお薦めします。
- X500 ディレクトリ・サービスを使用し、他のサード・パーティの LDAP ディレクトリが本番環境に存在しない企業では、国ベースのディレクトリ情報ツリー設計を選択することをお薦めします。たとえば、`o=mycompany, c=US` というルートを持つディレクトリ情報ツリー設計は、すでに X.500 ディレクトリ・サービスを使用している企業に適しています。
- ディレクトリは、Oracle およびサード・パーティの複数のアプリケーションで使用できるため、ディレクトリ情報ツリーの構造全体を構成する相対識別名（RDN）で使用されるネーミング属性を、予約済属性に制限する必要があります。通常、次の属性は、ほとんどのディレクトリ対応アプリケーションで予約済です。
  - `c`: 国の名前
  - `dc`: DNS ドメイン名のコンポーネント
  - `l`: 地域（都市、国、その他の地域など）の名前
  - `o`: 組織の名前
  - `ou`: 組織単位の名前
  - `st`: 州またはその他の地方行政区画の名前
- 企業の部門構造または組織構造のいずれかを反映してディレクトリ情報ツリーを設計するのは、よくある間違いです。ほとんどの企業が組織および部門の再編成を頻繁に行うため、この方法はお薦めしません。企業のディレクトリは、できるかぎり組織変更とは無関係にしておくことが重要です。

ユーザーおよびグループのネーミングおよび格納の計画

ディレクトリ情報ツリー設計全体に適用される設計に関するほとんどの考慮事項は、ユーザーおよびグループのネーミングと格納にも適用されます。この項では、Oracle Internet Directory でユーザーおよびグループのモデリングを行う場合の追加の考慮事項について説明します。

ユーザーに関する考慮事項

Oracle Identity Management インフラストラクチャでは、すべてのユーザーの識別情報のリポジトリとして Oracle Internet Directory を使用します。企業内の複数のアプリケーションにアクセスするアカウントを持つユーザーの場合も、そのユーザーの識別情報を示すエントリは Oracle Internet Directory 内に 1 つのみです。ディレクトリ情報ツリー全体でのこれらのエントリの位置と内容は、Oracle Internet Directory および Oracle Identity Management インフラストラクチャの他のコンポーネントを配置する前に計画する必要があります。

- 前述のとおり、所属部門の関係や階層に基づいてユーザーを編成する傾向があります。ただし、ほとんどの企業は組織および部門の再編成を頻繁に行うため、この方法はお薦めしません。個人のディレクトリ・エントリの属性として個人の組織情報を捉えると、管理しやすくなります。
- 部門関係や管理系統に基づいた階層でユーザー編成を行った場合、パフォーマンスは向上しません。ユーザーを格納するディレクトリ情報ツリーは、できるかぎり浅い階層にしておくことをお薦めします。
- 配置に様々なユーザーの集団が含まれ、それぞれの集団が異なる組織によってメンテナンスおよび管理される場合は、それらの管理境界に基づいてユーザーをいくつかのコンテナに分けることをお薦めします。これによって、アクセス制御の設定が簡単になり、レプリケーションが必要になった場合に役立ちます。
- 検索操作でユーザーを一意に識別するためのデフォルトのニックネーム属性は、`uid` です。これはログインで使用するデフォルトの属性です。識別名を構成するためのデフォルトのネーミング属性は、`cn` です。
- ユーザーを一意に識別するためのデフォルトの属性は、cn または CommonName です。CommonName の一般的な値は、そのユーザーのフルネームです。ただし、名前や電子メール・アドレスは変わることがあるため、この属性の値には適さない場合があります。可能であれば、従業員 ID など、ユーザーを一意に識別できる変更のない値を選択してください。
- 通常、ほとんどの企業には、従業員に一意の名前と番号を割り当てる規則を定める人事部門があります。ディレクトリ・エントリに対して一意のネーミング・コンポーネントを選択する場合、この管理インフラストラクチャを活用し、そのポリシーを使用するのが有効です。
- ディレクトリ内に作成するすべてのユーザー・エントリは、`inetOrgPerson` および `orclUserV2` というオブジェクト・クラスのメンバーである必要があります。
- サード・パーティのディレクトリがすでに存在する場合、または将来それを統合する場合は、Oracle Internet Directory でのユーザーのネーミングとディレクトリの格納を、サード・パーティのディレクトリ内で使用されるものと一致させるのが効果的です。これによって、分散ディレクトリの同期化およびそれ以降の管理が簡単になります。

注意： Oracle Internet Directory リリース 9.0.2 では、`nickname` 属性のデフォルト値は `cn` でした。リリース 9.0.4 以上では、この属性のデフォルト値は `uid` です。

グループに関する考慮事項

Oracle Identity Management インフラストラクチャと統合されたアプリケーションの一部では、Oracle Internet Directory での配置によって作成された企業全体にわたるグループに基づいて認可を行うこともできます。ユーザー・エントリ同様、これらのグループ・エントリの位置と内容も慎重に計画する必要があります。グループ設計時の考慮事項は、次のとおりです。

- 部門関係や所有権に基づいた階層で企業グループ編成を行った場合、パフォーマンスは向上しません。グループを格納するディレクトリ情報ツリーは、できるかぎり浅い階層にしておくことをお薦めします。これによって、すべてのアプリケーションによるグループの検出が簡単になり、アプリケーション間でのこれらのグループの共有が促進されます。
- エントリの各セットに個別の管理ポリシーを適用できるように、ディレクトリ情報ツリー内のユーザーおよびグループを分けることをお薦めします。
- グループを一意に識別するには、cn または CommonName 属性を使用する必要があります。
- 企業がディレクトリ内に作成するすべてのグループは、groupOfUniqueNames および orclGroup というオブジェクト・クラスに属している必要があります。前者のオブジェクト・クラスは、グループを表すインターネット標準です。後者のオブジェクト・クラスは、Oracle Internet Directory セルフ・サービス・コンソールを使用してグループを管理する場合に有効です。
- 企業全体にわたるグループごとに新しいディレクトリ・アクセス制御を作成するのではなく、次のように対応することを検討してください。
  1. グループの owner 属性を使用して、グループの所有者であるユーザーを示します。
  2. owner 属性で示されたすべてのユーザーに、様々な操作を実行する特別な権限を付与する上位レベルのアクセス制御ポリシーを作成します。
- description 属性には、グループの目的をユーザーが理解できるように情報を書き込みます。
- オブジェクト・クラス orclGroup での displayName 属性の使用を検討します。これによって、Oracle Delegated Administration Services および Oracle Internet Directory セルフ・サービス・コンソールで、読みやすいグループ名を表示できます。
- 様々なグループのセットがあり、それぞれのセットが独自の管理ポリシーを持つ異なる組織によってメンテナンスおよび管理される場合は、それらの管理境界に基づいてグループをいくつかのコンテナに分けます。これによって、アクセス制御の設定が簡単になります。また、レプリケーションが必要な場合にも役立ちます。
- サード・パーティのディレクトリがすでに存在する場合、または将来それを統合する場合は、Oracle Internet Directory でのグループのネーミングとディレクトリの格納を、サード・パーティのディレクトリ内で使用されるものと一致させます。これによって、分散ディレクトリの同期化およびそれ以降の管理が簡単になります。

ID 管理レルムの計画

前述の項では、ディレクトリ情報ツリー全体および配置対象のユーザーとグループの配置を構成する場合のガイドラインを示しました。これらのガイドラインを実装すると、膨大な数の配置構成を行うことになるため、配置の目的をディレクトリ自体にメタデータとして取得する必要があります。Oracle Identity Management インフラストラクチャに依存する Oracle ソフトウェアおよびサード・パーティのソフトウェアは、このメタデータによって配置の目的を認識し、カスタマイズされた環境で正常に機能できます。

Oracle Internet Directory では、配置の目的は、ID 管理レルムに取得されます。このレルムは、前述の項で配置について説明したユーザーおよびグループに対して、ID 管理ポリシーを設定する場合にも役立ちます。

ID 管理レルムは、ディレクトリ内の適用範囲が明確な領域で、次の要素で構成されています。

- 適用範囲が明確な企業識別情報の集合（米国内のすべての従業員など）
- これらの識別情報に関連付けられた ID 管理ポリシーの集合
- ID 管理ポリシーを設定しやすくするグループの集合（識別情報の集約）

ディレクトリ情報ツリー全体の構造およびユーザーとグループの配置を決定した後、ID 管理レルムのルートとして機能するディレクトリ・エントリを識別する必要があります。このエントリによって、レルムに定義された ID 管理ポリシーの施行範囲が決まります。デフォルトでは、ID 管理レルムのルート下のディレクトリ・サブツリー全体が、この ID 管理ポリシーの施行範囲になります。このエントリの下に、`OracleContext` という特別なエントリが作成されます。このエントリには、次の情報が含まれます。

- ユーザーおよびグループのネーミングおよび配置などの配置固有のディレクトリ情報ツリー設計（前述の項を参照）
- このレルムに関連付けられた ID 管理ポリシー
- Oracle アプリケーション特有のレルム固有の追加情報

ID 管理レルムを計画する場合は、次のことを考慮します。

- 企業のセキュリティ要件に基づいて、ID 管理レルムのルートを選択する必要があります。通常、ほとんどの企業で必要なレルムは 1 つのみです。ただし、個別の ID 管理ポリシーを使用して複数のユーザー集団を管理するときは、複数のレルムが必要になる場合があります。
- サード・パーティのディレクトリがすでに存在する場合、または将来それを統合する場合は、選択した ID 管理レルムのルートを、サード・パーティのディレクトリのディレクトリ情報ツリー設計と一致させます。これによって、分散ディレクトリの同期化およびそれ以降の管理が簡単になります。
- ID 管理レルムを構成し管理するには、Oracle Internet Directory で提供される管理ツールを使用します。これらのツールには、Oracle Internet Directory コンフィギュレーション・アシスタント、Oracle Internet Directory セルフ・サービス・コンソール、コマンドライン・ツールなどが含まれます。
- Oracle Internet Directory ツールを使用して ID 管理レルムを構成した後、配置によって行われたカスタマイズを反映するために、ディレクトリのネーミングおよび格納ポリシーの更新を計画します。この更新は、Oracle Identity Management インフラストラクチャを使用する他の Oracle コンポーネントをインストールして使用する前に行う必要があります。

図 23-2 に、MyCompany という会社の ID 管理レルムの例を示します。

図 23-2 ID 管理レルムの例

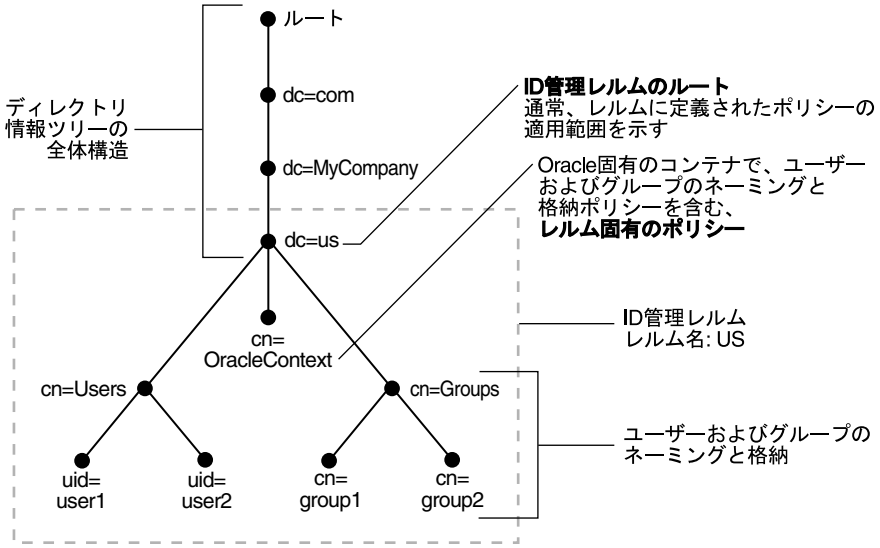


図 23-2 の例は、ドメイン名ベースのディレクトリ情報ツリー構造を使用する配置になっています。コンテナ `dc=us,dc=mycompany,dc=com` は、ID 管理レルムのルートです。その結果、デフォルトで、適用範囲が `dc=us` エントリ下のディレクトリ・サブツリー全体に限定される新しい ID 管理レルムが作成されます。ID 管理レルムの名前は `US` です。

サード・パーティ・ディレクトリからの DIT の移行

サード・パーティ・ディレクトリから DIT を移行するには、『Oracle Identity Management 統合ガイド』に記載した方法で、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化およびサード・パーティ・ディレクトリとの統合を行います。Microsoft Active Directory 環境から DIT を移行する場合は、Microsoft Active Directory 環境との統合の章も参照してください。Oracle Internet Directory の DIT をサード・パーティの DIT と同一になるように構成することをお薦めします。

企業内配置における ID 管理レルム

この項では、単一および複数の ID 管理レルムを使用する配置について説明します。この項の項目は次のとおりです。

- 企業における単一 ID 管理レルム
- 企業における複数 ID 管理レルム

企業における単一 ID 管理レルム

この場合、企業には、ユーザーの集団が 1 つあり、そのすべてのユーザーが同一の ID 管理ポリシーによって管理されます。すべての Oracle 製品のデフォルトの構成です。Oracle Internet Directory に存在するデフォルトの ID 管理レルムは 1 つのみであり、企業内のすべての Oracle コンポーネントが、このレルムのユーザーに対応します。図 23-3 に、この使用方法を示します。

図 23-3 企業での使用例 : 単一 ID 管理レルム

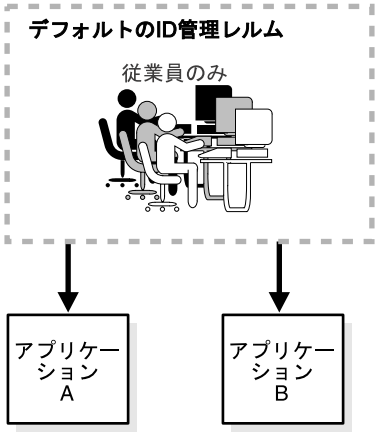


図 23-3 の例には、従業員のみを含む単一のデフォルト ID 管理レルムがあります。このレルムでは、すべてのユーザーおよびグループが管理され、同じアプリケーションであるアプリケーション A およびアプリケーション B へのアクセスを共有しています。

企業における複数 ID 管理レルム

同一の ID 管理インフラストラクチャを使用して、内部ユーザーと外部の自己登録ユーザーの両方に対応することも可能です。内部ユーザーと外部ユーザーでは ID 管理ポリシーが異なるため、内部ユーザー用と外部ユーザー用にレルムを 1 つずつ配置できます。23-8 ページの図 23-4 に、この使用方法を示します。

図 23-4 企業での使用例 : 複数 ID 管理レルム

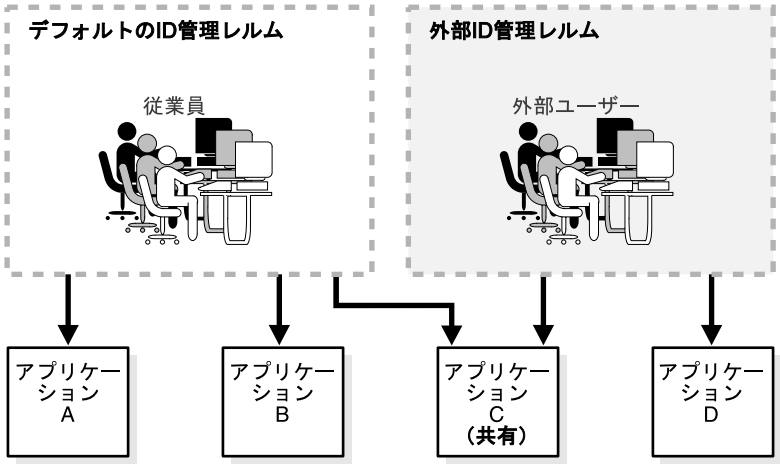


図 23-4 の例では、デフォルトの ID 管理レルムが内部ユーザー（従業員）用です。内部ユーザーは、アプリケーション A、B および C へのアクセス権を所有しています。外部 ID 管理レ

ルムは外部ユーザー用に使用されます。外部ユーザーは、アプリケーション C および D へのアクセス権を所有しています。

ホスティングされた配置における ID 管理レルム

ホスティングされた配置では、アプリケーション・サービス・プロバイダ（ASP）が、1 社以上に ID 管理サービスを提供し、これらの企業にかわってアプリケーションのホスティングを行います。ホスティングされた各企業は、その企業のユーザーが管理される個別の ID 管理レルムに対応付けられます。アプリケーション・サービス・プロバイダに属するユーザーは、別のレルム（通常は、デフォルトのレルム）で管理されます。

図 23-5 に、ホスティングされた配置（2 社をホスティング）を示します。

図 23-5 ホスティングされた配置での使用例

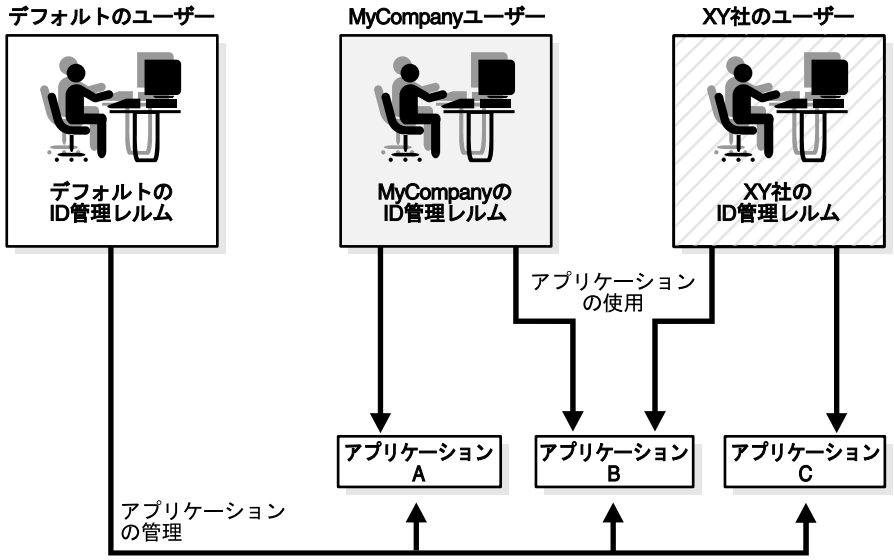


図 23-5 の例では、ASP ユーザーはデフォルトの ID 管理レルムに存在します。ASP は、そのレルムのユーザー、グループおよび関連するポリシーを管理します。ASP ユーザーは、ホスティングされた企業のためにアプリケーション A、B、C を管理しています。ホスティングされた企業の MyCompany ユーザーは、MyCompany という ID 管理レルムに存在します。これらのユーザーは、アプリケーション A およびアプリケーション B を使用します。ホスティングされた企業の XY Corp ユーザーは、XY Corp という ID 管理レルムに存在します。この XY Corp ユーザーは、アプリケーション B およびアプリケーション C を使用します。

Oracle Internet Directory での ID 管理レルムの実装

表 23-1 に、ID 管理レルムのオブジェクトを示します。

表 23-1 Oracle Identity Management オブジェクト

オブジェクト	説明
ルート Oracle コンテキスト（Root Oracle Context）	このオブジェクトには、次のものが含まれます。 ■ インフラストラクチャ内のデフォルトの ID 管理レルムへのポインタ ■ 単純な名前の指定によりレルムの位置を特定する方法に関する情報
ID 管理レルム	特別なオブジェクト・クラスが関連付けられた通常のディレクトリ・エントリ。
ID 管理レルム固有の Oracle コンテキスト	このオブジェクトには、レルムごとに次のものが含まれます。 ■ ID 管理レルムのユーザー・ネーミング・ポリシー（ユーザーに名前を付け、配置する方法） ■ 必須認証属性 ■ ID 管理レルム内のグループの位置 ■ ID 管理レルムに対する権限の割当て（レルムにユーザーを追加する権限の割当てなど） ■ レルムに関するアプリケーション固有のデータ（認可など）

デフォルトのディレクトリ情報ツリーおよび ID 管理レルム

構成を簡単にするために、Oracle Internet Directory のインストール時に、デフォルトのディレクトリ情報ツリーが作成され、デフォルトの ID 管理レルムが設定されます。

図 23-6 デフォルト ID 管理レルム

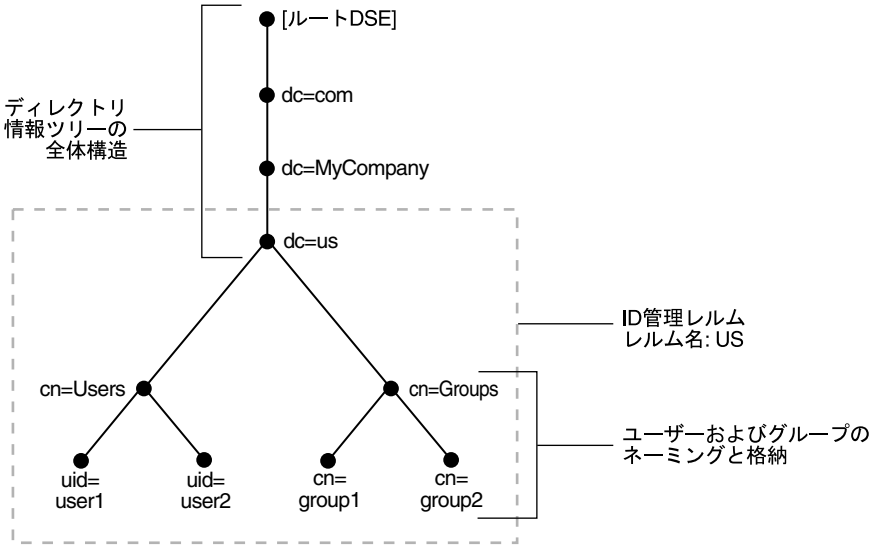


図 23-6 に示されているとおり、デフォルトの ID 管理レルムは、グローバル・ディレクトリ情報ツリーの一部です。ルート DSE の下には、dc=com、dc=MyCompany、dc=us の順でノードが続きます。これら 4 つのノードにより、ディレクトリ情報ツリー構造全体が表現されます。ノード dc=us は、デフォルトの ID 管理レルムのルートです。このノードには、ユーザーおよびグループの情報を格納するための cn=Users と cn=Groups という 2 つのサブツリーが含まれます。説明上の理由から、cn=Users ノードには、uid=user1 と uid=user2 という 2 つの

リーフが含まれます。同様に、cn=Groups ノードには、cn=group1 と cn=group2 が含まれます。

オプションで、Oracle Internet Directory をインストールするコンピュータのドメインに基づいて、ディレクトリ情報ツリーを設定することもできます。たとえば、oidhost.us.mycompany.com というコンピュータにインストールすると、デフォルトの ID 管理レルムのルートは、dc=us,dc=mycompany,dc=com となります。

また、「**Internet Directory のネームスペースの指定**」インストール画面で、配置要件を満たす別の識別名を、デフォルトの ID 管理レルムのルートとして指定することも可能です。たとえば、独自の ID 管理インストール環境をサード・パーティ・ディレクトリと統合する予定がある場合、サード・パーティ・ディレクトリのデフォルト・ネーミング・コンテキストの識別名と一致する識別名を指定することをお薦めします。サード・パーティ・ディレクトリからデフォルト・ネーミング・コンテキストを取得する方法の詳細は、『Oracle Identity Management 統合ガイド』のサード・パーティ・ディレクトリとの統合に関する章を参照してください。

構成中に、Oracle Internet Directory によって次のものが作成されます。

- デフォルトの ID 管理レルムに関連付けられた Oracle コンテキスト。Oracle コンテキストには、レルム固有のすべてのポリシーとメタデータが格納されます。前述の例の場合は、cn=OracleContext,dc=us,dc=mycompany,dc=com という識別名を持つ Oracle コンテキストが作成されます。このエントリとその下にあるノードによって、Oracle ソフトウェアはレルム固有のポリシーと設定を検出できます。
- デフォルトの ID 管理レルムでのディレクトリ構造およびネーミング・ポリシー。これによって、Oracle コンポーネントが様々な識別情報を検索できるようになります。これらのデフォルト値は、次のとおりです。
  - すべてのユーザーは、ID 管理レルムのベースの下にあるコンテナ cn=users に配置されます。この例では、cn=users,dc=us,dc=mycompany,dc=com がこのコンテナです。
  - Oracle Identity Management インフラストラクチャを使用して ID 管理レルム内に作成した新規ユーザーも、コンテナ cn=users の下に作成されます。
  - Oracle Identity Management インフラストラクチャを使用して ID 管理レルム内に作成したすべての新規ユーザーは、オブジェクト・クラス orclUserV2 および inetOrgPerson に属します。
  - すべてのグループは、ID 管理レルムのベースの下にあるコンテナ cn=groups に配置されます。この例では、cn=groups,dc=us,dc=mycompany,dc=com がこのコンテナです。
- ID 管理レルム管理者。このユーザーは、ユーザー・コンテナの下に配置されます。この例では、レルム管理者の完全修飾された識別名は orcladmin,cn=users,dc=us,dc=mycompany,dc=com です。

  注意： レルム管理者のアカウントがロックされた場合は、Oracle Internet Directory のスーパーユーザーが Oracle Directory Manager を使用してレルム管理者のアカウントのパスワードを変更することにより、ロックを解除できます。

- 認証サービスで適切な処理を実行できるようにするデフォルトの認証ポリシー。次のポリシーが含まれます。
  - デフォルトのディレクトリ・パスワード・ポリシー（パスワードの長さ、ロックアウト、有効期限など）
  - ユーザーのプロビジョニングを行う際に自動生成される必要がある追加のパスワード・ベリファイア

- ID 管理の権限。これらの権限は、Oracle Internet Directory によって、Oracle Internet Directory セルフ・サービス・コンソールを介してこれらの権限を委任できるレルム管理者に付与されます。これらの権限の例は、次のとおりです。
  - 共通の ID 管理操作権限（ユーザーの作成、ユーザー・プロファイルの変更、グループの作成など）
  - Oracle Identity Management インフラストラクチャを使用して新しい Oracle コンポーネントをインストールする権限
  - Oracle Internet Directory セルフ・サービス・コンソールを管理する権限

関連資料：

- `orclUserV2` オブジェクト・クラスの詳細は、『Oracle Identity Management ユーザー・リファレンス』の Oracle Identity Management の LDAP オブジェクト・クラスに関する項を参照してください。
- Oracle Identity Management におけるデフォルトのアクセス制御ポリシーの詳細は、第 21 章「Oracle テクノロジ配置のための権限の委任」を参照してください。

ID 管理レルムの管理

この項では、ID 管理レルムに対して実行できる様々な管理タスクについて説明します。この項の項目は次のとおりです。

- デフォルトの ID 管理レルムのカスタマイズ
- ホスティングされた配置での ID 管理レルムの追加作成

デフォルトの ID 管理レルムのカスタマイズ

レルムを作成した後、様々な要素をカスタマイズできます。表 23-2 に、カスタマイズできる要素、各種のカスタマイズで使用可能なツールおよび参照先を示します。

表 23-2 デフォルトの ID 管理レルムのカスタマイズ

カスタマイズ可能な対象	ツール	参照箇所
ディレクトリ構造およびネーミング・ポリシー	Oracle Internet Directory セルフ・サービス・コンソール Oracle Directory Manager コマンドライン・ツール	23-13 ページの「デフォルトの ID 管理レルムでのユーザーおよびグループの位置の変更」 23-2 ページの「ID 管理を行うためのディレクトリ情報ツリーの計画」 『Oracle Identity Management 委任管理ガイド』の Oracle Internet Directory セルフ・サービス・コンソールの使用方法に関する章
認証ポリシー	Oracle Directory Manager コマンドライン・ツール	第 19 章「Oracle Internet Directory のパスワード・ポリシー」
ID 管理の権限	Oracle Internet Directory セルフ・サービス・コンソール Oracle Directory Manager コマンドライン・ツール	第 21 章「Oracle テクノロジ配置のための権限の委任」 『Oracle Identity Management 委任管理ガイド』の Oracle Internet Directory セルフ・サービス・コンソールの使用方法に関する章

デフォルトの ID 管理レルムでのユーザーおよびグループの位置の変更

この変更を必要とする可能性のある典型的な使用例は、Oracle Identity Management インストール環境をサード・パーティ・ディレクトリと統合する場合です。

たとえば、デフォルトの ID 管理レルムが dc=mycompany,dc=com であり、cn=users,dc=mycompany,dc=com の下にユーザーが存在すると仮定します。

サード・パーティ・ディレクトリのネーミング・コンテキストが、デフォルト・レルム内のユーザーおよびグループの現在の検索ベースと一致しない場合は、既存のユーザーとサード・パーティのユーザーがどちらも Single Sign-On を使用してログインできるように、デフォルト・レルムのユーザーおよびグループの検索ベースを変更できます。既存のユーザーとサード・パーティのユーザーをともに含むことができて最も下位にあるユーザー検索ベースを選択します。この検索ベースを、最下位の共通ユーザー検索ベースと呼ぶことにします。

注意： このアプローチでは、Single Sign-On ログインで選択されるユーザーの nickname 属性が、既存のユーザー検索ベースとサード・パーティ・ディレクトリのネーミング・コンテキスト全体で一意であると仮定しています。一意でない場合、nickname 属性の値が競合しているすべてのユーザーは、Single Sign-On 認証に失敗します。

配置環境が次の 1 ～ 5 の使用例のいずれかと一致する場合は、23-14 ページの「ユーザーおよびグループの既存の検索ベースを更新する手順」で説明されている手順に従ってください。

使用例 1:

サード・パーティのネーミング・コンテキストは、デフォルト・レルムの下にありますが、レルムのユーザー検索ベース以外のコンテナ内に存在します。

たとえば、既存のユーザーが cn=users,dc=mycompany,dc=com の下に存在し、サード・パーティのネーミング・コンテキストが cn=users,o=employees,dc=mycompany,dc=com の下に存在する場合です。この場合、最下位の共通ユーザー検索ベースは、dc=mycompany,dc=com です。

使用例 2:

サード・パーティのネーミング・コンテキストは、デフォルト・レルムの外部にありますが、最下位の共通ユーザー検索ベースが存在します。

たとえば、既存のユーザーが cn=users,dc=mycompany,dc=com の下に存在し、サード・パーティのネーミング・コンテキストが cn=users, dc=mycompanyecorp,dc=com の下に存在する場合です。この場合、最下位の共通ユーザー検索ベースは、dc=com です。

最下位の共通ユーザー検索ベースがルート DSE の場合は、使用例 6: で説明されている手順に従ってください。

1. 23-15 ページの「追加の検索ベースの設定」
2. 23-16 ページの「Single Sign-On の更新」
3. 23-17 ページの「プロビジョニング・プロファイルの再構成」

使用例 3:

サード・パーティのネーミング・コンテキストは、デフォルト・レルムの識別名と同じです。

たとえば、既存のユーザーが cn=users,dc=mycompany,dc=com の下に存在し、サード・パーティのネーミング・コンテキストが dc=mycompany,dc=com のすぐ下に存在する場合です。この場合、最下位の共通ユーザー検索ベースは、dc=mycompany,dc=com です。

使用例 4:
サード・パーティのネーミング・コンテキストに、デフォルト・レルムの識別名の親が含まれます。

たとえば、識別名（DN）が dc=us,dc=mycompany,dc=com であるデフォルト・レルムがあり、既存のユーザーが cn=users,dc=us,dc=mycompany,dc=com の下に存在し、サード・パーティのネーミング・コンテキストが dc=com のすぐ下に存在する場合です。この場合、最下位の共通ユーザー検索ベースは、dc=com です。

使用例 5:
サード・パーティのネーミング・コンテキストは、既存のユーザー検索ベースの下に存在します。

たとえば、既存のユーザーが cn=users,dc=mycompany,dc=com の下に存在し、サード・パーティのネーミング・コンテキストが l=emea,cn=users,dc=mycompany,dc=com のすぐ下に存在する場合です。この場合、最下位の共通ユーザー検索ベースは、cn=users,dc=mycompany,dc=com です。この使用例の場合、ユーザー検索ベースを変更する必要はありません。

ユーザーおよびグループの既存の検索ベースを更新する手順 サード・パーティ・ディレクトリとの同期化を設定する前に、次の手順を実行する必要があります。

1. Oracle Internet Directory データベースをバックアップします。
2. サード・パーティ・ディレクトリにまだエントリが存在していない場合、Oracle Directory Manager を使用してそのディレクトリにユーザーおよびグループ・コンテナを作成します。
3. 次の手順に従って新規ユーザー・コンテナに適切な ACL を適用します。
   a. ACL テンプレート・ファイル $ORACLE_HOME/ldap/schema/oid/oidUserAdminACL.sbs の変数 %USERBASE% と %REALMBASE% をインスタンス化し、usracl.ldif ファイルを作成します。変数 %USERBASE% は新規ユーザー・コンテナの識別名に、変数 %REALMBASE% はデフォルト・レルムの識別名に設定します。
   b. ldapmodify コマンドを使用してインスタンス化した LDIF ファイルの usracl.ldif をアップロードします。
4. 次の手順に従って新規グループ・コンテナに適切な ACL を適用します。
   a. ACL テンプレート・ファイル $ORACLE_HOME/ldap/schema/oid/oidGroupAdminACL.sbs の変数 %GRPBASE% と %REALMBASE% をインスタンス化し、grpacl.ldif ファイルを作成します。変数 %USERBASE% は新規ユーザー・コンテナの識別名に、変数 %REALMBASE% はデフォルト・レルムの識別名に設定します。
   b. ldapmodify コマンドを使用してインスタンス化した LDIF ファイルの grpacl.ldif をアップロードします。
5. 既存のユーザーとサード・パーティのユーザーをともに含むことができる最下位の共通ユーザー検索ベースを決定します。

   たとえば、既存のユーザーが cn=users,dc=mycompany,dc=com の下に存在し、サード・パーティのユーザーが l=emea,dc=mycompany,dc=com の下に存在する場合、最下位の共通ユーザー検索ベースは、dc=mycompany,dc=com です。

   最下位の共通ユーザー検索ベースが、ルート・エントリになることもあります。たとえば、既存のユーザーが cn=users,dc=mycompany,dc=com の下に存在し、サード・パーティのユーザーが dc=mycompanycorp,dc=net の下に存在する場合です。この場合は、23-15 ページの使用例 6 の「追加の検索ベースの設定」で説明されている配置例までスキップしてください。
6. グループも同期化する必要がある場合は、既存のグループとサード・パーティのグループをともに含むことができて最も下位にあるグループ検索ベースを決定します。この検索ベースを、最下位の共通グループ検索ベースと呼ぶことにします。

たとえば、既存のグループが cn=groups,dc=mycompany,dc=com の下に存在し、サード・パーティのグループが l=emea,dc=mycompany,dc=com の下に存在する場合、最下位の共通グループ検索ベースは、dc=mycompany,dc=com です。

7. レルムの管理者（通常は orcladmin）としてセルフ・サービス・コンソールにログインします。
8. 「**構成**」タブに移動し、ユーザー検索ベースを手順 5 で決定した最下位の共通ユーザー検索ベースに設定します。グループも同期化する場合は、グループ検索ベースを手順 6 で決定した最下位の共通グループ検索ベースに設定します。
9. Oracle Application Server Single Sign-On にこれらの変更を認識させるため、23-16 ページの「Single Sign-On の更新」に説明されている手順を実行します。
10. orcladmin としてログインし、元のユーザー検索ベースのユーザーによる Single Sign-On ログインを検証します。
11. 変更されたユーザーおよびグループ・ベースを反映するように、プロビジョニングされているアプリケーションも再構成する必要があります。23-17 ページの「プロビジョニング・プロファイルの再構成」に説明されている手順に従ってください。

注意： ユーザーおよびグループの検索ベースの属性に加え、ログイン名（ニックネーム）の属性や RDN の属性など、ID 管理レルムの他の構成設定もセルフ・サービス・コンソールを使用して変更できます。詳細は、『Oracle Identity Management 委任管理ガイド』の「Oracle Internet Directory セルフ・サービス・コンソールの使用」の ID 管理レルムの構成設定の変更に関する項を参照してください。

使用例 6:

この場合、サード・パーティのネーミング・コンテキストはデフォルト・レルムの外部にあり、最下位の共通ユーザー検索ベースはルート DSE です。

たとえば、既存のユーザーが cn=users,dc=mycompany,dc=com の下に存在し、サード・パーティのネーミング・コンテキストが cn=users,dc=mycompanycorp,dc=net の下に存在する場合、最下位の共通ユーザー検索ベースは、ルート DSE です。

この場合、サード・パーティのネーミング・コンテキストを別の検索ベースとして追加する必要があります。この手順は次のとおりです。

1. 「追加の検索ベースの設定」
2. 「Single Sign-On の更新」
3. 「プロビジョニング・プロファイルの再構成」

追加の検索ベースの設定 サード・パーティ・ディレクトリとの同期化を設定する前に、次の手順を実行します。

1. Oracle Internet Directory データベースをバックアップします。
2. サード・パーティ・ディレクトリにまだエントリが存在していない場合、Oracle Directory Manager を使用してそのディレクトリにユーザーおよびグループ・コンテナを作成します。
3. 次の手順に従って新規ユーザー・コンテナに適切な ACL を適用します。
   a. ACL テンプレート・ファイル $ORACLE_HOME/ldap/schema/oid/oidUserAdminACL.sbs の変数 %USERBASE% と %REALMBASE% をインスタンス化し、usracl.ldif ファイルを作成します。変数 %USERBASE% は新規ユーザー・コンテナの識別名に、変数 %REALMBASE% はデフォルト・レルムの識別名に設定します。
   b. ldapmodify コマンドを使用してインスタンス化した LDIF ファイルの usracl.ldif をアップロードします。

4. 次の手順に従って新規グループ・コンテナに適切な ACL を適用します。

   a. ACL テンプレート・ファイル `$ORACLE_HOME/ldap/schema/oid/oidGroupAdminACL.sbs` の変数 `%GRPBASE%` と `%REALMBASE%` をインスタンス化し、`grpacl.ldif` ファイルを作成します。変数 `%USERBASE%` は新規ユーザー・コンテナの識別名に、変数 %REALMBASE% はデフォルト・レルムの識別名に設定します。

   b. `ldapmodify` コマンドを使用してインスタンス化した LDIF ファイルの `grpacl.ldif` をアップロードします。

5. レルムの管理者としてセルフ・サービス・コンソールにログインします。

6. 「**構成**」タブに移動します。

   a. 現在のレルムの `usersearchbase` に `cn=users,dc=mycompanycorp,dc=net` を追加します。

   b. 現在のレルムの `groupsearchbase` に `cn=groups,dc=mycompanycorp,dc=net` を追加します。

7. Oracle Application Server Single Sign-On にこれらの変更を認識させるため、23-16 ページの「Single Sign-On の更新」に説明されている手順を実行します。

8. `orcladmin` としてログインし、元のユーザー検索ベースのユーザーによる Single Sign-On ログインを検証します。

9. この ID 管理構成に基づいて中間層が構成されている場合、変更されたユーザーおよびグループ・ベースを反映するように、プロビジョニングされているアプリケーションも再構成する必要があります。23-17 ページの「プロビジョニング・プロファイルの再構成」に説明されている手順に従ってください。

注意： ユーザーおよびグループの検索ベースの属性に加え、ログイン名（ニックネーム）の属性や RDN の属性など、ID 管理レルムの他の構成設定もセルフ・サービス・コンソールを使用して変更できます。詳細は、『Oracle Identity Management 委任管理ガイド』の「Oracle Internet Directory セルフ・サービス・コンソールの使用」の ID 管理レルムの構成設定の変更に関する項を参照してください。

Single Sign-On の更新 Oracle Application Server Single Sign-On に構成変更を認識させる手順は、次のとおりです。

1. Single Sign-On 更新スクリプトを実行するために、`$ORACLE_HOME/sso/admin/plsql/sso/` ディレクトリに移動して次のように入力します。

   ```
   sqlplus orasso/password@ssoreoid.sql
   ```

   `orasso` スキーマのパスワードを取得する方法の詳細は、『Oracle Application Server Single Sign-On 管理者ガイド』の付録「Single Sign-On スキーマのパスワードの取得」を参照してください。

2. 次のように入力し、`OC4J_SECURITY` インスタンスを再起動します。

   ```
   opmnctl restartproc type=oc4j instancename=OC4J_SECURITY
   ```

プロビジョニング・プロファイルの再構成 ユーザーおよびグループの検索ベースを変更する前にデフォルトの ID 管理レルムに基づいて中間層アプリケーションをインストールしている場合、中間層のインストールによって作成されたプロビジョニング・プロファイルは、無効になります。この理由は、プロファイルの event subscriptions 属性に含まれるユーザーまたはグループの検索ベースの情報が古くなるためです。oidprovtool を使用して、すべてのプロファイルを変更する必要があります。

すべてのプロビジョニング・プロファイルに対して次の手順を実行します。

1. ldapsearch を使用して、すべてのプロビジョニング・プロファイル情報を LDIF ファイルに出力します。

```
ldapsearch -h oid_host -p oid_port \
           -D "cn=orcladmin" -w password -s sub \
           -b "cn=provisioning profiles,cn=changelog subscriber,\
               cn=oracle internet directory" \
           "objectclass=*" >  provprofiles.ldif
```

   イベント・サブスクリプションの例は、次のとおりです。

```
USER:cn=users,dc=mycompany,dc=com:MODIFY(list_of_attributes)
USER:cn=users,dc=mycompany,dc=com:DELETE
GROUP:cn=groups,dc=mycompany,dc=com:MODIFY(list_of_attributes)
GROUP:cn=groups,dc=mycompany,dc=com:DELETE
```

   ここで、cn=users,dc=mycompany,dc=com と cn=groups,dc=mycompany,dc=com は、それぞれアプリケーションのインストールおよび構成時に作成したユーザー検索ベースとグループ検索ベースです。

2. GUID に基づいて Oracle Internet Directory サーバーを検索することで、アプリケーション ID の実際の識別名を取得します。アプリケーションの識別名を取得するには、次のように入力します。

```
ldapsearch -h host -p port -D cn=orcladmin -w password \
           -s sub -b "" \
           "orclguid=Value_of_orclODIPProvisioningAppGuid" dn
```

   provprofiles.ldif の属性値から各プロファイルの GUID 値を取得できます。

3. 返された各プロファイルを次のように変更します。

```
$ORACLE_HOME/bin/oidprovtool operation=MODIFY \
        ldap_host=host ldap_port=port \

ldap_user_dn="cn=orcladmin" \

ldap_user_passwd=password \

interface_version=interfaceVersion \
        application_dn=applicationDN \
        organization_dn=identity_Realm_DN \
        event_subscription=New_Event_Subscription_1
        event_ subscription=New_Event_Subscription_2
        .
        .
        .
        event_subscription=New_Event_Subscription_n
```

   New_Event_Subscription 引数には、次の書式を使用する必要があります。

```
USER: new_user_search_base:MODIFY(list_of_attributes)
USER: new_user_search_base:DELETE
GROUP: new_group_search_base:MODIFY(list_of_attributes)
GROUP: new_group_search_base:DELETE
```

   ここで、organization_dn の値には、元の ID レルムの識別名を指定する必要があります。

ホスティングされた配置での ID 管理レルムの追加作成

Oracle Internet Directory セルフ・サービス・コンソールを使用して、ID 管理レルムを追加作成できます。

ASPAdmins グループのメンバーのみが、新しい ID 管理レルムを作成できます。Oracle Directory Manager を使用して、デフォルトの ID 管理レルム固有の Oracle コンテキストにおける ASPAdmins グループの uniquemember 属性にユーザー識別名を追加し、このグループにユーザーを追加します。詳細は、「Oracle Directory Manager を使用した静的グループ・エントリの変更」を参照してください。

注意： 複数の ID 管理レルムでは、動作しないアプリケーションもあります。

レルムを追加する場合は、追加したレルムが既存アプリケーションで認識されるように手動で設定する必要があります。詳細は、アプリケーション固有のマニュアルを参照してください。

Oracle Identity Management インストラクチャでは、Single Sign-On Server に対し特別な管理手順で追加レルムが認識されるようにする必要があります。Oracle Application Server Single Sign-On で複数のレルムを使用可能にする手順の詳細は、『Oracle Application Server Single Sign-On 管理者ガイド』の複数のレルムでのシングル・サインオンに関する項を参照してください。

関連資料：

- 13-8 ページの「Oracle Directory Manager を使用した静的グループ・エントリの変更」
- ID 管理レルムの追加作成の詳細は、『Oracle Identity Management 委任管理ガイド』の Oracle Internet Directory セルフ・サービス・コンソールに関する章を参照してください。

24

ディレクトリの容量計画

容量計画は、アプリケーションのディレクトリ・アクセス要件を評価し、許容速度でリクエスト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。

この章の項目は次のとおりです。

容量計画の概要

Oracle Internet Directory とそれに対応する Oracle Database 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 を新規インストールする場合は常に、次の事項が整っている必要があります。

- 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。

表 24-1 に、この章で使用する重要な用語を定義します。

表 24-1 容量計画の用語

用語	定義
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 秒当たりの操作件数）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。

この章では、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。

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、表 24-2 の仮定を設けて、ディレクトリのサイズを推測できるようにします。

表 24-2 エントリのタイプとサイズについての前提事項

エントリ・タイプ	サイズ
ユーザー数の合計	40,000
ユーザーごとのプライベート・エイリアスの平均数	10
ユーザーごとのプライベート配布リストの平均数	10
パブリック配布リストの合計数	4000
社内におけるパブリック・エイリアスの合計数	1000
このアプリケーションに関連しているディレクトリ内の各エントリにある属性数	20
カタログ化属性の数	10

前述の仮定に基づくと、Oracle Internet Directory における全体的なエントリ件数は、表 24-3 のように算出できます。

表 24-3 全体的なエントリ件数

エントリ・タイプ	サイズ
ユーザー・エントリ	40,000（このエントリはユーザー自身を表しています）
ユーザーのプライベート・エイリアス	40,000 × 10 = 400,000 エントリ
ユーザーのプライベート配布リスト	40,000 × 10 = 400,000 エントリ
会社全体の配布リスト	4000
会社全体のエイリアス	1000

前述の仮定から、ディレクトリに存在するエントリは約 100 万件であることがわかります。ユーザー数とディレクトリに存在するエントリ数が与えられたとして、パフォーマンス要件を導出するために、使用パターンを分析してみます。一般的なユーザーは、毎日平均 10 通の電子メールを送信し、外部から 1 日に平均 10 通の電子メールを受信します。ユーザーが送信する各メールに対して、平均 5 人の受信者がいると仮定すると、メールごとに 5 回ずつディレクトリ参照が行われます。

表 24-4 は、1 日に発生する可能性があるすべてのディレクトリ参照回数を要約したものです。

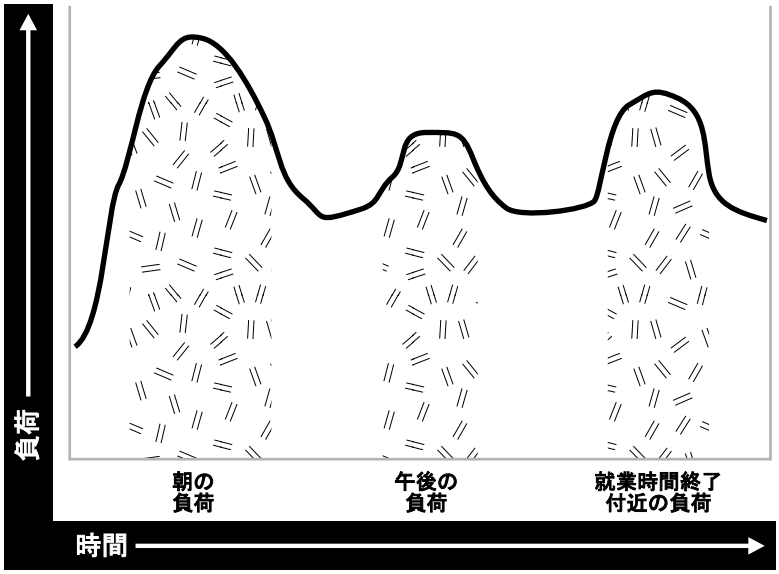
表 24-4 1 日のディレクトリ参照の数

ディレクトリ参照のタイプ	1 日のディレクトリ参照の数
各ユーザーからの送信メールを処理するメール転送エージェント（MTA）	5 × 10 × 40,000 = 2,000,000
外部からのメールを処理する MTA	10 × 40,000 = 400,000
その他のすべてのディレクトリ参照（IMAP クライアントによる特定のアドレスの検証など）	800,000

合計すると、毎日のディレクトリ参照の総数は約 3,200,000（320 万）となります。これらの参照が 1 日に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 24-1 のようになります。

図 24-1 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。表 24-5 に、8 時間勤務制の朝、昼食時、就業時間終了付近の負荷の時間帯を示します。

表 24-5 勤務時間内の負荷

負荷の時間帯	参照回数
朝の負荷	65%: 0.90 × 0.65 × 3,200,000 = 1,872,000 参照 /2 時間（936,000 参照 / 時）
昼食時の負荷	10%: 0.90 × 0.10 × 3,200,000 = 288,000 参照 /1 時間（288,000 参照 / 時）
就業時間終了付近の負荷	20%: 0.90 × 0.20 × 3,200,000 = 576,000 参照 /2 時間（288,000 参照 / 時）

これらの計算結果により、この場合のディレクトリは、ピーク時の負荷である 1 時間当たり 936,000 の参照を処理するように設計する必要があることが示されています。

データ・セットのサイズとパフォーマンス要件について理解したため、インストールの個々のコンポーネントを調べ、それぞれについて適切な値を見積もることができます。

I/O サブシステムの要件

この項の項目は次のとおりです。

- I/O サブシステムの概要
- 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 サブシステムの概要

I/O サブシステムは、CPU が負荷となる作業を実行できるように、CPU にデータを送り出すポンプにたとえることができます。I/O サブシステムには、データ記憶域を管理する役割もあります。I/O サブシステムの主なコンポーネントは、ディスク・コントローラによって制御される一連のディスク・ドライブです。

I/O サブシステムのサイズを決めるときは、記憶要件のみに基づいたサイズではなく、パフォーマンス要件を考慮することが重要です。ディスク・ドライブのサイズは増加していますが、スループット（ディスク・ドライブがデータを送り出す速度）は、比例して増加していません。I/O サブシステムのサイズを計算するときには、情報として次の要因を考慮する必要があります。

- データベースのサイズ
- システム上の CPU の数
- Oracle Internet Directory の作業負荷の初期見積り
- ディスクがデータを送出できる速度
- ロード前のデータ準備に必要な領域
- 索引作成とソート作業に必要な領域

様々な I/O サブシステムがある場合は、常にスループットが最大のドライブを選択してください。一般的に、次の技術を 1 つ以上使用すると、I/O スループットを最大にできます。

- I/O 操作で複数のディスク・スピンドルを使用するために、論理ボリュームをストライプ化
- 異なる表領域を、異なる論理ディスク・ボリュームと物理ディスク・ボリュームに格納
- ディスク・ボリュームを複数の I/O 制御装置に分散

Oracle Internet Directory 固有のデータ・ファイルを適切に動作させる方法のガイドラインは、第 25 章「ディレクトリのチューニングに関する考慮事項」を参照してください。ディスク障害の許容度によっては、異なるレベルの Redundant Arrays of Inexpensive Disks（RAID）を考慮することもできます。

可能なかぎり最良の I/O サブシステムを用意する決定が行われたと仮定して、次にディスク自体のサイズ設定を見積ります。

ディスク領域要件の概算

表 24-6 を使用すると、全般的なディスク要件を概算で見積もることができます。

表 24-6 ディスク領域要件

ディレクトリ情報ツリー内のエントリ数	ディスク要件
100,000	450MB ～ 650MB
200,000	850MB ～ 1.5GB
500,000	2.5GB ～ 3.5GB
1,000,000	4.5GB ～ 6.5GB
1,500,000	6.5GB ～ 10GB
2,000,000	9GB ～ 13GB

表 24-6 に示すデータから、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

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 Oracle Database 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、データを表 24-7 に示す表領域に格納します。

表 24-7 Oracle Internet Directory データを格納するために使用する表領域

表領域名	サイズ	コメント
OLTS_ATTR_STORE	LDIF ファイル・サイズの 3.5 倍	ディレクトリ・データをすべて格納。
OLTS_BATTRSTORE	バイナリ・データ値サイズの 1.5 倍	バイナリ・データをすべて格納。バイナリ・データをロードしない場合は、デフォルト・サイズのままにします。
OLTS_CT_STORE	LDIF ファイル・サイズの 3.5 倍	高速参照用のカタログ表を格納。サイズは、カタログ化された属性の数によって異なります。見積もりは、デフォルト構成に基づきます。
OLTS_DEFAULT	コメントを参照	bulkload の -check フェーズ中、および変更ログ・データと、いくつかのレプリケーションおよびプロセス構成表の保持のために使用。サイズは通常、ディレクトリでの更新回数とパージ構成の頻度に基づきます。
OLTS_SVRMGSTORE	2M	統計構成時に Oracle Internet Directory サーバー統計に使用。ほとんどの場合、デフォルトで十分です。

この項では、表 24-7 で参照される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、表 24-8 の変数に基づいて行われます。

表 24-8 サイズ計算に使用する変数

変数名	説明
num_entries	ディレクトリ内のエントリの合計数。
attrs_per_entry	ディレクトリ・エントリごとの属性の平均数。
avg_attr_size	属性値の平均サイズ（バイト）。
avg_dn_size	属性の識別名の平均サイズ（バイト）。
objectclass_per_entry	エントリが属しているオブジェクト・クラスの平均数。
objectclass_size	各オブジェクト・クラス名の平均サイズ（バイト）。
num_cataloged_attrs	エントリ内で使用されているカタログ化属性の数。
entries_per_catalog	カタログ表ごとのエントリの平均数。ディレクトリ情報ツリー内の全エントリにカタログ化属性が存在しているとはかぎらないため、この変数は必須です。
change_log_capacity	レプリケーション目的のためにバッファする変更の数。
num_acis	ディレクトリ内の ACI の全体数。
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、Oracle Internet Directory サーバー管理機能によって生成される統計エントリの数。
attrs_per_stats_entry	統計エントリごとの属性の平均数。

表 24-8 に示す変数を使用すると、個々の表領域のサイズを表 24-9 に示すように計算できます。

表 24-9 個々の表領域のサイズ

表が含まれている表領域	式
ATTRSTORE_INDEX_SIZE	num_entries*(attrs_per_entry+6) *10
CATALOG_INDEX_SIZE	entries_per_catalog*num_cataloged_attrs*avg_attr_size*db_index_ovhd +num_entries*objectclass_per_entry*objectclass_size*db_index_ovhd + num_acis*1.5*avg_dn_size*db_index_ovhd + num_auditlog_entries*2*avg_dn_size*db_index_ovhd
CN_SIZE	num_entries*avg_dn_size*db_storage_ovhd
DN_INDEX_SIZE	num_entries*2*(avg_dn_size * 3)
DN_SIZE	num_entries*2*(avg_dn_size+4)
OBJECTCLASSES_SIZE	num_entries*objectclass_per_entry*objectclass_size*db_storage_ovhd + num_auditlog_entries*2*avg_dn_size*db_storage_ovhd
OLTS_ATTR_STORE	(num_entries*(((attrs_per_entry)*(avg_attrname_len+avg_attr_size+22))+6*35)*db_storage_ovhd)+attrstore_index_size
OLTS_BATTRSTORE	6M+(((num_binary_attrs*avg_binval_length)+6*35)*db_storage_ovhd)
OLTS_CT_STORE	(cn_size+objectclasses_size+dn_size+catalog_index_size+dn_index_size)
OLTS_DEFAULT	(change_log_capacity*4*avg_attr_size*db_storage_ovhd*db_index_ovhd) + (initial_num_entries*2*(avg_dn_size+4))
OLTS_SVRMGSTORE	2M+num_stats_entries*((avg_attrname_len+avg_attr_size+20)*(2*attrs_per_stats_entry)* db_storage_ovhd*(orclstatsperiodicity/10)*12)
SYSTEM	300MB

この表の計算式は、Oracle Internet Directory の広範囲にわたる様々な配置例についての正確な領域要件を計算するために使用します。各表領域のサイズを合計すると、データベース全体のディスク要件がわかります。オプションで、その値に factor_of_safety 変数を乗算すると、予期せぬ事態にも対処可能な数値を算出できます。

Acme Corporation の例に戻り、前項に記述されている要件に基づいて各変数に値を代入します。表 24-10 は、この項で紹介する Acme Corporation の各変数の値を示したものです。

表 24-10 サイズ計算に使用する変数の値

変数名	値
num_entries	1,000,000
attrs_per_entry	20
avg_attr_size	32 バイト
avg_dn_size	40 バイト
objectclass_per_entry	5（各エントリが平均 5 つのオブジェクト・クラスに所属）
objectclass_size	10 バイト
num_cataloged_attrs	10
entries_per_catalog	1,000,000
change_log_capacity	80,000 の変更（ユーザーごとに 2 つの変更）
num_acis	80,000 の ACI（ユーザーごとに 2 つの ACI）
num_auditlog_entries	1000
db_storage_ovhd	1.4（40% のオーバーヘッド）

表 24-10 サイズ計算に使用する変数の値（続き）

変数名	値
db_index_ovhd	5.0（400% のオーバーヘッド）
factor_of_safety	1.5（50% の安全係数）
initial_num_entries	1,000,000
num_stats_entries	5
attrs_per_stats_entry	12
orclstatsperiodicity	60（ルート DSE 属性）
avg_attrname_len	6

これらの値を前述の等式に代入すると、表 24-11 にリストした値が得られます。

表 24-11 表領域のサイズ

表領域名	サイズ（バイト）	サイズ（MB）
OLTS_ATTRSTORE	2,223,000,000	2182
OLTS_CT_STORE	2,328,512,000	274
OLTS_DEFAULT	159,680,000	156
OLTS_SVRMGSTORE	2,701,568	3
SYSTEM	314,572,800	300
合計サイズ	5,038,093,862	4920

表 24-11 は、Acme Corporation のデータベースの見積りサイズが約 8.25GB であることを示しています。すべてのデータを一括してロードする場合、Oracle Internet Directory の bulkload ツールには、一時ファイルを格納するためにデータベースが使用する追加領域が 30% 必要です。Acme Corporation の場合は、領域要件の合計に約 2.5GB を追加します。

メモリー要件

メモリーは、Oracle Internet Directory などのあらゆるデータベース・アプリケーションが、多数の個別のタスク用に使用します。いずれかのタスクに対するメモリー・リソースが不十分な場合は、CPU の稼働率が低くなり、システム・パフォーマンスが低下します。また、メモリー使用量はデータベースへの同時接続数とディレクトリの同時ユーザー数に比例して増加します。容量計画の目的で、アクティブな接続は、クライアントがディレクトリとのバインドを要求したときに開始し、このバインドが完了したときに終了します。

処理に使用できるメモリーは、システム上の仮想メモリーから供給されます。これは、使用可能な物理メモリーよりもやや大きいメモリーです。全アクティブ・メモリー使用量の合計が、そのシステムで使用可能な物理メモリーを超えると、オペレーティング・システムは、ある程度のメモリー・ページをディスク上に格納する必要があります。この作業をページングと呼びます。使用可能な物理メモリーをはるかに超えるメモリーを使用すると、ページングによってパフォーマンスが低下することがあります。一般的に、物理メモリーの 20% を超えたメモリーは使用しないでください。ページングが発生した場合は、プロセスごとのメモリー使用量を減らすか、または物理メモリーを追加する必要があります。ただし、トレードオフに注意してください。追加できるメモリーには物理的な制限があり、プロセスごとのメモリー使用量を減らすとパフォーマンスが大幅に低下します。

メモリーを主に消費するのは、システム・グローバル領域（SGA）内のデータベース・バッファ・キャッシュおよび Oracle Internet Directory サーバー・エントリ・キャッシュ（使用可能な場合）です。バッファ・キャッシュおよびエントリ・キャッシュのヒット率を高くするには、各領域に十分なメモリーを割り当てる必要があります。次の計算式は、エントリ・キャッシュ内に 'N' 個のエントリをキャッシュするために必要な RAM の量の概算を示しています。

N * [150+ {attrs_per_entry + 6) * (avg_attrname_len + avg_attr_size + 40) }]
* 1.3

関連項目： SGA のチューニングの詳細は、第 25 章「ディレクトリのチューニングに関する考慮事項」を参照してください。

表 24-12 に、異なるディレクトリ構成別に最小メモリー要件を示します。

表 24-12 ディレクトリ構成別最小メモリー要件

ディレクトリのタイプ	エントリ件数	最小メモリー
小	600,000 未満	512MB
標準	600,000 ～ 2,000,000	1GB
大	2,000,001 以上	2GB

Acme Corporation の例では、ディレクトリ内のエントリ数は約 1,000,000（100 万）です。パフォーマンスを最大にするには、2GB を選択してください。

ネットワーク要件

ほとんどの場合、ネットワークがボトルネックとなることはありません。ただし、容量計画の段階では、慎重に考慮する必要があります。クライアントが Oracle Internet Directory とのメッセージ送受信用に十分なネットワーク帯域幅を確保していない場合は、全体的なスループットが非常に低く感じられます。たとえば、毎秒 800 の検索を処理するように Oracle Internet Directory を構成しても、Oracle ディレクトリ・サーバーを実行しているコンピュータへのアクセスに使用できるのが 10Mbps のネットワーク（10-Base-T イーサネット）のみなので、使用可能な帯域幅が 60 パーセントの場合、クライアントは、スループットが毎秒 600 検索操作であると理解します（各検索操作で 1024 バイトがネットワークで移送されると仮定した場合）。
表 24-13 に、2 種類の操作（1024 バイトの転送を必要とする操作と 2048 バイトの転送を必要とする操作）について、10Mbps と 100Mbps の 2 つのタイプのネットワークで、帯域幅の使用可能率が異なる場合の最大可能スループット（操作 / 秒）を示します。

表 24-13 2 種類の操作の最大可能スループット

帯域幅の使用可能率	操作 / 秒 1024 バイト		操作 / 秒 2048 バイト	
	10 Mbps	100 Mbps	10 Mbps	100 Mbps
30	300	3000	150	1500
40	400	4000	200	2500
50	500	5000	250	3500
60	600	6000	300	4500
70	700	7000	350	5500
80	800	8000	400	6500
90	900	9000	450	7500

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 時間当たり 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

この項の項目は次のとおりです。

CPU 構成

Oracle Internet Directory に関する CPU のサイズ設定は、ユーザーの作業負荷に直接影響を与えます。CPU 構成は、次の要因によって決まります。

- サポートする同時操作の数。この数は、操作を同時に実行しているユーザー数に直接依存します。
- 各操作の許容待機時間。たとえば、電子メール・アプリケーションの場合、1 操作ごとの待機時間が 100 ミリ秒であることが理想的ですが、多くの場合、500 ミリ秒でも許容範囲内です。

作業負荷の増加に従って、システムに CPU リソースを追加できますが、CPU リソースを追加しても、すべての操作にそのままスケーラビリティがもたらされることはほとんどありません。これは、多くの操作が単に CPU のみに制限されるわけではないためです。このため、すべてのベンダーから一般的に入手可能なパフォーマンス特性（SPECint_rate95 ベースライン）によって、コンピュータの処理能力が分類されます。この数値は、一連の整数テストから導き出され、すべてのシステム・ベンダーおよび SPEC の Web サイト（`http://www.spec.org`）から入手可能です。

注意： SPECint_rate95 の数値を、通常の SPECint95 のパフォーマンス数値と混同しないでください。SPECint95 のパフォーマンス数値は、特定の CPU の整数処理能力に関する知識を提供します（CPU が複数あるシステムの場合、この数値は通常正規化されます）。SPECint_rate95 は、正規化を実行せずにシステム全体の整数処理能力を提供します。

Oracle Internet Directory は、SMP コンピュータで複数の CPU を効率的に使用しているため、SPECint_rate95 の数値に基づいてコンピュータを分類できます。SPECint_rate95 の範囲では、一般的に公表されている結果と異なるベースラインの数値が選択されています。これは、一般的に公表されている結果が、実際にはコンピュータのピーク時のパフォーマンスであるのに対して、ベースラインの数値は、通常の状況下のパフォーマンスを表しているためです。

CPU 要件の概算

Oracle Internet Directory は、通常 Oracle Database 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、表 24-14 のように概算で見積もることができます。

表 24-14 CPU 要件の概算

使用方法	CPU の数	SPECint_rate95 ベースライン	システム
部門単位	2	60 ～ 200	Compaq AlphaServer 8400 5/300（300MHz × 2）
組織単位	4	200 ～ 350	IBM RS/6000 J50（200MHz × 4）
会社単位	4+	350+	Sun Ultra 450（296 MHz × 4）

CPU 要件の詳細な計算

CPU の消費量はいくつかの要因によって変化するため、所定の配置サイトですべての操作に対する CPU 要件を判断することは困難です。次のような要因があります。

- 操作の種類（ベース検索、サブツリー検索、変更、追加など）。
- SSL モードを使用可能にしているかどうか（SSL を使用すると、15 ～ 20% 多く CPU リソースが消費されます）。
- Oracle Internet Directory サーバーのエントリ・キャッシュを使用可能にしているかどうか（ヒット率が CPU 使用量に影響を与えるため）。
- 検索で返されるエントリの数。
- 検索操作中にチェックする必要があるアクセス制御ポリシーの数。

SSL を除くほとんどの場合、Oracle Internet Directory サーバー・プロセスとデータベースとの間にかなりの待機時間があることが予想されます。Oracle Internet Directory サーバー・プロセスのスレッドがデータベースの応答を待っているときは、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・リクエストの作業に充てることができます。この結果、操作のいかなる組合せでも、同時クライアントと Oracle Internet Directory サーバー・プロセスの組合せが常に実現でき、CPU 使用率が 100% になります。この場合は、CPU がボトルネックとなります。

この事実を考慮し、メッセージング・タイプのサブツリー検索操作を採用し、操作のスループットを低下させずに、指定された数の同時操作をサポートするために必要な CPU リソースを算出しています。メッセージング検索操作には、サブツリー有効範囲、単純な完全一致フィルタおよび 1 つのエントリの結果セットが関係します。Oracle Internet Directory 10*g*（10.1.4.0.1）の場合は、次のようになります。

SPECint_rate95 ベースライン = 0.5 ×（ピーク時のスループットでの同時操作最大数）

これは、操作のスループットを低下させずに、600 の同時クライアントをサポートする必要がある場合は、（0.5 × 600）= 300 以上の SPECint_rate95 ベースライン評価のコンピュータが必要であることを意味します。

操作のスループットについては、Oracle Internet Directory 10*g*（10.1.4.0.1）の場合、次のようになります。

SPECint_rate95 ベースライン = 0.4 ×（サポートされる同時操作最大数での操作のスループット）

これは、サポートされる同時操作数として指定した最大数に、毎秒 750 操作のスループットが必要な場合は、（0.4 × 750）= 300 以上の SPECint_rate95 ベースライン評価のコンピュータが必要であることを意味します。

Oracle Internet Directory は、追加 CPU リソースを確実に調整することが証明されています。これは次のことを意味します。

- 指定した操作同時実行性については、CPU リソースを追加することによって、より高いスループット（待機時間がより短い）の操作を達成できます。
- 指定した操作スループット（待機時間）については、別途の CPU リソースを追加することによって、より高い操作同時実行性を達成できます。

Acme Corporation の例に戻り、各クライアントにわずかな待機時間を見込みながら、500 の同時メッセージング・タイプのサブツリー検索操作をサポートする適切な CPU リソースが必要であると仮定します。安全係数を 20% とすると、CPU 要件の仮見積りは、360 以上の SPECint_rate95 ベースラインを持つコンピュータとなります。

Acme Corporation の容量計画のまとめ

ここまでの各項で、容量計画に関係する様々なコンポーネントを説明するとともに、それぞれのコンポーネントを、Acme Corporation という仮想の会社における Oracle Internet Directory の配置に適用する方法も紹介しました。この項では、前述のすべての推奨事項を簡単に要約して示します。最初の仮定は次のとおりです。

- ディレクトリ全体のサイズ : 3,200,000 エントリ（320 万）
- ユーザー数 : 40,000
- アプリケーションのタイプ : IMAP メッセージング
- ピーク時の検索率 : 500 クライアントの同時実行性で 750 検索 / 秒

この要件とその他の仮定に基づいて、次の推奨事項を提示しました。

- ディスク領域 : 5GB ～ 8GB
- メモリー : 2GB
- ネットワーク : 100 Base-T
- CPU: SPECint_rate95 の数値が 360 以上の CPU

サイズ設定の計算を直観的に理解できるように、いくつか単純な仮定を使用しました。

25

ディレクトリのチューニングに関する考慮事項

第 24 章「ディレクトリの容量計画」の説明に従って容量計画を完了し、必要なハードウェアを用意した後は、ハードウェアとソフトウェアの組合せで必要なレベルのパフォーマンスが得られることを確認する必要があります。この章では、Oracle Internet Directory のチューニングに関するガイドラインを示します。この章の項目は次のとおりです。

- 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
- 接続識別名のキャッシング
- 検索の最適化
- 制限時間モードの設定
- クライアント / サーバー間の接続のタイムアウトの設定
- 書込み操作のタイムアウトの設定

関連項目： L-9 ページの「ディレクトリの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 秒当た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。

Microsoft Windows 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 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 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。

Oracle Database 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

関連資料：

- `utlbstat.sql` および `utlestat.sql` の詳細は、Oracle Database ドキュメント・ライブラリの『Oracle Database リファレンス』を参照してください。
- Statspack の詳細は、『Oracle Database パフォーマンス・チューニング・ガイド』を参照してください。
- DBMS_STATS パッケージの ANALYZE ファンクションの詳細は、Oracle Database ドキュメント・ライブラリの『Oracle Database 概要』を参照してください。

オペレーティング・システム・ツール以外に、カスタマ環境で使用されている LDAP アプリケーションも待機時間やスループットの測定方法を提供しています。

さらに、様々なデータベース ods スキーマ・オブジェクトを分析して統計を見積もるために、*$ORACLE_HOME*/ldap/admin にあるデータベース統計収集ツール（oidstats.sql）が提供されています。

> **関連資料：**『Oracle Identity Management ユーザー・リファレンス』の oidstats.sql コマンドライン・ツールのリファレンス

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 24 章「ディレクトリの容量計画」では、所定のアプリケーション負荷に対して必要となる CPU 能力の概算を示しましたが、十分にチューニングされていないと、CPU リソースが効率的に使用されない原因となります。次の各項目のいずれかに該当する場合は、CPU リソースのチューニングを考慮してください。

- 最大負荷時に CPU 稼働率が 100% の場合。
- 最大負荷時に CPU が十分に活用されていない場合。システムにかなりのアイドル時間があり、このアイドル時間が高負荷時でもなくならない場合。

内部的なベンチマークでは、CPU リソースの約 70 ～ 75% が Oracle Internet Directory のプロセスで消費され、残りの約 25 ～ 30% がデータベース接続に対応する Oracle のフォアグラウンド・プロセスで消費されている場合に、Oracle Internet Directory が最も効率よく実行されることが示されています。CPU 使用量を監視すると同時に、システム領域で使用されている時間とユーザー領域で使用されている時間の割合を監視することも重要です。内部的なベンチマークでは、約 85% がユーザー時間、約 15% がシステム時間の場合にスループット値が最大であることが示されています。

この項の項目は次のとおりです。

- 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。表 25-1 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。

表 25-1 ORCLSERVERPROCS および ORCLMAXCC パラメータの推奨値

ORCLSERVERPROCS	ORCLMAXCC	操作スループットの低下なしでサポートされる同時クライアントの数	接続を切断せずにサポートされるクライアントの数	必要な CPU の数
1	2	40		1
2	10	400	800	2
4	10	800	1600	4
8	10	1600	3200	8

同時クライアントの数が 500 で、ORCLSERVERPROCS の値が 4、ORCLMAXCC の値が 10 の場合を例にとると、次のような構成になります。

- 4 個のサーバー・プロセスが作成されます。
- 各サーバー・プロセスは、実際に作業するワーカー・スレッドを 10 個起動します。
- 各サーバー・プロセスは、ワーカー・スレッド間で共有される 16（10+5+1）個のデータベース接続のプールをメンテナンスします。

Oracle Internet Directory は、操作スループットおよびクライアント同時実行性の両面に関して、CPU リソースを確実に調整します。前述の表より、4 つの CPU があり、クライアント n 台の同時実行性に対して、毎秒 p 件のピーク時操作スループットを維持できるとします。

CPU の数の追加またはより高速な CPU の使用によって、次の利点が得られます。

- クライアント n 台の同じ同時実行性に対して、p 件を超える高いスループットを達成できます。
- n 台を超える高い同時実行性に対して、同じ p 件の操作スループットを維持できます。

最大負荷時の CPU 使用量が 100% 未満で、かなりの割合の時間（5% 以上）システムがアイドル状態の場合は、Oracle Internet Directory プロセスの構成数が少なく、CPU リソースを十分利用していないことを示しています。この問題を解決するためには、ORCLSERVERPROCS と ORCLMAXCC の値を計画的に増やして、CPU 稼働率が 100% になり、システム時間とユーザー時間が次の割合になるように調整してください。

- ユーザー時間 : 85% 以上
- システム時間 : 15% 以下

Oracle のフォアグラウンド・プロセスに関する CPU のチューニング

次の条件の両方に該当する場合のみ、Oracle のフォアグラウンド・プロセスに関する CPU リソースのチューニングを考慮してください。

- 最大負荷時の CPU 稼働率が 100% に近い場合
- Oracle のフォアグラウンド・プロセスが使用可能な全 CPU リソースの 30% 以上を消費している場合

Oracle のフォアグラウンド・プロセスが過度に CPU を消費している場合は、Oracle Internet Directory のデータベースに対する問合せが、多数の CPU サイクルを使用していることを示しています。データベースが実行するこの種の基本的な操作の場合は、ユーザーが制御できる部分はほとんどありませんが、次のことを試してください。

- データベース上の ODS ユーザーに関連付けられているすべての表と索引に関するデータベース統計を、`ANALYZE` コマンドを使用して収集します。この統計は、コストベースのオプティマイザが、Oracle Internet Directory で生成される問合せ用に、より適した実行計画を作成するために役立ちます。統計の収集には、`$ORACLE_HOME/ldap/admin/oidstats.sql` 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。

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、Oracle Internet Directory 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 Oracle Database 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、Oracle Database 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。

この項の項目は次のとおりです。

Oracle Database 用の SGA のチューニング

SGA は、Oracle Database 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。

> **関連資料：** SGA を適切なサイズに設定する方法の詳細は、Oracle Database ドキュメント・ライブラリの『Oracle Database パフォーマンス・チューニング・ガイド』を参照してください。このマニュアルは、SGA サイズがページング・スワッピング・アクティビティを増やさないようにする方法について説明しています。後者はパフォーマンスに悪影響を及ぼします。

SGA の使用可能なサイズを設定した後、2 つの主なチューニング項目を考慮してください。

- 共有プール・サイズ
- バッファ・キャッシュ・サイズ

共有プール・サイズの初期見積りは、前項で決めた同時データベース接続ごとに 0.5MB です。

この見積りで、SGA 合計の 30% を超える領域を消費する場合は、SGA 合計の 30% を使用してください。

残りの使用可能な SGA サイズの 60% を、データベースに対するブロック・サイズで除算し、DB_BLOCK_BUFFERS の数にこの値を使用します。この 2 つの値は初期見積りであり、BSTAT/ESTAT やその他の RDBMS 監視ツールを使用してさらに詳細に見積もると、最大のパフォーマンスを得るための正確なサイズを設定できます。

メモリーがボトルネックとなっているシステムに関するその他の方法

データベースと Oracle ディレクトリ・サーバーを同じコンピュータ上で実行するためのメモリーが不足している場合は、データベースを別のコンピュータに配置できます。

セキュリティ・イベント追跡のチューニング

DSA 構成属性の orcloptracknumelemcontainers および orcloptrackmaxtotalsize は、セキュリティ・イベント追跡に使用されるメモリー量を制御します。

イベント追跡に割り当てられたメモリーのチューニング

DSA 構成設定属性 orcloptracknumelemcontainers により、Oracle Internet Directory サーバー内でセキュリティ・イベント追跡に割り当てられるメモリー内キャッシュ・コンテナ数を選択できます。この属性には 2 つのサブタイプがあります。1stlevel と 2ndlevel です。1stlevel サブタイプは、操作を行っているユーザーに関する情報を格納するためのメモリー内キャッシュ・コンテナ数を設定するためのものです。2ndlevel サブタイプは、比較操作にのみ適用され、詳細な比較操作統計がプログラムされている場合に、userpassword を比較され、追跡されるユーザーに関する情報用のメモリー内キャッシュ・コンテナの数を設定します。

両方のサブタイプのデフォルト値は 255 です。これらのサブタイプに適切な値は、環境内でのユーザー数や、ディレクトリへのアクセスに使用されるアプリケーション数によって、次のように異なります。

- 多数のエンド・ユーザーにかわって複数のアプリケーションが操作を実行する配置では、1stlevel を、アプリケーション数に比例した数値に、ディレクトリに直接アクセスするエンド・ユーザー用の数百を加えた値に設定します。2ndlevel は、エンド・ユーザー数に比例した値に設定します。
- エンド・ユーザー自身が操作を実行する配置では、1stlevel をエンド・ユーザー数に比例した値に設定し、2ndlevel は小さな値（25 など）に設定します。
- 一般的な比例値は、5 分の 1 です。大部分の環境では、比率は 10 分の 1 と 2 分の 1 の間です。

配置で必要な場合は、orcloptracknumelemcontainers の値を、セキュリティ・イベント収集が有効になっている場合にのみ設定します。

注意： 1stlevel の値のみを構成、または両方のサブタイプの値を構成した後、次の統計周期の 1 サイクルについてのセキュリティ・イベント情報は収集されません。

各操作に使用されるメモリーのチューニング

DSA 構成属性 orcloptrackmaxtotalsize は、セキュリティ・イベント追跡で各タイプの操作に使用できる RAM の最大バイト数を指定します。ディレクトリ・サーバーが、1 つの操作に関して収集される情報に設定したこの制限を超えると、サーバーは新しい情報の収集を停止し、サーバー・ログ・ファイルに適切なメッセージを記録します。比較操作の場合、ディレクトリ・サーバーではこの属性値の 2 倍のメモリーを使用します。これは、比較操作を実行するユーザーと、パスワードを比較されているユーザーに関する情報を合せた量です。
orcloptrackmaxtotalsize のデフォルト値は 100MB で、大部分の配置ではこれで十分です。この値は 200MB まで増やせます。

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

関連資料： ディスク I/O の均衡化とチューニングの概要は、Oracle Database ドキュメント・ライブラリの『Oracle Database パフォーマンス・チューニング・ガイド』を参照してください。

データベースのチューニング

この項では、Oracle Internet Directory のインストールに有効な、その他のチューニング可能なパラメータについて説明します。

表 25-2 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。

表 25-2 様々なクライアント負荷に対する RDBMS の推奨値

パラメータ	同時 LDAP クライアントの数が 500 の場合	同時 LDAP クライアントの数が 1000 の場合	同時 LDAP クライアントの数が 1500 の場合	同時 LDAP クライアントの数が 2000 の場合
OPEN_CURSORS	200	200	200	200
SESSIONS	225	600	800	1200
DATABASE_BLOCK_BUFFERS	200 ～ 250MB	200 ～ 250MB	200 ～ 250MB	200 ～ 250MB
DATABASE_BLOCK_SIZE	8192	8192	8192	8192
SHARED_POOL_SIZE	30 ～ 40MB	30 ～ 40MB	30 ～ 40MB	30 ～ 40MB
PROCESSES	400	800	1000	1500

この項では、チューニング可能な各 RDBMS パラメータについての詳細を説明します。この項の項目は次のとおりです。

- 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 Oracle Database 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 のレプリケーションは、データベースのレプリケーションに依存しています。Oracle Internet Directory のレプリケーションを使用する場合は、JOB_QUEUE_PROCESSES および PARALLEL_MIN_SERVERS の各データベース・パラメータを 1 以上に設定します。次に例を示します。

```
JOB_QUEUE_PROCESSES=1
PARALLEL_MIN_SERVERS=1
```

Oracle Internet Directory 10*g*（10.1.4.0.1）では、`Database_block_size` に指定できる絶対最小値は 4KB です。

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た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、Oracle Database ドキュメント・ライブラリの『Oracle Database Net Services 管理者ガイド』および『Oracle Database 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、25-5 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 ログ領域リクエスト /REDO エントリ）> 1/5000 となるように十分に大きい値を使用して、LGWR プロセスが遅延しないようにしてください。この数値は全体でも、可変の SGA サイズにほとんど影響しないサイズであるため、この値の多少の増加が問題となることはありません。

エントリ・キャッシング

Oracle Internet Directory 10*g*（10.1.4.0.1）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も大きな効果が得られます。次のような小中規模のディレクトリ配置では、エントリ・キャッシュの使用をお薦めします。

- ディレクトリ・エントリのワーキング・セットが合理的に完全にキャッシュできる場合
- クライアントの同時実行性が単一のディレクトリ・サーバー・インスタンスで処理できる場合

内部ベンチマークでは、エントリのワーキング・セットが数十万のエントリであるディレクトリ配置の場合、エントリ・キャッシュによって、最大 1000 の同時クライアントに対する操作のスループットが 2 倍になることが示されています。

より大規模なディレクトリ・エントリのワーキング・セットが存在し、クライアントの同時実行性が高いディレクトリ配置では、マルチプロセス・ディレクトリ・サーバー・インスタンスが使用され、Oracle のバッファ・キャッシュによって、スケーラビリティが増大します。

> **関連項目：** エントリ・キャッシングを使用可能にして構成するために設定する属性の詳細は、7-7 ページの「システム操作属性の設定」を参照してください。

接続識別名のキャッシング

サーバーは、バインド操作を実行するたびに、バインドを実行している ID（接続識別名）が属する権限グループ（ネストされたグループも含む）のリストを算出します。各接続識別名について算出された権限グループのリストは、Oracle Internet Directory サーバーにキャッシュされます。属する権限グループをキャッシュできる接続識別名の数は、DSA 構成エントリ内の orclmaxconnincache 属性によって制御されます。デフォルト値は ID（接続識別名）25000 です。インストールのユーザーが 25000 人を超える場合は、orclmaxconnincache の値を増やします。たとえば、orclmaxconnincache を 50000 ユーザーに増やすには、次のような LDIF ファイルを作成します。

```
dn: cn=dsaconfig,cn=configsets,cn=oracle internet directory
changetype:modify
replace: orclmaxconnincache
orclmaxconnincache: 50000
```

それから、次のようなコマンドラインを使用します。

```
ldapmodify -p port -D cn=orcladmin -w adminPasswd -f filename
```

検索の最適化

この項の項目は次のとおりです。

- 大きいグループ・エントリの検索の最適化
- 偏りのある属性の検索の最適化

サブツリー検索の最適化

サブツリーの検索時に、サーバーは、設定された数のエントリが処理されるまで、クライアントに書込みを行いません。この数は、DSA 構成エントリ内の orclmaxentinber 属性によって制御されます。デフォルトではこの値は 5 です。エントリが 8000 バイトを超える場合は、この値を 1 に減らします。

大きいグループ・エントリの検索の最適化

member または uniquemember 属性のいずれかの値が、数千の属性値を持つグループ・エントリの検索では、待機時間が長くなる可能性があります。待機時間が受け入れ難いほど長いことがわかった場合、これを減らせる方法があります。

最も簡単な方法は、検索する属性数を減らすことです。グループ・エントリの属性をすべて取得する必要がないのであれば、待機時間を最適化するために検索リクエストに必須属性を指定します。

必須属性を指定してもなお待機時間が長すぎる場合は、待機時間を減らすために試せる 2 つのチューニング技術があります。これらは、「エントリ・キャッシュが使用可能な構成」と「エントリ・キャッシュが無効な構成」として知られています。

エントリ・キャッシュが使用可能な構成

この技術では、ラージ・グループ・エントリのエントリ・キャッシュへのキャッシュを試みます。これには、Oracle Internet Directory サーバー構成エントリ（cn=dsaconfig,cn=configsets,cn=oracle internet directory）内の orclEcacheMaxEntSize 属性の値を増やします。この属性は、キャッシュ・エントリの最大サイズを制御します。デフォルト値は 1M です。ラージ・グループ・エントリのサイズが orclEcacheMaxEntSize の値より大きい場合は、この値を、ラージ・グループ・エントリを確実にキャッシュできる大きな値に変更します。

注意：

- ラージ・グループに対する更新が頻繁になることが予想される場合は、このチューニング方法を使用しないでください。かわりに「エントリ・キャッシュが無効な構成」を使用してください。
- マルチサーバー LDAP インスタンスを使用している場合、またはこのサーバーが、同じデータベースに接続している別のマシン上の複数の Oracle Internet Directory サーバーとの高可用性構成の一部である場合、エントリ・キャッシュは自動的に無効になります。かわりに「エントリ・キャッシュが無効な構成」を使用してください。

エントリ・キャッシュが無効な構成

この技術では、ルート DSE エントリで orclecacheenabled 属性の値を 0（ゼロ）に設定して、エントリ・キャッシュを無効にします。この手順は次のとおりです。

1. Oracle Internet Directory インスタンスを停止します。
2. ODS ユーザーとして Oracle Internet Directory データベースにログインし、次の問合せを実行します。

```
DROP INDEX EI_ATTRSTORE;

CREATE BITMAP INDEX EI_ATTRSTORE ON DS_ATTRSTORE(ENTRYID,ATTRNAME)
TABLESPACE OLTS_ATTRSTORE
PARALLEL COMPUTE STATISTICS NOLOGGING;
```

3. Oracle Internet Directory インスタンスを起動します。

注意： この方法で EI_ATTRSTORE を再作成することにより、通常のメッセージング検索操作のパフォーマンスが 5% ～ 10% 低下する可能性がありますので、慎重にかつ必要なときのみ使用してください。

偏りのある属性の検索の最適化

通常の検索リクエストを処理する場合、ディレクトリ・サーバーは SQL 文を Oracle Database に送信します。指定された属性のレスポンス時間が、属性の値によって大きく異なる場合、この属性は偏りのある属性であるとみなされます。たとえば、my_attribute=value1 と my_attribute=value2 の検索で、レスポンス時間が大きく異なる場合、my_attribute は偏りのある属性であるとみなされます。

このような属性を、dsaconfig エントリにある orclskewedattribute 属性の値として追加することにより、検索時のレスポンス時間を均一にできます。dsaconfig エントリの識別名は、cn=dsaconfig,cn=configsets,cn=oracle internet directory です。

デフォルトでは、objectclass 属性は、orclskewedattribute 属性内に値としてリストされます。

Oracle Directory Manager を使用した偏りのある属性の検索の最適化

データベースへの問合せを最適化する手順は、次のとおりです。

1. ナビゲータ・ペインで、「Oracle Internet Directory サーバー」を展開して、ディレクトリ・サーバー・インスタンスを選択します。
2. 右側のペインで「**問合せの最適化**」タブを選択します。この「**問合せの最適化**」タブ・ページの各フィールドの説明は、A-30 ページの表 A-44 を参照してください。
3. 「**問合せの最適化**」タブ・ページの「**低カーディナリティの属性**」フィールドで、偏りのある属性として指定する属性を入力します。
4. 「**適用**」を選択します。

ldapmodify を使用した偏りのある属性の検索の最適化

偏りのある属性の検索を最適化するには、ldapmodify を使用して、その属性を orclskewedattribute 属性の値として追加します。

たとえば、my_attribute を orclskewedattribute 属性に追加するには、次のように入力します。

```
ldapmodify –D "cn=orcladmin" –w password -h host -p port <<!
dn: cn=dsaconfig,cn=configsets,cn=oracle internet directory
changetype: modify
add: orclskewedattribute
orclskewedattribute: my_attribute
!
```

制限時間モードの設定

7-7 ページの「システム操作属性の設定」の説明に従って、サーバー処理の制限時間を設定する場合は、検索の完了までの最大時間（秒）を指定します。サーバーのパフォーマンスを調整する場合は、検索制限時間モードを厳密に設定するか、おおよその時間に設定することもできます。正確な時間に設定すると、検索は必ず指定した秒数で終了します。おおよその時間に設定すると、検索は指定した秒数から 2 秒の範囲内で終了します。作業負荷が低い場合は、後者の方がより高いパフォーマンスを得られます。

Oracle Directory Manager を使用した制限時間モードの設定

制限時間モードを設定する手順は、次のとおりです。

1. ナビゲータ・ペインで、「Oracle Internet Directory サーバー」を展開して、ディレクトリ・サーバー・インスタンスを選択します。
2. 右側のペインで「**問合せの最適化**」タブを選択します。
3. 「**問合せの最適化**」タブ・ページの「時間制限モード」フィールドで、「**精度**」または「**近似**」を選択します。
4. 「**適用**」を選択します。

ldapmodify を使用した制限時間モードの設定

正確な時間か、おおよその時間のいずれかの検索制限時間モードを指定するには、orcltlimitmode 属性を設定します。値 0 は正確な時間で、値 1 はおおよその時間です。デフォルト値は 1 です。

クライアント / サーバー間の接続のタイムアウトの設定

クライアントとディレクトリ・サーバー間の接続のアイドル・タイムを指定できます。クライアント / サーバー間の接続のタイムアウトを設定する手順は、次のとおりです。

1. ナビゲータ・ペインで、「Oracle Internet Directory サーバー」を展開して、ディレクトリ・サーバー・インスタンスを選択します。
2. 右側のペインで「**問合せの最適化**」タブを選択します。
3. 「**問合せの最適化**」タブ・ページの「**LDAP 接続タイムアウト**」フィールドに、接続が終了するまで、ディレクトリ・クライアントがアイドル状態を維持できる最大秒数を入力します。デフォルトは 0 です。これはタイムアウトがないことを意味します。
4. 「**適用**」を選択します。

書込み操作のタイムアウトの設定

LDAP クライアントが操作を開始し、サーバーに対して構成された秒数で応答しない場合、サーバーは接続をクローズします。この秒数は、DSA 構成エントリ内の orclnwrwtimeout 属性によって制御されます。デフォルトは 300 秒です。これを 500 秒に増やすには、次のような LDIF ファイルを作成します。

```
dn: cn=dsaconfig,cn=configsets,cn=oracle internet directory
changetype:modify
replace: orclnwrwtimeout
orclnwrwtimeout: 500
```

それから、次のようなコマンドラインを使用します。

```
ldapmodify -p port -D cn=orcladmin -w adminPasswd -f filename
```

26

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

ガベージとは、ディレクトリで不要になっているが領域を使用しているデータを指します。結果として、このような不要なデータや古いデータでディスクが一杯になり、ディレクトリのパフォーマンスが低下します。ディレクトリからこの不要なデータを削除する処理を、ガベージ・コレクションと呼びます。

この章の項目は次のとおりです。

Oracle Internet Directory ガベージ・コレクション・フレームワークの概要

ガベージ・コレクタは、ディレクトリから不要なデータを削除する、バックグラウンドのデータベース・プロセスです。Oracle Internet Directory ガベージ・コレクション・フレームワークには、ガベージ・コレクタの標準セットがあります。このフレームワークにより、これらのコレクタを変更できます。また、Oracle Internet Directory 統計情報コレクタでも、Oracle Internet Directory ガベージ・コレクション・フレームワークが使用されます。

この項の項目は次のとおりです。

- Oracle Internet Directory ガベージ・コレクション・フレームワークのコンポーネント
- Oracle Internet Directory ガベージ・コレクションの動作
- ガベージ・コレクタ・エントリと Oracle Internet Directory 統計情報コレクタ・エントリ
- マルチマスター・レプリケーションの変更ログの削除

Oracle Internet Directory ガベージ・コレクション・フレームワークのコンポーネント

この項では、Oracle Internet Directory ガベージ・コレクション・フレームワークを構成するコンポーネントであるガベージ・コレクション・プラグインとバックグラウンドのデータベース・プロセスについて説明します。

ガベージ・コレクション・プラグイン

Oracle Internet Directory のガベージ・コレクションは、ガベージ・コレクタの管理リクエストを受け取るガベージ・コレクション・プラグインを使用します。このプラグインは、Oracle Internet Directory とともにインストールされ、デフォルトで使用可能になります。このプラグインのエントリは、`cn=plugin,cn=subconfigsubentry` です。

このプラグインには、3 つのトリガーがあります。

- ガベージ・コレクション・ジョブの作成に使用するプラグイン・トリガー。識別名は、次のとおりです。
  `cn=Add PurgeConfig,cn=plugin,cn=subconfigsubentry`
- ガベージ・コレクション・ジョブの変更に使用するプラグイン・トリガー。識別名は、次のとおりです。
  `cn=Modify PurgeConfig,cn=plugin,cn=subconfigsubentry`
- ガベージ・コレクション・ジョブの削除に使用するプラグイン・トリガー。識別名は、次のとおりです。
  `cn=Delete PurgeConfig,cn=plugin,cn=subconfigsubentry`

> **関連資料：** ガベージ・コレクション・プラグインの属性のリストおよび説明は、『Oracle Identity Management ユーザー・リファレンス』の「Oracle Internet Directory 構成のスキーマ要素」を参照してください。

バックグラウンドのデータベース・プロセス

ガベージ・コレクション・プラグインによって起動されるバックグラウンドのデータベース・プロセスには、ガベージ・コレクタや Oracle Internet Directory 統計情報コレクタがあります。

ガベージ・コレクタ 次のガベージ・コレクタの動作を設定して管理できます。

- 起動時間
- 削除するデータの経過時間
- 実行頻度
- 削除するデータの種類
- 一度に削除するエントリの数

事前定義済ガベージ・コレクタ Oracle Internet Directory のデフォルトのインストールに含まれている事前定義済ガベージ・コレクタは、次のとおりです。

- 監査ログのガベージ・コレクタ : ディレクトリを監査するために作成されたエントリのうち、使用されなくなったものをクリーンアップします。このガベージ・コレクタのコンテナは、次のとおりです。
  `cn=auditlog purgeconfig,cn=purgeconfig,cn=subconfigsubentry`
- 変更ログのガベージ・コレクタ : ディレクトリ内のコンシューム済変更ログ・エントリをクリーンアップします。このガベージ・コレクタのコンテナは、次のとおりです。
  `cn=changelog purgeconfig,cn=purgeconfig,cn=subconfigsubentry`
- 一般統計のガベージ・コレクタ : ディレクトリの一般統計情報を監視するために Oracle Internet Directory サーバー管理機能により作成され、使用されなくなったエントリをクリーンアップします。このガベージ・コレクタのコンテナは、次のとおりです。
  `cn=general stats purgeconfig,cn=purgeconfig,cn=subconfigsubentry`
- 一般統計のガベージ・コレクタ : ディレクトリの一般統計情報を監視するために Oracle Internet Directory サーバー管理機能により作成され、使用されなくなったエントリをクリーンアップします。このガベージ・コレクタのコンテナは、次のとおりです。
  `cn=health stats purgeconfig,cn=purgeconfig,cn=subconfigsubentry`
- セキュリティおよびリフレッシュ・イベントのガベージ・コレクタ : ディレクトリのセキュリティおよびリフレッシュ・イベントを監視するために Oracle Internet Directory サーバー管理機能により作成され、使用されなくなったエントリをクリーンアップします。このガベージ・コレクタのコンテナは、次のとおりです。
  `cn=secrefresh events purgeconfig,cn=purgeconfig,cn=subconfigsubentry`
- システム・リソース・イベントのガベージ・コレクタ : ディレクトリのシステム・リソース・イベントを監視するために Oracle Internet Directory サーバー管理機能により作成され、使用されなくなったエントリをクリーンアップします。このガベージ・コレクタのコンテナは、次のとおりです。
  `cn=sysresource events purgeconfig,cn=purgeconfig,cn=subconfigsubentry`
- 削除済とマークされたエントリのガベージ・コレクタ : ディレクトリ内で削除済とマークされた、使用されなくなったエントリをクリーンアップします。このガベージ・コレクタのコンテナは、次のとおりです。
  `cn=tombstone purgeconfig,cn=purgeconfig,cn=subconfigsubentry`
- LDAP パフォーマンス監視ガベージ・コレクタ : LDAP サーバー・パフォーマンス統計データをクリーンアップします。このガベージ・コレクタのコンテナは、次のとおりです。
  `cn=perf stats purgeconfig,cn=purgeconfig,cn=subconfigsubentry`
- LDAP バインド・パフォーマンス監視ガベージ・コレクタ : セキュリティ・イベント追跡用に収集されたバインド・パフォーマンス・データをクリーンアップします。このガベージ・コレクタのコンテナは、次のとおりです。
  `cn=bindsec stats purgeconfig,cn=purgeconfig, cn=subconfigsubentry`

- LDAP バインド・パフォーマンス監視ガベージ・コレクタ : セキュリティ・イベント追跡用に収集されたバインド・パフォーマンス・データをクリーンアップします。このガベージ・コレクタのコンテナは、次のとおりです。
  `cn=comparesec stats purgeconfig, cn=purgeconfig,cn=subconfigsubentry`
- LDAP 比較パフォーマンス監視ガベージ・コレクタ : セキュリティ・イベント追跡用に収集された比較失敗パフォーマンス・データをクリーンアップします。このガベージ・コレクタのコンテナは、次のとおりです。
  `cn=comparefailure stats purgeconfig,cn=purgeconfig,cn=subconfigsubentry`

関連資料 :

- 14-15 ページの「Oracle Internet Directory サーバー管理機能の機能」
- 『Oracle Identity Management ユーザー・リファレンス』の Oracle Internet Directory 構成のスキーマ要素に関する項

注意 : 事前定義済ガベージ・コレクタは削除しないことをお薦めします。これらのガベージ・コレクタを 1 つ以上削除すると、不要なデータが増加し、最終的には使用可能なすべてのディスク領域を使い果すことになります。

ただし、動作をカスタマイズするために、事前定義済ガベージ・コレクタを変更してもかまいません。

Oracle Internet Directory 統計情報コレクタ 次の Oracle Internet Directory 統計情報コレクタの動作を設定して管理できます。

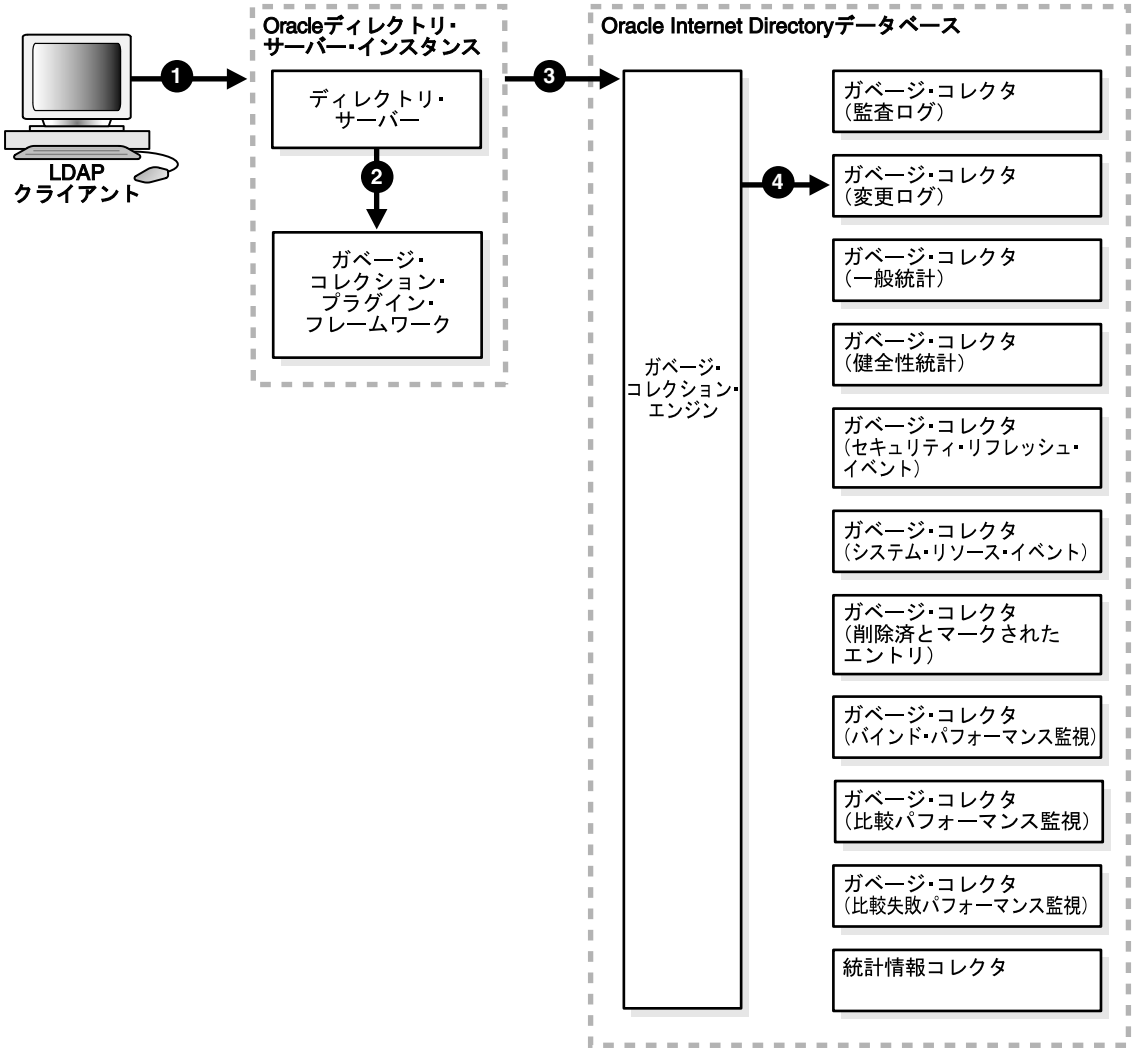
- 起動時間
- 実行頻度

Oracle Internet Directory 統計情報コレクタは、Oracle Internet Directory に関する統計情報を収集します。このバックグラウンド・データベース・プロセスのコンテナは、次のとおりです。
`cn=oidstats_config`
`cn=purgeconfig,cn=subconfigsubentry.`

Oracle Internet Directory ガベージ・コレクションの動作

図 26-1 に、変更ログ・エントリを削除するガベージ・コレクタの動作の例を示します。

図 26-1 例 : 変更ログ・エントリのガベージ・コレクション



26-5 ページの図 26-1 の例に示すとおり、ガベージ・コレクション・プロセスは、次のように動作します。

1. LDAP クライアントが、特定のガベージ・コレクション操作リクエストをディレクトリ・サーバーに送信します。これらの操作には、削除されたとみなされるエントリ、変更ログのエントリ、監査ログのエントリの削除などがあります。
2. ディレクトリ・サーバーが、リクエストをガベージ・コレクション・プラグインに渡します。
3. ガベージ・コレクション・プラグインが、Oracle Internet Directory で指定されたデータベースのガベージ・コレクション・エンジンにリクエストを送信します。
4. ガベージ・コレクション・エンジンが、対応するバックグラウンド・データベース・プロセス（この場合は、変更ログのガベージ・コレクタ）をトリガーします。バックグラウンド・データベース・プロセスは、構成設定エントリに指定されているパラメータに従って動作します。

ガベージ・コレクタ・エントリと Oracle Internet Directory 統計情報コレクタ・エントリ

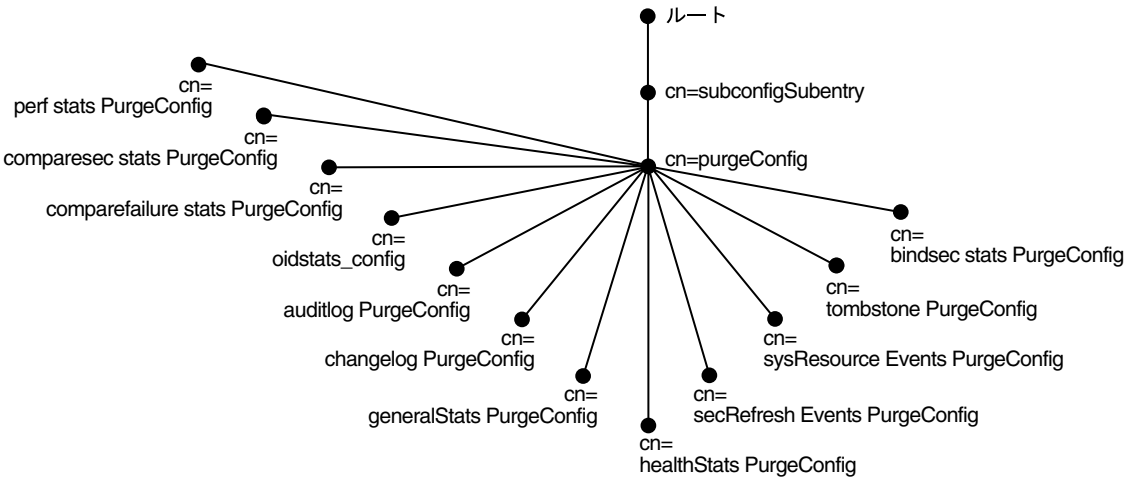
各ガベージ・コレクタ・エントリは、動作を指定する属性を持ち、エントリ `cn=subconfigsubentry` の直下にあるエントリ `cn=purgeconfig` に存在します。

> **関連資料：** ガベージ・コレクタの各属性の詳細は、『Oracle Identity Management ユーザー・リファレンス』の「Oracle Internet Directory 構成のスキーマ要素」を参照してください。

Oracle Internet Directory 統計情報コレクタ・エントリは、属性を持ち、エントリ `cn=subconfigsubentry` の直下にあるエントリ `cn=purgeconfig` にも存在します。

図 26-2 に、これらのエントリの場所を示します。

図 26-2 ディレクトリ情報ツリー内のガベージ・コレクション・エントリ



マルチマスター・レプリケーションの変更ログの削除

レプリケーションと Oracle Directory Integration Platform はいずれも、変更ログを使用して、サプライヤ・ディレクトリの情報をコンシューマ・ディレクトリに伝達します。変更ログはすべて `ods_chg_log` という表に格納されます。また、レプリケーション変更ログは `asr_chg_log` に格納されます。変更ログのガベージ・コレクタが実行されると、どの変更ログ・コンシューマからも必要とされなくなった変更ログが削除されます。これで、Oracle Internet Directory データベースで変更ログ・ストアが大きくなりすぎるのを防ぐことができます。

変更ログの削除方法

変更ログのガベージ・コレクタでは、次の 2 つの方法で削除する変更ログを決定します。

- 変更番号ベースの削除

  変更番号ベースの削除では、すべての変更ログ・コンシューマの変更ステータスが考慮されます。つまり、変更ログは、すべてのコンシューマによってコンシュームされてから削除されます。変更ログのガベージ・コレクタを実行すると、レプリケーション、Oracle Directory Integration Platform およびその他のコンシューマによってコンシュームされたすべての変更ログが削除されます。

- 時間ベースの削除

  時間ベースの削除は、特定の時間が経過した変更ログの削除を目的とする代替方法です。この方法では、すべての変更ログ・サブスクライバによってコンシュームされていないものであっても、古い変更ログが確実に削除されます。時間ベースの削除では、レプリケーションの変更ステータスが考慮されますが、その他のコンシューマの変更ステータスは考慮されません。変更ログのガベージ・コレクタは、レプリケーションで必要とされず、かつ `orclpurgetargetage` の時間以上が経過したすべての変更ログを削除します。`orclpurgetargetage` がゼロの場合、変更ログのガベージ・コレクタはすぐにこの動作を実行します。`orclpurgetargetage` が無効な数値である場合や、定義されていない場合のデフォルト値は、240 時間（10 日）です。レプリケーションで必要とされる変更ログは、レプリケーションでコンシュームされた後で削除されます。

  Oracle Directory Integration Platform を配置していて、時間ベースの削除を有効にする場合は、変更ログが Oracle Directory Integration Platform によって処理されてから削除されるように、`orclpurgetargetage` を十分に大きな値に設定してください。値を 240 にすると、10 日が経過してから変更ログが削除されます。

変更ログの削除の構成

時間ベースの削除は、変更ログ削除構成エントリの `orclpurgetargetage` 属性を変更して構成します。次の例では、120 時間（5 日）の時間ベース削除を構成しています。次のような LDIF ファイルを使用します。

```
dn: cn=changelog purgeconfig,cn=purgeconfig,cn=subconfigsubentry
changetype:modify
replace: orclpurgetargetage
orclpurgetargetage: 120
```

LDIF ファイル `mod.ldif` を適用するには、次のように入力します。

```
ldapmodify -p port -h host -D dn -w password -f mod.ldif
```

注意： 変更ログのガベージ・コレクタのコンテナは、次のとおりです。
`cn=changelog purgeconfig,`
`cn=purgeconfig,cn=subconfigsubentry`

関連資料：『Oracle Identity Management ユーザー・リファレンス』の「Oracle Internet Directory 構成のスキーマ要素」

Oracle Internet Directory ガベージ・コレクタの変更

この項の項目は次のとおりです。

Oracle Directory Manager を使用したガベージ・コレクタの変更

ガベージ・コレクタを変更する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「<ディレクトリ・サーバー・インスタンス>」、「**ガベージ・コレクション管理**」の順に展開し、構成するガベージ・コレクタを選択します。右側のペインに「ガベージ・コレクタ」ウィンドウが表示されます。
2. 「**ガベージ・コレクタ**」ウィンドウで、このガベージ・コレクタの値を入力します。フィールドについては、A-6 ページの表 A-9 を参照してください。
3. 「**適用**」を選択します。

コマンドライン・ツールを使用したガベージ・コレクタの変更

この項では、コマンドライン・ツールを使用してガベージ・コレクタを変更する方法の例を示します。変更できるガベージ・コレクション属性は、『Oracle Identity Management ユーザー・リファレンス』の「Oracle Internet Directory 構成のスキーマ要素」を参照してください。

例 1: ガベージ・コレクタの変更

削除済とマークされたエントリのガベージ・コレクタをすぐに実行するとします。LDIF ファイルは次のようになります。

```
dn: cn=tombstone purgeconfig, cn=purge config, cn=subconfigsubentry
changetype:modify
replace: orclpurgenow
orclpurgenow: 1
```

ldapmodify を使用して、このエントリをロードします。

```
ldapmodify -h hostname -p port# -D username -w passwd \
           -f file_name_of_defined_entry
```

例 2: ガベージ・コレクタの変更ログの使用禁止

変更ログのガベージ・コレクタを使用禁止にするとします。

```
dn: cn=changelog purgeconfig, cn=purgeconfig, cn=subconfigsubentry
changetype: modify
replace: orclpurgeenable
orclpurgeenable: 0
```

ldapmodify を使用して、このエントリをロードします。

```
ldapmodify -h hostname -p port# -D username -w passwd \
           -f file_name_of_defined_entry
```

Oracle Internet Directory 統計情報コレクタの変更

Oracle Internet Directory 統計情報コレクタは、ガベージ・コレクタと同じ方法で変更しますが、変更可能なフィールドは 3 つだけです。A-6 ページの「Oracle Directory Manager の Oracle Internet Directory 統計情報コレクタ管理フィールド」を参照してください。

Oracle Internet Directory ガベージ・コレクタのロギングの有効化、無効化および監視

この項の項目は次のとおりです。

- Oracle Internet Directory ガベージ・コレクタのロギングの有効化
- Oracle Internet Directory ガベージ・コレクタのロギングの無効化
- ガベージ・コレクションのロギングの監視

Oracle Internet Directory ガベージ・コレクタのロギングの有効化

ガベージ・コレクタのロギングを有効にすると、ディレクトリ・サーバーは、ファイル・システム内のファイルに、情報を書き込みます。これには次の情報が含まれます。

- ジョブ識別子
- ガベージ・コレクタのジョブ説明
- 削除されたエントリ数
- 操作のステータス
- タイムスタンプ
- 捕捉されたエラー

ガベージ・コレクション情報のロギングを有効にする手順は、次のとおりです。

1. `orclpurgedebug` 属性を必要に応じて 1 に設定します。orclpurgedebug を 1 に設定すると、さらに詳細なデバッグ情報が記録されます。こうしておくと、ガベージ・コレクションの問題のトラブルシューティングに役立ちます。
2. ログ・ファイルの有効なファイル名（`oidgc001.log` など）を、`orclpurgefilename` 属性に設定します。
3. ログ・ファイルのあるディレクトリのパス名（`/private/qzhou/oracle/ldap/log` など）を、`orclpurgefileloc` 属性に設定します。
4. 手順 3 で指定したディレクトリへの PL/SQL I/O アクセスを有効にします。これには、次の内容をデータベースに指定します。

   `UTL_FILE_DIR=`*`PATH_NAME`*

   `PATH_NAME` は、手順 3 で指定したパスです。

   > **関連資料：**『Oracle Database リファレンス』の UTL_FILE_DIR パラメータに関する項

5. レプリケーション・サーバーを停止し、次に Oracle Internet Directory サーバーを停止します。
6. データベースを再起動します。
7. Oracle Internet Directory サーバーを起動し、次にレプリケーション・サーバーを起動します。

Oracle Internet Directory ガベージ・コレクタのロギングの無効化

ガベージ・コレクション情報のロギングを無効にするには、orclpurgedebug 属性を 0 に設定します。

注意： orclpurgedebug がゼロに設定されている場合も、ガベージ・コレクタの処理を示すために、ガベージ・コレクタの操作に関する最小限の情報が記録されます。

ガベージ・コレクションのロギングの監視

ガベージ・コレクションのログの情報は、ガベージ・コレクションの監視とトラブルシューティングに役立ちます。このログの場所は、ロギングを有効にする際に属性を設定して指定します。たとえば、次のように構成したとします。

```
orclpurgefilename = oidgc001.log
orclpurgefileloc     = /private/qzhou/oracle/ldap/log
```

ロギングを有効にすると、/private/qzhou/oracle/ldap/log/oidgc001.log ファイルを読み取ることによって変更ログのガベージ・コレクションの処理を監視できます。

次に、管理者が変更ログのガベージ・コレクション構成エントリの orclpurgenow 属性を変更した場合に記録される情報の例を示します。

```
Running Garbage Collector: cn=changelog purgeconfig
Starting time: 2005/03/24 11:03:23
PurgeConfig object located, Eid= 936
purge_ODSChglog: Nothing to be purged(no_work_to_do)
purge_ODSChglog: 107 chglogs successfully purged
purge_ASRChglog: Nothing to be purged(no_work_to_do)
purge_ASRChglog: 0 chglogs successfully purged
purge_ASRChglog: 0 chglogs successfully purged

Modifying Garbage Collector for at "2005/03/24 11:03:23
Garbage Collector DN recognized, rdn=cn=changelog purgeconfig
orclPurgeNow successfully retrieved.
Garbage Collector job found: jobno=21
Garbage Collector has been run
Garbage collector is updated successfully!
```

orclpurgenow の変更により、変更ログのガベージ・コレクタがすぐに実行されます。最初のパラグラフで示されているように、ods_chg_log 表から 107 個の変更ログが削除され、asr_chg_log 表からは 0 個の変更ログが削除されています。また、2 番目のパラグラフの情報は、orclpurgenow 属性が正常に変更されたことを示しています。

27

他のデータ・リポジトリからのデータの移行

この章では、LDAP バージョン 3 準拠のディレクトリおよびアプリケーション固有のデータ・リポジトリから Oracle Internet Directory へのデータの移行方法を説明します。

この章の項目は次のとおりです。

Oracle Internet Directory のデフォルトのディレクトリ構造

Oracle Internet Directory のインストール時に、Oracle Universal Installer によって、デフォルトのスキーマとディレクトリ情報ツリー（DIT）が作成されます。デフォルトのディレクトリ情報ツリー・フレームワークの詳細は、第 3 章「ディレクトリの概念およびアーキテクチャ」および第 23 章「Oracle Identity Management レルムの配置」を参照してください。このフレームワークには柔軟性があるため、配置要件に応じて適切に変更できます。

Oracle Internet Directory 10*g*（10.1.4.0.1）では、次のディレクトリ要素がデフォルトで作成されます。

- ルート Oracle コンテキスト（`cn=OracleContext`）: 企業全体の構成データが Oracle 製品によって格納されるコンテナです。
- デフォルトの ID 管理レルム（`dc=`*`dns_domain_of_host`*`,dc=com`）: Oracle 製品による企業ユーザーおよびグループの検索対象となるコンテナです。企業の DIT 構造と似ています。たとえば、`my_computer.us.my_company.com` というホスト名のコンピュータに Oracle Internet Directory をインストールした場合、Oracle Internet Directory のインストール時に作成されるデフォルトの ID 管理レルムは、`dc=us,dc=my_company,dc=com` となります。Oracle 製品による検索対象となるのは、`cn=users,dc=us,dc=my_company,dc=com` の下のすべてのユーザーおよび `cn=groups,dc=us,dc=my_company,dc=com` の下のすべてのグループです。デフォルトの ID 管理レルム・エントリを作成すると、他の Oracle Internet Directory 対応コンポーネントが自動的にブートストラップされるように、Oracle Internet Directory コンフィギュレーション・アシスタントによってルート Oracle コンテキストにポインタが格納されます。

このデフォルトの ID 管理レルムは、配置要件に応じて変更してもかまいません。

LDAP 準拠のディレクトリからのデータの移行

この項では、LDAP 準拠のサード・パーティのディレクトリから Oracle Internet Directory にデータを移行する際に役立つ情報を提供します。すでに確立された構造を持つディレクトリが存在し、データをそのディレクトリからデフォルトのディレクトリ構造の環境に移行する場合は、この項の指示に従ってください。

この項の項目は次のとおりです。

- ツール
- 一般的な使用例
- 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

ツール

サード・パーティの LDAP データを Oracle Internet Directory に移行する際には、3 つのツールがよく使用されます。これには次のようなものがあります。

- bulkload
- dipassistant
- Oracle Directory Integration Platform Server

どのツールを使用するかは、インポートするデータのサイズやデータをマップする必要があるかどうかなど、いくつかの要因によって変わってきます。

bulkload

バルク・ロード・ツールの bulkload は、多数のエントリをディレクトリ・サーバーにロードするコマンドライン・ツールです。Oracle SQL*Loader を使用してディレクトリ・エントリをロードします。bulkload ツールは、入力ファイルが LDAP Data Interchange Format（LDIF）であることを想定しています。bulkload ツールでは、LDIF 入力の参照整合性を検証できますが、データにマッピングなどの変換を実行することはできません。

表 27-1「bulkload と dipassistant の機能」に、bulkload と dipassistant bootstrap との機能の比較を示します。bulkload の構文情報と例は、『Oracle Identity Management ユーザー・リファレンス』の、Oracle Internet Directory のデータ管理ツールに関する項を参照してください。

dipassistant

ディレクトリ統合アシスタントである dipassistant は、Oracle Directory Integration and Provisioning Server によってスケジュールされた同期プロファイルを管理するためのコマンドライン・ツールです。管理者は、Oracle Directory Integration and Provisioning Server で継続的に同期を実行するように構成する際に、dipassistant bootstrap 操作を使用して、接続ディレクトリと Oracle Internet Directory との間で初期のデータ移行を実行することができます。この操作は、継続した同期のない、1 回かぎりのデータの移行にも使用できます。

dipassistant bootstrap 操作では、データをサード・パーティの LDAP 準拠ディレクトリから直接受け取るか、LDIF ファイル、タグ付きファイルまたは CSV ファイルから受け取ることができます。同期プロファイルまたは構成ファイルのいずれかで、マッピング・ルールを指定する必要があります。

表 27-1「bulkload と dipassistant の機能」に、dipassistant bootstrap と bulkload との機能の比較を示します。dipassistant の構文情報、構成ファイルのプロパティ、入力ファイルのタイプ情報および例は、次を参照してください。

『Oracle Identity Management ユーザー・リファレンス』および『Oracle Identity Management 統合ガイド』のツールに関する項

表 27-1 bulkload と dipassistant の機能

機能	bulkload	dipassistant
速度	高速	低速
データ転送方式	SQL	LDAP
受け入れ可能な入力のタイプ	LDIF ファイルのみ	LDIF ファイル、LDAP ディレクトリ、タグ付きファイル、CSV ファイル
データの変換	×	○
LDIF 入力の検証	○	×

Oracle Directory Integration Platform Server

場合によっては、管理者は Oracle Directory Integration Server を構成するときに、dipassistant を使用しないことがあります。Oracle Directory Integration Server の構成後は、このサーバー自体で接続ディレクトリから Oracle Internet Directory にデータを移行することができます。また、Oracle Directory Integration Server を 1 回かぎりのデータの移行に使用することもできます。詳細は、『Oracle Identity Management 統合ガイド』を参照してください。

一般的な使用例

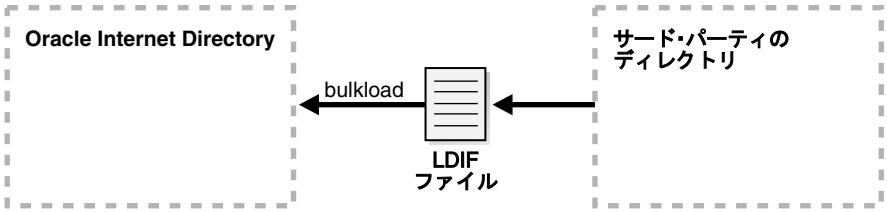
この項では、「ツール」の項で説明されているツールの各種の使用例を示します。次の使用例について説明します。

- 使用例 1: LDIF ファイルと bulkload の使用
- 使用例 2: dipassistant の直接の使用
- 使用例 3: LDIF ファイルと dipassistant の使用
- 使用例 4: dipassistant、bulkload および LDIF ファイルの使用
- 使用例 5: Oracle Directory Integration Platform Server の使用

使用例 1: LDIF ファイルと bulkload の使用

変換が不要でデータが非常に大きい（50 万件以上）場合、サード・パーティのディレクトリから Oracle Internet Directory にデータを移行するには `bulkload` が最も適しています。このツールは高速で、LDIF 入力の検証が可能です。この方法を使用する場合は、図 27-1「LDIF ファイルと bulkload の使用」に示すように、まずサード・パーティのディレクトリから LDIF ファイルにデータをエクスポートする必要があります。

図 27-1 LDIF ファイルと bulkload の使用



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には、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するツールがあります。

> **関連資料：** IETF の RFC 2849 は、`http://www.ietf.org` で入手可能です。

LDIF ファイルと bulkload を使用してデータを Oracle Internet Directory に移行するには、次のタスクを実行する必要があります。

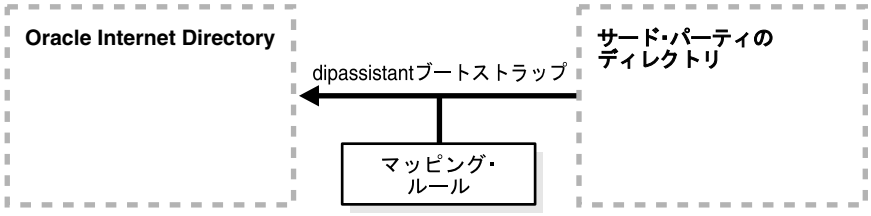
- タスク 1: 非 Oracle Internet Directory サーバーから LDIF ファイル形式へのデータのエクスポート
- タスク 2: LDIF データで参照される必須スキーマの追加のための LDIF ユーザー・データの分析
- タスク 3: Oracle Internet Directory 内のスキーマの拡張
- タスク 4: LDIF ファイルからの独自のディレクトリ・データの削除
- タスク 5: LDIF ファイルからの操作属性の削除
- タスク 6: LDIF ファイルからの非互換の userPassword 属性値の削除
- タスク 7: bulkload の check="TRUE" 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

これらのタスクの詳細は、27-7 ページの「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」を参照してください。

使用例 2: dipassistant の直接の使用

サード・パーティのディレクトリから Oracle Internet Directory にデータを移行するときにマッピングを実行する必要があり、データのサイズが小さい場合は、`dipassistant` を使用できます。図 27-2「dipassistant の直接の使用」に示すように、サード・パーティのディレクトリ自体を `dipassistant` への入力として使用することができます。

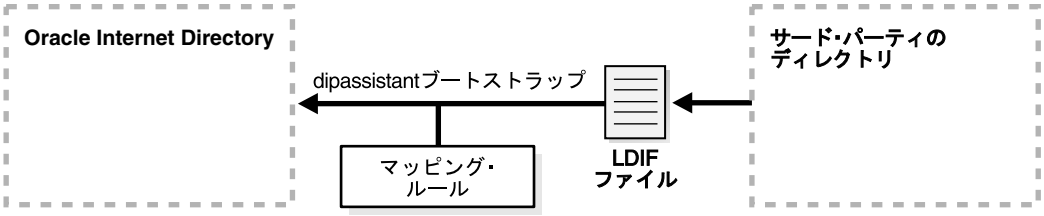
図 27-2 dipassistant の直接の使用



使用例 3: LDIF ファイルと dipassistant の使用

使用例 3 は、使用例 2 のバリエーションです。サード・パーティのディレクトリに直接アクセスできない場合は、管理者に依頼してデータを LDIF ファイルにエクスポートすることができます。図 27-3「LDIF ファイルと dipassistant の使用」に示すように、`dipassistant` は LDIF ファイルから入力を受け取ることができます。また、Oracle Directory Integration Server を使用してデータを移行することもできます。

図 27-3 LDIF ファイルと dipassistant の使用



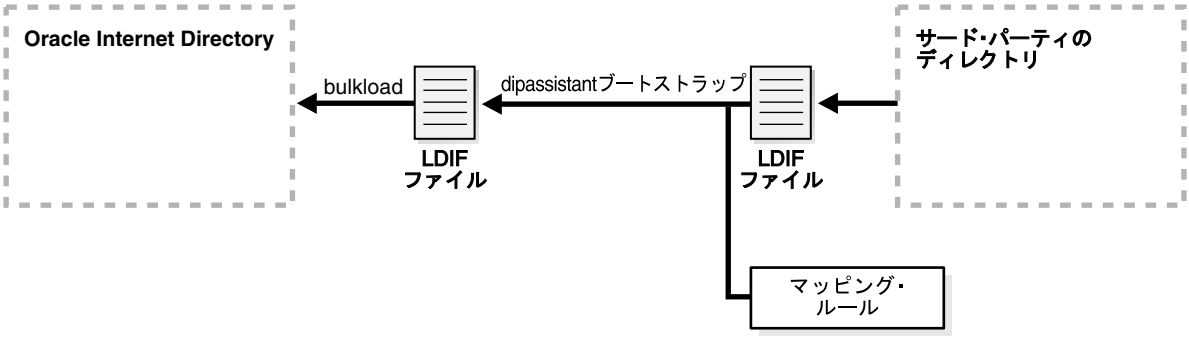
LDIF ファイルと bulkload を使用してデータを Oracle Internet Directory に移行する場合には、いくつかのタスクを実行する必要があります。この使用例では、`dipassistant` または Oracle Directory Integration Platform とともにマッピング・ファイルを使用するため、「使用例 1: LDIF ファイルと bulkload の使用」に示されているすべてのタスクを実行する必要はありません。実行する必要のあるタスクは、次のとおりです。

- 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
- 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
- タスク 3: Oracle Internet Directory 内のスキーマの拡張

使用例 4: dipassistant、bulkload および LDIF ファイルの使用

大量のデータがあり、データにマッピングを実行する必要がある場合は、ツールを組み合せて使用することができます。図 27-4「dipassistant、bulkload および LDIF ファイルの使用」に示すように、サード・パーティのディレクトリから LDIF ファイルにデータをエクスポートし、`dipassistant bootstrap` を使用して別の LDIF ファイルにデータをマッピングして、そのファイルを `bulkload` でロードすることができます。

図 27-4 dipassistant、bulkload および LDIF ファイルの使用



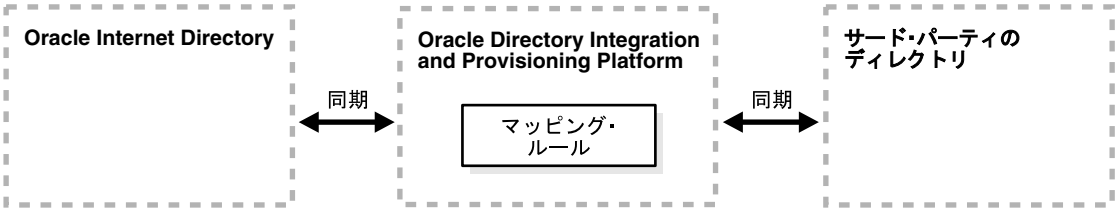
「使用例 3: LDIF ファイルと dipassistant の使用」に示すように、実行する必要のあるタスクは、次のとおりです。

- 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
- 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
- タスク 3: Oracle Internet Directory 内のスキーマの拡張

使用例 5: Oracle Directory Integration Platform Server の使用

Oracle Directory Integration Server を使用すると、図 27-5「Oracle Directory Integration Server の使用」に示すように、Oracle Internet Directory とサード・パーティのディレクトリの間に双方向で継続的な統合を構成できます。詳細は、『Oracle Identity Management 統合ガイド』を参照してください。

図 27-5 Oracle Directory Integration Server の使用



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 LDIF ファイルを使用してデータを移行するには、この項で説明するタスクを実行します。

27-4 ページの「一般的な使用例」で説明したように、`dipassistant` または Oracle Directory Integration Platform とともにマッピング・ファイルを使用する場合は、タスク 4 ～ 7 を実行する必要はありません。

- 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
- 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
- タスク 3: Oracle Internet Directory 内のスキーマの拡張
- 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
- タスク 5: LDIF ファイルからの操作属性の削除
- タスク 6: LDIF ファイルからの非互換の userPassword 属性値の削除
- タスク 7: bulkload の check="TRUE" 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
- `http://www.ietf.org` で入手可能な IETF RFC 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 11 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（『Oracle Identity Management ユーザー・リファレンス』を参照）を使用して実行できます。

他の Oracle 製品を使用するユーザーがいる場合は、オブジェクト・クラスが `orclUserV2` で必須属性を持ったユーザーを作成する必要があります。Active Directory との統合には、オブジェクト・クラスが `orclADUser` で必須属性を持ったユーザーを作成する必要があります。これらのオブジェクト・クラスとその属性の詳細は、『Oracle Identity Management ユーザー・リファレンス』を参照してください。

タスク 4: LDIF ファイルからの独自のディレクトリ・データの削除

ACI 属性など、LDAP バージョン 3 規格の一部の要素は、まだ正式に承認されていません。その結果、様々なディレクトリ・ベンダーがベンダー間で正常に変換できない方法で、ACI ポリシー・オブジェクトを実装しています。

クリーンアップされた LDIF ファイルから Oracle Internet Directory に基本エントリ・データをインポートした後、Oracle Internet Directory 環境でセキュリティ・ポリシーを明示的に再適用する必要があります。この作業は、Oracle Directory Manager またはコマンドライン・ツールと、必要な ACP 情報を含む LDIF ファイルを使用して実行できます。

この他にもアクセス制御に関連しない独自のメタデータが含まれている場合があります。これも同様に削除する必要があります。様々な IETF RFC を理解することで、どのディレクトリ・メタデータが特定のベンダー独自のものであり、どれが LDAP 規格に準拠していて LDIF ファイルによって移植できるかを判断できます。

タスク 5: LDIF ファイルからの操作属性の削除

エントリが作成またはインポートされるたびに、標準の LDAP バージョン 3 操作属性のうち、`creatorsName`、`createTimestamp`、`modifiersName` および `modifyTimestamp` の 4 つの属性が、Oracle Internet Directory によって自動的に生成されます。たとえば、LDIF ファイルのインポートを使用して、既存のディレクトリ・データからこれらの値をインスタンス化することはできません。したがって、インポートする前にこれらの属性をファイルから削除する必要があります。

タスク 6: LDIF ファイルからの非互換の userPassword 属性値の削除

Oracle Internet Directory 10*g*（10.1.4.0.1）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**
- SSHA
- **UNIX Crypt**

一部のベンダー製品で使用されている userPassword 属性のハッシュ値は、Oracle Internet Directory と互換性がありません。そのため、`userPassword` 属性と値に対応する行はすべて LDIF データ・ファイルから削除する必要があります。ただし、それらの行がプレーン・テキストで表されている場合、または値を含んでいない場合を除きます。LDIF データをインポートした後、手動で再入力するか、ハッシュされた userPassword 情報を別途ディレクトリにアップロードする必要があります。パスワードが Oracle Internet Directory パスワード・ポリシーに準拠し、クリア・テキストになっていることを確認します。

タスク 7: bulkload の check="TRUE" モードの実行とスキーマ違反または重複エラーが残っているかどうかの判断

LDIF ファイルを生成してロードする前には、必ず bulkload ユーティリティのチェック・モードを使用して LDIF ファイルのチェックを実行してください。bulkload の出力によって、データの非一貫性が報告されます。

> **関連資料：** bulkload のチェック・モードの使用方法は、『Oracle Identity Management ユーザー・リファレンス』の bulkload コマンドライン・ツールのリファレンスを参照してください。

ユーザー・データのアプリケーション固有リポジトリからの移行

ユーザー・データをアプリケーション固有のリポジトリから移行するには、次の処理が必要です。

- ユーザー・データをアプリケーション固有のリポジトリから収集し、ディレクトリが読み込める書式に設定します。
- ディレクトリ管理者がそのデータを使用できるようにします。ディレクトリ管理者は、次の作業を行う必要があります。
  - ディレクトリ内でデータを格納する場所を指定します。
  - データをディレクトリにインポートします。

中間テンプレート・ファイル

この移行を実行するには、Oracle Directory Provisioning Integration Service は、アプリケーション固有のリポジトリを使用して、そのデータを中間テンプレート・ファイルにエクスポートする必要があります。このテンプレート・ファイル内のレコードは、完全な LDIF にはなっていません。これらのレコードには、情報が最終的に格納されるディレクトリの場所などに関連する置換変数が入っています。これらの変数は未定義のまま残されるため、ディレクトリ管理者は後で定義できます。

ユーザー・データをこの中間テンプレート・ファイルから適切な LDIF に変換するには、OID 移行ツール（ldifmigrator）を使用します。LDIF に変換されたデータは、ディレクトリにロードできます。

要約すると、アプリケーション固有のリポジトリからデータを移行するには、通常、次の手順を実行します。

1. アプリケーション固有のデータを中間テンプレート・ファイルとしてエクスポートします。
2. ディレクトリ管理者は、OID 移行ツール（ldifmigrator）を使用して、不完全な LDIF エントリをテンプレート・ファイルからロードし、配置の選択に基づいて完全な LDIF エントリに変換します。
3. ディレクトリ管理者は、この完全な LDIF のデータを Oracle Internet Directory にロードします。
4. アプリケーションは、独自の仕様に従って移行処理を完了します。

アプリケーション・リポジトリ内のデータと Oracle Internet Directory の既存データとの調停

アプリケーション固有のリポジトリから移行しているデータが、Oracle Internet Directory にすでに存在している場合があります。この場合、OID 移行ツール（ldifmigrator）の調停機能を使用して、2 つのディレクトリ間の差分を調整できます。

> **関連資料：** OID 移行ツールの調停機能の詳細は、『Oracle Identity Management ユーザー・リファレンス』の ldifmigrator コマンドライン・ツールのリファレンスを参照してください。

アプリケーション固有のリポジトリからデータを移行するためのタスク

アプリケーション固有のリポジトリからデータを移行するには、中間テンプレート・ファイルを作成してから、OID 移行ツールを実行します。

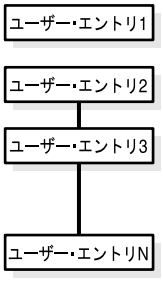
タスク 1: 中間テンプレート・ファイルの作成

各国語のデータを生成するアプリケーションでは、中間テンプレート・ファイルにデータを AL32UTF8 で格納する必要があります。詳細は、`http://www.ietf.org` で、IETF の RFC 2849「The LDAP Data Interchange Format（LDIF）- Technical Specification（LDAP Data Interchange Format（LDIF）- 技術仕様）」を参照してください。

中間テンプレート・ファイルの生成時に、移行を実行するアプリケーションでは、RFC 2849 で定義されているレコード・セパレータを使用して、すべてのユーザー・レコードを順にリストする必要があります。OID 移行ツール（ldifmigrator）は、デフォルトの ID 管理レルム（企業自体に対応しています）にすべてのユーザーを割り当てます。

図 27-6 に、ユーザー・エントリが格納される中間テンプレート・ファイルの全体構造を示します。

図 27-6 中間ユーザー・ファイルの構造



中間テンプレート・ファイルでは、次の形式を使用して、有効なユーザー・エントリが生成されます。**太字**の文字列は、すべてアプリケーション固有のリポジトリから提供されます。

```
dn: cn=UserID, %s_UserContainerDN%
sn: Last_Name
orclGlobalID: GUID_for_User
%s_UserNicknameAttribute%: UserID
objectClass: inetOrgPerson
objectClass: orclUserV2
```

このテンプレートの文字列 *%s_UserContainerDN%* と *%s_UserNicknameAttribute%* は置換変数で、OID 移行ツールによって値が提供されます。OID 移行ツールは、配置に固有な考慮事項に従ってこれらの値を判別します。引数は、アプリケーションが OID 移行ツールに渡すか、ツールがディレクトリから取得します。

例 : 中間テンプレート・ファイル内のユーザー・エントリ 次の中間テンプレート・ファイルには、アプリケーション固有の移行ロジックによって生成されたユーザー・エントリが格納されます。この例にある**太字**のデータは、すべてアプリケーション固有のユーザー・リポジトリから提供されます。

```
dn: cn=jdoe, %s_UserContainerDN%
sn: Doe
%s_UserNicknameAttribute%: jdoe
objectClass: inetOrgPerson
objectClass: orclUserV2
title: Member of Technical Staff
homePhone: 415-584-5670
homePostalAddress: 234 Lez Drive$ Redwood City$ CA$ 94402
```

```
dn: cn=jsmith, %s_UserContainerDN%
sn: Smith
%s_UserNicknameAttribute%: jsmith
objectClass: inetOrgPerson
objectClass: orclUserV2
title: Member of Technical Staff
homePhone: 650-584-5670
homePostalAddress: 232 Gonzalez Drive$ San Francisco$ CA$ 94404

dn: cn=lrider, %s_UserContainerDN%
sn: Rider
%s_UserNicknameAttribute%: lrider
objectClass: inetOrgPerson
objectClass: orclUserV2
title: Senior Member of Technical Staff
homePhone: 650-584-5670
```

中間ファイルの形式に変換されたすべてのユーザー・データは、さらに、OID 移行ツールによって、Oracle Internet Directory にロード可能な適切な LDIF ファイルに変換されます。

中間テンプレート・ファイルの例は、*$ORACLE_HOME*/ldap/schema/oid にあります。

ユーザー・エントリの属性 各ユーザー・エントリには、必須とオプションの属性があります。

表 27-2 に、ユーザー・エントリの必須属性を示します。

表 27-2 ユーザー・エントリの必須属性

属性	説明
dn	適切な置換変数を持つユーザー・エントリの識別名。エントリの相対識別名には、必ず cn 属性を含める必要があります。
sn	ユーザーの姓。
objectclass	エントリが最小限、属する必要があるオブジェクト・クラス。inetOrgPerson および orclUserV2 があります。

関連資料：

- inetOrgPerson オブジェクト・クラスの各属性については、http://www.ietf.org で、IETF の RFC 2798「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の属性の詳細は、『Oracle Identity Management ユーザー・リファレンス』の、Oracle Identity Management 用オブジェクト・クラスのリファレンスに関する項を参照してください。

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 に移行できます。データの移行後は、そのアプリケーションと Oracle Internet Directory を同期化することによって、アプリケーションに関連するあらゆるデータを更新できます。同期化には、Oracle Directory Synchronization Service を使用します。

関連資料： OID 移行ツールの使用手順の詳細は、『Oracle Identity Management ユーザー・リファレンス』の ldifmigrator コマンドライン・ツールのリファレンスを参照してください。

28

サーバー・チェーン

ディレクトリ・サーバー・チェーンは、10*g*（10.1.4.0.1）で導入された Oracle Internet Directory の新機能です。これは新しい Java プラグイン・フレームワークを使用して実装されました。

サーバー・チェーンを使用すると、サード・パーティの LDAP ディレクトリにあるエントリを、ディレクトリ・ツリーの一部にマップし、同期やデータの移行なしに、Oracle Internet Directory を介してアクセスできます。サーバー・チェーンにより、識別データが Oracle Internet Directory の外部にある場合も、Oracle Internet Directory の認可フレームワークを使用できます。

サーバー・チェーンは、Oracle Directory Integration Platform にかわるものではありません。むしろ、Oracle Directory Integration Platform に補完的機能を提供します。

サーバー・チェーンは、仮想ディレクトリとは異なります。Oracle Virtual Directory などの仮想ディレクトリは、複数の ID リポジトリとアプリケーションの間の柔軟な仮想化レイヤーです。仮想ディレクトリは、識別情報の同期化やディレクトリ・サーバーに補完的サービスを提供します。仮想ディレクトリを使用すると、組織は、複数のディレクトリやデータベースにまたがる可能性のあるデータの統合された、論理（仮想）ビューを作成できます。

サーバー・チェーンは、より簡単で柔軟性のあるソリューションであり、Oracle Internet Directory サーバーに埋め込まれていて、OracleAS Single Sign-On とエンタープライズ・ユーザー・セキュリティの顧客には特に適しています。管理や更新が簡単になります。特別な構成の手順を実行せずに、Oracle Internet Directory の認可フレームワークも提供します。

この章の項目は次のとおりです。

外部サーバーのサポート

Oracle Internet Directory サーバー・チェーンは、次の外部サーバーをサポートします。

- Microsoft Active Directory
- Sun Java System Directory Server（以前の SunONE iPlanet）

Oracle Internet Directory の実装で、1 つの Active Directory サーバー、1 つの Sun Java System Directory Server、またはその両方と接続できます。

統合された Oracle 製品

次の製品が、Oracle Internet Directory サーバー・チェーンに統合されました。

- Oracle Application Server Single Sign-On
- エンタープライズ・ユーザー・セキュリティ

サーバー・チェーンが使用可能な場合、外部ディレクトリからのユーザーは、次のことができます。

- OracleAS Single Sign-On を介したログイン

Oracle Internet Directory サーバー・チェーンにより、識別データを Oracle Internet Directory と同期させることなく、エンタプライズ・ユーザー・セキュリティを実装できます。識別データは外部リポジトリに置かれたままで、Oracle Internet Directory のデータ・ストアにはサーバー・チェーンのメタデータのみが格納されます。

Sun Java System Directory Server が外部ディレクトリの場合、サーバー・チェーンは、エンタープライズ・ユーザー・セキュリティとのパスワードベースの認証をサポートします。Active Directory が外部ディレクトリの場合、サーバー・チェーンは、エンタープライズ・ユーザー・セキュリティとの Kerberos ベースの認証をサポートします。外部ユーザーは、エンタープライズ・ユーザー・セキュリティの認証設定が完了すると、Oracle Database にログインできます。

> **関連資料：** エンタープライズ・ユーザー・セキュリティのパスワード認証および Kerberos 認証用の構成の詳細は、『Oracle Database エンタープライズ・ユーザー管理者ガイド』を参照してください。

サポートされる操作

サーバー・チェーンでは、次の操作をサポートします。

- バインド
- 比較
- 変更
- 検索

比較、変更および検索操作は、構成パラメータの設定により有効または無効にできます。

Oracle Internet Directory クライアント・アプリケーションから LDAP 検索リクエストが発行されると、Oracle Internet Directory は自身のデータと外部ディレクトリからの検索結果を統合します。

Oracle Internet Directory クライアント・アプリケーションから LDAP バインド、比較または変更リクエストが発行されると、Oracle Internet Directory はリクエストを外部ディレクトリにリダイレクトします。

10*g*（10.1.4.0.1）では、比較操作は `userpassword` 属性に対してのみサポートされています。

10*g*（10.1.4.0.1）では、次の 2 つの場合に、属性変更がサポートされます。

- 外部属性は、Oracle Internet Directory 属性と同じ名前を持っています。これは大部分の LDAP 属性についても当てはまります。
- 外部属性は Oracle Internet Directory 属性にマップされ、外部属性と Oracle Internet Directory 属性のどちらも操作属性ではありません。

注意： Active Directory ユーザー・パスワードは、Oracle Internet Directory からサーバー・チェーンを介して変更できません。

サーバー・チェーンとレプリケーション

サーバー・チェーンをレプリケーション環境で使用する場合は、すべてのノード上でサーバー・チェーンを設定し、エントリがノード全体で一貫性を保てるようにします。サーバー・チェーンを構成して、マップされた外部ディレクトリがレプリケートされたすべてのノードにとって同じになるようにします。

サーバー・チェーンの構成

Oracle Internet Directory には、サーバー・チェーンの無効のサンプル・エントリが付属しています。

Active Directory の場合、サーバー・チェーン・エントリの識別名は次のようになります。

```
cn=oidscad,cn=OID Server Chaining,cn=subconfigsubentry
```

Sun Java System Directory Server の場合、エントリ識別名は次のようになります。

```
cn=oidsciplanet,cn=OID Server Chaining,cn=subconfigsubentry
```

これらのエントリを自分の環境に合うようにカスタマイズし、それらを有効にすることで、サーバー・チェーンを構成します。これは、コマンドラインから、または Oracle Directory Manager を使用して実行できます。

この項の項目は次のとおりです。

コマンドラインからのサーバー・チェーンの構成

コマンドラインからサーバー・チェーンを構成するには、次の手順を実行します。

1. LDIF ファイルを作成して、手動でユーザーおよびグループのコンテナを追加します。これらのコンテナの識別名を決定するには、28-5 ページの「ユーザー・コンテナとグループ・コンテナの要件」を参照してください。たとえば、ユーザー検索ベースが `cn=users,dc=us,dc=oracle,dc=com`、グループ検索ベースが `cn=groups,dc=us,dc=oracle,dc=com` の場合、LDIF ファイルで次のエントリを使用します。

```
dn: cn=AD,cn=users,dc=us,dc=oracle,dc=com
cn: AD
objectclass: orclcontainer
objectclass: top

dn: cn=iPlanet,cn=users,dc=us,dc=oracle,dc=com
cn: iPlanet
objectclass: orclcontainer
objectclass: top

dn: cn=AD,cn=groups,dc=us,dc=oracle,dc=com
cn: AD
objectclass: orclcontainer
objectclass: top

dn: cn=iPlanet,cn=groups,dc=us,dc=oracle,dc=com
cn: iPlanet
objectclass: orclcontainer
objectclass: top
```

2. `ldapadd` と、エントリを追加するために作成した LDIF ファイルを使用します。

```
ldapadd -p port -h  host -D "binddn" -w password -v -f container_ldif_file_name
```

3. もう 1 つの LDIF ファイルを作成し、サーバー・チェーン構成エントリを変更し、有効にします。LDIF ファイルの例は、28-8 ページの「Active Directory の例」と 28-9 ページの「Sun Java System Directory Server（iPlanet）の例」を参照してください。属性の表は、28-6 ページの「サーバー・チェーン構成エントリ」にあります。属性のマッピングについては、28-6 ページの「属性マッピング」で説明しています。

4. `ldapmodify` コマンドと作成した LDIF ファイルを使用してサーバー・チェーン構成エントリを変更します。次の形式のコマンドラインを使用します。

```
ldapmodify -p port -h host -D "binddn" -w password -v -f entry_ldif_file_name
```

Oracle Directory Manager を使用したサーバー・チェーンの構成

Oracle Directory Manager には、Oracle Internet Directory サーバー・チェーン構成エントリの変更に便利なインタフェースが備わっています。Oracle Directory Manager を使用してサーバー・チェーンを構成するには、次の手順を実行します。

1. ナビゲータ・ペインで、「Oracle Internet Directory サーバー」、ディレクトリ・サーバー・インスタンスの順に展開します。
2. 「サーバー・チェーン」を選択します。右側のペインに「サーバー・チェーン管理」ウィンドウが表示されます。
3. サーバー・チェーン構成エントリを変更するには、エントリを選択し、「**編集**」を選択します。iPlanet（Sun Java System Directory Server）または Active Directory 用の「サーバー・チェーン管理」ウィンドウが表示されます。
4. 「**適用**」をクリックして、構成の変更を有効にします。

「サーバー・チェーン管理」ウィンドウのフィールドの説明は、A-37 ページの表 A-52 またはオンライン・ヘルプを参照してください。フィールドの大部分は、28-7 ページの「構成エントリ属性」で説明されている属性に対応します。

次の「ユーザー・コンテナとグループ・コンテナの要件」の項では、「外部ユーザー・コンテナ」と「外部グループ・コンテナ」のフィールドについて詳細を示しています。属性のマッピングについては、28-6 ページの「属性マッピング」で説明しています。

ユーザー・コンテナとグループ・コンテナの要件

ターゲットのユーザー・コンテナおよびグループ・コンテナは、OracleAS Single Sign-On と使用するために、Oracle Internet Directory 検索ベースの下に置く必要があります。Active Directory には `cn=AD`、Sun Java System Directory Server（iPlanet）には `cn=iPlanet` というコンテナ名を使用します。たとえば、ユーザー検索ベースが次の場合について考えます。

```
cn=users,dc=us,dc=oracle,dc=com
```

この場合、Active Directory ユーザー用のターゲット・ユーザー・コンテナとして、

```
cn=AD,cn=users,dc=us,dc=oracle,dc=com
```

を使用し、Sun Java System Directory Server ユーザー用のターゲット・ユーザー・コンテナとして、

```
cn=iPlanet,cn=users,dc=us,dc=oracle,dc=com
```

を使用します。同様に、グループ検索ベースの場合について考えます。

```
cn=groups,dc=us,dc=oracle,dc=com
```

この場合、Active Directory グループのターゲット・コンテナとして、

```
cn=AD,cn=groups,dc=us,dc=oracle,dc=com
```

を使用し、Sun Java System Directory Server グループ用のターゲット・コンテナとして、

```
cn=iPlanet,cn=groups,dc=us,dc=oracle,dc=com
```

を使用します。

ターゲットのユーザー・コンテナおよびグループ・コンテナは、外部ディレクトリ専用のものです。これらのノードの下に表示されるユーザーおよびグループはすべて、外部ディレクトリによりデータが移入されます。これらのコンテナの下に、Oracle Internet Directory から直接エントリを追加しないでください。

属性マッピング

外部ディレクトリの属性と Oracle Internet Directory 属性が同じ場合、マッピングは不要です。サーバー・チェーンは、デフォルトでいくつかの属性マッピングを実行します。デフォルト・マッピングのリストは次のとおりです。

表 28-1 Active Directory に対するデフォルトの属性マッピング

Oracle Internet Directory 属性	Active Directory 属性
orclguid	objectGUID
uid	name
orclsamaccountname	samaccountname
krbprincipalname	userprincipalname

表 28-2 Sun Java System Directory Server に対するデフォルトの属性マッピング

Oracle Internet Directory 属性	Sun Java System Directory Server 属性
orclguid	nsuniqueid
authpassword	userpassword
krbprincipalname	mail

次のオブジェクトはマップできません。

- 操作属性。
- オブジェクト・クラス。
- Oracle Internet Directory 固有の属性。これらの属性には通常、`orcl` で始まる名前が付いています。

サーバー・チェーン構成エントリ

この項の項目は次のとおりです。

構成エントリ属性

表 28-3 は、サーバー・チェーンの構成エントリ属性を示しています。

表 28-3 サーバー・チェーンの構成エントリ属性

属性	必須	説明
orclOIDSCExtHost	○	外部ディレクトリ・ホストのホスト名。これは単一値属性です。
orclOIDSCExtPort	○	外部ディレクトリ・ホストのポート番号。これは単一値属性です。デフォルト値は 389 です。
orclOIDSCExtDN	○	外部ディレクトリの識別名。サーバー・チェーンは、検索および変更操作を実行するために、この識別情報を使用して、外部ディレクトリに対してバインドされます。この識別情報には、操作を実行するために十分な権限が必要です。これは単一値属性です。
orclOIDSCExtPassword	○	外部ディレクトリの識別名のパスワード。これは単一値属性です。ユーザーがこの属性をクリアテキストで取得できないようにするため、必ずプライバシ・モードを有効にします。16-3 ページの「受信した機密の属性のプライバシ」を参照してください。
orclOIDSCExtUserContainer	○	ユーザー検索操作を実行する外部ディレクトリ内のユーザー・コンテナ。これは単一値属性です。
orclOIDSCExtGroupContainer	×	グループ検索操作を実行する外部ディレクトリ内のグループ・コンテナ。これは単一値属性です。 外部ユーザー・コンテナと外部グループ・コンテナが同じ場合、この属性はオプションです。この場合、グループ検索操作は、外部ユーザー・コンテナで実行されます。
orclOIDSCTargetUserContainer	○	外部ユーザー・コンテナが存在する Oracle Internet Directory 内のユーザー・コンテナ。詳細は、28-5 ページの「ユーザー・コンテナとグループ・コンテナの要件」を参照してください。
orclOIDSCTargetGroupContainer	○	外部グループーが存在する Oracle Internet Directory 内のグループ・コンテナ。詳細は、28-5 ページの「ユーザー・コンテナとグループ・コンテナの要件」を参照してください。
orclOIDSCAttrMapping	×	外部ディレクトリと Oracle Internet Directory 間の各属性マッピングを指定します。たとえば、eMail 属性を Active Directory から Oracle Internet Directory の mail 属性にマップするには、この属性を次のように設定します。 orclOIDSCAttrMapping;mail:eMail 詳細は、28-6 ページの「属性マッピング」を参照してください。
orclOIDSCExtSearchEnabled	○	外部検索機能。0 = 無効（デフォルト）、1 = 有効。これは単一値属性です。
orclOIDSCExtModifyEnabled	○	外部変更機能。0 = 無効（デフォルト）、1 = 有効。これは単一値属性です。
orclOIDSCExtAuthEnabled	○	外部認証機能。0 = 無効（デフォルト）、1 = 有効。これは単一値属性です。

Active Directory の例

次の例は、Active Directory サーバー dlin-pc9.us.oracle.com、ポート 389 を、外部ディレクトリ・ストアとして使用するために構成されたサーバー・チェーンを示しています。属性はすべて、28-7 ページの表 28-3 で説明しています。

```
cn=oidscad,cn=OID Server Chaining,cn= subconfigsubentry
orclOIDSCExtHost: dlin-pc9.us.oracle.com
orclOIDSCExtPort: 389
orclOIDSCExtDN: cn=administrator,cn=users,dc=oidvd,dc=com
orclOIDSCExtPassword: *******
orclOIDSCExtUserContainer: cn=users,dc=oidvd,dc=com
orclOIDSCTargetUserContainer: cn=AD,cn=users,dc=us,dc=oracle,dc=com
orclOIDSCTargetGroupContainer: cn=AD,cn=groups,dc=us,dc=oracle,dc=com
orclOIDSCExtSearchEnabled: 1
orclOIDSCExtModifyEnabled: 1
orclOIDSCExtAuthEnabled: 1
orclOIDSCAttrMapping;description: title
```

次の例は、構成エントリを変更するために使用される LDIF ファイルです。

```
dn: cn=oidscad,cn=oid server chaining,cn=subconfigsubentry
changetype: modify
replace: orcloidscextdn
orcloidscextdn: administrator@dlin.net
-
replace: orcloidscextpassword
orcloidscextpassword: welcome1
-
replace: orcloidscexthost
orcloidscexthost: dlin-pc9.us.oracle.com
-
replace: orcloidscextport
orcloidscextport: 389
-
replace: orcloidsctargetusercontainer
orcloidsctargetusercontainer: cn=ad,cn=users,dc=us,dc=oracle,dc=com
-
replace: orcloidsctargetgroupcontainer
orcloidsctargetgroupcontainer: cn=ad,cn=groups,dc=us,dc=oracle,dc=com
-
replace: orcloidscextusercontainer
orcloidscextusercontainer: cn=users,dc=dlin,dc=net
-
replace: orcloidscextgroupcontainer
orcloidscextgroupcontainer: cn=users,dc=dlin,dc=net
-
replace: orcloidscextsearchenabled
orcloidscextsearchenabled: 1
-
replace: orcloidscextmodifyenabled
orcloidscextmodifyenabled: 1
-
replace: orcloidscextauthenabled
orcloidscextauthenabled: 1
```

Sun Java System Directory Server（iPlanet）の例

次の例は、Sun Java System Directory Server dlin-pc10.us.oracle.com、ポート 10389 を、外部ディレクトリ・ストアとして使用するために構成されたサーバー・チェーンを示しています。属性はすべて、28-7 ページの表 28-3 で説明しています。

```
cn=oidsciplanet,cn=OID Server Chaining,cn=subconfigsubentry
orclOIDSCExtHost: dlin-pc10.us.oracle.com
orclOIDSCExtPort: 10389
orclOIDSCExtDN: cn=directory manager
orclOIDSCExtPassword: ********
orclOIDSCExtUserContainer: ou=people,dc=acme,dc=com
orclOIDSCExtGroupContainer: ou=groups,dc=acme,dc=com
orclOIDSCTargetUserContainer: cn=iPlanet,cn=users,dc=us,dc=oracle,dc=com
orclOIDSCTargetGroupContainer: cn=iPlanet,cn=groups,dc=us,dc=oracle,dc=com
orclOIDSCExtSearchEnabled: 1
orclOIDSCExtModifyEnabled: 1
orclOIDSCExtAuthEnabled: 1
```

次の例は、構成エントリを変更するために使用される LDIF ファイルです。

```
dn: cn=oidsciplanet,cn=oid server chaining,cn=subconfigsubentry
changetype: modify
replace: orcloidscextdn
orcloidscextdn: cn=directory manager
-
replace: orcloidscextpassword
orcloidscextpassword: welcome1
-
replace: orcloidscexthost
orcloidscexthost: dlin-pc10.us.oracle.com
-
replace: orcloidscextport
orcloidscextport: 10389
-
replace: orcloidsctargetusercontainer
orcloidsctargetusercontainer: cn=iplanet,cn=users,dc=us,dc=oracle,dc=com
-
replace: orcloidsctargetgroupcontainer
orcloidsctargetgroupcontainer: cn=iplanet,cn=groups,dc=us,dc=oracle,dc=com
-
replace: orcloidscextusercontainer
orcloidscextusercontainer: ou=people,dc=us,dc=oracle,dc=com
-
replace: orcloidscextgroupcontainer
orcloidscextgroupcontainer: ou=groups,dc=us,dc=oracle,dc=com
-
replace: orcloidscextsearchenabled
orcloidscextsearchenabled: 1
-
replace: orcloidscextmodifyenabled
orcloidscextmodifyenabled: 1
-
replace: orcloidscextauthenabled
orcloidscextauthenabled: 1
```

サーバー・チェーンのデバッグ

サーバー・チェーンのデバッグを行うには、次の手順を実行します。

1. Oracle Internet Directory サーバーのデバッグ・ロギング・レベルを、14-6 ページの「デバッグ・ロギング・レベルの設定」で説明されているように設定します。ロギング・レベル値 402653184 を使用します。この値は、Java プラグイン・フレームワーク関連の全メッセージのロギングを可能にします。

2. Oracle Internet Directory サーバー・チェーンのデバッグ設定を変更します。`cn=oidscad,cn=oid server chaining,cn=subconfigsubentry` と `cn=oidsciplanet,cn=oid server chaining, cn=subconfigsubentry` の両方について、`orcloidscDebugEnabled` 属性を 1 に設定します。

   たとえば、`cn=oidscad,cn=oid server chaining,cn=subconfigsubentry` で `orcloidscDebugEnabled` を 1 に設定するには、次のように入力します。

   ```
   $ORACLE_HOME/bin/ldapmodify -h host -p port -D cn=orcladmin -w orcladminpwd <<EOF
   dn: cn=oidscad,cn=oid server chaining,cn=subconfigsubentry
   changetype: modify
   replace: orcloidscDebugEnabled
   orcloidscDebugEnabled: 1
   EOF
   ```

   関連資料：『Oracle Identity Management アプリケーション開発者ガイド』の Java Plug-in のデバッグおよびロギングに関する項

第 V 部

ディレクトリ・レプリケーション

第Ⅴ部では、レプリケーションおよび高可用性の詳細とその計画および管理方法について説明します。第Ⅴ部は次の各章で構成されています。

29

Oracle Internet Directory レプリケーションの概要

この章では、Oracle Internet Directory レプリケーションの概要を説明します。レプリケーションは、複数のディレクトリ・サーバーに同じネーミング・コンテキストをコピーし、管理するプロセスです。レプリケーションは、問合せを処理するサーバーを増やし、データをクライアントに近づけることで、パフォーマンスを改善できます。シングル・ポイント障害に関連したリスクを排除することにより、信頼性を高めます。

この章の項目は次のとおりです。

レプリケーションの概念

この項では、レプリケーションの基本的な概念を簡単に紹介します。その後の各項では、これらの概念を詳細に説明します。

この項の項目は次のとおりです。

- レプリケートされるコンテンツ : 完全または部分
- 方向 : 一方向または双方向
- 転送メカニズム : アドバンスト・レプリケーションまたは LDAP
- ディレクトリ・レプリケーション・グループ（DRG）のタイプ

レプリケートされるコンテンツ : 完全または部分

レプリケーションの設定時には、ディレクトリ情報ツリー（DIT）を 1 つのノードから別のノードにどの程度レプリケートするかを決定する必要があります。選択肢は次の 2 つです。

表 29-1 完全または部分レプリケーション

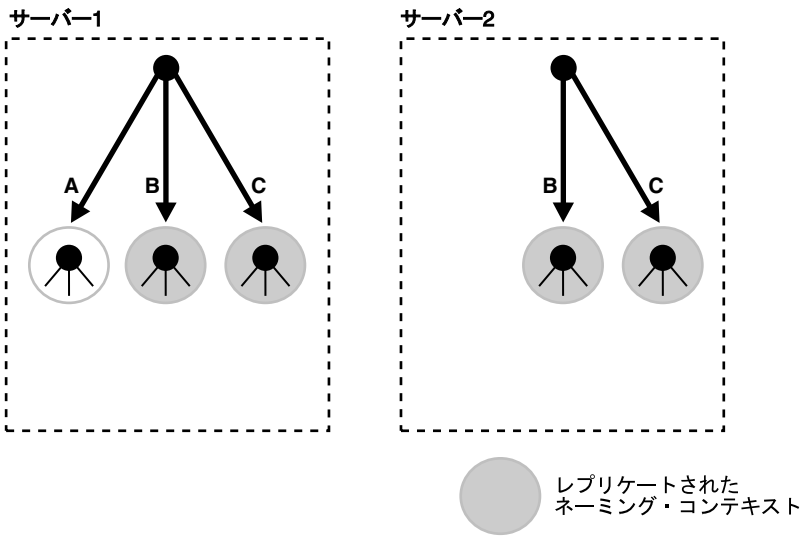
レプリケートするコンテンツ	説明
完全	DIT 全体を別のノードに伝播します。
部分	DIT 全体ではなく、1 つ以上のサブツリーを別のノードに伝播します。

完全レプリケーションでは、DIT 全体を別のノードに伝播します。このタイプのレプリケーションでは、ディレクトリ全体の高可用性が保証されます。このレプリケーションを使用して、ディレクトリ全体の操作を様々なノードに分散することもできます。完全レプリケーションは、Oracle Database アドバンスト・レプリケーションまたは LDAP のどちらかに基づきます。

部分レプリケーションでは、DIT 全体ではなく、1 つ以上のサブツリーを別のノードに伝播できます。この方法でディレクトリを分散することによって、サーバー間の作業負荷を均衡化し、フォルト・トレランスおよびフェイルオーバー機能を備え、可用性に優れた分散ディレクトリを構築することができます。部分レプリケーションは、レプリケーション環境管理ツールを使用して構成できます。部分レプリケーションは、ほとんどの場合 LDAP ベースです。

図 29-1 に、部分レプリケーションの例を示します。

図 29-1 部分レプリケーションの例



方向 : 一方向または双方向

レプリケーションの方向は、ノード間で設定したレプリケーション承諾のプロパティです。方向は次のいずれかです。

表 29-2 レプケーションの方向

方向	説明
一方向	一方のノードがサプライヤとして、もう一方がコンシューマとして構成されます。コンシューマは読取り専用です。
双方向	どちらのノードも、サプライヤとコンシューマの両方の役割を果します。読取りと書込みの両方が可能、つまり更新可能です。
peer-to-peer	レプリケーション・グループ内のすべてのノードが、他のノードすべてに対してサプライヤでありコンシューマでもあります。

読取り専用や読取り / 書込みという用語は、レプリケーションの方向を説明するために使用されることがあります。一方向レプリケーション承諾では、コンシューマ・ノードは読取り専用と言われます。つまり、他のノードに対する変更をそのノードに書き込むことで伝播できません。双方向レプリケーション承諾では、両方のノードが読取り / 書込み兼用と考えられます。読取り / 書込みは、更新可能とも呼ばれます。

転送メカニズム : アドバンスト・レプリケーションまたは LDAP

Oracle Internet Directory では、1 つのノードから別のノードへのデータのレプリケーションに使用できる 2 つのプロトコルをサポートしています。プロトコルは次のとおりです。

表 29-3 転送プロトコル

転送メカニズム	説明
Oracle Database アドバンスト・レプリケーション	Oracle Database のレプリケーション機能を使用します。アドバンスト・レプリケーションとも呼ばれます。
LDAP	業界標準の Lightweight Directory Access Protocol バージョン 3 を使用します。

アドバンスト・レプリケーションは、通常 peer-to-peer です。LDAP レプリケーションは、一方向または双方向のいずれかに構成できます。

ディレクトリ・レプリケーション・グループ（DRG）のタイプ

指定したネーミング・コンテキストのレプリケーションの対象となるディレクトリ・サーバーは、ディレクトリ・レプリケーション・グループ（DRG）を形成します。DRG を構成するディレクトリ・サーバー間の関係は、各ノード上でレプリケーション承諾と呼ばれる特別なディレクトリ・エントリによって表されます。レプリケーション承諾は、一方向または双方向のいずれかです。

サーバー内に格納されているネーミング・コンテキストの各コピーは、レプリカと呼ばれます。他のサーバーに更新情報を送信するサーバーをサプライヤといい、その更新情報を受け取るサーバーをコンシューマといいます。サーバーは、サプライヤとコンシューマのどちらにもなることができます。

ディレクトリ・レプリケーション・グループは、表 29-4 で説明するように、単一マスター、マルチマスターまたはファンアウトになります。

表 29-4 ディレクトリ・レプリケーション・グループのタイプ

グループ	説明
単一マスター	1 つ以上のコンシューマに変更をレプリケートするサプライヤが 1 つのみ存在します。クライアントは、マスター・ノードのみ更新できます。また、任意のコンシューマのデータの読取りのみ可能です。このタイプのグループは通常 LDAP を使用します。1 つのグループ内で 1 ノードを除くすべてのノードを読取り専用モードに切り替えることで、アドバンスト・レプリケーションを単一マスターとして構成することもできます。
マルチマスター	同等のものとして機能する複数のサイトが、レプリケートされたデータのグループを管理できるようにします。マルチマスター・レプリケーション環境では、各ノードはサプライヤとコンシューマ・ノードのどちらにもなります。10*g*（10.1.4.0.1）では、マルチマスター・レプリケーションに、転送メカニズムとしてアドバンスト・レプリケーションが必要です。完全な DIT が各ノードにレプリケートされます。レプリケーションは常に peer-to-peer です。
ファンアウト	point-to-point レプリケーション・グループとも呼ばれ、コンシューマに直接レプリケートするサプライヤを持っています。そのコンシューマは、1 つ以上の別のコンシューマにレプリケートできます。ファンアウトは、転送メカニズムとして LDAP を使用します。レプリケーションには、完全レプリケーションと部分レプリケーションがあります。レプリケーションは、一方向または双方向のいずれかです。

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

ディレクトリ・レプリケーション・グループ

この項の項目は次のとおりです。

ディレクトリ・レプリケーション・グループでのノード間のデータ転送

ディレクトリ・レプリケーション・グループの場合、データを転送するプロトコルは、Oracle Database アドバンスト・レプリケーションまたは LDAP のいずれかに基づきます。表 29-5 に、各タイプによるレプリケーションの様々な機能の処理方法、および詳細情報の参照先を示します。

表 29-5 ディレクトリ・レプリケーション・グループでのノード間のデータ転送のタイプ

機能	LDAP ベースのレプリケーション	アドバンスト・レプリケーション
変更の伝播	サプライヤからコンシューマへの変更の伝播は、LDAP を介して行われます。	サプライヤからコンシューマへの変更の伝播は、アドバンスト・レプリケーションを介して行われます。
レプリケートされるコンテンツ	完全レプリカ。 部分レプリカ。	完全レプリカ（通常）。
レプケーションの方向	一方向。 双方向。	peer-to-peer。
配置構成	単一マスター・レプリケーション。 ファンアウト・レプリケーション。	マルチマスター・レプリケーション。 単一マスター・レプリケーション（マルチマスター構成内の 1 つを除く他のすべてのマスターを読取り専用モードに切り替えた場合）。

単一マスター・レプリケーション・グループ

単一マスター・レプリケーション・グループには、1 つ以上のコンシューマに変更を提供するサプライヤのレプリカが 1 つのみ存在します。すべてのレプリケーション承諾は、サプライヤからコンシューマへの一方向です。クライアントは、マスター・レプリカのみ更新できます。また、任意のコンシューマのデータの読取りのみ可能です。

図 29-2「単一マスター・レプリケーションの例」に、単一マスター・レプリケーション環境を示します。

図 29-2 単一マスター・レプリケーションの例

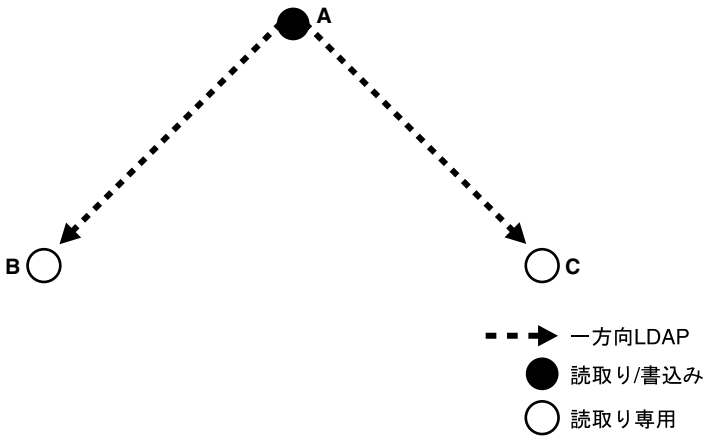


図 29-2 にある 3 つの円は、Oracle Internet Directory のノードを表しています。ノード A はサプライヤであり、コンシューマ・ノード B および C をレプリケートします。ノード A は読取り / 書込み可能、ノード B と C は読取り専用です。データ転送プロトコルは LDAP です。

マルチマスター・レプリケーション・グループ

マルチマスター・レプリケーション・グループは、peer-to-peer レプリケーション・グループとも呼ばれ、同等に機能する複数のノードが、レプリケートされたデータのグループを管理します。マルチマスター・レプリケーション・グループでは、各ディレクトリ・サーバーは、変更のサプライヤであると同時にコンシューマであり、各ノードでディレクトリ全体がレプリケートされます。

図 29-3 の例に、マルチマスター・レプリケーション・グループ内で相互に更新する 3 つのノード（A、B、C）を示します。ノード間のレプリケーションは双方向です。

図 29-3 マルチマスター・レプリケーションの例

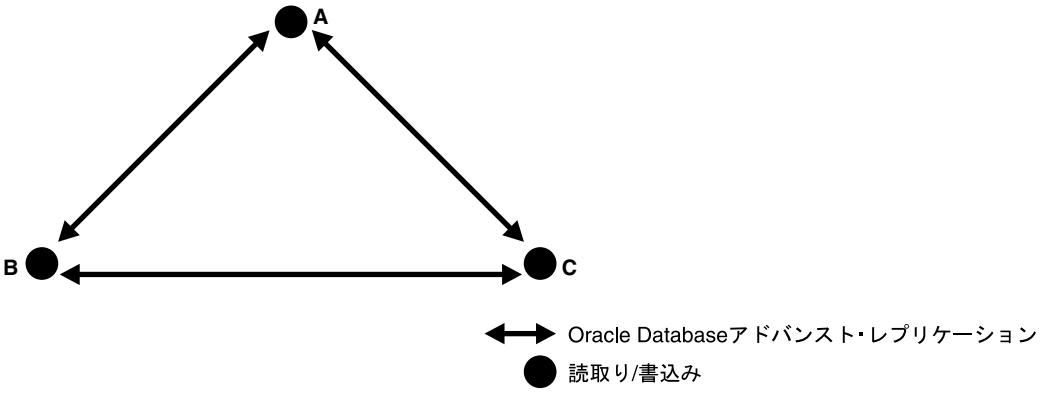


図 29-3 では、すべてのレプリケーションが双方向で、データ転送プロトコルはアドバンスト・レプリケーションに基づきます。

注意： Oracle Application Server Single Sign-On でサポートされているレプリケーション方式はマルチマスター・レプリケーションのみです。詳細は、『Oracle Application Server Single Sign-On 管理者ガイド』の高可用性に関する章でレプリケーションのための Oracle Application Server Single Sign-On の構成に関する項を参照してください。

関連項目： マルチマスター・レプリケーションの詳細は、29-21 ページの「Oracle Database アドバンスト・レプリケーション」を参照してください。

ファンアウト・レプリケーション・グループ

ファンアウト・レプリケーション・グループは、point-to-point レプリケーション・グループとも呼ばれ、コンシューマに直接レプリケートするサプライヤを持っています。そのコンシューマは、1 つ以上の別のコンシューマに同一データを提供できます。レプリケーションには、完全レプリケーションと部分レプリケーションがあり、一方向または双方向のいずれかです。

図 29-4 に、ファンアウト・レプリケーション環境を示します。

図 29-4 ファンアウト・レプリケーションの例

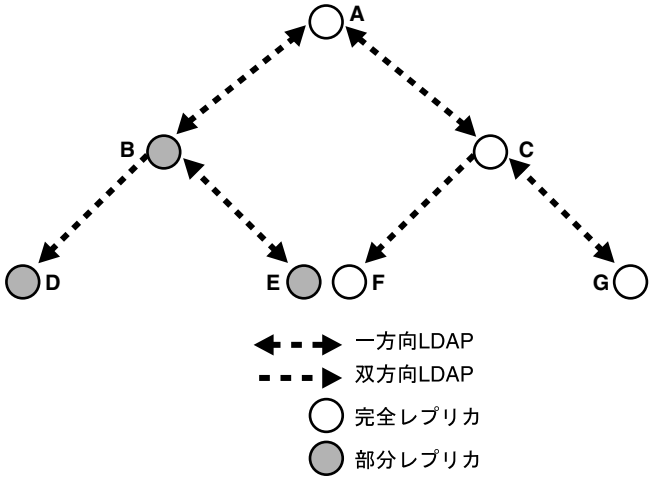


図 29-4 で、サプライヤ A は、B と C の 2 つのコンシューマをレプリケートします。コンシューマ・ノード B には、A の部分的なレプリカが含まれます。一方、コンシューマ・ノード C には、A の完全なレプリカが含まれます。

これらの各ノードが、データを他の 2 つのコンシューマにレプリケートするサプライヤとして機能します。ノード B はノード D および E に対して部分レプリケーションを行い、ノード C はノード F および G に対して完全レプリケーションを行います。ノード D および F は読取り専用です。

ファンアウト・レプリケーションでは、ノードは LDAP を使用してデータを転送します。

ディレクトリ・レプリケーションの各タイプの比較

表 29-6 に、マルチマスター、単一マスターおよびファンアウト・レプリケーションの比較を示します。

表 29-6 マルチマスター、単一マスターおよびファンアウト・レプリケーションの比較

マルチマスター・レプリケーション	単一マスター・レプリケーション	ファンアウト・レプリケーション
アドバンスト・レプリケーションのみを使用します。	LDAP ベースのレプリケーションまたはアドバンスト・レプリケーションを使用します（マルチマスター構成内の 1 つを除く他のすべてのマスターを読取り専用モードに切り替えた場合）。	LDAP ベースのレプリケーションを使用します。
更新は任意のノードで行うことができ、他のすべてのノードに伝播されます。	更新はマスター・ノード（サプライヤ）でのみ行うことができ、他のすべての読取り専用（コンシューマ）レプリカにレプリケートされます。	一方向ファンアウトの場合、更新はサプライヤ・レプリカでのみ行うことができ、コンシューマ・レプリカにレプリケートされます。 双方向ファンアウトの場合、更新は一方のレプリカでのみ行うことができ、他方のレプリカにレプリケートされます。

ファンアウトを使用したマルチマスター・レプリケーション

Oracle Internet Directory は、マルチマスター・レプリケーション・グループ内の任意のノードが、LDAP ベースのレプリケーション承諾の対象にもなるようにします。LDAP を使用して接続した先のノードは、次にデータをファンアウト構成内の他のノードに提供します。マルチマスター・レプリケーション承諾内では、ノード間のデータ転送は Oracle Database アドバンスト・レプリケーションを介して行われます。ファンアウト・レプリケーション承諾内では、サプライヤからコンシューマへのデータ転送は LDAP を介して行われます。LDAP レプリケーション承諾は、一方向または双方向のいずれかです。

注意： LDAP ベースのレプリカが読取り / 書込み可能な場合、このノードに対する変更は、コンシューマには伝播されますが、サプライヤには伝播されません。

図 29-5 に、ファンアウト・レプリケーションと組み合せて使用するマルチマスター・レプリケーションの例を示します。

図 29-5 ファンアウトを使用するマルチマスター・レプリケーションの例

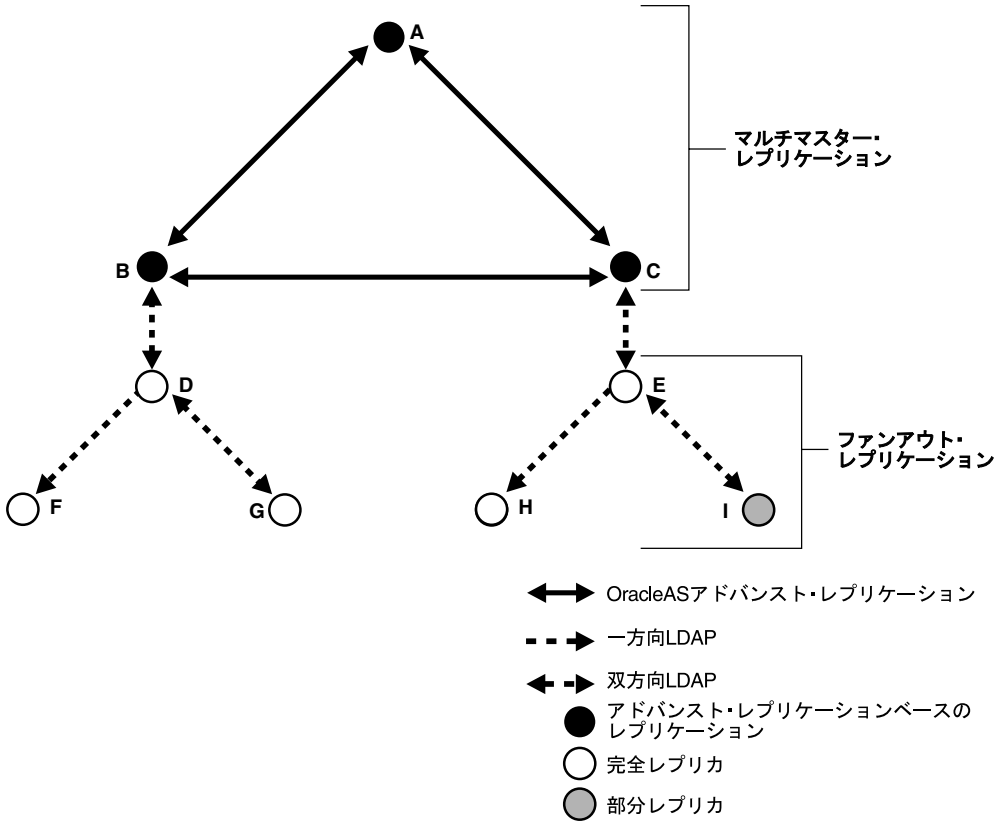


図 29-5 の例では、3 つのノード（A、B、C）がマルチマスター・レプリケーション・グループを形成しています。これらのノード間では、アドバンスト・レプリケーションを使用してデータを転送します。

ノード B は、ディレクトリ全体のレプリカであるノード D に変更を提供します。ノード D は、LDAP ベースのレプリケーションを使用して、ノード F および G に変更を提供します。ノード F および G は、ディレクトリ全体のレプリカです。同様にノード E はノード C の完全なレプリカです。ノード E は、LDAP ベースのレプリケーションを使用して、ディレクトリ全体のレプリカであるノード H および部分レプリカであるノード I に変更を提供します。ノード F および H は、読取り専用です。

> **関連項目：** ファンアウト・レプリケーションの詳細は、29-24 ページの「LDAP ベースのレプリケーション」を参照してください。

ディレクトリ内のレプリケーション構成オブジェクト

この項では、レプリケーション構成情報を含むディレクトリ内のオブジェクトについて説明します。この項の項目は次のとおりです。

レプリケーション構成コンテナ

ノードに関するすべてのレプリケーション情報は、ルート DSE にあるコンテナ cn=replication configuration 内に存在します。このエントリは、DRG 内の各ノードに存在します。次に、レプリケーション構成コンテナ・エントリの例を示します。

```
dn: cn=replication configuration
orclaci: access to entry by * (browse)
orclaci: access to attr=(*) by * (search,read)
orclnormdn: cn=replication configuration
cn: replication configuration
description: Replication agreement Container object
objectclass: top
objectclass: orclcontainerOC
```

レプリカ・サブエントリ

このサブエントリは、インストール時にレプリケーション構成コンテナの下に作成されます。サブエントリには、それが表すノードの特性を識別し、定義する属性が含まれています。表 29-7 では、レプリカ・サブエントリの属性を説明しています。

表 29-7 レプリカ・サブエントリの属性

属性	説明
OrclReplicaID	レプリカ・サブエントリのネーミング属性。この値は、インストール時に初期化される各ディレクトリ・サーバー・ノードに対し一意です。インストール時に割り当てられるこの属性の値は、各ディレクトリ・ノードに対し一意で、ルート DSE の orclreplicaID 属性の値と一致します。この値は変更できません。
orclReplicaURI	このレプリカに接続する際に使用できる ldapURI 形式の情報を指定します。
orclReplicaSecondaryURI	orclReplicaURI 値を使用できない場合に使用可能な ldapURI 形式のアドレスを含みます。
orclReplicaType	読取り専用、読取り / 書込みなどのレプリカのタイプを定義します。 次のいずれかの値です。 ■ 0（読取り / 書込み） ■ 1（読取り専用）
orclReplicaState	レプリカの状態を定義します。詳細は、付録 H「LDAP のレプリカ状態」を参照してください。

29-19 ページの図 29-8 では、レプリカ・サブエントリは orclReplicaID=*UID_of_node_D*,cn=replication configuration で表されています。

次に、レプリカ・サブエントリの例を示します。

```
dn: orclreplicaid=myhost1_repl1,cn=replication configuration
objectclass: top
objectclass: orclreplicasubentry
orclreplicaid: myhost1_repl1
orclreplicauri: ldap://myhost1:3060/
orclreplicasecondaryuri: ldap://myhost1.mycompany.com:3060/
orclreplicastate: 1
```

> **関連資料：** レプリカ・サブエントリの属性の詳細は、『Oracle Identity Management ユーザー・リファレンス』のレプリケーションのスキーマ要素に関する項を参照してください。

レプリケーション承諾エントリ

このエントリには、複数のノード間のレプリケーション承諾を定義する属性が含まれており、orclReplAgreementEntry オブジェクト・クラスに関連付けられます。承諾には次の 2 つの種類があります。

1. Oracle Database アドバンスト・レプリケーション承諾。Oracle Database アドバンスト・レプリケーション・ノードのレプリケーション承諾は、レプリケーション構成エントリの下に存在します。たとえば図 29-7 では、Oracle Database アドバンスト・レプリケーション承諾のエントリが orclagreementID=000001 で表されています。
2. LDAP ベースのレプリケーション承諾。LDAP ノードのレプリケーション承諾は、サプライヤのレプリカ・サブエントリの下に存在します。たとえば図 29-8 では、LDAP ベースのレプリケーション承諾のエントリが orclagreementID=000003, orclReplicaID=UID_of_node_D,cn=replication configuration で表されています。

レプリケーション承諾エントリの属性

表 29-8 に、レプリケーション承諾の属性を示します。

表 29-8 レプリケーション承諾エントリの属性

属性	説明
orclagreementID	レプリケーション承諾エントリのネーミング属性。この属性は変更できません。
OrclReplicaDN	LDAP ベースのレプリケーション専用。レプリケーション承諾においてコンシューマを識別するためのレプリカの識別名を指定します。この属性は変更できません。
OrclReplicationProtocol	レプリカへの変更伝播用のレプリケーション・プロトコルを定義します。指定可能な値は次のとおりです。 ■ ODS_ASR_1.0 は、アドバンスト・レプリケーション・ベースのプロトコルを指定します。 ■ ODS_LDAP_1.0 は、LDAP ベースのレプリケーションを指定します。 この属性は変更できません。
OrclDirReplGroupDSAs	アドバンスト・レプリケーション・ベースのグループの場合は、このレプリケーション・グループのすべてのノードの orclreplicaid 値。このリストは、グループのすべてのノードで同一であることが必要です。この属性は変更可能です。 この属性は、LDAP ベースの承諾に適用できません。
OrclUpdateSchedule	新規の変更および再試行される変更のレプリケーションの更新間隔。この値は分単位です。この属性は変更可能です。

表 29-8 レプリケーション承諾エントリの属性（続き）

属性	説明
OrclHIQSchedule	ディレクトリ・レプリケーション・サーバーが変更適用プロセスを繰り返す間隔（分単位）。この属性は変更可能です。
OrclLDAPConnKeepAlive	この属性は、ディレクトリ・レプリケーション・サーバーをディレクトリ・サーバーに常時接続するか、様々なスケジュールに基づいた変更ログ処理が行われるたびに接続するかを定義します。このフィールドは変更可能です。
Orcllastappliedchangenumber	これは、コンシューマ・レプリカで転送または適用された最後の変更番号です。LDAP ベース承諾の場合、この属性には、変更ログ処理のフェーズと、この変更番号が表すレプリケーションの方向を指定するサブタイプが含まれます。書式は次のとおりです。 orcllastappliedchangenumber; *status_type*$*supplier_replicaID*$*consumer_replicaID*: Number *status_type* は、この Orcllastappliedchangenumber によって表される変更ログ処理のフェーズを示します（29-24 ページの「LDAP ベースのレプリケーション」を参照）。次のいずれかの値です。 ■ transport ■ apply *supplier_replicaID* および *consumer_replicaID* は、この Orcllastappliedchangenumber によって表される LDAP データ・フローの方向を示します。 Number は、最後に適用された変更番号です。これは、Number より小さい変更番号を持つ *supplier_replicaID* から *consumer_replicaID* への変更ログは、*consumer_replicaID* で転送または適用されたことを示します。 この属性は、アドバンスト・レプリケーション・ベースの承諾に適用されますが、ベース型のみ使用されます。この属性は変更できません。
orclexcludednamingcontexts	この複数値属性の値は、レプリケーションから除外する 1 つ以上のサブツリーを指定します。 この属性は、アドバンスト・レプリケーション・ベースの承諾に適用されます。LDAP レプリケーションは、レプリケーション・ネーミング・コンテキスト・エントリ（表 29-9 を参照）を使用します。 この属性は変更可能です。
orclreplicationid	一方向、双方向または peer-to-peer レプリケーション・グループの一意の識別子。
orclagreementtype	レプリケーション承諾の識別子。レプリケーション承諾には次の 3 種類があります。 ■ 一方向 / 読取り専用ファンアウト・レプリケーション承諾 ■ 双方向 / 更新可能ファンアウト・レプリケーション承諾 ■ マルチマスター・レプリケーション承諾
changeloginfo	将来の使用のために予約。
orclsizelimit	一度に処理できる変更ログ数のバッチ・サイズ制限。

アドバンスト・レプリケーション承諾

アドバンスト・レプリケーションの場合、各ノードのレプリケーション承諾に、グループ内のすべてのノードが示されます。レプリケーション承諾は各ノードで同一ですが、ローカル・ディレクトリ・サーバー上にパーティション化されたネーミング・コンテキストなどのローカル・オプションは異なります。

このタイプのレプリケーション承諾のエントリは、コンテナ・エントリ cn=replication configuration の直下に存在します。たとえば、このような承諾の DN は、orclagreementID=000001,cn=replication configuration のようになります。

LDAP レプリケーション承諾

LDAP ベースのレプリケーションの場合、サプライヤとコンシューマの関係ごとに、別々のレプリケーション承諾があります。一方向レプリケーションの場合、単一の一方向レプリケーション承諾があります。

LDAP ベースのレプリケーション承諾のエントリは、サプライヤとして機能するノードのレプリカ・サブエントリの直下にあります。したがって、サプライヤ・ノードに対するレプリケーション承諾は、次のようになります。

orclagreementID=*unique_identifier_of_the_replication_agreement*, orclReplicaID=*unique_identifier_of_supplier_node*, cn=replication configuration

同様に、コンシューマ・ノードに対するレプリケーション承諾は、次のようになります。

orclagreementID=*unique_identifier_of_the_replication_agreeement*, orclReplicaID=*unique_identifier_of_supplier_node*, cn=replication configuration

ファンアウト・レプリケーション承諾の場合、親ノードを調べることで、承諾エントリと関連付けられているノードを識別できます。次に、レプリケーション承諾エントリの例を示します。

orclagreementID=000002,orclReplicaID=node_A,cn=replication configuration

この例では、orclagreementID=000002 で表されたレプリケーション承諾がノード A と関連付けられていることを確認できます。これは、orclagreementID=000002 の親が orclReplicaID=node_A であるためです。

注意： コンテナ・エントリ cn=replication configuration は、すべてのノードでレプリケートされますが、すべてのノードで同一ではない場合があります。

注意： LDAP ベースのレプリケーション承諾の orclreplicadn 属性は、関連付けられるコンシューマ・ノードを指定します。

双方向 LDAP レプリケーション承諾

双方向レプリケーションの場合、サプライヤとコンシューマの関係ごとに、単一の双方向レプリケーション承諾か 2 つの一方向承諾のいずれかになります。次に、双方向レプリケーション承諾エントリの例を示します。

```
dn: orclagreementid=000002, orclreplicaid=stadd58, cn=replication configuration
orclagreementid: 000002
orclreplicationprotocol: ODS_LDAP_1.0
orclreplicadn: orclreplicaid=stadd57,cn=replication configuration
orclldapconnkeepalive: 1
orclagreementtype: 1
orclreplicationid: 000002
orcllastappliedchangenumber;transport$stadd57$stadd58: 106
orcllastappliedchangenumber;transport$stadd58$stadd57: 2421
orcllastappliedchangenumber;apply$stadd57$stadd58: 106
orcllastappliedchangenumber;apply$stadd58$stadd57: 2421
orclupdateschedule: 0
orclhiqschedule: 1
objectclass: orclReplAgreementEntry
objectclass: top
```

> **関連資料：** レプリケーション承諾エントリの属性の詳細は、『Oracle Identity Management ユーザー・リファレンス』のレプリケーションのスキーマ要素に関する項を参照してください。

レプリケーションのネーミング・コンテキスト・コンテナ・エントリ

このエントリには、LDAP ネーミング・コンテキストのすべてのオブジェクトが含まれています。

このエントリには、相対識別名（RDN）`cn=replication namecontext` が含まれています。この相対識別名は、レプリケーションの構成時に `orclagreementID` エントリの下に作成されます。次に、レプリケーションのネーミング・コンテキスト・コンテナ・エントリの例を示します。

```
dn: cn=replication namecontext,orclagreementid=000002,
 orclreplicaid=myhost1_repl1,cn=replication configuration
objectclass: top
objectclass: orclcontainerOC
cn: replication namecontext
```

レプリケーションのネーミング・コンテキスト・オブジェクト・エントリ

このエントリには、LDAP ネーミング・コンテキストのすべてのオブジェクトが含まれています。これらのオブジェクトは、レプリケーション・フィルタ・ポリシー、つまり LDAP ベースの部分レプリカに対するレプリケーションに何を含めるか、あるいはレプリケーションから何を除外するかを指定します。

注意： アドバンスト・レプリケーション・ベースの承諾では、ネーミング・コンテキストの含めたり、属性を除外したりできません。アドバンスト・レプリケーション承諾では、表 29-8 で説明されているベース属性の `orclexcludednamingcontexts` を使用します。

このエントリは、レプリケーションの構成時に、ネーミング・コンテキスト・コンテナ・エントリの下に作成されます。このエントリは構成可能です。たとえば 29-19 ページの図 29-8 では、レプリケーション・ネーミング・コンテキスト・オブジェクトは `cn=namingcontext001,cn=replication namecontext,orclagreementID=000003,orclReplicaID=`*`UID_of_node_D`*`,cn=replication configuration` です。

表 29-9 レプリケーション・ネーミング・コンテキスト・エントリの属性

属性	説明
`orclincludednaming contexts`	レプリケートされるネーミング・コンテキストのルート。この属性には、ネーミング・コンテキストを含めるレプリケーションの方向を指定するサブタイプがあります。書式は次のとおりです。 `orclincludednamingcontexts ;` *`supplier_replicaID`*`$consumer_replicaiD: DN` この属性は単一の値です。ネーミング・コンテキスト・オブジェクトごとに、各方向に 1 つの一意のサブツリーのみを指定できます。 部分レプリケーションでは、orclexcluednamingcontexts 属性に指定されたサブツリーを除き、ネーミング・コンテキストに含まれているサブツリーはすべてレプリケートされます。 この属性は変更可能です。
`orclexcludednaming contexts`	レプリケーションから除外する、サブツリー（含まれているネーミング・コンテキスト内）のルート。この属性には、ネーミング・コンテキストが除外されるレプリケーションの方向を指定するサブタイプがあります。書式は次のとおりです。 `orclexcludednamingcontexts;` *`supplier_replicaID$consumer_replicaiD`* `: DN` この属性は複数値です。orclincludednamingcontexts 属性で指定したネーミング・コンテキスト内から、各方向で部分レプリケーションから除外する 1 つ以上のサブツリーを指定できます。 この属性は変更可能です。
`orclexcludedattributes`	含まれているネーミング・コンテキスト内にある、レプリケーションから除外する属性。`orclexcludedattributes` には、指定した属性を除外するレプリケーションの方向を指定するサブタイプがあります。書式は次のとおりです。 `orclexcludedattributes;` *`supplier_replicaID$consumer_replicaiD`*`: attribute_name` この属性は複数値です。 この属性は変更可能です。

次に、レプリケーションのネーミング・コンテキスト・オブジェクト・エントリの例を示します。

```
dn:cn=namectx001,
cn=replication namecontext,
orclagreementid=unique_identifier_of_the_replication_agreement,
orclreplicaid=replica_id_of_node_A,
cn=replication configuration
orclincludednamingcontexts: cn=mycompany
orclexcludednamingcontexts; replica_id_of_node_A$ replica_id_of_node_B :
c=us,cn=mycompany
orclexcludedattributes; replica_id_of_node_B$ replica_id_of_node_A : userPassword
```

この例では、次のレプリケーション・フィルタを指定しています。

- ネーミング・コンテキスト cn=mycompany は、ノード A とノード B の双方向のレプリケーションに含まれます。
- ネーミング・コンテキスト c=us,cn=mycompany は、ノード A からノード B へのレプリケーションでのみ除外されます。
- userPassword 属性は、ノード B からノード A へのレプリケーションで除外されます。

関連資料:

- 29-32 ページの「LDAP レプリケーションのフィルタリングの例」
- 『Oracle Identity Management ユーザー・リファレンス』のレプリケーションのスキーマ要素に関する項

ディレクトリ・レプリケーション・サーバー構成パラメータ

表 29-10 に、次の識別名を持つレプリケーション・サーバー構成設定エントリの属性およびその説明を示します。

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

表 29-10 ディレクトリ・レプリケーション・サーバー構成パラメータ

パラメータ名	説明
modifyTimestamp	エントリの作成または変更の日時。 このパラメータは変更できません。
modifiersName	エントリの作成者または変更者の名前。 このパラメータは変更できません。
orclChangeRetryCount	単一値の属性。管理者操作キューに移動される前に、変更エントリに対して行われる処理再試行回数。このパラメータの値は、1 以上にする必要があります。 デフォルトは 10 です。このパラメータは変更できます。
orclThreadsPerSupplier	変更ログを転送または適用するために、各サプライヤで生成されたワーカー・スレッド数。このパラメータには 2 つのサブタイプがあります。書式は次のとおりです。 orclthreadspersupplier; *work_type*: Number *work_type* に使用可能な値は次のとおりです。 ■ transport ■ apply デフォルトは、転送に 1 ワーカー・スレッド、適用に 5 ワーカー・スレッドです。このパラメータは変更できます。

ディレクトリ内のレプリケーション構成オブジェクトの例

この項で説明するレプリケーション・オブジェクトの例は、図 29-6 に示すレプリケーション環境に依存します。

図 29-6 例 : マルチマスター・レプリケーションおよびファンアウト・レプリケーション

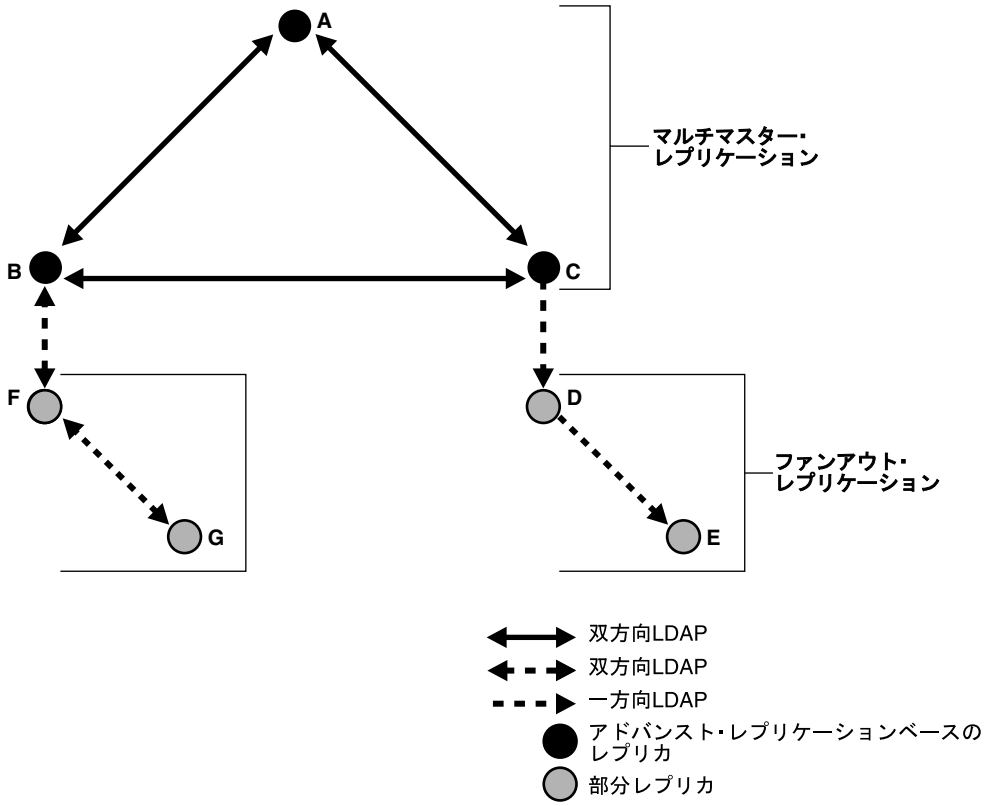


図 29-6 では、3 つのノード（A、B、C）がマルチマスター・レプリケーション・グループを形成しています。ノード C は、4 番目のノード D に対してレプリケーションを行い、ノード D はノード E にファンアウトします。

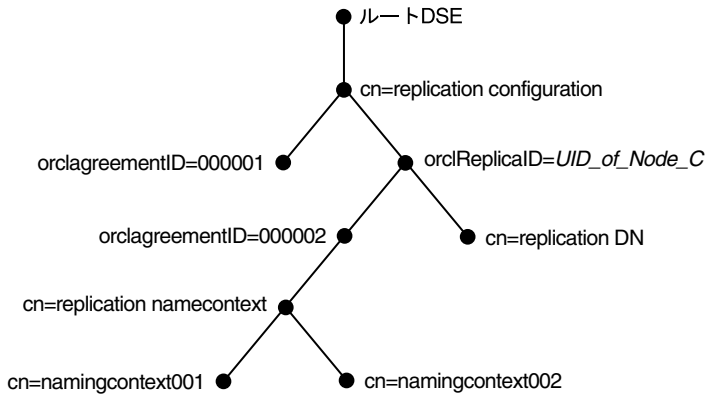
この環境のレプリケーション承諾は、次のとおりです。

- ノード A には、ノード B および C とのマルチマスター関係を表す 1 つのレプリケーション承諾があります。
- ノード B には、2 つのレプリケーション承諾があります。1 つは、ノード A および C とのマルチマスター関係を表し、もう 1 つは、ノード F との関係を表しています。ノード B および F 間のレプリケーション承諾は双方向です。
- ノード C には、2 つのレプリケーション承諾があります。1 つは、ノード A および B とのマルチマスター関係を表し、もう 1 つは、ノード C との関係を表しています。後者は一方向レプリケーション承諾で、ノード C がサプライヤでノード D がコンシューマです。
- ノード D には、2 つのレプリケーション承諾があります。どちらのレプリケーション承諾も一方向です。1 つは、ノード D が変更情報を消費するサプライヤ・ノード C との関係を表し、もう 1 つは、ノード D がサプライヤとなるコンシューマ・ノード E との関係を表しています。
- ノード E には、ノード D との一方向レプリケーション承諾が 1 つあります。ノード E はコンシューマです。

- ノード F には、2 つのレプリケーション承諾があります。1 つは、ノード B との関係を表し、もう 1 つは、ノード B との関係を表しています。どちらも両方向レプリケーション承諾です。
- ノード E には、ノード D との一方向レプリケーション承諾が 1 つあります。ノード E はコンシューマです。

図 29-7 に、29-17 ページの図 29-6 で説明したノード C に関連する DIT 内のレプリケーション・オブジェクトを示します。

図 29-7 例 : ノード C についてのレプリケーション構成エントリ



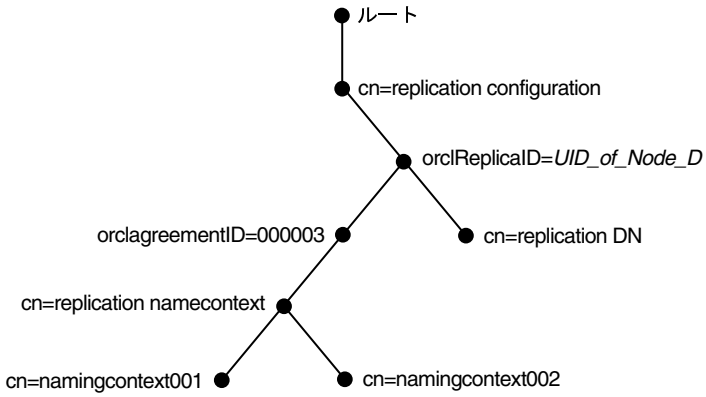
ノード C の場合、ルート DSE にあるエントリ `cn=replication configuration` には、次の RDN が含まれています。

- `orclagreementID=000001`: ノード C をノード A およびノード B に関連付けるマルチマスター・レプリケーション承諾。
- `orclReplicaID=UID_of_node_C`: ノード C の一意識別子。ノード C に関する情報が含まれています。
- `orclagreementID=000002`: サプライヤ・ノード C とコンシューマ・ノード D 間の関係を表す一意の識別子。この場合、ノード C が親になっているため、`orclagreementID=000002` がサプライヤ・ノード C のレプリケーション承諾です。

  このエントリには、`orclreplicaDN` 属性が含まれています。この属性の値は、レプリケーション承諾がノード C に含まれているコンシューマ・ノード D のレプリカ・エントリ DN です。
- `cn=replication DN`: ノード C 上のディレクトリ・レプリケーション・サーバーが、ディレクトリ・サーバーにバインドするときに使用するバインド識別名。
- `cn=replication namecontext`: レプリケーションに含まれるネーミング・コンテキストに関する情報のコンテナ。
- `cn=namingcontext001` および `cn=namingcontext002`: レプリケーションに含まれているか、またはレプリケーションから除外されている実際のオブジェクト。レプリケーションに含まれるネーミング・コンテキストには、レプリケーションから除外する 1 つ以上のサブツリーを指定できます。また、レプリケーションから除外する属性も指定できます。

図 29-8 に、29-17 ページの図 29-6 で説明したノード D に関連する DIT 内のレプリケーション承諾エントリを示します。

図 29-8 例 : ノード D についてのレプリケーション構成エントリ



ノード D の場合、ルート DSE にあるエントリ `cn=replication configuration` には、次の RDN が入っています。

- `orclReplicaID=`*`UID_of_node_D`*: ノード D の一意識別子。ノード D に関する情報が含まれています。
- `orclagreementID=000003`: サプライヤ・ノード D とコンシューマ・ノード E 間の関係を表す一意の識別子。この場合、ノード D が親になっているため、`orclagreementID=000003` がサプライヤ・ノード D のレプリケーション承諾です。

  このエントリには、`orclreplicaDN` 属性が含まれています。この属性の値は、レプリケーション承諾がノード D に含まれているコンシューマ・ノード E の DN です。
- `cn=replication DN`: ノード D 上のディレクトリ・レプリケーション・サーバーが、ディレクトリ・サーバーにバインドするときに使用するバインド識別名。
- `cn=replication namecontext`: レプリケーションに含まれるネーミング・コンテキストに関する情報のコンテナ。
- `cn=namingcontext001` および `cn=namingcontext002` レプリケーションに含まれるネーミング・コンテキストを指定するオブジェクト。レプリケーションに含まれるネーミング・コンテキストには、レプリケーションから除外する 1 つ以上のサブツリーまたは特定の属性を指定できます。

レプリケーションのセキュリティ

この項の項目は次のとおりです。

認証およびディレクトリ・レプリケーション・サーバー

認証は、Oracle ディレクトリ・レプリケーション・サーバーが、ディレクトリ・サーバーへの接続時に、サーバー自身の正確な識別情報を取得するプロセスです。認証は、LDAP セッションが ldapbind 操作によって確立されたときに発生します。

ディレクトリ・レプリケーション・サーバーが、ディレクトリへのアクセスを許可される前に適切に認証されることが重要です。

ディレクトリ・レプリケーション・サーバーは、一意識別子とパスワードを使用して、ディレクトリ・サーバーに対する認証を行います。ディレクトリ・レプリケーション・サーバーの識別情報は、`cn=replication dn,orclreplicaid=`*`unique_identifier_of_node`*`, cn=replication configuration` の形式をとります。

ディレクトリ・レプリケーション・サーバーは、起動時、Oracle Internet Directory の安全な Wallet から識別情報とパスワードを読み取り、これらの資格証明を使用して認証を行います。レプリケーションのバインド識別名を変更する場合は、レプリケーション環境管理ツールの `-pchgpwd`、`-presetpwd` または `-pchgwalpwd` オプションを使用する必要があります。レプリケーションの識別情報の Wallet は、`$ORACLE_HOME/ldap/admin/oidpwdr`*`Oracle_SID`* にあります。

> **関連資料：**『Oracle Identity Management ユーザー・リファレンス』の `remtool` コマンドライン・ツールのリファレンス

注意： 以前のリリースでは、レプリケーション・サーバーを実行するには、ディレクトリ・サーバーで匿名バインドを許可する必要がありました。このリリースではその必要はありません。

Secure Sockets Layer（SSL）と Oracle Internet Directory レプリケーション

Oracle Internet Directory レプリケーションは、SSL の使用に関係なく配置できます。ターゲットの Oracle Internet Directory インスタンスが SSL ポートで実行しているかどうかは、レプリケーションで自動的に検出されます。レプリケーション・サーバーが Oracle Internet Directory インスタンスの SSL ポートにバインドしている場合は、自動的に SSL 上で動作します。

注意： Oracle Internet Directory 10*g*（10.1.4.0.1）の場合、Oracle ディレクトリ・レプリケーション・サーバーは、双方向（相互）認証をサポートする SSL 対応の LDAP サーバーと直接通信できません。LDAP サーバーが SSL 相互認証用に構成されていると、レプリケーション・サーバーの起動は失敗し、停止します。

SSL 暗号化を使用するように LDAP ベースのレプリケーションを構成するには、サプライヤ連絡先情報が含まれている `orclReplicaURI` 属性に、SSL ポートのポート番号を指定します。

SSL 暗号化を使用するようにアドバンスト・レプリケーションを構成するには、Oracle Advanced Security を使用します。

> **関連資料：** SSL 暗号化を使用するようにアドバンスト・レプリケーションを構成する方法は、『Oracle Advanced Security 管理者ガイド』を参照してください。

ディレクトリ・レプリケーションの変更ログ

Oracle Internet Directory は、各変更をエントリとして変更ログ・ストアに記録します。コンシューマは、最後に適用した変更の番号を記録しておき、その番号よりも大きい番号を持つ変更のみをサプライヤから取得します。

変更ログ・ストアの各エントリ（各変更ログ・オブジェクト）には、一意の変更番号が含まれています。コンシューマは、最後に適用した変更の番号よりも大きい番号を持つ変更のみをサプライヤから取得します。

- LDAP ベース・レプリケーション承諾では、変更ログの処理は、変更ログの転送と変更ログの適用という 2 つのフェーズで構成されています。LDAP ベース承諾ごとに、2 つの変更ログ処理のステータス（各フェーズに 1 つ）があります。ディレクトリ・レプリケーション・サーバーは、最後に転送した変更番号を、レプリケーション承諾エントリの `orlcllastappliedchangenumber` 属性の `transport` サブタイプに格納します。ディレクトリ・レプリケーション・サーバーは、最後に適用した変更番号を、レプリケーション承諾エントリの `orllclastappliedchangenumber` 属性の `apply` サブタイプに格納します。`orlcllastappliedchangenumber` 属性の書式は、29-11 ページの表 29-8「レプリケーション承諾エントリの属性」を参照してください。
- アドバンスト・レプリケーション・ベースのレプリケーション承諾では、ディレクトリ・レプリケーション・サーバーによって、最後に転送された変更番号が `changestatus` エントリの `changenumber` 属性に格納されます。`changenumber` 属性は、次のようになります。

  ```
  changenumber=last_applied_change_number, supplier=supplier_node,
  consumer=consumer_node
  ```

  たとえば、コンシューマが最後に適用した変更の番号が 250 の場合、それ以降サプライヤから取得する変更の番号は、250 より大きい番号である必要があります。

変更ログは、レプリケーション・サーバーがコンシュームした後、ガベージ・コレクタによって消去されます。

関連項目：

- 第 26 章「Oracle Internet Directory におけるガベージ・コレクション」
- 29-21 ページの「Oracle Database アドバンスト・レプリケーション」
- 29-24 ページの「LDAP ベースのレプリケーション」

Oracle Database アドバンスト・レプリケーション

この項では、Oracle Database アドバンスト・レプリケーションの詳細を説明します。この項の項目は次のとおりです。

- Oracle Database アドバンスト・レプリケーションの機能
- Oracle Database アドバンスト・レプリケーションのアーキテクチャ

関連項目：

- 第 31 章「Oracle Internet Directory レプリケーションの監視および管理」
- 付録 F「マルチマスター・レプリケーション・プロセス」

Oracle Database アドバンスト・レプリケーションの機能

Oracle Database アドバンスト・レプリケーションでは、レプリケーション承諾がなされたノード間における更新情報の転送は、Oracle Database アドバンスト・レプリケーションのストア / フォワード機能によって管理されます。アドバンスト・レプリケーションを使用すると、2 つの Oracle データベース間で、データベース表を同期化させることができます。

Oracle Database アドバンスト・レプリケーション

- ローカルの変更内容を格納し、コンシューマに定期的にまとめて伝播します。コンシューマ・レプリケーション・サーバーは、リモートの変更内容をサーバー固有のローカルのディレクトリ・サーバーに適用し、ローカル・ストアから適用済のリモートの変更内容を削除します。
- Oracle レプリケーション・グループ内のどこにあるディレクトリ表に対しても読取りおよび更新アクセスできるようにします。一般的なアドバンスト・レプリケーション構成では、行レベル・レプリケーションが使用されます。
- 実証済のネットワーク・トレランスを提供します。データ転送は、Oracle Enterprise Manager 10*g* Application Server Control コンソールで制御および監視できます。このような管理機能によって、データ移送のスケジュール方法に高度な柔軟性を与えることができます。

注意： Oracle Internet Directory と同じデータベース内に常駐する Oracle Application Server Single Sign-On のデータベース・スキーマも、アドバンスト・レプリケーションを使用してレプリケートします。

関連資料：

- 『Oracle Application Server Single Sign-On 管理者ガイド』の高可用性に関する章でレプリケーションのための Oracle Application Server Single Sign-On の構成に関する項を参照してください。
- アドバンスト・レプリケーションの詳細は、Oracle Database ドキュメント・ライブラリの『Oracle Database アドバンスト・レプリケーション』を参照してください。

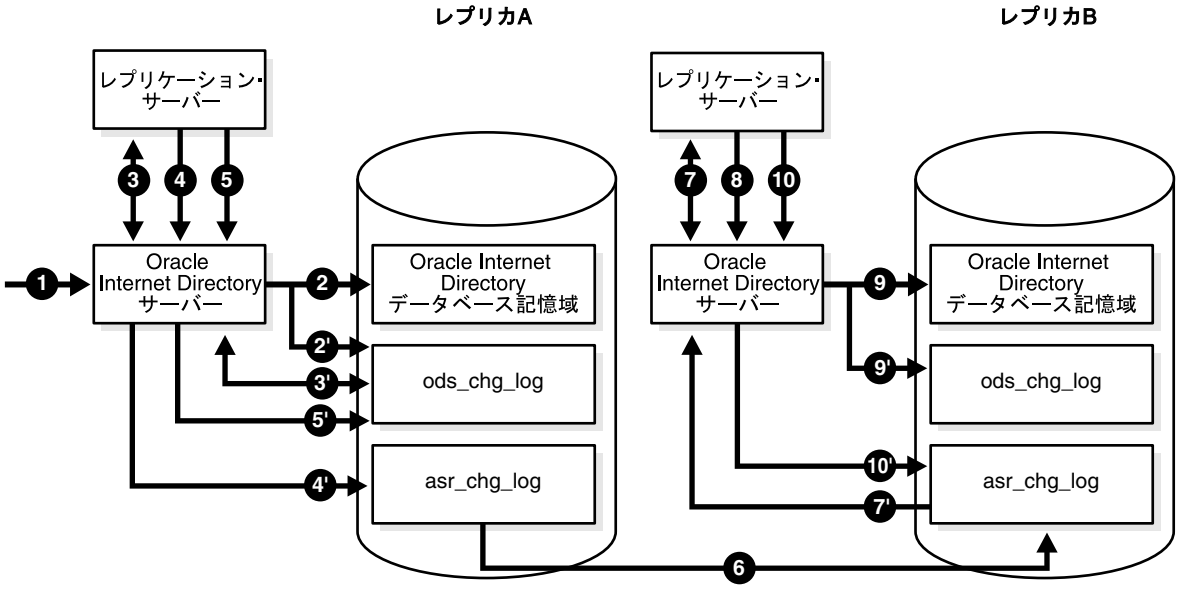
Oracle Database アドバンスト・レプリケーションのアーキテクチャ

一般的な Oracle Database アドバンスト・レプリケーション構成では、サプライヤが変更内容を変更ログに書き込み、バッチ処理された変更を他のコンシューマに定期的に送信する非同期データ伝播を使用します。コンシューマは変更ログ・データを受信し、変更内容をローカルに適用します。

レプリケーションを構成する場合は、レプリケーション・グループ内で変更を共有するノードを指定します。レプリケーションの基本アーキテクチャは、レプリケーション環境に導入するノードの数に関係なく一定です。ローカル変更はリモート・マスター・サイト（RMS）に配布されます。ここで、クライアントとして機能するレプリケーション・サーバーが Oracle Internet Directory サーバーにコマンドを送信し、ディレクトリ・サーバーは受け取ったコマンドを実行します。

図 29-9 とその後に続く説明では、Oracle Database アドバンスト・レプリケーション・プロセスの概要を示します。

図 29-9 アドバンスト・レプリケーション・プロセス



プロセスは次のとおりです。

1. レプリカ A の Oracle Internet Directory サーバーで変更リクエストが作成されます。
2. 変更は、受け入れられ、Oracle Internet Directory データベースのストレージにコミットされます。

   2'. この操作に対して新規の変更ログが生成され、ods_chg_log 表（server = レプリカ A）に格納されます。
3. レプリカ A 上のレプリケーション・サーバーは、ローカルの ods_chg_log 表に新規のアウトバウンド変更ログを問い合せます。この問合せには次のフィルタが使用されます。

   ```
   (& (objectclass=changeLogEntry) (servername=ReplicaID_of_A)
        (changeNumber>= Last_Applied_ChgNum_From_A_TO_A) )
   ```

   この検索操作とともに、処理承諾で指定された orclreplicationid の値で制御も渡されます。値 1 は、アドバンスト・レプリケーション承諾のために予約されています。

   Last_Applied_ChgNum_From_A_TO_A は、アウトバウンド変更ログ処理ステータスです。
4. ods_chg_log から取得した新規の変更ログは、ローカルの asr_chg_log にコピーされます。
5. レプリケーション・サーバーは、Oracle Internet Directory サーバーに対して、変更ログ retry_cnt のステータスを正しく更新するようにリクエストします。

   5'. Oracle Internet Directory サーバーは、ods_chg_log 表にある変更ログの retry_cnt を更新します。
6. 新規の変更ログは、Oracle Database アドバンスト・レプリケーションを介して、レプリカ A からレプリカ B に送信されます。
7. レプリカ B 上のレプリケーション・サーバーは、ローカルの asr_chg_log 表に新規のインバウンド変更ログを問い合せます。次のフィルタが使用されます。

   ```
   (& (objectclass=changeLogEntry)  (servername=ReplicaID_of_A)
          (changeNumber>= Last_Applied_ChgNum_From_A_TO_B))
   ```

8. レプリケーション・サーバーは、レプリカ B で新規の変更を適用します。
9. レプリカ B の Oracle Internet Directory サーバーは、変更を受け入れ、Oracle Database のストレージにコミットします。

   9'. ローカル・レプリカに LDAP ベースのコンシューマ・レプリカがある場合、変更ログがレプリカ B にある `ods_chg_log` 表で、次の規則に従って再生成されます。

   ```
   server = server of local replica,
   ReplicaB orclreplicationid/chg_rid =  1
   Modifiersname = Replbind_DN_of_A
   ```

   `orclreplicatid/chg_rid` は、処理承諾の `orclreplicationid` の値に設定されます。この場合、変更がアドバンスト・レプリケーションを介してレプリケートと処理が行われるため、値はアドバンスト・レプリケーション用に予約されている 1 に設定されます。
10. レプリケーション・サーバーは、Oracle Internet Directory サーバーに対して、シャドウ変更ログ `retry_cnt` のステータスを正しく更新するようにリクエストします。

    10'. Oracle Internet Directory サーバーは、データベースのシャドウ変更ログの `retry_cnt` を更新します。

適用済のエントリや候補の変更に従って削除されたエントリのパージが定期的に発生します。ローカルの変更ログ表にあるリモート変更の記録は、その変更がローカルで適用されると、ガベージ・コレクション・スレッドによってパージされます。ローカルの変更ログ表にあるローカル変更の記録は、その変更がすべてのコンシューマに配布されると、ガベージ・コレクション・スレッドによってパージされます。

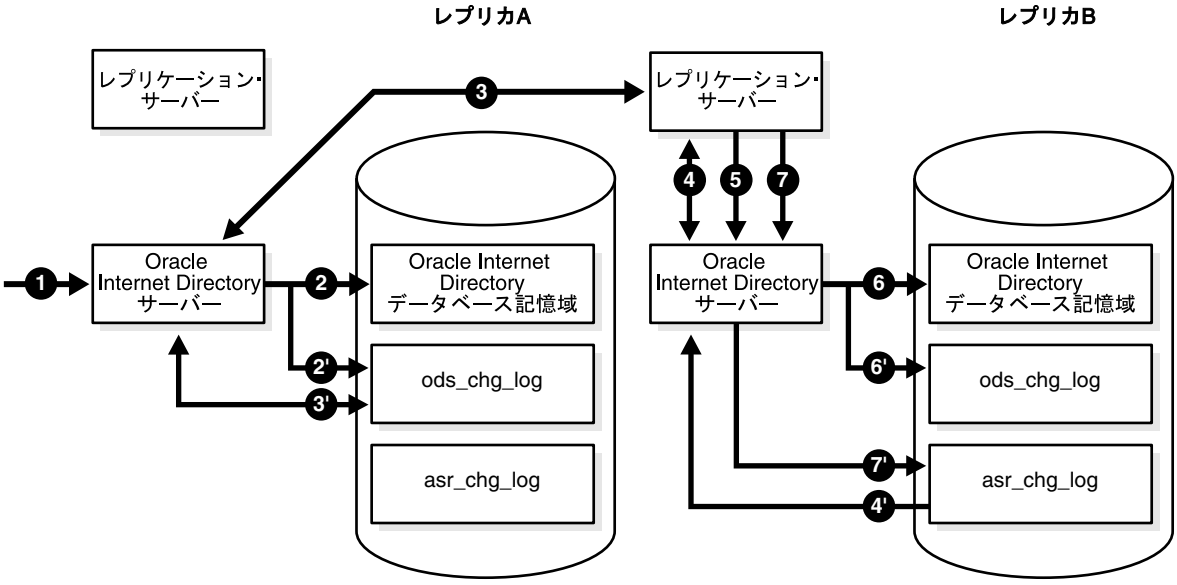
> **関連項目：** レプリケーションの構成方法は、第 31 章「Oracle Internet Directory レプリケーションの監視および管理」を参照してください。

LDAP ベースのレプリケーション

この項では、LDAP レプリケーションの詳細を説明します。LDAP レプリケーションでのデータ・フローは、転送と適用の 2 つのフェーズで構成されます。

図 29-10 およびその後に続く説明では、LDAP レプリケーション・プロセスを示します。

図 29-10 LDAP レプリケーション・プロセス



1. LDAP 変更リクエストが、レプリカ A の Oracle Internet Directory サーバーで作成されます。
2. 変更は、受け入れられ、Oracle Internet Directory データベースのストレージにコミットされます。

   2'. この操作に対して新規の変更ログが生成され、ods_chg_log 表に格納されます。

   server = レプリカ A

   orclreplicationid/chg_rid = 0（値 0 はユーザー操作）

   Modifiersname = 修飾子のユーザー識別名（デフォルト）
3. レプリカ B 上のレプリケーション・サーバーは、サプライヤのレプリカ、レプリカ A の ods_chg_log 表に新規のインバウンド変更ログを問い合せます。この問合せには次のフィルタが使用されます。

   ```
   (& (objectclass=changelogentry)
   (changeNumber>=Last_Transported_ChgNum_From_A_TO_B)
   (! (modifiersname=ReplicaID_of_B))
   (! (orclreplicatonid = Orclreplicationid_Attribute_Value_of_Processing_Agreement))
   (!(targetdn=*,excluded_naming_ctx_dn ) (….) (….) ….)
   (targetdn=cn=catalogs) (targetdn=cn=subschemasubentry)
   (targetdn=cn=oracleschemaversion) (targetdn=*,included_naming_ctx_dn) (targetdn=….)
   …)
   ```

   この検索操作とともに、処理承諾で指定された orclreplicationid の値で制御も渡されます。
4. レプリカ B のレプリケーション・サーバーは、レプリカ B の Oracle Internet Directory に新規の変更ログをシャドウ変更ログとして格納するようにリクエストします。

   4'. レプリカ B の Oracle Internet Directory サーバーは、レプリカ B の asr_chg_log 表にシャドウ変更ログを格納します。

   手順 3、3' および 4 は、LDAP ベース変更ログ処理の転送部分と一致します。
5. レプリカ B のレプリケーション・サーバーは、ローカルの変更ログ・ストア asr_chg_log にレプリカ A の新規の変更ログを問い合せます。この問合せには次のフィルタが使用されます。

   ```
   (& (objectclass=changeLogEntry) (servername=ReplicaID_of_A)
     (changeNumber>= Last_Applied_ChgNum_From_A_TO_B))
   ```
6. レプリカ B のレプリケーション・サーバーは、レプリカ B の Oracle Internet Directory サーバーに取得した変更をストレージに適用するようにリクエストします。
7. レプリカ B の Oracle Internet Directory サーバーは、変更を受け入れ、Oracle Internet Directory データベースのストレージにコミットします。

   7'. ローカルのレプリカがその他のレプリカのソースである場合、レプリカ B の ods_chg_log 表に変更ログが、次の変更ログ再生成規則に従って再生成されます。

   ```
   server = server of local replica, ReplicaB
   orclreplicationid/chg_rid =  N
   Modifiersname = Replbind_DN_of_A
   ```

   orclreplicatid/chg_rid は、処理承諾の orclreplicationid 値に設定されます。
8. レプリケーション・サーバーは、サーバーに対して、シャドウ変更ログ retry_cnt のステータスを正しく更新するようにリクエストします。

Oracle レプリケーションにおける競合の解消

Oracle Database アドバンスト・レプリケーションと双方向 LDAP ベース・レプリケーションにより、複数のディレクトリ・サーバーに対する更新が可能になります。競合は、ディレクトリ・レプリケーション・サーバーがサプライヤからコンシューマにリモートの変更を適用しようとして失敗した場合、常に発生します。

レプリケーション・プロセスで変更が適用できないことがあります。たとえば、サプライヤのノード A がコンシューマに変更を送信し、その直後にサプライヤのノード B が同じエントリの更新をコンシューマ送信したとします。このとき、なんらかの問題が発生して、サプライヤのノード A からのエントリ送信が遅れたが、サプライヤのノード B からの更新送信にはそのような問題が発生しなかったとします。この結果、サプライヤのノード B からの更新が、エントリの変更よりも先にコンシューマに到着することになります。この場合、レプリケーション・サーバーは、指定された回数まで変更の適用を試みます。指定された回数に達しても変更が適用できなかった場合、レプリケーション・サーバーは変更内容を管理者操作キューに移動し、それ以降は指定した間隔よりも少ない頻度で定期的に適用を試みます。

次の 4 種類の LDAP 操作が競合を引き起こす可能性があります。

- 追加
- 削除
- 変更
- 相対識別名または識別名の変更

レプリケーション競合が発生するレベル

競合には次の 2 つのタイプがあります。

- エントリ・レベルの競合
- 属性レベルの競合

表 29-11 レプリケーション競合のタイプ

レプリケーション競合のレベル	説明
エントリ・レベルの競合	ディレクトリ・レプリケーション・サーバーが、コンシューマに変更を適用するときに発生します。次のいずれかのタイプの変更がコンシューマで発生する可能性があります。 ■ すでに存在しているエントリの追加 ■ 存在していないエントリの削除 ■ 存在していないエントリの変更 ■ 存在していない識別名に対する識別名の変更操作 これらの競合は、解消するのが難しい場合があります。たとえば、次のような原因の場合は競合を解消するのが不可能な可能性があります。 ■ エントリが別の位置に移動 ■ エントリがサプライヤから未到着 ■ エントリが削除済 ■ エントリがコンシューマに存在しない 存在する必要がないエントリが存在している場合は、以前に追加済であるか、最近識別名の操作変更があった可能性があります。
属性レベルの競合	2 つのディレクトリが、同じ属性を異なる値で異なる時間に更新している場合に発生します。属性が単一値の場合、レプリケーション・プロセスは、競合に含まれている変更のタイムスタンプを検証して、競合を解消します。

競合の一般的な原因

通常、競合は Wide Area Network 上で発生する場合がある通信速度の低下や送信エラーが原因で発生する変更の時間的なずれが原因です。また、過去に発生した不整合がタイムリに解消されていない場合、引き続き競合が発生する可能性があります。

競合の自動解消

ディレクトリ・レプリケーション・サーバーは、次の処理によって、発生した競合をすべて解消しようとします。

1. 変更が適用されたときに、競合が検出されます。
2. レプリケーション・プロセスは、特定の待機期間が過ぎると、特定回数分または反復による変更の再適用を、特定期間試行します。
3. レプリケーション・プロセスが変更の適用に成功しないまま再試行制限に達した場合、変更に競合のフラグを付けた後、解消を試みます。解消規則（次の項で説明）に従って競合を解消できない場合は、優先順位の低い管理者操作キューにその変更を移動します。変更は、レプリケーション承諾された `orclHIQSchedule` パラメータに指定した時間単位に従って適用されます。ディレクトリ・レプリケーション・サーバーは、変更を移動する前にシステム管理者用のログ・ファイルに競合を書き込みます。

注意： レプリケーション時に、スキーマ、カタログおよびグループ・エントリの競合の解消は行われません。これは、多数の複数値の属性の競合を解消しようとすると、パフォーマンスに重大な影響を及ぼす可能性があるためです。一度に複数のマスターからこのようなエントリの更新を行うことは、回避してください。

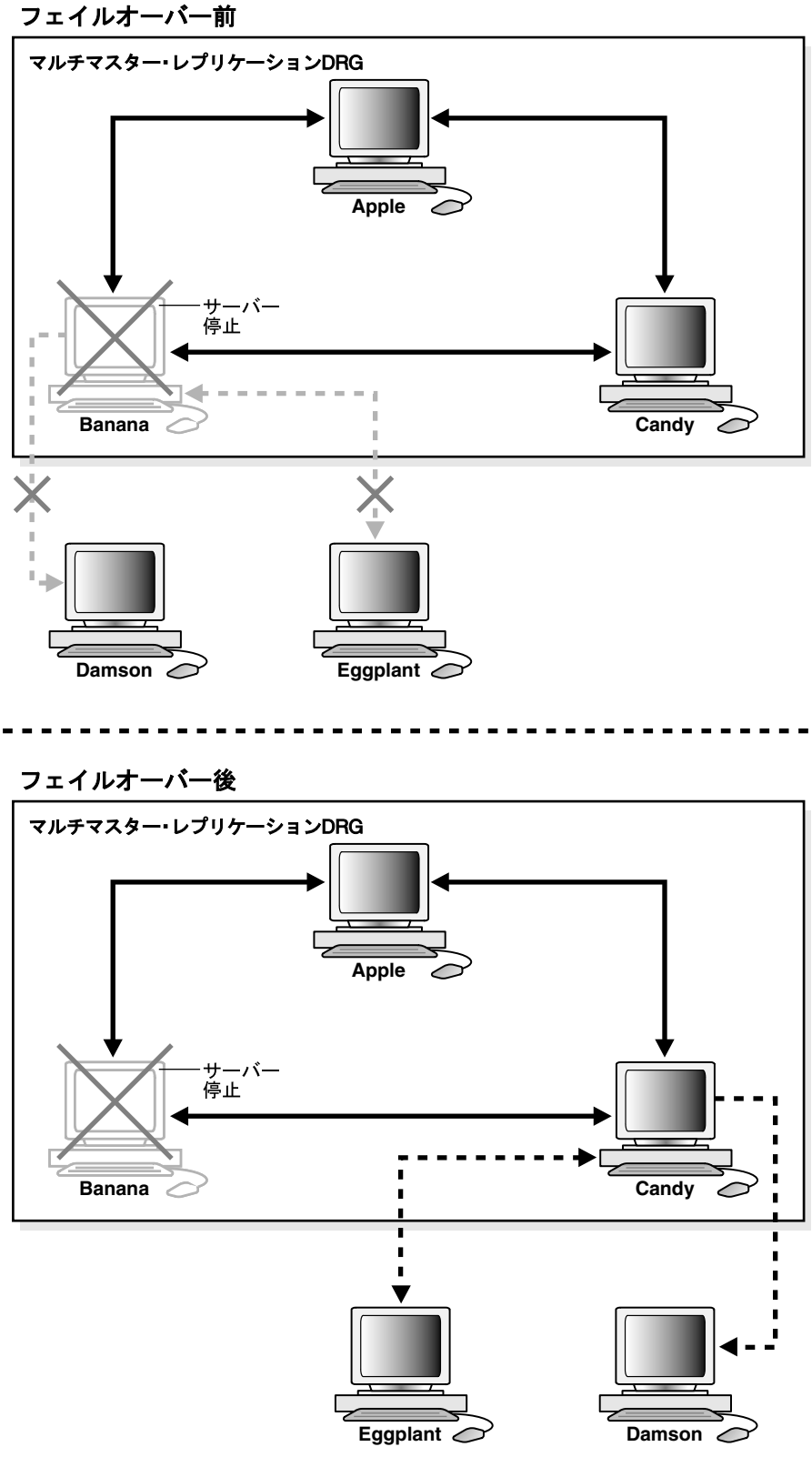
関連資料：

- マルチマスター・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は、付録 F「マルチマスター・レプリケーション・プロセス」を参照してください。
- スキーマについて不明な点がある場合は、『Oracle Identity Management ユーザー・リファレンス』の Oracle Identity Management LDAP スキーマのリファレンスに関する項を参照してください。
- カタログについて不明な点がある場合は、『Oracle Identity Management ユーザー・リファレンス』の `catalog` コマンドライン・ツールのリファレンスを参照してください。
- グループ・エントリについて不明な点がある場合は、『Oracle Identity Management 委任管理ガイド』のグループ・エントリの管理に関する項を参照してください。

レプリケーション・フェイルオーバー

10*g*（10.1.4.0.1）, Oracle Internet Directory では、1 つのサプライヤからもう 1 つのサプライヤへの LDAP レプリケーションのフェイルオーバーをサポートしています。管理者操作が必要です。図 29-11 は、一般的なフェイルオーバーの使用例を示しています。

図 29-11 レプリケーション・フェイルオーバーの使用例



この使用例には、次の機能があります。

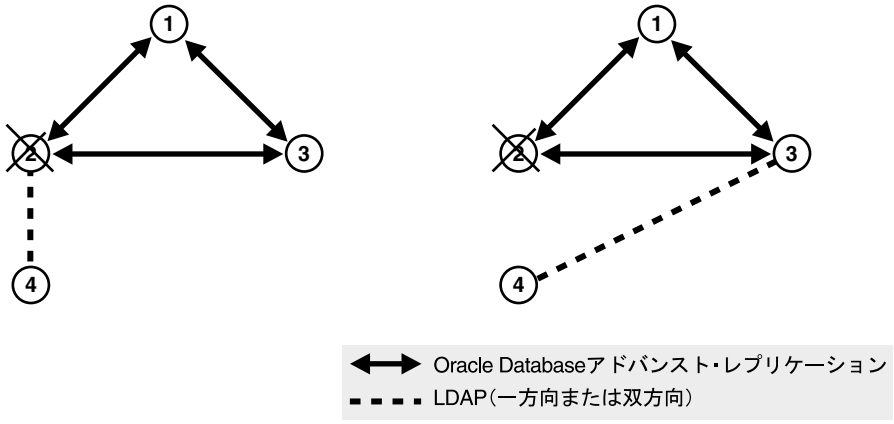
- Apple、Banana および Candy は、同じ DRG 内のマルチマスター・レプリカです。
- Damson は、Banana の読取り専用ファンアウト・レプリカです。つまり、一方向 LDAP レプリケーションを使用した部分レプリカです。
- Eggplant は、Banana の更新可能なファンアウト・レプリカです。つまり、双方向 LDAP レプリケーションを使用した部分レプリカです。
- Banana が停止すると、マルチマスター DRG とそのファンアウト・レプリカ間のレプリケーションは中断されます。

  管理者は、Eggplant と Damson を新しいサプライヤの Candy に切り替えることができます。

フェイルオーバー・トポロジは 2 つのタイプのみがサポートされています。

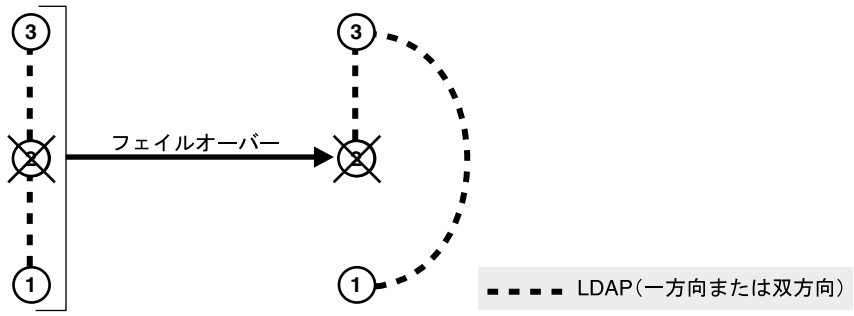
- コンシューマは、LDAP ベース承諾により旧サプライヤに接続され、旧サプライヤは同じアドバンスト・レプリケーション・グループ内で新規のサプライヤとして機能します。これは、図 29-12 に示されています。ノード 2 とノード 3 は、同じアドバンスト・レプリケーション DRG 内にあります。ノード 2 は、ノード 4 の元のサプライヤです。ノード 4 が機能しなくなると、ノード 4 を新規のサプライヤ、ノード 3 にフェイルオーバーできます。

図 29-12 同じアドバンスト・レプリケーション・グループ内の新旧のサプライヤ



- コンシューマと新規サプライヤは、どちらも LDAP ベース・レプリケーションにより旧サプライヤに接続されます。これは、図 29-13 に示されています。ノード 1 とノード 3 はどちらも、ノード 2 との LDAP レプリケーション承諾を持っています。ノード 2 は、ノード 1 の旧サプライヤです。ノード 2 が機能しなくなると、ノード 1 を新規のサプライヤ、ノード 3 にフェイルオーバーできます。

図 29-13 LDAP により旧サプライヤに接続されるコンシューマと新規サプライヤ



部分レプリケーションに含まれるネーミング・コンテキストと除外されるネーミング・コンテキスト

アドバンスト・レプリケーションで可能なのは、ネーミング・コンテキストの除外のみです。

LDAP ベースのレプリケーションでは、特定のネーミング・コンテキストをレプリケーションに追加し、そのネーミング・コンテキスト内の 1 つ以上のサブツリーをレプリケーションから除外できます。ネーミング・コンテキスト内の 1 つ以上の属性もレプリケーションから除外できます。

LDAP ベースのレプリケーションでは、レプリケーションに含むことを明示的に指定したネーミング・コンテキストのみがレプリケートされます。しかし、Oracle Database アドバンスト・レプリケーションの場合は、デフォルトですべてのネーミング・コンテキストが含まれます。

Oracle アドバンスト・レプリケーションでネーミング・コンテキストをレプリケーションから除外するには、Oracle アドバンスト・レプリケーション・ベースのレプリケーション承諾エントリ `orclagreementid=000001` の `orclexcludednamingcontext` 属性で除外ネーミング・コンテキストを指定します。

図 29-14 およびその後に続く説明では、ネーミング・コンテキスト・コンテナとそのオブジェクトの使用例を示します。

図 29-14 ネーミング・コンテキスト・コンテナおよびオブジェクトの例

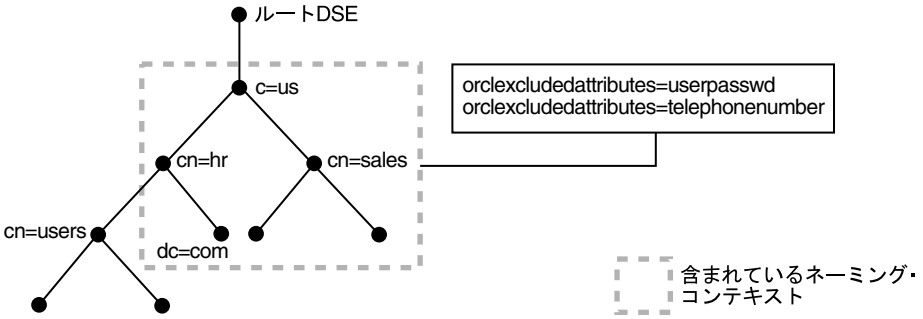


図 29-14 では、レプリケーションに含まれるネーミング・コンテキストは `c=us` です。このネーミング・コンテキスト内では、1 つのサブツリー（`cn=user1,cn=hr, c=us`）がレプリケーションから除外されています。さらに、ネーミング・コンテキスト `c=us` の `userPassword` および `telephonenumber` という 2 つの属性がレプリケーションから除外されています。

関連項目： 29-15 ページの「レプリケーションのネーミング・コンテキスト・オブジェクト・エントリ」

Oracle Database アドバンスト・レプリケーションのフィルタリング

この項では、Oracle Database アドバンスト・レプリケーションのフィルタリングの規則について説明します。

次のネーミング・コンテキストはレプリケートできません。

- DSE ルート固有のエントリ
- `orclagreementid=000001,cn=replication configuration`
- `cn=subconfigsubentry`
- `cn=Oracle Internet Directory`
- `cn=subregistrysubentry`

次のネーミング・コンテキストはレプリケーションから除外できません。

- `cn=catalogs`
- `cn=subschemasubentry`
- `cn=oracleschemaversion`
- `cn=replication configuration`

LDAP レプリケーションのフィルタリング

この項では、LDAP 部分レプリケーションでネーミング・コンテキストを指定する場合の規則および最良の方法について説明します。項目は次のとおりです。

- LDAP 部分レプリケーションのフィルタリングの規則
- LDAP レプリケーションのフィルタリングの例
- ネーミング・コンテキストおよび属性の管理規則
- 部分レプリケーションのネーミング・コンテキストの最適化によるパフォーマンスの向上

LDAP 部分レプリケーションのフィルタリングの規則

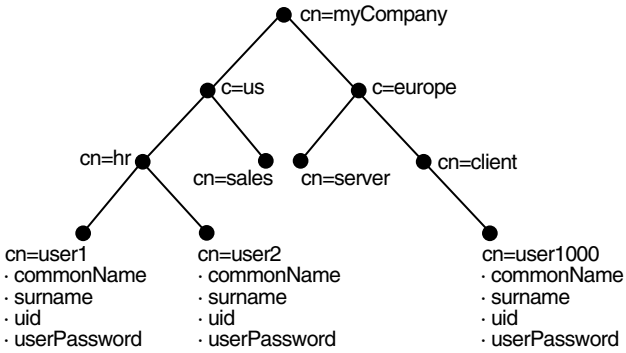
レプリケーションに対して複数のネーミング・コンテキストを構成する場合、フィルタリングは次の規則に基づいて行われます。

1. 各ネーミング・コンテキスト・オブジェクトで定義されて含まれているすべてのネーミング・コンテキストの集合が、レプリケーションに含まれる全体的なネーミング・コンテキストになります。
2. 各ネーミング・コンテキスト・オブジェクトで定義された除外ネーミング・コンテキストの集合が、レプリケーションから除外される全体的なネーミング・コンテキストになります。
3. 1 つのネーミング・コンテキスト・オブジェクトでの属性の除外は、そのネーミング・コンテキスト・オブジェクトのみに限定されます。
4. 包含されるネーミング・コンテキストと除外されるネーミング・コンテキストとの間で矛盾がある場合は、除外されるネーミング・コンテキストが優先されます。たとえば、ネーミング・コンテキスト・オブジェクト A の包含ネーミング・コンテキストが、別のネーミング・コンテキスト・オブジェクト B の除外ネーミング・コンテキストのサブツリーだった場合、ネーミング・コンテキスト・オブジェクト B の `orclexcludednamingcontexts` で指定されているサブツリーは、レプリケートされません。つまり、ネーミング・コンテキスト・オブジェクト A でのレプリケーションのフィルタリングは無視されます。

LDAP レプリケーションのフィルタリングの例

図 29-15 に示すネーミング・コンテキストのサンプルに基づいて説明します。cn=user1、cn=user2 および cn=user1000 の下には、ユーザー属性リストの一部が示されています。

図 29-15 ネーミング・コンテキストのサンプル



> **関連資料：** レプリケーションのネーミング・コンテキスト・エントリの属性の詳細は、『Oracle Identity Management ユーザー・リファレンス』のレプリケーションのスキーマ要素に関する項を参照してください。

前述の規則が実際にどのように働くかを次の例で説明します。

- 使用例 A: あるネーミング・コンテキスト・オブジェクトで、レプリケーションに含まれるネーミング・コンテキストが、別のネーミング・コンテキスト・オブジェクトで、レプリケーションに含まれるネーミング・コンテキストのサブツリーになっている
- 使用例 B: あるネーミング・コンテキスト・オブジェクトで、レプリケーションに含まれるネーミング・コンテキストが、別のネーミング・コンテキスト・オブジェクトで、レプリケーションから除外されるネーミング・コンテキストのサブツリーになっている
- ネーミング・コンテキストおよび属性の管理規則
- 部分レプリケーションのネーミング・コンテキストの最適化によるパフォーマンスの向上

使用例 A: あるネーミング・コンテキスト・オブジェクトで、レプリケーションに含まれるネーミング・コンテキストが、別のネーミング・コンテキスト・オブジェクトで、レプリケーションに含まれるネーミング・コンテキストのサブツリーになっている

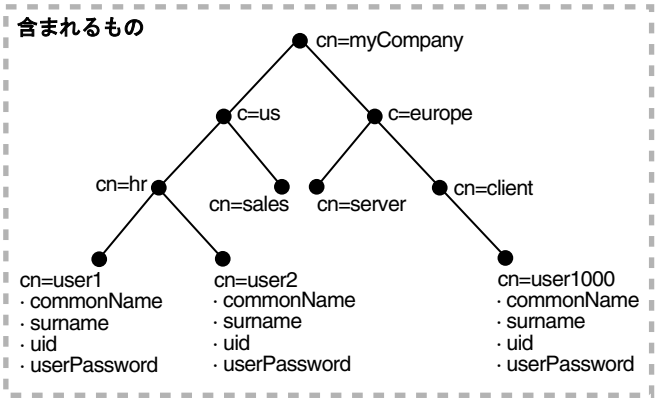
この例では、ネーミング・コンテキスト・オブジェクト 2 の包含ネーミング・コンテキストが、オブジェクト 1 の包含ネーミング・コンテキストのサブツリーになっているとします。

ネーミング・コンテキスト・オブジェクト 1

```
dn:cn=namectx001,
 cn=replication namecontext,
 orclagreementid=unique_identifier_of_the_replication_agreement,
 orclreplicaid=unique_identifier_of_the_supplier,
 cn=replication configuration
orclincludednamingcontexts: cn=mycompany
```

図 29-16 で示すように、ネーミング・コンテキスト・オブジェクト 1 には、cn=myCompany の下の DIT 全体が含まれます。

図 29-16 ネーミング・コンテキスト・オブジェクト 1

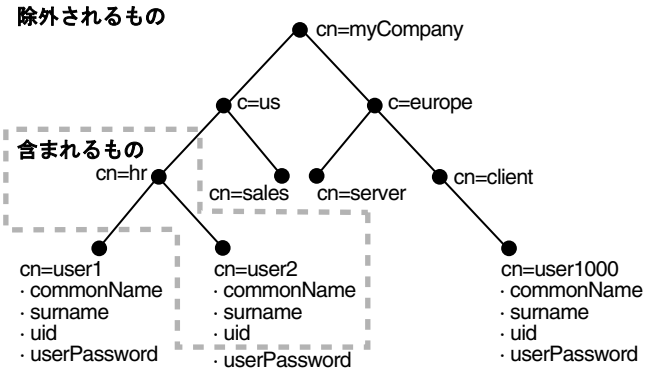


ネーミング・コンテキスト・オブジェクト 2

```
dn:cn=namectx002,
 cn=replication namecontext,
 orclagreementid=unique_identifier_of_the_replication_agreement,
 orclreplicaid=unique_identifier_of_the_supplier,
 cn=replication configuration
orclincludednamingcontexts: cn=hr,c=us,cn=mycompany
orclexcludednamingcontexts: cn=user1,cn=hr,c=us,cn=mycompany
orclexcludedattributes: userPassword
```

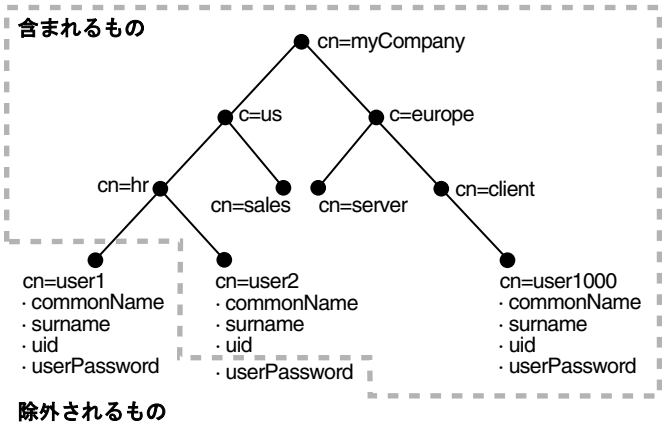
図 29-17 で示すように、ネーミング・コンテキスト・オブジェクト 2 には、cn=hr,c=us,cn=mycompany 以下の DIT が含まれますが、cn=user1 と属性 userPassword は除外されます。

図 29-17 ネーミング・コンテキスト・オブジェクト 2



ネーミング・コンテキスト・オブジェクトの 1 と 2 を組み合せた結果を、図 29-18 に示します。

図 29-18 ネーミング・コンテキスト・オブジェクト 1 および 2 を組み合せた結果



この使用例では、レプリケートされるネーミング・コンテキストは、orclincludednamingcontexts 属性で最上位に指定されたネーミング・コンテキストです。除外対象ネーミング・コンテキストはレプリケートされません。サブツリー cn=mycompany の下の変更がレプリケートされますが、cn=user1,cn=hr,c=us,cn=mycompany、および cn=hr,c=us,cn=mycompany の下にある属性 userPassword はレプリケーションから除外されます。ただし、他の DIT の下にある属性 userPassword は、レプリケーションから除外されません。これは、userPassword の除外はネーミング・コンテキスト・オブジェクト 2 に対してのみ指定されており、このオブジェクト 2 には、cn=hr の下の DIT しか含まれていないためです。

使用例 B: あるネーミング・コンテキスト・オブジェクトで、レプリケーションに含まれるネーミング・コンテキストが、別のネーミング・コンテキスト・オブジェクトで、レプリケーションから除外されるネーミング・コンテキストのサブツリーになっている

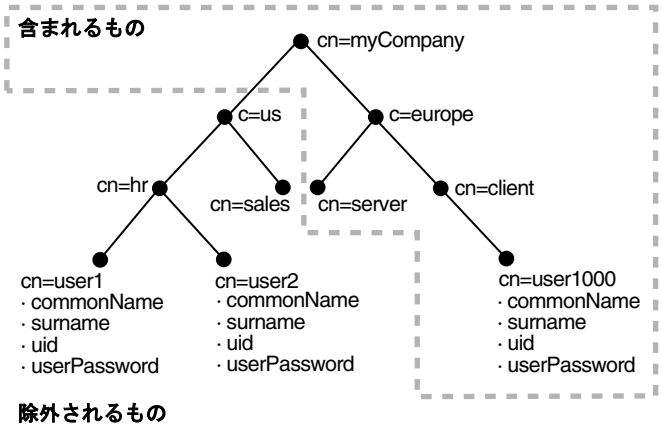
この例では、ネーミング・コンテキスト・オブジェクト 4 の除外ネーミング・コンテキストが、オブジェクト 3 で定義されている除外ネーミング・コンテキストのサブツリーになっているとします。

ネーミング・コンテキスト・オブジェクト 3

```
dn:cn=namectx001,cn=replication namecontext,
 orclagreementid=identifier,orclreplicaid=supplier,cn=replication configuration
orclincludednamingcontexts: cn=mycompany
orclexcludednamingcontexts: c=us,cn=mycompany
```

図 29-19 に示すように、ネーミング・コンテキスト・オブジェクト 3 では、c=us,cn=mycompany の下にあるすべてのものが除外されます。

図 29-19 ネーミング・コンテキスト・オブジェクト 3

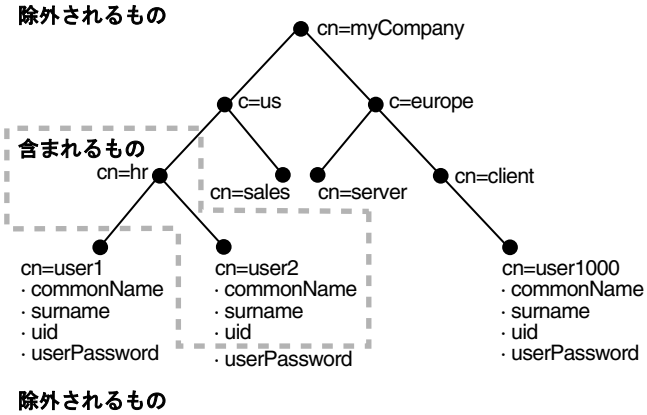


ネーミング・コンテキスト・オブジェクト 4

```
dn:cn=namectx002,cn=replication
 namecontext,orclagreementid=identifier,orclreplicaid=supplier,
 cn=replication configuration
orclincludednamingcontexts: cn=hr, c=us,cn=mycompany
orclexcludednamingcontexts: cn=user1,cn=hr,c=us,cn=mycompany
orclexcludedattributes: userPassword
```

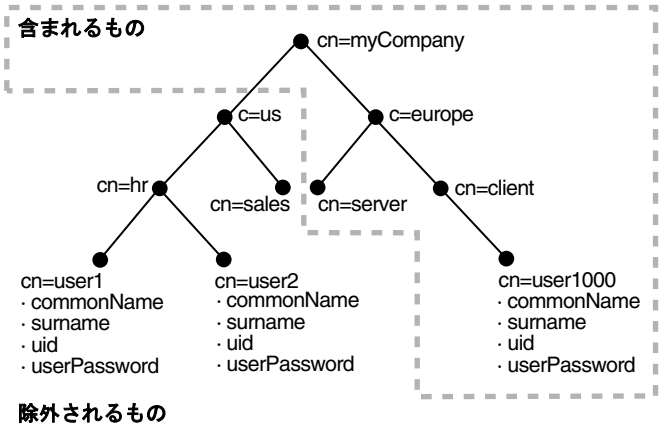
図 29-20 で示すように、ネーミング・コンテキスト・オブジェクト 4 には、cn=hr,c=us,cn=mycompany 以下の DIT が含まれますが、user1、および全ユーザーの userPassword 属性は除外されています。

図 29-20 ネーミング・コンテキスト・オブジェクト 4



ネーミング・コンテキスト・オブジェクトの 3 と 4 を組み合せた結果を、図 29-21 に示します。

図 29-21 ネーミング・コンテキスト・オブジェクト 3 および 4 を組み合せた結果



この使用例では、ネーミング・コンテキスト・オブジェクト 4 に指定した、レプリケーションに含まれるネーミング・コンテキストはレプリケートされません。このネーミング・コンテキストは、ネーミング・コンテキスト・オブジェクト 3 で指定された除外ネーミング・コンテキストのサブツリーです。その場合、ネーミング・コンテキスト・オブジェクト 4 は無視され、`cn=hr,c=us,cn=mycompany` の下の変更はレプリケートされません。

ネーミング・コンテキストおよび属性の管理規則

次のネーミング・コンテキストはレプリケートできません。

- DSE ルート固有のエントリ
- `orclagreementid=000001,cn=replication configuration`
- `cn=subconfigsubentry`
- `cn=Oracle Internet Directory`
- `cn=subregistrysubentry`

次のネーミング・コンテキストはレプリケーションから除外できません。

- `cn=catalogs`
- `cn=subschemasubentry`
- `cn=oracleschemaversion`
- `cn=replication configuration`

次の属性は、必須またはオプションに関係なく、レプリケーションから除外できません。これらの属性をレプリケーションから除外するように指定しても、常にレプリケートされます。

- `orclguid`
- `creatorsname`
- `createtimestamp`
- `cn`
- `dn`
- `attributetypes`
- `objectclasses`
- `objectclass`

- orclindexedattribute
- orclproductversion

必須属性は、レプリケーションから除外できません。たとえば、my_object_class というオブジェクト・クラスがあるとします。これには、mandatory_attribute_1、optional_attribute_1 および optional_attribute_2 属性が含まれています。この場合、レプリケーションから mandatory_attribute_1 を除外できません。

LDAP 操作の実行に必要な属性をレプリケーションから除外するように指定した場合、レプリケーションは行われません。

Oracle Internet Directory ノードの特定のネーミング・コンテキストからファンアウト・レプリケーション・ノードへの部分レプリケーションを構成する場合は、レプリケーション元ノードでネーミング・コンテキスト・エントリの名前を変更しないでください。

部分レプリケーションの場合、ldapmoddn を使用して作成したネーミング・コンテキストのルート・エントリには変更がレプリケートされません。

部分レプリケーションのネーミング・コンテキストの最適化によるパフォーマンスの向上

部分レプリケーションは慎重に計画して、レプリケーション・プロセスのパフォーマンスを低下させないようにする必要があります。最高のパフォーマンスを得るには、使用するネーミング・コンテキスト・オブジェクトの数をできるだけ少なくします。たとえば、ネーミング・コンテキスト・オブジェクトの 5 と 6 を組み合せる場合も、ネーミング・コンテキスト・オブジェクト 7 を使用する場合も、実行される条件は同じですが、パフォーマンスは、ネーミング・コンテキスト・オブジェクト 7 を使用する方がよくなります。

この項では、次の例について説明します。

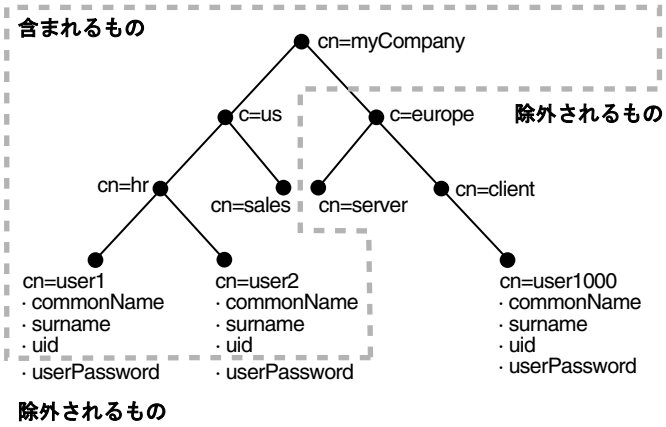
- ネーミング・コンテキスト・オブジェクト 5
- ネーミング・コンテキスト・オブジェクト 6
- ネーミング・コンテキスト・オブジェクト 7

ネーミング・コンテキスト・オブジェクト 5

```
cn=namectx001,cn=replication
namecontext,orclagreementid=identifier,orclreplicaid=supplier,cn=replication
configuration
orclincludednamingcontexts: cn=mycompany
orclexcludednamingcontexts: c=europe,cn=mycompany
orclexcludedattributes: userPassword
```

ネーミング・コンテキスト・オブジェクト 5 は図 29-22 のようになっています。このオブジェクトには、cn=mycompany の下の DIT が含まれていますが、c=europe の下のものはすべて除外されています。また、属性 userPassword も除外されています。

図 29-22 ネーミング・コンテキスト・オブジェクト 5

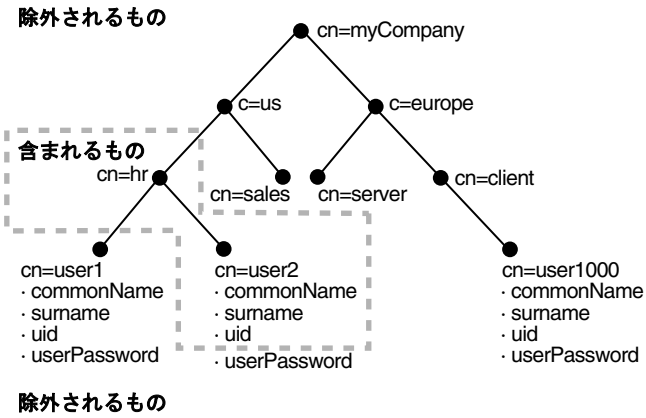


ネーミング・コンテキスト・オブジェクト 6

```
cn=namectx002,cn=replication
namecontext,orclagreementid=<id>,orclreplicaid=<supplier>,cn=replication configuration
orclincludednamingcontexts: cn=hr, c=us,cn=mycompany
orclexcludednamingcontexts: cn=user1,cn=hr, c=us,cn=mycompany
orclexcludedattributes: userPassword
```

ネーミング・コンテキスト・オブジェクト 6 は図 29-23 のようになっています。このオブジェクトには、cn=hr, c=us, cn=mycompany の下の DIT が含まれていますが、user1 と属性 userPassword は除外されています。

図 29-23 ネーミング・コンテキスト・オブジェクト 6



ネーミング・コンテキスト・オブジェクトの 5 と 6 を組み合せた場合は、cn=europe,c=mycompany、cn=user1,cn=hr,c=us,cn=mycompany、および属性 userPassword を除いて、cn=mycompany の下の変更がすべてレプリケートされます。

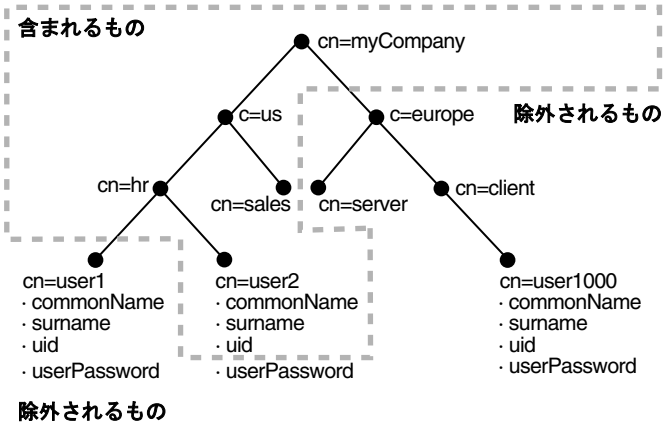
ただし、同じ条件はネーミング・コンテキスト・オブジェクト 7 でも実現できます。使用するネーミング・コンテキスト・オブジェクトが 1 つのみの場合、部分レプリケーションのパフォーマンスが向上します。

ネーミング・コンテキスト・オブジェクト 7

```
cn=namectx001,cn=replication
namecontext,orclagreementid=identifier,orclreplicaid=supplier,cn=replication
configuration
orclincludednamingcontexts: cn=mycompany
orclexcludednamingcontexts: c=europe,cn=mycompany
orclexcludednamingcontexts: cn=user1,cn=hr, c=us,cn=mycompany
orclexcludedattributes: userPassword
```

ネーミング・コンテキスト・オブジェクト 7 は図 29-24 のようになっています。

図 29-24 ネーミング・コンテキスト・オブジェクト 7



30

Oracle Internet Directory 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および構成方法を説明します。

10*g*（10.1.4.0.1）では、レプリケーションのインストールに 4 つのタイプがあります。これには次のようなものがあります。

- Oracle Internet Directory をマスターとしてインストール
- Oracle Internet Directory をアドバンスト・レプリケーション・ベースのレプリカとしてインストール
- Oracle Internet Directory を一方向 LDAP ベースのレプリカとしてインストール
- Oracle Internet Directory を双方向 LDAP ベースのレプリカとしてインストール

3 タイプのレプリカのインストール手順は非常に似ているため、これらは 1 項目にまとめて説明します。いくつかの相違については、手順の中で指摘しています。

この章の項目は次のとおりです。

Oracle Internet Directory のリリースとレプリケーション

マルチマスター・レプリケーションまたは双方向ファンアウト・レプリケーションのいずれも、レプリケーション・グループ内に 10*g*（10.1.4.0.1）を実行しているノードがある場合、すべてのノードで 10*g*（10.1.4.0.1）を実行する必要があります。

一方向ファンアウト配置では、10*g*（10.1.4.0.1）コンシューマのサプライヤは、10*g* リリース 3（10.1.2.0.2）を実行することができます。これは、LDAP ベース・レプリケーションまたはアドバンスト・レプリケーション・ベース・レプリケーションのいずれのサプライヤにも当てはまります。

レプリケーション・グループをインストールし構成するための前提情報

この項では、レプリケーション・グループの構成を実行するために必要なインストールのタイプを説明します。また、様々な構成タスクを実行できるレプリケーション環境管理ツールについても説明します。

この項の項目は次のとおりです。

- Oracle Internet Directory のインストール
- Oracle Internet Directory をマスターとしてインストールする場合
- Oracle Internet Directory をアドバンスト・レプリケーション・ベースのレプリカ、あるいは一方向または双方向の LDAP ベースのレプリカとしてインストールする場合
- レプリケーション環境管理ツール

Oracle Internet Directory のインストール

任意のノードに Oracle Internet Directory を Oracle Application Server の一部としてインストールすると、製品を選択するように要求されます。この場合、「Oracle Application Server Infrastructure」を選択します。

後のインストール・プロセスで、インストール・タイプを選択するように要求されます。

- マルチマスター・レプリケーションを実行するには、マスター定義サイト（MDS）が 1 つだけ必要です。その場合は、30-3 ページの「Oracle Internet Directory をマスターとしてインストールする場合」の指示に従ってください。
- その他のサイトはすべてレプリカであり、アドバンスト・レプリケーション・ベースのレプリカと LDAP レプリカのいずれかです。
  - **Oracle Database アドバンスト・レプリケーション・ベースのレプリカ**は、本当の意味でのマルチマスター・レプリケーションを実行します。つまり、マスターに加えられた変更はレプリカにレプリケートされ、レプリカに加えられた変更はマスターとその他すべてのレプリカにレプリケートされます。

    アドバンスト・レプリケーション・ベースのレプリカとして使用されるサイトを最初にマスターとしてインストールすることも可能ですが、この方法はお薦めしません。目的の各レプリカを最初からレプリカとしてインストールする方法をお薦めします。

    したがって、アドバンスト・レプリケーション・ベースのレプリカを作成する場合は、30-4 ページの「Oracle Internet Directory をアドバンスト・レプリケーション・ベースのレプリカ、あるいは一方向または双方向の LDAP ベースのレプリカとしてインストールする場合」の指示に従い、「アドバンスト・レプリケーション」オプションが表示されたらそれを選択します。

- **LDAP レプリカ**は、一方向または双方向のいずれかです。
  - **一方向 LDAP レプリカ**は読取り専用です。マスターに対して加えられた変更のみが、レプリカにレプリケートされます。レプリカからマスターへのレプリケーションはありません。

    一方向 LDAP レプリカを作成する場合は、30-4 ページの「Oracle Internet Directory をアドバンスト・レプリケーション・ベースのレプリカ、あるいは一方向または双方向の LDAP ベースのレプリカとしてインストールする場合」の指示に従い、「一方向 LDAP レプリケーション」オプションが表示されたらそれを選択します。
  - **双方向 LDAP レプリカ**は、双方向に更新可能です。一方のレプリカに対して加えられた変更が他方のレプリカにレプリケートされます。

    双方向 LDAP レプリカを作成する場合は、30-4 ページの「Oracle Internet Directory をアドバンスト・レプリケーション・ベースのレプリカ、あるいは一方向または双方向の LDAP ベースのレプリカとしてインストールする場合」の指示に従い、「双方向 LDAP レプリケーション」オプションが表示されたらそれを選択します。

  LDAP レプリカは、ディレクトリ情報ツリーの全体ではなく、一部をレプリケートする場合にも使用できます。部分レプリケーションでは、レプリカのネーミング・コンテキスト・オブジェクトを定義することにより、レプリケートするものとしないものを決めます。これは、一方向レプリカと双方向レプリカのどちらにもできます。

  関連項目： この章の後の項で示すネーミング・コンテキストの設定および使用方法の詳細と例を参照してください。

Oracle Internet Directory をマスターとしてインストールする場合

1. Oracle Application Server のインストレーション・ガイドの「レプリケーション・モードでの Oracle Internet Directory のインストール」に記載されているインストール手順に従います。インストールする製品を選択するよう求められたら、「Oracle Application Server Infrastructure」を選択します。
2. インストール・タイプについては、次のように選択します。
   a. 既存の Oracle Application Server Metadata Repository がない（または既存の Oracle Application Server Metadata Repository を使用しない）場合は、「**Identity Management and Oracle Application Server Metadata Repository**」選択します。
   b. 既存の Oracle Application Server Metadata Repository を使用する場合、「**Identity Management**」を選択します。
3. 「**構成オプションの選択**」画面で「**Oracle Internet Directory**」が選択されていることを確認します。
4. マスターのインストール時には、レプリケーションの「**構成オプションの選択**」画面で「**高可用性およびレプリケーション**」を選択しないでください。「**高可用性およびレプリケーション**」を選択しない場合、デフォルトの Oracle Internet Directory インストールが実行されます。つまり、新しい Oracle Internet Directory がマスター・ノードとしてインストールされます。（ただし、**仮想ホスト**または **OracleAS クラスタ**を構成する際には、「**構成オプションの選択**」画面で「**高可用性およびレプリケーション**」を選択してもかまいません。）
5. Oracle Application Server のインストレーション・ガイドの「レプリケーション・モードでの Oracle Internet Directory のインストール」で説明されているとおりにインストールを完了します。

Oracle Internet Directory をアドバンスト・レプリケーション・ベースのレプリカ、あるいは一方向または双方向の LDAP ベースのレプリカとしてインストールする場合

1. Oracle Application Server のインストレーション・ガイドの「レプリケーション・モードでの Oracle Internet Directory のインストール」に記載されているインストール手順に従います。インストールする製品を選択するよう求められたら、「Oracle Application Server Infrastructure」を選択します。
2. インストール・タイプについては、次のように選択します。
   a. 既存の Oracle Application Server Metadata Repository がない（または既存の Oracle Application Server Metadata Repository を使用しない）場合、「**Identity Management and Oracle Application Server Metadata Repository**」を選択します。
   b. 既存の Oracle Application Server Metadata Repository を使用する場合、「**Identity Management**」を選択します。
3. 構成オプションについては、「**Oracle Internet Directory**」と「**高可用性およびレプリケーション**」の両方が選択されていることを確認します。
4. 「**構成オプションの選択**」画面で「**高可用性およびレプリケーション**」を選択したため、「**高可用性またはレプリケーション・オプションの選択**」画面が表示されます。「**レプリケーション**」を選択します。
5. 次に、「**Oracle Internet Directory レプリケーション・モード**」画面が表示されます。作成するレプリカのタイプを選択します。
   - アドバンスト・レプリケーション・ベースの（マルチマスター）レプリケーションの場合、「**アドバンスト・レプリケーション**」を選択します。
   - 一方向（読取り専用）LDAP レプリカの場合、**一方向 LDAP レプリカ**を選択します。
   - 双方向（読取り / 書込み可能）LDAP レプリカの場合、**双方向 LDAP レプリカ**を選択します。
6. 「**Oracle Internet Directory マスター・ノード**」画面で、この現在作成中のノードによってレプリケートされるサプライヤ・ノードのホスト名およびポートを指定します。そのノードとの接続に SSL プロトコルが必要な場合は、この画面で対応するボックスを選択します。
7. Oracle Application Server のインストレーション・ガイドで説明されているとおりにインストールを完了します。

レプリケーション環境管理ツール

インストールおよび構成時、様々なタスクの実行にレプリケーション環境管理ツールを使用します。このツールは、次のタスクを支援します。

- レプリケーション・グループの構成
- レプリカの追加および削除
- ディレクトリ・レプリケーション・グループの管理
- レプリケーション・バインド識別名パスワードの変更または再設定
- データベース・レプリケーション・ユーザー REPADMIN パスワードの変更
- 変更ログの伝播に関する様々なエラーおよびステータス情報の表示

注意： 部分レプリケーション（LDAP ベースのレプリケーション）を実行するのに、アドバンスト・レプリケーションは不要です。

ディレクトリ・レプリケーション・グループのノードによって Oracle Database 10*g* のパッチ・セットのリリースが異なる場合でも、ノードにある Oracle Internet Directory のリリースと同じであれば、レプリケートを実行できます。

ただし、ディレクトリ・レプリケーション・グループのノードで稼働している Oracle Internet Directory のバージョンが異なる場合は、それらのノードでのディレクトリ・サーバーの変更には制約が課せられます。新しいリリースの Oracle Internet Directory で加えられた変更を、そのリリースへのアップグレードが行われていないノードにレプリケートしないでください。レプリケートすると、旧リリースでは正しく解析されない情報が変更内容に含まれてしまいます。

関連資料： レプリケーション環境管理ツールの詳細は、『Oracle Identity Management ユーザー・リファレンス』の `remtool` コマンドライン・ツールのリファレンスを参照してください。

マルチマスター・レプリケーションのインストールと構成

この項では、マルチマスター・レプリケーション・グループのインストールと構成の方法、およびそのグループでの競合を手動で解決する方法について説明します。この項の項目は次のとおりです。

- Oracle Database アドバンスト・レプリケーション・ベースのディレクトリ・レプリケーションの構成に関する規則
- マルチマスター・レプリケーション・グループのインストールと構成
- マルチマスター・レプリケーション用のノードの追加（Oracle Database アドバンスト・レプリケーション・タイプのみ）
- マルチマスター・レプリケーション・グループからのノードの削除

関連資料：

- Oracle Application Server のインストレーション・ガイドの「レプリケーション・モードでの Oracle Internet Directory のインストール」
- 『Oracle Application Server 高可用性ガイド』のマルチマスター・レプリケーションに関する章

Oracle Database アドバンスト・レプリケーション・ベースのディレクトリ・レプリケーションの構成に関する規則

次の 9 つの規則は、アドバンスト・レプリケーション（ASR とも呼ばれます）・ベースのレプリケーションに適用されます。

1. このタイプのディレクトリ・レプリケーション・グループ（DRG）には、マスター定義サイト（MDS）とみなされるノードが 1 つ必要です。これがグループ・マスターとなります。レプリケーションに関与するその他のノードはすべてレプリカです。これは、データベース・レプリケーションにおけるリモート・マスター・サイト（RMS）と呼ばれます。MDS は、レプリカ（アドバンスト・レプリケーション・ベースのレプリカや LDAP ベースのレプリカ）としてではなく、マスター・ノードとして作成する必要があります。

   注意： アドバンスト・レプリケーション・ベースのレプリカは、中央のマスターでなくても、次の 2 つの理由でリモート・マスター・サイト（RMS）と呼ばれることがあります。第 1 に、アドバンスト・レプリケーションでは、情報がサイト間を移動する場合に、転送された情報の受信側はリモート・マスター・サイトと呼ばれます。第 2 に、アドバンスト・レプリケーション・ベースのレプリカに直接加えられた個々の変更は、グループのすべてのメンバーにもレプリケートされるため、レプリケート処理中にはそのレプリカがマスターになります。あるメンバーへの変更がその他すべてのメンバーにレプリケートされるようなグループは、マルチマスター・レプリケーション・グループと呼ばれます。

   関連項目：

   - 新規マスター・ノードの作成方法は、30-3 ページの「Oracle Internet Directory をマスターとしてインストールする場合」を参照してください。
   - 新規レプリカ・ノードの作成方法は、30-4 ページの「Oracle Internet Directory をアドバンスト・レプリケーション・ベースのレプリカ、あるいは一方向または双方向の LDAP ベースのレプリカとしてインストールする場合」を参照してください。

2. マルチマスター・レプリケーションのインストールと構成を行う場合、ディレクトリ・レプリケーション・グループ（DRG）のマスター・ノードとアドバンスト・レプリケーション・ベースのレプリカになる各ノードが最初は空であることが必要です。つまり、Oracle Internet Directory を新たにインストールする必要があります。

   注意： マスター・ノードが新たにインストールしたものではない場合は、30-14 ページの「マルチマスター・レプリケーション用のノードの追加（Oracle Database アドバンスト・レプリケーション・タイプのみ）」で説明する手順に従って、レプリカを追加します。この手順では、レプリケーション・グループの初期化も行います。

   ---

3. Oracle Database アドバンスト・レプリケーション・ベースのレプリカを追加する場合、新規レプリカが空であることが必要です。つまり、Oracle Internet Directory を新たにインストールする必要があります。
4. アドバンスト・レプリケーション・ベースの各レプリカのスポンサ・ノードは、次のいずれかです。
   - マスター・ノード
   - 既存のマルチマスター DRG のアドバンスト・レプリケーション・ベースのレプリカ
   - LDAP レプリカ（その他の LDAP レプリカのコンシューマ LDAP レプリカではない）のサプライヤ

5. LDAP レプリカのコンシューマをアドバンスト・レプリケーション・ベースのレプリカにすることはできません。
6. Oracle Internet Directory 10*g*（10.1.4.0.1）では、1 つのノードを複数のマルチマスター・レプリケーション・グループの一部にすることはできません。
7. 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。

   関連項目： 29-31 ページの「Oracle Database アドバンスト・レプリケーションのフィルタリング」

8. マルチマスター・レプリケーション・グループを構成すると、Oracle Application Server Single Sign-On データベース・スキーマが自動的にレプリケーション内に構成されます。
9. DRG にノードを追加する場合、そのノードは、DRG 内の他のノードと同じリリースの Oracle Internet Directory を実行している必要があります。新規の 10*g*（10.1.4.0.1）ノードを、旧リリースのノードを含む DRG に追加する場合、まず既存のノードすべてを 10*g*（10.1.4.0.1）にアップグレードします。

マルチマスター・レプリケーション・グループのインストールと構成

この項では、マルチマスター・レプリケーション・グループをインストールおよび構成する際に実行する一般的なタスクを説明します。この項の項目は次のとおりです。

30-8 ページの「タスク 1: マスター定義サイト（MDS）へのマスターとしての Oracle Internet Directory のインストール」

30-8 ページの「タスク 2: リモート・マスター・サイト（RMS）へのレプリカとしての Oracle Internet Directory のインストール」

30-9 ページの「タスク 3: ディレクトリ・レプリケーション・グループ用の Oracle Database アドバンスト・レプリケーションの設定」

30-12 ページの「タスク 4（オプション）: ディレクトリへのデータのロード」

30-13 ページの「タスク 5: 全ノードで Oracle ディレクトリ・サーバー・インスタンスが起動していることの確認」

30-13 ページの「タスク 6: DRG の全ノードでのレプリケーション・サーバーの起動」

30-14 ページの「タスク 7: ディレクトリ・レプリケーションのテスト」

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、30-14 ページの「マルチマスター・レプリケーション用のノードの追加（Oracle Database アドバンスト・レプリケーション・タイプのみ）」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、識別名の文字の大文字と小文字の区別が保持されない場合があります。

タスク 1: マスター定義サイト（MDS）へのマスターとしての Oracle Internet Directory のインストール

Oracle Net Services を使用して、マスター定義サイトのデータベースおよび DRG 内の他のすべてのノードに接続できる必要があります。

注意： インストール時に、各 Oracle Internet Directory のデータベース・インスタンス名が各マシンで一意であることを確認してください。

マスターとしての実際のインストール方法は、30-3 ページの「Oracle Internet Directory をマスターとしてインストールする場合」の指示に従ってください。

関連資料： Oracle Application Server のインストレーション・ガイドの「レプリケーション・モードでの Oracle Internet Directory のインストール」

タスク 2: リモート・マスター・サイト（RMS）へのレプリカとしての Oracle Internet Directory のインストール

アドバンスト・レプリケーション・ベースのレプリカとして使用されるサイトは、最初からマスターとしてではなくレプリカとしてインストールすることをお薦めします。

レプリカとしての実際のインストール方法は、30-4 ページの「Oracle Internet Directory をアドバンスト・レプリケーション・ベースのレプリカ、あるいは一方向または双方向の LDAP ベースのレプリカとしてインストールする場合」の指示に従ってください。

既存のマスターをリモート・マスター・サイトとして使用する場合 レプリカは空の状態から始めることをお薦めしていますが、最初にレプリカではなくマスターとして構成されたマシンを使用してレプリケーションを設定することも可能です。最初にマスター（RMS）として構成されたマシンを使用する場合は、次のように、まずメタデータを MDS に移行する必要があります。

- プロセス（remtool –backupmetadata）が正しく機能するように、Oracle Internet Directory サーバーが MDS および対象となる各レプリカで稼働していることを確認します。
- 新たに作成したノードから、次のコマンドを実行します。

```
remtool -backupmetadata  \
   -replica "new_node_host:new_node_port/new_node_repldn_pwd" \
   -master "master_host:master_port/master_repl_dn_pwd"
```

master_host:master_port/master_repdn_pwd は、対象となるレプリカのサプライヤのホスト名、ポート番号およびレプリケーション識別名パスワードです。

注意： Oracle Delegated Administration Services が構成されていない場合、`remtool` を `-backupmetadata` オプションを指定して実行すると、次のようなエラー・メッセージが表示されます。

```
Failed to add "orclApplicationCommonName=ias.acme.com,
cn=IAS Instances, cn=IAS, cn=Products, cn=OracleContext"
as "uniquemember" to entry "cn=Associated Mid-tiers,
orclapplicationcommonname=DASApp, cn=DAS,cn=products,
cn=OracleContext at replica ldap://myhost:389
```

このエラー・メッセージは無視してください。

- このツールは、メタデータをマスター・レプリカにロードする以外に、メタデータのバックアップを含む *ocbkup.new_replica_id.TO.master_replicaid.timestamp*.dat という名前のファイルを作成します。このファイルは $ORACLE_HOME/ldap/log ディレクトリに作成されます。このファイルには、LDIF 形式でのマスター・レプリカの変更と、SSO のコンテナ・エントリ [orclApplicationCommonName=ORASSO_SSOSERVER, cn=SSO, cn=Products, cn=OracleContext] および DAS の URL コンテナ・エントリ [cn=OperationURLs, cn=DAS, cn=Products, cn=OracleContext] のコピーが格納されます。
- メタデータのバックアップに成功すると、端末に次のメッセージ表示されます。

  ```
  Backup of metadata will be stored in
  $ORACLE_HOME/ldap/log/ocbkup.new_replica_id.TO.master_replica_id.timestamp.dat.
  Metadata copied successfully.
  ```

  メッセージには、ORACLE_HOME の実際のパスが含まれます。
- この操作を行っている間にエラーが発生した場合、remtool を起動した端末にエラーが表示されます。エラー・メッセージは、$ORACLE_HOME/ldap/log/remtool.log ファイルにも記録されます。

マスターのメタデータを MDS に正しく移行できたら、次は、30-9 ページの「タスク 3: ディレクトリ・レプリケーション・グループ用の Oracle Database アドバンスト・レプリケーションの設定」に進みます。

タスク 3: ディレクトリ・レプリケーション・グループ用の Oracle Database アドバンスト・レプリケーションの設定

次の各項では、レプリケーション管理ツールを使用してアドバンスト・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。

> **関連資料：** Oracle Database アドバンスト・レプリケーションの構成方法は、Oracle Database ドキュメント・ライブラリの『Oracle Database アドバンスト・レプリケーション』、およびレプリケーション管理ツールのオンライン・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）を設定するには、次のタスクを実行してアドバンスト・レプリケーション環境を構成する必要があります。

- 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 Oracle Database アドバンスト・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 ディレクトリ・レプリケーション・グループの各ノードについて、ここに示す手順を実行します。（各手順の詳細は、このリストに続く項を参照してください。）

1. sqlnet.ora を構成します。
2. tnsnames.ora を構成します。
3. リスナーを停止して、再起動します。
4. 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 = global_database_domain
   ```

   UNIX では、sqlnet.ora ファイルは $ORACLE_HOME/network/admin にあります。

Microsoft Windows では、sqlnet.ora ファイルは *%ORACLE_HOME%*¥network¥admin にあります。

2. tnsnames.ora を構成します。

DRG の各ノードで、DRG のすべての Oracle Internet Directory データベース・インスタンスを定義します。各 tnsnames.ora ファイルには、それぞれの Oracle Internet Directory データベースについて、接続記述子情報が次の形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 = port_no_of_listener))
(CONNECT_DATA =
(service_name = service_name_of_database)))
```

net_service_name はデータベースのグローバル名です。たとえば、データベースのグローバル名が mds.sales.com の場合、*net_service_name* は mds.sales.com でなければなりません。データベースのグローバル名および net_service_name がドメイン修飾されていることを確認してください。この例の場合、グローバル名と net_service_name は sales.com でドメイン修飾されています。

注意：

- データベースのグローバル名は、データベースの初期化パラメータ DB_NAME と DB_DOMAIN で構成されます。たとえば、データベースの DB_NAME が mds で、DB_DOMAIN が sales.com である場合、そのデータベースのグローバル名は mds.sales.com になります。DB_DOMAIN 初期化パラメータを指定しない場合は、グローバル名がドメイン修飾されません。
- sqlnet.ora ファイルの NAMES.DEFAULT_DOMAIN パラメータの値は、データベースの DB_DOMAIN 初期化パラメータの値と一致している必要があります。

関連資料： tnsnames.ora 構文の詳細は、『Oracle Database Net Services リファレンス』を参照してください。

UNIX では、tnsnames.ora ファイルは $ORACLE_HOME/network/admin にあります。

Microsoft Windows では、tnsnames.ora 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. 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]

quit
```

4. 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。

   重要 : 次の 2 つのコマンドを使用して接続を試みます。

   ```
   sqlplus ods/ods_password@net_service_name_without_domain_name
   sqlplus ods/ods_password@net_service_name_with_domain_name
   ```

   接続できない場合、レプリケーションは行われません。

MDS でのディレクトリ・レプリケーション用の Oracle Database アドバンスト・レプリケーションの構成 これは、次の手順に従って行います。

1. MDS コンソールから、システム・ユーザーとしてすべてのノード（MDS を含む）に接続します。すべてのノードで、次のことを確認してください。
   - Oracle Internet Directory データベースが実行中であること
   - Oracle Internet Directory リスナーが実行中であること
   - 接続文字列が正しいこと
   - システム・パスワードが正しいこと
2. 次の Wallet がリモート・サイトに存在することを確認してください。
   - Oracle Internet Directory に指定されたデータベースにパスワードを保存するための Wallet。この Wallet は、`oidpwdlldap1` という名前で、ディレクトリ `$ORACLE_HOME/ldap/admin` にあります。
   - レプリケーション管理者のパスワードを保存するための Wallet。この Wallet は、`oidpwdr`*`oracle_sid`* という名前で、ディレクトリ `$ORACLE_HOME/ldap/admin` にあります。（*`oracle_sid`* は環境変数 SID からではなく、接続データベースから取得されます。）

   Wallet が特定のサイトに存在しない場合は、リモート・ノードで次のコマンドを入力して作成します。

   ```
   oidpasswd connect=connect_string create_wallet=true
   ```

3. 次の「注意」の前提条件を確認します。その後、MDS のコマンド・プロンプトで remtool（レプリケーション環境管理ツール）を使用し、次のスクリプトを実行してアドバンスト・レプリケーションを構成します。

   ```
   $ORACLE_HOME/ldap/bin/remtool -asrsetup
   ```

   注意 :
   - レプリケーション環境管理ツール（`remtool`）の `-asrsetup` オプションの使用方法の詳細は、『Oracle Identity Management ユーザー・リファレンス』の `remtool` コマンドライン・ツールのリファレンスを参照してください。
   - データベースとリスナーが実行中であることを確認する方法は、Oracle Database ドキュメント・ライブラリの『Oracle Database 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、Oracle Database ドキュメント・ライブラリの『Oracle Database Net Services 管理者ガイド』を参照してください。

注意： エラーが発生した場合は、レプリケーション環境管理ツールの `-asrcleanup` オプションを使用して、環境をクリーンアップします。その後、手順 3 を繰り返します。

注意：「タスク 3: ディレクトリ・レプリケーション・グループ用の Oracle Database アドバンスト・レプリケーションの設定」では、レプリケーション環境管理ツール（`remtool`）によってレプリケーション構成パラメータのデフォルト値が設定されるので、レプリケーション・サーバーを簡単に起動できます。レプリケーション構成パラメータを変更する場合は、第 30 章「Oracle Internet Directory レプリケーションのインストールと構成」

タスク 4（オプション）: ディレクトリへのデータのロード

データをディレクトリにロードする方法は、次の 2 つから選択できます。

- 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ます。`ldapadd` を使用して、データをいずれかのノードにロードします。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。

  a. 次のように入力して、DRG のすべてのノードで LDAP サーバーを停止します。

  ```
  opmnctl stopproc ias-component=OID
  ```

  b. DRG の一部であり、ldif ファイルをディレクトリにロードするノード上で、次のように入力します。

  ```
  bulkload connect="connect_string" check="TRUE" \
     generate="TRUE" file="file_with_absolute_path_name"
  ```

  注意： `ldifwrite` を使用して Oracle Internet Directory からデータを抽出した場合は、他のオプションに加え、`restore="TRUE"` オプションを使用して、操作属性をリストアします。

  c. 同じノードで、次のコマンドを入力します。

  ```
  bulkload connect="connect_string_1" load="TRUE"
  ```

  同じノードで手順 c を繰り返します。その際、*connect_string_1* には DRG の各ノードの接続文字列を指定して、DRG 内のすべてのノードにデータをロードします。たとえば、次のように入力します。

  ```
  bulkload connect="connect_string_2" load="TRUE"
  ```

  さらに、次のように入力します。

  ```
  bulkload connect="connect_string_3" load="TRUE"
  ```

  同様の手順で、DRG 内のすべてのノードにデータをロードします。

  注意：

  - *connect_string* は、Oracle Internet Directory ローカル・データベースの接続文字列です。
  - レプリケーションを正常に行うには、レプリケートされるすべてのノードで、エントリに同じ `orclguid`（グローバル識別子）が含まれている必要があります。そのためには、手順 b を一度実行し、DRG 内の各ノードについて手順 c を繰り返します。

関連資料： 構文および使用時の注意点については、『Oracle Identity Management ユーザー・リファレンス』の bulkload コマンドライン・ツールのリファレンスを参照してください。

タスク 5: 全ノードで Oracle ディレクトリ・サーバー・インスタンスが起動していることの確認

デフォルトの構成では、Oracle Internet Directory LDAP サーバー・インスタンス #1 の変更ロギングは TRUE に設定されています。Oracle Internet DirectoryLDAP サーバーのデフォルトのインスタンスは、次のように opmn を使用して開始されます。

```
opmnctl startproc ias-component=OID
```

注意： この時点では opmnctl startall コマンドは使用しないでください。このコマンドを使用した場合、HTTP サーバーと Oracle Internet Directory サーバーは起動できますが、OC4J サーバーを起動しようとすると停止してしまいます。タスク 6 を完了した後でなければ、OC4J サーバーは起動できません。DRG のすべてのノードでレプリケーション・サーバーを起動し、レプリケーションがすべてのノードに伝播した後は、opmnctl startall コマンドを正常に使用できます。

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 4 章「インストール後に実行するタスクと情報」を参照してください。

タスク 6: DRG の全ノードでのレプリケーション・サーバーの起動

すべてのノードでレプリケーション・サーバーを起動するには、各ノードで次のコマンドを入力します。

```
oidctl connect=connect_string server=oidrepld instance=1 \
       flags='-h host_on_which_the_directory_server_is_running -p port' start
```

インスタンス番号は、DRG 全体で一意である必要はありません。

注意： 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する場合、ディレクトリ・レプリケーション・サーバーでマルチマスター・フラグをオフにすると、パフォーマンス・オーバーヘッドを低減できます。そのためには、Oracle ディレクトリ・レプリケーション・サーバーの OID 制御ユーティリティ・コマンドで、-m フラグの値をデフォルト（TRUE）から FALSE に変更します。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。

Oracle Internet Directory レプリケーション・サーバーが oidctl の使用を開始している場合、Oracle Internet Directory コンポーネントを停止または起動する opmnctl コマンドは、Oracle Internet Directory レプリケーション・サーバー・プロセスも停止または開始されていることを確認します。

関連項目：

Oracle Internet Directory のプロセス制御の詳細は、第 6 章「Oracle Internet Directory のプロセス制御コンポーネント」を参照してください。

29-26 ページの「Oracle 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・サーバーの起動方法は、第 7 章「Oracle ディレクトリ・サーバーの管理」を参照してください。

タスク 7: ディレクトリ・レプリケーションのテスト

Oracle Directory Manager を使用して、ディレクトリ・レプリケーション・サーバーが実行されていることを確認した後、次の手順を実行してディレクトリ・レプリケーションをテストします。

1. Oracle Directory Manager に `orcladmin` でログインします。
2. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「<ディレクトリ・サーバー・インスタンス>」、「**エントリ管理**」の順に展開します。
3. MDS ノードに単一のエントリを作成します。

   同一のエントリが、RMS に約 1 ～ 10 分後に表示されます。このタイミングは、レプリケーション・サーバーの構成設定エントリで調整できます。エントリが DRG のいずれかのノードで変更されると、その変更はレプリケートされます。

注意： Oracle Application Server Single Sign-On のレプリケーションを構成するには、Oracle Application Server Single Sign-On 用のインストール後の手順を実行します。これらの手順は、『Oracle Application Server Single Sign-On 管理者ガイド』のレプリケーションのインストールに関する項を参照してください。

マルチマスター・レプリケーション用のノードの追加（Oracle Database アドバンスト・レプリケーション・タイプのみ）

注意： 既存のマルチマスター・レプリケーション・グループに追加する新規ノードには、Oracle Application Server Infrastructure がインストールされている必要があります。インストールの際には、「**Oracle Application Server with Metadata Repository**」をインストール・タイプとして選択しておく必要があります。詳細は、30-8 ページの「タスク 2: リモート・マスター・サイト（RMS）へのレプリカとしての Oracle Internet Directory のインストール」を参照してください。

マスター・ノード、または他の LDAP ベースのレプリカのコンシューマではない LDAP ベースのサプライヤ・レプリカにノードを追加し、マルチマスター DRG を形成できます。その場合、この項の手順に従えば、アドバンスト・レプリケーションの初期インストールおよび構成が自動的に実行されます。

稼働中のレプリケーション・グループまたは大規模なマスター・ノードに新規レプリケーション・ノードを追加するには、次の手順を実行します。

- Oracle Net Services 環境の準備
- タスク 1: 全ノードでのディレクトリ・レプリケーション・サーバーの停止
- タスク 2: スポンサ・ノードの特定とリモート・サイトへのレプリカとしての Oracle Internet Directory のインストール
- タスク 3: スポンサ・ノードの読取り専用モードへの切替え
- タスク 4: ldifwrite を使用したスポンサ・ノードのバックアップ
- タスク 5: アドバンスト・レプリケーションのノード追加設定の実行
- タスク 6: スポンサ・ノードの更新可能モードへの切替え
- タスク 7: 新規ノード以外の全ノードでのディレクトリ・レプリケーション・サーバーの起動
- タスク 8: bulkload を使用した新規ノードへのデータのロード
- タスク 9: 新規ノードでのディレクトリ・サーバーの起動

- タスク 10: 新規ノードでのディレクトリ・レプリケーション・サーバーの起動

注意： 以降の各タスクの中で示されているコマンドを実行するには、次のタイプのファイルが、対応するディレクトリに格納されている必要があります。

- バイナリ : `$ORACLE_HOME/bin`
- SQL スクリプト : `$ORACLE_HOME/ldap/admin`
- UNIX スクリプト : `$ORACLE_HOME/ldap/bin`

「タスク 2: スポンサ・ノードの特定とリモート・サイトへのレプリカとしての Oracle Internet Directory のインストール」を開始する前に、これら 3 つのタイプのファイルがそれぞれのパスに存在することを確認してください。

Oracle Net Services 環境の準備

この環境を準備するプロセスは、「全ノードでのレプリケーション用の Oracle Net Services 環境の準備」を参照してください。

タスク 1: 全ノードでのディレクトリ・レプリケーション・サーバーの停止

ディレクトリ・レプリケーション・サーバーを停止するには、LDAP レプリケーション・グループ内の各ノードで次のコマンドを実行します。

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

注意： インスタンス番号が 1 でない場合もあります。実行中のプロセスをチェックし、ここで使用するインスタンス番号を確認してください。

タスク 2: スポンサ・ノードの特定とリモート・サイトへのレプリカとしての Oracle Internet Directory のインストール

このタスクでは、スポンサ・ノードを特定する必要があります。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。

RMS 用には、Oracle Internet Directory の新規インスタンスをアドバンスト・レプリケーション・レプリカとしてインストールすることをお薦めします。（既存のマスター・ノードを RMS として使用することも可能ですが、手動の手順を別途実行する必要があります。）

RMS 用のアドバンスト・レプリケーション・レプリカとして Oracle Internet Directory を新しくインストールする場合は、30-4 ページの「Oracle Internet Directory をアドバンスト・レプリケーション・ベースのレプリカ、あるいは一方向または双方向の LDAP ベースのレプリカとしてインストールする場合」の指示に従い、「アドバンスト・レプリケーション」オプションが表示されたらそれを選択します。

既存のマスターを RMS として使用する場合は、30-8 ページの「既存のマスターをリモート・マスター・サイトとして使用する場合」の指示に従って、マスターのメタデータをスポンサ・ノードに移行する必要があります。マスターのメタデータを MDS に移行したら、次は、「タスク 3: スポンサ・ノードの読取り専用モードへの切替え」に進みます。

タスク 3: スポンサ・ノードの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 adminPassword -h host_name_of_sponsor_node \
           -p port -f change_mode.ldif
```

このコマンドは、Oracle ディレクトリ・サーバーの *name_of_sponsor_node* をスポンサ・モードから読取り専用モードに変更します。

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。

また、スポンサ・ノードと MDS が同じノードの可能性もあります。

タスク 4: ldifwrite を使用したスポンサ・ノードのバックアップ

この処理は時間がかかる場合もあるので、バックアップ処理中に「タスク 5: アドバンスト・レプリケーションのノード追加設定の実行」を開始してもかまいません。

スポンサ・ノードで、次のコマンドを入力します。

```
ldifwrite connect="connect_string" \
          basedn="orclAgreementID=000001,cn=replication configuration" \
          file="output_ldif_file"
```

これで、スポンサ・ノードのディレクトリがバックアップされます。

タスク 5: アドバンスト・レプリケーションのノード追加設定の実行

注意： レプリケーションを行うすべてのノードで、Oracle Net Service が正しく構成されている必要があります。30-9 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」を参照してください。

アドバンスト・レプリケーションのノード追加設定は、30-16 ページの「タスク 4: ldifwrite を使用したスポンサ・ノードのバックアップ」を実行するときに同時に実行できます。

スポンサ・ノードで、次のコマンドを入力します。

```
remtool -addnode
```

レプリケーション環境管理ツールによって、DRG にノードが追加されます。

注意：

remtool -addnode を実行してレプリケーション・グループの最初のアドバンスト・レプリケーション・レプリカを追加すると、remtool -asrsetup を使用した場合と同様のレプリケーションの初期設定が自動的に行われます。remtool -addnode を使用する際には、スポンサ・ノードの接続識別子を指定する必要があります。

remtool -addnode を使用する場合、レプリケートされた表の行数とノード間のネットワーク待機時間によっては、操作に長時間かかることがあります。この操作の進捗状況を確認するには、-v オプションを使用します。

エラーが発生した場合は、まず -asrverify オプションを使用します。このオプションでもエラーが発生した場合には、-asrrectify オプションを使用して、そのエラーを修正します。-asrverify および -asrrectify は、DRG 内のすべてのノードをリストします。新規ノードがリストにない場合は、-delnode オプションを使用してレプリケーション環境管理ツールを再度実行し、新規ノードを削除します。その後、-addnode オプションを使用して新規ノードを再度追加します。

関連資料： レプリケーション環境管理ツールの -addnode オプションの使用方法は、『Oracle Identity Management ユーザー・リファレンス』の remtool コマンドライン・リファレンスを参照してください。

タスク 6: 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 adminDN -w adminPassword -h host_name_of_sponsor_node \
           -p port -f change_mode.ldif
```

このコマンドは、Oracle ディレクトリ・サーバーの *host_name_of_sponsor_node* をスポンサ・モードから読取り / 書込みモードに戻します。

注意： タスク 6 は、タスク 3 と類似しています。この手順では change_mode.ldif の orclservermode パラメータが、rw（すなわち読取り / 書込み）に設定される点のみが異なります。

タスク 7: 新規ノード以外の全ノードでのディレクトリ・レプリケーション・サーバーの起動

ディレクトリ・レプリケーション・サーバーを起動するには、新規ノード以外のすべてのノード上で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確認するため、次のように入力します。

```
opmnctl stopproc ias-component=OID
```

タスク 8: bulkload を使用した新規ノードへのデータのロード

データをロードするには、新規ノードで次のコマンドを入力します。

```
bulkload connect="db_connect_string_of_new_node" check="TRUE" generate="TRUE" \
   load="TRUE" restore ="TRUE" \
   file="absolute_path_to_the_ldif_file_generated_by_ldifwrite"
```

注意： Oracle Internet Directory の旧リリース（10*g* リリース 2（10.1.2.0.2）など）のデータを、10*g*（10.1.4.0.1）が稼働しているノードにロードする場合、パスワード・ポリシー・エントリを、30-32 ページの「パスワード・ポリシーとファンアウト・レプリケーション」で説明しているように更新する必要があります。

タスク 9: 新規ノードでのディレクトリ・サーバーの起動

ディレクトリ・サーバーを起動するには、新規ノードで次のコマンドを入力します。

```
opmnctl startproc ias-component=OID
```

タスク 10: 新規ノードでのディレクトリ・レプリケーション・サーバーの起動

注意： 構成パラメータまたは承諾パラメータの変更が必要な場合は、第 31 章「Oracle Internet Directory レプリケーションの監視および管理」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、新規ノードで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="-p port" start
```

注意： ディレクトリ・サーバー・インスタンスがレプリケーション承諾のメンバーとなった後は、データのノードへの追加に bulkload ツールを使用しないでください。かわりに、ldapadd を使用してください。

レプリケーションに Oracle Application Server Single Sign-On が必要な場合は、『Oracle Application Server Single Sign-On 管理者ガイド』のレプリケーションのインストールに関する項を参照し、Oracle Application Server Single Sign-On を対象としたインストール後の手順を実行してください。

マルチマスター・レプリケーション・グループからのノードの削除

システム・エラーが発生して新しいノードを追加できなかった場合などは、ノードを DRG から削除する必要があります。

レプリケーション・ノードを削除するには、次のタスクを実行します。

- タスク 1: 全ノードでのディレクトリ・レプリケーション・サーバーの停止
- タスク 2: 削除するノード内の全 Oracle Internet Directory プロセスの停止
- タスク 3: マスター定義サイトからのノードの削除
- タスク 4: 全ノードでのディレクトリ・レプリケーション・サーバーの起動

タスク 1: 全ノードでのディレクトリ・レプリケーション・サーバーの停止

ディレクトリ・レプリケーション・サーバーを停止するには、DRG 内の各ノードで次のコマンドを実行します。

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

注意： インスタンス番号は違う場合があります。

タスク 2: 削除するノード内の全 Oracle Internet Directory プロセスの停止

削除するノードで、opmn を使用して Oracle Internet Directory を停止します。

```
$ORACLE_HOME/opmn/bin/opmnctl stopproc ias-component=OID
```

関連資料： Oracle Internet Directory の停止の詳細は、『Oracle Identity Management ユーザー・リファレンス』の opmn コマンドライン・ツールのリファレンスを参照してください。

タスク 3: マスター定義サイトからのノードの削除

MDS から、次のスクリプトを実行します。

```
remtool -delnode
```

レプリケーション環境管理ツールによって、レプリケーション・グループからノードが削除されます。

関連資料： レプリケーション環境管理ツールの -delnode オプションの使用方法は、『Oracle Identity Management ユーザー・リファレンス』の remtool コマンドライン・ツールのリファレンスを参照してください。

この処理は、システム・リソースと DRG のサイズによって、長時間かかる場合があります。-v オプションを使用すると、進捗状況を確認できます。

注意： エラーが発生した場合は、まず -asrverify オプションを使用します。このオプションでもエラーが発生した場合には、-asrrectify オプションを使用して、そのエラーを修正します。-asrverify および -asrrectify は、DRG 内のすべてのノードをリストします。削除するノードがリストにない場合は、-delnode オプションを使用してレプリケーション環境管理ツールを再度実行し、ノードを削除します。

タスク 4: 全ノードでのディレクトリ・レプリケーション・サーバーの起動

ディレクトリ・レプリケーション・サーバーを起動するには、DRG のその他の各ノードで次のコマンドを入力します。

```
oidctl connect=connect_string server=oidrepld instance=1 \
       flags='-h host -p port' start
```

関連資料：『Oracle Identity Management ユーザー・リファレンス』の opmn コマンドライン・ツールのリファレンス

一方向または双方向 LDAP ベース・レプリケーションのインストールと構成

この項の項目は次のとおりです。

- LDAP ベースのレプリケーションの構成に関する規則
- ldifwrite と bulkload を使用した LDAP データのバックアップ
- 一方向または双方向 LDAP ベース・レプリカのデフォルト設定でのインストールと構成
- カスタム設定を使用した LDAP ベースのレプリカのインストールと構成
- LDAP ベースのレプリカの削除
- LDAP ベースの部分レプリケーションでのレプリケート対象の決定

関連資料：『Oracle Application Server 管理者ガイド』の「LDAP ベースのレプリカ構成の補足手順」

LDAP ベースのレプリケーションの構成に関する規則

次の規則は、LDAP ベースの完全レプリケーションと部分レプリケーションの両方に適用されます。

1. LDAP ベースのレプリケーションでは、ルート DSE の `namingcontexts` 属性にリストされているネーミング・コンテキストのみ、コンシューマにレプリケートできます。

   関連項目： namingcontexts の詳細は、次の項を参照してください。

   - A-13 ページの「Oracle Directory Manager のレプリケーション・フィールド」
   - 29-30 ページの「部分レプリケーションに含まれるネーミング・コンテキストと除外されるネーミング・コンテキスト」
   - 30-34 ページの「Oracle Directory Manager を使用したレプリカのネーミング・コンテキスト・オブジェクトの表示と変更」

2. LDAP ベースのレプリカのサプライヤは、スタンドアロン・ノード、マルチマスター・レプリケーション・グループのメンバー、別の LDAP ベースのレプリカのいずれかです。

   関連項目： スタンドアロン・ノードにインストールする方法は、30-3 ページの「Oracle Internet Directory をマスターとしてインストールする場合」を参照してください。

3. LDAP ベースのレプリカは、別の LDAP ベースのレプリカのコンシューマの場合もあります。そのコンシューマはファンアウト・レプリカと呼ばれます。

4. Oracle Internet Directory 10*g*（10.1.4.0.1）LDAP レプリカを、旧リリース（10*g* リリース 2（9.0.4）または 10*g* リリース 2（10.1.2）など）を実行している Oracle Internet Directory 10*g* マスターに追加できます。また、10*g*（9.0.4）または（10.1.2）マスターの LDAP レプリカを 10*g*（10.1.4.0.1）にアップグレードできます。ただし、旧リリースは、10*g*（10.1.4.0.1）の全機能をサポートしていないことを承知しておいてください。

注意： スキーマが同期していることを確認してください。同期していないと、レプリケーション・サーバーがコンシューマ・レプリカに変更を適用できない場合があります。

5. 双方向 LDAP ベース・レプリケーションには、下位互換性がありません。10*g*（10.1.4.0.1）を実行しているレプリカ間でのみサポートされます。
6. 新規コンシューマ・ノードは空であることが必要です。つまり、Oracle Internet Directory を新たにインストールする必要があります。

ldifwrite と bulkload を使用した LDAP データのバックアップ

ldifwrite ユーティリティを使用して、保存されている操作属性とともに LDAP データをバックアップします。この操作を実行した後は、bulkload ユーティリティを使用して、グループ内のすべてのレプリカにデータをロードします。

`bulkload` に `check="TRUE"`、`generate="TRUE"` および `restore="TRUE"` の引数を指定して使用し、次に `load="TRUE"` 引数を指定して使用します。すべてのレプリカに同じ中間ファイル（`generate="TRUE"` 引数を使用して生成）を使用することにより、操作属性を保存します。10*g*（10.1.4.0.1）では、`connect="`*`connect_string`*`"` をレプリカごとに適切な接続文字列を指定して使用することにより、`bulkload` コマンドの 1 回の起動で複数のレプリカをロードできます。

100 万件のエントリがあるディレクトリの場合、この方法でのバックアップには長時間かかります。

関連資料：

- 第 9 章「バルク・ツールの使用方法」
- 『Oracle Identity Management ユーザー・リファレンス』の Oracle Identity Management のコマンドライン・ツールのリファレンスに関する項

一方向または双方向 LDAP ベース・レプリカのデフォルト設定でのインストールと構成

この項では、サプライヤ・レプリカからコンシューマ・レプリカへの LDAP ベースのレプリケーションを構成する 1 つの方法として、すべての `namingcontext` を指定したデフォルトの `namingcontext` 構成設定の使用方法について説明します。つまり、サプライヤ・レプリカの DIT 全体がコンシューマにレプリケートされるようにレプリケーションを構成します。

デフォルト設定を使用して LDAP レプリカをインストールおよび構成すると、自動ブートストラップにより、サプライヤからコンシューマへの初期データ同期化が実行されます。新規 LDAP レプリカのインストールが完了した後、LDAP ベースのレプリケーションが構成され、レプリケーション・プロセスが自動的に開始されます。

注意： デフォルト設定を使用して LDAP レプリカをインストールすると、コンシューマ・レプリカのメタデータがサプライヤ・レプリカに自動的に移行されます。その際、すべてのメタデータがネーミング・コンテキスト `cn=oraclecontext` の下にあると想定されます。レルム固有のネーミング・コンテキストなど、異なるネーミング・コンテキストを使用する必要がある場合は、30-23 ページの「カスタム設定を使用した LDAP ベースのレプリカのインストールと構成」を参照してください。

関連項目： 自動ブートストラップの詳細は、付録 H「LDAP のレプリカ状態」を参照してください。

タスク 1: サプライヤ・ノードでのディレクトリ・サーバーの特定と起動

LDAP ベースのレプリカのサプライヤを特定します。次のいずれかがサプライヤとなります。

- スタンドアロン・ディレクトリ
- マルチマスター・レプリケーション・グループのノード
- 別の LDAP ベースのレプリカ

サプライヤ・ノードで Oracle Internet Directory サーバーが起動していることを確認します。ディレクトリ・サーバーを起動するには、次のコマンドを入力します。

```
opmnctl startproc ias-component=OID
```

タスク 2: LDAP レプリカとしての Oracle Internet Directory のインストール

30-4 ページの「Oracle Internet Directory をアドバンスト・レプリケーション・ベースのレプリカ、あるいは一方向または双方向の LDAP ベースのレプリカとしてインストールする場合」の手順を使用します。

- 一方向（読取り専用）LDAP レプリカの場合、**一方向 LDAP レプリカ**を選択します。
- 双方向（読取り / 書込み可能）LDAP レプリカの場合、**双方向 LDAP レプリカ**を選択します。

デフォルト設定を使用して LDAP レプリカをインストールすると、ブートストラップが自動的に起動され、サプライヤからコンシューマにデータが移行されます。

注意： ブートストラップには長時間かかることがあります。

ブートストラップの実行中は、サプライヤ側の Oracle Internet Directory スキーマを更新しないでください。更新すると、レプリケーションのブートストラップに失敗します。失敗した場合は、再度ブートストラップを試みる前に、コンシューマ側の Oracle Internet Directory スキーマがサプライヤ側のスキーマと同期していることを確認します。

ブートストラップ中にサプライヤ側の Oracle Internet Directory を更新すると、Oracle Internet Directory レプリケーション・サーバーが警告メッセージを発します。サプライヤに加えた変更はコンシューマにレプリケートされます。ただし、管理者操作キューに移動される変更もあります。

インストールが完了すると、LDAP レプリケーションが構成されます。コンシューマ側のレプリケーション・サーバーは、変更をサプライヤからレプリケートします。

新規 LDAP レプリカのレプリケーション・ログ・ファイルを表示すれば、レプリケーション・アクティビティをチェックできます。

タスク 3: ディレクトリ・レプリケーション・サーバーの起動の確認

タスク 2 を完了すると、新しいレプリカ上のレプリケーション・サーバーが自動的に起動されます。これが一方向レプリカの場合、他に何もする必要はありません。ただし、これが双方向レプリカの場合は、スポンサと新しいレプリカの両方で、レプリケーション・サーバーが起動していることを確認する必要があります。

スポンサ・レプリカで Oracle Internet Directory レプリケーションを起動または再起動するには、次のように入力します。

```
oidctl server=oidrepld connect=connect_string_of_sponsor replica  \
   instance=instance_number_of_consumer_replica \
   flags= "-p port_of_oid_server_running_at_sponsor_replica \
           -h hostname_of_sponsor_replica" start
```

カスタム設定を使用した LDAP ベースのレプリカのインストールと構成

カスタム設定を行うには、まず新規ノードをマスター・ノード（スタンドアロン）としてインストールする必要があります。このタスクを実行するには、30-3 ページの「Oracle Internet Directory をマスターとしてインストールする場合」の手順に従います。

remtool を使用して LDAP ベースのレプリケーションを構成した後、LDAP ベースのノードに対してレプリケートされる項目を定義する namingcontext をカスタマイズできます。

> **関連項目：** ネーミング・コンテキストの詳細は、30-34 ページの「LDAP ベースの部分レプリケーションでのレプリケート対象の決定」を参照してください。

カスタム設定を使用して LDAP ベースのレプリカをインストールおよび構成する場合、ディレクトリのデータをどのように移行するかによって、2 つの方法があります。

- コマンドライン・ツールを使用します。ldifwrite を使用してサプライヤ・レプリカのデータをバックアップした後、bulkload を使用してコンシューマ・レプリカにデータをリストアします。
- 自動ブートストラップを使用します。これはレプリケーション・サーバーの機能で、レプリケーション構成に基づいてサプライヤ・レプリカからコンシューマ・レプリカにデータを自動的にブートストラップします。

表 30-1 に、2 つの方法の比較を示します。

表 30-1 ldifwrite/bulkload を使用したデータ移行と自動ブートストラップを使用したデータ移行の比較

ldifwrite/bulkload を使用した移行	自動ブートストラップを使用した移行
手動プロシージャ	自動プロシージャ
高速パフォーマンス	部分レプリケーションのフィルタ機能を使用
大量のデータに最適	エントリ数が少ない場合に最適

データの移行方法として自動ブートストラップを選択した場合は、30-23 ページの「自動ブートストラップを使用した LDAP ベースのレプリカの構成」の指示に従って、LDAP ベースのレプリカをカスタマイズします。

データの移行方法として ldifwrite/bulkload を選択した場合は、30-28 ページの「ldifwrite ツールを使用した LDAP ベースのレプリカの構成」の指示に従って、LDAP ベースのレプリカを構成します。

自動ブートストラップを使用した LDAP ベースのレプリカの構成

次の 8 つのタスクを実行すると、自動ブートストラップを使用して LDAP ベースのレプリカを構成できます。各タスクの詳細は、このリストの後で説明します。

- タスク 1: サプライヤ・ノードでのディレクトリ・サーバーの特定と起動
- タスク 2: Oracle Internet Directory をマスターとしてインストールすることで新規コンシューマ・ノードを作成
- タスク 3: 新規コンシューマ・ノードのメタデータのバックアップ
- タスク 4: レプリケーション環境管理ツールを使用した LDAP ベースのレプリカの追加
- タスク 5: コンシューマ側でコンシューマ・レプリカを自動ブートストラップ用に構成
- タスク 6: オプション : デフォルトのレプリケーション・パラメータの変更
- タスク 7: ディレクトリ・レプリケーション・サーバーの起動の確認
- タスク 8: 新規ノードに DAS または SSO がインストールされている場合､新規ノードのディレクトリ内のエントリをリストア

タスク 1: サプライヤ・ノードでのディレクトリ・サーバーの特定と起動 LDAP ベースのレプリカのサプライヤを特定します。次のいずれかがサプライヤとなります。

- スタンドアロン・ディレクトリ
- マルチマスター・レプリケーション・グループのノード
- 別の LDAP ベースのレプリカ

サプライヤ・ノードで Oracle Internet Directory サーバーが起動していることを確認します。ディレクトリ・サーバーを起動するには、次のコマンドを入力します。

```
opmnctl startproc ias-component=OID
```

タスク 2: Oracle Internet Directory をマスターとしてインストールすることで新規コンシューマ・ノードを作成 カスタム設定を使用して LDAP ベースのレプリカをインストールおよび構成するには、新規コンシューマ・ノードをマスターとしてインストールする必要があります。新しい Oracle Internet Directory をマスターとしてインストールする場合は、30-3 ページの「Oracle Internet Directory をマスターとしてインストールする場合」の指示に従ってください。

タスク 3: 新規コンシューマ・ノードのメタデータのバックアップ カスタム設定を使用して新規ノードを LDAP ベースのレプリカとして構成する前に、まず新規ノードのメタデータを次のようにサプライヤ・ノードに移行する必要があります。

- バックアップ・プロセス（remtool -backupmetadata）が正しく機能するように、Oracle Internet Directory サーバーがサプライヤ・ノードとタスク 2 で作成した新規ノードの両方で稼働していることを確認します。
- 新たに作成したノードから、次のコマンドを実行します。

  ```
  remtool -backupmetadata \
          -replica "new_node_host:new_node_port/new_node_repldn_pwd" \
          -master "master_host:master_port/master_repl_dn_pwd"
  ```

  master_host:*master_port*/*master_repdn_pwd* は、対象となるレプリカのサプライヤのホスト名、ポート番号およびレプリケーション識別名パスワードです。

  注意： Oracle Delegated Administration Services が構成されていない場合、`remtool` を `-backupmetadata` オプションを指定して実行すると、次のようなエラー・メッセージが表示されます。

  ```
  Failed to add "orclApplicationCommonName=ias.acme.com,
  cn=IAS Instances, cn=IAS, cn=Products, cn=OracleContext"
  as "uniquemember" to entry "cn=Associated Mid-tiers,
  orclapplicationcommonname=DASApp, cn=DAS,cn=products,
  cn=OracleContext at replica ldap://myhost:389
  ```

  このエラー・メッセージは無視してください。

  関連資料： `-backupmetadata` など、`remtool` オプションの詳細は、『Oracle Identity Management ユーザー・リファレンス』の `remtool` コマンドライン・ツールのリファレンスを参照してください。

- このコマンドは、メタデータをマスター・レプリカにロードする以外に、メタデータのバックアップを含む `ocbkup.`*new_replica_id*`.TO.`*master_replicaid*`.`*timestamp*`.dat` という名前のファイルを作成します。このファイルは `$ORACLE_HOME/ldap/log` ディレクトリに作成されます。このファイルには、LDIF 形式でのマスター・レプリカの変更と、SSO のコンテナ・エントリ [orclApplicationCommonName=ORASSO_SSOSERVER, cn=SSO, cn=Products, cn=OracleContext] および DAS の URL コンテナ・エントリ [cn=OperationURLs, cn=DAS, cn=Products, cn=OracleContext] のコピーが格納されます。

- メタデータのバックアップに成功した場合、次のメッセージが端末に表示されます。

  ```
  Backup of metadata will be stored in
  $ORACLE_HOME/ldap/log/ocbkup.new_replica_id.TO.master_replicaid.timestamp.dat.
  Metadata copied successfully.
  ```

  メッセージには、ORACLE_HOME のパスが含まれます。

- メタデータのバックアップに失敗した場合、`$ORACLE_HOME/ldap/log/remtool.log` ファイルにエラー・メッセージが記録されます。`remtool` を端末から起動した場合は、その端末にエラー・メッセージが表示されます。

タスク 4: レプリケーション環境管理ツールを使用した LDAP ベースのレプリカの追加 レプリカを追加するには、コンシューマ・レプリカで次のように入力します。

```
remtool -paddnode [-v] [-bind supplier_host_name:port/replication_dn_password]
```

remtool ユーティリティから承諾のタイプの指定を求められます。追加するレプリカのタイプに応じて、一方向 LDAP または双方向 LDAP のいずれかを選択します。

> **関連資料：** レプリケーション環境管理ツールの詳細は、『Oracle Identity Management ユーザー・リファレンス』の `remtool` コマンドライン・ツールのリファレンスを参照してください。

タスク 5: コンシューマ側でコンシューマ・レプリカを自動ブートストラップ用に構成 自動ブートストラップ機能を使用するには、コンシューマ側で、次のようにコンシューマ・レプリカのサブエントリの `orclReplicaState` 属性を `0` に設定します。

1. サンプル・ファイル `mod.ldif` を、次のように編集します。

   ```
   Dn: orclreplicaid=unique_replicaID_of_consumer, cn=replication configuration
   Changetype:modify
   add:orclReplicaState
   OrclReplicaState: 0
   ```

2. コンシューマ側で ldapmodify を使用して、コンシューマ・レプリカのサブエントリの `orclreplicastate` 属性を更新します。

   ```
   ldapmodify -D "cn=orcladmin" -w administrator_password -h consumer_host \
              -p port -f mod.ldif
   ```

> **関連項目：** LDAP ベースのレプリケーションのブートストラップ機能の詳細は、第 31 章「Oracle Internet Directory レプリケーションの監視および管理」を参照してください。

タスク 6: オプション : デフォルトのレプリケーション・パラメータの変更 レプリケーション承諾およびレプリカ・サブエントリのデフォルトのパラメータを変更できます。

> **関連項目：**
>
> - 29-10 ページの「ディレクトリ内のレプリケーション構成オブジェクト」
> - 30-34 ページの「LDAP ベースの部分レプリケーションでのレプリケート対象の決定」
> - 31-2 ページの「ディレクトリ・レプリケーション・サーバーの構成パラメータの表示および変更」
> - 31-4 ページの「特定のレプリカ・ノードについてのパラメータの表示および変更」
> - 31-6 ページの「レプリケーション承諾のパラメータの変更」

タスク 7: ディレクトリ・レプリケーション・サーバーの起動の確認 レプリケーション・サーバーを起動する正確な手順は、サーバーが一方向レプリカまたは双方向レプリカのいずれにあるのかによって異なります。

- 一方向 LDAP レプリケーションの場合は、コンシューマでレプリケーション・サーバーを起動する必要があります。次のように入力します。

```
oidctl server=oidrepld connect=connect_string_of_consumer_replica \
   instance=instance_number_of_consumer_replica  \
   flags= "-p port_of_oid_server_running_at_consumer \
           -h hostname_of_sponsor_replica -m false" start
```

  一方向 LDAP レプリケーションのために、コンシューマで Oracle Internet Directory レプリケーション・サーバーを起動する際には、`-m false` オプションの使用をお薦めします。これにより競合解消が無効になり、パフォーマンスが向上します。

- 双方向 LDAP レプリケーションの場合は、スポンサ・レプリカと新規レプリカの両方で、Oracle Internet Directory レプリケーション・サーバーを次のように起動する必要があります。

  1. スポンサ・レプリカでレプリケーションを起動または再起動します。次のように入力します。

```
oidctl server=oidrepld connect=connect_string_of_sponsor_replica \
   instance=instance_number_of_sponsor_replica \
   flags= "-p port_of_oid_server_running_at_sponsor_replica
           -h hostname_of_consumer_replica" start
```

  2. 新規レプリカでレプリケーション・サーバーを起動します。次のように入力します。

```
oidctl server=oidrepld connect=connect_string_of_consumer_replica \
    instance=instance_number_of_consumer_replica \
    flags= "-p port_of_oid_server_running_at_new_replica  \
            -h hostname_of_consumer_replica"
```

  関連資料 :『Oracle Identity Management ユーザー・リファレンス』の `oidctl` コマンドライン・ツールのリファレンス

レプリケーション・サーバーが起動すると、サプライヤからコンシューマへのデータのブートストラップが開始されます。ブートストラップが正常に完了すると、レプリケーション・サーバーが自動的にオンライン・モードに変わり、変更内容をサプライヤからコンシューマに適用します。

タスク 8: 新規ノードに DAS または SSO がインストールされている場合、新規ノードのディレクトリ内のエントリをリストア DAS および SSO のエントリは、各サービスのローカル・インスタンスを参照する必要があります。しかし、レプリケーションをサプライヤからコンシューマに最初にダウンロードしたときには、サプライヤからレプリケートされた値を使用してこれらのエントリが作成されます。各サービスが実際にはコンシューマ・ノードに構成されている場合、これらの値をコンシューマ・ノードに適した正しい情報に置き換える必要があります。

- Delegated Administration Service（DAS）がコンシューマ・ノードに構成されている場合、次の手順に従って DAS をリストアする必要があります。

  1. タスク 3 で作成した `ocbkup.new_replicaid.TO.master_replicaid.timestamp.dat` ファイルで、DAS の URL を見つけてコピーします。DAS の URL コンテナ・エントリの識別名は、cn=OperationURLs, cn=DAS, cn=Products, cn=OracleContext です。通常、これはファイルの最後から 2 番目のエントリです。

  関連資料 :『Oracle Identity Management 委任管理ガイド』

2. LDIF ファイル change_das_url.ldif を作成します。このファイルの内容は次のとおりです。

```
dn: cn=OperationURLs,cn=DAS,cn=Products,cn=OracleContext
changetype: modify
replace: orcldasurlbase
orcldasurlbase: copy_paste_the_URL_from_backup_file
```

3. 次のコマンドを実行して、DAS の URL を変更します。

```
ldapmodify -p consumer_port -h consumer_host -D super_user_DN \
           -w super_user_password -f change_das_URL.ldif
```

- 同様に、Single Sign-On（SSO）がコンシューマ・ノードに構成されている場合、次の手順に従って SSO をリストアする必要があります。

1. タスク 3 で作成した ocbkup.*timestamp*.dat ファイルで、SSO のコンテナ・エントリを見つけてコピーします。コピーするのは手順 2 に示した属性のみです。SSO のコンテナ・エントリの識別名は、orclApplicationCommonName=ORASSO_SSOSERVER, cn=SSO, cn=Products, cn=OracleContext です。通常、これはファイルの最後のエントリです。

   関連資料：『Oracle Application Server Single Sign-On 管理者ガイド』

2. LDIF ファイル add_SSO_container.ldif を作成します。このファイルの内容は次のとおりです。

```
dn: orclApplicationCommonName=ORASSO_SSOSERVER,
 cn=SSO,cn=Products,cn=OracleContext
orclapplicationcommonname: ORASSO_SSOSERVER
orclappfullname: ORASSO_SSOSERVER
orclversion: 10.1.2.0.0
objectclass: orclApplicationEntity
objectclass: top
userpassword: userpassword_copied_from_backup_file
```

   注意： authpassword;oid、createtimestamp、creatorsname、modifiersname、modifytimestamp、orclguid の各属性はコピーしないでください。

3. 次のコマンドを実行して、SSO のコンテナ・エントリを追加します。

```
ldapadd -p consumer_port -h consumer_host -D super_user_DN \
        -w super_user_password -f add_SSO_container.ldif
```

4. LDIF ファイル mod.ldif を作成します。このファイルの内容は次のとおりです。

```
dn: cn=OracleUserSecurityAdmins,cn=Groups,cn=OracleContext
changetype:modify
add: uniquemember
uniquemember: orclApplicationCommonName=ORASSO_SSOSERVER,
 cn=SSO,cn=Products,cn=OracleContext

dn: cn=verifierServices, cn=Groups,cn=OracleContext
changetype:modify
add: uniquemember
uniquemember: orclApplicationCommonName=ORASSO_SSOSERVER,
 cn=SSO,cn=Products,cn=OracleContext
```

5. 次のコマンドを実行して、mod.ldif を適用します。

```
ldapmodify -p consumer_port -h consumer_host -D super_user_DN \
           -w super_user_password -f mod.ldif
```

変更を有効にするために、OC4J セキュリティを再起動します。

```
$ORACLE_HOME/opmn/bin/opmnctl  stopproc process-type=OC4J_SECURITY
$ORACLE_HOME/opmn/bin/opmnctl startproc process-type=OC4J_SECURITY
```

6. ブラウザを使用して、Oracle Delegated Administration Services ページと OracleAS Single Sign-On ページをテストします。

   Oracle Delegated Administration Services をテストするには、admin ユーザー `orcladmin` として Oracle Delegated Administration Services ページ（`http(s)://new_node_hostname:new_node_http_port/oiddas/`）にログインします。ログインできない場合は、『Oracle Identity Management 委任管理ガイド』のトラブルシューティングに関する付録を参照してください。

   OracleAS Single Sign-On をテストするには、admin ユーザー `orcladmin` として OracleAS Single Sign-On ページ（`http(s)://new_node_hostname:new_node_http_port/pls/orasso/`）にログインします。ログインできない場合は、『Oracle Application Server Single Sign-On 管理者ガイド』のトラブルシューティングに関する付録を参照してください。

ldifwrite ツールを使用した LDAP ベースのレプリカの構成

この項では、ldifwrite ツールを使用して、LDAP ベースのレプリカを構成する場合に実行する一般的なタスクを説明します。この項の項目は次のとおりです。

タスク 1: サプライヤ・ノードとコンシューマ・ノードの両方でディレクトリ・サーバーを起動

1. LDAP ベースのレプリカのサプライヤを特定します。次のいずれかがサプライヤとなります。

   - スタンドアロン・ディレクトリ
   - マルチマスター・レプリケーション・グループのノード
   - 別の LDAP ベースのレプリカ

   サプライヤ・ノードで Oracle Internet Directory サーバーが起動していることを確認します。ディレクトリ・サーバーを起動するには、次のコマンドを入力します。

   ```
   opmnctl startproc ias-component=OID
   ```

2. コンシューマ・ノードを特定します。コンシューマ・ノードは、マスターとしてインストールされた新規 Oracle Internet Directory であることが必要です。新しい Oracle Internet Directory をマスターとしてインストールする場合は、30-3 ページの「Oracle Internet Directory をマスターとしてインストールする場合」の指示に従ってください。新規コンシューマ・ノードで Oracle Internet Directory サーバーが起動していることを確認します。ディレクトリ・サーバーを起動するには、次のコマンドを入力します。

   ```
   opmnctl startproc ias-component=OID
   ```

タスク 2: 新規コンシューマ・ノードのメタデータのバックアップ カスタム設定を使用してコンシューマを LDAP ベースのレプリカとして構成する前に、まずコンシューマのメタデータを次のようにサプライヤ・ノードに移行する必要があります。

- バックアップ・プロセス（remtool -backupmetadata）が正しく機能するように、Oracle Internet Directory サーバーがサプライヤ・ノードとタスク 2 で作成した新規ノードの両方で稼働していることを確認します。
- コンシューマ・ノードから、次のコマンドを実行します。

```
remtool –backupmetadata \
        –replica "consumer_host:consumer_port/consumer_repl_dn_pwd" \
        –master "supplier_host:supplier_port/supplier_repl_dn_pwd"
```

- このコマンドは、メタデータをマスター・レプリカにロードする以外に、メタデータのバックアップを含む ocbkup.*consumer_replica_id*.TO.*supplier_replica_id.timestamp*.dat という名前のファイルを作成します。このファイルは $ORACLE_HOME/ldap/log ディレクトリに作成されます。このファイルには、LDIF 形式でのマスター・レプリカの変更と、SSO のコンテナ・エントリ [orclApplicationCommonName=ORASSO_SSOSERVER, cn=SSO, cn=Products, cn=OracleContext] および DAS の URL コンテナ・エントリ [cn=OperationURLs, cn=DAS, cn=Products, cn=OracleContext] のコピーが格納されます。
- メタデータのバックアップに成功した場合、次のメッセージが端末に表示されます。

```
Backup of metadata will be stored in
$ORACLE_HOME/ldap/log/ocbkup.consumer_replica_id.TO.supplier_replicaid.timestamp.dat.
Metadata copied successfully.
```

このメッセージには、ORACLE_HOME の実際のパスとファイル名が含まれます。

メタデータのバックアップに失敗した場合、$ORACLE_HOME/ldap/log/remtool.log ファイルにエラー・メッセージが記録されます。remtool を端末から起動した場合は、その端末にエラー・メッセージが表示されます。

タスク 3: サプライヤ側のディレクトリ・サーバーの読取り専用モードへの切替え データ整合性を保証するために、サプライヤ・ノードのディレクトリ・サーバーを読取り専用モードに切り替えます。これは、次の手順に従って行います。

1. LDIF ファイルを作成します。このファイルの内容は次のとおりです。

```
Dn:
Changetype: modify
Replace: orclservermode
Orclservermode: r
```

2. サプライヤ側で、次のコマンドを実行します。

```
ldapmodify –D "cn=orcladmin" –w administrator_password \
           –h host_name_of_supplier_node –p port –f name_of_LDIF_file.ldif
```

タスク 4: レプリケーション環境管理ツールを使用した LDAP ベースのレプリカの追加 レプリカを追加するには、コンシューマ・レプリカで次のように入力します。

```
remtool -paddnode [-v] [-bind supplier_host_name:port/replication_dn_password]
```

remtool ユーティリティから承諾のタイプの指定を求められます。追加するレプリカのタイプに応じて、一方向 LDAP または双方向 LDAP のいずれかを選択します。

> **関連資料：** レプリケーション環境管理ツールの詳細は、『Oracle Identity Management ユーザー・リファレンス』の remtool コマンドライン・ツールのリファレンスを参照してください。

タスク 5: レプリケートするネーミング・コンテキストのバックアップ LDAP ベースのレプリカにレプリケートするエントリが、ネーミング・コンテキスト内に大量にある場合は、サプライヤ・ノードでこれらのネーミング・コンテキストをバックアップし、それを LDAP ベースのレプリカにロードすることをお薦めします。

ネーミング・コンテキストをバックアップする手順は、次のとおりです。

1. 30-29 ページの「タスク 4: レプリケーション環境管理ツールを使用した LDAP ベースのレプリカの追加」で作成したレプリケーション承諾識別名を確認します。

```
ldapsearch -h supplier_host -p port \
           -b "orclreplicaid=supplier_replicaID,cn=replication configuration" \
           -s sub "(orclreplicadn= orclreplicaid=consumer_replica_ID, \
                    cn=replication configuration)" dn
```

2. サプライヤ側で、次のコマンドを使用してサプライヤからデータを取得します。ファイルにロードされたデータは、構成済の承諾に基づきます。

```
ldifwrite connect="connect_string_of_sponsor_node" \
          basedn="replication_agreement_dn_retrieved_in_step_1" \
          file="name_of_output_LDIF_file"
```

関連資料 :

30-34 ページの「LDAP ベースの部分レプリケーションでのレプリケート対象の決定」

ldifwrite を使用してネーミング・コンテキストの一部をバックアップする方法は、『Oracle Identity Management ユーザー・リファレンス』の `ldifwrite` コマンドライン・ツールのリファレンスを参照してください。

タスク 6: サプライヤ側のディレクトリ・サーバーの読取り / 書込みモードへの切替え

30-29 ページの「タスク 3: サプライヤ側のディレクトリ・サーバーの読取り専用モードへの切替え」を実行した場合は、サプライヤ側のディレクトリ・サーバーを読取り / 書込みモードに戻します。これは、次の手順に従って行います。

1. LDIF ファイルを作成します。このファイルの内容は次のとおりです。

```
Dn:
Changetype: modify
Replace: orclservermode
Orclservermode: rw
```

2. 次のコマンドを実行します。

```
ldapmodify -D "cn=orcladmin" -w administrator_password \
           -h host_name_of_supplier_node -p port -f name_of_LDIF_file
```

タスク 7: 新規コンシューマへのデータのロード これは、次の手順に従って行います。

1. 複数のファイルがある場合は、たとえば、`backup_data.ldif` などの 1 つのファイルにまとめます。

2. LDAP ベースのコンシューマ・レプリカにネーミング・コンテキストがある場合は、bulkdelete を使用して削除します。次のように入力します。

```
bulkdelete connect="connect_string_of_replica" basedn="naming_context"
```

30-30 ページの「タスク 5: レプリケートするネーミング・コンテキストのバックアップ」でバックアップした各ネーミング・コンテキストについて、この手順を実行します。

コンシューマ側で、bulkload を追加モードで使用してデータをレプリカにロードします。次のように入力します。

```
bulkload connect="connect_string_of_replica" append="TRUE" check="TRUE" \
   generate="TRUE" restore="TRUE" file="backup_data.ldif"
bulkload connect="connect_string_of_replica" load="TRUE"
```

注意： Oracle Internet Directory の旧リリース（10*g* リリース 2（10.1.2.0.2）など）のデータを、10*g*（10.1.4.0.1）が稼働しているノードにロードする場合、パスワード・ポリシー・エントリを、30-32 ページの「パスワード・ポリシーとファンアウト・レプリケーション」で説明しているように更新する必要があります。

関連資料：

- デフォルト・モードまたは追加モードで bulkload を使用する方法は、『Oracle Identity Management ユーザー・リファレンス』の `bulkload` コマンドライン・ツールのリファレンスを参照してください。
- 『Oracle Identity Management ユーザー・リファレンス』の `bulkdelete` コマンドライン・ツールのリファレンス

タスク 8: 新規ノードに DAS または SSO がインストールされている場合、新規ノードのディレクトリ内のエントリをリストア 30-26 ページの「タスク 8: 新規ノードに DAS または SSO がインストールされている場合、新規ノードのディレクトリ内のエントリをリストア」に記載されている手順に従います。

タスク 9: オプション : デフォルトのレプリケーション・パラメータの変更 レプリケーション承諾、レプリカ・サブエントリ、およびレプリケーション・ネーミング・コンテキスト構成オブジェクトのデフォルトのパラメータを変更できます。

関連項目：

- 31-2 ページの「ディレクトリ・レプリケーション・サーバーの構成パラメータの表示および変更」
- 31-4 ページの「特定のレプリカ・ノードについてのパラメータの表示および変更」
- 31-6 ページの「レプリケーション承諾のパラメータの変更」
- 29-10 ページの「ディレクトリ内のレプリケーション構成オブジェクト」
- 30-34 ページの「LDAP ベースの部分レプリケーションでのレプリケート対象の決定」

タスク 10: ディレクトリ・レプリケーション・サーバーの起動の確認 レプリケーション・サーバーを起動する正確な手順は、サーバーが一方向レプリカまたは双方向レプリカのいずれにあるのかによって異なります。

- 一方向 LDAP レプリケーションの場合は、コンシューマでレプリケーション・サーバーを起動する必要があります。次のように入力します。

```
oidctl server=oidrepld connect=connect_string_of_consumer_replica \
   instance=instance_number_of _consumer_replica  \
   flags= "-p port_of_oid_server_running_at_consumer_replica \
           -h hostname_of_consumer_replica -m false" start
```

一方向 LDAP レプリケーションのために、コンシューマで Oracle Internet Directory レプリケーション・サーバーを起動する際には、`-m false` オプションの使用をお薦めします。これにより競合解消が無効になり、パフォーマンスが向上します。

- 双方向 LDAP レプリケーションの場合は、スポンサ・レプリカと新規レプリカの両方で、Oracle Internet Directory レプリケーション・サーバーを次のように起動する必要があります。

  1. スポンサ・レプリカでレプリケーションを起動または再起動します。次のように入力します。

     ```
     oidctl server=oidrepld connect=connect_string_of_sponsor_replica \
        instance=instance_number_of_sponsor_replica \
        flags= "-p port_of_oid_server_running_at_sponsor_replica
                -h hostname_of_sponsor_replica" start
     ```

  2. 新規レプリカでレプリケーション・サーバーを起動します。次のように入力します。

     ```
     oidctl server=oidrepld connect=connect_string_of_consumer_replica \
         instance=instance_number_of_consumer_replica \
         flags="-p port_of_oid_server_running_at_new_replica  \
                 -h hostname_of_consumer_replica"
     ```

     関連資料 :『Oracle Identity Management ユーザー・リファレンス』の oidctl コマンドライン・ツールのリファレンス

パスワード・ポリシーとファンアウト・レプリケーション

10*g*（10.1.4.0.1）では、Oracle Internet Directory は旧リリースより細かいパスワード・ポリシーをサポートしています。このため、マスター・ノードが旧リリース（10*g* リリース 2（10.1.2.0.2）など）で、新規のファンアウト・ノードが 10*g*（10.1.4.0.1）の場合、問題が発生する可能性があります。マスター・ノードのパスワード・ポリシー・エントリは、ブートストラップやファンアウト・ノードへの移行の際に、予想どおりに動作しない場合があります。この問題を解決するには、ファンアウト・ノードの設定の一部として、マスターのデータをブートストラップするか移行した後、Java クラス oracle.ldap.oidinstall.backend.OIDUpgradePasswordPolicies を起動することにより、パスワード・ポリシー・エントリを更新する必要があります。コマンドライン構文は次のとおりです。

```
java –cp oracle_home/ldap/lib/oidca.jar:oracle_home/ldap/jlib/ldapjclnt10.jar
oracle.ldap.oidinstall.backend.OIDUpgradePasswordPolicies host port bindDN bindPassword
oracle_home[protocol]
```

表 30-2 に、コマンドラインのパラメータを示します。

表 30-2 OIDUpgradePasswordPolicies に対するコマンドライン・パラメータ

パラメータ	説明
host	10*g*（10.1.4.0.1）ディレクトリ・サーバーが稼働しているホスト。
port	10*g*（10.1.4.0.1）ディレクトリ・サーバーがリスニングを行っているポート。プロトコルが ssl の場合、port は SSL ポートであることが必要です。
bindDN	権限を持つ管理ユーザーは通常 cn=orcladmin。
bindPwd	bindDN に関連付けられたユーザー・パスワード。
oracle_home	Oracle Internet Directory のこのインスタンスの Oracle ホーム。
protocol	オプション・パラメータ。SSL 環境では ssl に設定します。

ツールにより実行されるアクションはすべて、*oracle_home*\ldap\log ディレクトリにある ppUpgrade.log に記録されます。

注意： ツールを実行する前に、該当する環境変数が正しく設定されていることを確認します。

- Linux や Solaris では、`LD_LIBRARY_PATH` 変数には、*oracle_home*`\lib` と *oracle_home*`\network\lib` が含まれている必要があります。
- 64 ビット Solaris では、`LD_LIBRARY_PATH` 変数には、*oracle_home*`\lib32` と *oracle_home*`\network\lib32` が含まれている必要があります。
- Windows では、`PATH` 変数には、*oracle_home*`¥bin` と *oracle_home*`¥network¥bin` が含まれている必要があります。

関連項目： 第 19 章「Oracle Internet Directory のパスワード・ポリシー」

LDAP ベースのレプリカの削除

この項では、LDAP ベースのレプリカの削除方法を説明します。この項の項目は次のとおりです。

- タスク 1: 削除するノードでのディレクトリ・レプリケーション・サーバーの停止
- タスク 2: レプリケーション・グループからのレプリカの削除
- タスク 3: 削除するノードでのディレクトリ・サーバーの停止

注意： 別のレプリカのサプライヤになっているレプリカは、削除できません。このようなレプリカを削除するには、先にそのすべてのコンシューマをレプリケーション・グループから削除する必要があります。

タスク 1: 削除するノードでのディレクトリ・レプリケーション・サーバーの停止

『Oracle Identity Management ユーザー・リファレンス』の `oidctl` コマンドライン・ツールのリファレンスで説明されている手順に従って、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。

タスク 2: レプリケーション・グループからのレプリカの削除

このタスクは、レプリケーション環境管理ツールを使用して行います。次のように入力します。

```
remtool -pdelnode [-v] [-bind hostname:port_number/replication_dn_password]
```

関連資料：『Oracle Identity Management ユーザー・リファレンス』の `remtool` コマンドライン・ツールのリファレンス

タスク 3: 削除するノードでのディレクトリ・サーバーの停止

関連資料：『Oracle Identity Management ユーザー・リファレンス』の `oidctl` コマンドライン・ツールのリファレンス

LDAP ベースの部分レプリケーションでのレプリケート対象の決定

LDAP ベースの部分レプリケーションでは、レプリカのネーミング・コンテキスト・オブジェクトを定義することにより、レプリケートするものとしないものを決めることができます。これらのオブジェクトのパラメータは、次の識別名を持つエントリに格納されます。

```
cn=namingcontext_ID,cn=replication namecontext,
 orclAgreementID=numeric_identifier_of_replication_agreement,
 orclReplicaId=unique_identifier_of_replica, cn=replication configuration
```

注意 : ディレクトリ・レプリケーション・サーバーは、レプリカのネーミング・コンテキスト・オブジェクトを、サプライヤ側にある承諾から読み込むため、すべての変更をサプライヤ側およびコンシューマ側（オプション）のネーミング・コンテキスト・オブジェクトに適用する必要があります。

Oracle Directory Manager を使用したレプリカのネーミング・コンテキスト・オブジェクトの表示と変更

レプリカのネーミング・コンテキスト・オブジェクトのパラメータを表示および変更する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」、「**レプリケーション管理**」、「**レプリカ・ノード : < レプリカ識別子 >**」、「**レプリカ承諾 : < レプリケーション承諾識別子 >**」の順に展開します。
2. 変更するレプリカのネーミング・コンテキストを選択します。「**レプリカのネーミング・コンテキスト**」タブ・ページが右側のペインに表示されます。このタブ・ページのフィールドの説明は、表 A-24「「レプリカ承諾」の「レプリカのネーミング・コンテキスト」タブ・ページのフィールド」を参照してください。
3. 適切な情報を入力した後、「**OK**」を選択します。

Oracle Directory Manager を使用したレプリカのネーミング・コンテキスト・オブジェクトの追加

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」、「**レプリケーション管理**」、「**レプリカ・ノード : < レプリカ識別子 >**」、「**レプリカ承諾 : < レプリケーション承諾識別子 >**」の順に展開します。
2. 「**ネーミング・コンテキスト : < ネーミング・コンテキストの識別子 >**」を選択します。
3. ツールバーの「作成」ボタンを選択します。「新しいレプリカ承諾のネーミング・コンテキスト」ダイアログ・ボックスが表示されます。
4. 「新しいレプリカ承諾のネーミング・コンテキスト」ダイアログ・ボックスのフィールドに、適切な情報を入力します。このダイアログ・ボックスのフィールドの説明は、表 A-24「「レプリカ承諾」の「レプリカのネーミング・コンテキスト」タブ・ページのフィールド」を参照してください。
5. 「OK」を選択します。

Oracle Directory Manager を使用したレプリカのネーミング・コンテキスト・オブジェクトの削除

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「**< ディレクトリ・サーバー・インスタンス >**」、「**レプリケーション管理**」、「**レプリカ・ノード : < レプリカ識別子 >**」、「**レプリカ承諾 : < レプリケーション承諾識別子 >**」の順に展開します。
2. 「**ネーミング・コンテキスト : < ネーミング・コンテキストの識別子 >**」を右クリックします。
3. 「**削除**」を選択します。

ldapmodify を使用したレプリカのネーミング・コンテキスト・オブジェクト・パラメータの変更

レプリカのネーミング・コンテキスト・オブジェクト・パラメータとその説明は、『Oracle Identity Management ユーザー・リファレンス』のレプリケーションのスキーマ要素に関する項を参照してください。

> **注意 :** レプリケーション・サーバーは、サプライヤ・レプリカからネーミング・コンテキスト・オブジェクトを読み取ります。

例 30-1 LDAP ベースのレプリカのネーミング・コンテキスト・オブジェクトの追加

この例では、次の処理を行うネーミング・コンテキスト・オブジェクトを作成します。

- ou=Americas,cn=mycompany ネーミング・コンテキストをレプリケート
- レプリケーションから cn=customer profile, ou=Americas,cn=mycompany ネーミング・コンテキストを除外
- レプリケーションから userpassword 属性を除外

手順は、次のとおりです。

1. サンプル・ファイル mod.ldif を、次のように編集します。

```
dn: cn=naming_context_identifier, cn=replication  namecontext,
 orclagreementid=replication_agreement_identifier,
 orclreplicaid=supplier_replica_identifier,cn=replication configuration
orclincludednamingcontexts: ou=Americas,cn=mycompany
orclexcludednamingcontexts: cn=customer profile, ou=Americas, cn=mycompany
orclexcludedattributes: userpassword
objectclass: top
objectclass: orclreplnamectxconfig
```

2. ldapadd を使用して、部分レプリケーションのネーミング・コンテキスト・オブジェクトをサプライヤに追加します。

```
ldapadd -D "cn=orcladmin" -w administrator_password -h supplier_host \
        -p port_number -f mod.ldif
```

例 30-2 ネーミング・コンテキスト・オブジェクトの削除

例 30-1 で作成したネーミング・コンテキスト・オブジェクトを削除するには、次のように入力します。

```
ldapdelete -D "cn=orcladmin" -w administrator_password \
           -h supplier_host -p supplier_host_port_number \
           "cn=naming_context_identifier, cn=replication namecontext, \
            orclagreementid=replication_agreement_identifier, \
            orclreplicaid=supplier_replica_identifier, \
            cn=replication configuration"
```

例 30-3 レプリカのネーミング・コンテキスト・オブジェクトの orclIncludedNamingContexts 属性の変更

ディレクトリ・レプリケーション・サーバーは、レプリカのネーミング・コンテキスト・オブジェクトの orclIncludedNamingcontexts 属性の値を使用して、部分レプリケーションに含める最上位サブツリーを指定します。

この例では、含める対象ネーミング・コンテキストが c=us に設定されます。これは、c=us が部分レプリケーションに含められることを意味しています。

1. サンプル・ファイル mod.ldif を、次のように編集します。

```
DN:cn=naming_context_identifier,cn=replication namecontext,
 orclagreementid=replication_agreement_identifier,
 orclreplicaid=supplier_replica_identifier,cn=replication configuration
Changetype:modify
Replace: orclIncludedNamingcontexts
orclIncludedNamingcontexts: c=us
```

2. ldapmodify を使用して、レプリケーション承諾の orclupdateschedule 属性を更新します。

```
ldapmodify -D "cn=orcladmin" -w administrator_password -h supplier_host \
           -p port -f mod.ldif
```

3. ディレクトリ・レプリケーション・サーバーを再起動します。

例 30-4 レプリカのネーミング・コンテキスト・オブジェクトの orclExcludedNamingContexts 属性の変更

ディレクトリ・レプリケーション・サーバーは、レプリカのネーミング・コンテキスト・オブジェクトの orclExcludedNamingcontexts 属性の値を使用して、部分レプリケーションから除外する最上位サブツリーを指定します。

この例では、除外対象ネーミング・コンテキストが ou=Europe,c=us および ou=Americas,c=us に設定されます。これは、この 2 つのネーミング・コンテキストが部分レプリケーションから除外されることを意味しています。

1. サンプル・ファイル mod.ldif を、次のように編集します。

```
DN:cn=naming_context_identifier,
 cn=replication namecontext,
 orclagreementid=replication_agreement_identifier,
 orclreplicaid=supplier_replica_identifier,cn=replication configuration
Changetype:modify
Replace: orclExcludedNamingcontexts
orclExcludedNamingcontexts: ou=Europe, c=us
orclExcludedNamingcontexts: ou=Americas, c=us
```

2. ldapmodify を使用して、レプリケーション承諾の orclupdateschedule 属性を更新します。

```
ldapmodify -D "cn=orcladmin" -w administrator_password \
           -h supplier_host -p port -f mod.ldif
```

3. ディレクトリ・レプリケーション・サーバーを再起動します。

注意： orclexcludednamingcontexts 属性に指定されたサブツリーは、同一レプリカのネーミング・コンテキスト・オブジェクトで指定される includednamingcontext のサブツリーである必要があります。

例 30-5 レプリカのネーミング・コンテキスト・オブジェクトの orclExcludedAttributes 属性の変更

含めるネーミング・コンテキストに加えられた特定の変更を、属性レベルで部分レプリケーションから除外するように指定できます。ディレクトリ・レプリケーション・サーバーは、レプリカのネーミング・コンテキスト・オブジェクトの orclExcludedAttributes 属性の値を使用して、除外する属性を判別します。

この例では、orclincludednamingcontexts 属性に指定された `telephonenumber` 属性および `title` 属性が、レプリケーションから除外されます。

1. サンプル・ファイル `mod.ldif` を、次のように編集します。

```
DN:cn=naming_context_identifier,
 cn=replication namecontext,
 orclagreementid=replication_agreement_identifier,
 orclreplicaid=supplier_replica_identifier,cn=replication configuration
Changetype:modify
Replace: orclExcludedAttributes
orclExcludedAttributes: telephonenumber
orclExcludedAttributes: title
```

2. ldapmodify を使用して、レプリケーション承諾の orclupdateschedule 属性を更新します。

```
ldapmodify -D "cn=orcladmin" -w administrator_password -h my_host \
           -p port -f mod.ldif
```

3. ディレクトリ・レプリケーション・サーバーを再起動します。

手動でのレプリケーション・グループ内の競合の解消

この項の項目は次のとおりです。

レプリケーション変更の競合の監視

競合がログに書き込まれた場合、それは、システムに備わった解消手順では競合を解消できないということを意味します。以前に適用されなかった変更によって新しいレプリケーション変更の競合が発生することを防止するために、ログを定期的に監視することが重要です。

レプリケーション変更の競合を監視するには、レプリケーション・ログの内容を検証します。それぞれに付加されているタイムスタンプによって、各メッセージを識別できます。

競合解消メッセージの例

競合解消メッセージは、ファイル oidrepld00.log に記録されます。この項ではメッセージの例を示します。このファイルのパスは、$ORACLE_HOME/ldap/log です。レプリケーション競合の解消を試みた結果は、各競合解消メッセージの最後に記述されています。

例 30-6 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 30-7 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 30-8 存在しないエントリを削除しようとした場合

```
2000/08/03::10:59:06:  ************ Conflict Resolution Message ************
2000/08/03::10:59:06:  Conflict reason: Attempted to delete a non-existent entry.
2000/08/03::10:59:06:  Change number:1365.
2000/08/03::10:59:06:  Supplier:eastlab-sun.
2000/08/03::10:59:06:  Change type:Delete.
2000/08/03::10:59:06:  Target DN:cn=Lou Smith,ou=recruiting,ou=hr,ou=americas,o=imc,c=us.
2000/08/03::10:59:06:  Result: Change moved to low priority queue after failing on 10th
retry.
```

管理者操作キュー操作ツールの概要

管理者操作キュー操作ツールを使用すると、変更を管理者操作キューからリトライ・キューまたはパージ・キューへ移動できます。パージ・キューへの変更の移動は、ログ・エントリに対する変更の再適用を以降は試みないということを意味します。管理者操作キューの変更を処理するには、次の一般的な手順を実行してください。

1. ディレクトリ・レプリケーション・サーバーを停止します。
2. レプリケーション・ログを分析します。
3. 管理者操作キュー操作ツールを使用して、変更をリトライ・キューまたはパージ・キューへ移動します。詳細は、次項を参照してください。

注意： Oracle Internet Directory サーバーのパラメータ orclSizeLimit（デフォルト値は 1000）は、管理者操作キュー操作ツールが処理できるエントリ数を制限します。管理者操作キューのエントリ数が 1,000 を超える場合は、orclSizeLimit の値を大きくする必要があります。このパラメータ値を大きくしないと一部のエントリが処理されません。ただし、orclSizeLimit パラメータの設定値を大きくしすぎるとサーバーのパフォーマンスに影響を与えます。これは orclSizeLimit が、検索時に返されるエントリの最大数も制御するためです。

関連資料 : 管理者操作キュー操作ツールの使用方法は、『Oracle Identity Management ユーザー・リファレンス』の `hiqretry.sh` コマンドライン・ツールのリファレンスを参照してください。

Oracle Internet Directory 比較調整ツールの概要

ディレクトリ・レプリケーション・サーバーが一貫性のないデータを検出した場合、Oracle Internet Directory 比較調整ツールを使用して、コンシューマのエントリをサプライヤのエントリと同期化させることができます。その場合、次の一般的な手順を実行します。

1. サプライヤとコンシューマを、読取り専用モードに設定します。
2. サプライヤとコンシューマが安定した状態、つまり変更の供給も適用も行っていない状態にあることを確認します。安定した状態にない場合は、更新が完了するまで待ちます。
3. コンシューマ上の一貫性のないエントリまたはサブツリーを識別します。
4. Oracle Internet Directory 比較調整ツールを使用して、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。

関連資料 :

- ノードを読取り専用モードに設定する方法は、「タスク 3: スポンサ・ノードの読取り専用モードへの切替え」を参照してください。
- Oracle Internet Directory 比較調整ツールの構文と動作の説明は、『Oracle Identity Management ユーザー・リファレンス』の `oidcmprec` コマンドライン・ツールのリファレンスを参照してください。

例 : ファンアウトと組み合せたマルチマスター・レプリケーション・グループのインストールおよび構成

この項では、ファンアウトと組み合せたマルチマスター・レプリケーション・グループのインストールおよび構成を、表 30-3 に示す 4 つのシステムを使用した例で説明します。

表 30-3 部分レプリケーション配置例におけるノード

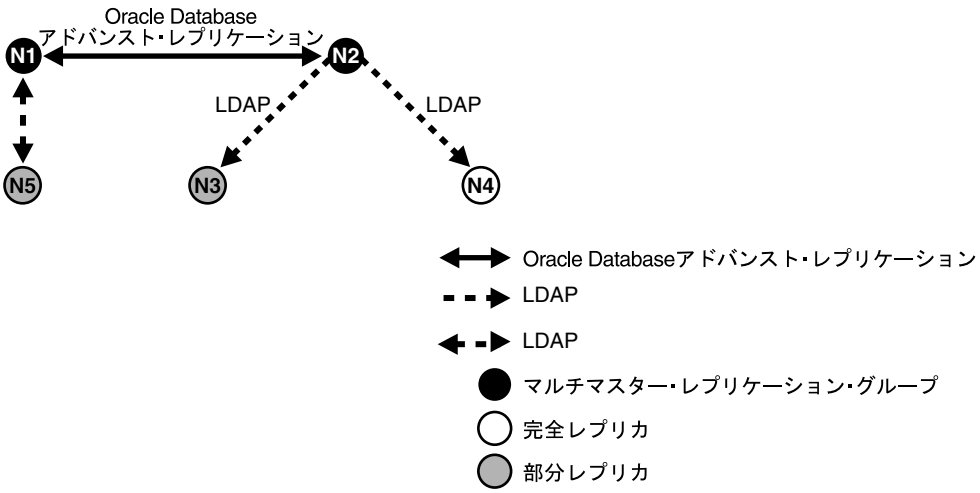
ノード	ホスト名	ポート
ノード 1	mycompany1.com	3000
ノード 2	mycompany2.com	4000
ノード 3	mycompany3.com	5000
ノード 4	mycompany4.com	6000
ノート 5	mycompany5.com	7000

この例では、ユーザーが次の要件に従って設定を済ませています。

- **要件 1:** いずれかのノードに加えられた変更が他のノードにレプリケートされるように、ノード 1 とノード 2 とを同期させる必要がありますが、ネーミング・コンテキスト `cn=private users, cn=mycompany` は、このレプリケーションから除外されます。
- **要件 2:** ノード 2 の `ou=Americas, cn=mycompany` の下で行われた変更のみがノード 3 にレプリケートされるように、ノード 3 のネーミング・コンテキスト `ou=Americas,cn=mycompany` は、ノード 2 から部分的に同期させます。このレプリケーションから除外される変更を、次に示します。
  - `cn=customer profile, ou=Americas, cn=mycompany` の下で行われた変更
  - `userpassword` 属性に加えられた変更

- **要件 3:** ノード 4 は、ノード 2 の完全なレプリカとして構成します。つまり、ノード 2 のすべてのネーミング・コンテキストに対する変更がノード 4 に（一方向でのみ）レプリケートされます。
- **要件 4:** ノード 5 は、ノード 1 の双方向（更新可能）の完全なレプリカとして構成します。

図 30-1 ファンアウト・レプリケーションの例



この例の 1 つ目の要件を満たすために、マルチマスター・レプリケーション・グループをノード 1 およびノード 2 について設定します。2 つ目の要件を満たすには、部分レプリカをノード 2 およびノード 3 について設定し、3 つ目の要件を満たすには、ノード 2 からノード 4 への完全な LDAP レプリケーションを設定します。

この項の項目は次のとおりです。

- タスク 1: ノード 1 およびノード 2 を対象としたマルチマスター・レプリケーション・グループの設定
- タスク 2: レプリケーション承諾の構成
- タスク 3: ノード 1 およびノード 2 でのレプリケーション・サーバーの起動
- タスク 4: ノード 1 とノード 2 間のディレクトリ・レプリケーションのテスト
- タスク 5: ノード 3 をノード 2 の部分レプリカとしてインストールし、構成
- タスク 6: 部分レプリケーション承諾のカスタマイズ
- タスク 7: DRG の全ノードでのレプリケーション・サーバーの起動
- タスク 8: ノード 4 をノード 2 の完全なレプリカとしてインストールし、構成
- タスク 9: ノード 2 からノード 4 へのレプリケーションのテスト
- タスク 10: ノード 4 をノード 2 の完全なレプリカとしてインストールし、構成
- タスク 11: ノード 1 とノード 2 間のディレクトリ・レプリケーションのテスト

タスク 1: ノード 1 およびノード 2 を対象としたマルチマスター・レプリケーション・グループの設定

ノード 1 およびノード 2 のマルチマスター・レプリケーション・グループを設定するには、30-7 ページの「マルチマスター・レプリケーション・グループのインストールと構成」に記載されているタスク 1 ～ 5 を実行します。

タスク 2: レプリケーション承諾の構成

ノード 1 とノード 2 間のレプリケーション承諾では、orclExcludedNamingcontexts 属性の値を、cn=private users,cn=mycompany として指定します。これは、次の手順に従って行います。

1. サンプル・ファイル mod.ldif を、次のように編集します。

```
dn: orclAgreementID=000001,cn=replication configuration
Changetype:modify
Replace: orclExcludedNamingcontexts
orclExcludedNamingcontexts: cn=private users,cn=mycompany
```

2. ldapmodify を使用して、ノード 1 とノード 2 のレプリケーション承諾の orclExcludedNamingcontexts 属性を更新します。この手順を実行するには、次のように入力します。

```
ldapmodify -D "cn=orcladmin" -w administrator_password -h mycompany1.com \
           -p 3000 -f mod.ldif
ldapmodify -D "cn=orcladmin" -w administrator_password -h mycompany2.com \
           -p 4000 -f mod.ldif
```

タスク 3: ノード 1 およびノード 2 でのレプリケーション・サーバーの起動

このタスクを実行するには、30-13 ページの「タスク 6: DRG の全ノードでのレプリケーション・サーバーの起動」に記載されている指示に従ってください。

タスク 4: ノード 1 とノード 2 間のディレクトリ・レプリケーションのテスト

このタスクを実行するには、30-14 ページの「タスク 7: ディレクトリ・レプリケーションのテスト」に記載されている指示に従ってください。

タスク 5: ノード 3 をノード 2 の部分レプリカとしてインストールし、構成

部分レプリケーションのブートストラップ機能を使用する場合は、「自動ブートストラップを使用した LDAP ベースのレプリカの構成」で説明したタスク 1 ～ 5 に従ってください。

ldifwrite ツールを使用してレプリカを構成する場合は、30-28 ページの「ldifwrite ツールを使用した LDAP ベースのレプリカの構成」で説明したタスク 1 ～ 9 に従ってください。

ノード 2 をサプライヤ、ノード 3 をコンシューマと指定します。

タスク 6: 部分レプリケーション承諾のカスタマイズ

これは、次の手順に従って行います。

- この例の要件 2 を満たすには、まずノード 2 とノード 3 の間にデフォルトのレプリケーションを構成する必要があります。

  部分レプリケーションでは、デフォルトでネーミング・コンテキスト cn=oraclecontext がレプリケートされます。このネーミング・コンテキストをサプライヤ（ノード 2、mycompany2.com）とコンシューマ（ノード 3、mycompany3.com）の両方で削除すれば、レプリケートされることはなくなります。

```
ldapdelete -D "cn=orcladmin" -w administrator_password -h mycompany2.com \
           -p 4000 "cn=includednamingcontext000001, \
                    cn=replication namecontext,orclagreementid=000002, \
                    orclreplicaid==node2_replica_id, \
                    cn=replication configuration"
```

```
ldapdelete -D "cn=orcladmin" -w administrator_password -h mycompany3.com \
          -p 5000 "cn=includednamingcontext000001, \
                   cn=replication namecontext,orclagreementid=000002, \
                   orclreplicaid==node2_replica_id, \
                   cn=replication configuration"
```

- ネーミング・コンテキスト ou=Americas,cn=mycompany をレプリケートし、ネーミング・コンテキスト cn=customer profile, ou=Americas, cn=mycompany および userpassword 属性をレプリケーションから除外するには、ネーミング・コンテキスト・オブジェクトを次のように作成します。

  a. サンプル・ファイル mod.ldif を、次のように編集します。

```
dn: cn=includednamingcontext000002,cn=replication namecontext,
 orclagreementid=000002,orclreplicaid=node2_replica_id,
 cn=replication configuration
orclincludednamingcontexts: ou=Americas,cn=mycompany
orclexcludednamingcontexts: cn=customer profile, ou=Americas, cn=mycompany
orclexcludedattributes: userpassword
objectclass: top
objectclass: orclreplnamectxconfig
```

  b. ldapadd を使用して、部分レプリケーションのネーミング・コンテキスト・オブジェクトをノード 2 とノード 3 の両方に追加します。

```
ldapadd -D "cn=orcladmin" -w administrator_password -h mycompany2.com \
        -p 4000 -f mod.ldif
ldapadd -D "cn=orcladmin" -w administrator_password -h mycompany3.com \
        -p 5000 -f mod.ldif
```

- 部分レプリケーションの自動ブートストラップ機能を使用する場合は、サンプル・ファイル mod.ldif を編集し、次に ldapmodify を使用して、ノード 2 とノード 3 の両方で部分レプリカの orclreplicastate 属性を変更します。詳細は、30-25 ページの「タスク 5: コンシューマ側でコンシューマ・レプリカを自動ブートストラップ用に構成」を参照してください。

タスク 7: DRG の全ノードでのレプリケーション・サーバーの起動

このタスクを実行するには、30-31 ページの「タスク 10: ディレクトリ・レプリケーション・サーバーの起動の確認」に記載されている指示に従ってください。

タスク 8: ノード 4 をノード 2 の完全なレプリカとしてインストールし、構成

完全なレプリカによるレプリケーションは、新規ノードを LDAP レプリカとしてインストールした場合のデフォルト構成です。30-21 ページの「一方向または双方向 LDAP ベース・レプリカのデフォルト設定でのインストールと構成」に記載されている指示に従ってください。サプライヤ情報の入力を求められたら、サプライヤのホスト名 mycompany2.com、サプライヤのポート 4000、およびサプライヤのユーザー・パスワードを指定します。

注意 : 30-4 ページの「Oracle Internet Directory をアドバンスト・レプリケーション・ベースのレプリカ、あるいは一方向または双方向の LDAP ベースのレプリカとしてインストールする場合」の説明に従ってノード 4 をインストールする際に、サプライヤのホスト名、ポートおよびスーパーユーザー cn=orcladmin のパスワードを指定するよう求められます。

タスク 9: ノード 2 からノード 4 へのレプリケーションのテスト

30-14 ページの「タスク 7: ディレクトリ・レプリケーションのテスト」の指示に従って、このレプリケーションをテストします。

タスク 10: ノード 4 をノード 2 の完全なレプリカとしてインストールし、構成

完全なレプリカによるレプリケーションは、新規ノードを LDAP レプリカとしてインストールした場合のデフォルト構成です。30-21 ページの「一方向または双方向 LDAP ベース・レプリカのデフォルト設定でのインストールと構成」に記載されている指示に従ってください。サプライヤ情報の入力を求められたら、サプライヤのホスト名 `mycompany1.com`、サプライヤのポート `3000`、およびサプライヤのユーザー・パスワードを指定します。

タスク 11: ノード 1 とノード 2 間のディレクトリ・レプリケーションのテスト

Oracle Directory Manager または `ldapadd` コマンドライン・ツールを使用して、ノード 1 にエントリを作成します。エントリがノード 5 でレプリケートされるのを待ちます。ノード 5 にエントリがレプリケートされたら、`ldapmodify` コマンドライン・ツールまたは Oracle Directory Manager のいずれかを使用して、ノード 5 でそのエントリに対する変更を適用します。変更はノード 1 にレプリケートされます。

レプリケーション・フェイルオーバーの構成

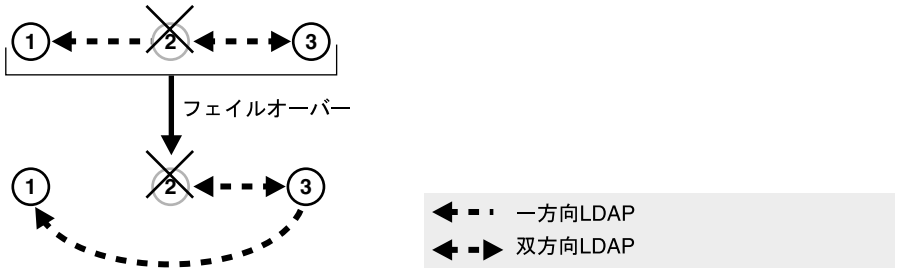
この項の項目は次のとおりです。

レプリケーション・フェイルオーバーに関する制限事項と警告

この項では、レプリケーション・フェイルオーバーの使用に関する制限事項と警告について説明します。

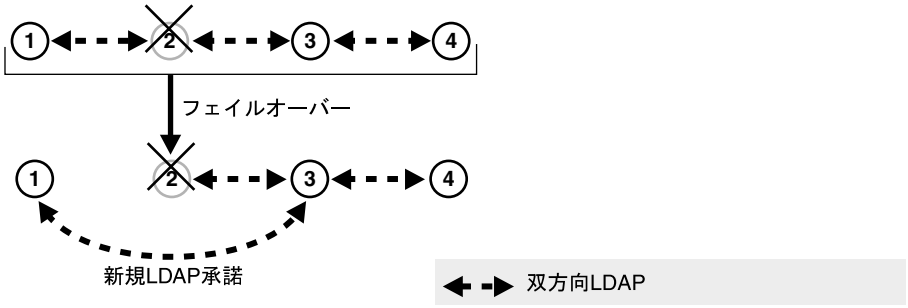
- Oracle Internet Directory 10*g*（10.1.4.0.1）では、レプリケーション・フェイルオーバーには、管理者の操作が必要です。
- フェイルオーバーの直後に、管理者はコンシューマと新規サプライヤを比較し、調整する必要があります。
- 新規の承諾は、旧承諾と同じタイプと方向のものであることが必要です。
- 2 つのトポロジ・タイプのみがサポートされています。29-27 ページの「レプリケーション・フェイルオーバー」を参照してください。
- サプライヤが機能しなくなると、直接接続しているレプリカは、同様にそのサプライヤに接続している別のレプリカに対してのみフェイルオーバーができます。
- 新規サプライヤと旧サプライヤ間の承諾のレプリケーション・フィルタリング・ポリシーは、旧サプライヤとコンシューマ間の承諾と一致させる必要があります。
- ほとんどの場合、レプリカは元のレプリカ・タイプを維持する方法でフェイルオーバーする必要があります。図 30-2 に示した例では、ノード 2 は、ノード 1 とノード 3 の両方にとっての旧サプライヤであり、ノード 1 は読取り専用です。ノード 2 が機能しなくなった場合、理論上は、ノード 1 またはノード 3 のいずれかを新しいサプライヤ・ノードとして設定できます。しかし、最良の方法は、ノード 1 をフェイルオーバーして、ノード 3 をサプライヤにすることです。この方法により、ノード 1 の元の読取り専用レプリカ・タイプが維持されます。

図 30-2 レプリカ・タイプを維持するフェイルオーバー



- 新規の承諾が双方向承諾の場合、コンシューマをその新しいサプライヤと比較し、調整した後、新しいサプライヤと接続しているその他すべてのレプリカについても、新しいサプライヤと比較し、調整する必要があります。たとえば、図 30-3 では、ノード 2 にはノード 3 との双方向承諾があります。ノード 3 は、もう 1 つのレプリカ、ノード 4 に接続しています。ノード 2 が機能しなくなると、ノード 3 とノード 1 の双方向承諾を設定します。ノード 3 をノード 1 と比較、調整した後、ノード 4 もノード 3 と比較、調整し、レプリカを確実に同期化します。

図 30-3 接続レプリカすべての比較および調整



使用するレプリケーション・フェイルオーバーのタイプの決定

レプリケーション・フェイルオーバーには 2 つのタイプがあります。次のタイプです。

- ステートレス
- 時間ベース

事前にフェイルオーバーを計画できない場合は、ステートレス・フェイルオーバーを使用します。ステートレス・レプリケーション・フェイルオーバーでは、レプリカの状態について想定は行いません。いつでも新しいサプライヤにフェイルオーバーできます。ステートレス・フェイルオーバーには、フェイルオーバー後、ノードを同期化するためにより多くの作業が必要です。

計画的なフェイルオーバーには、時間ベース・フェイルオーバーを使用します。時間ベース・フェイルオーバーは、フェイルオーバー後の作業が少なくなります。ただし、後続の想定がフェイルオーバー時に必ず当てはまるように、事前に時間を設定する必要があります。

- ノードは大部分は同期化されます。
- 新規のサプライヤは、完全な同期化がすぐに実行できるように、変更ログを保存しています。

ステートレス・レプリケーション・フェイルオーバーの実行

この項では、ステートレス・レプリケーション・フェイルオーバーの実行方法について説明します。実行には、次のタスクを行います。

- タスク 1: 関連ノードでのすべてのディレクトリ・レプリケーション・サーバーの停止
- タスク 2: 旧レプリケーション承諾の破棄と新規承諾の設定
- タスク 3: 最後に適用された変更番号の保存
- タスク 4: 新規サプライヤとコンシューマの比較および調整
- タスク 5: 新規承諾の最後に適用された変更番号の更新
- タスク 6: 旧サプライヤでの旧承諾のクリーンアップ
- タスク 7: 関連ノードでのすべてのディレクトリ・レプリケーション・サーバーの起動

タスク 1: 関連ノードでのすべてのディレクトリ・レプリケーション・サーバーの停止

新規サプライヤ、旧サプライヤおよびコンシューマ上の Oracle ディレクトリ・レプリケーション・サーバーを、次のように入力することにより停止します。

```
oidctl connect=db_connect_string server=oidrepld instance=instance_number \
   host=hostname stop
```

関連資料 :

- 第 6 章「Oracle Internet Directory のプロセス制御コンポーネント」
- 『Oracle Identity Management ユーザー・リファレンス』の `oidctl` コマンドライン・ツールのリファレンス

タスク 2: 旧レプリケーション承諾の破棄と新規承諾の設定

旧サプライヤとコンシューマ間の古いレプリケーション承諾を破棄し、新規サプライヤとコンシューマ間の新規承諾を設定します。このタスクは、レプリケーション環境管理ツールを使用して行います。次のように入力します。

```
remtool -pchgmaster [-v] [-bind consumer_host::port_number/replication_dn_password]
```

関連資料 :『Oracle Identity Management ユーザー・リファレンス』の `remtool` コマンドライン・ツールのリファレンス

タスク 3: 最後に適用された変更番号の保存

新規サプライヤから最後に適用された変更番号を取得します。

一方向承諾の場合、次のコマンドを使用します。

```
ldapsearch -h new_supplier_host -p port_number -b "" \
   -s base "objectclass=*" lastchangenumber
```

双方向承諾の場合、次のコマンドを使用します。

```
ldapsearch -h consumer_host -p port_number -b "" \
   -s base "objectclass=*" lastchangenumber
```

この番号を保存します。

タスク 4: 新規サプライヤとコンシューマの比較および調整

Oracle Internet Directory 比較調整ツールを使用して、新規サプライヤとコンシューマを比較し、調整します。一方向承諾の場合は、次のように入力します。

```
oidcmprec operation=reconcile \
   source=new_supplier_host:port/new_supplier_replication_dn_passwd \
   destination=consumer_host:port/consumer_replication_dn_passwd \
   base='""' scope=sub
```

双方向承諾の場合は、次のように入力します。

```
oidcmprec operation=merge \
   source=new_supplier_host:port/new_supplier_replication_dn_passwd \
   destination=consumer_host:port/consumer_replication_dn_passwd \
   base='""' scope=sub
```

この例では、ディレクトリ全体がレプリケートされることを想定しており、したがって、base は "" に設定されています。部分レプリケーションを使用する場合は、base 引数と dns2exclude 引数を oidcmprec ツールに使用して、希望する DIT を含めます。

> **関連資料:**『Oracle Identity Management ユーザー・リファレンス』の oidcmprec コマンドライン・ツールのリファレンス

タスク 5: 新規承諾の最後に適用された変更番号の更新

新規サプライヤ側で、検索の結果見つかった最後に適用された変更番号を使用して、新規の承諾を変更します。これは、次の手順に従って行います。

1. 「タスク 3: 最後に適用された変更番号の保存」で取得した最後に適用された変更番号により、LDIF ファイルを作成します。

   一方向承諾の場合、次のようになります。

   ```
   dn: agreement_dn
   changetype: modify
   replace: orclLastAppliedChangeNumber;apply$new_supplier_host$consumer_host
   orclLastAppliedChangeNumber;apply$new_supplier_host$consumer_host:
    last_change_number_retrieved.
   -
   replace: orclLastAppliedChangeNumber;transport$new_supplier_host$consumer_host
   orclLastAppliedChangeNumber;transport$new_supplier_host$consumer_host:
    last_change_number_retrieved_from_new_supplier
   ```

   双方向承諾の場合、次のようになります。

   ```
   dn: agreement_dn
   changetype: modify
   replace: orclLastAppliedChangeNumber;apply$new_supplier_host$consumer_host
   orclLastAppliedChangeNumber;apply$new_supplier_host$consumer_host:
    last_change_number_retrieved_from_new_supplier
   -
   replace: orclLastAppliedChangeNumber;transport$new_supplier$consumer
   orclLastAppliedChangeNumber;transport$new_supplier$consumer:
    last_change_number_retrieved_from_new_supplier
   -
   replace: orclLastAppliedChangeNumber;apply$consumer_host$new_supplier_host
   orclLastAppliedChangeNumber;apply$consumer_host$new_supplier_host:
    last_change_number_retrieved_from_consumer
   -
   replace: orclLastAppliedChangeNumber;transport$consumer_host$new_supplier_host
   orclLastAppliedChangeNumber;transport$consumer_host$new_supplier_host:
    last_change_number_retrieved_from_consumer
   ```

2. ldapmodify を使用して承諾を変更する方法は次のとおりです。

   ```
   ldapmodify -D "cn=orcladmin" -w password -h host_name -p port_number \
      -f LDIF_file
   ```

タスク 6: 旧サプライヤでの旧承諾のクリーンアップ

「タスク 2: 旧レプリケーション承諾の破棄と新規承諾の設定」の実行時に旧サプライヤが停止した場合、旧サプライヤ上の旧承諾はクリーンアップされません。ここで、レプリケーション環境管理ツールを使用して、これをクリーンアップします。次のように入力します。

```
remtool -pcleanup -agrmt [-v] [-bind
consumer_host::port_number/replication_dn_password]
```

関連資料:『Oracle Identity Management ユーザー・リファレンス』の `remtool` コマンドライン・ツールのリファレンス

タスク 7: 関連ノードでのすべてのディレクトリ・レプリケーション・サーバーの起動

新規サプライヤ、旧サプライヤおよびコンシューマ上の Oracle ディレクトリ・レプリケーション・サーバーを、次のように入力することにより起動します。

```
oidctl connect=db_connect_string server=oidrepld instance=instance_number \
    host=hostname flags='-p port_number' start
```

関連資料:

- 第 6 章「Oracle Internet Directory のプロセス制御コンポーネント」
- 『Oracle Identity Management ユーザー・リファレンス』の `oidctl` コマンドライン・ツールのリファレンス

時間ベース・レプリケーション・フェイルオーバーの実行

この項では、時間ベース・レプリケーション・フェイルオーバーの実行方法について説明します。この項の項目は次のとおりです。

- タスク 1: 新規サプライヤでの変更ログ・ガベージ・コレクションの構成
- タスク 2: 新規サプライヤの最後に適用された変更番号の保存
- タスク 3: 新規サプライヤでの変更ログ・レプリケーションの有効化
- タスク 4: 希望する期間が経過するのを待機
- タスク 5: 関連ノードでのすべてのディレクトリ・レプリケーション・サーバーの停止
- タスク 6: 旧レプリケーション承諾の破棄と新規承諾の設定
- タスク 7: 新規承諾の最後に適用された変更番号の更新
- タスク 8: 旧サプライヤでの旧承諾のクリーンアップ
- タスク 9: 関連ノードでのすべてのディレクトリ・レプリケーション・サーバーの起動

タスク 1: 新規サプライヤでの変更ログ・ガベージ・コレクションの構成

新規サプライヤ上で、希望する期間（たとえば、24 時間）の変更ログを保存するように変更ログ削除構成エントリを構成する手順は、次のとおりです。

1. 次のような LDIF ファイルを作成します。

   ```
   dn: cn=changelog purgeconfig,cn=purgeconfig,cn=subconfigsubentry
   changetype:modify
   replace: orclpurgetargetage
   orclpurgetargetage: 24
   ```

2. LDIF ファイルを適用するために、次のように入力します。

   ```
   ldapmodify -p port -h host -D dn -w password -f LDIF_file
   ```

関連項目: 第 26 章「Oracle Internet Directory におけるガベージ・コレクション」

タスク 2: 新規サプライヤの最後に適用された変更番号の保存

新規サプライヤから最後に適用された変更番号を、次のように取得します。

```
ldapsearch -h new_supplier_host -p port_number -D cn=orcladmin -w admin_pwd \
   -b "" -s base "objectclass=*" lastchangenumber
```

この番号を保存します。

タスク 3: 新規サプライヤでの変更ログ・レプリケーションの有効化

新規サプライヤで変更ログ・レプリケーションを、次のようにして有効化します。

1. 次のような LDIF ファイルを作成します。

   ```
   dn:
   changetype: modify
   replace: orcldiprepository
   orcldiprepository: TRUE
   ```

2. LDIF ファイルを適用するために、次のように入力します。

   ```
   ldapmodify -D "cn=orcladmin" -w password -h host_name -p port_number \
      -f LDIF_file
   ```

タスク 4: 希望する期間が経過するのを待機

変更ログ削除構成エントリの `orclpurgetargetage` の値より短い期間を待ちます。

タスク 5: 関連ノードでのすべてのディレクトリ・レプリケーション・サーバーの停止

新規サプライヤ、旧サプライヤおよびコンシューマ上の Oracle ディレクトリ・レプリケーション・サーバーを、次のように入力することにより停止します。

```
oidctl connect=db_connect_string server=oidrepld instance=instance_number host=hostname
stop
```

関連資料 :

- 第 6 章「Oracle Internet Directory のプロセス制御コンポーネント」
- 『Oracle Identity Management ユーザー・リファレンス』の `oidctl` コマンドライン・ツールのリファレンス

タスク 6: 旧レプリケーション承諾の破棄と新規承諾の設定

旧サプライヤとコンシューマ間の古いレプリケーション承諾を破棄し、新規サプライヤとコンシューマ間の新規承諾を設定します。このタスクは、レプリケーション環境管理ツールを次のように使用して行います。

```
remtool -pchgmaster [-v] [-bind hostname:port_number/replication_dn_password]
```

関連資料 :『Oracle Identity Management ユーザー・リファレンス』の `remtool` コマンドライン・ツールのリファレンス

タスク 7: 新規承諾の最後に適用された変更番号の更新

新規サプライヤで、最後に適用された変更番号が、「タスク 2: 新規サプライヤの最後に適用された変更番号の保存」で取得した値になるように、次のように新規承諾変更します。

1. 取得した最後に適用された変更番号を使用して、次のような LDIF ファイルを作成します。

```
dn: agreement_dn
changetype: modify
replace: orclLastAppliedChangeNumber
orclLastAppliedChangeNumber: last_change_number_retrieved
```

2. `ldapmodify` を使用して、LDIF ファイルを承諾に適用します。

```
ldapmodify -D "cn=orcladmin" -w password -h host_name -p port_number \
-f LDIF_file
```

タスク 8: 旧サプライヤでの旧承諾のクリーンアップ

「タスク 6: 旧レプリケーション承諾の破棄と新規承諾の設定」の実行時に旧サプライヤが停止した場合、旧サプライヤ上の旧承諾はクリーンアップされません。ここで、レプリケーション環境管理ツールを使用して、これをクリーンアップします。次のように入力します。

```
remtool -pcleanup -agrmt [-v] [-bind hostname:port_number/replication_dn_password]
```

関連資料:『Oracle Identity Management ユーザー・リファレンス』の `remtool` コマンドライン・ツールのリファレンス

タスク 9: 関連ノードでのすべてのディレクトリ・レプリケーション・サーバーの起動

新規サプライヤ、旧サプライヤおよびコンシューマ上の Oracle ディレクトリ・レプリケーション・サーバーを、次のように入力することにより起動します。

```
oidctl connect=db_connect_string server=oidrepld instance=instance_number host=hostname
start
```

関連資料:

- 第 6 章「Oracle Internet Directory のプロセス制御コンポーネント」
- 『Oracle Identity Management ユーザー・リファレンス』の `oidctl` コマンドライン・ツールのリファレンス

31

Oracle Internet Directory レプリケーションの監視および管理

この章では、Oracle Internet Directory のレプリケーションの監視および管理方法を説明します。

レプリケーションのインストールおよび構成後は、レプリケーションに関連するオブジェクトのデフォルト値を表示または変更できます。この項の項目は次のとおりです。

- ディレクトリ・レプリケーション・サーバーの構成パラメータの表示および変更
- 特定のレプリカ・ノードについてのパラメータの表示および変更
- レプリケーション承諾のパラメータの変更
- Oracle Database アドバンスト・レプリケーションを使用した、全ノードでのレプリケーション管理者パスワードの変更
- 変更ログの管理
- ディレクトリ・レプリケーションの速度変更
- トポロジの管理および監視
- 比較調整ツール

関連項目：

- 29-11 ページの「レプリケーション承諾エントリ」
- 29-10 ページの「レプリカ・サブエントリ」

注意： レプリケーション・サーバーを再起動するまで、構成パラメータまたはレプリケーション承諾への変更は有効になりません。

ディレクトリ・レプリケーション・サーバーの構成パラメータの表示および変更

ディレクトリ・レプリケーション・サーバーの構成パラメータとその説明は、『Oracle Identity Management ユーザー・リファレンス』のレプリケーションのスキーマ要素に関する項で、ディレクトリ・サーバーの構成パラメータについて参照してください。これらのパラメータは、識別名が `cn=configset0,cn=osdrepld,cn=subconfigsubentry` であるレプリケーション・サーバー configuration set entry に格納されます。このエントリには、レプリケーション処理を制御するレプリケーション属性が含まれています。この属性の一部は変更できます。

Oracle Directory Manager を使用したディレクトリ・レプリケーション・サーバーの構成パラメータの表示

ディレクトリ・レプリケーション・サーバーの構成パラメータを表示する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」、「**サーバー管理**」の順に展開します。
2. 「**レプリケーション・サーバー**」を選択します。次のタブ・ページが、右側のペインに表示されます。
   - **アクティブ・レプリケーション・サーバー :** 現在実行中のディレクトリ・レプリケーション・サーバーが表示されます。
   - **レプリケーション・ステータス :** 各サプライヤから DRG 内の各コンシューマに適用された最終変更の番号が表示されます。
   - **変更ログ・サブスクライバ・ステータス :** 変更ログに対応するすべてのサブスクライバ、およびこのノードから適用された最終変更の番号が表示されます。

Oracle Directory Manager を使用したディレクトリ・レプリケーション・サーバーの構成パラメータの変更

ディレクトリ・レプリケーション・サーバーの構成パラメータを変更する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」、「**サーバー管理**」、「**レプリケーション・サーバー**」の順に展開します。
2. パラメータを変更するレプリケーションの構成設定を選択します。対応するタブ・ページが、右側のペインに表示されます。
3. 「**一般**」タブ・ページで、各フィールドの情報を必要に応じて変更します。

   これらのフィールドの詳細は、表 A-20「レプリケーション・サーバーの「構成設定」の「一般」タブ・ページのフィールド」を参照してください。
4. アドバンスト・レプリケーション・ベースの承諾の場合は、「**ASR 承諾**」タブ・ページで、各フィールドの情報を必要に応じて変更します。

   これらのフィールドの詳細は、表 A-21「「ASR 承諾」タブ・ページのフィールド」を参照してください。
5. ディレクトリ・レプリケーション・サーバーを再起動して、変更内容を反映させます。

注意 : DRG の全ノードのホスト名すべてを「レプリケーション・グループ・ノード」フィールドに必ず追加してください。DRG の全ノードに対して、この追加を実行してください。

コマンドライン・ツールを使用したディレクトリ・レプリケーション・サーバーの構成パラメータの変更

コマンドライン・ツールを使用してレプリケーション構成パラメータを変更する場合は、『Oracle Identity Management ユーザー・リファレンス』の ldapmodify コマンドライン・ツールのリファレンスに記載されている構文を使用してください。

レプリケーション・サーバーの構成パラメータの詳細は、『Oracle Identity Management ユーザー・リファレンス』のレプリケーションのスキーマ要素に関する項を参照してください。表に示されているように、レプリケーションの変更可能な構成パラメータは、次のとおりです。

- orclChangeRetryCount
- orclThreadsPerSupplier

orclThreadsPerSupplier 構成パラメータには、2 つのサブタイプがあります。

- apply: 変更ログを適用するためのワーカー・スレット数
- transport: 変更ログを転送するためのワーカー・スレッド数

例 31-1 変更がパージ・キューに移動される前の再試行回数の変更

この例では、mod.ldif という名前の入力ファイルを使用して、再試行の回数をデフォルトの 10 回から 5 回に変更します。具体的には、更新を 5 回試行すると、その更新は削除され、レプリケーション・ログに記録されます。

1. サンプル・ファイル mod.ldif を、次のように編集します。

```
dn: cn=configset0,cn=osdrepld,cn=subconfigsubentry
changetype: modify
replace: orclChangeRetryCount
orclChangeRetryCount: 5
```

2. レプリケーション・サーバーの configset0 パラメータの値を更新するには、次のように ldapmodify を使用します。

```
ldapmodify –D "cn=orcladmin" –w administrator_password -h my_host \
          -p port -f mod.ldif
```

3. ディレクトリ・レプリケーション・サーバーを再起動します。

例 31-2 変更ログの適用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、変更ログの適用で使用されるワーカー・スレッドの数を 5 に変更します。

1. サンプル・ファイル mod.ldif を、次のように編集します。

```
dn: cn=configset0, cn=osdrepld, cn=subconfigsubentry
changetype:modify
replace: orclthreadspersupplier;apply
orclthreadspersupplier;apply: 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 consumer_host_name -p consumer_port -D cn=orcladmin \
   -w administrator_password -v -f mod.ldif
```

3. ディレクトリ・レプリケーション・サーバーを再起動します。

```
oidctl connect=connect_string server=oidrepld instance=instance_number restart
```

> **関連資料:** 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、『Oracle Identity Management ユーザー・リファレンス』の oidctl コマンドライン・ツールのリファレンスを参照してください。

例 31-3 変更ログの転送および適用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、次の変更を行います。

- 変更ログの適用に使用されるワーカー・スレッド数を 1 に変更
- 変更ログの転送に使用されるワーカー・スレッド数を 1 に変更

手順はすべて例 31-2 と同じです。LDIF ファイルのみが異なります。

サンプル・ファイル mod.ldif を、次のように編集します。

```
dn: cn=configset0, cn=osdrepld, cn=subconfigsubentry
changetype:modify
replace: orclthreadspersupplier;transport
orclthreadspersupplier;transport: 1
replace: orclthreadspersupplier;apply
orclthreadspersupplier;apply: 1
```

この変更を行うと、レプリケーション承諾の 2 つのレプリカ間で、レプリケーションの方向ごとにワーカー・スレッドとリーダー・スレッドが 1 つずつ生成されます。

特定のレプリカ・ノードについてのパラメータの表示および変更

特定のレプリカ・ノードを変更するには、レプリカ・サブエントリを変更します。レプリカ・サブエントリで変更できるパラメータは、『Oracle Identity Management ユーザー・リファレンス』のレプリケーションのスキーマ要素に関する項を参照してください。

注意： ディレクトリ・レプリケーション・サーバーは、レプリケーション・ノードのオブジェクトをコンシューマから読み込むため、すべての変更をコンシューマおよびサプライヤ（オプション）に適用する必要があります。

関連資料： レプリカ・サブエントリの詳細は、29-10 ページの「レプリカ・サブエントリ」を参照してください。

Oracle Directory Manager を使用した特定のレプリカ・ノードのパラメータの表示と変更

Oracle Directory Manager を使用して特定のレプリカ・ノードを表示および変更する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」、「**レプリケーション管理**」の順に展開します。
2. 表示または変更するレプリカ・ノードを選択します。対応するタブ・ページが、右側のペインに表示されます。
3. 「**一般**」タブ・ページで、各フィールドの情報を必要に応じて変更します。このタブ・ページのフィールドについては、表 A-22「「レプリカ・ノード」の「一般」タブ・ページのフィールド」を参照してください。
4. 「**レプリカ承諾**」タブ・ページでは、指定ノードがメンバーとなっているレプリケーション承諾の詳細を参照できます。このタブ・ページの列の説明は、表 A-23「「レプリカ承諾」タブ・ページの列」を参照してください。
5. レプリカ・ノードを表示し、変更した後は、ディレクトリ・レプリケーション・サーバーを再起動します。

コマンドライン・ツールを使用した特定のレプリカ・ノードの変更

コマンドライン・ツールを使用してレプリケーション構成パラメータを変更する場合は、『Oracle Identity Management ユーザー・リファレンス』の ldapmodify コマンドライン・ツールのリファレンスに記載されている構文を使用してください。

例 31-4 特定のレプリカ・ノードの orclReplicaURI 属性の変更

ディレクトリ・レプリケーション・サーバーは、レプリカ・サブエントリの orclReplciaURI 属性の値を使用して、そのレプリカのディレクトリ・サーバーを検索します。ディレクトリ・サーバーが稼働しているポートまたはホストが変更された場合は、この属性も変更する必要があります。

1. サンプル・ファイル mod.ldif を、次のように編集します。

```
Dn: orclreplicaid=unique_replica_identifier, cn=replication configuration
Changetype:modify
Replace:orclReplicaURI
OrclReplicaURI: ldap://host_name:port_number/
```

2. ldapmodify を使用して、レプリカ・サブエントリの orclreplicauri 属性を更新します。

```
ldapmodify -D "cn=orcladmin" -w administrator_password -h my_host \
           -p port -f mod.ldif
```

3. ディレクトリ・レプリケーション・サーバーを再起動します。

例 31-5 特定のレプリカの orclReplicaSecondaryURI 属性の変更

ディレクトリ・レプリケーション・サーバーは、orclReplicaSecondaryURI 属性の値を代替位置として使用して、特定のレプリカをディレクトリ・サーバーに問い合せます。ユーザーは、ldapURI を代替属性として追加でき、この属性は、ディレクトリ・サーバーにとって特定のレプリカについての問合せ先となります。ldapURI 属性を追加する手順は、次のとおりです。

1. サンプル・ファイル mod.ldif を、次のように編集します。

```
Dn: orclreplicaid=unique_replica_identifier, cn=replication configuration
Changetype:modify
add:orclReplicaSecondaryURI
OrclReplicaSecondaryURI: ldap://host_name:port_number/
```

2. ldapmodify を使用して、レプリカ・サブエントリの OrclReplicaSecondaryURI 属性を更新します。

```
ldapmodify -D "cn=orcladmin" -w administrator_password -h my_host \
           -p port -f mod.ldif
```

3. ディレクトリ・レプリケーション・サーバーを再起動します。

例 31-6 特定のレプリカの orclReplicaState 属性の変更

OrclReplicaState は、特定のレプリカの状態を表します。レプリカをブートストラップ（再初期化）するには、この属性を次のように更新します。

1. サンプル・ファイル mod.ldif を、次のように編集します。

```
Dn: orclreplicaid=unique_replicaID, cn=replication configuration
Changetype:modify
replace:orclReplicaState
OrclReplicaState: 0
```

2. コンシューマ・レプリカが稼働しているホストで、ldapmodify を使用してレプリカ・サブエントリの orclreplicastate 属性を更新します。

```
ldapmodify -D "cn=orcladmin" -w administrator_password -h consumer_host \
           -p port -f mod.ldif
```

3. ディレクトリ・レプリケーション・サーバーを再起動します。

レプリケーション承諾のパラメータの変更

この項では、アドバンスト・レプリケーション・ベースおよび LDAP ベースのレプリケーション承諾を変更する方法について説明します。

Oracle Database アドバンスト・レプリケーション・ベースのレプリケーション承諾のパラメータの変更

アドバンスト・レプリケーション・ベースのレプリケーション承諾のパラメータは、レプリケーション承諾エントリに格納されています。識別名は次のとおりです。

```
orclAgreementID=000001,cn=replication configuration
```

注意：

- アドバンスト・レプリケーション・ベースのレプリケーション承諾では、DirectoryReplicationGroupDSAs パラメータに、DRG 内のすべてのノードのホスト名を入力します。このリストは、すべてのノードで同一であることが必要です。
- Oracle Internet Directory 10*g*（10.1.4.0.1）の場合、使用できる Oracle Database アドバンスト・レプリケーション・ベースのレプリケーション承諾は 1 つのみです。このレプリケーション承諾の識別名は、orclagreementid=000001,cn=replication configuration です。
- レプリケーション承諾のパラメータを変更する前に、すべてのノードで Oracle Internet Directory を起動していることを確認してください。

関連項目：

- 31-7 ページの「Oracle Directory Manager を使用した Oracle Database アドバンスト・レプリケーション・ベースのレプリケーション承諾の表示と変更」
- 31-7 ページの「ldapmodify を使用したアドバンスト・レプリケーション・ベースのレプリケーション承諾の管理」

Oracle Directory Manager を使用した Oracle Database アドバンスト・レプリケーション・ベースのレプリケーション承諾の表示と変更

Oracle Directory Manager を使用してレプリケーション承諾のパラメータを表示および変更する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「**< ディレクトリ・サーバー・インスタンス >**」、「**レプリケーション管理**」の順に展開します。次のタブ・ページが、右側のペインに表示されます。

   - **レプリケーション・ステータス :** 各サプライヤから DRG 内の各コンシューマに適用された最終変更の番号が表示されます。
   - **レプリカ状態 :** レプリカの状態（オンライン、オフライン、ブートストラップ中）が表示されます。
   - **変更ログ・サブスクライバ・ステータス :** 変更ログに対応するすべてのサブスクライバ、およびこのノードから適用された最終変更の番号が表示されます。
   - **ASR 承諾 :** アドバンスト・レプリケーション・ベースのレプリケーション承諾についての情報を表示し、必要に応じて変更できます。このタブ・ページのフィールドの説明は、表 A-21「「ASR 承諾」タブ・ページのフィールド」を参照してください。

   注意 : DRG の全ノードのホスト名すべてを「レプリケーション・グループ・ノード」フィールドに必ず追加してください。DRG の全ノードに対して、この追加を実行してください。

2. 値の変更中に、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 を使用したアドバンスト・レプリケーション・ベースのレプリケーション承諾の管理

レプリケーション承諾パラメータの一覧とその説明、および変更可能なパラメータは、『Oracle Identity Management ユーザー・リファレンス』のレプリケーションのスキーマ要素に関する項を参照してください。

レプリケーション承諾エントリの値にノードを追加するには、LDIF フォーマットのファイルを参照して、コマンドラインで ldapmodify を実行します。

例 31-7 レプリケーション承諾へのノードの追加

この例では、`mod.ldif` という名前の入力ファイルを使用して、レプリケーション承諾に 2 つのノードを追加します。

1. `mod.ldif` を次のように編集します。

```
dn: orclagreementid=000001,cn=replication configuration
changetype: modify
add: orcldirreplgroupdsas
orcldirreplgroupdsas: hollis
orcldirreplgroupdsas: eastsun-11
```

2. レプリケーション・サーバーの `configset0` パラメータの値を更新するには、次のように ldapmodify を使用します。

```
ldapmodify -D "cn=orcladmin" -w administrator_password -h host \
          -p port -f mod.ldif
```

3. ディレクトリ・レプリケーション・サーバーを再起動します。

このプロシージャは、識別名が `orclagreementid=000001,cn=replication configuration` のレプリケーション承諾が含まれているエントリを変更します。入力ファイルを適用すると、`oraclagreementid=000001` で管理されているレプリケーション・グループに、`hollis` と `eastsun-11` の 2 つのノードが追加されます。

注意： レプリケーション・プロセスを起動する前に、レプリケート環境の各ノードの `orclDirReplGroupDSAs` パラメータに、新規ノード（例：前述の LDIF ファイルの例では `hollis` と `eastsun-11`）を組み込む必要があります。

新しいノードをレプリケーション環境に追加する手順は、30-14 ページの「マルチマスター・レプリケーション用のノードの追加（Oracle Database アドバンスト・レプリケーション・タイプのみ）」を参照してください。

Oracle Internet Directory 10*g*（10.1.4.0.1）でディレクトリ・レプリケーション・サーバーのためにサポートされている構成設定は 1 つのみのため、構成設定を指定する必要はありません。

例 31-8 Oracle Database アドバンスト・レプリケーションのレプリカ承諾の orclExcludedNamingContexts 属性の変更

アドバンスト・レプリケーション・ベースのレプリケーション承諾では、ディレクトリ・レプリケーション・サーバーは、レプリカ承諾エントリの `orclExcludedNamingcontexts` 属性の値を使用して、レプリケーションから除外する最上位サブツリーを指定します。

この例では、`c=us` と `c=uk` という 2 つの上位ネーミング・コンテキストがアドバンスト・レプリケーションから除外されます。

1. サンプル・ファイル `mod.ldif` を、次のように編集します。

```
dn: orclAgreementID=000001, cn=replication configuration
Changetype:modify
Replace: orclExcludedNamingcontexts
orclExcludedNamingcontexts: c=us
orclExcludedNamingcontexts: c=uk
```

2. ldapmodify を使用して、レプリケーション承諾の `orclupdateschedule` 属性を更新します。

```
ldapmodify -D "cn=orcladmin" -w administrator_password -h consumer_host \
           -p port -f mod.ldif
```

3. ディレクトリ・レプリケーション・サーバーを再起動します。

LDAP ベースのレプリケーション承諾のパラメータの変更

LDAP ベースのレプリケーション承諾のパラメータは、レプリケーション承諾エントリに格納されています。識別名は次のとおりです。

```
orclAgreementID=unique_identifier_of_the_replication_agreement,
 orclReplicaId=unique_identifier_of_the_supplier, cn=replication configuration
```

注意： 承諾がサプライヤ側およびコンシューマ側の両方で同一であることを確認します。レプリケーション・サーバーは、最後に適用された変更番号とネーミング・コンテキストをサプライヤ・ノードの承諾から読み取ります。その他の承諾属性はコンシューマ側から読み取ります。

Oracle Directory Manager を使用した LDAP ベースのレプリケーション承諾のパラメータの表示と変更

Oracle Directory Manager を使用してレプリケーション承諾のパラメータを表示および変更する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」、「**レプリケーション管理**」、「**レプリカ・ノード : < レプリカ識別子 >**」の順に展開します。
2. 表示または変更するレプリカ承諾を選択します。次のタブ・ページが、右側のペインに表示されます。
   - **一般 :** LDAP ベースのレプリケーション承諾についての情報が表示され、必要に応じて変更できます。このタブ・ページのフィールドの説明は、表 A-23「「レプリカ承諾」タブ・ページの列」を参照してください。
   - **レプリカのネーミング・コンテキスト :** LDAP ネーミング・コンテキストのオブジェクトを表示、追加、削除および変更できます。このタブ・ページのフィールドの説明は、表 A-24「「レプリカ承諾」の「レプリカのネーミング・コンテキスト」タブ・ページのフィールド」を参照してください。

ldapmodify を使用した LDAP ベースのレプリケーション承諾のパラメータの変更

レプリケーション承諾パラメータの説明、および変更可能なパラメータは、『Oracle Identity Management ユーザー・リファレンス』のレプリケーションのスキーマ要素に関する項を参照してください。

例 31-9 特定のレプリカ承諾の orclUpdateSchedule 属性の変更

ディレクトリ・レプリケーション・サーバーは、レプリカ承諾エントリの `orclupdateschedule` 属性の値を使用して、レプリケーション・サーバーがサプライヤからの新しい変更ログを処理する間隔（分単位）を決めます。

次の例では、レプリケーション・サーバーがサプライヤからの新しい変更ログを 1 分ごとに処理します。

1. サンプル・ファイル `mod.ldif` を、次のように編集します。

```
dn: orclAgreementID=id_number,orclReplicaId=replica_identifier,
 cn=replication configuration
Changetype:modify
Replace: orclupdateschedule
orclupdateschedule: 1
```

2. ldapmodify を使用して、レプリケーション承諾の orclupdateschedule 属性を更新します。

```
ldapmodify -D "cn=orcladmin" -w administrator_password -h consumer_host \
           -p port -f mod.ldif
```

3. ディレクトリ・レプリケーション・サーバーを再起動します。

例 31-10 特定のレプリカ承諾の orclLastAppliedChangeNumber 属性の変更

ディレクトリ・レプリケーション・サーバーは、`orclLastAppliedChangeNumber` 属性の値を使用して、コンシューマが処理した適用済最終変更ログの番号を判別します。

レプリケーション・サーバーは、サプライヤ側の同じ複製承諾から `orclLastAppliedChangeNumber` を読み込むため、`orclLastAppliedChangeNumber` 属性の変更をサプライヤ・ノードに適用する必要があります。

この例では、サプライヤ側の同じ複製承諾の orclLastAppliedChangeNumber 属性が 700 に設定されています。これは、700 より小さい変更ログ番号を持つすべての変更ログがレプリケーション・サーバーによって処理されていることを表しています。

注意： 部分レプリケーションのノード追加プロシージャ時に指示されている場合を除き、orclLastAppliedChangeNumber 属性は変更できません。

---

1. サンプル・ファイル mod.ldif を、次のように編集します。

```
dn: orclAgreementID=unique_identifier_of_the_replication_agreement,
 orclReplicaId=unique_identifier_of_the_supplier,cn=replication configuration
Changetype:modify
Replace: orclLastAppliedChangeNumber
orclLastAppliedChangeNumber: 700
```

2. ldapmodify を使用して、サプライヤ側でレプリケーション承諾の orclupdateschedule 属性を更新します。

```
ldapmodify -D "cn=orcladmin" -w administrator_password \
           -h supplier_host -p port -f mod.ldif
```

3. ディレクトリ・レプリケーション・サーバーを再起動します。

Oracle Database アドバンスト・レプリケーションを使用した、全ノードでのレプリケーション管理者パスワードの変更

DRG のすべてのノードで、レプリケーション管理者のデータベース・アカウントのパスワードは、Oracle Database アドバンスト・レプリケーションを使用して、レプリケーション環境管理ツール remtool に -chgpwd 引数を指定することで変更できます。この引数を使用するには、次のように入力します。

```
remtool -chgpwd
```

remtool ユーティリティを実行すると、MDS グローバル名（つまり、マスター定義サイトの名前）、現行のパスワードおよび新規パスワードを要求するプロンプトが表示されます。さらに、新規パスワードの確認を要求されます。誤った現行のパスワードを入力した場合は、再びレプリケーション環境管理ツールを実行する必要があります。

remtool の -pchgpwd 引数を使用して、レプリカのレプリケーション識別名のパスワードを変更することもできます。

レプリケーション Wallet の $ORACLE_HOME/dap/admin 内でのみパスワードを変更するには、remtool の -pchgwalpwd 引数を使用します。この引数を使用するには、次のように入力します。

```
remtool -pchgwalpwd
```

関連資料： remtool の使用方法の詳細は、『Oracle Identity Management ユーザー・リファレンス』の remtool コマンドライン・ツールのリファレンスを参照してください。

変更ログの管理

Oracle Directory Manager では、最近実行された 25 件の変更を表示し、これらの変更を変更ログ番号別、発生した操作の種類別（追加、変更、削除など）および各変更が加えられたエントリ別にリストすることができます。特定の変更を指定して、その詳細を表示することもできます。

変更ログを管理するには、ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「<ディレクトリ・サーバー・インスタンス>」の順に展開し、「**変更ログ管理**」を選択します。右側のペインに、直近の変更から順に最近の 25 件の変更が表示されます。変更番号、変更が発生した操作の種類および変更が行われたエントリも表示されます。

特定の変更の詳細を表示するには、右側のペインで該当する変更を選択し、「**プロパティの表示**」を選択します。「変更ログ」ウィンドウが表示されます。「変更ログ」ウィンドウの各フィールドの説明は、表 A-27「「変更ログ」ウィンドウのフィールド」を参照してください。

ディレクトリ・レプリケーションの速度変更

レプリケーションのデフォルトの構成では、`orclupdateschedule` 属性の値は `1`（1 分を表す）に設定されています。`orclupdateschedule` 属性の値を `0`（1 秒を表す）に変更すると、レプリケーションの処理時間を短縮できます。

Oracle Database アドバンスト・レプリケーションを使用している場合のディレクトリ・レプリケーションの速度変更

アドバンスト・レプリケーション・ベースのディレクトリ・レプリケーションのデフォルト構成では、処理時間は約 2.5 分です。

- 1 分で、サプライヤがコンシューマに送信する変更を準備
- 30 秒で、アドバンスト・レプリケーションが変更をコンシューマに送信
- 1 分で、コンシューマが変更を適用

アドバンスト・レプリケーションの場合、`orclupdateschedule` 属性のデフォルト値を `0` に変更すると、レプリケーション時間は 32 秒になります。これは、次の手順に従って行います。

1. `mod.ldif` を次のように編集します。

```
dn: orclagreementid=000001, cn=replication configuration,
 cn=replication configuration
changetype:modify
replace: orclupdateschedule
orclupdateschedule: 0
```

2. `mod.ldif` を次のようにアップロードします。

```
ldapmodify -D "cn=orcladmin" -w administrator_password -h host_name -p port \
          -v -f mod.ldif
```

3. ディレクトリ・レプリケーション・サーバーを再起動します。

```
oidctl connect=connect_string server=oidrepld instance=instance_number restart
```

LDAP ベースのレプリケーションを使用している場合のディレクトリ・レプリケーションの速度変更

LDAP ベースのディレクトリ・レプリケーションのデフォルト構成では、変更がサプライヤから取得され、コンシューマに適用されるまでの処理時間は約 1 分です。orclupdateschedule 属性のデフォルト値を 0 に変更すると、レプリケーション時間は 1 秒になります。これは、次の手順に従って行います。

1. mod.ldif を次のように編集します。

```
dn: orclAgreementID=unique_identifier_of_the_replication_agreement,
 orclReplicaId=unique_identifier_of_the_supplier,
 cn=replication configuration
changetype:modify
replace: orclupdateschedule
orclupdateschedule: 0
```

2. コンシューマ・ホストで、mod.ldif を次のようにアップロードします。

```
ldapmodify -h consumer_host_name -p consumer_port -D cn=orcladmin \
           -w administrator_password -v -f mod.ldif
```

3. ディレクトリ・レプリケーション・サーバーを再起動します。

```
oidctl connect=connect_string server=oidrepld instance=instance_number restart
```

トポロジの管理および監視

レプリケーション環境管理ツール、remtool を使用すれば、レプリケーション・プロセスの状態を監視できます。remtool を定期的に実行して、レプリケーション・プロセスが正常に実行されていることを確認できます。

レプリケーション・プロセスの状態を監視するための remtool オプションは、-pdipqstat と -pverify です。これらは、キュー統計表示ツールとレプリケーション検証ツールとも呼ばれます。構文は次のとおりです。

```
remtool -pdispqstat [-v] [-bind hostname:port_number/replication_dn_password]

remtool -pverify [-v] [-bind hostname:port_number/replication_dn_password] [-hiqmax
hiqmax] [-tbtmax tbtmax]
```

まず、キュー統計表示ツールを実行します。DRG のキュー統計が表示されます。管理者操作キュー（HIQ）エントリと、転送される変更ログ（ログ TBP）の数が通常より多いかどうかをチェックします。多い場合は、レプリケーションの実行速度が本来よりも遅いことを意味します。レプリケーション検証ツールを実行して、レプリケーションの構成を検証します。

レプリケーション検証ツールによりテストの失敗が報告された場合は、生成されるレポートをチェックし、レポートの提案に従い、失敗を修正します。

比較調整ツール

比較調整ツール oidcmprec を使用すれば、2 つのディレクトリを比較できます。このツールは、競合を検出し、解消します。2 つのディレクトリのうち、一方のディレクトリはソース・ディレクトリ、つまり真のソースとみなされます。もう一方のディレクトリは、宛先ディレクトリで、ソース・ディレクトリと同期させる必要があります。比較の対象となるディレクトリは、スタンドアロンのディレクトリ、同じレプリケーション・グループの一部、または異なるレプリケーション・グループの一部のいずれでもかまいません。

この項では、oidcmprec ツールの概要と、oidcmprec の使用例のいくつかについて説明します。この項の項目は次のとおりです。

- 競合の例
- oidcmprec でサポートされる操作
- oidcmprec からの出力
- oidcmprec の動作
- ソース・ディレクトリと宛先ディレクトリの設定
- 操作の DIT の選択
- 操作属性の選択
- 変更ログ生成の制御
- パラメータ・ファイルの使用
- ディレクトリ・スキーマの包含
- 事前に定義された競合解消規則の無視
- ユーザー定義の比較調整操作の使用
- oidcmprec ツールの既知の制限事項

> **関連資料：** 操作、競合の例、競合解消規則を含む oidcmprec の完全な構文は、『Oracle Identity Management ユーザー・リファレンス』の oidcmprec コマンド・リファレンス

競合の例

oidcmprec ツールは、次の競合の例を検出し、解消できます。

- ソース・ディレクトリ内のみのエントリ（entos）
- 宛先ディレクトリ内のみのエントリ（entod）
- ソース・ディレクトリ内のみの属性（atros）
- 宛先ディレクトリ内のみの属性（entod）
- 異なる単一値属性（svatrdif）
- 異なる複数値属性（mvatrdif）
- 異なるエントリ識別名（dndif）

  dndif の例は、一方のノードで実行された modrdn または moddn 操作が、もう一方のノードにレプリケートされないときに、レプリケーション環境で発生する可能性があります。結果として、そのエントリは、orclguid は同じでも、識別名が 2 つのノードで異なります。ツールでは、orclguid 属性を使用して、この競合を検出します。

oidcmprec ツールは、次のスキーマの競合の例も検出し、解消できます。

- オブジェクト・クラス定義が、ソース・ディレクトリにのみ存在（odefos）
- オブジェクト・クラス定義が、宛先ディレクトリにのみ存在（odefod）
- ソースおよび宛先ディレクトリで異なるオブジェクト・クラス定義（odefdif）

- 属性定義が、ソース・ディレクトリにのみ存在（adefos）
- 属性定義が、宛先ディレクトリにのみ存在（adefod）
- ソースおよび宛先ディレクトリで異なる属性定義（adefdif）

oidcmprec でサポートされる操作

oidcmprec ツールは、5 つの操作をサポートします。各操作は、エントリを比較し、競合を検出し、オプションで競合を解消します。操作は、競合の解消方法に違いがあります。操作は次のとおりです。

- 比較操作 : 2 つのディレクトリを比較し、変更を LDIF レコードとしてファイルに格納します。LDIF ファイルは、宛先ディレクトリに適用でき、ソース・ディレクトリと同一にできます。ソース・ディレクトリ内のデータのみが有効とみなされます。
- 調整操作 : 2 つのディレクトリを比較し、宛先ディレクトリ側で、ソース・ディレクトリに一致させるために必要な変更を適用します。ディレクトリに対して加えられた変更はすべて、LDIF 記録としてファイルに格納されます。ソース・ディレクトリ内のデータのみが有効とみなされます。
- マージまたは双方向調整操作 : 2 つのディレクトリを比較し、ソース・ディレクトリまたは宛先ディレクトリで、2 つを一致させるために必要な変更を適用します。両ディレクトリのデータは有効とみなされます。たとえば、エントリが宛先ディレクトリにのみ存在することがツールにより検出された場合、ツールはこのエントリをソースに追加します。この操作ではまた、ディレクトリに加えられた変更をすべて、LDIF レコードとしてファイルに記録します。
- マージ・リハーサル操作 : マージ操作と同様に 2 つのディレクトリを比較しますが、ディレクトリでの変更適用は行いません。かわりに、変更を LDIF 記録としてファイルに格納します。ソース・ディレクトリと宛先ディレクトリに適用される変更は、2 つの異なるファイルに格納されます。
- ユーザー定義の比較調整操作 : 競合の例ごとに選択した競合解消規則を使用します。各競合の例に使用できる競合解消規則のリストは、『Oracle Identity Management ユーザー・リファレンス』を参照してください。

oidcmprec からの出力

oidcmprec ツールでは、すべての操作について、次のファイルを生成します。

- *filename*.rpt: 比較されたすべてのエントリの識別名と比較結果が含まれます。
- *filename*.s2d.ldif: 宛先ディレクトリに適用された、または宛先ディレクトリに後から適用するために格納されたすべての変更が含まれます。名前は、宛先ディレクトリからソース・ディレクトリへの省略形です。
- *filename*.d2s.ldif: ソース・ディレクトリに適用された、またはソース・ディレクトリに後から適用するために格納されたすべての変更が含まれます。名前は、宛先ディレクトリからソース・ディレクトリへの省略形です。
- *filename*.eos.rpt: ソース・ディレクトリ内にのみ存在するエントリの識別名のリストが含まれます。スキーマが操作の対象に含まれている場合には、ソース・ディレクトリでのみ定義されている属性およびオブジェクト・クラスの名前のリストも含まれます。名前は、ソース・ディレクトリでのみ使用可能なエントリの省略形です。
- *filename*.eod.rpt: 宛先ディレクトリ内にのみ存在するエントリの識別名のリストが含まれます。スキーマが操作の対象に含まれている場合には、宛先ディレクトリでのみ定義されている属性およびオブジェクト・クラスの名前のリストも含まれます。名前は、宛先ディレクトリでのみ使用可能なエントリの省略形です。
- *filename*.dif.rpt: 異なるすべてのエントリの識別名と、異なる属性の名前のリストが含まれます。スキーマが操作の対象に含まれている場合には、定義が異なる属性およびオブジェクト・クラスの名前のリストも含まれます。このファイルは、dif ファイルと呼ばれます。

- *filename*.err: すべてのエラー・メッセージが含まれます。このファイルは、err ファイルと呼ばれます。

oidcmprec の動作

レプリケーション識別名とレプリケーション識別名パスワードを資格証明として使用して、ツールは 3 つのタスクを実行します。まず、スキーマ情報をメモリーにロードします。次に、比較対象のエントリを収集し、それらを属性ごとに比較します。ツールは、スキーマ情報を使用して、属性ごとに使用する比較規則を判断します。次に、比較結果に基づき、必要な処置を行います。これらの操作は、異なるスレッドによって実行されます。

- 識別名スレッドは、比較対象のエントリの収集を担当します。エントリの収集中、スレッドはツリー全体を一度にフェッチしません。まず、ベース・エントリをフェッチして処理します。次に、ベース・エントリ直下の子をフェッチして処理し、さらにその下の子という具合に処理していきます。収集されたエントリは、ワーカー・スレッドに渡されます。識別名スレッドの数は、dnthreads 引数を使用して制御できます。
- ワーカー・スレッドは、エントリを属性ごとに比較し、競合解消規則を適用する作業を担当します。ワーカー・スレッドは、その後、エントリをログ・ライター・スレッドに渡します。ワーカー・スレッドの数は、threads 引数を使用して制御できます。ワーカー・スレッドと識別名スレッドの合計数は、6 ×（CPU 数）- 2 に相当する最大値以下です。これを超える値を指定すると、ツールは、ワーカー・スレッドと識別名スレッドの数を、最大値を超えないように調整します。
- ログ・ライター・スレッドは、31-14 ページの「oidcmprec からの出力」に示した 7 つの出力ファイルすべてへのコンテンツの書込みを担当します。ログ・ライター・スレッドは 1 つのみです。この数は増やせません。

これらのスレッドは、メイン・スレッドによって生成、監視、終了されます。メイン・スレッドは、コマンドラインの引数とパラメータ・ファイルを処理し、別のスレッドを生成します。メイン・スレッドは、全操作の完了を検出すると、ただちにすべてのスレッドを終了し、接続をすべてクリーンアップします。

各スレッドは、ソース・ディレクトリと宛先ディレクトリへの LDAP 接続を確立します。これらの接続は、すべての操作がスレッドによって完了されるまで、オープンのままです。なんらかの理由で接続がクローズされると、contonerr 引数が TRUE の場合、ツールは接続を再確立します。ツールが接続を再確立できると、操作を続行します。

注意： contonerr 引数を使用して、ツールがエラーの処理を続行するかどうかを指定します。この引数は、TRUE にも FALSE にも設定できます。デフォルトでは、TRUE に設定されています。

ソース・ディレクトリと宛先ディレクトリの設定

source オプションと destination オプションを使用して、ソース・ディレクトリと宛先ディレクトリを設定します。

```
oidcmprec source=staqj13:3060 destination=staqj:3070 base="''" \
          scope=subtree file=temp operation=compare
```

コマンドラインでパスワードが指定されていないと、ツールがパスワードを要求します。

```
Enter replication DN password of the source directory      :
Enter replication DN password of the destination directory :
```

操作の DIT の選択

base、dns2exclude および scope オプションを使用して、比較と調整の対象となる領域を選択します。

次の例では、c=us,dc=mycom,dc=com と c=uk,dc=mycom,dc=com を除く、ディレクトリ全体を比較します。

```
oidcmprec base="''" \
          dns2exclude="'c=us,dc=mycom,dc=com' 'c=uk,dc=mycom,dc=com'" \
          operation=compare scope=subtree \
          source=myhost1.mycom.com:389/replication_dn_pwd \
          destination=myhost2.mycom.com:389/replication_dn_pwd \
          threads=5 dnthreads=2 file=cmpres
```

次の例では、c=us,dc=mycom,dc=com ツリーと c=uk,dc=myorg,dc=org ツリーを除く、ネーミング・コンテキスト dc=com および dc=org を比較します。

```
oidcmprec base="'dc=com' 'dc=org'" \
          dns2exclude="'c=us,dc=mycom,dc=com' 'c=uk,dc=myorg,dc=org'" \
          operation=compare scope=subtree \
          source=myhost1.mycom.com:389/replication_dn_pwd \
          destination=myhost2.mycom.com:389/replication_dn_pwd \
          threads=5 dnthreads=2 file=cmpres
```

操作属性の選択

デフォルトでは、oidcmprec は、操作属性の creatorsname、createtimestamp、modifiersname、modifytimestamp、orclentrydn および orclnormdn を除くすべての属性を比較します。選択した操作に含める、または操作から除外する属性は、それぞれ inclattr または exclattr を使用して制御できます。exclattr 引数と inclattr 引数により、パターン一致を制限できます。*attributename** を使用すれば、*attributename* で始まるすべての属性を一致させることができます。*attributename;** を使用すれば、*attributename* のすべてのサブタイプも一致させることができます。

次の例では、標準の除外属性に加えて、authpassword 属性（サブタイプのあるものとないもの）、さらに userpassword 属性と category 属性を除外します。

```
oidcmprec operation=compare scope=subtree base="'dc=com' 'dc=org'" \
          source=myhost1.mycom.com:389/replication_dn_pwd \
          destination=myhost2.mycom.com:389/replication_dn_pwd \
          exclattr="authpassword authpassword;* userpassword category" \
          threads=5 dnthreads=2 file=compare
```

次の例では、比較操作に属性 uid、cn、sn、givenname および mail のみを含めます。

```
oidcmprec operation=compare scope=subtree base="'dc=com'" \
          source=myhost1.mycom.com:389/replication_dn_pwd \
          destination=myhost2.mycom.com:389/replication_dn_pwd \
          inclattr="uid cn sn givenname mail" \
          file=compare
```

次の例では、orclguid、creatorsname および modifiersname を除き、比較操作の対象となるすべての属性を含めます。この例ではまた、contonerr=false を設定することで、エラーが発生したら停止するように、ツールに指示しています。

```
oidcmprec operation=compare scope=subtree base="'dc=com'" \
          source=myhost1.mycom.com:389/replication_dn_pwd \
          destination=myhost2.mycom.com:389/replication_dn_pwd \
          inclattr="*" exclattr="orclguid creatorsname modifiersname" \
          file=compare contonerr=false
```

変更ログ生成の制御

oidcmprec によって加えられた変更に対する変更ログの生成は、ルート DSE の orcldiprepository 属性によって決まります。ただし、変更ログ生成の動作は、genchglog 引数を使用することで制御できます。genchglog 引数には、次の値を指定できます。

- default: ディレクトリ・サーバーの設定により、変更ログが生成されるか、されないかが決まります。ルート・エントリの orcldiprepository 属性が true に設定されている場合は、変更ログが生成されます。orcldiprepository が false に設定されている場合、変更ログは生成されません。ソース・ディレクトリと宛先ディレクトリのどちらにも、同じ規則が適用されます。default が、gechglog のデフォルト値です。
- true: ソース・ディレクトリと宛先ディレクトリに対する設定に関係なく、変更ログは常に生成されます。
- false: ソース・ディレクトリと宛先ディレクトリに対する設定に関係なく、変更ログは常に生成されません。

次の例では、genchglog=false で、変更ログの生成を停止します。

```
oidcmprec operation=merge scope=subtree base="'dc=com'" \
          source=myhost1.mycom.com:389/replication_dn_pwd \
          destination=myhost2.mycom.com:389/replication_dn_pwd \
          inclattr="*" exclattr="orclguid creatorsname modifiersname" \
          file=merge genchglog=false
```

パラメータ・ファイルの使用

oidcmprec コマンドラインで指定可能な引数はすべて、パラメータ・ファイルに格納することもできます。パラメータ・ファイルは、paramfile オプションを使用して入力できます。コマンドラインとパラメータ・ファイルの両方で引数を指定した場合、コマンドラインで指定した引数が、パラメータ・ファイルで指定した引数に優先します。たとえば、次のようになります。

```
oidcmprec paramfile=comp_param threads=4
```

この例では、次のサンプル・パラメータ・ファイルを使用します。

```
###############################################
#Parameter file for compare and reconcile tool
#Creator   : John
#Date      : 21-Mar-2006
#File Name : comp_param
###############################################
operation=compare
source=staqj13:3060/ods
destination=staqj13:3070/ods
base="cn=oraclecontext"
base="c=uk,dc=mycom,dc=com"
base="c=us,dc=mycom,dc=com"
verbose=false
force=true
threads=6
dnthreads=2
exclattr="orclguid userpassword authpassword authpassword;*"
filename=cmp2006Feb01
```

この例では、ツールにより 4 つのワーカー・スレッドが生成されます。ここではコマンドライン引数が優先されます。

ディレクトリ・スキーマの包含

ベース引数に cn=subschemasubentry を含めると、oidcmprec 操作の対象にスキーマを含めることができます。たとえば、次のようになります。

```
oidcmprec operation=merge scope=subtree \
          base="'dc=com' 'cn=subschemasubentry'" \
          source=myhost1.mycom.com:389/replication_dn_pwd \
          destination=myhost2.mycom.com:389/replication_dn_pwd \
          inclattr="*" exclattr="orclguid creatorsname modifiersname" \
          file=merge genchglog=false
```

スキーマに加えてその他の識別名を含めた場合、oidcmprec は、最初にスキーマで操作を実行します。

事前に定義された競合解消規則の無視

各操作の競合の例と競合解消規則については、『Oracle Identity Management ユーザー・リファレンス』の oidcmprec コマンド・リファレンスを参照してください。

競合名と、コマンドラインまたはパラメータ・ファイルで使用する規則を指定することにより、事前に定義された競合解消規則を無視できます。次の例では、競合 dndif および mvatrdif に使用される競合解消規則を、compare 操作に対して ignore に変更します。

```
oidcmprec operation=compare source=host1:3060 destination=host2:3070 \
          base="''" scope=subtree file=temp operation=compare \
          dndif=ignore mvatrdif=ignore
```

ユーザー定義の比較調整操作の使用

事前に定義された compare、reconcile、merge および merge dry run 操作に加えて、oidcmprec にはユーザー定義の比較調整操作 userdefinedcr があり、競合解消規則引数を指定できます。userdefinedcr で指定しない競合解消規則はすべて、デフォルトが ignore に設定されます。次のコマンドラインでは、userdefinedcr 操作を使用しています。

```
oidcmprec operation=userdefinedcr scope=subtree \
          base="'dc=com' 'dc=org'" \
          source=myhost1.mycom.com:389/replication_dn_pwd \
          destination=myhost2.mycom.com:389/replication_dn_pwd \
          entos=add entod=ignore atros=add atrod=ignore \
          svatrdif=usesrc mvatrdif=usesrc dndif=ignore \
          threads=5 dnthreads=2 file=myreconcile
```

競合の例と競合解消規則については、『Oracle Identity Management ユーザー・リファレンス』の oidcmprec コマンド・リファレンスを参照してください。

oidcmprec ツールの既知の制限事項

oidcmprec ツールには、次の制限事項があります。

- LDIF レコードに対する変更をツリーの削除のために *filename*.s2d.ldif または *filename*.d2s.ldif ファイルに記録する際、ツールはまず親レコードを記録し、次にその子のレコードを記録します。ldapmodify コマンドライン・ツールを使用してこの変更を適用しようとすると、ディレクトリ・サーバーではリーフのないエントリの削除が許可されていないため、変更の適用は失敗します。ldapmodify の失敗を防ぐには、ldapmodify を実行する前に、ファイルを編集してレコードの順序を並べ替えます。
- エントリに対して削除操作を実行する際、ツールはそのエントリとその子を削除します。ツールにより、エントリが削除されたことは記録されますが、その子も削除されたことは記録されません。
- ツールには、複合相対識別名に関して制限事項があります。これらは、+ で区切られた複数の *attribute=attrvalue* のペアを含む相対識別名で、たとえば、次のようなものです。

  ```
  uid=jpaul + cn=john paul + mail=john.paul@oracle.com,dc=oracle,dc=com
  ```

  比較対象のディレクトリの 1 つに複合相対識別名が 1 つ含まれている場合、ツールが *filename*.s2d.ldif または *filename*.d2s.ldif ファイルでの modrdn/moddn の変更を推奨するとき、deleteoldrdn 値が間違っている可能性があります。

第 VI 部

ディレクトリ・プラグイン

第 VI 部は次の各章で構成されています。

32

Oracle Internet Directory サーバー・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。10*g*（10.1.4.0.1）で、Oracle Internet Directory は、PL/SQL はもとより、Java のプラグインもサポートしています。

この章の項目は次のとおりです。

関連資料：『Oracle Identity Management 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

ディレクトリ・サーバー・プラグインの概要

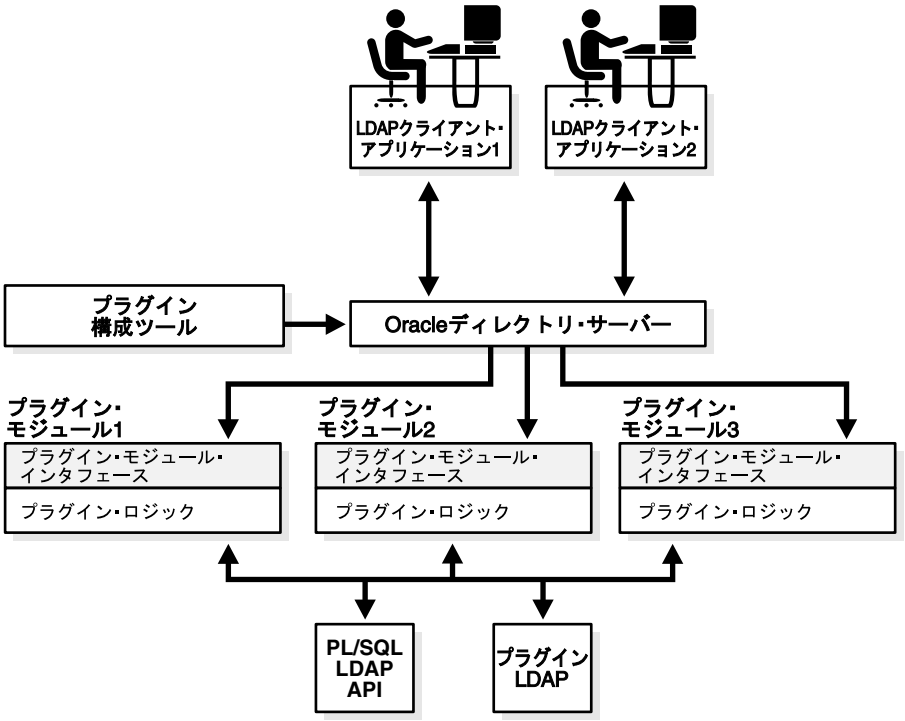
ディレクトリ・サーバーのプラグインは、次のような機能をディレクトリ・サーバーに追加します。

- ディレクトリ・サーバーによる操作実行前のデータの妥当性チェック
- サーバーによる操作実行後の指定処理の実行
- パスワード・ポリシーの定義
- 外部に格納された資格証明によるユーザーの認証

起動時に、ディレクトリ・サーバーはプラグイン構成およびライブラリをロードします。その後、リクエストを処理するときに、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 32-1 に、LDAP クライアントが個々のアプリケーションを使用して行う、Oracle ディレクトリ・サーバーとの間の情報の送受信について示します。同様に、プラグイン構成ツールもディレクトリ・サーバーに情報を送信します。ディレクトリ・サーバーはデータをプラグイン・モジュール 1、プラグイン・モジュール 2 およびプラグイン・モジュール 3 に送信します。各プラグイン・モジュールはプラグイン・モジュール・インタフェースとプラグイン・ロジックを備えています。各プラグイン・モジュールは、LDAP API およびプラグイン LDAP との間の情報の送受信を行います。

図 32-1 Oracle Internet Directory プラグイン・フレームワーク



通常のディレクトリ・サーバー操作の前後に実行するか、操作に追加して実行するかによって、プラグインが実行する作業は異なります。次の項では、様々な種類の操作ベースのプラグインについて説明します。

ディレクトリでサポートされている LDAP 操作およびタイミング

Oracle Internet Directory サーバーでは、次の LDAP 操作のプラグインをサポートしています。

- `ldapadd`
- `ldapbind`
- `ldapcompare`
- `ldapdelete`
- `ldapmoddn`（Java のみ）
- `ldapmodify`
- `ldapsearch`

Oracle Internet Directory では、プラグインに対して 4 つの操作タイミングをサポートしています。

- 前
- 後
- 操作時
- 操作時置換

これらについては、この後の 4 項で説明します。

操作前サーバー・プラグイン

サーバーは、LDAP 操作の実行前に、操作前プラグイン・モジュールをコールします。このタイプのプラグインの主な目的は、データが LDAP 操作で使用される前に、データを検証することです。

操作前プラグインで例外が発生すると、次のいずれかが発生します。

- 戻りエラー・コードが警告のステータスを示したとき、関連の LDAP リクエストは続行します。
- 戻りコードが失敗ステータスを示すと、リクエストは続行されません。

関連の LDAP リクエストが後で失敗すると、ディレクトリではプラグイン・モジュールでコミットされたコードをロールバックしません。

操作後サーバー・プラグイン

Oracle Internet Directory サーバーは、LDAP 操作の実行後に、操作後プラグイン・モジュールをコールします。このタイプのプラグインの主な目的は、特定の LDAP 操作が実行された後に、ファンクションを起動することです。たとえば、ロギングや通知は、操作後プラグイン・ファンクションです。

操作後プラグインで例外が発生すると、関連の LDAP 操作はロールバックされません。

関連の LDAP リクエストが失敗しても、操作後プラグインはそのまま実行されます。

操作時サーバー・プラグイン

ディレクトリは、標準の LDAP 操作の実行中に、操作時プラグイン・モジュールをコールします。操作時プラグインは、操作に対するサーバー自身のコードの直前に実行されます。このタイプのプラグインの主な目的は、同じ LDAP トランザクション内で既存の操作を強化することです。操作時プラグインが失敗すると、標準の LDAP 操作は実行されません。操作時プラグインが正常に完了しても、標準の LDAP 操作が失敗すると、プラグインで加えられた変更はロールバックされません。

たとえば、ldapcompare 操作とともに操作時プラグインを使用できます。ディレクトリでは、ディレクトリ自身のサーバー比較コードを実行し、プラグイン開発者によって定義されたプラグイン・モジュールを実行します。

PL/SQL 操作時プラグインは、`ldapadd`、`ldapdelete` および `ldapmodify` でサポートされています。Java 操作時プラグインは、`ldapadd`、`ldapdelete`、`ldapmoddn`、`ldapmodify` および `ldapsearch` でサポートされています。

操作時置換サーバー・プラグイン

操作時置換プラグインは、操作に対するサーバー自身のコードのかわりに実行されます。たとえば、ldapcompare 操作とともに操作時置換プラグインを使用できます。ディレクトリでは、ディレクトリ自身の比較コードは実行されません。かわりに、比較の実行はプラグイン・モジュールに任せます。

PL/SQL 操作時置換プラグインは、`ldapadd`、`ldapcompare`、`ldapdelete`、`ldapmodify` および `ldapbind` でのみサポートされています。

Java 操作時置換プラグインは、`ldapbind`、`ldapcompare`、`ldapdelete`、`ldapmoddn`、`ldapmodify` および `ldapsearch` でサポートされています。

プラグインの作成

プラグイン・フレームワークとは、プラグインを開発、構成および適用する環境です。個々のプラグイン・インスタンスは、プラグイン・モジュールと呼びます。

プラグイン・フレームワークには、次のものが含まれます。

- プラグイン構成ツール
- プラグイン・モジュール・インタフェース
- プラグイン LDAP API
  - PL/SQL パッケージ `ODS.LDAP_PLUGIN`
  - Java パッケージ `oracle.ldap.ospf`

どちらの言語の場合も、次の一般的手順に従い、サーバー・プラグイン・フレームワークを使用します。

1. ユーザー定義プラグイン・プロシージャを PL/SQL または Java で作成します。
2. プラグイン・モジュールをコンパイルします。
3. コマンドラインまたは Oracle Directory Manager のいずれかを使用し、構成エントリ・インタフェースを介して、プラグイン・モジュールを登録します。

PL/SQL プラグイン・モジュールの作成は、PL/SQL パッケージの作成と似ています。いずれも、仕様部分と本文に分かれています。この仕様は Oracle Internet Directory とカスタム・プラグインを接続するインタフェースの役割を果すため、プラグインではなくディレクトリによってプラグインの仕様が決まります。

セキュリティ上および LDAP サーバーの整合性の理由から、PL/SQL プラグインをコンパイルできるのは ODS データベース・スキーマにおいてのみです。これらを、Oracle Internet Directory のバックエンド・データベースの役割を果すデータベースにコンパイルする必要があります。

Java プラグインをコンパイルする前に、CLASSPATH が `$ORACLE_HOME/ldap/jlib/ospf.jar` に設定されていることを確認します。

関連資料： 詳細は、『Oracle Identity Management アプリケーション開発者ガイド』を参照してください。

プラグインの登録と管理

ディレクトリ・サーバーが適時にプラグインをコールできるように、プラグインをディレクトリ・サーバーに登録する必要があります。登録するには、プラグインの構成エントリを `cn=plugin,cn=subconfigsubentry` に作成します。このプラグインには、そのオブジェクト・クラスの 1 つとして `orclPluginConfig` が必要です。

関連資料：

- 『Oracle Identity Management アプリケーション開発者ガイド』のサーバー・プラグインに関する章
- 『Oracle Identity Management ユーザー・リファレンス』のプラグインのスキーマ要素に関する項

orclPluginConfig オブジェクト・クラスについては、これらを参照してください。

この項の項目は次のとおりです。

Oracle Directory Manager を使用したプラグインの登録と管理

この項では、Oracle Directory Manager を使用してプラグイン構成エントリを作成、変更および削除する例を示します。

Oracle Directory Manager によるプラグイン構成エントリの追加

プラグインを登録する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」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. 「**プラグイン管理**」を選択します。右側のペインに「プラグイン管理」ウィンドウが表示されます。
3. 「**作成**」を選択します。「新規プラグイン」ダイアログ・ボックスが表示されます。
4. 「新規プラグイン」ダイアログ・ボックスの「必須プロパティ」タブ・ページと「オプション・プロパティ」タブ・ページで、フィールドに値を入力します。フィールドについては、A-9 ページの表 A-15 と A-10 ページの表 A-16 を参照してください。
5. 値を入力した後、「**OK**」を選択します。「プラグイン管理」ウィンドウに戻ります。作成したプラグインが「プラグイン・エントリ名」列に表示されます。
6. 「**OK**」を選択します。

Oracle Directory Manager によるプラグインの編集

プラグイン・エントリを編集する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」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. 「**プラグイン管理**」を選択します。右側のペインに「プラグイン管理」ウィンドウが表示されます。
3. 右側のペインで、編集するプラグイン・エントリの名前を選択し、「**編集**」を選択します。「プラグイン」ダイアログ・ボックスが表示されます。
4. 「プラグイン」ダイアログ・ボックスの「必須プロパティ」タブ・ページと「オプション・プロパティ」タブ・ページで、該当するフィールドに値を変更します。フィールドについては、A-11 ページの表 A-17 と A-12 ページの表 A-18 を参照してください。「必須プロパティ」タブ・ページまたは「オプション・プロパティ」タブ・ページで表示されていない属性を追加するには、「拡張」タブ・ページ（A-12 ページの表 A-19 を参照）を使用します。
5. 「**OK**」を選択します。

Oracle Directory Manager によるプラグインの削除

プラグインを削除する手順は、次のとおりです。

1. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」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. 「**プラグイン管理**」を選択します。右側のペインに「プラグイン管理」ウィンドウが表示されます。
3. 右側のペインで、削除するプラグイン・エントリの名前を選択し、「**編集**」を選択します。「プラグイン」ダイアログ・ボックスが表示されます。
4. 「プラグイン」ダイアログ・ボックスで、「**削除**」を選択します。プロンプトに従って削除を確認します。「プラグイン管理」ウィンドウに戻ります。削除したプラグイン・エントリは、リストに表示されなくなります。

コマンドライン・ツールを使用したプラグインの登録と管理

この項では、コマンドライン・ツールを使用してプラグイン構成エントリを作成、変更および削除する例を示します。

関連資料：

- 『Oracle Identity Management アプリケーション開発者ガイド』のサーバー・プラグインに関する章
- 『Oracle Identity Management ユーザー・リファレンス』のプラグインのスキーマ要素に関する項

orclPluginConfig オブジェクト・クラスについては、これらを参照してください。

例 : コマンドライン・ツールによるプラグイン構成エントリの追加

コマンドラインからプラグイン構成エントリを追加するには、プラグイン構成を含む LDIF ファイルを作成します。cn=plugin,cn=subconfigsubentry で識別名を指定します。

次の 2 つの部分から成る LDIF ファイル my_ldif_file.ldif は、my_plugin1 という操作ベース・プラグイン用のエントリを作成します。

```
dn: 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
orclPluginAttributeList: userpassword

dn: 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
```

このファイルを、次のようなコマンドで、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
```

注意 : プラグイン構成エントリはレプリケートされません。レプリケートすると、一貫性のない状態になります。

例 : コマンドライン・ツールによるプラグイン構成エントリの変更

次に、プラグインを無効にする例を示します。

```
ldapmodify -h  host_name -p  port_number -D cn=orcladmin -w orcladminpwd <<EOF
dn: cn=post_mod_plugin,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclPluginEnable
orclPluginEnable: 0
EOF
```

例 : コマンドライン・ツールによるプラグイン構成エントリの削除

次に、プラグインを削除する例を示します。

```
ldapdelete -h  host_name -p port_number -D cn=orcladmin \
          -w orcladminpwd "cn=post_mod_plugin,cn=plugin,cn=subconfigsubentry"
```

33

Oracle Internet Directory のパスワード・ポリシー・プラグイン

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

この章の項目は次のとおりです。

パスワード・ポリシー・プラグインの動作

パスワードを追加または変更する場合、カスタマイズされたパスワード値チェックが次のように処理されます。

1. クライアントが、ldapadd リクエストまたは ldapmodify リクエストをディレクトリ・サーバーに送信します。
2. ディレクトリ・サーバーは、追加または変更を行う前にパスワード値をプラグインに渡します。
3. プラグインは次のように動作します。
   a. エントリを解析
   b. クリア・テキストの `userpassword` 属性値を取得
   c. 指定したパスワード値チェックを実施
4. パスワードが指定と一致する場合は、そのことがプラグインによってディレクトリ・サーバーに通知され、ディレクトリ・サーバーによって追加または変更が行われます。

   一致しない場合は、次のいずれかのエラー・メッセージがプラグインによってディレクトリ・サーバーに送信され、その後、ディレクトリ・サーバーからクライアントに渡されます。

   ```
   ldap_add: UnKnown Error Encountered
   ldap_add: additional info: PASSWORD POLICY VIOLATION:0000X, less than 8 chars

   ldap_add: UnKnown Error Encountered
   ldap_add: additional info: PASSWORD POLICY VIOLATION:0000X, contains dictionary
   word
   ```

   同じロジックが PRE ldapmodify プラグインにも適用されます。

パスワード・ポリシー・プラグインが実行できる値チェックには、次のような種類があります。

- アルファベットの最大および最小文字数
- 数字の最大文字数
- 記号の最大および最小文字数
- 連続した文字の最大文字数
- 任意の文字の最大インスタンス数
- 辞書の語句かどうかの確認

例 : カスタマイズされたパスワード・ポリシー・プラグインのインストール、構成および有効化

この例は、PL/SQL プログラム pluginpkg.sql（33-5 ページの「サンプル PL/SQL パッケージ pluginpkg.sql の内容」を参照）を使用しています。通常、このパッケージには次のものが含まれます。

- プラグイン・モジュール : pre_add および pre_modify
- パスワードが最小文字数要件の 8 文字を満たしていること、および 4 文字よりも長い辞書の語句を含んでいないことを確認する値チェック・ファンクション isGoodPwd

この例では、ユーザーが 8 文字未満の userpassword 値を入力すると、リクエストは拒否されます。同様に、ユーザー・パスワードを変更する際に、新しいパスワード値が 8 文字未満の場合はリクエストが拒否されます。また、userpassword の値 supersunday を使用してユーザー・パスワードを登録または変更しようとすると、super および sunday が辞書にあるため、そのパスワードは拒否されます。

辞書は 5 文字以上の語句のリストで、最初は words.text というファイルに保存されます。プラグインを実装する場合は、その前にデータベース・テーブルを設定し、語句を格納しておきます。テーブルを設定するには、create.sql を使用します。その内容は次のとおりです。

```
drop table mydic;
create table mydic (word varchar2(1024));
commit;
exit;
```

続いて、次の sqlldr コマンドを使用して語句をテーブルに格納します。

```
sqlldr control=words.txt userid=ods/ods_password
```

この項の項目は次のとおりです。

- PL/SQL プログラムのロードおよび登録
- パスワード・ポリシー・プラグインのコード化
- パスワード・ポリシー・プラグインのデバッグ
- サンプル PL/SQL パッケージ pluginpkg.sql の内容

PL/SQL プログラムのロードおよび登録

スタンドアロンの値チェック PL/SQL プログラムを実装したら、次の手順を実行します。

1. プラグイン・パッケージをデータベースにロードします。この例では、次のように入力します。

   ```
   sqlplus ods/odspwd @pluginpkg.sql
   ```

2. プラグインを登録します。この例では、次の内容のファイル pluginreg.dat を使用します。

   ```
   ### add plugin ###
   dn: cn=pre_add_plugin,cn=plugin,cn=subconfigsubentry
   objectclass:orclPluginConfig
   objectclass:top
   orclpluginname:pwd_plugin
   orclplugintype:operational
   orclplugintiming:pre
   orclpluginldapoperation:ldapadd
   orclpluginenable:1
   orclpluginversion:1.0.1
   cn:pre_add_plugin
   orclpluginsubscriberdnlist:dc=com;o=IMC ,c=US
   ```

```
### modify plugin ###
dn: cn=pre_mod_plugin,cn=plugin,cn=subconfigsubentry
objectclass:orclPluginConfig
objectclass:top
orclpluginname:pwd_plugin
orclplugintype:operational
orclplugintiming:pre
orclpluginldapoperation:ldapmodify
orclpluginenable:1
orclpluginversion:1.0.1
cn:pre_mod_plugin
orclpluginsubscriberdnlist:dc=com;o=IMC ,c=US
orclpluginattributelist:userpassword
```

このプラグインでは、ldapadd リクエストまたは ldapmodify リクエストを受け取った際に起動する 2 つのプラグイン・モジュールをディレクトリ・サーバーに認識させています。ターゲット・エントリが dc=com または o=IMC,c=US 下の場合のみプラグインが起動するように、orclpluginsubscriberdnlist:dc=com;o=IMC,c=US を使用しています。

このファイルをディレクトリに追加するには、次のとおり入力します。

```
ldapadd -p portnum -h hostname -D cn=orcladmin -w orcladminpwd -v \
        -f pluginreg.dat
```

パスワード・ポリシー・プラグインのコード化

標準 PL/SQL 文字ファンクションを使用して、パスワード値を処理できます。正規表現を行う PL/SQL プログラムをダウンロードします。値チェック・ファンクションとプラグイン・モジュールを統合することが重要です。

パスワード・ポリシー・プラグインのデバッグ

ディレクトリ・サーバー・プラグインを設定すると、プラグインのプロセスと内容を調べることができます。

ディレクトリ・サーバー・プラグインのデバッグを設定するには、次のコマンドを実行します。

```
sqlplus ods/password @$ORACLE/ldap/admin/oidspdsu.pls
```

ディレクトリ・サーバー・プラグインのデバッグを有効にするには、次のコマンドを実行します。

```
sqlplus ods/password @$ORACLE/ldap/admin/oidspdon.pls
```

ディレクトリ・サーバー・プラグインのデバッグを無効にするには、次のコマンドを実行します。

```
sqlplus ods/password @$ORACLE/ldap/admin/oidspdof.pls
```

ディレクトリ・サーバー・プラグインのデバッグ・メッセージを表示するには、次のコマンドを実行します。

```
sqlplus ods/password @$ORACLE/ldap/admin/oidspdsh.pls
```

ディレクトリ・サーバー・プラグインのデバッグ・メッセージを削除するには、次のコマンドを実行します。

```
sqlplus ods/password @$ORACLE/ldap/admin/oidspdde.pls
```

サンプル PL/SQL パッケージ pluginpkg.sql の内容

この例で使用するスクリプト pluginpkg.sql の内容は次のとおりです。

```
CREATE OR REPLACE PACKAGE pwd_plugin AS

PROCEDURE pre_add (ldapplugincontext IN  ODS.plugincontext,
   dn       IN  VARCHAR2,
   entry    IN  ODS.entryobj,
   rc       OUT INTEGER,
   errormsg OUT VARCHAR2
   );

PROCEDURE pre_modify (ldapplugincontext IN  ODS.plugincontext,
      dn       IN  VARCHAR2,
      mods     IN  ODS.modlist,
      rc       OUT INTEGER,
      errormsg OUT VARCHAR2
      );

-- Function: isGoodPwd
-- Parameter: inpwd
-- Purpose: 1. check if the password is at least
--          8 characters long
--          2. check if the password contains a
--          dictionary word (longer than 4 characters)

FUNCTION isGoodPwd(inpwd IN VARCHAR2)
  RETURN INTEGER;


END pwd_plugin;
/

show error

CREATE OR REPLACE PACKAGE BODY pwd_plugin AS

FUNCTION isGoodPwd(inpwd IN VARCHAR2)
  RETURN INTEGER
  IS
     i NUMBER;
     ret NUMBER DEFAULT 1;
     minpwdlen NUMBER DEFAULT 8;
     len       NUMBER DEFAULT 0;
     lcount    NUMBER DEFAULT 0;
     matched   VARCHAR2(1024) DEFAULT NULL;

     CURSOR c1 IS
     SELECT word FROM mydic WHERE length(word) > 4
     AND instr(lower(inpwd), lower(word), 1, 1) > 0;

BEGIN
   plg_debug( '=== begin of ISGOODPWD ===');
   plg_debug( 'password = ' || inpwd);
   len := LENGTH(inpwd);
   plg_debug( 'password length = ' || len);

   IF len < minpwdlen THEN
      RETURN 0;
    ELSE
      OPEN c1;
      LOOP
        FETCH c1 INTO matched;
```

```
        EXIT WHEN c1%NOTFOUND;
        lcount := lcount + 1;
      END LOOP;
      plg_debug( 'count = ' || lcount);
      IF lcount > 0 THEN
        RETURN 2;
      ELSE
        RETURN ret;
      END IF;
   END IF;

   plg_debug( '=== end of ISGOODPWD ===');

EXCEPTION
   WHEN OTHERS THEN
      plg_debug( 'Exception in isGoodPwd(). Error code is ' || TO_CHAR(SQLCODE));
      plg_debug( '   ' || Sqlerrm);
      RETURN 0;
END;


PROCEDURE pre_add (ldapplugincontext IN  ODS.plugincontext,
   dn       IN  VARCHAR2,
   entry    IN  ODS.entryobj,
   rc       OUT INTEGER,
   errormsg OUT VARCHAR2
   )
  IS
     inpwd VARCHAR2(256) DEFAULT NULL;
     ret   NUMBER        DEFAULT 1;
BEGIN
   plg_debug( '=== begin of PRE_ADD_PLUGIN ===');
   plg_debug( 'dn = ' || dn);

   plg_debug( 'entry obj ' || ':entryname = ' || entry.entryname);

   FOR l_counter1 IN 1..entry.attr.COUNT LOOP
      plg_debug( 'attrname[' || l_counter1 || '] = ' ||
entry.attr(l_counter1).attrname);
      FOR l_counter2 IN 1..entry.attr(l_counter1).attrval.COUNT LOOP
plg_debug( entry.attr(l_counter1).attrname ||
    '[' || l_counter1 || ']' ||
    '.val[' || l_counter2 || '] = ' ||
    entry.attr(l_counter1).attrval(l_counter2));
      END LOOP;

      IF entry.attr(l_counter1).attrname = 'userpassword' THEN
inpwd := entry.attr(l_counter1).attrval(1);
-- assuming only one attr val for userpassword
      END IF;

   END LOOP;

   IF (inpwd IS NOT NULL) THEN
      ret := isGoodPwd(inpwd);
   END IF;

   IF (inpwd IS NULL OR ret = 0) THEN
      rc := 1;
      errormsg := 'PASSWORD POLICY VIOLATION:0000X, less than 8 chars';
      plg_debug( ' we got an invalid password, too short ');
    ELSIF (ret = 2) THEN
      rc := 1;
```

```
      errormsg := 'PASSWORD POLICY VIOLATION:0000X, contains dictionary word';
      plg_debug( ' we got an invalid password, dictionary word ');
    ELSE
      plg_debug( ' we got a good password ');
      rc := 0;
      errormsg := 'no pre_mod plguin error msg';
   END IF;

   plg_debug( '=== end of PRE_ADD_PLUGIN ===');

EXCEPTION
   WHEN OTHERS THEN
      plg_debug( 'Exception in PRE_ADD plugin. Error code is ' || TO_CHAR(SQLCODE));
      plg_debug( '   ' || Sqlerrm);
      rc := 1;
      errormsg := 'exception: pre_add plguin';
END;

PROCEDURE pre_modify (ldapplugincontext IN  ODS.plugincontext,
     dn       IN  VARCHAR2,
     mods     IN  ODS.modlist,
     rc       OUT INTEGER,
     errormsg OUT VARCHAR2
     )
  IS
     old_passwd VARCHAR2(256) DEFAULT NULL;
     new_passwd VARCHAR2(256) DEFAULT NULL;
     ret        NUMBER        DEFAULT 1;

BEGIN
   plg_debug( '=== begin of PRE_MOD_PLUGIN ===');
   plg_debug( dn);

   FOR l_counter1 IN 1..mods.COUNT LOOP
      IF (mods(l_counter1).operation = 2) AND
(mods(l_counter1).type = 'userpassword') THEN

 FOR l_counter2 IN 1..mods(l_counter1).vals.COUNT LOOP
    new_passwd := mods(l_counter1).vals(l_counter2).val;
 END LOOP;
      END IF;

      IF (mods(l_counter1).operation = 0) AND
(mods(l_counter1).type = 'userpassword') THEN

 FOR l_counter2 IN 1..mods(l_counter1).vals.COUNT LOOP
    new_passwd := mods(l_counter1).vals(l_counter2).val;
 END LOOP;
      END IF;

      IF (mods(l_counter1).operation = 1) AND
(mods(l_counter1).type = 'userpassword') THEN

 FOR l_counter2 IN 1..mods(l_counter1).vals.COUNT LOOP
    old_passwd := mods(l_counter1).vals(l_counter2).val;
 END LOOP;
      END IF;
   END LOOP;

   plg_debug(' new password: ' || new_passwd);
   plg_debug(' old password: ' || old_passwd);
```

```
   IF (new_passwd IS NOT NULL) THEN
      ret := isGoodPwd(new_passwd);
   END IF;

   IF (new_passwd IS NULL OR ret = 0) THEN
      rc := 1;
      errormsg := 'PASSWORD POLICY VIOLATION:0000X, less than 8 chars';
      plg_debug( ' we got an invalid password, too short ');
    ELSIF (ret = 2) THEN
      rc := 1;
      errormsg := 'PASSWORD POLICY VIOLATION:0000X, contains dictionary word';
      plg_debug( ' we got an invalid password, dictionary word ');
    ELSE
      plg_debug( ' we got a good password ');
      rc := 0;
      errormsg := 'no pre_mod plguin error msg';
   END IF;

   plg_debug( '=== end of PRE_MOD_PLUGIN ===');

EXCEPTION
   WHEN OTHERS THEN
      plg_debug( 'Exception in PRE_MODIFY plugin. Error code is ' || TO_CHAR(SQLCODE));
      plg_debug( '    ' || Sqlerrm);
      rc := 1;
      errormsg := 'exception: pre_mod plguin';
END;

END pwd_plugin;
/
show error


EXIT;
```

34

カスタマイズされた外部認証プラグインの設定

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

この章の項目は次のとおりです。

ネイティブ認証と外部認証との対比

Oracle Internet Directory に格納されたセキュリティ資格証明に基づく認証を、ネイティブ認証と呼びます。ユーザーがセキュリティ資格証明を入力すると、ディレクトリ・サーバーは Oracle Internet Directory に格納されている資格証明とそれを比較します。資格証明が一致すると、ディレクトリ・サーバーはユーザーを認証します。

Oracle Internet Directory 以外のディレクトリに格納されたセキュリティ資格証明に基づく認証を、外部認証と呼びます。ユーザーがセキュリティ資格証明を入力すると、ディレクトリ・サーバーは他のディレクトリに格納されている資格証明とそれを比較します。この比較は次のものを使用して行われます。

- 外部認証作業を行う PL/SQL プログラム
- この PL/SQL プログラムを起動する外部認証プラグイン

例 : 外部認証プラグインのインストール、構成および有効化

この項の項目は次のとおりです。

サンプル PL/SQL パッケージ oidexaup.sql

この例は、PL/SQL プログラム `oidexaup.sql`（34-4 ページの「PL/SQL パッケージ oidexaup.sql の内容」を参照）を使用しています。このパッケージは、外部認証プラグイン PL/SQL パッケージをインストールするために使用します。このパッケージには次のものが含まれています。

- 2 つのプラグイン（`when_compare_replace` および `when_modify_replace`）
- ユーティリティ・ファンクション（`get_nickname`）

統合パッケージは、プラグイン・パッケージ `OIDEXTAUTH` です。このパッケージは、テンプレートとして使用し、配置環境に合せて変更することもできます。

外部認証プラグインをインストールおよび構成し、有効にする手順は、次のとおりです。

1. スタンドアロンの外部認証 PL/SQL プログラムを実装します。たとえば、ユーザー名とパスワードで認証する場合は、この 2 つのパラメータを取る PL/SQL プログラムを使用する必要があります。

   サンプル・コードでは、`oidexaup.sql`、`auth_external` はプログラム・パッケージ名で、`authenticate_user` は認証を行うファンクションです。スタンドアロンのプログラムが適切に動作していることを確認してから、次の手順に進んでください。

2. スタンドアロンのプログラムをプラグイン・モジュールに登録します。
3. プラグイン・パッケージをデータベースにロードします。この例では、次のように入力します。

   ```
   sqlplus ods/odspwd @oidexaup.sql
   ```

4. プラグインを登録します。プラグインの起動に必要な情報をディレクトリ・サーバーに提供する LDIF ファイルを作成し、アップロードすることにより登録します。

5. この例では、次の内容のファイル oidexauth.ldif を使用します。

```
dn: cn=whencompare,cn=plugin,cn=subconfigsubentry
objectclass:orclPluginConfig
objectclass:top
orclpluginname:oidextauth
orclplugintype:operational
orclplugintiming:when
orclpluginldapoperation:ldapcompare
orclpluginenable:1
orclpluginversion:1.0.1
orclPluginIsReplace:1
cn:whencompare
orclpluginsubscriberdnlist:dc=com;o=IMC,c=US
orclpluginattributelist:userpassword
orclpluginrequestgroup:$prgdn

dn: cn=whenmodify,cn=plugin,cn=subconfigsubentry
objectclass:orclPluginConfig
objectclass:top
orclpluginname:oidextauth
orclplugintype:operational
orclplugintiming:when
orclpluginldapoperation:ldapmodify
orclpluginenable:1
orclpluginversion:1.0.1
orclPluginIsReplace:1
cn:whenmodify
orclpluginsubscriberdnlist:dc=com;o=IMC,c=US
orclpluginattributelist:userpassword
orclpluginrequestgroup:$prgdn
```

このファイルでは、ldapcompare リクエストまたは ldapmodify リクエストがあった際に 2 つのプラグインが起動することをディレクトリ・サーバーに通知します。

ターゲット・エントリが dc=com または o=IMC、c=US 下の場合のみプラグインが起動するように、orclpluginsubscriberdnlist:dc=com;o=IMC,c=US を使用しています。

$prgdn を、プラグイン・リクエスト・グループ識別名に置換します。これはオプションの推奨セキュリティ機能です。Oracle Application Server Single Sign-On との統合には、この値が必須フィールドです。入力されたグループのメンバーのみがプラグインを起動できます。複数のグループの入力が可能です。エントリを区切るには、セミコロンを使用します。

推奨デフォルトは、
cn=OracleUserSecurityAdmins,cn=Groups,cn=OracleContext および
cn=OracleDASAdminGroup,cn=Groups,cn=OracleContext,o=default_subscriber,dc=com です。Oracle Application Server Single Sign-On Server は、最初のグループのメンバーです。また、配置環境に合せて o=default_subscriber を正しい値に置換してください。

このファイルをディレクトリに追加するには、次のとおり入力します。

```
ldapadd -p portnum -h hostname -D cn=orcladmin -w orcladminpwd -v \
        -f oidexauth.ldif
```

これで、すべての準備が完了しました。ldapcompare コマンドライン・ツールを使用すると、Oracle Application Server Single Sign-On からユーザーを認証する前にプラグインおよび認証プログラムが適切に動作していることを確認できます。

この例では、ユーザー・パスワードを外部変更するためのプラグイン・コードも提供されています。

外部認証プラグインのデバッグ

ディレクトリ・サーバー・プラグインを設定すると、プラグインのプロセスと内容を調べることができます。

ディレクトリ・サーバー・プラグインのデバッグを設定するには、次のコマンドを実行します。

```
sqlplus ods/password @$ORACLE_HOME/ldap/admin/oidspdsu.sql
```

ディレクトリ・サーバー・プラグインのデバッグを有効にするには、次のコマンドを実行します。

```
sqlplus ods/password @$ORACLE_HOME/ldap/admin/oidspdon.sql
```

ディレクトリ・サーバー・プラグインのデバッグを無効にするには、次のコマンドを実行します。

```
sqlplus ods/password @$ORACLE_HOME/ldap/admin/oidspdof.sql
```

ディレクトリ・サーバー・プラグインのデバッグ・メッセージを表示するには、次のコマンドを実行します。

```
sqlplus ods/password @$ORACLE_HOME/ldap/admin/oidspdsh.sql
```

ディレクトリ・サーバー・プラグインのデバッグ・メッセージを削除するには、次のコマンドを実行します。

```
sqlplus ods/password @$ORACLE_HOME/ldap/admin/oidspdde.sql
```

PL/SQL パッケージ oidexaup.sql の内容

この例で使用するスクリプト oidexaup.sql の内容は次のとおりです。

```
CREATE OR REPLACE PACKAGE OIDEXTAUTH AS

  PROCEDURE when_compare_replace (ldapplugincontext IN  ODS.plugincontext,
                                  result            OUT INTEGER,
                                  dn                IN  VARCHAR2,
                                  attrname          IN  VARCHAR2,
                                  attrval           IN  VARCHAR2,
                                  rc                OUT INTEGER,
                                  errormsg          OUT VARCHAR2
                                  );

  PROCEDURE when_modify_replace (ldapplugincontext IN  ODS.plugincontext,
                                 dn                IN  VARCHAR2,
                                 mods              IN  ODS.modlist,
                                 rc                OUT INTEGER,
                                 errormsg          OUT VARCHAR2
                                 );

  FUNCTION get_nickname (dn         IN  VARCHAR2,
                         my_session IN  DBMS_LDAP.session)
    RETURN VARCHAR2;

END OIDEXTAUTH;
/

SHOW ERROR

CREATE OR REPLACE PACKAGE BODY OIDEXTAUTH AS

  -- We use this function to convert the dn to nickname.
  -- When OID server receives the ldapcompare request, it
  -- only has the dn information. We need to use DBMS_LDAP_UTL
  -- package to find out the nickname attribute value of
  -- the entry.
```

```
FUNCTION get_nickname (dn         IN VARCHAR2,
                       my_session IN DBMS_LDAP.session)
  RETURN VARCHAR2
  IS
     my_pset_coll        DBMS_LDAP_UTL.PROPERTY_SET_COLLECTION;
     my_property_names   DBMS_LDAP.STRING_COLLECTION;
     my_property_values  DBMS_LDAP.STRING_COLLECTION;

     user_handle         DBMS_LDAP_UTL.HANDLE;
     user_id             VARCHAR2(2000);
     user_type           PLS_INTEGER;
     user_nickname       VARCHAR2(256) DEFAULT NULL;

     my_attrs            DBMS_LDAP.STRING_COLLECTION;
     retval              PLS_INTEGER;

BEGIN
   plg_debug( '=== Beginning of get_nickname() === ');
   user_type     := DBMS_LDAP_UTL.TYPE_DN;
   user_id       := dn;

   retval := DBMS_LDAP_UTL.create_user_handle(user_handle, user_type, user_id);

   plg_debug('create_user_handle() Returns ' || To_char(retval));

   retval := DBMS_LDAP_UTL.get_user_properties(my_session,
                                               user_handle,
                                               my_attrs,
                                               DBMS_LDAP_UTL.NICKNAME_PROPERTY,
                                               my_pset_coll);

   plg_debug( 'get_user_properties() Returns ' || To_char(retval));

   IF my_pset_coll.COUNT > 0 THEN
      FOR i IN my_pset_coll.first .. my_pset_coll.last LOOP
         retval := DBMS_LDAP_UTL.get_property_names(my_pset_coll(i),
                                                    my_property_names);
         IF my_property_names.COUNT > 0 THEN
            FOR j IN my_property_names.first .. my_property_names.last LOOP
               retval := DBMS_LDAP_UTL.get_property_values(my_pset_coll(i),
                                                           my_property_names(j),
                                                           my_property_values);
               IF my_property_values.COUNT > 0 THEN
                  FOR k IN my_property_values.FIRST..my_property_values.LAST LOOP
                     user_nickname := my_property_values(k);
                     plg_debug( 'user nickname = ' || user_nickname);
                  END LOOP;
               END IF;
            END LOOP;
         END IF; -- IF my_property_names.count > 0
      END LOOP;
   END IF; -- If my_pset_coll.count > 0

   plg_debug( 'got user_nickname: ' || user_nickname);

   -- Free my_properties
   IF my_pset_coll.count > 0 then
      DBMS_LDAP_UTL.free_propertyset_collection(my_pset_coll);
   END IF;

   DBMS_LDAP_UTL.free_handle(user_handle);

   RETURN user_nickname;
```

```
EXCEPTION
   WHEN OTHERS THEN
      plg_debug('Exception in get_nickname. Error code is ' || to_char(sqlcode));
      plg_debug('   ' || Sqlerrm);
      RETURN NULL;
END;


PROCEDURE when_compare_replace (ldapplugincontext IN  ODS.plugincontext,
                                result            OUT INTEGER,
                                dn                IN  VARCHAR2,
                                attrname          IN  VARCHAR2,
                                attrval           IN  VARCHAR2,
                                rc                OUT INTEGER,
                                errormsg          OUT VARCHAR2
                                )
  IS
     retval pls_integer;
     lresult BOOLEAN;

     my_session          DBMS_LDAP.session;
     my_property_names   DBMS_LDAP.STRING_COLLECTION;
     my_property_values  DBMS_LDAP.STRING_COLLECTION;
     my_attrs            DBMS_LDAP.STRING_COLLECTION;
     my_pset_coll        DBMS_LDAP_UTL.PROPERTY_SET_COLLECTION;
     user_handle         DBMS_LDAP_UTL.HANDLE;

     user_id             VARCHAR2(2000);
     user_type           PLS_INTEGER;
     user_nickname       VARCHAR2(60);
     remote_dn           VARCHAR2(256);

     i                   PLS_INTEGER;
     j                   PLS_INTEGER;
     k                   PLS_INTEGER;

BEGIN
   plg_debug( '=== Begin of WHEN-COMPARE-REPLACE plug-in');
   plg_debug( 'DN = ' || dn);
   plg_debug( 'Attr = ' || attrname);
   --plg_debug( 'Attrval = ' || attrval);

   DBMS_LDAP.USE_EXCEPTION := FALSE;
   errormsg := 'No error msg';
   rc := 0;

   -- converting dn to nickname
   my_session := LDAP_PLUGIN.init(ldapplugincontext);
   plg_debug( 'ldap_session =' || RAWTOHEX(SUBSTR(my_session,1,8)));

   retval := LDAP_PLUGIN.simple_bind_s(ldapplugincontext, my_session);
   plg_debug( 'simple_bind_res =' || TO_CHAR(retval));

   user_nickname := get_nickname(dn, my_session);
   plg_debug( 'user_nickname =' || user_nickname);

   -- unbind from the directory
   retval := DBMS_LDAP.unbind_s(my_session);
   plg_debug( 'unbind_res Returns ' || To_char(retval));
```

```
   IF (user_nickname IS NULL) THEN
      result := 32;
      errormsg := 'Can''t find the nickname';
      plg_debug( 'Can''t find the nickname');
      RETURN;
   END IF;

   plg_debug( '=== Now go to extauth ');

   BEGIN
      retval := auth_external.authenticate_user(user_nickname, attrval);
      plg_debug( 'auth_external.authenticate_user() returns = ' || 'True');
      result := 6; -- compare result is TRUE
   EXCEPTION
      WHEN OTHERS THEN
         result := 5; -- compare result is FALSE
         plg_debug( 'auth_external.authenticate_user() returns = ' || 'False');
         RETURN;
   END;

   plg_debug( '=== End of WHEN-COMPARE-REPLACE plug-in');
EXCEPTION
   WHEN OTHERS THEN
      rc := 1;
      errormsg := 'Exception: when_compare_replace plugin';
      plg_debug( 'EXCEPTION: ' || retval);
      plg_debug('Exception in when_compare. Error code is ' || to_char(sqlcode));
      plg_debug('   ' || Sqlerrm);
END;


PROCEDURE when_modify_replace (ldappluginсontext IN  ODS.plugincontext,
                               dn                IN  VARCHAR2,
                               mods              IN  ODS.modlist,
                               rc                OUT INTEGER,
                               errormsg          OUT VARCHAR2
                               )
  IS
     retval pls_integer;
     lresult BOOLEAN;

     my_session          DBMS_LDAP.SESSION;
     my_property_names   DBMS_LDAP.STRING_COLLECTION;
     my_property_values  DBMS_LDAP.STRING_COLLECTION;
     my_attrs            DBMS_LDAP.STRING_COLLECTION;
     my_modval           DBMS_LDAP.BERVAL_COLLECTION;
     my_pset_coll        DBMS_LDAP_UTL.PROPERTY_SET_COLLECTION;
     user_handle         DBMS_LDAP_UTL.HANDLE;

     l_mod_array         RAW(32);
     user_id             VARCHAR2(2000);
     user_type           PLS_INTEGER;
     user_nickname       VARCHAR2(2000);
     old_passwd          VARCHAR2(60) DEFAULT NULL;
     new_passwd          VARCHAR2(60) DEFAULT NULL;
     remote_dn           VARCHAR2(256);

     i                   PLS_INTEGER;
     j                   PLS_INTEGER;
     k                   PLS_INTEGER;

BEGIN
   plg_debug( '=== Begin of WHEN-MODIFY-REPLACE plug-in');
```

```
DBMS_LDAP.USE_EXCEPTION := FALSE;
user_type     := DBMS_LDAP_UTL.TYPE_DN;
user_id       := dn;

-- converting dn to nickname
my_session := LDAP_PLUGIN.init(ldapplugincontext);
plg_debug( 'ldap_session =' || RAWTOHEX(SUBSTR(my_session,1,8)));

retval := LDAP_PLUGIN.simple_bind_s(ldapplugincontext, my_session);
plg_debug( 'simple_bind_res =' || TO_CHAR(retval));

user_nickname := get_nickname(dn, my_session);
plg_debug( 'user_nickname =' || user_nickname);

-- unbind from the directory
retval := DBMS_LDAP.unbind_s(my_session);

FOR l_counter1 IN 1..mods.COUNT LOOP
   IF (mods(l_counter1).operation = 2) AND
     (mods(l_counter1).type = 'userpassword') THEN

      FOR l_counter2 IN 1..mods(l_counter1).vals.COUNT LOOP
         new_passwd := mods(l_counter1).vals(l_counter2).val;
      END LOOP;
   END IF;

   IF (mods(l_counter1).operation = 0) AND
     (mods(l_counter1).type = 'userpassword') THEN

      FOR l_counter2 IN 1..mods(l_counter1).vals.COUNT LOOP
         new_passwd := mods(l_counter1).vals(l_counter2).val;
      END LOOP;
   END IF;

   IF (mods(l_counter1).operation = 1) AND
     (mods(l_counter1).type = 'userpassword') THEN

      FOR l_counter2 IN 1..mods(l_counter1).vals.COUNT LOOP
         old_passwd := mods(l_counter1).vals(l_counter2).val;
      END LOOP;
   END IF;
END LOOP;

IF new_passwd IS NOT NULL AND old_passwd IS NOT NULL THEN
  BEGIN
     auth_external.change_passwd(user_nickname, old_passwd, new_passwd);
  EXCEPTION
     WHEN OTHERS THEN
        rc := 1;
        plg_debug( 'auth_external.change_passwd() raised exception.');
        errormsg := 'auth_external.change_passwd() raised exception.';
        RETURN;
  END;
 ELSIF new_passwd IS NOT NULL AND old_passwd IS NULL THEN
  BEGIN
     auth_external.reset_passwd(user_nickname, new_passwd);
  EXCEPTION
     WHEN OTHERS THEN
        plg_debug( 'auth_external.reset_passwd() raised exception.');
        rc := 1;
        errormsg := 'auth_external.reset_passwd() raised exception.';
        RETURN;
  END;
```

```
     ELSE
            rc := 1;
            errormsg := 'PLG_Exception. Not enough info to change passwd.';
    END IF;

    plg_debug( 'external change password succeed');
    rc := 0;
    errormsg := 'No when_mod_replace plguin error msg';

    retval := DBMS_LDAP.unbind_s(my_session);

    plg_debug( 'End of WHEN-MODIFY-REPLACE');
    --COMMIT;
  EXCEPTION
    WHEN others THEN
       rc := 1;
       errormsg := 'PLG_Exception: when_modify_replace plguin';
       plg_debug('Exception in when_modify. Error code is ' || to_char(sqlcode));
       plg_debug('   ' || Sqlerrm);
  END;

END OIDEXTAUTH;
/
SHOW ERRORS
--list


EXIT;
```

第 VII 部

付録

第 VII 部は次の各付録で構成されています。

- 付録 A「Oracle Directory Manager のウィンドウとフィールド」
- 付録 B「LDAP フィルタ定義」
- 付録 C「アクセス制御ディレクティブ書式」
- 付録 D「ディレクトリにおけるグローバリゼーション・サポート」
- 付録 E「ユーザーおよびグループの作成ベースおよび検索ベースに対するアクセス制御の設定」
- 付録 F「マルチマスター・レプリケーション・プロセス」
- 付録 G「ディレクトリでのユーザー証明書の検索」
- 付録 H「LDAP のレプリカ状態」
- 付録 I「データベース・コピー・プロシージャを使用したディレクトリ・ノードの追加」
- 付録 J「Oracle Internet Directory を使用した UNIX 認証およびユーザー・プロビジョニング」
- 付録 K「Oracle Internet Directory でサポートされている RFC」
- 付録 L「Oracle Internet Directory に関するトラブルシューティング」

A

Oracle Directory Manager のウィンドウとフィールド

この付録では、Oracle Directory Manager の様々なウィンドウとフィールドについて説明します。この付録の項目は次のとおりです。

Oracle Directory Manager の接続管理フィールド

表 A-1「資格証明」タブ・ページのフィールド

フィールド	説明
ユーザー	初めてログインするときは、**スーパーユーザー**または匿名でログインします。このセッション中に SSL の機能を構成する場合は、スーパーユーザーでログインします。 スーパーユーザーでログインする場合は、「ユーザー」ボックスに `cn=orcladmin` と入力します。 匿名でログインする場合は、「ユーザー」ボックスを空白のままにします。 LDAP のコマンドライン・ツールを使用してユーザーのエントリをすでに設定している場合は、次の 2 つの方法いずれかでそのユーザーのエントリを入力できます。 ■ 「ユーザー」フィールドの右側のボタンを使用し、そのエントリを参照して選択します。 ■ そのユーザーのエントリに対する**識別名**を、次の例のように正しい書式で入力します。 `cn=Susie Brown,ou=HR,o=acme,c=us`
パスワード	スーパーユーザーでログインし、インストール時にスーパーユーザー用のパスワードを指定している場合は、そのパスワードを「**パスワード**」フィールドに入力します。パスワードを指定していない場合は、デフォルトのパスワード `welcome` を入力します。Oracle Directory Manager にログインし、ディレクトリ・サーバーに接続した後、ディレクトリを保護するためにこのパスワードを変更してください。 匿名でログインする場合は、「**パスワード**」フィールドを空白のままにします。 特定のディレクトリ・ユーザーとしてログインする場合は、対応するパスワードを入力してください。 **関連項目：**パスワードの変更方法は、7-9 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。
サーバー	「**サーバー**」リストから、接続するディレクトリ・サーバーのあるホストを選択します。 ディレクトリ・サーバーにすでに接続している場合に、別のホストのディレクトリ・サーバーに接続する手順は、次のとおりです。 1. 「**サーバー**」リストの右側のボタンをクリックします。使用可能なサーバーのリストが、「ディレクトリ・サーバーの選択」ダイアログ・ボックスに表示されます。 2. サーバーを選択します。 3. 「**OK**」を選択します。 ディレクトリ・サーバーをリストに追加する手順は、次のとおりです。 1. 「ディレクトリ・サーバーの選択」ダイアログ・ボックスで、「**追加**」を選択します。「ディレクトリ・サーバーの接続」ダイアログ・ボックスが表示されます。 2. 「**サーバー**」フィールドに、追加するディレクトリ・サーバーの名前を入力します。 3. 「**ポート**」フィールドに、追加するサーバーのポート番号を入力します。 4. 「**OK**」を選択します。追加したディレクトリが、「ディレクトリ・サーバーの選択」ダイアログ・ボックスのリストに表示されます。 リストにあるディレクトリ・サーバーを変更する手順は、次のとおりです。 1. 変更するディレクトリ・サーバーを選択します。 2. 「**編集**」を選択します。「ディレクトリ・サーバーの接続」ダイアログ・ボックスが表示されます。 3. 「**サーバー**」フィールドおよび「**ポート**」フィールドを変更して、「**OK**」を選択します。サーバーに対する変更が、「ディレクトリ・サーバーの選択」ダイアログ・ボックスのリストに表示されます。

表 A-1「資格証明」タブ・ページのフィールド（続き）

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

表 A-2「SSL」タブ・ページのフィールド

フィールド	説明
SSL 位置	クライアントとサーバーの認証に使用するクライアントの Wallet を指定します。クライアントの Wallet がローカル・マシン上にある場合は、その Wallet のパスとファイル名を次の構文で入力します。 `file: absolute_path_name` Wallet が別のマシン上にある場合は、その位置にリンクして、Wallet のリンク・パスとファイル名を入力します。
SSL パスワード	ユーザーの Wallet をオープンするパスワード。
SSL 認証	認証レベルを次の中から選択します。 ■ SSL 認証なし : クライアントとサーバーのいずれも、相手に対して自己認証を行いません。証明書の送信または交換は行われません。「資格証明」タブの「SSL 有効」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認証 : 双方向認証。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 : 一方向認証。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。

Oracle Directory Manager のアクセス制御管理フィールド

表 A-3 に、Oracle Directory Manager のアクセス制御管理フィールドとその説明を示します。

表 A-3「アクセス制御管理」ペインのフィールド

フィールド	説明
サブツリー制御ポイントへのパス	ACP で定義されているパスが表示されます。
サブツリー制御ポイント	ACP が表示されます。

表 A-4 に認証の選択肢、つまりディレクトリに対してユーザーを認証できる方法とその説明を示します。

表 A-4「認証の選択」リストのフィールド

認証の選択	説明
MD5 ダイジェスト	MD5 ダイジェストを使用したバインドにより、「簡易」、「プロキシ」および「匿名」アクセスをブロックします。
PKCS12	PKCS12 を使用したバインドにより、「MD5 ダイジェスト」、「簡易」、「プロキシ」および「匿名」アクセスをブロックします。
プロキシ	■ プロキシ・ユーザーとしてバインドします。この認証オプションは、「匿名」アクセスをブロックします。
簡易	■ パスワード・ベースの認証。このオプションは、「プロキシ」および「匿名」アクセス両方をブロックします。

表 A-5 に暗号化の選択肢、つまりデータを暗号化する方法とその説明を示します。

表 A-5「暗号化の選択」リストのフィールド

認証の選択	説明
SASL	Simple Authentication and Security Layer
SSL 認証なし	クライアントとサーバーのいずれも、相手に対して自己認証を行いません。証明書の送信または交換は行われません。この場合は、SSL 暗号化 / 復号化のみ使用されます。
SSL 一方向	ディレクトリ・サーバーのみ、クライアントに対して自己認証を行います。ディレクトリ・サーバーは、そのサーバーが認証されていることを証明する証明書をクライアントに送信します。

関連項目： 18-8 ページの「バインド・モード」

表 A-6「責任者」タブ・ページでアクセス権限を付与するエンティティ

エンティティ	説明
すべての人 (*)	エントリにアクセスする人すべて。
特定のグループ	事前に定義したグループ名。
特定のエントリ	事前に定義したディレクトリ・エントリ。
サブツリー	ディレクトリ内の選択したサブツリー全体。
セッション・ユーザーの識別名（DN）が属性により識別された場合	識別名がエントリ内の属性である人すべて。たとえば、グループ・エントリに対する読取りアクセス権をグループのメンバーに付与する場合があります。

表 A-6「責任者」タブ・ページでアクセス権限を付与するエンティティ（続き）

エンティティ	説明
セッション・ユーザーのグループが属性により識別された場合	識別名がエントリ内の属性であるグループすべて。
セッション・ユーザーの一意 ID（orclGUID）が属性により識別された場合	このエントリに対してアクセス権を付与または制限するエントリのグローバル・ユーザー識別子（orclGUID）。
セッション・ユーザーの識別名（DN）がアクセス・エントリと一致する場合	指定したエントリで正常にログインしている人すべて。

表 A-7 属性に関するアクセス権

アクセス権	説明
読取り	属性値を読み取る権限。属性に対して読取り権限が与えられている場合でも、エントリ自体に参照権限がないかぎり値は返されません。
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の変更を行う権限。このレベルを使用すると、メンバーがリスト上の自分自身をメンテナンスできます。たとえば、次のコマンドを実行すると、グループ内のユーザーが member 属性上で、自分自身の識別名のみを追加または削除できます。 `access to attr=(member) by dnattr=(member) (selfwrite)` dnattr セレクタは、member 属性にリストされているエンティティにアクセス権が適用されるように指定します。selfwrite アクセス権セレクタは、そのメンバーが、属性上で自分自身の識別名のみを追加または削除できるように指定します。
比較	属性値で比較操作を実行する権限。

Oracle Directory Manager の属性一意性フィールド

表 A-8「新規制約」ダイアログ・ボックスのフィールド

フィールド	説明
属性一意性制約名	作成する属性一意性制約の名前。
一意属性名	ディレクトリ・サーバーがチェックする属性。
一意属性のオブジェクト・クラス	属性一意性制約を施行する、person などのオブジェクト・クラス。デフォルトでは、すべてのオブジェクト・クラスに施行されます。
一意属性の有効範囲	属性制約の検索時にディレクトリ・サーバーが使用するフィルタ。次に例を示します。 ■ base: ルート・エントリのみを検索 ■ onelevel: 1 レベルのみを検索 ■ sub: ディレクトリ全体を検索
一意属性のサブツリー	属性一意性制約を施行するサブツリー。デフォルトでは、ルート・ディレクトリから施行されます。

Oracle Directory Manager のガベージ・コレクション管理フィールド

表 A-9「ガベージ・コレクタ」ウィンドウのフィールド

フィールド	説明
ガベージ・コレクタ名	このフィールドは変更できません。
パージ・ベース	ガベージ・コレクション・タスクが適用されるネーミング・コンテキストのベース識別名。このフィールドは変更できません。
デバッグのパージ	このガベージ・コレクタのデバッグ・ログを有効にするか無効にするかを示すインジケータ。
パージ有効化ステータス	このガベージ・コレクタを有効または無効にします。デフォルトは「有効化」です。
パージ・ファイルの位置	ログ・ファイルがあるディレクトリの絶対パス名。
パージ・ファイル名	ログ・ファイルの名前。
パージの間隔	ガベージ・コレクション・ジョブが再度実行されるまでの間隔（時間単位）。たとえば、この値を 12 に設定すると、ガベージ・コレクションは 12 時間ごとに実行されます。この属性はオプションです。デフォルト値は 24 です。
すぐにパージ	このフィールドに任意の値を入力し、「適用」を選択するとすぐにガベージ・コレクションが開始されます。その時点で、このフィールドの値は自動的に NULL に戻ります。
パージの開始	ガベージ・コレクタが最初に実行される時間（秒単位）です。書式は、*YYYYMMDDHH24MISS* です。この属性はオプションです。デフォルト値が 0（ゼロ）の場合、ガベージ・コレクタはすぐに有効になります。
パージのターゲット期間	ターゲット・オブジェクトの経過時間（時間単位）です。指定された時間より古いオブジェクトは、午前 0 時に消去されます。この属性はオプションです。デフォルト値は 12 です。
パージのトランザクション・サイズ	1 回のトランザクション・コミットで消去されるオブジェクト数。この属性はオプションです。デフォルト値は 1000 です。

Oracle Directory Manager の Oracle Internet Directory 統計情報コレクタ管理フィールド

Oracle Internet Directory 統計情報コレクタでは、表 A-9 で説明した変更可能な 3 つのフィールドを使用できます。それらは、「**パージの間隔**」、「**すぐにパージ**」および「**パージの開始**」です。

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

表 A-10 パスワード・ポリシーの「一般」タブ・ページのフィールド

フィールド	説明
パスワードを変更する際には、旧パスワードの指定が必要	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選択します。デフォルトでは、旧パスワードは不要です。
ユーザー・パスワード可逆暗号化	パスワードを可逆暗号化形式で格納することを選択します。デフォルトでは、このオプションは無効です。
次のログイン時にパスワードをリセット	ユーザーが次回ログインしたときに、パスワードをリセットすることを選択します。デフォルトでは、このオプションは無効です。
旧パスワードを新規パスワードに変更	旧パスワードを新規パスワードとして使用することを許可します。デフォルトでは、このオプションは無効です。
ハッシュ消費を許可	ハッシュ・パスワード値を使用するログインを有効にするか、無効にするかを選択します。デフォルトでは、このオプションは有効です。
猶予期間ログイン制約	パスワードの期限切れ後の猶予期間ログインについて、次の制約のいずれかを選択します。 ■ なし（デフォルト） ■ パスワード期限切れ後の猶予期間ログインの数 ■ パスワード期限切れ後の猶予期間ログインの期間
パスワード期限切れ後の猶予期間ログインの数	パスワードの期限切れ後に許可する猶予期間ログインの最大数を入力します。デフォルト値は 0 です（デフォルトでは、猶予期間ログインは許可されません）。
パスワード期限切れ後の猶予期間ログインの期間	パスワードの期限切れ後の猶予期間ログインに許可される秒数を入力します（デフォルトでは、猶予期間ログインは許可されません）。
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・パスワードは期限切れになりません。
パスワード自己変更の最小期間	
パスワードの期限切れ警告	ディレクトリ・サーバーがユーザーに警告を送信する、パスワードの期限切れ前の秒数を入力します。パスワードの期限切れが有効の場合、デフォルトでは、ディレクトリ・サーバーは、パスワードの期限切れ 3 日前にユーザーに警告を送信します。警告はログインごとに送信されます。 ユーザーが、パスワードを期限切れになる前に変更しない場合、ディレクトリ・サーバーは変更を強制します。つまり、ユーザーは、管理者によってパスワードが変更されるまで、ロックアウトされます。 この機能を有効にするには、クライアントのアプリケーションがこの機能に対応している必要があります。
表示名	このパスワード・ポリシーの名前を入力します。

表 A-11 パスワード・ポリシーの「アカウントのロックアウト」タブ・ページのフィールド

フィールド	説明
グローバル・ロックアウト継続時間	次の両方に該当する場合に、ユーザーがグローバル・ディレクトリからロックアウトされる秒数を入力します。 ■ グローバル・ロックアウトが有効な場合 ■ `pwdMaxFailure` で指定された回数以上の試行を行うと、ディレクトリへのバインドが不可能になる場合。 特定の時間の間または管理者がパスワードを再設定するまでの間、ユーザーをロックアウトできます。デフォルト値は 24 時間です。ロックアウト時間が経過しても、そのユーザーが正しいパスワードにバインドされるまでは、ユーザー・アカウントはロックされたままになります。
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。

表 A-12 パスワード・ポリシーの「IP のロックアウト」タブ・ページのフィールド

フィールド	説明
IP のロックアウト継続時間	特定の IP アドレスに対し、アカウント・ロックアウトを施行する秒数を指定します。
IP のロックアウト失敗の最大数	アカウントがロックされた後、特定の IP アドレスからログイン失敗の最大数を指定します。

表 A-13 パスワード・ポリシーの「パスワード構文」タブ・ページのフィールド

フィールド	説明
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。
履歴内のパスワード数	許可される使用済パスワードの最大数を指定します。
無効なパスワード値	パスワードで許可しない値を入力します。
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。
英文字の最小数	パスワードに必要な最小英文字数を指定します。
特殊文字の最小数	パスワードに必要な英数字以外の文字（`%`、`#`、`$`、`@` などの特殊文字）数を指定します。
大文字の最小数	パスワードに必要な最小大文字数を指定します。
小文字の最小数	パスワードに最低限必要な小文字数を指定します。
繰返し文字の最大数	パスワードに必要な最大繰返し文字数を指定します。

Oracle Directory Manager のパスワード・ベリファイア・フィールド

表 A-14「パスワード検証プロファイル」ダイアログ・ボックスのフィールド

フィールド	説明
パスワード検証エントリへのパス	このパスワード検証エントリの完全識別名。このフィールドを使用して、特定のパスワード検証エントリの位置を特定します。このフィールドは変更できません。
パスワード検証エントリ	このパスワード・ベリファイアの相対識別名。このフィールドは変更できません。
所有者	この検証エントリの管理者の識別名。このフィールドは変更可能です。
アプリケーション ID	Oracle アプリケーションの一意の識別子。この ID は、アプリケーションのインストール時に生成されます。このフィールドは変更できません。

Oracle パスワード・パラメータ	このパスワード・ベリファイアを生成するための情報を含むパラメータ。このフィールドを使用して、このパスワード・ベリファイアのハッシング・アルゴリズムを指定します。構文は次のとおりです。
	`crypto:`*`hashing_algorithm`*
	たとえば、ORCLLM ハッシング・アルゴリズムを使用している場合は、次のように入力します。
	`crypto:ORCLLM`
	SASL/MD5 を使用している場合は、次のように入力します。
	`crypto:SASL/MD5 $ realm:dc=com`

Oracle Directory Manager のプラグイン管理フィールド

関連項目： 32-5 ページの「プラグインの登録と管理」

表 A-15「新規プラグイン」ダイアログ・ボックス、「必須プロパティ」タブ・ページのフィールド

フィールド	説明
プラグイン有効化	無効（デフォルト）または有効のいずれかです。
プラグインの置換	無効（デフォルト）または有効のいずれかです。 操作時置換タイミングの場合、「有効化」を選択し、「プラグインのタイミング」を「操作時」に設定します。
プラグイン・パッケージ名	このプラグインのパッケージ名。
プラグイン・タイプ	操作。操作プラグインは、既存の LDAP 操作を補強します。通常のディレクトリ・サーバー操作の前後に実行するか、操作に追加して実行するかによって、操作プラグインが実行する作業は異なります。 **関連項目：**第 32 章「Oracle Internet Directory サーバー・プラグイン・フレームワーク」を参照してください。
プラグインの種類	PL/SQL または Java。

表 A-15「新規プラグイン」ダイアログ・ボックス、「必須プロパティ」タブ・ページのフィールド（続き）

フィールド	説明
プラグイン LDAP 操作	次のいずれかの値です。 ■ ldapadd ■ ldapbind ■ ldapcompare ■ ldapdelete ■ ldapmodify ■ ldapsearch ■ ldapmoddn（Java のみ）
プラグインのタイミング	次のいずれかの値です。 ■ 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に対する値。 ■ 操作時 : ディレクトリ・サーバーが LDAP 操作の標準処理に追加してコールするプラグインに対する値。 ■ 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に対する値。

表 A-16「新規プラグイン」ダイアログ・ボックス、「オプション・プロパティ」タブ・ページのフィールド

フィールド	説明
プラグイン・クラス・リロード有効	有効（デフォルト）または無効のいずれかです。
プラグイン・バージョン	サポート対象のプラグイン・バージョン番号。
プラグイン・サブスクライバ DN リスト	セミコロンで区切られた識別名のリストで、プラグインの実行を制御します。たとえば、次のようになります。 `orclPluginSubscriberDNList=dc=COM,c=us;dc=us,dc=oracle,dc=com;dc=org,dc=us;o=IMC,c=US` LDAP 操作のターゲット識別名がリストに含まれている場合、プラグインが起動されます。
プラグインの属性リスト	プラグインの実行を制御する、セミコロンで区切られた識別名のリスト。ターゲット属性がリストに含まれている場合は、プラグインが呼び出されます。 ldapcompare プラグインおよび ldapmodify プラグインにのみ有効です。
プラグインの結果コード	LDAP の結果コードを指定する整数値。この値を指定すると、LDAP 操作がこの結果コードの状態の場合にのみ、プラグインが起動します。 POST プラグイン・タイプにのみ有効です。
プラグインのエントリ・プロパティ	LDAP 検索フィルタ・タイプ。たとえば、次のように指定すると、ターゲット・エントリに `inetorgperson` に等しい `objectclass` と、`Cezanne` に等しい `sn` がある場合、プラグインは起動されません。 `orclPluginEntryProperties:(&(objectclass=inetorgperson)(sn=Cezanne))` 「**参照**」ボタンをクリックすると、エントリ・プロパティをフィルタ処理できます。この例を使用して、「エントリ・フィルタ」ダイアログ・ボックスで、エントリ・プロパティ基準として、inetorgperson と Cezanne を入力します。

表 A-16「新規プラグイン」ダイアログ・ボックス、「オプション・プロパティ」タブ・ページのフィールド（続き）

フィールド	説明

プラグインのリクエスト・グループ	セミコロンで区切られたグループ・リストで、プラグインの実行を制御します。このグループを使用して、プラグインを実際に起動するユーザーを指定できます。
	たとえば、次のように指定したとします。
	`orclpluginrequestgropu:cn=security,cn=groups,dc=oracle,dc=com`
	プラグインを登録すると、そのグループに属しているユーザーから LDAP リクエストがないかぎり、プラグインは起動されません。
	`cn=security,cn=groups,dc=oracle,dc=com.`

プラグイン・バイナリ・フレックス・フィールド	Java プラグインに渡されるカスタム・バイナリ情報。これは、ファイルの位置（たとえば、`/home/user1/pic/mypicture.jpg`）です。
フレックス・フィールド	独自のカスタム・フレックス・フィールド値を作成できます。

表 A-17 プラグインの編集ダイアログ・ボックス、「必須プロパティ」タブ・ページのフィールド

フィールド	説明
プラグイン有効化	無効（デフォルト）または有効のいずれかです。
プラグインの置換	無効（デフォルト）または有効のいずれかです。 操作時置換タイミングの場合、「有効化」を選択し、「プラグインのタイミング」を「操作時」に設定します。
プラグイン・パッケージ名	このプラグインのパッケージ名。
プラグイン・タイプ	操作。操作プラグインは、既存の LDAP 操作を補強します。通常のディレクトリ・サーバー操作の前後に実行するか、操作に追加して実行するかによって、操作プラグインが実行する作業は異なります。 **関連項目：**第 32 章「Oracle Internet Directory サーバー・プラグイン・フレームワーク」を参照してください。
プラグインの種類	PL/SQL または Java。
プラグイン LDAP 操作	次のいずれかの値です。 ■ ldapadd ■ ldapbind ■ ldapcompare ■ ldapdelete ■ ldapmodify ■ ldapsearch ■ ldapmoddn（Java のみ）
プラグインのタイミング	次のいずれかの値です。 ■ 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に対する値。 ■ 操作時 : ディレクトリ・サーバーが LDAP 操作の標準処理に追加してコールするプラグインに対する値。 ■ 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に対する値。

表 A-18 プラグインの編集ダイアログ・ボックス、「オプション・プロパティ」タブ・ページのフィールド

フィールド	説明
プラグイン・クラス・リロード有効	有効（デフォルト）または無効のいずれかです。
プラグイン・バージョン	サポート対象のプラグイン・バージョン番号。
プラグイン・サブスクライバ DN リスト	セミコロンで区切られた識別名のリストで、プラグインの実行を制御します。たとえば、次のようになります。 `orclPluginSubscriberDNList=dc=COM,c=us; dc=us,dc=oracle,dc=com;dc=org,dc=us;o=IMC,c=US` LDAP 操作のターゲット識別名がリストに含まれている場合、プラグインが起動されます。
プラグインの属性リスト	プラグインの実行を制御する、セミコロンで区切られた識別名のリスト。ターゲット属性がリストに含まれている場合は、プラグインが呼び出されます。 ldapcompare プラグインおよび ldapmodify プラグインにのみ有効です。
プラグインの結果コード	LDAP の結果コードを指定する整数値。この値を指定すると、LDAP 操作がこの結果コードの状態の場合にのみ、プラグインが起動します。 POST プラグイン・タイプにのみ有効です。
プラグインのエントリ・プロパティ	LDAP 検索フィルタ・タイプ。たとえば、次のように指定すると、ターゲット・エントリに `inetorgperson` に等しい `objectclass` と、`Cezanne` に等しい `sn` がある場合、プラグインは起動されません。 `orclPluginEntryProperties:(&(objectclass=inetorgperson)(sn=Cezanne))` 「**参照**」ボタンをクリックすると、エントリ・プロパティをフィルタ処理できます。この例を使用して、「エントリ・フィルタ」ダイアログ・ボックスで、エントリ・プロパティ基準として、inetorgperson と Cezanne を入力します。

プラグインのリクエスト・グループ	セミコロンで区切られたグループ・リストで、プラグインの実行を制御します。このグループを使用して、プラグインを実際に起動するユーザーを指定できます。
	たとえば、次のように指定したとします。
	`orclpluginrequestgropu:cn=security,cn=groups,dc=oracle,dc=com`
	プラグインを登録すると、そのグループに属しているユーザーから LDAP リクエストがないかぎり、プラグインは起動されません。
	`cn=security,cn=groups,dc=oracle,dc=com.`

プラグイン・バイナリ・フレックス・フィールド	Java プラグインに渡されるカスタム・バイナリ情報。これは、ファイルの位置（たとえば、`/home/user1/pic/mypicture.jpg`）です。
フレックス・フィールド	独自のカスタム・フレックス・フィールド値を作成できます。

表 A-19 プラグインの編集ダイアログ・ボックス、「拡張」タブ・ページのフィールド

フィールド	説明
属性	「オプション・プロパティ」または「必須プロパティ」タブに表示されていない属性を入力します。
属性オプション	属性のオプションを入力します。
属性値	属性の値を入力します。

Oracle Directory Manager のレプリケーション・フィールド

表 A-20 レプリケーション・サーバーの「構成設定」の「一般」タブ・ページのフィールド

フィールド	説明
Orclnormdn	構成設定エントリの正規化された識別名。
変更再試行回数	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。このフィールドは変更可能です。
ダンプ・フラグ	サーバーのクラッシュ時に、スタック・ファイル（デフォルト値は 0）を生成するか、または OS レベル・コア・ファイル（値 1）を生成するかを指定します。
変更ログの存続期間	変更ログ・オブジェクトの存続期間の時間数を入力します。このフィールドは変更可能です。
サプライヤ当たりの移送するスレッド数	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・サーバーが転送用の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 1 です。このフィールドは変更できます。
サプライヤ当たりの適用するスレッド数	変更ログを処理するために、ディレクトリ・レプリケーション・サーバーが各サプライヤに提供するワーカー・スレッドの数を入力します。デフォルトは 5 です。このフィールドは変更できます。
設定	構成識別子。このフィールドは変更できません。

関連項目： 31-2 ページの「Oracle Directory Manager を使用したディレクトリ・レプリケーション・サーバーの構成パラメータの変更」

表 A-21「ASR 承諾」タブ・ページのフィールド

フィールド	説明
コンシューマ・レプリカ DN	この属性は、レプリケーション承諾においてコンシューマを識別するためのレプリカの識別名を指定します。この属性は変更できません。
除外されたネーミング・コンテキスト	この属性は、マルチマスター・レプリカでレプリケーションから除外されるすべてのネーミング・テキストを指定します。LDAP ベースのレプリカには適用されません。
HIQ スケジュール	ディレクトリ・レプリケーション・サーバーが変更適用プロセスを繰り返す間隔（分単位）。このフィールドは変更可能です。
レプリケーション・グループ・ノード	アドバンスト・レプリケーション・ベースのグループの場合は、このレプリケーション・グループのすべてのノードの orclreplicaid 値を入力します。このリストは、グループのすべてのノードで同一であることが必要です。 この属性は、LDAP ベースのレプリケーション承諾には適用されません。
LDAP 接続を継続して維持	この属性は、ディレクトリ・レプリケーション・サーバーをディレクトリ・サーバーに常時接続するか、様々なスケジュールに基づいた変更ログ処理が行われるたびに接続するかを定義します。このフィールドは変更可能です。
レプリカ承諾 ID	レプリケーション承諾エントリのネーミング属性。指定可能な値は次のとおりです。
レプリカ承諾プロトコル	この属性は、変更をレプリカに伝播するためのレプリケーション・プロトコルを定義します。 指定可能な値は次のとおりです。 ■ ODS_ASR_1.0（アドバンスト・レプリケーション・ベースのレプリケーション） ■ ODS_LDAP_1.0（LDAP ベースのレプリケーション）

表 A-21「ASR 承諾」タブ・ページのフィールド（続き）

フィールド	説明
更新スケジュール	この属性は、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を指定します。この値は分単位です。このフィールドは変更可能です。

表 A-22「レプリカ・ノード」の「一般」タブ・ページのフィールド

属性	説明
レプリカ URI	このレプリカに接続する際に使用できる ldapURI 形式の情報を指定します。
レプリカ 2 次 URI	`orclReplicaURI` 値を使用できない場合に使用可能な ldapURI 形式のアドレスを含みます。
現行のレプリカ状態	現行のレプリカ状態を定義する読取り専用の属性。次のいずれかの値です。 ■ オンライン ■ オフライン ■ ブートストラップ ■ ブートストラップ進行中 ■ ブートストラップ・エラー ■ ブートストラップ完了 ■ データベース・コピー追加モード
レプリカ状態	レプリカの状態を指定します。次のいずれかの値です。 ■ オンライン ■ オフライン ■ ブートストラップ
レプリカ・タイプ	読取り専用、読取り / 書込みなどのレプリカのタイプを定義します。 次のいずれかの値になります。 ■ 0（読取り / 書込み） ■ 1（読取り専用）

表 A-23「レプリカ承諾」タブ・ページの列

列	説明
コンシューマ・レプリカ DN	この属性は、レプリケーション承諾においてコンシューマを識別するためのレプリカの識別名を指定します。 このフィールドは変更できません。
HIQ スケジュール	ディレクトリ・レプリケーション・サーバーが変更適用プロセスを繰り返す間隔（分単位）。このフィールドは変更可能です。
LDAP 接続を継続して維持	この属性は、ディレクトリ・レプリケーション・サーバーをディレクトリ・サーバーに常時接続するか、様々なスケジュールに基づいた変更ログ処理が行われるたびに接続するかを定義します。このフィールドは変更可能です。
前回適用された変更番号	この属性は、LDAP ベースのレプリケーション承諾でサプライヤに関するコンシューマ・レプリカのステータスを示します。この属性は、アドバンスト・レプリケーション・ベースの承諾に適用しません。
レプリカ承諾 ID	レプリケーション承諾エントリのネーミング属性。

表 A-23「レプリカ承諾」タブ・ページの列（続き）

列	説明
レプリケーション・プロトコル	この属性は、変更をレプリカに伝播するためのレプリケーション・プロトコルを定義します。 指定可能な値は次のとおりです。 ■ ODS_ASR_1.0（アドバンスト・レプリケーション・ベースのレプリケーション） ■ ODS_LDAP_1.0（LDAP ベースのレプリケーション）
更新スケジュール	この属性は、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を定義します。この値は分単位です。このフィールドは変更可能です。

表 A-24「レプリカ承諾」の「レプリカのネーミング・コンテキスト」タブ・ページのフィールド

フィールド	説明
除外された属性	部分レプリケーションのみに使用します。 含まれているネーミング・コンテキスト内で、レプリケーションから除外する属性。 この属性は複数値です。
除外されたネーミング・コンテキスト	レプリケーションから除外されるサブツリーのルート。 この属性は複数値です。このフィールドは変更可能です。 LDAP ベース・レプリケーションでは、orclincludednamingcontexts 属性で指定されたネーミング・コンテキスト内から LDAP ネーミング・コンテキスト・オブジェクト内に 1 つ以上のサブツリーを指定し、部分レプリケーションから除外できます。 アドバンスト・レプリケーションに基づいたレプリケーションでは、1 つ以上のサブツリーを指定してレプリケーションから除外できます。
包含されたネーミング・コンテキスト	部分レプリカに含まれるネーミング・コンテキスト。 この属性は単一の値です。ネーミング・コンテキスト・オブジェクトごとに、一意のサブツリーのみを指定できます。 部分レプリケーションでは、orclexcludednamingcontexts 属性に指定されたサブツリーを除き、ネーミング・コンテキストに含まれているサブツリーはすべてレプリケートされます。 **注意：**この属性に従って 1 つ以上の部分レプリカを定義するのは、LDAP ベースのレプリケーション承諾のみです。この属性にアドバンスト・レプリケーション・ベースのレプリケーション承諾の任意の値が含まれている場合、この属性は無視されます。 この属性は変更可能です。
フィルタの同期化	双方向レプリカ承諾の場合にのみ、このチェック・ボックスが表示されます。チェック・ボックスが選択されている（デフォルト）場合、構成はどちらの方向も同じです。このチェック・ボックスが選択されていない場合は、追加の「ネーミング・コンテキスト」タブ・ページが表示されます。新しいページで、もう一方の方向のネーミング・コンテキストを別に構成できます。

関連項目： 30-34 ページの「LDAP ベースの部分レプリケーションでのレプリケート対象の決定」

表 A-25「新しいレプリカ承諾のネーミング・コンテキスト」タブ・ページのフィールド

フィールド	説明
除外された属性	部分レプリケーションのみに使用します。含まれているネーミング・コンテキスト内で、レプリケーションから除外する属性。 この属性は複数値です。
除外されたネーミング・コンテキスト	レプリケーションから除外されるサブツリーのルート。 この属性は複数値です。このフィールドは変更可能です。 LDAP ベース・レプリケーションでは、orclincludednamingcontexts 属性で指定されたネーミング・コンテキスト内から LDAP ネーミング・コンテキスト・オブジェクト内に 1 つ以上のサブツリーを指定し、部分レプリケーションから除外できます。 アドバンスト・レプリケーションに基づいたレプリケーションでは、1 つ以上のサブツリーを指定してレプリケーションから除外できます。
包含されたネーミング・コンテキスト	部分レプリカに含まれるネーミング・コンテキスト。 この属性は単一の値です。ネーミング・コンテキスト・オブジェクトごとに、一意のサブツリーのみを指定できます。 部分レプリケーションでは、orclexcludednamingcontexts 属性に指定されたサブツリーを除き、ネーミング・コンテキストに含まれているサブツリーはすべてレプリケートされます。 **注意 :** この属性に従って 1 つ以上の部分レプリカを定義するのは、LDAP ベースのレプリケーション承諾のみです。この属性にアドバンスト・レプリケーション・ベースのレプリケーション承諾の任意の値が含まれている場合、この属性は無視されます。

表 A-26「レプリカ承諾」ウィンドウの列

列	説明
承諾タイプ	読取り専用フィールド。次のいずれかの値です。 ■ 一方向 ■ 双方向
コンシューマ・レプリカ DN	この属性は、レプリケーション承諾においてコンシューマを識別するためのレプリカの識別名を指定します。 このフィールドは変更できません。
除外されたネーミング・コンテキスト	この属性は、マルチマスター・レプリカでレプリケーションから除外されるすべてのネーミング・テキストを指定します。LDAP ベースのレプリカには適用されません。
HIQ スケジュール	ディレクトリ・レプリケーション・サーバーが変更適用プロセスを繰り返す間隔（分単位）。このフィールドは変更可能です。
包含されたネーミング・コンテキスト	この属性は、部分レプリカに含めるすべてのネーミング・コンテキストを指定します。 **注意 :** この属性に従って部分レプリカを定義するのは、LDAP ベースのレプリケーション承諾のみです。この属性に Oracle Database アドバンスト・レプリケーション・ベースの承諾の値が含まれている場合、この属性は無視されます。このフィールドは変更可能です。
LDAP 接続を継続して維持	この属性は、ディレクトリ・レプリケーション・サーバーをディレクトリ・サーバーに常時接続するか、様々なスケジュールに基づいた変更ログ処理が行われるたびに接続するかを定義します。このフィールドは変更可能です。
レプリカ承諾 ID	レプリケーション承諾エントリのネーミング属性。

表 A-26「レプリカ承諾」ウィンドウの列（続き）

列	説明
レプリカ承諾プロトコル	この属性は、変更をレプリカに伝播するためのレプリケーション・プロトコルを定義します。 指定可能な値は次のとおりです。 ■ ODS_ASR_1.0（アドバンスト・レプリケーション・ベースのレプリケーション） ■ ODS_LDAP_1.0（LDAP ベースのレプリケーション）
更新スケジュール	この属性は、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を指定します。この値は分単位です。このフィールドは変更可能です。
レプリケーション・ステータス	一方向承諾タイプの場合、この表にはデータが 1 行表示されます。双方向承諾タイプの場合、データが 2 行表示されます。表には、サプライヤ・ノードとコンシューマ・ノード、最後に適用された変更、および最後に転送された変更が示されます。

表 A-27「変更ログ」ウィンドウのフィールド

フィールド	説明
変更ログ番号	この変更の一意の識別子。
変更ログ操作	この変更を行った操作の種類（追加、削除、変更、比較など）。
変更ログ・ターゲット DN	この変更が行われたエントリの識別名。
変更ログ・ターゲット DN の変更	エントリに対して行われた変更。
変更再試行回数	レプリケートされた環境内の他のノードに対してこの変更を適用しようとした回数。
変更者名	この変更を実行したユーザーの名前。
操作時間	変更が行われた日時。
Orcl GUID	変更が行われたエントリの Global Unique Identifier。
Orcl Parent GUID	変更が行われたエントリの親の Global Unique Identifier。
サーバー名	この変更を発行したサーバーの名前。

Oracle Directory Manager のスキーマ管理フィールド

関連項目： 第 11 章「ディレクトリ・スキーマの管理」

この項の項目は次のとおりです。

Oracle Directory Manager のオブジェクト・クラス・フィールド

表 A-28 Oracle Directory Manager の検索で表示されるオブジェクト・クラス・プロパティ

オプション	説明
名前	検索するオブジェクト・クラスの名前。たとえば、「名前」「完全一致」「subAcl」と指定すると、subAcl オブジェクト・クラスを検索できます。
オブジェクト ID	検索するオブジェクト・クラスのオブジェクト識別子。たとえば、「オブジェクト ID」「次の文字で始まる」「2.5.2」と指定すると、オブジェクト ID が 2.5.2 で始まるオブジェクト・クラスのリストが表示されます。 オブジェクト識別子は、IETF 規格に基づいた、標準化された数値順序です。一意、かつ組織内に設定されたシステムに準拠したものである必要があります。通常この値は、ANSI または ISO など、登録機関によって割り当てられた ID から導出されます。
説明	「説明」フィールドに含まれている語。たとえば、Description Contains Shoe と指定すると、説明列に shoe を含むオブジェクト・クラスのリストが表示されます。説明を記述するオプションのフィールドです。
型	検索するオブジェクト・クラスの型。「抽象型」、「構造型」または「補助型」のいずれかを指定します。
スーパー・クラス	検索するオブジェクト・クラスのスーパークラス。「追加」をクリックすると「スーパー・クラス・セレクタ」ダイアログ・ボックスが表示され、追加するスーパークラスを選択できます。
必須属性	検索するオブジェクト・クラスの必須属性。たとえば、Mandatory Attributes Contains cn と指定すると、cn 属性が必須の、すべてのオブジェクト・クラスのリストが表示されます。
オプション属性	検索するオブジェクト・クラスのオプション属性。

表 A-29 オブジェクト・クラスの検索フィルタ

フィルタ	説明
次の文字で始まる	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。
次で終わる	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」「次で終わる」「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。
次を含む	選択したプロパティに入力値が含まれる（必ずしもその値に限定されない）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」「次を含む」「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。
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きい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さいか等しいオブジェクト・クラスを検索します。たとえば、「名前」「以下」「orcl」と指定すると、orcl で始まるオブジェクト・クラスから、アルファベットの最初の文字で始まるオブジェクト・クラスまでのリストが表示されます。
存在	選択したプロパティが存在するすべてのオブジェクト・クラスを検索します。たとえば、「必須属性」「存在」と指定すると、必須属性を含むすべてのオブジェクト・クラスのリストが表示されます。

表 A-30 Oracle Directory Manager のオブジェクト・クラスの検索時に使用されるボタン

ボタン	説明
新規作成	「**基準**」フィールドに、新しい検索基準バーを作成します。このボタンは、「**基準**」バーが削除されている場合にのみ有効です。
AND	「**基準**」フィールドに、別の検索基準バーを作成します。指定した 2 つの基準を両方満たすオブジェクト・クラスをすべて検索します。
OR	「**基準**」フィールドに、別の検索基準バーを作成します。指定した 2 つの属性のいずれかを持つオブジェクト・クラスをすべて検索します。
NOT	選択した検索基準バーの基準を無効にし、指定した基準を満たさないオブジェクト・クラスをすべて取り出します。
削除	選択した検索基準バーを削除します。

表 A-31「新規オブジェクト・クラス」ダイアログ・ボックスのフィールド

オプション	説明
名前	オブジェクト・クラスの名前。
オブジェクト ID	オブジェクト識別子。これは、IETF 規格に基づいた、標準化された数値順序です。一意、かつ組織内に設定されたシステムに準拠したものである必要があります。通常この値は、ANSI または ISO など、登録機関によって割り当てられた ID から導出されます。
説明	このオプションのフィールドは、説明の記述のみに使用します。
型	オブジェクト・クラスの型。「抽象型」、「構造型」、「補助型」または「なし」のいずれかを指定します。
スーパー・クラス	このオブジェクト・クラスを導出するクラスです。このオブジェクト・クラスは、選択したスーパークラスの属性をすべて継承します。構造型オブジェクト・クラスの場合は、そのスーパークラスの 1 つとして必ず top を設定する必要があります。「追加」をクリックすると「スーパー・クラス・セレクタ」ダイアログ・ボックスが表示され、追加するスーパークラスを選択できます。
必須属性	値の入力が必要な属性です。「追加」をクリックすると「必須属性セレクタ」ダイアログ・ボックスが表示され、追加する必須属性を選択できます。
オプション属性	値が必須ではない属性です。「追加」をクリックすると「オプション属性セレクタ」ダイアログ・ボックスが表示され、追加するオプション属性を選択できます。

Oracle Directory Manager の属性フィールド

表 A-32 Oracle Directory Manager の「属性」タブ・ページの列

列	説明
名前	属性の標準化型名。
索引付け	属性が索引付けされているかどうかを示すチェック・ボックス。
オブジェクト ID	各属性の標準化オブジェクト識別子。
説明	各属性を説明する語。
構文	データ・エントリに関して各属性の型に適用される標準化規則。
サイズ	各オブジェクトの最大サイズ。
使用方法	属性の使用方法を指定する規格。次の 4 つのオプションがあります。 ■ `userApplications` ■ `directoryOperation` ■ `distributedOperation` ■ `dSAOperation`
順序	値に対して設定される優先順位を指定する規格。
等価	比較と検索操作における等価の判断方法を指定する規格。
サブストリング	一致する正規表現の文字列。
単一値	ある 1 つの最大値を含む属性の型。
スーパー	各属性のスーパー属性。

表 A-33 属性の検索フィルタ

オプション	説明
次の文字で始まる	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。
次で終わる	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」「次で終わる」「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。
次を含む	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」「次を含む」「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きい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。

表 A-34 Oracle Directory Manager の属性の検索時に使用されるボタン

ボタン	説明
新規作成	「**基準**」フィールドに、新しい検索基準バーを作成します。このボタンは、「**基準**」フィールドが空の場合にのみ有効です。
AND	「**基準**」フィールドに、別の検索基準バーを作成します。指定した 2 つのプロパティが両方ある属性をすべて検索します。
OR	「**基準**」フィールドに、別の検索基準バーを作成します。指定した 2 つのプロパティのいずれかを持つ属性をすべて検索します。
NOT	選択した検索基準バーの基準を無効にし、指定したプロパティがない属性をすべて検索します。
削除	選択した検索基準バーを削除します。

表 A-35「新規属性の型」ダイアログ・ボックスの「一般」タブ・ページのフィールド

フィールド	説明
名前	この属性の名前。
オブジェクト ID	この属性のオブジェクト ID。オブジェクト ID は、IETF 規格に基づいた、標準化された数値順序です。値は一意であることが必要です。通常この値は、ANSI または ISO など、登録機関によって割り当てられた ID から導出されます。 標準識別子の説明は、現行の LDAP 規格を参照してください。LDAP 規格は IETF の Web サイト `http://www.ietf.org` で参照できます。
説明	説明の記述のみに使用するオプションのフィールド。
構文	データ・エントリに関してこの属性の型に適用される標準化規則。
サイズ	このオブジェクトの最大サイズ。
単一値	この属性の型の値が最大 1 つであることを示します。

表 A-36「新規属性の型」ダイアログ・ボックスの「拡張」タブ・ページのフィールド

フィールド	説明
索引付け	このフィールドを選択するとこの属性が索引に追加され、検索で使用できるようになります。等価の一致規則を持つ属性のみが索引付けできます。
使用方法	属性の使用方法を指定する規格を指定します。オプションは次のとおりです。 ■ `userApplications` ユーザーが値を入力する必要がある属性 （例 : `telephoneNumber`） ■ `directoryOperation` ディレクトリ・サーバーによって値が入力される属性 （例 : `creatorName` または `timeStamp`） ■ `distributedOperation` ■ `dSAOperation` サーバーの内部操作用に使用される属性 （例 : orclUpdateSchedule）
順序	値に対して設定される優先順位を指定する規格を指定します。
等価	比較と検索操作における等価の判断方法を指定する規格を指定します。
サブストリング	一致規則を指定します。
スーパー	この属性のスーパー属性を追加します。これは、次の手順に従って行います。 **1.** このフィールドの横の「追加」ボタンを選択します。「スーパー属性セレクタ」が表示されます。 **2.** 追加するスーパー属性を選択して、「選択」を選択します。 **3.** 必要に応じてこの処理を繰り返します。 「スーパー」フィールドからスーパー属性を削除するには、削除する属性を選択して、「削除」を選択します。

Oracle Directory Manager の一致規則フィールド

表 A-37「一致ルール」タブ・ページのフィールド

列見出し	説明
名前	属性一致規則の名前
オブジェクト ID	この一致規則の一意な識別子
説明	一致規則を説明する語（オプション）
構文	この一致規則に使用される構文

Oracle Directory Manager のコンテンツ規則管理フィールド

表 A-38「新規コンテンツ・ルール」ダイアログ・ボックスのフィールド

フィールド	説明
構造化オブジェクト・クラス	このコンテンツ規則を割り当てる構造型オブジェクト・クラスの名前。
オブジェクト ID	作成するコンテンツ規則の一意な識別子。
ラベル	このコンテンツ規則のわかりやすい名前。
補助クラス	指定の構造型オブジェクト・クラスに関連付ける属性を持つ補助型オブジェクト・クラス。補助型クラスを指定する手順は、次のとおりです。 **1.** 「追加」を選択します。「補助クラス・セレクタ」ダイアログ・ボックスが表示されます。 **2.** 追加する補助型クラスを選択します。 **3.** 「選択」を選択します。「新規コンテンツ・ルール」ダイアログ・ボックスに戻ります。「補助クラス」フィールドに指定した補助型クラスが表示されます。
必須属性	指定の構造型オブジェクト・クラスに関連付ける必須属性。必須属性を指定する手順は、次のとおりです。 **1.** 「追加」を選択します。「必須属性セレクタ」ダイアログ・ボックスが表示されます。 **2.** 追加する必須属性を選択します。この属性に索引付けをする場合、「索引付け」列の対応するチェック・ボックスを選択します。 **3.** 「選択」を選択します。「新規コンテンツ・ルール」ダイアログ・ボックスに戻ります。「必須属性」フィールドに指定した必須属性が表示されます。
オプション属性	指定の構造型オブジェクト・クラスに関連付けるオプションの属性。オプション属性を指定する方法は次のとおりです。 **1.** 「追加」を選択します。「オプション属性セレクタ」ダイアログ・ボックスが表示されます。 **2.** 追加するオプション属性を選択します。この属性に索引付けをする場合、「索引付け」列の対応するチェック・ボックスを選択します。 **3.** 「選択」を選択します。「新規コンテンツ・ルール」ダイアログ・ボックスに戻ります。「オプション属性」フィールドに指定したオプション属性が表示されます。

表 A-39「コンテンツ・ルール」ダイアログ・ボックスのフィールド

フィールド	説明
構造化オブジェクト・クラス	このコンテンツ規則を割り当てる構造型オブジェクト・クラスの名前。
オブジェクト ID	作成するコンテンツ規則の一意な識別子。
ラベル	このコンテンツ規則のわかりやすい名前。
補助クラス	指定の構造型オブジェクト・クラスに関連付ける属性を持つ補助型オブジェクト・クラス。補助型クラスを指定する手順は、次のとおりです。 1. 「追加」を選択します。「補助クラス・セレクタ」ダイアログ・ボックスが表示されます。 2. 追加する補助型クラスを選択します。 3. 「選択」を選択します。「新規コンテンツ・ルール」ダイアログ・ボックスに戻ります。「補助クラス」フィールドに指定した補助型クラスが表示されます。
必須属性	指定の構造型オブジェクト・クラスに関連付ける必須属性。必須属性を指定する手順は、次のとおりです。 1. 「追加」を選択します。「必須属性セレクタ」ダイアログ・ボックスが表示されます。 2. 追加する必須属性を選択します。この属性に索引付けをする場合、「索引付け」列の対応するチェック・ボックスを選択します。 3. 「選択」を選択します。「新規コンテンツ・ルール」ダイアログ・ボックスに戻ります。「必須属性」フィールドに指定した必須属性が表示されます。
オプション属性	指定の構造型オブジェクト・クラスに関連付けるオプションの属性。オプション属性を指定する方法は次のとおりです。 1. 「追加」を選択します。「オプション属性セレクタ」ダイアログ・ボックスが表示されます。 2. 追加するオプション属性を選択します。この属性に索引付けをする場合、「索引付け」列の対応するチェック・ボックスを選択します。 3. 「選択」を選択します。「新規コンテンツ・ルール」ダイアログ・ボックスに戻ります。「オプション属性」フィールドに指定したオプション属性が表示されます。

Oracle Directory Manager のサーバーの管理フィールド

この項の項目は次のとおりです。

Oracle Directory Manager の構成設定フィールド

関連項目： 7-3 ページの「Oracle Directory Manager を使用したサーバーの構成設定エントリの管理」

表 A-40「構成設定」ダイアログ・ボックスの「一般」タブ・ページのフィールド

フィールド	説明
DB の最大接続数	1 つのディレクトリ・サーバー・プロセスで処理可能なデータベースの同時接続数を入力します。デフォルトは 10 です。
要素のプロセスの数	単一のインスタンスが起動できるサーバー・プロセスの数を入力します。デフォルトは 1 です。
非 SSL ポート	デフォルトの非 SSL ポートは 389 です。この非 SSL ポートは変更できます。
設定	このフィールドには、構成設定エントリの数が表示されます。デフォルトの構成設定は 0（ゼロ）です。異なる構成設定を必要な数だけ設定できます。複数のインスタンスで同じパラメータを必要とする場合は、同一の構成設定を使用できます。設定番号は変更可能です。
SASL 認証モード	デフォルト値は 1 です。このリリースの Oracle Internet Directory では、これ以外の値はサポートされていません。
SASL メカニズム	デフォルト値は DIGEST-MD5 です。このリリースの Oracle Internet Directory では、これ以外の値はサポートされていません。
SASL 暗号の選択	この複数値属性のデフォルト値は次のとおりです。 ■ RC4-56 ■ DES ■ 3DES

表 A-41「SSL 設定」タブ・ページのフィールド

フィールド	説明
SSL 認証	次の中から 1 つ選択します。 ■ SSL 認証なし : クライアントとサーバーのいずれも、相手に対して自己認証を行いません。証明書の送信または交換は行われません。この場合は、SSL 暗号化 / 復号化のみ使用されます。 ■ SSL クライアントとサーバー認証 : 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 有効化	次の中から 1 つ選択します。 ■ SSL と非 SSL の両方 : 非保護操作と SSL 認証両方の場合。 ■ 非 SSL のみ : 非保護操作のみの場合。デフォルト・ポートは 389 で、この SSL ポート・フィールドで変更可能です。 ■ SSL のみ : SSL 認証の場合。デフォルト・ポートは 636 で、この SSL ポート・フィールドで変更可能です。

表 A-41「SSL 設定」タブ・ページのフィールド（続き）

フィールド	説明

SSL ウォレット 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`
	Microsoft Windows では、このパラメータは次のように設定します。
	`file:C:¥my_dir¥my_wallet`

SSL ポート	デフォルトの SSL ポートは 636 です。SSL ポートは変更できます。

Oracle Directory Manager のシステム操作属性フィールド

関連項目： 7-8 ページの「Oracle Directory Manager を使用したシステム操作属性の設定」

表 A-42 Oracle Directory Manager に表示されるシステム操作属性

フィールド	説明	デフォルト値	変更可能
匿名ユーザーによるバインドを許可	匿名バインドを許可するかどうかを示します。1 に設定すると、匿名バインドが許可されます。0（ゼロ）に設定すると許可されません。	1	○
代替サーバー	ローカル・サーバーとの接続が失われた場合に、クライアントは、この属性にリストされているサーバーの 1 つにアクセスすることができます。ローカル・サーバーと同じネーミング・コンテキストのセットを持つ、システム内の他の Oracle ディレクトリ・サーバーを指定します。書式は次のとおりです。 ldap://*host_name*:*port_number* **関連資料：**『Oracle Application Server 高可用性ガイド』の「Oracle Directory Manager を使用した代替サーバー・リストの設定」	なし	○
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`	×
重大イベント・レベル	記録する必要があるセキュリティおよびシステムに関連する重要なイベントを指定します。 スーパーユーザー、プロキシ、およびレプリケーション・ログイン以外のイベントについては、この機能を有効にするために `orclStatsFlag` 属性の値を 1 に設定する必要もあります。 **関連項目：**監視できる重要なイベントのリストは、14-20 ページの「クリティカル・イベントの構成」を参照してください。	0	○
DIP リポジトリ	ディレクトリ・レプリケーション・サーバーで使用され、Oracle Directory Integration and Provisioning Server でコンシュームするために、変更ログがコンシューマ・ノードで生成されるかどうかを示します。	FALSE	○
ディレクトリ・バージョン	使用している Oracle Internet Directory のバージョン（リリース）。	9.0.4.0.0	×

表 A-42 Oracle Directory Manager に表示されるシステム操作属性（続き）

フィールド	説明	デフォルト値	変更可能
エントリ・キャッシュの有効化	エントリ・キャッシング（3-10 ページの「エントリ・キャッシング」を参照）を有効にするかどうかを指定します。有効にする場合は 1、無効にする場合は 0（ゼロ）です。	1	○
グループ・キャッシュの有効化	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	○
MatchDN 処理の有効化	検索リクエスト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、最も近い識別名を返します。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有効になります。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	○
統計の収集の有効化	Oracle Internet Directory サーバー管理機能フレームワークを有効にするか、無効にするかを示すインジケータです。有効にするには、1 に設定します。無効にするには、0（ゼロ）に設定します。	0	○
エントリ・キャッシュ・サイズ（バイト）	エントリ・キャッシュが使用できる RAM の最大バイト数。	100M	○
索引付き属性の位置	すべての索引付き属性を含むファイルの識別名を指定します。	cn=catalogs	×
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	○
TCP 接続の最大アイドル時間	アイドル状態の接続を終了するまでの時間を指定します。	120	
ネーミング・コンテキスト	このサーバーに格納されている、公開するネーミング・コンテキストの最上位識別名を指定します。ネーミング・コンテキストとして識別名を公開するには、スーパーユーザー権限を持っている必要があります。	なし	○
暗号化パスワード	パスワードを暗号化するハッシュ・アルゴリズム。オプションは次のとおりです。 ■ MD4 セキュア・ハッシュ・アルゴリズム ■ MD5 セキュア・ハッシュ・アルゴリズム ■ 暗号化を使用しない ■ **SHA** ■ **UNIX Crypt**	MD4	○
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	×

表 A-42 Oracle Directory Manager に表示されるシステム操作属性（続き）

フィールド	説明	デフォルト値	変更可能
問合せエントリの返送制限	検索で返されるエントリの最大数。	1000	○
レプリカ ID	レプリケーション承諾のノードの一意識別子。		
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	×
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	×
レプリケーション・ステータスの位置	このサーバーに変更ステータスを保持しているエントリの識別名。	cn=changestatus	×
スキーマ定義の位置	スキーマの識別名。	cn=subschemasubentry	×
サーバー・モード	サーバーにデータを書き込むことができるかどうかを示します。この値は、「読取り / 書込み」か「読取り専用」のいずれかに変更できます。レプリケーション処理時はデフォルトを「読取り専用」に変更してください。	読取り / 書込み	選択肢は「読取り / 書込み」、「読取り / 更新」および「読取り専用」です。
サーバー処理の制限時間	検索の最大実行時間（秒）。	3600	○
変更ログ属性の簡易変更	マルチマスター・レプリケーション・グループでは、特定の属性値の変更で発生した競合を解消するために多くのリソースが必要な場合があります。このフィールドでその属性を指定することにより、パフォーマンス低下を回避できます。 このフィールドで属性を指定すると、その属性の値の変更は変更ログに反映されます。ただし、マルチマスター・レプリケーション・グループでは、この属性に対する競合解消はオフとなります。	uniquemember member	○
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	○
統計レベル	Oracle Internet Directory サーバー管理機能フレームワークを有効にするか、無効にするかを指定します。有効にするには、1 に設定します。無効にするには、0（ゼロ）に設定します。	0	○
サポートされる制御リスト	任意の LDAP 操作の拡張情報を入力します。Oracle Internet Directory がサポートしている制御の種類は、supportedcontrol 属性の値としてルート DSE にリストされています。制御の各種類には、LDAP 規格で定義されているオブジェクト識別子が関連付けられています。supportedcontrol 属性の値は、制御の種類に割り当てられた標準のオブジェクト識別子です。	manageDSACtrl	×
サポートされている拡張子	このリリースの Oracle Internet Directory がサポートしている LDAP 操作に対する独自拡張機能の一意識別子です。 リリース 9.0.4 では、拡張操作が 1 つあります。この操作は、プラグインが、データベースの PL/SQL パッケージを使用してディレクトリ・サーバーへバインドできるようにします。	2.16.840.1.113894.1.9.1	×

表 A-42 Oracle Directory Manager に表示されるシステム操作属性（続き）

フィールド	説明	デフォルト値	変更可能
サポートされる 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`	×
サポートされている SASL メカニズム	クライアントの一部では、Simple Authentication and Security Layer（SASL）を使用できます。このフィールドは、ディレクトリ・サーバーがサポートしている認証メカニズムを示します。 **関連項目：** 16-8 ページの「Simple Authentication and Security Layer（SASL）を使用した認証」	`DIGEST-MD5`	×
アップグレード進行中	アップグレード用に予約済です。	FALSE	×

Oracle Directory Manager のスーパーユーザー、ゲスト・ユーザーおよびプロキシ・ユーザー・フィールド

関連項目： 7-10 ページの「Oracle Directory Manager を使用したスーパーユーザー、ゲスト・ユーザーおよびプロキシ・ユーザーの管理」

表 A-43「システム・パスワード」タブ・ページのフィールド

フィールド	説明
スーパーユーザー名	スーパーユーザーの名前を入力するか、「参照」をクリックし検索します。デフォルトは `orcladmin` です。
スーパーユーザー・パスワード	スーパーユーザーのパスワードを入力します。デフォルトは、インストール時に Oracle Application Server 管理者に指定したパスワード（ias_admin）と同じです。このパスワードはすぐに変更してください。
ゲストのログイン名	ゲスト・ログイン名を入力するか、「参照」をクリックし検索します。ゲストには、そのディレクトリ内の**アクセス制御リスト**で指定されている権限が与えられます。デフォルトは `guest` です。
ゲストのログイン・パスワード	ゲスト・ログイン・パスワードを入力します。デフォルトは `guest` です。
プロキシ・ログイン名	プロキシ・ログイン名を入力するか、「参照」をクリックし検索します。プロキシ・ユーザーには、そのディレクトリ内の ACP で指定されている権限が与えられます。デフォルトは `proxy` です。
プロキシ・ログイン・パスワード	プロキシ・ログイン・パスワードを入力します。デフォルトは `proxy` です。このパスワードはすぐに変更してください。

Oracle Directory Manager の問合せ最適化フィールド

関連項目： 25-12 ページの「Oracle Directory Manager を使用した偏りのある属性の検索の最適化」

表 A-44「問合せの最適化」タブ・ページのフィールド

フィールド	説明
動的グループ・キャッシュ・リフレッシュを起動	動的グループ・キャッシュのリフレッシュの強制を選択します。
参照プロセスをスキップ	検索のために生成された SQL で参照をスキップすることを選択します。ディレクトリ内に参照エントリがない場合、参照のスキップは、検索のパフォーマンスの最適化に役立ちます。
強制フラッシュ・デバッグ・メッセージ	ディレクトリ・サーバーによってメッセージが記録されるときに、ログ・ファイルに書き込まれるメッセージのデバッグを有効にすることを選択します。この機能は、デフォルトでは無効です。
キャッシュされたユーザー・グループ接続の最大数	属する権限グループをキャッシュできる接続識別名の数を指定します。デフォルト値は ID（接続識別名）25000 です。インストールのユーザーが 25000 人を超える場合は、値を増やします。
BER でキャッシュされた検索エントリの最大数	許可される BER エントリの最大数を指定します。サブツリーの検索時に、サーバーは、この数のエントリが処理されるまで、クライアントに書込みを行いません。デフォルトではこの値は 5 です。エントリが 8000 バイトを超える場合は、この値を 1 に減らします。
OID サーバーが LDAP クライアントを読取り / 書込みする最大時間	ネットワークの読取り / 書込みのタイムアウトを秒単位で指定します。LDAP クライアントが操作を開始し、サーバーに対してこの秒数で応答しない場合、サーバーは接続をクローズします。デフォルトは 300 秒です。
キャッシュ内の最大エントリ・サイズ	キャッシュに格納できるエントリ・サイズの上限をバイト単位で指定します。デフォルトは 5000、つまり 5KB です。
監視中のユーザーの DN	LDAP 操作を追跡する対象となるユーザー識別名のリストを指定します。
セキュリティ・イベント追跡のレベル	バインドおよび比較情報収集のレベルを指定します。次のいずれかのレベルです。 ■ 1: バインド識別名のみ ■ 2: バインド識別名と IP アドレス ■ 4: 識別名のみを比較 ■ 8: 識別名と IP アドレスを比較 ■ 16: 識別名、IP アドレスおよび失敗の詳細を比較 バインドおよび比較のレベルは追加できます。たとえば、18 は、バインド識別名と IP アドレス、および識別名、IP アドレスおよび失敗の詳細の比較を指定します。
セキュリティ・イベントの追跡に使用される最大 RAM 空き容量	セキュリティ・イベントの追跡に使用される最大メモリーをバイト単位で指定します。デフォルトは 100MB です。

表 A-44「問合せの最適化」タブ・ページのフィールド（続き）

フィールド	説明
PKI マッピング / 一致ルール	ユーザーの PKI 証明書識別名を Oracle Internet Directory 内のユーザーのエントリ識別名にマップするための一致規則を指定します。次の一致規則の値を使用できます。 ■ 0: 完全一致。PKI 証明書識別名は、ユーザーのエントリ識別名と一致する必要があります。 ■ 1: 証明書ハッシュ検索。ユーザーが、Oracle Internet Directory に用意された PKI 証明書を持っているかどうかを確認します。 ■ 2: 完全一致と証明書ハッシュ検索の組合せ。完全一致が失敗した場合、証明書検索が実行されます。 ■ 3: マッピング・ルールのみ。マッピング・ルールを使用して、ユーザー PKI 証明書識別名を Oracle Internet Directory 識別名にマップします。 ■ 4: 1（マッピング・ルール）、2（証明書ハッシュ検索）、3（完全一致）の順序で試します。
ダンプ・フラグ	ダンプ・フラグ。
LDAP 接続タイムアウト	ディレクトリ・クライアントが、接続が終了するまでアイドル状態を保持する最大時間（秒）を入力します。デフォルトは 0 です。これはタイムアウトがないことを意味します。
時間制限モード	サーバーのパフォーマンスを調整するために、検索時間を厳密に設定するかおおよその時間に設定します。正確な時間に設定すると、検索は必ず指定した秒数で終了します。おおよその時間に設定すると、検索は指定した秒数から 2 秒の範囲内で終了します。ワークロードが少ない場合は、おおよその時間を指定することで、パフォーマンスが向上します。
低カーディナリティの属性	偏った属性として指定する属性を入力します。 関連項目 : 偏った属性の詳細は、25-10 ページの「検索の最適化」を参照してください。

Oracle Directory Manager のエントリ検索フィールドおよびボタン

表 A-45 エントリの検索フィルタ

フィルタ	説明
次の文字で始まる	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。
次で終わる	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」「次で終わる」「son」と指定すると、Baldisson、Jacobson、Johnson などが取り出されます。
次を含む	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」「次を含む」「Wins」と指定すると、cn 属性に wins を含むエントリがすべて取り出されます。この場合は、Winslow、Czerwinski、Winship などが取り出されます。
完全一致	指定した属性がユーザーの入力値に一致するエントリを検索します。たとえば、「cn」「完全一致」「Franklin Baldwins」と指定すると、cn 属性の値が Franklin Baldwins のエントリがすべて取り出されます。

表 A-45 エントリの検索フィルタ（続き）

フィルタ	説明
以上	指定した属性が、数値順またはアルファベット順で入力値より大きい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、最初の 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、最初の Frank からアルファベットの最初の文字までの cn 属性がすべて取り出されます。
存在	指定した属性を持つエントリが、ツリーのそのレベルに存在するかどうかを判断します。この関連の使用に値の入力は不要です。「cn」「存在」と指定すると、ツリーのそのレベルで、cn 属性を持つエントリがすべて取り出されます。

表 A-46 エントリ検索ボタン

ボタン	説明
新規作成	「**基準**」フィールドに、新しい検索基準バーを作成します。このボタンは、「**基準**」フィールドが空の場合にのみ有効です。
AND	「**基準**」フィールドに、別の検索基準バーを作成します。指定した両方の属性を持つエントリをすべて検索します。たとえば、`cn=Baldwins And title=Laborer` と指定すると、cn が Baldwins で、かつ title が laborer のエントリがすべて取り出されます。
OR	「**基準**」フィールドに、別の検索基準バーを作成します。指定した属性のいずれかを持つエントリをすべて検索します。たとえば、`title=Laborer Or title=Foreman` と指定すると、title が laborer または foreman の従業員がすべて取り出されます。
NOT	選択した検索基準バーの基準を無効にし、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。
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：** ■ 11-14 ページの「Oracle Directory Manager を使用した属性の索引付け」 ■ 11-16 ページの「コマンドライン・ツールを使用した属性の索引付け」

Oracle Directory Manager の SSL 管理フィールド

関連項目：

- A-25 ページの表 A-41「「SSL 設定」タブ・ページのフィールド」
- 17-4 ページの「Oracle Directory Manager を使用した SSL パラメータの構成」

表 A-47「SSL 設定」タブ・ページのフィールド

フィールド	説明
SSL 認証	次の中から 1 つ選択します。 ■ SSL 認証なし : クライアントとサーバーのいずれも、相手に対して自己認証を行いません。証明書の送信または交換は行われません。「資格証明」タブの「SSL 使用可能」チェック・ボックスを選択して、このオプションを選択した場合は、SSL 暗号化 / 復号化のみが使用されます。 ■ SSL クライアントとサーバー認証 : 双方向認証。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 : 一方向認証。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。
SSL 有効化	次の中から 1 つ選択します。 ■ **SSL と非 SSL の両方 :** 非保護操作と SSL 認証両方の場合。 ■ **非 SSL のみ :** 非保護操作のみの場合。 ■ **SSL のみ :** SSL 認証のみの場合。

SSL ウォレット 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`
	Microsoft Windows では、このパラメータは次のように設定します。
	`file:C:¥my_dir¥my_wallet`

SSL ポート	デフォルトの SSL ポートは 636 です。SSL ポートは変更できます。

Oracle Directory Manager の同期フィールド

この項では、ディレクトリの同期管理に使用する Oracle Directory Manager のフィールドについて説明します。これらのフィールドは、ディレクトリ統合プロファイルの登録用です。

表 A-48 Oracle Directory Manager の同期に関する「一般」タブ・ページのフィールド

フィールド	説明
プロファイル名	プロファイルの名前を指定します。入力した名前は、この統合プロファイルの識別名の相対識別名コンポーネントとして使用されます。たとえば、プロファイル名 `MSAccess` を指定して、`orclodipagentname=MSAccess,cn=subscriber profile, cn=changelog subscriber, cn=oracle internet directory` という名前の統合プロファイルを作成します。 このフィールドは必須です。このフィールドにデフォルトの設定はありません。
同期モード	インポート操作かエクスポート操作かを指定します。インポート操作は、接続ディレクトリの変更を Oracle Internet Directory に移します。エクスポート操作は、Oracle Internet Directory から接続ディレクトリに変更を送信します。 このフィールドは必須です。デフォルトは `IMPORT` です。
プロファイルのステータス	プロファイルが有効か無効かを指定します。 このフィールドは必須です。デフォルトは `ENABLE` です。
プロファイルのパスワード	ディレクトリ統合サーバーがプロファイルのかわりに Oracle Internet Directory にバインドするときに使用するパスワードを指定します。このフィールドは必須で、デフォルトは `welcome` です。
スケジューリングの間隔	接続ディレクトリと Oracle Internet Directory の同期の、試行間隔の秒数を指定します。 このフィールドは必須です。デフォルトは `60` です。
最大再試行回数	ディレクトリ統合サーバーが同期を無効にするまでに同期を試行する回数の、最大数を指定します。このフィールドは必須です。 デフォルトは 5 です。最初の再試行は最初の失敗の 1 分後に行われます。2 回目の再試行は 2 回目の失敗の 2 分後に、後続の再試行は n 回目の失敗の n 分後に行われます。
プロファイルのバージョン	このプロファイルが作成された Oracle Directory Integration Platform のバージョン。

表 A-49 Oracle Directory Manager の同期に関する「実行」タブ・ページのフィールド

フィールド	説明

エージェント実行コマンド	ディレクトリ統合サーバー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。このフィールドにデフォルトの設定はありません。
	一般的な実行コマンドは、次の形式です。
	`odicmd user=%orclodipcondirAccessAccount pass=%orclodipcondiraccesspassword`
	`odicmd` は、実行するコマンドです（パスに指定されている場合に使用可能、またはフルパス名で指定）。
	`user=%orclodipcondirAccessAccount pass=%orclodipcondiraccesspassword`
	はコマンドライン引数です。ユーザー（user）に渡される値は `orclodipcondiraccessaccount` 属性から、パス（pass）に渡される値は `orclodipcondiraccesspassword` 属性から導出されます。
	一般的な例は、Oracle Human Resources エージェントにあります。

接続されたディレクトリ・アカウント	コネクタまたはエージェントが接続ディレクトリにアクセスするために使用するアカウントを指定します。たとえば、接続ディレクトリがデータベースの場合、アカウントは `Scott` などになります。接続ディレクトリが別の LDAP 準拠ディレクトリの場合、アカウントは `cn=Directory Manager` などになります。 このフィールドはオプションです。このフィールドにデフォルトの設定はありません。
接続されたディレクトリ・アカウントのパスワード	コネクタまたはエージェントが接続ディレクトリにアクセスするときに使用するパスワードを指定します。このフィールドはオプションです。このフィールドにデフォルトの設定はありません。
追加構成情報	このフィールドには、ディレクトリ統合サーバーがエージェントに渡す追加情報が表示されます。このフィールドは Oracle Directory Manager で変更できません。このフィールドを変更する唯一の方法は、ldapuploadagentfile.sh を使用することです。デフォルトはありません。
接続されたディレクトリ URL	接続ディレクトリへの接続に必要な接続詳細。このパラメータは、ホスト名とポート番号を `host:port:sslmode` の形式で示します。 SSL を使用して接続するには、*`host:port`*:1 を入力します。 ディレクトリに接続するための証明書が Wallet に格納され、その場所が `odi.properties` ファイルに指定されていることを確認します。 **注意：**SSL を使用して SunONE Directory Server に接続するには、サーバー証明書を Wallet にロードする必要があります。 **関連資料：**『Oracle Advanced Security 管理者ガイド』の Oracle Wallet Manager に関する章を参照してください。
インタフェース・タイプ	インポート・ファイルまたはエクスポート・ファイルが使用する形式。選択できるのは、`DB`、`LDAP`、`LDIF`、および `TAGGED` です。このフィールドはオプションです。デフォルトは `TAGGED` です。

表 A-50 Oracle Directory Manager の同期に関する「マッピング」タブ・ページのフィールド

フィールド	説明
マッピング・ルール	このフィールドには、接続ディレクトリと Oracle Internet Directory の間でデータを変換するためのマッピング・ルールが表示されます。このフィールドにデフォルトの設定はありません。 **注意 :** マッピング・ルール・ファイルは、Oracle Directory Manager では編集できません。ファイルのマッピング・ルールは手動で編集し、`dipassistant` を使用してプロファイルにアップロードします。『Oracle Identity Management ユーザー・リファレンス』の `dipassistant` コマンドライン・ツール・リファレンスを参照してください。
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。
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。

表 A-51 Oracle Directory Manager の同期に関する「ステータス」タブ・ページのフィールド

フィールド	説明
OID 前回適用された変更番号 (インポート操作のみ)	エクスポート操作の場合、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、無効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。
前回適用された変更番号 (エクスポート操作のみ)	接続ディレクトリに正常に適用された最新の変更ログ・エントリの番号。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、無効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。

サーバー・チェーン管理

表 A-52「サーバー・チェーン管理」ウィンドウのフィールド（Active Directory または iPlanet の場合）

フィールド	説明
認証の有効化	外部認証機能を有効にします。
変更の有効化	外部変更機能を有効にします。
検索の有効化	外部検索機能を有効にします。
ユーザー・コンテナ	ユーザー検索操作を実行する外部ディレクトリ内のユーザー・コンテナ。
ターゲット・ユーザー・コンテナ	外部ユーザー・コンテナが存在する Oracle Internet Directory 内のユーザー・コンテナ。
グループ・コンテナ	グループ検索操作を実行する外部ディレクトリ内のグループ・コンテナ。
ターゲット・グループ・コンテナ	グループ検索操作を実行する外部ディレクトリ内のグループ・コンテナ。
ホスト	外部ディレクトリ・ホストのホスト名。これは単一値属性です。
ポート	外部ディレクトリ・ホストのポート番号。デフォルト値は 389 です。
ログイン・ユーザー DN	外部ディレクトリの識別名。サーバー・チェーンは、検索および変更操作を実行するために、この識別情報を使用して、外部ディレクトリに対してバインドされます。この識別情報には、操作を実行するために十分な権限が必要です。
ログイン・ユーザー・パスワード	外部ディレクトリの識別名のパスワード。
属性マッピング	外部ディレクトリと Oracle Internet Directory 間の各属性マッピングを指定します。たとえば、Email 属性をターゲット・ディレクトリから Oracle Internet Directory の mail 属性にマップするには、この属性を次のように設定します。 OID Attribute: mail, Target Directory Attribute: eMail

B

LDAP フィルタ定義

この付録に記載されている文書は、Internet Engineering Task Force（IETF）の RFC2254 の許可を得て転載されています。この文書は、次の URL で参照できます。
`http://www.ietf.org`

この文書より後で発行された文書または他の情報が、ここに記載された内容より優先される場合があります。追加情報または補足情報は、前述の Web サイトおよび関連サイトをチェックしてください。

注意： オラクル社は、すべての保証を明示的にも暗黙的にも行いません。ここでいう保証には、この情報の使用がいかなる権利も侵害しないという保証や、特定の目的に対する商業性と適合性への暗示的な保証が含まれますが、これに限定されるものではありません。

Network Working Group — T. Howes
Request for Comments: 2254 — Netscape Communications Corp.
Category: Standards Track — December 1997

The String Representation of LDAP Search Filters

1. Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

IESG Note

This document describes a directory access protocol that provides both read and update access. Update access requires secure authentication, but this document does not mandate implementation of any satisfactory authentication mechanisms.

In accordance with RFC 2026, section 4.4.1, this specification is being approved by IESG as a Proposed Standard despite this limitation, for the following reasons:

a. to encourage implementation and interoperability testing of these protocols (with or without update access) before they are deployed, and

b. to encourage deployment and use of these protocols in read-only applications. (e.g. applications where LDAPv3 is used as a query language for directories which are updated by some secure mechanism other than LDAP), and

c. to avoid delaying the advancement and deployment of other Internet standards-track protocols which require the ability to query, but not update, LDAPv3 directory servers.

Readers are hereby warned that until mandatory authentication mechanisms are standardized, clients and servers written according to this specification which make use of update functionality are UNLIKELY TO INTEROPERATE, or MAY INTEROPERATE ONLY IF AUTHENTICATION IS REDUCED TO AN UNACCEPTABLY WEAK LEVEL.

Implementors are hereby discouraged from deploying LDAPv3 clients or servers which implement the update functionality, until a Proposed Standard for mandatory authentication in LDAPv3 has been approved and published as an RFC.

2. Abstract

The Lightweight Directory Access Protocol (LDAP) [1] defines a network representation of a search filter transmitted to an LDAP server. Some applications may find it useful to have a common way of representing these search filters in a human-readable form. This document defines a human-readable string format for representing LDAP search filters.

This document replaces RFC 1960, extending the string LDAP filter definition to include support for LDAP version 3 extended match filters, and including support for representing the full range of possible LDAP search filters.

3. LDAP Search Filter Definition

An LDAPv3 search filter is defined in Section 4.5.1 of [1] as follows:

```
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
```

where the LDAPString above is limited to the UTF-8 encoding of the ISO 10646 character set [4]. The AttributeDescription is a string representation of the attribute description and is defined in [1].

The AttributeValue and AssertionValue OCTET STRING have the form defined in [2]. The Filter is encoded for transmission over a network using the Basic Encoding Rules defined in [3], with simplifications described in [1].

4. String Search Filter Definition

The string representation of an LDAP search filter is defined by the following grammar, following the ABNF notation defined in [5]. The filter format uses a prefix notation.

```
    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 from Section 4.1.5 of [1]
    matchingrule = MatchingRuleId from Section 4.1.9 of [1]
```

value = AttributeValue from Section 4.1.6 of [1]

The attr, matchingrule, and value constructs are as described in the corresponding section of [1] given above.

If a value should contain any of the following characters

Character	ASCII value
*	0x2a
(	0x28
)	0x29
\	0x5c
NUL	0x00

then the character must be encoded as the backslash '\' character (ASCII 0x5c) followed by the two hexadecimal digits representing the ASCII value of the encoded character. The case of the two hexadecimal digits is not significant.

This simple escaping mechanism eliminates filter-parsing ambiguities and allows any filter that can be represented in LDAP to be represented as a NUL-terminated string. Other characters besides the ones listed above may be escaped using this mechanism, for example, non-printing characters.

For example, the filter checking whether the "cn" attribute contained a value with the character "*" anywhere in it would be represented as

"(cn=*\2a*)".

Note that although both the substring and present productions in the grammar above can produce the "attr=*" construct, this construct is used only to denote a presence filter.

5. Examples

This section gives a few examples of search filters written using this notation.

(cn=Babs Jensen)

(!(cn=Tim Howes))

(&(objectClass=Person)(|(sn=Jensen)(cn=Babs J*)))

(o=univ*of*mich*)

The following examples illustrate the use of extensible matching.

(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)

The second example illustrates the use of the ":dn" notation to indicate that matching rule "2.4.6.8.10" should be used when making comparisons, and that the attributes of an entry's distinguished name should be considered part of the entry when evaluating the match.

The third example denotes an equality match, except that DN components should be considered part of the entry when doing the match.

The fourth example is a filter that should be applied to any attribute supporting the matching rule given (since the attr has been left off). Attributes supporting the matching rule contained in the DN should also be considered.

The following examples illustrate the use of the escaping mechanism.

(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)

The first example shows the use of the escaping mechanism to represent parenthesis characters. The second shows how to represent a "*" in a value, preventing it from being interpreted as a substring indicator. The third illustrates the escaping of the backslash character.

The fourth example shows a filter searching for the four-byte value 0x00000004, illustrating the use of the escaping mechanism to represent arbitrary data, including NUL characters.

The final example illustrates the use of the escaping mechanism to represent various non-ASCII UTF-8 characters.

6. Security Considerations

This memo describes a string representation of LDAP search filters. While the representation itself has no known security implications, LDAP search filters do. They are interpreted by LDAP servers to select entries from which data is retrieved. LDAP servers should take care to protect the data they maintain from unauthorized access.

7. References

[1] Wahl, M., Howes, T., and S. Kille, "Lightweight Directory Access

Protocol (v3)", RFC 2251, December 1997.

[2] Wahl, M., Coulbeck, A., Howes, T., and S. Kille, "Lightweight

Directory Access Protocol (v3): Attribute Syntax Definitions", RFC

2252, December 1997.

[3] Specification of ASN.1 encoding rules: Basic, Canonical, and

Distinguished Encoding Rules, ITU-T Recommendation X.690, 1994.

[4] Yergeau, F., "UTF-8, a transformation format of Unicode and ISO

10646", RFC 2044, October 1996.

[5] Crocker, D., "Standard for the Format of ARPA Internet Text

Messages", STD 11, RFC 822, August 1982.

8. Author's Address

Tim Howes
Netscape Communications Corp.
501 E. Middlefield Road
Mountain View, CA 94043
USA
Phone: +1 415 937-3419
EMail: howes@netscape.com

9. Full Copyright Statement

Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

C

アクセス制御ディレクティブ書式

この付録では、**アクセス制御情報項目**の書式（構文）について説明します。項目は次のとおりです。

- orclACI のスキーマ
- orclEntryLevelACI のスキーマ

orclACI のスキーマ

ユーザー属性 orclACI で定義されているアクセス制御ディレクティブのスキーマは、次のとおりです。

```
OrclACI:
{ object_identifier NAME 'orclACI' DESC 'Stores an inheritable ACI' EQUALITY
accessDirectiveMatch SYNTAX 'accessDirectiveDescription'  USAGE
'directoryOperation'}

accessDirectiveDescription has the following BNF:
<accessDirectiveDescription>
                  ::= access to <object> [by <subject> ( <accessList> )]+

<object> ::= [attr <EQ-OR-NEQ> ( * | (<attrList>) ) | entry] [filter=(<ldapFilter>)]
[DenyGroupOverride] [AppendToAll]

<subject> ::= <entity> [<BindMode>] [Added_object_constraint=(<ldapFilter>)]
<entity> ::= * | self | dn="<regex>" | dnAttr=(<dn_attribute>) | group="<dn>" |
guidattr=(<guid_attribute>) | groupattr=(<group_attribute>) | [SuperUser]

BindMode=(LDAP_authentication_choice)|LDAP_security_choice)
LDAP_authentication_choice::= proxy | simple | MD5Digest | PKCS12
LDAP_security_choice::= SSLNoAuth | SSLOneWay | SASL

<accessList> ::= <access> | <access>, <accessList>

<access> ::= none | compare | search | browse | proxy | read | selfwrite | write | add
| delete | nocompare | nosearch | nobrowse | noproxy |noread | noselfwrite | nowrite |
noadd | nodelete

<attrList> ::=  <attribute name> | <attribute name>,<attrList>

<EQ-OR-NEQ> ::=  = | !=

<regex> ::= <dn> | *,<dn_of_any_subtree_root>
```

注意： 前述の正規表現は、任意の式のどれにでも対応するという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> )]+
```

D

ディレクトリにおけるグローバリゼーション・サポート

Oracle Internet Directory ではグローバリゼーション・サポートを使用して、システム固有の言語でデータの格納、処理および取得を行います。グローバリゼーション・サポートは、Oracle Internet Directory のユーティリティとエラー・メッセージを、システム固有の言語とロケールに自動的に調整します。

この付録では、Oracle Internet Directory で使用されるグローバリゼーション・サポートと、Oracle Internet Directory 環境における様々なコンポーネントとツールに必要な環境変数 NLS_LANG について説明します。

> **関連項目：** グローバリゼーション・サポートを構成する前に、3-18 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。

この付録の項目は次のとおりです。

- キャラクタ・セットおよびディレクトリの概要
- 環境変数 NLS_LANG
- 非 AL32UTF8 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 LDAP 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

キャラクタ・セットおよびディレクトリの概要

コンピュータ・システムで文字を処理する場合、文字のグラフィカルな表現のかわりに数値コードを使用します。たとえば、データベースに A という文字を格納する場合、実際にはソフトウェアによって文字として解釈される数値コードが格納されます。

文字グループ（アルファベット文字、表意文字、記号、句読点および制御文字など）は、キャラクタ・セットとしてエンコードできます。エンコードされた各キャラクタ・セットでは、セット内の各文字に一意のコードを割り当てます。たとえば、ASCII コード体系では、英語の大文字アルファベットの最初の文字の文字コードは Ox4 ですが、EBCDIC コード体系では Oxc1 です。

コンピュータ業界では多くのエンコードされたキャラクタ・セットが使用されています。これらのキャラクタ・セットは、利用可能な文字の数やタイプおよび様々な面で異なります。

データベースの作成時には、エンコードされたキャラクタ・セットを指定します。キャラクタ・セットを選択すると、特に、データベース内で表示される言語が決定されます。

ほとんどの各国語キャラクタ・セット、国際キャラクタ・セットおよびベンダー固有キャラクタ・セットの標準がサポートされています。

この項の項目は次のとおりです。

Unicode の概要

日々の E-Business の要件を満たすために必要な文字が十分に含まれている単一のキャラクタ・セットはありません。たとえば、欧州連合内のすべての言語を表すことのできる各国語キャラクタ・セットはありません。さらに、異なるキャラクタ・セットでは同じ文字が異なるコードで表されている場合もあるため、キャラクタ・セット間で競合が起きる可能性もあります。

この障害を克服するため、Unicode と呼ばれるグローバルなキャラクタ・セットが開発されました。これは、句読点、発音符、数学記号、技術記号、音符などを含めたあらゆる言語の情報を格納できる、汎用のエンコードされたキャラクタ・セットです。Unicode 標準のバージョン 3.2 では、世界中のアルファベット、表意文字のセットおよび記号のコレクションから 95,000 文字以上をサポートしています。45,000 以上の補助文字も含まれています。これらのほとんどは、まれにしか使用されないものの、電子文書で表示するために必要な中国語、日本語および韓国語の文字です。

Unicode には 2 つ以上の標準が実装されており、これらは表 D-1 に示されています。

表 D-1 Unicode の実装

実装	説明
UTF-8	Unicode の可変幅 8 ビット・エンコーディング。1 つの Unicode 文字は 1、2、3 または 4 バイトになります。ヨーロッパ言語の記述に含まれる文字は、1 バイトまたは 2 バイトで表示されます。アジア言語の記述に含まれる文字は 3 バイトで表示され、補助文字は 4 バイトで表示されます。
UCS-2	Unicode の固定幅 16 ビット・エンコーディング。記述に関係なく、各文字は 2 バイトです。
UTF-16	Unicode の 16 ビット・エンコーディング。Unicode 3.1 で追加された補助文字をサポートするための UCS-2 の拡張方式です。 1 つの文字は 2 バイトまたは 4 バイトです。ヨーロッパ言語およびアジア言語の記述に含まれる文字は 2 バイトで表示され、補助文字は 4 バイトで表示されます。

Oracle と UTF-8 の概要

オラクル社では、Oracle データベース・バージョン 7 からデータベース・キャラクタ・セットとして Unicode のサポートを開始しました。Oracle9*i* では、AL32UTF8 と呼ばれる新しい UTF-8 キャラクタ・セットを追加しました。このデータベース・キャラクタ・セットは、最新の補助文字を含む最新バージョンの Unicode（3.2）をサポートしています。オラクル社では、Unicode 標準の将来のバージョンをサポートするため、必要に応じて AL32UTF8 を拡張する予定です。

Oracle Internet Directory のアップグレード時の UTF8 から AL32UTF8 への移行

Oracle Internet Directory では AL32UTF8 をサポートするようになりました。Oracle Internet Directory を 10*g*（10.1.4.0.1）以前のバージョンからアップグレードする場合は、パフォーマンスの向上のため、ディレクトリ・データベースのキャラクタ・セットを UTF8 から AL32UTF8 へ変更することをお薦めします。これは、次の手順に従って行います。

1. Character Set Scanner（CSSCAN）を実行して、現在のデータベースに無効な UTF8 文字が含まれていないことを確認します。
2. CSALTER スクリプトを実行して、データベースを AL32UTF8 に更新します。

> **関連資料：** Oracle Database ドキュメント・ライブラリの『Oracle Database グローバリゼーション・サポート・ガイド』のキャラクタ・セットの移行に関する章

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。

NLS_LANG パラメータのコンポーネントは、表 D-2 に示すとおりです。

表 D-2 NLS_LANG パラメータのコンポーネント

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。 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。 **関連資料：** 言語の完全なリストは、Oracle Database ドキュメント・ライブラリの『Oracle 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。 **関連資料：** 地域の完全なリストは、Oracle Database ドキュメント・ライブラリの『Oracle 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。

表 D-2 NLS_LANG パラメータのコンポーネント（続き）

コンポーネント	説明
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、WE8MSWIN1252、JA16SJIS または AL32UTF8 などの一意の頭字語があります。 **関連資料 :** キャラクタ・セットの完全なリストは、Oracle Database ドキュメント・ライブラリの『Oracle 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。

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 AL32UTF8 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 AL32UTF8 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

関連資料 :『Oracle Identity Management ユーザー・リファレンス』の LDIF ファイルの形式化規則と例に関する項

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 では、属性の値への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 文字列のみの値を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 ファイルで使用することも、キーボードで入力することもできます。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）

`-E` *`character_set`* 引数を、コマンドライン・ツール `dipassistant` と、コマンドライン LDAP ツール `ldapadd`、`ldapaddmt`、`ldapbind`、`ldapcompare`、`ldapmoddn`、`ldapmod`、`ldapdelete` および `ldapsearch` で使用します。`encode="`*`character_set`*`"` 引数を、コマンドライン・バルク・ツール `bulkload`、`bulkmodify`、`bulkdelete` および `ldifwrite` で使用します。

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

`-E` *`character_set`* 引数や `encode=`*`character_set`* 引数を、コマンドライン・ツールで使用する必要はありません。Oracle Internet Directory 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

`-E character_set` 引数を、コマンドライン・ツール `dipassistant`、`ldapadd`、`ldapaddmt`、`ldapbind`、`ldapcompare`、`ldapmoddn`、`ldapmod`、`ldapdelete` および `ldapsearch` で使用します。`encode=character_set` 引数を、`bulkload`、`bulkmodify`、`bulkdelete` および `ldifwrite` で使用します。

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キャラクタ・セットは 1 つのみです。

コマンドライン LDAP ツールでのグローバリゼーション・サポートの使用方法

Oracle Internet Directory のコマンドライン・ツールは、キーボード入力または LDIF ファイル入力を次の方法で読み取ります。

- ASCII 文字のみ
- 非 ASCII 入力（ネイティブ言語キャラクタ・セット）
- UTF-8 またはネイティブ文字列の BASE64 でエンコードされた値（LDIF ファイル入力のみ）

LDIF ファイルまたはキーボードからの入力として使用されているキャラクタ・セットが UTF-8 以外の場合、コマンドライン・ツールは、LDAP サーバーに送信する前に、その入力を UTF-8 形式に変換する必要があります。

コマンドライン・ツールで入力を UTF-8 に変換するには、`-E character_set` 引数を、`dipassistant` または任意のコマンドライン LDAP ツールで指定します。`encode="character_set"` 引数を、`bulkload`、`bulkmodify`、`bulkdelete` および `ldifwrite` で指定します。

この項の項目は次のとおりです。

- 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 LDAP 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、ディレクトリ・サーバーに送信される前に、簡体字中国語（GBK）から Unicode 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 AL32UTF8 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、ディレクトリ・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"` に変換されます。

例 : コマンドライン LDAP ツールでの -E 引数の使用方法

表 D-3 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 AL32UTF8 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 GBK 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。

表 D-3 の例には、.ZHS16GBK キャラクタ・セットに属している実際の文字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・セット内の実際の文字が含まれる場合は、-E 引数を使用する必要があります。

> **関連資料 :** 各コマンドライン・ツールの構文と使用方法は、『Oracle Identity Management ユーザー・リファレンス』の、Oracle Internet Directory サーバーの管理ツールに関する項を参照してください。

表 D-3 例 : コマンドライン・ツールでの -E 引数の使用方法

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 のキャラクタ・セット・コンポーネントはデフォルトで 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、AL32UTF8 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 AL32UTF8 キャラクタ・セットが使用されます。

注意： Microsoft 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 をリセット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。AL32UTF8 は使用できません。MS-DOS セッションでコマンドライン・ツールに使用するキャラクタ・セットの詳細は、Oracle Database の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 Oracle Database を使用している場合、データベース・キャラクタ・セットも AL32UTF8 に設定する必要があります。

関連資料 : Oracle Database ドキュメント・ライブラリの『Oracle Database グローバリゼーション・サポート・ガイド』および Oracle Database のインストレーション・ガイドを参照してください。

レジストリの NLS_LANG パラメータの値を変更しないように注意してください。

バルク・ツールでのグローバリゼーション・サポートの使用方法

Oracle Internet Directory は、LDIF ファイルのテキスト・データの読取り / 書込みを、LDAP で指定されている UTF-8 エンコーディングで常に行います。

この項では、次の各バルク・ツールに使用する引数の例を紹介します。

- bulkload でのグローバリゼーション・サポートの使用方法
- ldifwrite でのグローバリゼーション・サポートの使用方法
- bulkdelete でのグローバリゼーション・サポートの使用方法
- bulkmodify でのグローバリゼーション・サポートの使用方法

関連資料 : 各バルク・ツールの引数リストは、『Oracle Identity Management ユーザー・リファレンス』の、Oracle Internet Directory サーバーの管理ツールに関する項を参照してください。

bulkload でのグローバリゼーション・サポートの使用方法

コマンドに引数 -encode="*character_set*" を追加します。この入力の LDIF ファイルは *"character_set"* でエンコードされています。

たとえば、次のように入力します。

```
bulkload connect="connect_string" encode=".ZHS16GBK" check="TRUE" \
   generate="TRUE" file="my_ldif_file"
```

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。

次に例を示します。

```
ldifwrite connect="connect_string" basedn="baseDN" file="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 AL32UTF8 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（GBK）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（GBK）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。

次に例を示します。

```
bulkdelete connect="connect_string" encode=".ZHS16GBK" \
            base="ou=manufacturing,o=acme,c=us"
```

この例では、-base オプションの値に、ZHS16GBK ネイティブ・キャラクタ・セット（簡体字中国語）を使用できます。

bulkmodify 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。

次に例を示します。

```
bulkmodify connect="my_service_name" encode=".ZHS16GBK" \
             basedn="ou=manufacturing,o=acme,c=us" replace="title" \
             value=Foreman filter="objectclass=*"
```

この例では、basedn、value および filter の各引数の値を簡体字中国語（GBK）キャラクタ・セットを使用して指定できます。

E

ユーザーおよびグループの作成ベースおよび検索ベースに対するアクセス制御の設定

ユーザー検索ベース、ユーザー作成ベース、グループ検索ベース、グループ作成ベースを変更すると、新しいコンテナに対するアクセス制御を適切に設定する必要があります。この付録の項目は次のとおりです。

ユーザー検索ベースおよびユーザー作成ベースに対するアクセス制御の設定

ユーザー検索ベースおよびユーザー作成ベースに対するアクセス制御を設定するには、次のようにします。

1. 次の内容で、LDIF（user_aci.ldif）ファイルを作成します。

```
--- BEGIN LDIF file contents---
dn: %usersearch_or_createbase_dn%
changetype: modify
add: orclaci
orclaci: access to entry by group="cn=oracledascreateuser,
 cn=groups,cn=OracleContext,%subscriberdn%"
 added_object_constraint=(objectclass=orcluser*) (browse,add) by
 group="cn=Common User Attributes, cn=Groups,
 cn=OracleContext,%subscriberdn%" (browse) by
 group="cn=PKIAdmins, cn=groups, cn=OracleContext,%subscriberdn%" (browse)
orclaci: access to entry filter=(objectclass=inetorgperson) by
 group="cn=oracledascreateuser, cn=groups,cn=OracleContext,%subscriberdn%"
 added_object_constraint=(objectclass=orcluser*) (browse,add) by
 group="cn=oracledasdeleteuser, cn=groups,cn=OracleContext,%subscriberdn%"
 (browse,delete) by group="cn=oracledasedituser,
 cn=groups,cn=OracleContext,%subscriberdn%" (browse) by
 group="cn=UserProxyPrivilege, cn=Groups,cn=OracleContext,%subscriberdn%"
 (browse,
 proxy) by dn="orclApplicationCommonName=DASApp, cn=DAS,
 cn=Products,cn=oraclecontext" (browse,proxy) by self (browse, nodelete, noadd)
 by
 group="cn=Common User Attributes, cn=Groups,cn=OracleContext,%subscriberdn%"
 (browse) by * (browse, noadd, nodelete)
orclaci: access to attr=(*) filter=(objectclass=inetorgperson) by
 group="cn=oracledasedituser, cn=groups,cn=OracleContext,
 %subscriberdn%" (read,search,write,compare) by self (
 read,search,write,selfwrite,compare) by *
 (read, nowrite, nocompare)
orclaci: access to attr=(userPassword)
 filter=(objectclass=inetorgperson) by
 group="cn=OracleUserSecurityAdmins,cn=Groups,
 cn=OracleContext, %subscriberdn%"
 (read,search,write,compare) by group="cn=oracledasedituser,
 cn=groups,cn=OracleContext,%subscriberdn%"
 (read,search,write,compare) by self
 (read,search,write,selfwrite,compare) by group="cn=authenticationServices,
 cn=Groups,cn=OracleContext,%subscriberdn%" (compare) by * (none)
orclaci: access to attr=(authpassword, orclpasswordverifier, orclpassword) by
 group="cn=oracledasedituser,cn=groups,cn=OracleContext,%subscriberdn%"
 (read,search,write,compare) by
 group="cn=verifierServices,cn=Groups,cn=OracleContext,%subscriberdn%"
 (search, read, compare) by self (search,read,write,compare) by * (none)
orclaci: access to attr=(orclpwdaccountunlock) by
 group="cn=oracledasedituser,cn=groups,cn=OracleContext,%subscriberdn%" (
 write) by * (none)
orclaci: access to attr=(usercertificate, usersmimecertificate) by
 group="cn=PKIAdmins,cn=Groups,cn=OracleContext,%subscriberdn%"
 (read, search, write, compare) by self (read, search, compare) by *
 (read, search, compare)
orclaci: access to attr=(mail) by
 group="cn=EmailAdminsGroup,cn=EmailServerContainer,cn=Products,
 cn=OracleContext" (write) by group="cn=oracledasedituser,
 cn=groups,cn=OracleContext,%subscriberdn%" (read,search,write,compare)
orclaci: access to attr=(orclguid, orclisenabled, modifytimestamp,mail)
 by group="cn=Common User Attributes,
```

```
 cn=Groups,cn=OracleContext,%subscriberdn%"
 (read, search, compare) by group="cn=oracledasedituser,
 cn=groups,cn=OracleContext,%subscriberdn%" (read,search,write,compare)
 by * (read, nowrite, nocompare)
orclaci: access to attr=(orclpasswordhintanswer) by
 group="cn=Common User Attributes,
 cn=Groups,cn=OracleContext,%subscriberdn%" (read, search, compare) by self
 (read,search,write,selfwrite,compare) by * (noread, nowrite, nocompare)
orclaci: access to attr=(orclpasswordhint) by
 group="cn=Common User Attributes,
 cn=Groups,cn=OracleContext,%subscriberdn%" (read, search, compare) by self
 (read,search,write,selfwrite,compare) by
 group="cn=OracleUserSecurityAdmins,cn=Groups,cn=OracleContext,
 %subscriberdn%" (read,search,write,compare) by *
 (noread, nowrite, nocompare)
orclaci: access to attr=(displayName, preferredlanguage,
 orcltimezone,orcldateofbirth,orclgender,orclwirelessaccountnumber,cn,
 uid,homephone,telephonenumber) by group="cn=Common User Attributes,
 cn=Groups,cn=OracleContext,%subscriberdn%"
 (read, search, compare) by group="cn=oracledasedituser,
 cn=groups,cn=OracleContext,%subscriberdn%" (read,search,write,compare)
 by self (read,search,write,selfwrite,compare) by *
 (read, nowrite, nocompare)
        -
add: orclentrylevelaci
orclentrylevelaci: access to entry by group="cn=oracledascreateuser,
 cn=groups,cn=OracleContext,%subscriberdn%" added_object_constraint=
 (objectclass=orcluser*) (browse, add) by * (browse)
---END LDIF file contents------
```

2. `%subscriberdn%` をサブスクライバの DN に置き換え、`%usersearch_or_createbase_dn%` を、新しいユーザー検索 / 作成ベースが示すコンテナの新しい DN 値に置き換えます。
3. 次のように、ldapmodify コマンドを入力します。

```
ldapmodify -p oidport -h oidhost -D cn=orcladmin -w Instance  Password -v \
           -f  user_aci.ldif
```

グループ検索ベースおよびグループ作成ベースに対するアクセス制御の設定

グループ検索ベースおよびグループ作成ベースに対するアクセス制御を設定するには、次のようにします。

1. 次の内容で、ldif（group_aci.ldif）ファイルを作成します。

```
--- BEGIN LDIF file contents---
dn: %groupsearch_or_createbase_dn%
changetype: modify
add: orclaci
orclaci: access to entry by group="cn=IASAdmins,
 cn=groups,cn=OracleContext,%subscriberdn%"
 added_object_constraint=(objectclass=orclcontainer) (browse,add)
orclaci: access to entry by group="cn=oracledascreategroup,
 cn=groups,cn=OracleContext,%subscriberdn%"
 added_object_constraint=(objectclass=orclgroup*) (browse,add) by
 group="cn=Common
 Group Attributes, cn=Groups,cn=OracleContext,%subscriberdn%" (browse)
orclaci: access to entry filter=(&(objectclass=orclgroup)(orclisvisible=false))
 by
 groupattr=(owner) (browse, add, delete) by dnattr=(owner)
 (browse, add, delete) by
 group="cn=Common Group Attributes, cn=Groups,cn=OracleContext,%subscriberdn%"
```

```
 (browse) by * (none)
orclaci: access to entry
 filter=(&(objectclass=orclgroup)(!(orclisvisible=false))) by
 group="cn=oracledascreategroup, cn=groups,cn=OracleContext,%subscriberdn%"
 added_object_constraint=(objectclass=orclgroup) (browse,add) by
 group="cn=oracledasdeletegroup, cn=groups,cn=OracleContext,%subscriberdn%"
 (browse,delete) by group="cn=oracledaseditgroup,
 cn=Groups,cn=OracleContext,%subscriberdn%" (browse) by groupattr=(owner) (
 browse,
 add, delete) by dnattr=(owner) (browse, add, delete) by group="cn=Common Group
 Attributes, cn=Groups,cn=OracleContext,%subscriberdn%" (browse)
orclaci: access to attr=(*)
 filter=(&(objectclass=orclgroup)(orclisvisible=false)) by
 groupattr=(owner) (read,search,write,compare) by dnattr=(owner)
 (read,search,write,compare) by * (none) by group="cn=Common Group Attributes,
 cn=Groups,cn=OracleContext,%subscriberdn%" (read, search, compare)
orclaci: access to attr=(*)
 filter=(&(objectclass=orclgroup)(!(orclisvisible=false))) by
 groupattr=(owner) (read,search,write,compare) by dnattr=(owner)
 (read,search,write,compare)  by group="cn=oracledaseditgroup,
 cn=groups,cn=OracleContext,%subscriberdn%" (read,search,write,compare) by
 group="cn=Common Group Attributes, cn=Groups,cn=OracleContext,%subscriberdn%"
 (read, search, compare)
      -
add: orclentrylevelaci
orclentrylevelaci: access to entry by group="cn=oracledascreategroup,
 cn=groups,cn=OracleContext,%subscriberdn%"
 added_object_constraint=(objectclass=orclgroup) (browse, add) by
 group="cn=IASAdmins, cn=groups,cn=OracleContext,%subscriberdn%"
 added_object_constraint=(objectclass=orclcontainer) (browse,add) by * (browse)
---END LDIF file contents------
```

2. `%subscriberdn%` をサブスクライバの DN に置き換え、`%groupsearch_or_createbase_dn%` を、新しいグループ検索 / 作成ベースが示すコンテナの新しい DN 値に置き換えます。
3. 次のように、ldapmodify コマンドを入力します。

```
ldapmodify -p oidport -h oidhost -D cn=orcladmin -w instance password \
           -v -f  group_aci.ldif
```

F

マルチマスター・レプリケーション・プロセス

この付録では、マルチマスター・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。項目は次のとおりです。

- マルチマスター・レプリケーション・プロセスがコンシューマに新規エントリを追加する動作
- マルチマスター・レプリケーション・プロセスがエントリを削除する動作
- マルチマスター・レプリケーション・プロセスがエントリを変更する動作
- マルチマスター・レプリケーション・プロセスが相対識別名を変更する動作
- マルチマスター・レプリケーション・プロセスが識別名を変更する動作

マルチマスター・レプリケーション・プロセスがコンシューマに新規エントリを追加する動作

ディレクトリ・レプリケーション・サーバーは、コンシューマに新規エントリを追加すると、次の変更適用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適用プロセスを繰り返します。

2 回目から最終試行前までの試行で変更エントリが正常に適用されなかった場合

ディレクトリ・レプリケーション・サーバーは変更エントリをリトライ・キューに保持したまま、再試行回数を減らして、変更適用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重複していないかどうかをチェックします。

変更エントリが重複エントリの場合

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。

変更エントリが重複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適用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、管理者によるアクションを待ちながら、指定した間隔で変更適用プロセスを繰り返します。管理者は、Oracle Internet Directory 比較調整ツールおよび管理者操作キュー操作ツールを使用して、競合を解消できます。

マルチマスター・レプリケーション・プロセスがエントリを削除する動作

ディレクトリ・レプリケーション・サーバーは、コンシューマからエントリを削除すると、次の変更適用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、変更適用プロセスを繰り返します。

2 回目から最終試行前までの試行で変更エントリが正常に適用されなかった場合

ディレクトリ・レプリケーション・サーバーは変更エントリをリトライ・キューに保持したまま、再試行回数を減らして、変更適用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適用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、管理者によるアクションを待ちながら、指定した間隔で変更適用プロセスを繰り返します。管理者は、Oracle Internet Directory 比較調整ツールおよび管理者操作キュー操作ツールを使用して、競合を解消できます。

マルチマスター・レプリケーション・プロセスがエントリを変更する動作

ディレクトリ・レプリケーション・サーバーは、コンシューマのエントリを変更すると、次の変更適用プロセスを実行します。

1. ディレクトリ・レプリケーション・サーバーは、コンシューマ内で変更エントリの GUID と一致する GUID を持つエントリを探します。
2. 一致するエントリがコンシューマ内にある場合、ディレクトリ・レプリケーション・サーバーは、変更エントリ内の各属性と、ターゲット・エントリ内の各属性を比較します。
3. その後、ディレクトリ・レプリケーション・サーバーは、次の競合解消規則を適用します。
   a. 変更時間が最新の属性を使用します。
   b. 最新バージョンの属性を使用します（バージョン 1、2 または 3 など）。
   c. ホスト上の変更された属性のうち、アルファベットの A に最も近い名前のエントリを使用します。
4. ディレクトリ・レプリケーション・サーバーは、フィルタ処理済の変更を適用し、変更エントリをパージ・キューに入れます。

1 回目の試行で変更エントリが正常に適用されなかった場合

ディレクトリ・レプリケーション・サーバーは変更エントリをリトライ・キューに入れ、再試行回数を指定の最大値に設定して、変更適用プロセスを繰り返します。

2 回目から最終試行前までの試行で変更エントリが正常に適用されなかった場合

ディレクトリ・レプリケーション・サーバーは変更エントリをリトライ・キューに保持したまま、再試行回数を減らして、変更適用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適用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、管理者によるアクションを待ちながら、指定した間隔で変更適用プロセスを繰り返します。管理者は、Oracle Internet Directory 比較調整ツールおよび管理者操作キュー操作ツールを使用して、競合を解消できます。

マルチマスター・レプリケーション・プロセスが相対識別名を変更する動作

ディレクトリ・レプリケーション・サーバーは、コンシューマのエントリの相対識別名を変更すると、次の変更適用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、変更適用プロセスを繰り返します。

2 回目から最終試行前までの試行で変更エントリが正常に適用されなかった場合

ディレクトリ・レプリケーション・サーバーは変更エントリをリトライ・キューに保持したまま、再試行回数を減らして、変更適用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・エントリと重複していないかどうかをチェックします。

変更エントリが重複エントリの場合

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。

変更エントリが重複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適用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、管理者によるアクションを待ちながら、指定した間隔で変更適用プロセスを繰り返します。管理者は、Oracle Internet Directory 比較調整ツールおよび管理者操作キュー操作ツールを使用して、競合を解消できます。

マルチマスター・レプリケーション・プロセスが識別名を変更する動作

ディレクトリ・レプリケーション・サーバーは、コンシューマのエントリの識別名を変更すると、次の変更適用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、変更適用プロセスを繰り返します。

2 回目から最終試行前までの試行で変更エントリが正常に適用されなかった場合

ディレクトリ・レプリケーション・サーバーは変更エントリをリトライ・キューに保持したまま、再試行回数を減らして、変更適用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・エントリと重複していないかどうかをチェックします。

変更エントリが重複エントリの場合

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。

変更エントリが重複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適用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、管理者によるアクションを待ちながら、指定した間隔で変更適用プロセスを繰り返します。管理者は、Oracle Internet Directory 比較調整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。

G

ディレクトリでのユーザー証明書の検索

10*g*（10.1.4.0.1）より、コマンドラインからのバイナリ属性 `usercertificate` の検索が可能になりました。

10*g* リリース 2（10.1.2.0.2）より前のリリースでは、証明書からユーザーを特定するには、証明書で指定されている識別名を使用する必要がありました。これを証明書の一致といいます。Oracle Internet Directory では、10*g* リリース 2（10.1.2.0.2）から、証明書の一致に加えて、証明書のマッピングも使用できるようになりました。証明書の一致では、ユーザー証明書がディレクトリに用意されている必要があります。証明書のマッピングでは、ユーザー証明書を用意する必要はありません。

この付録の項目は次のとおりです。

証明書のマッピング

証明書のマッピングを使用すれば、証明書とユーザーの識別名とのマッピング・ルールを定義できます。証明書のマッピング・ルールは、証明書を解析するためのルールと、ディレクトリにユーザー ID を問い合せるためのルールの集まりです。マッピング・ルールでは、証明書のカスタム拡張のみを使用できます。

次の例は、証明書マッピング・ルールを追加、削除および変更する方法を示しています。

証明書マッピング・ルールの追加

ldapmodify を使用してマッピング・ルールを追加する方法は次のとおりです。

```
ldapmodify -h hostName -p  port_number -f certMapRuleAdd.ldif
```

certMapRuleAdd.ldif ファイルは次のようになります。

```
dn: cn=maprule1,cn=SASL-EXTERNAL,cn=Identity Mapping Configurations,cn=Server
Configurations
cn: maprule1
objectclass: orclidmapping
objectclass: orclcertidmapping
orclSearchScope: subtree
orclSearchFilter: (cn=$\(2.16.750.5.14.2.81.2.5.1\))
orclcertExtensionOID: 2.16.750.5.14.2.81.2.5
orclcertExtensionAttribute: 2.16.750.5.14.2.81.2.5.1
```

証明書マッピング・ルールの削除

ldapdelete を使用してマッピング・ルールを削除する方法は次のとおりです。

```
ldapdelete hostName -p  port_number "cn=maprule1,cn=SASL-EXTERNAL,cn=Identity Mapping
Configurations,cn=Server Configurations"
```

証明書マッピング・ルールの変更

ldapmodify を使用してマッピング・ルールを変更する方法は次のとおりです。

```
ldapmodify -h hostName -p  port_number -f certMapRuleMod.ldif
```

certMapRuleMod.ldif ファイルは次のようになります。

```
dn: cn=maprule1,cn=SASL-EXTERNAL,cn=Identity Mapping Configurations,cn=Server
Configurations
changetype:modify
replace: <attrName>
<attrName>: <attrValue>
```

検索タイプ

次の 2 種類の ldapsearch フィルタを使用できます。

- "usercertificate=*certificate_serial_number*$*certificate_issuer_DN*" 形式のフィルタ。証明書の検索には、証明書のシリアル番号および証明書発行者の DN の組合せが使用されます。この組合せを、証明書の一致値と言います。
- "usercertificate;binary=*base_64_encoded_value_of_certificate*" 形式のフィルタ。このフィルタを使用すると、次の 2 つの事柄に応じて、6 つの検索タイプのいずれかを使用できます。
  - DSA 構成設定の属性（DN: "cn=dsaconfig,cn=configsets,cn=oracle internet directory"）の値、orclpkimatchingrule
  - LDAP 制御 2.16.840.1.113894.1.8.23 の有無

  "usercertificate;binary=*base_64_encoded_value_of_certificate*" 形式のフィルタで使用可能な 6 つの検索タイプは次のとおりです。

LDAP 制御の存在	orclpkimatchingrule の値	検索の動作
なし	使用しない	usercertificate の検索に、クライアント証明書のハッシュ値を使用する。
存在	0	完全一致検索を実行する。クライアント証明書のサブジェクト DN が検索ベースとなる。この DN とディレクトリ内のユーザー DN とが比較される。検索範囲は Base。フィルタは objectclass=*。
存在	1	usercertificate の検索に、クライアント証明書のハッシュ値を使用する。
存在	2（デフォルト）	usercertificate の検索に、クライアント証明書のハッシュ値を使用する。この検索の結果がない場合は、完全一致検索を実行する。
存在	3	マッピング・ルールが使用される。
存在	4	最初にマッピング・ルールが使用される。何も検索されない場合は、値を 2 とみなして検索が続行される。

orclpkimatchingrule に必要な値を設定するには、ldapmodify ツールを使用します。

注意：

- サブストリング・フィルタを使用して usercertificate 属性を検索することはできません。
- 完全一致検索では、検索フィルタに使用できる属性値のアサーションは 1 つのみです。
- 1 レベル検索およびサブツリー検索のみがサポートされています。
- catalog ツールでは、ユーザー証明書のカタログ（ct_orclcertificatehash および ct_orclcertificatematch）はサポートされていません。
- 10*g*（10.1.4.0.1）に証明書のハッシュ値を導入する場合は、証明書を以前のリリースからアップグレードする必要があります。『Oracle Identity Management ユーザー・リファレンス』の upgradecert.pl コマンドライン・ツール・リファレンスを参照してください。

関連項目： 16-4 ページの「直接認証」

H

LDAP のレプリカ状態

この付録では、LDAP ベースのレプリケーションのレプリカ状態について説明します。LDAP レプリカは、アドバンスト・レプリケーションには影響しません。

LDAP ベースのレプリケーションを構成し、レプリケーション・サーバーを起動すると、サーバーはローカルのレプリカ（orclreplicaid=*local_Replica_ID*, cn=replication configuration）からレプリカ状態 orclreplicastate を読み取ります。表 H-1 に示すとおり、レプリケーション・サーバーの動作はローカルのレプリカ状態によって異なります。レプリケーション・サーバーは、ローカル（コンシューマ）・ノードからローカルのレプリカ状態を読み取ります。

表 H-1 LDAP のレプリカ状態

値	意味	レプリケーション・サーバーの動作
0	ブートストラップ。	レプリケーションのネーミング・コンテキスト構成に基づき、サプライヤからコンシューマ・ディレクトリを同期化するためのレプリケーションのブートストラップ・プロセスを開始する。ブートストラップの進行に合せてレプリカ状態を更新する。 ■ ブートストラップの開始直後は、レプリカ状態を 3（ブートストラップ進行中）にする。 ■ cn=oraclecontext のブートストラップが正常に完了すると、レプリカ状態を 4（ブートストラップ進行中、cn=oraclecontext のブートストラップが完了）にする。 ■ ブートストラップが完了したが、ブートストラップ中に障害が検出された場合は、レプリカ状態を 5（ブートストラップ・エラーの発生）にする。次に、レプリカ状態がリセットされるまで待機する。**注意：**管理者操作が必要。詳細は L-15 ページの「Oracle Internet Directory レプリケーションのトラブルシューティング」を参照。 ■ ブートストラップが正常に完了すると、レプリカ状態を 1（オンライン）にする。次に、レプリケーションを自動的に開始し、通常のレプリケーション・プロセスを実行する。
1	オンライン。	通常のレプリケーション・プロセスを開始し、サプライヤからコンシューマへ変更をレプリケートする。
2	オフライン。	エラー・メッセージを、次のように oidrepld.log に記録する。 `2004/09/24:17:41:44 * Replica(dlsun1418_replica2) is in OFFLINE mode, Please update the replica state and restart OIDREPLD...` 管理者は、レプリカ状態を適切に設定し、レプリケーション・サーバーを再起動する必要がある。
3	ブートストラップ進行中。	レプリカ状態を 0（ブートストラップ）に戻し、状態が 0 である場合と同様に、ブートストラップを再度開始する。

表 H-1 LDAP のレプリカ状態（続き）

値	意味	レプリケーション・サーバーの動作
4	ブートストラップ進行中、cn=oraclecontext のブートストラップが完了。	レプリカ状態を 0（ブートストラップ）に戻し、状態が 0 である場合と同様に、ブートストラップを再度開始する。
5	ブートストラップの完了。1 つ以上のネーミング・コンテキストで障害を検出。	エラー・メッセージを、次のように oidrepld.log に記録する。 2004/09/24:17:13:30 * Replication BOOTSTRAP_ERROR mode detected for replica(dlsu n1418_replica2) 次に、レプリカ状態が適切にリセットされるまで待機する。
6	データベース・コピー・ベースの addnode。Oracle Database アドバンスト・レプリケーション・ベースのレプリケーションでのみ使用。	このモードは、Oracle Database アドバンスト・レプリケーション・ベースのレプリケーションの場合、レプリカがデータベース・コピー・ベースの addnode であることを示します。このレプリカ状態は、LDAP ベースのレプリケーションでは使用されません。

Oracle Internet Directory レプリケーション・サーバーでは、Oracle Internet Directory レプリケーション・サーバー・ログ（$ORACLE_HOME/ldap/log/oidrepld00.log）にブートストラップ・プロセスが記録されます。

ブートストラップが正常に完了した場合、ログは次の例と同様になり、レプリケーション・サーバーが自動的に通常のレプリケーション・プロセスを開始します。

```
2004/10/06:17:13:25 * Starting OIDREPLD against isunnad03:5555...
2004/10/06:17:13:26 * Starting scheduler...
2004/10/06:17:13:27 * Start to BootStrap from supplier=isunnad03_purify to
consumer=isunnad03_purify3
2004/10/06:17:13:28 * gslrbssSyncDIT:Replicating namingcontext=cn=oraclecontext ......
2004/10/06:17:14:21 * gslrbssSyncDIT:Sync done successfully for namingctx:
cn=oraclecontext, 222 entries matched
2004/10/06:17:14:21 * gslrbssSyncDIT:Replicating namingcontext=c=india ......
2004/10/06:17:14:21 * gslrbssSyncDIT:Sync done successfully for namingctx: c=india, 0
entries matched
2004/10/06:17:14:21 * gslrbssSyncDIT:Replicating namingcontext=c=uk ......
2004/10/06:17:19:57 * gslrbssSyncDIT:Sync done successfully for namingctx: c=uk, 1087
entries matched
2004/10/06:17:19:57 * gslrbssSyncDIT:Replicating namingcontext=cn=oracleschemaversion
......
2004/10/06:17:19:59 * gslrbssSyncDIT:Sync done successfully for namingctx:
cn=oracleschemaversion, 10 entries matched
2004/10/06:17:20:01 * gslrbsbBootStrap: BOOTSTRAP DONE SUCCESSFULL
```

障害が検出された場合、ログは次の例と同様になります。

```
2004/09/14:12:57:23 * Starting OIDREPLD against dlsun1418:4444...
2004/09/14:12:57:25 * Starting scheduler...
2004/09/14:12:57:26 * Start to BootStrap from supplier=dlsun1418_replica to
consumer=dlsun1418_replica2
2004/09/14:12:57:27 * gslrbssSyncDIT:Replicating namingcontext=cn=oraclecontext ......
2004/09/14:12:58:21 * gslrbssSyncDIT:Sync done successfully for namingctx:
cn=oraclecontext, 222 entries matched
2004/09/14:12:58:21 * gslrbssSyncDIT:Replicating namingcontext=cn=quan zhou ......
2004/09/14:12:58:23 * BootStrap failure when adding DN=cn=Quan
Zhou,server=dlsun1418_replica2,err=Constraint violation.
```

```
2004/09/14:12:58:23 * gslrbssSyncDIT:Sync failed for namingctx: cn=quan zhou, only 1
entries retrieved
2004/09/14:12:58:23 * gslrbssSyncDIT:Replicating namingcontext=cn=oracleschemaversion
......
2004/09/14:12:58:25 * gslrbssSyncDIT:Sync done successfully for namingctx:
cn=oracleschemaversion, 10 entries matched
2004/09/14:12:58:51 * gslrbsbBootStrap: Failure occured when bootstrapping 1 out of 3
namingcontext(s) from the supplier
```

ヒント： ブートストラップの障害のトラブルシューティングには 2 つのオプションがあります。

- オプション 1: ブートストラップの障害の原因を特定し、修正します。次に、コンシューマ・レプリカの `orclreplicastate` をブートストラップ・モードにして、ブートストラップを再起動します。
- オプション 2: ブートストラップに失敗したネーミング・コンテキストを特定し、`oidreconcile` を使用してこれらを調整します。次に、コンシューマ・レプリカの `orclreplicastate` をオンライン・モードにして、レプリケーションを再開します。

注意： このとき、`Oidrepld` は Bootstrap_error モードになっているので、コンシューマ・レプリカのレプリカ状態（`orclreplicastate`）をリセットする必要があります。

データベース・コピー・プロシージャを使用したディレクトリ・ノードの追加

この付録では、データベース・コピー・プロシージャを使用して、既存のレプリケート・システムに新規ノードを追加する方法について説明します。データベース・コピー・プロシージャはコールド・バックアップとも呼ばれます。このプロシージャは Oracle Internet Directory でのみ機能します。Oracle Application Server Certificate Authority や Oracle Application Server Single Sign-On など、その他の Oracle Identity Management コンポーネントがインストールされている場合は、このプロシージャを使用しないでください。Oracle Internet Directory ノードがスタンドアロンの場合は、データベース・コピー・プロシージャを使用して新しいディレクトリ・レプリケーション・グループを作成できます。

このプロシージャは、Oracle Database アドバンスト・レプリケーション・ベースのレプリカと、完全 LDAP ベース・レプリカにのみ適用できます。アドバンスト・レプリケーションの手順は、LDAP レプリケーションの手順と多少異なります。ノードを追加する際には、必ず Oracle Database アドバンスト・レプリケーション・ベースのレプリカ用の手順（「Oracle Database アドバンスト・レプリケーション・ベースのディレクトリ・ノードの追加」を参照）と完全 LDAP ベース・レプリカ用の手順（「LDAP レプリケーション・ベースのディレクトリ・ノードの追加」を参照）を使用してください。

この付録の項目は次のとおりです。

定義

スポンサ・サイトは、Oracle Internet Directory とそのリポジトリ（Oracle データベース）がインストールされているサイト、ホストまたはノードです。スポンサ・サイトはスポンサ・ノードとも呼ばれます。

新規サイトは、Oracle Internet Directory リポジトリのコピー先となるサイト、ホストまたはノードです。新規サイトは新規ノードとも呼ばれます。

前提条件

このプロシージャを開始するには、コンピューティング環境が次の前提条件を満たしている必要があります。

1. 新規ディレクトリ・サイトとスポンサ・ディレクトリ・サイトで、オペレーティング・システム、バージョンおよびパッチ・レベルが同じでなければなりません。オペレーティング・システムのパッチ・レベルが異なると、このプロシージャが機能しない場合があります。
2. このプロシージャを実行する前に、スポンサ・ディレクトリのリポジトリのバックアップを強くお薦めします。
3. このプロシージャでは Oracle データ・ファイルをコピーするので、使用しているネットワーク環境によってパフォーマンスが異なります。ネットワークの通信速度が遅い場合、第 30 章「Oracle Internet Directory レプリケーションのインストールと構成」で説明されている方法でレプリケーション・グループを設定した方が効率的になることがあります。または、圧縮した Oracle データ・ファイルをリムーバブル・メディアに保存し、物理的に移動する方法もあります。ネットワークについては、ローカルのシステム管理者またはネットワーク管理者に確認してください。
4. Oracle データベースをよく理解しているユーザーのみが、このプロシージャを実行してください。

スポンサ・ディレクトリ・サイトの環境

この付録の例は、スポンサ・ディレクトリ・サイトが次の環境であることを前提としています。

```
Hostname = rst-sun
Domain name = acme.com
ORACLE_BASE = /private/oracle/app/oracle
ORACLE_HOME = /private/oracle/app/oracle/product/OraHome_1
ORACLE_SID  = LDAP
LD_LIBRARY_PATH = $ORACLE_HOME/lib
NLS_LANG    = AMERICAN_AMERICA.AL32UTF8
datafile location = /private/oracle/oradata/LDAP
Dump destination =  /private/oracle/app/oracle/admin/LDAP/pfile,
                    /private/oracle/app/oracle/admin/LDAP/bdump,
                    /private/oracle/app/oracle/admin/LDAP/cdump,
                    /private/oracle/app/oracle/admin/LDAP/udump,
                    /private/oracle/app/oracle/admin/LDAP/create
```

新規ディレクトリ・サイトの環境

この付録の例は、新規ディレクトリ・サイトが次の環境であることを前提としています。

```
Hostname = dsm-sun
Domain name = acme.com
ORACLE_BASE = /private1/oracle/app/oracle
ORACLE_HOME = /private1/oracle/app/oracle/product/OraHome_1
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
```

新規ノードで実行する準備タスク

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. Oracle Universal Installer を使用して、Identity Managemen と Metadata Repository をインストールします。インストールする必要があるのは Oracle Internet Directory だけです。したがって、インストーラの「**構成オプションの選択**」画面で Oracle Internet Directory のみを選択します。インストール時に、ORACLE_SID を `NLDAP` に設定し、グローバル名を `NLDAP.ACME.COM` に設定します。

   関連資料： Oracle Application Server のインストレーション・ガイドの OracleAS Infrastructure のインストールに関する項
3. 次のコマンドを発行して、インストール固有のすべてのエントリをスポンサ・ディレクトリにコピーします。

   ```
   remtool -backupmetadata \
      -replica "new_node_host:new_node_port/new_node_repldn_pwd" \
      -master "sponsor_host:master_port/sponsor_repl_dn_pwd"
   ```

   sponsor_host、*sponsor_port* および *sponsor_repdn_pwd* は、それぞれスポンサ・ノードのホスト名、ポート番号およびレプリケーション識別名パスワードです。

   注意： Oracle Delegated Administration Services が構成されていない場合、`remtool` を `-backupmetadata` オプションを指定して実行すると、次のようなエラー・メッセージが表示されます。

   ```
   Failed to add "orclApplicationCommonName=ias.acme.com,
   cn=IAS Instances, cn=IAS, cn=Products, cn=OracleContext"
   as "uniquemember" to entry "cn=Associated Mid-tiers,
   orclapplicationcommonname=DASApp, cn=DAS,cn=products,
   cn=OracleContext at replica ldap://myhost:389
   ```

   このエラー・メッセージは無視してください。

   関連項目： 第 30 章「Oracle Internet Directory レプリケーションのインストールと構成」の 30-8 ページの「既存のマスターをリモート・マスター・サイトとして使用する場合」

Oracle Database アドバンスト・レプリケーション・ベースのディレクトリ・ノードの追加

この項では、アドバンスト・レプリケーション・ベースのディレクトリ・ノードの追加について説明します。この項の項目は次のとおりです。

スポンサ・アドバンスト・レプリケーション・ノードで実行するタスク

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 RESETLOGS;
   ```

   このコマンドを実行すると、ダンプ先ディレクトリの下にトレース・ファイルが作成されます。この例の場合、ダンプ先ディレクトリは `/private/oracle/app/oracle/admin/LDAP/udump` になります。

   トレース・ファイルは次の形式で作成されます。

   $ORACLE_SID_ora_processid.trc

   次に例を示します。

   ```
   ldap_ora_4765.trc
   ```

2. LDAP、レプリケーション・サーバーおよび OID モニターの各プロセスを停止します。LDAP とレプリケーション・サーバーを停止してから、OID モニター・プロセスを停止してください。

   ```
   $ oidctl connect=connect_string server=oidrepld instance=instance_number stop
   $ oidctl connect=connect_string server=oidldapd instance=instance_number stop
   $ oidmon connect=connect_string stop
   ```

   OIDMON および LDAP サーバー・プロセスは、opmn を使用して停止することもできます。必ず、レプリケーション・サーバー、ディレクトリ・サーバーおよび OIDMON を停止してから、次の手順に進んでください。

   これらのコマンドで、*connect_string* は、ノードの `tnsnames.ora` ファイルにあるネット・サービス名です。

3. ディレクトリ・レプリケーション・グループ（DRG）の他のノードで、LDAP レプリケーション・サーバーのみを停止します。

   ```
   $ oidctl connect=connect_string server=oidrepld instance=instance_number stop
   ```

   スポンサ・ノード以外のすべてのノードで、この手順を繰り返します。対応するノードに適したネット・サービス名を指定してください。

4. ノードを既存の DRG に追加する場合のみ、この手順を実行します。マスター定義サイト（MDS）で次のコマンドを実行して、Oracle Database アドバンスト・レプリケーションを静止させます。

   ```
   cd $ORACLE_HOME/ldap/admin
   ```

   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 repadmin/repadmin_password;
   SQL> @oidrsusp.sql
   ```

注意： この手順は、マスター定義サイトでのみ実行してください。

この時点では、他のノードの LDAP 編集のみが可能で、レプリケーションは行われません。

5. 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
$ sqlplus /nolog
SQL> connect /as sysdba
SQL> shutdown normal
SQL> exit
```

デフォルトのリスナー名は LISTENER です。

6. 手順 1 で作成したトレース・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・エディタで newdb.sql を編集し、STARTUP NOMOUNT 文と CREATE CONTROLFILE 文以外のすべての行を削除します。編集後の newdb.sql ファイルは次のようになります。

```
STARTUP NOMOUNT
CREATE CONTROLFILE REUSE SET DATABASE "LDAP" RESETLOGS  NOARCHIVELOG
    MAXLOGFILES 16
    MAXLOGMEMBERS 3
    MAXDATAFILES 100
    MAXINSTANCES 8
    MAXLOGHISTORY 454
LOGFILE
  GROUP 1 '/private/oracle/oradata/LDAP/redo01.log'  SIZE 10M,
  GROUP 2 '/private/oracle/oradata/LDAP/redo02.log'  SIZE 10M,
  GROUP 3 '/private/oracle/oradata/LDAP/redo03.log'  SIZE 10M
-- STANDBY LOGFILE
DATAFILE
  '/private/oracle/oradata/LDAP/system01.dbf',
  '/private/oracle/oradata/LDAP/sysaux01.dbf',
  '/private/oracle/oradata/LDAP/users01.dbf',
  '/private/oracle/oradata/LDAP/dcm.dbf',
  '/private/oracle/oradata/LDAP/portal.dbf',
  '/private/oracle/oradata/LDAP/ptldoc.dbf',
  '/private/oracle/oradata/LDAP/ptlidx.dbf',
  '/private/oracle/oradata/LDAP/ptllog.dbf',
  '/private/oracle/oradata/LDAP/oca.dbf',
  '/private/oracle/oradata/LDAP/discopltc1.dbf',
  '/private/oracle/oradata/LDAP/discopltm1.dbf',
  '/private/oracle/oradata/LDAP/oss_sys01.dbf',
  '/private/oracle/oradata/LDAP/wcrsys01.dbf',
  '/private/oracle/oradata/LDAP/uddisys01.dbf',
  '/private/oracle/oradata/LDAP/b2b_dt.dbf',
  '/private/oracle/oradata/LDAP/b2b_rt.dbf',
  '/private/oracle/oradata/LDAP/b2b_idx.dbf',
  '/private/oracle/oradata/LDAP/b2b_lob.dbf',
  '/private/oracle/oradata/LDAP/bam.dbf',
  '/private/oracle/oradata/LDAP/orabpel.dbf',
  '/private/oracle/oradata/LDAP/attrs1_oid.dbf',
  '/private/oracle/oradata/LDAP/battrs1_oid.dbf',
  '/private/oracle/oradata/LDAP/gcats1_oid.dbf',
  '/private/oracle/oradata/LDAP/gdefault1_oid.dbf',
  '/private/oracle/oradata/LDAP/svrmg1_oid.dbf',
  '/private/oracle/oradata/LDAP/ias_meta01.dbf',
```

```
  '/private/oracle/oradata/LDAP/undotbs.dbf'
CHARACTER SET AL32UTF8
;
```

8. サンプル・ファイル mod.ldif を、次のように編集します。

a. 次の行が変更対象の行です。

```
CREATE CONTROLFILE REUSE DATABASE "LDAP" RESETLOGS  NOARCHIVELOG
```

この行を次のように変更します。

```
CREATE CONTROLFILE REUSE SET DATABASE "NLDAP" RESETLOGS  NOARCHIVELOG
```

b. データベースとログ・ファイルの UNIX ディレクトリ位置を変更し、新規ノード・サイトのディレクトリを指し示すようにします。

この例では、newdb.sql を次のように変更します。

```
STARTUP NOMOUNT
CREATE CONTROLFILE REUSE SET DATABASE "NLDAP" RESETLOGS  NOARCHIVELOG
    MAXLOGFILES 16
    MAXLOGMEMBERS 3
    MAXDATAFILES 100
    MAXINSTANCES 8
    MAXLOGHISTORY 454
LOGFILE
  GROUP 1 '/private1/oracle/oradata/NLDAP/redo01.log'  SIZE 10M,
  GROUP 2 '/private1/oracle/oradata/NLDAP/redo02.log'  SIZE 10M,
  GROUP 3 '/private1/oracle/oradata/NLDAP/redo03.log'  SIZE 10M
-- STANDBY LOGFILE
DATAFILE
  '/private1/oracle/oradata/NLDAP/system01.dbf',
  '/private1/oracle/oradata/NLDAP/sysaux01.dbf',
  '/private1/oracle/oradata/NLDAP/users01.dbf',
  '/private1/oracle/oradata/NLDAP/dcm.dbf',
  '/private1/oracle/oradata/NLDAP/portal.dbf',
  '/private1/oracle/oradata/NLDAP/ptldoc.dbf',
  '/private1/oracle/oradata/NLDAP/ptlidx.dbf',
  '/private1/oracle/oradata/NLDAP/ptllog.dbf',
  '/private1/oracle/oradata/NLDAP/oca.dbf',
  '/private1/oracle/oradata/NLDAP/discopltc1.dbf',
  '/private1/oracle/oradata/NLDAP/discopltm1.dbf',
  '/private1/oracle/oradata/NLDAP/oss_sys01.dbf',
  '/private1/oracle/oradata/NLDAP/wcrsys01.dbf',
  '/private1/oracle/oradata/NLDAP/uddisys01.dbf',
  '/private1/oracle/oradata/NLDAP/b2b_dt.dbf',
  '/private1/oracle/oradata/NLDAP/b2b_rt.dbf',
  '/private1/oracle/oradata/NLDAP/b2b_idx.dbf',
  '/private1/oracle/oradata/NLDAP/b2b_lob.dbf',
  '/private1/oracle/oradata/NLDAP/bam.dbf',
  '/private1/oracle/oradata/NLDAP/orabpel.dbf',
  '/private1/oracle/oradata/NLDAP/attrs1_oid.dbf',
  '/private1/oracle/oradata/NLDAP/battrs1_oid.dbf',
  '/private1/oracle/oradata/NLDAP/gcats1_oid.dbf',
  '/private1/oracle/oradata/NLDAP/gdefault1_oid.dbf',
  '/private1/oracle/oradata/NLDAP/svrmg1_oid.dbf',
  '/private1/oracle/oradata/NLDAP/ias_meta01.dbf',
  '/private1/oracle/oradata/NLDAP/undotbs.dbf'
CHARACTER SET AL32UTF8
;
```

9. スポンサ・ディレクトリのデータベースの初期化パラメータ・ファイル init$ORACLE_SID.ora を init$ORACLE_SID_NEW_DIR_DB.ora にコピーします。初期化パラメータ・ファイルのデフォルトの場所は、UNIX の場合は $ORACLE_HOME/dbs、Windows の場合は %ORACLE_HOME%¥database です。ここでは、次に示すように、/private/oracle/app/oracle/product/OraHome_1/dbs/initLDAP.ora を /private/oracle/app/oracle/product/OraHome_1/dbs/initNLDAP.ora にコピーします。

```
$cd $ORACLE_HOME/dbs
$cp initLDAP.ora initNLDAP.ora
```

初期化パラメータ・ファイルのかわりにサーバー・パラメータ・ファイル spfile$ORACLE_SID.ora または spfile.ora を使用している場合は、次の例に示すように、サーバー・パラメータ・ファイルから初期化パラメータ・ファイルを作成します。

```
$sqlplus /nolog
SQL> connect / as sysdba
SQL> create pfile from spfile
```

前述の例は、spfile$ORACLE_SID.ora がデフォルトの場所 $ORACLE_HOME/dbs にあることを前提としています。この例の場合、前の手順を実行すると、spfileLDAP.ora から initLDAP.ora ファイルが作成され、/private/oracle/app/oracle/product/OraHome_1 に配置されます。サーバー・パラメータ・ファイルがデフォルトの場所にない場合は、次の例のように、完全なパスを指定する必要があります。

```
$sqlplus /nolog
SQL> connect / as sysdba
SQL> create pfile='/private/oracle/initLDAP.ora' from
 spfile=/private/oracle/initLDAP.ora
```

初期化パラメータ・ファイルを作成したら、この手順の最初に説明した方法でそのファイルのコピーを作成します。

10. 新しい初期化パラメータ・ファイルで、次の変更を行います。

a. JOB_QUEUE_PROCESSES パラメータをコメント化します。

b. dbname パラメータを LDAP から NLDAP に変更します。

c. 新規サイトのドメイン名がスポンサ・ディレクトリのドメイン名と異なる場合は、db_domain パラメータも変更します。

d. 次のパラメータの場所を変更して、新規サイトの場所を指し示すようにします。

```
background_dump_dest
core_dump_dest
user_dump_dest
control_files
db_recovery_file_dest
```

e. 手順 c に記載されているパラメータに加え、DB_RECOVERY_FILE_DEST や DB_CREATE_FILE_DEST など、ノード固有のパラメータが初期化パラメータ・ファイルに含まれている場合は、それらのパラメータも変更します。

この例の場合、変更後の初期化パラメータ・ファイル initNLDAP.ora は次のようになります。

```
*.aq_tm_processes=1
*.background_dump_dest='/private1/oracle/app/oracle/admin/NLDAP/bdump'
*.compatible='10.1.0.2.0'
*.control_files='/private1/oracle/app/oracle/admin/NLDAP/control01.ctl',
                '/private1/oracle/app/oracle/admin/NLDAP/control02.ctl',
'/private1/oracle/app/oracle/admin/NLDAP/control03.ctl'
*.core_dump_dest='/private1/oracle/app/oracle/admin/NLDAP/cdump'
*.db_block_size=8192
*.db_cache_size=50331648
*.db_domain='acme.com'
```

```
*.db_file_multiblock_read_count=16
*.db_name='NLDAP'
*.db_recovery_file_dest='/private/oracle1/app/oracle/flash_recovery_area'
*.db_recovery_file_dest_size=2147483648
*.dispatchers='(PROTOCOL=TCP)(PRE=oracle.aurora.server.GiopServer)',
              '(PROTOCOL=TCP)(PRE=oracle.aurora.server.SGiopServer)'
*.java_pool_size=67108864
#*.job_queue_processes=5
*.large_pool_size=8388608
*.max_commit_propagation_delay=0
*.open_cursors=300
*.pga_aggregate_target=33554432
*.processes=150
*.remote_login_passwordfile='EXCLUSIVE'
*.sessions=400
*.shared_pool_size=150994944
*.undo_management='AUTO'
*.undo_tablespace='UNDOTBS'
*.user_dump_dest='/private1/oracle/app/oracle/admin/NLDAP/udump'
```

11. tnsnames.ora ファイルを編集して、新規ノードの接続情報を追加します。次のサンプル・ファイルを参照してください。

```
LDAP.ACME.COM =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = rst-sun)(PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = ldap.acme.com)
    )
  )
NLDAP.ACME.COM =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = dsm-sun)(PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = nldap.acme.com)
    )
  )
```

12. listener.ora ファイルを list.bak にコピーします。コピーした list.bak ファイルを編集して、新規ノードに関する情報を追加します。次のサンプル・ファイルを参照してください。

```
# 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/OraHome_1)
      (SID_NAME = NLDAP)
    )
    (SID_DESC =
      (SID_NAME = extproc)
      (ORACLE_HOME = /private1/oracle/app/oracle/product/OraHome_1)
      (PROGRAM = extproc)
    )
```

```
  )
STARTUP_WAIT_TIME_LISTENER = 0
CONNECT_TIMEOUT_LISTENER = 10
TRACE_LEVEL_LISTENER = OFF
```

tnsnames.ora および listener.ora のデフォルトの場所は、UNIX の場合は $ORACLE_HOME/network/admin ディレクトリ、Windows の場合は ORACLE_HOME¥network¥admin ディレクトリです。次のいずれかの場所も指定できます。

- TNS_ADMIN 環境変数またはレジストリ値で指定されているディレクトリ。
- UNIX オペレーティング・システムでは、グローバル構成ディレクトリ。たとえば Solaris の場合、このディレクトリは /var/opt/oracle になります。

13. 更新した tnsnames.ora ファイルを他のノードにコピーします。他のノードにコピーするときは、FTP または別の適切な方法を使用できます。

tnsnames.ora ファイルを新規ノードにコピーする前に、その新規ノードに Oracle データベース・ソフトウェアをインストールしてください。さらに、list.bak ファイル、listener.ora ファイルおよび sqlnet.ora ファイルもスポンサ・ノードから新規ノードにコピーします。

14. 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。次に例を示します。

```
>> $ find / -name *.dbf -print \
        -exec tar rvf tar_file_name_with_absolute_path {} \;
```

注意： newdb.sql の DATAFILE の下に示されたファイルはすべて、アーカイブに保存する必要があります。

このコマンドを実行すると、ルート・ディレクトリから順に、拡張子 .dbf を持つすべてのファイルが検索されます。この場合、ノードにインストールされたデータベース・サーバーのインスタンスが 1 つだけあり、データ・ファイルの拡張子が .dbf であることが前提となります。

アーカイブ・ファイルを圧縮します。

```
>> $ compress  tar_file_name_with_absolute_path
```

ここに示した手順は、ファイルのバックアップ方法の一例にすぎません。この方法を使用すると、Oracle データ・ファイルが絶対パスでバックアップされます。カレント・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。これによって、データ・ファイルのリストア場所がより柔軟になります。データベースをバックアップする前に、システム管理者に確認してください。

新規アドバンスト・レプリケーション・ノードで実行するタスク

新規ノードで次の手順を実行します。

1. 新規ノードで、Application Server Control、DCM、opmn、データベースおよびリスナーの各サービスを停止します。

```
$> emctl stop iasconsole
$> $ORACLE_HOME/dcm/bin/dcmctl stop
$> $ORACLE_HOME/opmn/bin/opmnctl stopall
$> sqlplus "/ as sysdba"
SQL> shutdown immediate;
SQL> exit
$> lsnrctl [listener_name] stop
```

2. FTP または他の適切なツールを使用して、初期化パラメータ・ファイル `initNLDAP.ora` を、スポンサ・ノード（rst-sun）から新規ノードの UNIX ディレクトリ `$ORACLE_HOME/dbs` へコピーします。コピーを行った後、コピーした `initNLDAP.ora` ファイルのデータが破損していないことを確認してください。

3. `$ORACLE_HOME/dbs` ディレクトリ（UNIX）または `ORACLE_HOME¥database` ディレクトリ（Windows）に、次のファイルが存在しないことを確認します。

   - spfileNLDAP.ora
   - spfile.ora

   これらのファイルのいずれかが存在する場合、スポンサ・ノードからコピーした `initNLDAP.ora` ファイルではなく、そのファイルが使用されます。

4. スポンサ・ノードで実行した手順 14 ではアーカイブ・ファイルを作成しました。FTP またはその他の適切なツールを使用して、このアーカイブ・ファイルをコピーします。次の例では、FTP ツールを使用して rst-sun からアーカイブ・ファイルをコピーします。

```
$ ftp
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・ファイルのサイズが非常に大きく（数 GB または TB）、ネットワーク帯域幅が狭いときは、圧縮したファイルをテープやディスクなどのメディアに保存し、スポンサ・ノードから新規ノードへ物理的に移動した方が効率的な場合もあります。

   新規ノードでアーカイブ・ファイルを展開します。次に例を示します。

```
$ uncompress oradb.tar.Z
$ tar xvf oradb.tar
```

   データ・ファイルが正しいディレクトリに展開されたことを確認してください。この例では、/private1/oracle/oradata/NLDAP ディレクトリに展開します。

5. FTP またはその他の適切なツールを使用して、I-16 ページの「スポンサ LDAP レプリケーション・ノードで実行するタスク」の手順 5 で作成した `newdb.sql` ファイルをコピーします。次に例を示します。

```
$ cd /private1/oracle/app/oracle/admin/NLDAP/udump
$ ftp
ftp> open rst-sun
ftp> cd /private1/oracle/app/oracle/admin/LDAP/udump
ftp> mget newdb.sql
```

6. UNIX シェル・プロンプトで、ORACLE_BASE、ORACLE_HOME および ORACLE_SID の各環境変数を設定します。次に例を示します（C シェルを使用）。

```
$ setenv ORACLE_BASE /private1/oracle/app/oracle
$ setenv ORACLE_HOME /private1/oracle/app/oracle/product/OraHome_1
$ setenv ORACLE_SID NLDAP
```

7. 同じ UNIX シェルで、次の例に示すように、SQL*Plus を使用して newdb.sq を実行します。

```
$ sqlplus /nolog
SQL> connect /as sysdba
SQL> @newdb.sql
SQL> shutdown normal
SQL>exit
```

8. $ORACLE_HOME/dbs ディレクトリにある初期化パラメータ・ファイル initNLDAP.ora を編集して、コメント化された job_queue_processes パラメータを元に戻します。このパラメータの値は、ディレクトリ・レプリケーション・グループ内のノード数以上でなければなりません。

9. 次のように、データベースとリスナーを起動します。

```
$ sqlplus /nolog
SQL> connect /as sysdba
SQL> startup mount
SQL> alter database open resetlogs
SQL> exit
$ lsnrctl start
```

10. スポンサ・ノードにログインし、スポンサ・ノードでデータベースとリスナーを起動します。この例では、スポンサ・ノードは rst-sun です。

```
$ telnet rst-sun
$ sqlplus /nolog
SQL> connect /as sysdba
SQL> startup
SQL> exit
$ lsnrctl start
$ exit
```

11. 新規ノードのグローバル・データベース名を変更します。

```
SQL> connect /as sysdba
SQL> alter database rename global_name to NLDAP;
SQL> exit
```

12. 次のコマンドを使用して、一時ファイルを表領域に追加します。

```
SQL> connect /as sysdba
SQL> ALTER TABLESPACE TEMP ADD TEMPFILE 'temp01.dbf' size 2000k;
SQL> exit
```

13. 新規ノードで、Wallet ファイル oidpwdlldap1 と oidpwdr* を削除し、ODS パスワードをリセットします。

```
$ cd $ORACLE_HOME/ldap/admin
$ rm oidpwdlldap1 oidpwdr*
```

14. パスワードをリセットして、Oracle Internet Directory プロセスを起動します。

```
$ oidpasswd connect=nldap.acme.com create_wallet=true current_password=ods

$ oidmon connect=nldap.acme.com start
$ oidctl connect=nldap.acme.com server=oidldapd instance=1 start
```

15. 新規ノードで ReplicaID をリセットします。データベースをコピーすると、新規ノードのデータベースの replicaid は、スポンサ・ノードのデータベースの replicaid と同じになります。したがって、新規ノードの replicaid を置き換える必要があります。replicaid の新しい値は、*hostname*_sid の形式でなければなりません。*hostname* は、Oracle Internet Directory サーバーのリポジトリを実行する新規ノードのホスト名（ドメイン名なし）です。sid は、新規ノード・データベースの ORACLE_SID です。この例では、replicaid は dsm-sun_nldap です。replicaid のすべての文字が小文字であることを確認してください。replicaid の値をリセットするには、次の手順を実行します。

    a. chgrid.ldif ファイルを作成します。内容は次のとおりです。

    ```
    dn:
    changetype: modify
    replace: orclreplicaid
    orclreplicaid: dsm-sun_nldap
    ```

    b. ldapmodify ツールを使用して replicaid を変更します。

    ```
    $ $ORACLE_HOME/bin/ldapmodify -p port#_of_ldap_server -h new_node_hostname \
       -f chgrid.ldif
    ```

16. 新規ノードのレプリカ ID は手順 15 で変更されたので、新規ノードに相対的なレプリカ・エントリを次のように再作成する必要があります。

    ```
    $ remtool –pcleanup –bind "new_node_host:new_node_port/new_node_repl_pswd"
    ```

    remtool コマンドによりエラーが報告され、前の手順のレプリカ ID に対応するレプリカ・エントリがまだないため、入力を求められます。remtool は、その入力を使用して、エラーを修正します。たとえば、次のようになります。

    ```
    remtool -pcleanup -bind "new_node_host:new_node_port/new_node_repl_pswd"


    Error occurred while getting replication configuration information.

    This tool will try to rectify the problem if super user DN and password are
    provided.

    Do you want to continue? [y/n] : y


    Enter superuser DN                          : cn=orcladmin


    Enter superuser password                    :

    Enter new password of replication DN        :

    Reenter new password of replication DN      :

    DRG identified by replica ldap://new_node_host:new_node_port (new_replica_id) will
    be cleaned up.

    Do you want to continue? [y/n] : y


    ------------------------------------------------------------------------------

    ------------------------------------------------------------------------------

    Replica replica ldap://new_node_host:new_node_port (new_replica_id) has been
    cleaned up.
    ```

17. レプリカ・サブエントリの名前を変更したら、レプリカ・サブエントリの orclreplicauri 属性および orclreplicasecondaryuri 属性も変更します。orclreplicauri 属性と orclreplicasecondaryuri 属性には、新規ノードの LDAP サーバーの URI を追加する必要があります。次の手順を実行します。

    a. LDIF ファイル modsubentry.ldif を作成します。このファイルの内容は次のとおりです。

    ```
    dn: orclreplicaid=new_replicaid,
     cn=replication configuration
    changetype: modify
    replace: orclreplicauri
    #Use your host name and port number
    #where ldap server is listening
    orclreplicauri: ldap://dsum-sun:389/
    -
    replace:orclreplicasecondaryuri
    #Use your fully qualified host name and
    #the port number where ldap server is listening
    orclreplicasecondaryuri:
    ldap://dsum-sun.acme.com:389/
    -
    replace:orclreplicastate
    orclreplicastate: 6
    ```

    b. ldapmodify ツールを使用して、ディレクトリを次のように変更します。

    ```
    $ ldapmodify -p port#_of_ldap_server -h new_node_hostname -f modsubentry.ldif
    ```

    注意： リモート・マスター・サイトとして動作するノードで、構成エントリ orclreplicaid=*replicaid*,cn=replication configuration の orclreplicastate 属性を 6 に設定してください。前述の例は、新規ノードがリモート・マスター・サイトとなり、orclreplicastate 属性が 6 に設定されていることを前提としています。新規ノードをマスター定義サイトとして使用し、スポンサ・ノードをリモート・マスター・サイトとして使用する場合は、スポンサ・ノードで orclreplicastate 属性を 6 に設定してください。

18. 別のノードを使用して構成されたアドバンスト・レプリケーションを持つノードからデータベース・コピーを実行した場合、新規ノードで LDAP_REP レプリケーション・グループを削除する必要があります。これを行うには、次のコマンドを実行します。

    ```
    $> sqlplus  rep_admin_db_account_name/password@db_conn_str_of_new_node
    SQL> exec dbms_repcat.drop_master_repgroup( gname => 'LDAP_REP' )
    ```

19. Oracle Internet Directory プロセスを停止します。

    ```
    oidmon connect=connect_string stop
    ```

20. 新規ノードで、changelog 表をクリーンアップします。

    ```
    $ sqlplus /nolog
    SQL> connect ods/ods_password;
    SQL> truncate table ods.ods_chg_log;
    SQL> truncate table ods.ods_chg_stat;
    SQL> truncate table ods.asr_chg_log;
    ```

21. 新規ノードを既存の DRG に追加する場合、Oracle Database アドバンスト・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。

    ```
    $ remtool -addnode
    ```

    スポンサ・ノードと新規ノードで構成された新しい DRG を作成する場合、Oracle Database アドバンスト・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。

```
$ remtool -asrsetup
```

関連資料：『Oracle Identity Management ユーザー・リファレンス』の remtool コマンドライン・ツールのリファレンス

22. 新規ノードとスポンサ・ノードを含め、すべてのノードで Oracle Internet Directory と LDAP レプリケーション・サーバーを起動します。

注意： スポンサ・ノードには、データベース・コピー・プロシージャを実行する前に行った操作の変更ログが含まれる場合があります。これらの変更ログは、レプリケーション・サーバーを起動すると新規ノードに反映されます。ただし、新規データベース・コピー・ノードのディレクトリ・データがスポンサ・ノードのデータとすでに一致している場合は、反映に失敗します。その結果、これらの変更ログは、データベース・コピー・ノードの管理者操作キューに追加されます。

スポンサ・ノードと新規ノードで構成される新しい DRG を作成した場合、このエラーを回避するには、スポンサ・ノードで ods_chg_log 表を切り詰めます。その後、スポンサ・ノードで LDAP サーバーを起動してください。

新規ノードを既存の DRG に追加した場合は、スポンサ・ノードでこの表を切り詰めないでください。その場合、新規ノードの管理者操作キューに変更が追加されます。第 30 章の「手動でのレプリケーション・グループ内の競合の解消」の説明に従って管理者がキューをクリーンアップする必要があります。

---

23. $ORACLE_HOME/config/ias.properties ファイルで、OIDport パラメータと OIDsslport パラメータを更新します。その際、新規ノードのディレクトリ・サーバーが現在リスニングしている非 SSL ポートおよび SSL ポートを指定します。

```
[ComponentConfig]
...
[InstallData]
...
OIDhost=dsm-sun
OIDport=current_non_ssl_port_of_ldap_server
OIDsslport=current_ssl_port_of_ldap_server
...
FarmAdminSupported=FALSE
```

アドバンスト・レプリケーション・ベースのレプリカ・ノードの検証

SQL*Plus を使用して Oracle データベースにログインします。ユーザー名として ODS を指定し、パスワードの入力で ods を指定します。

ods_chg_stat 表を参照し、行が適切であるか、同一であるかをすべてのノードについて確認します。ods_chg_stat 表には *number_of_nodes* × *number_of_nodes* 行が含まれています。たとえば、Oracle Database アドバンスト・レプリケーション・ベースのレプリケーションに 2 つのノードが関係しており、さらに 3 つ目のノードを追加した場合、各ノードについて 9 行（3 × 3）が ods_chg_stat 表に追加されます。これらの行を次の表に示します。

サプライヤ	コンシューマ	変更番号
ノード 1	ノード 2	1
ノード 1	ノード 3	2
ノード 1	ノード 1	3
ノード 2	ノード 1	4
ノード 2	ノード 2	5
ノード 2	ノード 2	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である行には、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によって処理された最新の変更が含まれます。サプライヤ名とコンシューマ名が異なる行には、サプライヤから対象コンシューマに対してすでに処理されている最新の変更番号が含まれます。

ノード 3 は新規ノードなので、ノード 3 による変更はまだありません。したがって、ノード 3 をサプライヤとする変更番号はいずれも 0 です。

すべてのノードの行が同じになるまでに少し時間がかかる場合がありますが、この時間は長くても 2 ～ 3 分です。

LDAP レプリケーション・ベースのディレクトリ・ノードの追加

この項では、完全 LDAP レプリカ・ディレクトリ・ノードの追加について説明します。このノードに対する LDAP レプリケーションは、一方向または双方向のいずれかです。この項の項目は次のとおりです。

- スポンサ LDAP レプリケーション・ノードで実行するタスク
- 新規 LDAP レプリケーション・ノードで実行するタスク
- LDAP ベースのレプリカ・ノードの検証

スポンサ LDAP レプリケーション・ノードで実行するタスク

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 RESETLOGS;
   ```

   このコマンドを実行すると、ダンプ先ディレクトリの下にトレース・ファイルが作成されます。この例の場合、ダンプ先ディレクトリは /private/oracle/app/oracle/admin/LDAP/udump になります。

   トレース・ファイルは次の形式で作成されます。

   $ORACLE_SID_ora_processid.trc

   次に例を示します。

   ldap_ora_4765.trc

2. LDAP、レプリケーション・サーバーおよび OID モニターの各プロセスを停止します。LDAP とレプリケーション・サーバーを停止してから、OID モニター・プロセスを停止してください。

   ```
   $ oidctl connect=connect_string server=oidrepld instance=instance_number stop
   $ oidctl connect=connect_string server=oidldapd instance=instance_number stop
   $ oidmon connect=connect_string stop
   ```

   OIDMON および LDAP サーバー・プロセスは、opmn を使用して停止することもできます。必ず、レプリケーション・サーバー、ディレクトリ・サーバーおよび OIDMON を停止してから、次の手順に進んでください。

   これらのコマンドで、*connect_string* は、ノードの tnsnames.ora ファイルにあるネット・サービス名です。

3. REMOVE

4. 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
   $ sqlplus /nolog
   SQL> connect /as sysdba
   SQL> shutdown normal
   SQL> exit
   ```

   デフォルトのリスナー名は LISTENER です。

5. 手順 1 で作成したトレース・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
   ```

6. テキスト・エディタで newdb.sql を編集し、STARTUP NOMOUNT 文と CREATE CONTROLFILE 文以外のすべての行を削除します。編集後の newdb.sql ファイルは次のようになります。

   ```
   STARTUP NOMOUNT
   CREATE CONTROLFILE REUSE SET DATABASE "LDAP" RESETLOGS  NOARCHIVELOG
       MAXLOGFILES 16
       MAXLOGMEMBERS 3
       MAXDATAFILES 100
       MAXINSTANCES 8
       MAXLOGHISTORY 454
   LOGFILE
     GROUP 1 '/private/oracle/oradata/LDAP/redo01.log'  SIZE 10M,
     GROUP 2 '/private/oracle/oradata/LDAP/redo02.log'  SIZE 10M,
     GROUP 3 '/private/oracle/oradata/LDAP/redo03.log'  SIZE 10M
   ```

```
-- STANDBY LOGFILE
DATAFILE
  '/private/oracle/oradata/LDAP/system01.dbf',
  '/private/oracle/oradata/LDAP/sysaux01.dbf',
  '/private/oracle/oradata/LDAP/users01.dbf',
  '/private/oracle/oradata/LDAP/dcm.dbf',
  '/private/oracle/oradata/LDAP/portal.dbf',
  '/private/oracle/oradata/LDAP/ptldoc.dbf',
  '/private/oracle/oradata/LDAP/ptlidx.dbf',
  '/private/oracle/oradata/LDAP/ptllog.dbf',
  '/private/oracle/oradata/LDAP/oca.dbf',
  '/private/oracle/oradata/LDAP/discopltc1.dbf',
  '/private/oracle/oradata/LDAP/discopltm1.dbf',
  '/private/oracle/oradata/LDAP/oss_sys01.dbf',
  '/private/oracle/oradata/LDAP/wcrsys01.dbf',
  '/private/oracle/oradata/LDAP/uddisys01.dbf',
  '/private/oracle/oradata/LDAP/b2b_dt.dbf',
  '/private/oracle/oradata/LDAP/b2b_rt.dbf',
  '/private/oracle/oradata/LDAP/b2b_idx.dbf',
  '/private/oracle/oradata/LDAP/b2b_lob.dbf',
  '/private/oracle/oradata/LDAP/bam.dbf',
  '/private/oracle/oradata/LDAP/orabpel.dbf',
  '/private/oracle/oradata/LDAP/attrs1_oid.dbf',
  '/private/oracle/oradata/LDAP/battrs1_oid.dbf',
  '/private/oracle/oradata/LDAP/gcats1_oid.dbf',
  '/private/oracle/oradata/LDAP/gdefault1_oid.dbf',
  '/private/oracle/oradata/LDAP/svrmg1_oid.dbf',
  '/private/oracle/oradata/LDAP/ias_meta01.dbf',
  '/private/oracle/oradata/LDAP/undotbs.dbf'
CHARACTER SET AL32UTF8
;
```

7. newdb.sql を次のように変更します。

a. 次の行が変更対象の行です。

```
CREATE CONTROLFILE REUSE DATABASE "LDAP" RESETLOGS  NOARCHIVELOG
```

この行を次のように変更します。

```
CREATE CONTROLFILE REUSE SET DATABASE "NLDAP" RESETLOGS  NOARCHIVELOG
```

b. データベースとログ・ファイルの UNIX ディレクトリ位置を変更し、新規ノード・サイトのディレクトリを指し示すようにします。

この例では、newdb.sql を次のように変更します。

```
STARTUP NOMOUNT
CREATE CONTROLFILE REUSE SET DATABASE "NLDAP" RESETLOGS  NOARCHIVELOG
    MAXLOGFILES 16
    MAXLOGMEMBERS 3
    MAXDATAFILES 100
    MAXINSTANCES 8
    MAXLOGHISTORY 454
LOGFILE
  GROUP 1 '/private1/oracle/oradata/NLDAP/redo01.log'  SIZE 10M,
  GROUP 2 '/private1/oracle/oradata/NLDAP/redo02.log'  SIZE 10M,
  GROUP 3 '/private1/oracle/oradata/NLDAP/redo03.log'  SIZE 10M
-- STANDBY LOGFILE
DATAFILE
  '/private1/oracle/oradata/NLDAP/system01.dbf',
  '/private1/oracle/oradata/NLDAP/sysaux01.dbf',
  '/private1/oracle/oradata/NLDAP/users01.dbf',
  '/private1/oracle/oradata/NLDAP/dcm.dbf',
  '/private1/oracle/oradata/NLDAP/portal.dbf',
  '/private1/oracle/oradata/NLDAP/ptldoc.dbf',
```

```
  '/private1/oracle/oradata/NLDAP/ptlidx.dbf',
  '/private1/oracle/oradata/NLDAP/ptllog.dbf',
  '/private1/oracle/oradata/NLDAP/oca.dbf',
  '/private1/oracle/oradata/NLDAP/discopltc1.dbf',
  '/private1/oracle/oradata/NLDAP/discopltm1.dbf',
  '/private1/oracle/oradata/NLDAP/oss_sys01.dbf',
  '/private1/oracle/oradata/NLDAP/wcrsys01.dbf',
  '/private1/oracle/oradata/NLDAP/uddisys01.dbf',
  '/private1/oracle/oradata/NLDAP/b2b_dt.dbf',
  '/private1/oracle/oradata/NLDAP/b2b_rt.dbf',
  '/private1/oracle/oradata/NLDAP/b2b_idx.dbf',
  '/private1/oracle/oradata/NLDAP/b2b_lob.dbf',
  '/private1/oracle/oradata/NLDAP/bam.dbf',
  '/private1/oracle/oradata/NLDAP/orabpel.dbf',
  '/private1/oracle/oradata/NLDAP/attrs1_oid.dbf',
  '/private1/oracle/oradata/NLDAP/battrs1_oid.dbf',
  '/private1/oracle/oradata/NLDAP/gcats1_oid.dbf',
  '/private1/oracle/oradata/NLDAP/gdefault1_oid.dbf',
  '/private1/oracle/oradata/NLDAP/svrmg1_oid.dbf',
  '/private1/oracle/oradata/NLDAP/ias_meta01.dbf',
  '/private1/oracle/oradata/NLDAP/undotbs.dbf'
CHARACTER SET AL32UTF8
;
```

8. スポンサ・ディレクトリのデータベースの初期化パラメータ・ファイル init$ORACLE_SID.ora を init$ORACLE_SID_NEW_DIR_DB.ora にコピーします。初期化パラメータ・ファイルのデフォルトの場所は、UNIX の場合は $ORACLE_HOME/dbs、Windows の場合は %ORACLE_HOME%¥database です。ここでは、次に示すように、/private/oracle/app/oracle/product/OraHome_1/dbs/initLDAP.ora を /private/oracle/app/oracle/product/OraHome_1/dbs/initNLDAP.ora にコピーします。

   ```
   $cd $ORACLE_HOME/dbs
   $cp initLDAP.ora initNLDAP.ora
   ```

   初期化パラメータ・ファイルのかわりにサーバー・パラメータ・ファイル spfile$ORACLE_SID.ora または spfile.ora を使用している場合は、次の例に示すように、サーバー・パラメータ・ファイルから初期化パラメータ・ファイルを作成します。

   ```
   $sqlplus /nolog
   SQL> connect / as sysdba
   SQL> create pfile from spfile
   ```

   前述の例は、spfile$ORACLE_SID.ora がデフォルトの場所 $ORACLE_HOME/dbs にあることを前提としています。この例の場合、前の手順を実行すると、spfileLDAP.ora から initLDAP.ora ファイルが作成され、/private/oracle/app/oracle/product/OraHome_1 に配置されます。サーバー・パラメータ・ファイルがデフォルトの場所にない場合は、次の例のように、完全なパスを指定する必要があります。

   ```
   $sqlplus /nolog
   SQL> connect / as sysdba
   SQL> create pfile='/private/oracle/initLDAP.ora' from
    spfile=/private/oracle/initLDAP.ora
   ```

   初期化パラメータ・ファイルを作成したら、この手順の最初に説明した方法でそのファイルのコピーを作成します。

9. 新しい初期化パラメータ・ファイルで、次の変更を行います。

   a. dbname パラメータを LDAP から NLDAP に変更します。

   b. 新規サイトのドメイン名がスポンサ・ディレクトリのドメイン名と異なる場合は、db_domain パラメータも変更します。

c. 次のパラメータの場所を変更して、新規サイトの場所を指し示すようにします。

```
background_dump_dest
core_dump_dest
user_dump_dest
control_files
db_recovery_file_dest
```

d. 手順 c に記載されているパラメータに加え、DB_RECOVERY_FILE_DEST や DB_CREATE_FILE_DEST など、ノード固有のパラメータが初期化パラメータ・ファイルに含まれている場合は、それらのパラメータも変更します。

この例の場合、変更後の初期化パラメータ・ファイル initNLDAP.ora は次のようになります。

```
*.aq_tm_processes=1
*.background_dump_dest='/private1/oracle/app/oracle/admin/NLDAP/bdump'
*.compatible='10.1.0.2.0'
*.control_files='/private1/oracle/app/oracle/admin/NLDAP/control01.ctl',
                '/private1/oracle/app/oracle/admin/NLDAP/control02.ctl',
'/private1/oracle/app/oracle/admin/NLDAP/control03.ctl'
*.core_dump_dest='/private1/oracle/app/oracle/admin/NLDAP/cdump'
*.db_block_size=8192
*.db_cache_size=50331648
*.db_domain='acme.com'
*.db_file_multiblock_read_count=16
*.db_name='NLDAP'
*.db_recovery_file_dest='/private/oracle1/app/oracle/flash_recovery_area'
*.db_recovery_file_dest_size=2147483648
*.dispatchers='(PROTOCOL=TCP)(PRE=oracle.aurora.server.GiopServer)',
              '(PROTOCOL=TCP)(PRE=oracle.aurora.server.SGiopServer)'
*.java_pool_size=67108864
#*.job_queue_processes=5
*.large_pool_size=8388608
*.max_commit_propagation_delay=0
*.open_cursors=300
*.pga_aggregate_target=33554432
*.processes=150
*.remote_login_passwordfile='EXCLUSIVE'
*.sessions=400
*.shared_pool_size=150994944
*.undo_management='AUTO'
*.undo_tablespace='UNDOTBS'
*.user_dump_dest='/private1/oracle/app/oracle/admin/NLDAP/udump'
```

10. 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。次に例を示します。

```
>> $ find / -name *.dbf -print \
            -exec tar rvf tar_file_name_with_absolute_path {} \;
```

注意： newdb.sql の DATAFILE の下に示されたファイルはすべて、アーカイブに保存する必要があります。

このコマンドを実行すると、ルート・ディレクトリから順に、拡張子 .dbf を持つすべてのファイルが検索されます。この場合、ノードにインストールされたデータベース・サーバーのインスタンスが 1 つだけあり、データ・ファイルの拡張子が .dbf であることが前提となります。

アーカイブ・ファイルを圧縮します。

```
>> $ compress  tar_file_name_with_absolute_path
```

ここに示した手順は、ファイルのバックアップ方法の一例にすぎません。この方法を使用すると、Oracle データ・ファイルが絶対パスでバックアップされます。カレント・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。これによって、データ・ファイルのリストア場所がより柔軟になります。データベースをバックアップする前に、システム管理者に確認してください。

新規 LDAP レプリケーション・ノードで実行するタスク

新規ノードで次の手順を実行します。

1. 新規ノードで、Application Server Control、DCM、opmn、データベースおよびリスナーの各サービスを停止します。

```
$> emctl stop iasconsole
$> $ORACLE_HOME/dcm/bin/dcmctl stop
$> $ORACLE_HOME/opmn/bin/opmnctl stopall
$> sqlplus "/ as sysdba"
SQL> shutdown immediate;
SQL> exit
$> lsnrctl [listener_name] stop
```

2. FTP または他の適切なツールを使用して、初期化パラメータ・ファイル `initNLDAP.ora` を、スポンサ・ノード（rst-sun）から新規ノードの UNIX ディレクトリ `$ORACLE_HOME/dbs` へコピーします。コピーを行った後、コピーした `initNLDAP.ora` ファイルのデータが破損していないことを確認してください。

3. `$ORACLE_HOME/dbs` ディレクトリ（UNIX）または `ORACLE_HOME¥database` ディレクトリ（Windows）に、次のファイルが存在しないことを確認します。

   - spfileNLDAP.ora
   - spfile.ora

   これらのファイルのいずれかが存在する場合、スポンサ・ノードからコピーした `initNLDAP.ora` ファイルではなく、そのファイルが使用されます。

4. スポンサ・ノードで実行した手順 14 ではアーカイブ・ファイルを作成しました。FTP またはその他の適切なツールを使用して、このアーカイブ・ファイルをコピーします。次の例では、FTP ツールを使用して rst_sun からアーカイブ・ファイルをコピーします。

```
$ ftp
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・ファイルのサイズが非常に大きく（数 GB または TB）、ネットワーク帯域幅が狭いときは、圧縮したファイルをテープやディスクなどのメディアに保存し、スポンサ・ノードから新規ノードへ物理的に移動した方が効率的な場合もあります。

   新規ノードでアーカイブ・ファイルを展開します。次に例を示します。

```
$ uncompress oradb.tar.Z
$ tar xvf oradb.tar
```

   データ・ファイルが正しいディレクトリに展開されたことを確認してください。この例では、/private1/oracle/oradata/NLDAP ディレクトリに展開します。

5. FTP またはその他の適切なツールを使用して、I-16 ページの「スポンサ LDAP レプリケーション・ノードで実行するタスク」の手順 5 で作成した newdb.sql ファイルをコピーします。次に例を示します。

```
$ cd /private1/oracle/app/oracle/admin/NLDAP/udump
$ ftp
ftp> open rst-sun
ftp> cd /private1/oracle/app/oracle/admin/LDAP/udump
ftp> mget newdb.sql
```

6. UNIX シェル・プロンプトで、ORACLE_BASE、ORACLE_HOME および ORACLE_SID の各環境変数を設定します。次に例を示します（C シェルを使用）。

```
$ setenv ORACLE_BASE /private1/oracle/app/oracle
$ setenv ORACLE_HOME /private1/oracle/app/oracle/product/OraHome_1
$ setenv ORACLE_SID NLDAP
```

7. 同じ UNIX シェルで、次の例に示すように、SQL*Plus を使用して newdb.sq を実行します。

```
$ sqlplus /nolog
SQL> connect /as sysdba
SQL> @newdb.sql
SQL> shutdown normal
SQL>exit
```

8. $ORACLE_HOME/dbs ディレクトリにある初期化パラメータ・ファイル initNLDAP.ora を編集して、コメント化された job_queue_processes パラメータを元に戻します。このパラメータの値は、ディレクトリ・レプリケーション・グループ内のノード数以上でなければなりません。

9. 次のように、データベースとリスナーを起動します。

```
$ sqlplus /nolog
SQL> connect /as sysdba
SQL> startup mount
SQL> alter database open resetlogs
SQL> exit
$ lsnrctl start
```

10. スポンサ・ノードにログインし、スポンサ・ノードでデータベースとリスナーを起動します。この例では、スポンサ・ノードは rst-sun です。

```
$ telnet rst-sun
$ sqlplus /nolog
SQL> connect /as sysdba
SQL> startup
SQL> exit
$ lsnrctl start
$ exit
```

11. 新規ノードのグローバル・データベース名を変更します。

```
SQL> connect /as sysdba
SQL> alter database rename global_name to NLDAP;
SQL> exit
```

12. 次のコマンドを使用して、一時ファイルを表領域に追加します。

```
SQL> connect /as sysdba
SQL> ALTER TABLESPACE TEMP ADD TEMPFILE 'temp01.dbf' size 2000k;
SQL> exit
```

13. 新規ノードで、Wallet ファイル oidpwdlldap1 と oidpwdr* を削除し、ODS パスワードをリセットします。

```
$ cd $ORACLE_HOME/ldap/admin
$ rm oidpwdlldap1 oidpwdr*
```

14. パスワードをリセットして、Oracle Internet Directory プロセスを起動します。

```
$ oidpasswd connect=nldap.acme.com create_wallet=true current_password=ods

$ oidmon connect=nldap.acme.com start
$ oidctl connect=nldap.acme.com server=oidldapd instance=1 start
```

15. 新規ノードで ReplicaID をリセットします。データベースをコピーすると、新規ノードのデータベースの `replicaid` は、スポンサ・ノードのデータベースの `replicaid` と同じになります。したがって、新規ノードの `replicaid` を置き換える必要があります。`replicaid` の新しい値は、*hostname*_sid の形式でなければなりません。*hostname* は、Oracle Internet Directory サーバーのリポジトリを実行する新規ノードのホスト名（ドメイン名なし）です。`sid` は、新規ノード・データベースの ORACLE_SID です。この例では、replicaid は dsm-sun_nldap です。replicaid のすべての文字が小文字であることを確認してください。replicaid の値をリセットするには、次の手順を実行します。

a. `chgrid.ldif` ファイルを作成します。内容は次のとおりです。

```
dn:
changetype: modify
replace: orclreplicaid
orclreplicaid: dsm-sun_nldap
```

b. `ldapmodify` ツールを使用して replicaid を変更します。

```
$ $ORACLE_HOME/bin/ldapmodify -p port#_of_ldap_server -h new_node_hostname \
   -f chgrid.ldif
```

16. 新規ノードのレプリカ ID は手順 15 で変更されたので、新規ノードに相対的なレプリカ・エントリを次のように再作成する必要があります。

```
$ remtool –pcleanup –bind "new_node_host:new_node_port/new_node_repl_pswd"
```

remtool コマンドによりエラーが報告され、前の手順のレプリカ ID に対応するレプリカ・エントリがまだないため、入力を求められます。remtool は、その入力を使用して、エラーを修正します。たとえば、次のようになります。

```
remtool -pcleanup -bind "new_node_host:new_node_port/new_node_repl_pswd"


Error occurred while getting replication configuration information.

This tool will try to rectify the problem if super user DN and password are
provided.

Do you want to continue? [y/n] : y


Enter superuser DN                          : cn=orcladmin


Enter superuser password                    :

Enter new password of replication DN        :

Reenter new password of replication DN      :

DRG identified by replica ldap://new_node_host:new_node_port (new_replica_id) will
be cleaned up.

Do you want to continue? [y/n] : y


--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
```

```
Replica replica ldap://new_node_host:new_node_port (new_replica_id) has been
cleaned up.
```

17. レプリカ・サブエントリの名前を変更したら、レプリカ・サブエントリの orclreplicauri 属性、orclreplicasecondaryuri 属性、orclreplicastate 属性も変更します。orclreplicauri 属性と orclreplicasecondaryuri 属性には、新規ノードの LDAP サーバーの URI を追加する必要があります。orclreplicastate 属性は 6 に設定します。remtool はこの属性を使用して、データベース・コピー・ベースの addnode であることを識別します。この属性値を変更するには、次の手順を実行します。

    a. LDIF ファイル modsubentry.ldif を作成します。このファイルの内容は次のとおりです。

    ```
    dn: orclreplicaid=new_replicaid,
     cn=replication configuration
    changetype: modify
    replace: orclreplicauri
    #Use your host name and port number
    #where ldap server is listening
    orclreplicauri: ldap://dsum-sun:389/
    -
    replace:orclreplicasecondaryuri
    #Use your fully qualified host name and
    #the port number where ldap server is listening
    orclreplicasecondaryuri:
    ldap://dsum-sun.acme.com:389/
    ```

    b. ldapmodify ツールを使用して、ディレクトリを次のように変更します。

    ```
    $ ldapmodify -p port#_of_ldap_server -h new_node_hostname -f modsubentry.ldif
    ```

18. 別のノードを使用して構成されたアドバンスト・レプリケーションを持つノードからデータベース・コピーを実行した場合、新規ノードで LDAP_REP レプリケーション・グループを削除する必要があります。これを行うには、次のコマンドを実行します。

    ```
    sqlplus  rep_admin_db_account_name/password
    SQL> exec dbms_repcat.drop_master_repgroup( gname => 'LDAP_REP' )
    ```

19. Oracle Internet Directory プロセスを停止します。

    ```
    oidmon connect=connect_string stop
    ```

20. 新規ノードで、changelog 表をクリーンアップします。

    ```
    $ sqlplus /nolog
    SQL> connect ods/ods_password;
    SQL> truncate table ods.ods_chg_log;
    SQL> truncate table ods.ods_chg_stat;
    SQL> truncate table ods.asr_chg_log;
    ```

21. LDAP レプリケーションを構成し、完全レプリカをファンアウトとして次のように追加します。

    a. データベースと Oracle Internet Directory サーバーがスポンサ・ノードで実行されていることを確認します。スポンサ・ノードで、次のように入力します。

    ```
    $ sqlplus /nolog
    SQL> connect /as sysdba
    SQL> startup
    SQL> exit
    $ lsnrctl start

    $ oidmon connect=sponor_connect_string start
    $ oidctl server=oidldapd inst=1 connect=sponsor_connect_string flags="-p
    sponsor_node_port " start
    ```

b. Oracle Internet Directory サーバーがスポンサ・ノードで実行されていることを確認します。新規ノードで、次のように入力します。

```
$ oidmon connect=new_connect_string start
$ oidctl server=oidldapd inst=1 connect=new_connect_string flags="p
new_node_port " start
```

c. remtool を使用して、LDAP ベース・レプリケーションを次のように構成します。

```
remtool -paddnode
```

関連資料：『Oracle Identity Management ユーザー・リファレンス』の remtool コマンドライン・ツールのリファレンス

22. 新規レプリケーション承諾のレプリケーション変更ステータスを初期化します。

a. スポンサ・ノードから、最大の使用済変更番号を取得します。

```
$ ldapsearch -h sponsor_node_host  -p sponor_node_port -b " " \
   -s base "objectclass=*" lastchangenumber
```

b. LDIF ファイル chgstatus.ldif を作成します。このファイルの内容は次のとおりです。

```
dn: orclagreementid=new_agreement_id,
orclreplicaid=new_replica_id,cn=replication configuration
changetype:modify
replace: orcllastappliedchangenumber
orcllastappliedchangenumber: Number_from_step_a
```

c. dapmodify を使用して、スポンサ・ノードと新規ノードの両方に変更を適用します。

```
ldapmodify -p sponsor_node_port -h sponsor_node_host -v -f chgstatus.ldif
ldapmodify -p new_node_port -h new_node_host -v -f chgstatus.ldif
```

23. 全ノードで、Oracle Internet Directory と LDAP レプリケーション・サーバーを起動します。一方向レプリケーションの場合は、コンシューマ・ノードでのみレプリケーションを開始します。

注意： スポンサ・ノードには、データベース・コピー・プロシージャを実行する前に行った操作の変更ログが含まれる場合があります。これらの変更ログは、レプリケーション・サーバーを起動すると新規ノードに反映されます。ただし、新規データベース・コピー・ノードのディレクトリ・データがスポンサ・ノードのデータとすでに一致している場合は、反映に失敗します。その結果、これらの変更ログは、データベース・コピー・ノードの管理者操作キューに追加されます。

スポンサ・ノードと新規ノードで構成される新しい DRG を作成した場合、このエラーを回避するには、スポンサ・ノードで ods_chg_log 表を切り詰めます。その後、スポンサ・ノードで LDAP サーバーを起動してください。

新規ノードを既存の DRG に追加した場合は、スポンサ・ノードでこの表を切り詰めないでください。その場合、新規ノードの管理者操作キューに変更が追加されます。第 30 章の「手動でのレプリケーション・グループ内の競合の解消」の説明に従って管理者がキューをクリーンアップする必要があります。

---

24. $ORACLE_HOME/config/ias.properties ファイルで、OIDport パラメータと OIDsslport パラメータを更新します。その際、新規ノードのディレクトリ・サーバーが現在リスニングしている非 SSL ポートおよび SSL ポートを指定します。

```
[ComponentConfig]
...
[InstallData]
...
OIDhost=dsm-sun
```

```
OIDport=current_non_ssl_port_of_ldap_server
OIDsslport=current_ssl_port_of_ldap_server
...
FarmAdminSupported=FALSE
```

LDAP ベースのレプリカ・ノードの検証

Oracle Directory Manager を使用して、ディレクトリ・レプリケーション・サーバーが実行されていることを確認した後、次の手順を実行してディレクトリ・レプリケーションをテストします。

1. Oracle Directory Manager に `orcladmin` でログインします。
2. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「< ディレクトリ・サーバー・インスタンス >」、「**エントリ管理**」の順に展開します。
3. スポンサ・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、コンシューマ・ノードに約 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。

J

Oracle Internet Directory を使用した UNIX 認証およびユーザー・プロビジョニング

Oracle Internet Directory を中央ディレクトリとして、UNIX または Linux 環境でのユーザー認証および認可のために使用できます。これには次のような利点があります。

- Oracle Internet Directory が従来の `/etc/passwd` ファイルまたは Network Information System（NIS）や Yellow Pages（YP）の役割を果す。
- パスワード・ポリシーの強化が容易になる。
- ユーザーを複数の権限グループに分類し、使用しているサーバーやサービスに応じて、異なる権限で管理できる。

Oracle ホワイト・ペーパー『Centralizing UNIX Authentication and User Provisioning with Oracle Internet Directory』では、このソリューションを実行するために必要な手順を詳細に説明しています。このドキュメントでは、Oracle Internet Directory のプラッガブル認証モジュール（PAM）との使用に関するほぼ完全な情報が提供されています。ただし、ホワイト・ペーパーに加えて、この付録も読む必要があります。この付録の項目は次のとおりです。

スキーマのカスタマイズ

10*g* リリース 2（10.1.2）以降のリリースでは、ホワイト・ペーパーで説明されているように、スキーマをカスタマイズする必要はありません。必要な属性やオブジェクト・クラスは、標準の Oracle Internet Directory で使用可能です。例外として考えられるのは、カスタマイズされたログイン属性です。カスタム・ログイン属性は、次の項で説明するように、スキーマへの追加が必要になる場合があります。

UID 属性の問題

デフォルトでは、OracleAS Portal などの Oracle 製品では、Oracle Internet Directory の `uid` 属性を認証および認可に使用します。また、デフォルトで、UNIX ベースのオペレーティング・システムや PAM は、`uid` 属性を認証および認可に使用します。残念ながら、Oracle と UNIX では、使用できる `uid` 文字列の要件が異なります。たとえば、メール・アドレス *`user@address`* は、Oracle Internet Directory では `uid` の一般的な書式です。しかし、UNIX では、`uid` に `@` 文字を使用できません。この違いを対処するには、2 つの方法があります。

- PAM 認証および認可にカスタム・ログイン属性を使用します。これには、PAM への変更の他に、Oracle Internet Directory スキーマに対する変更も必要です。詳細は、Oracle ホワイト・ペーパー『Centralizing UNIX Authentication and User Provisioning with Oracle Internet Directory』を参照してください。

  関連項目： 11-10 ページの「ディレクトリの属性」

- Oracle Internet Directory の `uid` 属性を UNIX と使用しますが、電子メール・アドレスには、別の書式を選択します。たとえば、`jsmith` のような短いユーザー名を使用できます。

K

Oracle Internet Directory でサポートされている RFC

表 K-1 は、Oracle Internet Directory でサポートされている RFC のリストです。

表 K-1 サポートされている RFC

番号	タイトル
RFC 1274	The COSINE and Internet X.500 Schema
RFC 1488	The X.500 String Representation of Standard Attribute Syntaxes
RFC 1777	Lightweight Directory Access Protocol
RFC 1778	The String Representation of Standard Attribute Syntaxes
RFC 1779	A String Representation of Distinguished Names
RFC 1960	A String Representation of LDAP Search Filters
RFC 2079	Definition of an X.500 Attribute Type and an Object Class to Hold Uniform Resource Identifiers (URIs)
RFC 2247	Using Domains in LDAP/X.500 Distinguished Names
RFC 2251	Lightweight Directory Access Protocol (v3)
RFC 2252	Lightweight Directory Access Protocol (v3) Attribute Syntax Definitions
RFC 2253	Lightweight Directory Access Protocol (v3) UTF-8 String Representation of Distinguished Names
RFC 2254	The String Representation of LDAP Search Filters
RFC 2255	The LDAP URL Format
RFC 2256	A summary of the X500 (96) User Schema for use with LDAPv3
RFC 2307	An Approach for Using LDAP as a Network Information Service
RFC 2377	Naming Plan for Internet Directory-Enabled Applications
RFC 2396	Uniform Resource Identifiers (URI): Generic Syntax
RFC 2596	Use of Language Codes in LDAP
RFC 2696	LDAP Control Extension for Simple Paged Results Manipulation
RFC 2713	Schema for Representing Java(tm) Objects in an LDAP Directory
RFC 2798	Definition of the inetOrgPerson LDAP Object Class
RFC 2829	Authentication Methods for LDAP
RFC 2830	Lightweight Directory Access Protocol（v3）: Extension for Transport Layer Security
RFC 2849	The LDAP Data Interchange Format（LDIF）- Technical Specification

表 K-1 サポートされている RFC（続き）

番号	タイトル
RFC 2891	LDAP Control Extension for Server Side Sorting of Search Results
RFC 3112	LDAP Authentication Password Schema
RFC 3296	Named Subordinate References in Lightweight Directory Access Protocol（LDAP）Directories
RFC 3377	Core LDAP Requirements
RFC 3671	Collective Attributes in the Lightweight Directory Access Protocol（LDAP）

関連資料： Internet Engineering Task Force のホームページ（`http://www.ietf.org/`）

L

Oracle Internet Directory に関する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。この付録の項目は次のとおりです。

問題と解決方法

この項では、Oracle Internet Directory の一般的なエラー・メッセージ、問題点および解決方法について説明します。この項の項目は次のとおりです。

インストール時のエラー

Oracle Database のインストール時および構成時には、マルチバイト・キャラクタに伴う問題を回避するため、キャラクタ・セット UTF-8 を選択することをお薦めします。

TCP/IP の問題

オペレーティング・システムの TCP/IP の不具合によって、Oracle Internet Directory サービスに影響が及ぶ場合があります。

Microsoft Windows 2003 Server 上で Oracle Internet Directory サーバーの可用性を監視するときは TCP ベースの監視を使用しない

『Oracle Application Server 高可用性ガイド』において Oracle Application Server Cluster（Identity Management）のロード・バランサの構成に関する項で説明されているように、F5 ロード・バランサを使用して Oracle Internet Directory サーバーの可用性を監視する場合は、LDAP または HTTP ベースの監視を使用するようにロード・バランサを構成してください。TCP ベースの監視を使用すると、Windows 2003 Server のオペレーティング・システムの不具合によりサービスを使用できなくなる場合があります。

DaimondCS Port Explorer をインストールしない

システムに DaimondCS Port Explorer がインストールされていると、Oracle Internet Directory は動作しません。

ディレクトリ・サーバーのエラー・メッセージとその原因

この項では、発生する可能性のある Oracle ディレクトリ・サーバーのすべてのエラー・メッセージを示します。各メッセージに続いて、そのエラーに関して最も可能性の高い原因が記述されています。

クライアント接続の中断が原因の Oracle データベース・サーバー・エラー

エラー `sgslunrRead` または `30SendPort` が表示されます。

問題

これらのエラーは、LDAP クライアントの接続が突然切断されたことを示しています。

考えられる原因は次のとおりです。

- クライアント・プログラムが、バインド解除や中止を実行せずに、接続を終了した。

  クライアントのマシンが停止した。
- ネットワークのコンポーネント（ロード・バランサやファイアウォールなど）が、構成されたタイムアウト設定が原因で接続を切断した。
- ネットワークが停止中。

解決方法

これらのエラーは、サーバー外部の状況が原因です。必要な場合は、ネットワーク管理者に報告してください。

スキーマ変更が原因の Oracle データベース・サーバー・エラー

エラー `ORA-1562` が表示されます。

問題

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。

解決方法

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。

ユーザーまたはグループを編集したか、レルムを作成したことが原因の制約違反エラー

`oidldap*.log` に次のエラーが記録されます。

```
ORA-01483: invalid length for DATE or NUMBER bind variable.
```

次のエラーも画面に表示される場合があります。

```
LDAP: error code 19 - Constraint Violation
```

これらのエラーは断続的に発生する場合があります。

問題

AL32UTF8 キャラクタ・セットを使用する Oracle 10*g* Database に OracleAS Metadata Repository をロードした場合、ユーザーやグループを編集しようとしたり、Oracle Internet Directory に ID 管理レルムを作成しようとしたりすると、エラーが発生することがあります。ユーザーの編集には、既存ユーザーの属性を編集する作業も含まれます。

解決方法

しばらくしてから、ユーザーをもう一度編集してください。

Oracle ディレクトリ・サーバーから戻される標準エラー・メッセージ

表 L-1 は、標準的なエラー・メッセージとその原因を示しています。Oracle Internet Directory ではその他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、L-5 ページの「ディレクトリ・サーバーのその他のエラー・メッセージ」を参照してください。

表 L-1 標準のエラー・メッセージ

エラー	原因
00: LDAP_SUCCESS	操作が正常に完了しました。
01: LDAP_OPERATIONS_ERROR	リクエストの処理時に、サーバーで一般的なエラーが発生しました。
02: LDAP_PROTOCOL_ERROR	クライアント・リクエストが、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、受信したリクエスト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リクエストまたは変更リクエストで、値が指定されていない場合。SSL 資格証明の読取りでエラーが発生した場合。変更操作で指定されたタイプが不明な場合（LDAP_MOD_ADD、LDAP_MOD_DELETE および LDAP_MOD_REPLACE 以外）。検索範囲が不明な場合。
03: LDAP_TIMELIMIT_EXCEEDED	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: LDAP_SIZELIMIT_EXCEEDED	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 1000 が使用されます。
05: LDAP_COMPARE_FALSE	指定した値は、エントリ内の値と同一ではありません。
06: LDAP_COMPARE_TRUE	指定した値は、エントリ内の値と同一です。
07: LDAP_STRONG_AUTH_NOT_SUPPORTED	リクエストしたバインド方法がサーバーでサポートされていません。たとえば、SASL クライアントが Oracle Internet Directory による Kerberos 認証をリクエストすると、このエラーを受け取ります。
09: LDAP_PARTIAL_RESULTS	サーバーから参照が戻されました。
10: LDAP_REFERRAL	サーバーから参照が戻されました。
12: LDAP_UNAVAILABLE_CRITICALEXTENSION	指定したリクエストはサポートされていません。
16: LDAP_NO_SUCH_ATTRIBUTE	リクエスト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: LDAP_UNDEFINED_TYPE	指定した属性の型が、スキーマ内で定義されていません。
19: LDAP_CONSTRAINT_VIOLATION	リクエスト内の値が、特定の制約に違反しています。
20: LDAP_TYPE_OR_VALUE_EXISTS	属性に指定した値が重複しています。
21: LDAP_INVALID_SYNTAX	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: LDAP_NO_SUCH_OBJECT	操作用に指定したベースが存在していません。
34: LDAP_INVALID_DN_SYNTAX	識別名構文にエラーがあります。
49: LDAP_INVALID_CREDENTIALS	資格証明が正しくないため、バインドに失敗しました。
50: LDAP_INSUFFICIENT_ACCESS	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。

表 L-1 標準のエラー・メッセージ（続き）

エラー	原因
53: LDAP_UNWILLING_TO_PERFORM	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。
65: LDAP_OBJECT_CLASS_VIOLATION	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: LDAP_NOT_ALLOWED_ON_NONLEAF	削除対象のエントリに子エントリがあります。
67: LDAP_NOT_ALLOWED_ON_RDN	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: LDAP_ALREADY_EXISTS	追加条件が重複しています。
81: LDAP_SERVER_DOWN	ディレクトリ・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: LDAP_LOCAL_ERROR	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: LDAP_ENCODING_ERROR	クライアントで、リクエスト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: LDAP_DECODING_ERROR	クライアントで、リクエスト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: LDAP_TIMEOUT	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: LDAP_AUTH_UNKNOWN	認証方式が、クライアントの SDK で理解されません。
87: LDAP_FILTER_ERROR	検索フィルタが正しくありません。
88: LDAP_USER_CANCELLED	ユーザーが操作を取り消しました。
89: LDAP_PARAM_ERROR	LDAP ルーチンに対するパラメータが正しくありません。
90: LDAP_NO_MEMORY	メモリー不足です。

ディレクトリ・サーバーのその他のエラー・メッセージ

表 L-2 に、ディレクトリ・サーバーのその他のエラー・メッセージとその原因を示します。これらのメッセージには、エラー・コードは表示されません。

後述のメッセージの一部で使用されているパラメータ・タグは、Oracle Internet Directory アプリケーションによって、対応する実行時の値に置換されます。

表 L-2 その他のエラー・メッセージ

エラー	原因
(string には文字列が入ります) string 属性が見つかりません。	特定の属性の型が、スキーマに定義されていません。
< パラメータ > が属性 < パラメータ > に見つかりません。	値がその属性に見つかりません。(ldapmodify)
オブジェクト・クラス < パラメータ > のスキーマ情報が管理ドメインに含まれていません。	リクエストで指定したオブジェクト・クラスが、スキーマに存在していません。
クラスの追加に使用した OID< パラメータ > は別のクラスで使用されています。	指定したオブジェクト識別子が重複しています。(スキーマ変更)
属性 < パラメータ > はすでに使用されています。	属性名が重複しています。(スキーマ変更)

表 L-2 その他のエラー・メッセージ（続き）

エラー	原因
属性 < パラメータ > に構文エラーがあります。	属性名の定義に構文エラーがあります。（スキーマ変更）
属性 < パラメータ > はスキーマでサポートされていません。	属性が定義されていません。（すべての操作）
属性 < パラメータ > は単一の値です。	属性は単一値です。（ldapadd および ldapmodify）
属性 < パラメータ > がエントリに存在していません。	エントリに、この属性は存在していません。（ldapmodify）
属性の定義が正しくありません。	属性の定義に構文エラーがあります。（スキーマ変更）
現在はサポートされていません。	このバージョンの LDAP リクエストは、このサーバーではサポートされていません。
削除対象のエントリが見つかりません。	削除操作に指定した識別名が見つかりません。
変更対象のエントリが見つかりません。	リクエストで指定したエントリが見つかりません。
< パラメータ > をエントリに追加中にエラーが発生しました。	modify の add 操作が呼び出されたときに戻されました。システム・リソースが使用できないことが原因と考えられます。
属性値の暗号化時にエラーが発生しました。	ユーザー・パスワードの暗号化時にエラーが発生しました。（すべての操作）
DN の正規化でエラーが発生しました。	指定された識別名（DN）が無効です。DN の解析時に構文エラーが見つかりました。（すべての操作）
< パラメータ > 属性のハッシングでエラーが発生しました。	属性に対するハッシュ・エントリの作成時にエラーが発生しました。（スキーマ変更）
< パラメータ > オブジェクト・クラスのハッシングでエラーが発生しました。	オブジェクト・クラスに対するハッシュ・エントリの作成時にエラーが発生しました。（スキーマ変更）
スキーマ・ハッシュの作成でエラーが発生しました。	スキーマに対するハッシュ表作成時にエラーが発生しました。（スキーマ変更）
< パラメータ > の置換でエラーが発生しました。	この属性の置換でエラーが発生しました。（ldapmodify）
属性 < パラメータ > に対する値の正規化時にエラーが発生しました。	属性に対する値の正規化時にエラーが発生しました。（すべての操作）
< パラメータ > が必須またはオプションの属性リストで見つかりません。	指定した属性が、オブジェクト・クラスの要件どおりに、必須属性またはオプション属性のリストに存在していません。
この機能は組み込まれていません。	その機能またはリクエスト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。	リクエストで指定した特定のアクセス制御情報アイテム（ACI）が無効です。
必須属性 < パラメータ > が管理ドメイン < パラメータ > に定義されていません。	未定義の属性を参照しています。（スキーマ変更）
必須属性が不足しています。	特定のエントリに対する必須属性が、特定のオブジェクト・クラスの要件どおりに存在していません。
一致規則 < パラメータ > が定義されていません。	サーバーに一致規則が定義されていません。（スキーマ変更）
最大接続数に達しました。	LDAP サーバーへの最大同時接続数に達しました。

表 L-2 その他のエラー・メッセージ（続き）

エラー	原因
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。	ldapmodify を使用して命名属性を変更することはできません。cn などの命名属性は識別名の要素です。
新しい親が見つかりません。	識別名の変更操作で指定した新しい親が存在していません。（ldapmodifydn）
オブジェクトはすでに存在しています。	エントリが重複しています。（ldapadd および ldapmodifydn）
オブジェクト ID< パラメータ > はすでに使用されています。	指定したオブジェクト識別子が重複しています。（スキーマ変更）
オブジェクト・クラス < パラメータ > はすでに使用されています。	オブジェクト・クラス名が重複しています。（スキーマ変更）
オブジェクト・クラスの属性が不足しています。	この特定のエントリに対するオブジェクト・クラスの属性が不足しています。
OID< パラメータ > に構文エラーがあります。	オブジェクト識別子の定義に構文エラーがあります。（スキーマ変更）
エントリ内の属性の 1 つに重複した値があります。	作成中のエントリで、同じ属性に対して値を 2 つ入力しました。
< パラメータ > での操作は許可されていません。	このエントリでの操作は許可されていません。（変更、追加および削除）
ディレクトリ・サーバー・エントリでの操作は許可されていません。	ディレクトリ・サーバー・エントリで、この操作を行うことはできません。（削除）
オプション属性 < パラメータ > が管理ドメイン < パラメータ > に定義されていません。	未定義の属性を参照している可能性があります。（スキーマ変更）
ディレクトリ内に親のエントリが見つかりません。	親エントリが存在していません。（ldapadd および ldapmodifydn）
スーパー・オブジェクト < パラメータ > が管理ドメイン < パラメータ > に定義されていません。	スーパー・タイプが、存在していないクラスを参照しています。（スキーマ変更）
スーパー・タイプが未定義です。	スーパー・タイプが存在していません。（スキーマ変更）
スーパーユーザーの追加は許可されていません。	スーパーユーザーのエントリを作成することはできません。（ldapadd）
構文 < パラメータ > が未定義です。	構文がサーバーに定義されていません。（スキーマ変更）
RDN で指定された属性または値がエントリ内に存在していません。	相対識別名（RDN）として指定した属性値がエントリ内に存在していません。（ldapadd）
検索範囲が不明です。	LDAP リクエストで指定した検索範囲が認識されません。
このバージョンはサポートされていません。	このバージョンの LDAP リクエストは、このサーバーではサポートされていません。

パスワード・ポリシーに関するトラブルシューティング

この項では、パスワード・ポリシーに関連したエラー・メッセージと問題について説明します。

パスワード・ポリシーのエラー・メッセージ

表 L-3 に、パスワード・ポリシー違反が発生した結果、クライアントに送信されるエラー・メッセージを示します。エラー・コードは、標準の LDAP エラー・コードではありません。このエラー・メッセージは、LDAP 結果の追加情報の一部として送信されます。

表 L-3 パスワード・ポリシー違反のエラー・メッセージ

エラー番号	例外	コメントまたは解消方法
9000	GSL_PWDEXPIRED_EXCP	ユーザー・パスワードが期限切れです。
9001	GSL_ACCOUNTLOCKED_EXCP	ユーザー・アカウントがロックされています。
9002	GSL_EXPIREWARNING_EXCP	ユーザー・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	ユーザー・パスワードが必要な文字数に達していません。
9004	GSL_PWDNUMERIC_EXCP	ユーザー・パスワードに必要な数字が含まれていません。
9005	GSL_PWDNULL_EXCP	ユーザー・パスワードが NULL です。これは許可されていません。
9006	GSL_PWDINHISTORY_EXCP	ユーザーの新規パスワードが、履歴に保存されている旧パスワードと同じです。これは認められません（pwdinhistory 属性が、履歴に保存されているパスワード数を制御します）。
9007	GSL_PWDILLEGALVALUE_EXCP	入力されたユーザー・パスワードは、orclpwdillegalvalues で定義されている無効な値ですので、使用できません。
9008	GSL_GRACELOGIN_EXCP	ユーザー・パスワードが期限切れです。ユーザーには、pwdgraceloginlimit 猶予ログインが残っているか、猶予ログインが許される orclpwdgracelogintimelimit の時間（秒）があります。
9012	GSL_PWDALPHA_EXCP	パスワードには、少なくとも orclpwdminalphachars 英文字を含める必要があります。
9013	GSL_PWDSPECIAL_EXCP	パスワードには、少なくとも orclpwdminspecialchars 特殊文字を含める必要があります。
9014	GSL_PWDUPPER_EXCP	パスワードには、少なくとも orclpwdminuppercase 大文字を含める必要があります。
9015	GSL_PWDMAXCHAR_EXCP	パスワードには、orclpwdmaxrptchars 繰り返し文字しか含められません。
9016	GSL_PWDLOWER_EXCP	パスワードには、少なくとも orclpwdminlowercase 小文字を含める必要があります。
9017	GSL_EC_PWDPOLSUBENTINV	指定された pwdPolicysubentry は無効です（識別名は、ディレクトリに存在する有効なパスワード・ポリシーのものではありません）。
9018	GSL_EC_PWDPOLINUSE	削除しようとしている pwdPolicy エントリは、現在使用中です（パスワード・ポリシー自体を削除する前に、パスワード・ポリシーに対する参照を削除する必要があります）。
9019	GSL_EC_PWDPOLOBJ	pwdPolicy エントリの識別名は、変更できない可能性があります。
9020	GSL_PWDMINAGE_EXCP	パスワードは、少なくとも pwdminage の秒数が経ってからでないと変更できません。
9032	GSL_EC_GRACE_CONST	orclgracelogintimelimit と pwdgraceloginlimit は、互いに排他的です。どちらもゼロ以外にはできません。

表 L-3 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
9033	GSL_EC_NOROOTDSEPWDPOL	ルート DSE の pwdpolicysubentry 属性は、削除できません（これは、適用可能なパスワード・ポリシーなしにディレクトリから出てしまうので、許可されません）。
9034	GSL_EC_NOTROCPWDPOL	ルート Oracle コンテキストで定義されたパスワード・ポリシーのみが、ルート DSE で適用できます（これにより、ディレクトリ全体の権限を持つ管理者が指定したポリシーのみが、ディレクトリ全体に適用できることが保証されます）。
9050	GSL_ACCTDISABLED_EXCP	ユーザー・アカウントが使用禁止になっています。

関連項目： 19-9 ページの「パスワード・ポリシー、アカウントおよびパスワードの管理」

ディレクトリの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不十分

LDAP 検索のパフォーマンスが不十分です。

問題

様々な問題があります。

解決方法

次のことを確認してください。

- 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、`&(objectclass=person)(uid=john.doe)` よりも `&(uid=john.doe)(objectclass=person)` の方が適切です。

LDAP 追加または変更のパフォーマンスが不十分

LDAP 追加または変更のパフォーマンスが不十分です。

問題

様々な問題があります。

解決方法

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

統計を見積もる際には、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することができます。

14-3 ページの「デバッグ・ロギングの使用」で説明したトレース機能とデータベース・トレース・イベント 10046 は、パフォーマンスの問題を診断する際に役立ちます。

関連資料： OID データベース統計収集ツールの使用方法は、『Oracle Identity Management ユーザー・リファレンス』の `oidstats.sql` コマンドライン・ツールのリファレンスを参照してください。

検索を最適化する方法は、25-10 ページの「検索の最適化」を参照してください。

グループ・エントリのパフォーマンスに関する問題の詳細は、`http://metalink.oracle.com` にある Oracle MetaLink の MetaLink note 243006.1 を参照してください。

ディレクトリ・サーバーの起動、停止および再起動に関するトラブルシューティング

ディレクトリ・サーバーの起動および停止に関するトラブルシューティングを行うには、関係する各ツールの目的、すべてのツールがどのように連携するか、およびサーバーの起動および停止のプロセス全般について知っておく必要があります。

関連項目： 第 25 章「ディレクトリのチューニングに関する考慮事項」

ディレクトリ・サーバー・インスタンスを起動、停止および再起動するためのツールの概要

ディレクトリ・サーバーを Oracle Application Server コンポーネントとして起動および停止するためのツールは OPMN です。OPMN のトラブルシューティングの詳細は、『Oracle Process Manager and Notification Server 管理者ガイド』の付録「トラブルシューティング」を参照してください。

ディレクトリ・サーバー・インスタンスの起動、停止および再起動に使用するツールは、OID 制御ユーティリティ（OIDCTL）と OID モニター（OIDMON）の 2 つです。

OIDCTL　OIDCTL を実行すると、OIDCTL はユーザー `ODS` としてデータベースに接続します。コマンドで使用するオプションに応じて、OIDCTL は、`ODS.ODS_PROCESS` という表に行を挿入するか、この表の行を更新します。`START` オプションを使用すると、行が挿入されます。`STOP` または `RESTART` オプションを使用すると、行が更新されます。

ODS.ODS_PROCESS 表には次の情報が含まれています。

- `instance`: 一意のインスタンス番号。0 ～ 1000 の任意の値です。
- `pid`: プロセス識別子。プロセスが起動されると、OIDMON によって更新されます。
- `state`: リクエストされた操作のタイプ。

  `state` の値は次のいずれかです。

  - 0= 停止
  - 1= 起動
  - 2= 実行中
  - 3= 再起動
  - 4= シャットダウン
  - 5= フェイルオーバー済

注意： OPMN を使用してディレクトリ・サーバーを停止した場合、state の値は当初 4（シャットダウン）です。ただし、OPMN が再度ディレクトリ・サーバーを起動すると、state の値は 2（実行中）になります。

OIDMON 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には、OIDMON が実行中であることが必要です。このデーモンは、ODS.ODS_PROCESS 表の state 列の値を指定の間隔でチェックします。

state=0 の行が見つかると、pid を読み取ってプロセスを停止します。

state=1 または state=4 の行が見つかると、新規プロセスを起動し、pid 列を新しいプロセス識別子で更新します。

state=2 の行が見つかると、pid を読み取り、その pid を持つプロセスが実行中であることを検証します。実行中でない場合は、新規プロセスを起動し、pid 列を新しいプロセス識別子で更新します。

state=3 の行が見つかると、pid を読み取ってプロセスを停止し、新規プロセスを起動して、それに合せて pid を更新します。

なんらかの理由でサーバーを起動できない場合は、再試行します。OIDMON が Oracle Application Server Cluster（Identity Management）構成のノードで実行されていない場合、10 回再試行しても成功しないときは、その行を ODS.ODS_PROCESS 表から削除します。OIDMON が Oracle Application Server Cluster（Identity Management）構成のノードで実行されている場合は、100 回再試行します。

それでも起動できない場合は、別のノードにリクエストをプッシュします。

つまり、OIDCTL は、ODS.ODS_PROCESS 表の行に対して状態情報の挿入および更新を行います。OIDMON は、その情報を読み取り、指定されたタスクを実行します。

ディレクトリ・サーバーの起動、停止および再起動に関与するプロセスの概要

ディレクトリ・サーバーの起動、停止および再起動には、いくつかのプロセスが関与します。OIDMON はその 1 つです。UNIX では、OIDMON を oidmon と呼びます。Microsoft Windows 環境では、oidmon.exe と呼びます。

インスタンスを起動する場合、OIDMON は、前の項で説明した instance 列の一意の数をチェックします。その後、リスナー / ディスパッチャ（Oracle Net Services のリスナー・プロセスとは異なります）という別のプロセスを起動します。この新しいプロセスのプロセス識別子は、pid 列に格納されます。

一方、リスナー / ディスパッチャは、構成設定エントリに定義されたいくつかのサーバー・プロセスを起動します。これらのサーバー・プロセスは、OIDMON ではなくリスナー / ディスパッチャによって制御されます。いずれかのプロセスが失敗すると、リスナー / ディスパッチャによって自動的に再起動されます。

リスナー / ディスパッチャとサーバー・プロセスが組み合されて、ディレクトリ・サーバー・インスタンスとなります。UNIX では、このディレクトリ・サーバー・インスタンスを oidldapd と呼びます。Microsoft Windows では、oidldapd.exe と呼びます。

要約すれば、少なくとも 3 つのプロセスがあります。OIDMON のプロセスが 1 つ、ディレクトリ・サーバー自体のプロセスが少なくとも 2 つです。すべてのプロセスが実行されているときには、UNIX コンピュータに次のような内容が表示されます。

```
% ps -ef|grep oid
root 12387 12381 0 Mar 28 ? 0:05 oidldapd -i 1 -conf 0 key=811436710
root 12381 1 0 Mar 28 ? 0:10 oidmon start
root 13297 1 0 Mar 28 ? 0:14 oidldapd
```

サーバー情報を取得するには、ldapcheck を実行するという方法もあります。その場合、次のような内容が表示されます。

```
Checking Oracle Internet Directory Processes ...
Process oidmon is Alive as PID 12381
Process oidldapd is Alive as PID 12387
Process oidldapd is Alive as PID 13297
Not Running ---- Process oidrepld
```

ディレクトリ・サーバーの起動、停止および再起動に関する問題

この項では、ディレクトリ・サーバーを起動、停止または再起動するときに発生する場合がある問題について説明します。

OIDCTL または OIDMON が正常に動作しない OIDCTL または OIDMON が正常に動作しない場合は、いくつかの理由が考えられます。

問題

構文が正しくありません。

解決方法

『Oracle Identity Management ユーザー・リファレンス』の、Oracle Internet Directory サーバーの管理ツールに関する説明を参照し、正しい構文を使用しているかどうかを確認してください。OIDCTL を使用する場合の接続オプションの正しい値は TNS 別名（接続文字列）です。ホスト名やその他の値ではありません。`http://metalink.oracle.com` にある Oracle MetaLink の Oracle MetaLink note 155790.1 を参照してください。

問題

Oracle Internet Directory で指定されたデータベースが稼働していません。

Oracle Net Services の構成が正しくありません。

解決方法

Oracle Internet Directory で指定されたデータベースと Oracle Net Services のコンポーネントが正しく構成され、稼働していることを確認します。そのためには、OIDCTL と同じ *ORACLE_HOME* にインストールされている SQL*Plus を使用して、データベースに接続できるかどうかを確認します。`ODS/`*`ods_password@tns_alias`* としてログインします（*`tns_alias`* は、OIDCTL の `connect` オプションで使用する場合と同じです）。`http://metalink.oracle.com` にある Oracle MetaLink の Oracle MetaLink note 155790.1 を参照してください。

問題

LDAP の名前解決には Oracle Internet Directory のインスタンスが 2 つ必要ですが、1 つしか稼働していません。

解決方法

`ldap.ora` ファイルの `DIRECTORY_SERVERS` パラメータの値が、`sqlnet.ora` ファイルの `NAMES.DIRECTORY_PATH` で指定されている値と違うことを確認します。これらのファイルはいずれも、*`ORACLE_HOME`*`/network/admin` にあります。何も問題がなければ、`ODS.ODS_PROCESS` から選択すると、L-10 ページの「OIDCTL」で説明した state 値を持つ行が取得されます。`http://metalink.oracle.com` にある Oracle MetaLink の Oracle MetaLink note 155790.1 を参照してください。

ODS.ODS_PROCESS の情報が正しいにもかかわらず、プロセスが起動されない。

何も問題がないときには、少なくとも 3 つのプロセスが存在します。oidmon が 1 つ、oidldapd が少なくとも 2 つです。OIDMON はサーバー・プロセスの起動、停止および再起動を行います。これらの処理は指定の間隔で実行されるため、リクエストされた操作が完了するまでしばらく時間がかかります。

問題

`oidldapd` ファイルがありません。

解決方法

`oidmon.log` を参照します。「`No such file or directory`」というメッセージを探してください。この問題を修正するには、実行可能ファイルを置き換えます。

問題

oidldapd 実行可能ファイルの権限が不適切です。

解決方法

「Exec of OIDLDAPD failed with error 13」というメッセージを探します。UNIX の場合、$ORACLE_HOME/bin/oidldapd ファイルには次の権限が必要です。

```
-rws--x---    1 root     dba       1691802 Jan 20 10:30 oidldapd
```

権限が正しくない場合は、ルートとして次のように入力します。

```
cd $ORACLE_HOME/bin
chown root:dba oidldapd
chmod 0710 oidldapd
chmod u+s oidldapd
```

問題

権限が不十分なユーザーとして実行しています。

解決方法

これが問題になっていることを確認するには、oidmon.log を参照します。「Permission denied」または「Open Wallet failed」というメッセージを探してください。これは、root または dba グループのユーザーとして実行していない場合に発生します。この問題を修正するには、正しいユーザーとして再試行します。

問題

ポートが使用中です。

解決方法

oidldapd*XX*.log（*XX* はサーバーのインスタンス番号）を参照します。「Bind failed on...」というメッセージを探してください。これは、oidldapd のリスニング対象として構成されているポートが他のプロセスによって使用されていることを示します。ポートを使用しているプロセスを特定するには、次のように入力します。

```
netstat -a | grep portNum
```

必要に応じて、別のポートを使用するようにもう一方のプロセスを再構成するか、configset を追加して別のポートをリスニングするように oidladapd を構成します。デフォルトでは、oidladapd が 2 つのポート（SSL ポートと非 SSL ポート）でリスニングすることに注意してください。

問題

クラスタ構成または Oracle Application Server Cluster（Identity Management）構成において、OIDMON は、ローカル・ノードでサーバーを起動できない場合に、クラスタ内の別のノードにそのサーバーをプッシュします。

解決方法

oidmon.log を参照します。「gslsgfrPushServer: Could not start *server*on *NodeA*,trying to start on node*NodeB*」というメッセージを探してください。この問題を修正するには、まず OIDMON がローカル・ノードでサーバーを起動できない理由を特定する必要があります。

問題
Oracle Net Services またはデータベース自体で問題が発生している可能性があります。

解決方法
`oidmon.log`、`oidsrv.log`、`oidldapd`*`xx`*`.log`（*`xx`* はサーバーのインスタンス番号）および `oidrepd`*`xx`*`.log`（*`XX`* は Oracle Directory Integration and Provisioning Server のインスタンス番号）を参照し、問題の詳細を確認します。

ODS.ODS_PROCESS の行が欠落している。

問題
クラスタ構成または Oracle Application Server Cluster（Identity Management）構成において、OIDMON が両方のノードで `oidldapd` を正常に起動しましたが、タイムスタンプの相違によりフェイルオーバーを開始しました。

解決方法
`oidmon.log` を参照します。行が欠落しているノードで、「`Successfully failed over from` *`NodeA`* `to` *`NodeB`*」というメッセージを探してください。もう一方のノードには `oidldapd` が余分に存在します。この問題を修正するには、すべてのノードで相互の誤差が 250 秒以内になるようにシステム時間を調整します。

解決方法
トレース・ファイル `oidldapd`*`xx`*`.log`（*`xx`* はインスタンス番号）および `oidldapd`*`xx`*`s`*`yy`*`.log`（xx はインスタンス番号、*`yy`* はプロセス識別子）を参照してください。トレース・ファイルに有益な情報や Oracle MetaLink ドキュメントへのポインタが記録されていない場合は、次の手順を実行します。(1) ディレクトリ・サーバー・プロセスを停止します。(2) 旧トレース・ファイルを削除または名前変更します。(3) OIDMON およびディレクトリ・サーバーを最大デバッグ・レベル（11744051）で起動します。トレース・ファイルを作成するには、サーバーを単に再起動するのではなく、停止してから起動する必要がありますので注意してください。新規トレース・ファイルを調べます。また、必要に応じて、Oracle サポート・サービスに iTAR を提出し、トレース・ファイルを iTAR にアップロードします。`http://metalink.oracle.com` にある Oracle MetaLink の Oracle MetaLink note 155790.1 を参照してください。

> **関連資料：** フェイルオーバーの詳細は、『Oracle Application Server 高可用性ガイド』の「Oracle Application Server Cluster（Identity Management）環境でのフェイルオーバーの動作」を参照してください。

OIDCTL エラー 実行中のプロセスがないにもかかわらず、OIDCTL を使用すると、指定のインスタンスはすでに使用されているというエラーが表示されます。

問題
これは、OIDMON が実行されていないときにマシンを再起動した後などに発生します。

解決方法
OIDMON を起動することで、ディレクトリ・サーバーを起動します。`http://metalink.oracle.com` にある Oracle MetaLink の Oracle MetaLink note 155790.1 を参照してください。

解決方法
OIDCTL の `stop` オプションを使用して、指定のインスタンスを停止します。`http://metalink.oracle.com` にある Oracle MetaLink の Oracle MetaLink note 155790.1 を参照してください。

解決方法

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無視し、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。`oidctl` のコマンドライン・オプションを使用して、異なる構成値でサーバーを起動すると、定義済の構成設定が `configset0` の値を除いてすべて無視されます。この技術は `configset0` の最小かつデフォルトの内容に基づいているため、*`configset0`* を変更しないでください。

解決方法

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・ファイルを表示するには、`$`*`ORACLE_HOME`*`/ldap/log` にナビゲートします。

> **関連資料：** フェイルオーバーの詳細は、『Oracle Identity Management ユーザー・リファレンス』の `oidctl` コマンドライン・リファレンスを参照してください。

Oracle Internet Directory レプリケーションのトラブルシューティング

この項では、ディレクトリ・レプリケーションの問題について説明します。

レプリケーションの問題を調査するときは、必ずログ・ファイル `$ORACLE_HOME/ldap/oidrepld00.log` および `oidldapdxx.log` の内容を確認してください。

レプリケーション・サーバーは複数のデバッグ・レベルをサポートしています。レプリケーションのデバッグをオンにするには、サーバー起動時に `-d` *`decimal_debug_level`* フラグを指定します。次に例を示します。

```
oidctl server=oidrepld connect=connect_string instance=instance_number \
       flags="-h host -p port -d decimal_debug_level"
```

> **注意：** デバッグをオンにすると、レプリケーションのパフォーマンスに影響が出ます。

> **関連項目：** デバッグの詳細は、第 14 章「ディレクトリのロギング、監査および監視」を参照してください。

レプリケーション・サーバーが起動しない

レプリケーション・サーバーを起動できない場合は、いくつかの問題があります。

問題

`oidctl` の構文に誤りがあります。

解決方法

次の構文を使用してレプリケーション・サーバーを起動します。

```
oidctl server=oidrepld connect=connect string instance=instance_number \
       flags="-h host -p port"
```

問題

レプリケーション・サーバーを起動するときにコマンドラインで指定したホストおよびポートで Oracle Internet Directory が稼働していません。そのため、ターゲット Oracle Internet Directory への匿名バインドに失敗しました。

解決方法

指定したホストおよびポートでターゲット Oracle Internet Directory が稼働していることを確認します。

問題

レプリケーション・サーバーが、レプリカ・エントリの orclreplicaprimaryurl または orclreplicasecondaryurl 属性で指定したホストおよびポートへのバインドを試みていますが、Oracle Internet Directory は別のホストまたはポートで稼働しています。

解決方法

Oracle Internet Directory を別のホストまたはポートで実行する場合は、次の手順で、レプリカ・エントリの orclreplicasecondaryurl 属性に新しい情報を追加します。

1. 変更ファイル mod.ldif を準備します。たとえば、ホストを my.us.oracle.com に、ポートを 4444 に変更する場合は、次のように指定します。

   ```
   dn: orclreplicaid=replica_ID, cn=replication configuration
   changetype: modify
   add: orclreplicasecondaryurl
   orclreplicasecondaryurl: ldap://my.us.oracle.com:4444/
   ```

2. 次のコマンドを実行します。

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

問題

レプリケーション Wallet $ORACLE_HOME/ldap/admin/oidr*ORACLE_SID* 内の ReplBind 資格証明が破損しているか無効です。つまり、Wallet に格納されているパスワードと、ディレクトリに格納されているパスワードが同じではないか、Wallet が存在しません。そのため、レプリケーションのバインドに失敗し、レプリケーション・サーバーがエラーで終了しました。

oidrepld*XX*.log ファイルに、次のようなメッセージが記録される場合があります。

```
2005/07/21:11:13:28 * gslrcfdReadReplDnPswd:Error reading repl passwd
2005/07/21:11:13:28 * gslrcfcReadReplConfig:Error found.
2005/07/21:11:13:28 * Failed to read replication configuration information.
```

解決方法

remtool を使用して、レプリケーション Wallet 内のレプリケーション・バインドの資格証明を修正するか、Oracle Internet Directory とレプリケーション Wallet を同期させます。

- remtool -pchgpwd は、レプリカのレプリケーション識別名のパスワードを変更します。ディレクトリに格納されている現在のレプリケーション識別名パスワードを知っており、ディレクトリに格納されているパスワードと Wallet 内の証明を両方変更する場合は、このオプションを使用します。
- remtool -presetpwd は、レプリカのレプリケーション識別名のパスワードをリセットします。ディレクトリに格納されている現在のレプリケーション識別名パスワードを知っており、ディレクトリに格納されているパスワードと Wallet 内の証明を両方変更する場合は、このオプションを使用します。
- remtool -pchgwalpwd は、レプリカのレプリケーション識別名のパスワードを Wallet 内でのみ変更します。ディレクトリに格納されているレプリケーション識別名のパスワードは知っているが、Wallet のパスワードが正しいかどうか不明な場合、または Wallet ファイルを作成する必要がある場合に、このオプションを使用してください。

これらすべてのオプションは、Wallet がまだ存在しない場合に新しい Wallet を作成します。

関連資料 :

- remtool の使用方法の詳細は、『Oracle Identity Management ユーザー・リファレンス』の remtool コマンドライン・ツールのリファレンスを参照してください。
- oidpasswd の使用方法の詳細は、『Oracle Identity Management ユーザー・リファレンス』の oidpasswd コマンドライン・ツールのリファレンスを参照してください。

リポジトリ作成アシスタントのエラー

問題

Oracle Application Server ツール RepCA を使用して、Oracle Internet Directory スキーマを既存の Oracle 10.1.0.3 Database にロードする場合、$ORACLE_HOME/assistants/repca/log/repca*log ファイルに次のようなエラー・メッセージが出力されることがあります。

```
SP2-0332: Cannot create spool file.
```

解決方法

このエラー・メッセージは無視してかまいません。

レプリケーションのブートストラップに関するエラー

レプリケーションのブートストラップでは、いくつかのエラーが発生する場合があります。

問題

一部のネーミング・コンテキストのブートストラップに失敗しました。

解決方法

ブートストラップに失敗したネーミング・コンテキストを特定し、oidreconcile ツールを使用して調整します。その後、コンシューマのレプリカ状態をオンライン・モードに設定して、レプリケーションを再開します。

問題

様々な原因。

解決方法

ブートストラップに失敗した原因を特定し、修正します。その後、コンシューマのレプリカ状態をブートストラップ・モードに設定して、ブートストラップを再開します。

解決方法

エラーの正確な原因を特定するには、ログ・ファイル oidldapdxx.log を調べます。次の例に示すようなエラー・メッセージを探します。

```
2004/09/14:12:57:23 * Starting OIDREPLD against dlsun1418:4444...
2004/09/14:12:57:25 * Starting scheduler...
2004/09/14:12:57:26 * Start to BootStrap from supplier=dlsun1418_replica to
consumer=dlsun1418_replica2
2004/09/14:12:57:27 * gslrbssSyncDIT:Replicating namingcontext=cn=oraclecontext ......
2004/09/14:12:58:21 * gslrbssSyncDIT:Sync done successfully for namingctx:
cn=oraclecontext, 222 entries matched
2004/09/14:12:58:21 * gslrbssSyncDIT:Replicating namingcontext=cn=joe smith ......
2004/09/14:12:58:23 * BootStrap failure when adding DN=cn=Joe Smith,
server=dlsun1418_replica2,err=Constraint violation.
2004/09/14:12:58:23 * gslrbssSyncDIT:Sync failed for namingctx: cn=joe smith, only 1
entries retrieved
2004/09/14:12:58:23 * gslrbssSyncDIT:Replicating namingcontext=cn=oracleschemaversion
......
2004/09/14:12:58:25 * gslrbssSyncDIT:Sync done successfully for namingctx:
cn=oracleschemaversion, 10 entries matched
2004/09/14:12:58:51 * gslrbsbBootStrap: Failure occured when bootstrapping 1 out of 3
namingcontext(s) from the supplier
```

ブートストラップに失敗した原因を特定し、修正します。問題の原因となったネーミング・コンテキストを特定し、oidreconcile を使用してネーミング・コンテキストの比較および調整を行うことができます。問題が解決したら、Oracle Internet Directory レプリケーション・サーバーを起動して、再度ブートストラップを開始します。

問題
ブートストラップ中に Oracle Internet Directory サーバーが停止しました。

解決方法
サプライヤ側の Oracle Internet Directory サーバーとコンシューマ側の Oracle Internet Directory サーバーが、レプリケーションのブートストラップ中に稼働していることを確認します。

問題
制約違反のため、ブートストラップ対象のエントリの一部をコンシューマ側で適用できません。

解決方法
レプリケーションのブートストラップを開始する前に、コンシューマ側の Oracle Internet Directory スキーマがサプライヤ側の Oracle Internet Directory スキーマと同期していることを確認します。LDAP レプリカを追加する場合、コンシューマ・レプリカの Oracle Internet Directory スキーマはサプライヤ・レプリカの Oracle Internet Directory スキーマと必ず同期します。

問題
ブートストラップ中にレプリケーションの不適切なフィルタ処理が行われました。ブートストラップ中に 1 つ以上の属性をレプリケーションから除外できます。ただし、エントリの必須属性を除外する構成を行った場合、objectclass 違反のため、そのエントリをコンシューマ側で適用できません。

解決方法
第 30 章「Oracle Internet Directory レプリケーションのインストールと構成」のレプリケーション・ネーミング・コンテキスト構成規則に従って、レプリケーションのフィルタ処理を正しく構成します。

LDAP レプリケーションをデバッグする場合、LDAP レプリカの状態をよく理解しておく必要があります。LDAP ベースのレプリケーションが構成されている場合、レプリケーション・サーバーは、起動後、ローカル・レプリカからレプリカの状態を読み取ります。レプリケーション・サーバーの動作はローカル・レプリカの状態によって異なります。LDAP レプリケーション・エラーは `oidldapdxx.log` に記録されます。

関連資料： 付録 H「LDAP のレプリカ状態」

問題
エントリ数が 5000 を超えるネーミング・コンテキストのブートストラップに失敗した後、そのレプリケーション・サーバーを再起動すると、次のようなエラー・メッセージがログ・ファイル `oidrepld00.log` に出力される場合があります。

```
2005/04/05:13:21:55 * gslrbssSyncDIT:Replicating namingcontext=dc=com ......
2005/04/05:15:36:09 * gslrbssSyncDIT:Subtree delete on dc=com failed.
Error=DSA is unwilling to perform
2005/04/05:15:36:09 * gslrbssSyncDIT:Sync failed for namingctx: dc=com, only
0 entries retrieved
```

レプリケーション・サーバーは、ブートストラップ操作時に 2 つの手順を実行します。まず、コンシューマ側で、ブートストラップが必要なネーミング・コンテキストを削除します。次に、それらのネーミング・コンテキストに属するエントリをサプライヤからコンシューマへコピーします。数千のエントリを含むネーミング・コンテキストをレプリケーション・サーバーが削除すると、非常に大規模なトランザクションが発生します。この大規模なトランザクションに対応するには、UNDO 表領域として十分な領域を確保しなければなりません。データベースの UNDO 表領域の領域が不十分な場合は、ORA-30036 エラーが発生します。

解決方法
UNDO 表領域の領域を追加するようデータベース管理者に依頼します。または、bulkdelete ツールを使用して必要なネーミング・コンテキストを削除してから、レプリケーション・サーバーを起動します。

変更がレプリケートされない

変更内容が別のノードにレプリケートされません。

問題
レプリケーション・サーバーの表領域が不足しています。

解決方法
サーバー・ログで、次のメッセージを探してください。

```
OCI Error ORA-1653 : ORA-01653: unable to extend table ODS.ASR_CHG_LOG by 8192 in
tablespace OLTS_DEFAULT
```

表領域を拡張し、表領域が増大し続けている原因を調べます。

問題
ターゲットの Oracle Internet Directory サーバーが停止しています。

解決方法
ターゲットの Oracle Internet Directory サーバーを再起動します。

問題
様々な原因

解決方法
レプリケーション・サーバーが、マルチマスター・レプリケーションのすべてのノード、および単一マスター・レプリケーションまたはファンアウト・レプリケーションのコンシューマ・ノードで起動していることを確認します。

マルチマスターの Oracle Database アドバンスト・レプリケーションでは、remtool を使用して問題の診断と修正を行います。

- `remtool -asrverify` は、DRG の設定が正しいかどうかを検証し、問題を報告します。
- `remtool -asrrectify` は、DRG の設定が正しいかどうかを検証し、問題を報告して、問題の修正を試みます。

レプリケーション・ログおよび LDAP ログにエラー・メッセージが記録されていないかどうかチェックし、調査が終わったら、エラーの原因を修正します。

> **関連資料：** remtool の使用方法の詳細は、『Oracle Identity Management ユーザー・リファレンス』の remtool コマンドライン・ツールのリファレンスを参照してください。

レプリケーション操作の停止

問題

レプリカ間でデータがレプリケートされません。OID 管理者操作キューのエントリがいずれかのノードに適用された後、実行中のレプリケーション設定作業が停止してしまうことがあります。新規レプリカの追加や削除を行うと問題や障害が発生することもあります。

問題

様々な原因。

解決方法

`http://metalink.oracle.com` にある Oracle MetaLink から、次の Oracle MetaLink note を参照してください。

Note 171693.1「Resolving Conflicts」

Note 122039.1「Troubleshooting Basics for Advanced Replication」

Note 213910.1「Debugging OID Replication when ASR_CHG_LOG Never Gets Populated」

検索ボックスに replication などの語を入力して、Oracle MetaLink note を検索できます。

SSL 設定に関するトラブルシューティング

問題

Oracle Internet Directory で、SSL による一方向の LDAP 接続を設定しようとすると失敗します。

解決方法

configset 0 の SSL ポートを Wallet モード 2 または 3 で設定しないでください。この設定を行うと、暗号化 SSL ポートで Oracle Internet Directory と通信しようとしている Oracle Delegated Administration Services やその他のサービスおよびアプリケーションに障害が発生します。

Oracle Internet Directory を SSL 用に正しく構成し、テストするには、`http://metalink.oracle.com` にある Oracle MetaLink から Oracle Metalink note 178714.1 の指示に従ってください。また、http://www.oracle.com/technology/obe/obe_as_10g に掲載されているチュートリアル『Getting Started with Oracle Internet Directory』の SSL の項も参照してください。

この項では、SSL の構成時に発生する可能性のある問題について説明します。

変更ログのガベージ・コレクションに関するトラブルシューティング

レプリケーションと Oracle Directory Integration Platform はいずれも、変更ログを使用して、サプライヤ・ディレクトリの情報をコンシューマ・ディレクトリに伝達します。変更ログはすべて ods_chg_log という表に格納されます。また、レプリケーション変更ログは asr_chg_log に格納されます。

この項では、変更ログのガベージ・コレクションの際に発生する可能性のある問題について説明します。

変更ログが削除されない

変更ログのサイズが非常に大きくなります。

問題

レプリケーションの問題のため、変更ログは削除されません。たとえば、レプリケーション・サーバーが数日間停止した場合、レプリケーションのリカバリで必要になるので、レプリケーション変更ログは削除されません。

解決方法

レプリケーションの問題を解決します。L-15 ページの「Oracle Internet Directory レプリケーションのトラブルシューティング」を参照してください。

問題

属性 orclpurgetargetage に非常に大きい値が設定されています。さらに、有効化されているが、アクティブではない変更ログ・サブスクライバが 1 つ以上あり、サブスクライバ・プロファイルの orclLastAppliedChangeNumber を更新していません。変更数ベースの削除機能は、コンシュームされていない変更ログを削除しません。時間ベースの削除機能は、十分な時間が経過していないことから変更ログを削除しません。

解決方法

属性 orclpurgetargetage の値を小さくして、変更ログがより早く削除されるようにしてください。

解決方法

非アクティブな変更ログ・サブスクライバを無効にして、変更ログ数ベースで変更ログが削除されるようにします。有効化されているが、アクティブではないサブスクライバ・プロファイルを探すには、次のように入力して、すべてのサブスクライバ・プロファイルの orclLastAppliedChangeNumber を調べます。

```
ldapsearch -v -p port -h host -D cn=orcladmin -w password \
           -b "cn=changelog subscriber,cn=oracle internet directory" \
           -s sub "objectclass=orclchangesubscriber" \
           orcllastappliedchangenumber orclsubscriberdisable
```

orclSubscriberDisabled がゼロで、orclLastAppliedChangeNumber の値がまったく変化していないエントリを探してください。そのようなエントリが存在し、変更ログのガベージ・コレクタの orclpurgetargetage がゼロ以上の場合は、orclpurgetargetage の値を削除します。orclpurgetargetage が定義されていない場合、またはゼロより小さい場合、別のサブスクライバが orclLastAppliedChangeNumber を更新していなくても、ガベージ・コレクタはレプリケーション・サーバーによって適用された変更を削除します。

関連資料： 26-6 ページの「マルチマスター・レプリケーションの変更ログの削除」

動的パスワード・ベリファイアに関するトラブルシューティング

表 L-4 に、動的パスワード・ベリファイアのエラー・メッセージとその説明を示します。

表 L-4 動的パスワード・ベリファイアのエラー・メッセージ

エラー・コード	説明
9022	ユーザー・エントリに可逆暗号化パスワードがありません。
9023	LDAP リクエスト制御で指定した暗号タイプはサポートされていません。
9024	LDAP リクエスト制御に username パラメータがありません。

ディレクトリがベリファイアを比較でき、比較の結果が FALSE の場合、ディレクトリは標準エラー LDAP_COMPARE_FALSE をクライアントに送信します。同様に、認証中のユーザーがディレクトリ・エントリを持たない場合、ディレクトリは標準エラー LDAP_NO_SUCH_OBJECT を送信します。

> **関連資料：**『Oracle Identity Management ユーザー・リファレンス』の「パスワード・ベリファイアのスキーマ要素」

Oracle Internet Directory パスワード Wallet に関するトラブルシューティング

Oracle Internet Directory サーバーには、`oidpwdlldap1` と `oidpwdr`*`SID`* の 2 つのパスワード Wallet があります。

`oidpwdlldap1` ファイルには、ODS ユーザーの識別名およびパスワードが暗号化形式で格納されます。Oracle Internet Directory サーバーは、起動時に、資格証明を使用してバックエンド・データベースに接続します。

Oracle Internet Directory サーバーが起動しない

`oidctl` または `opmn` が Oracle Internet Directory サーバー・インスタンスの起動に失敗します。

問題

`oidpwdlldap1` Wallet に格納されているパスワードが、バックエンド・データベースの ODS パスワードと同期していません。

解決方法

`sqlplus` コマンドを使用して、データベースへの接続を再試行します。

```
sqlplus ods /ods_password@connect_string
```

接続に成功した場合は、`oidpasswd` ツールを使用して正しいパスワードを持つ新規 Wallet を作成することで、Wallet 内のパスワードを ODS パスワードと同期させます。次に例を示します。

```
>> oidpasswd connect=connect_string create_wallet=true
```

接続に失敗した場合は、データベース管理者としてバックエンド・データベースにログインし、sql コマンドを使用して ODS パスワードを変更する必要があります。

```
>> alter user ods identified by some_new_password
```

その後、`oidpwdlldap1` を新たに作成して、新規パスワードを格納します。

解決方法

Oracle Internet Directory サーバーの起動を再試行します。

oidpwdr*SID* ファイルには、レプリカ識別名の識別名およびパスワードが暗号化形式で格納されます。Oracle Internet Directory レプリケーション・サーバーは、起動時に、資格証明を使用して Oracle Internet Directory サーバーに接続します。

レプリケーション・パスワード Wallet oidpwdr*SID* の例を次に示します。

```
/------BEGIN REPL CREDENTIAL:cn=replication dn,orclreplicaid=qdinh-sun_
adeldap,cn=replication configuration-----
ezNkZXMtY2JjLXBrY3M1cGFkfQUnaz0TsfzcP0nM1HcHAXchf5mJw+sb4y0bLvvw3RvSg7H
S7/WsKJB02fdSGRlmfWAV+6llkRQ26g==
-----END REPL CREDENTIAL:cn=replication dn,orclreplicaid=qdinh-sun_
adeldap,cn=replication configuration-----/
```

パスワードが同期されない

oidctl または opmn が Oracle Internet Directory サーバー・インスタンスの起動に失敗し、バインドできないというメッセージがレプリケーション・サーバー・ログ・ファイル oidrepld00.log に記録されます。

問題

oidpwdr*SID* に格納されたレプリカ識別名のパスワードが、Oracle Internet Directory サーバーのレプリカ識別名のパスワードと同期していません。

解決方法

ldapbind コマンドを使用して、Oracle Internet Directory サーバー・インスタンスへの接続を試みます。oidpwdr*SID* に格納されているレプリカ識別名とレプリカ識別名のパスワードを指定します。次に例を示します。

```
>> ldapbind -h host -p port -D "cn=replication dn,orclreplicaid=qdinh-sun_adeldap,
cn=replication configuration" -w replica_dn_password
```

接続に成功した場合は、remtool をオプション -pchgwalpwd とともに使用して、oidpwdr*SID* Wallet 内のパスワードをリセットします。これで、レプリカのレプリケーション識別名のパスワードが Wallet 内でのみ変更されます。レプリケーション識別名のパスワードがわからない場合は、remtool をオプション -prestpwd とともに使用してリセットします。これで、レプリカのレプリケーション識別名のパスワードがリセットされます。

レプリケーション・パスワード Wallet をリセットした後、opmnctl または oidctl を使用して、レプリケーション・サーバー・インスタンスをもう一度再起動します。

bulkload のトラブルシューティング

次の手順に進む前に、bulkload がスローしたすべてのエラーを調べ、修正することを強くお薦めします。bulkload エラーを無視すると、後から深刻な問題が発生する可能性があります。

大部分の bulkload エラーは、データ・ロード中または索引作成中に発生します。

問題

bulkload コマンドライン・ツールが、データ・ロード中に失敗しました。

解決方法

次のいずれかの方法を使用して、ディレクトリをデータ・ロード前の状態にリストアします。

- bulkload recover オプションを使用する。
- bulkload を起動する前に取ったバックアップからディレクトリをリストアする。

問題

bulkload コマンドライン・ツールが、索引作成中に失敗しました。

解決方法

bulkload.log を調べます。索引作成失敗の原因となった問題を特定し、修正します。bulkload に index オプションを指定して、再び実行します。

索引エラーの修正に失敗すると、Oracle Internet Directory の表に重複エントリや重複行が生じる可能性があります。

問題

bulkload コマンドライン・ツールが、データベースへの接続切断のために失敗しました。これは、たとえばホストのクラッシュや、Real Application Clusters でのフェイルオーバーが原因で、発生する可能性があります。

解決方法

次の手順に従ってください。

1. データベースが正常に再起動したか確認します。
2. bulkload の起動に check="TRUE" オプションまたは generate="TRUE" オプションのみを使用し、load="TRUE" オプションを使用しなかった場合は、手順 3 に進んでください。

   失敗したのが bulkload load="TRUE" オプションだった場合、データベースを失敗前の状態にリストアする必要があります。どのように行うかは、bulkload load="TRUE" コマンドを発行する前に、データベースのバックアップを取ったかどうかによって決まります。

   - バックアップがある場合は、それを使用して、データベースを bulkload コマンドを発行する前の元の状態にリストアします。
   - バックアップがない場合は、bulkload recover コマンドを使用して、データベースを bulkload load="TRUE" コマンド発行前の状態に戻します。
3. 失敗した bulkload コマンドを再発行します。

bulkdelete および bulkmodify のトラブルシューティング

次の手順に進む前に、bulk ツールがスローしたすべてのエラーを調べ、修正することを強くお薦めします。

問題

bulkdelete または bulkmodify コマンドライン・ツールが、データベースへの接続切断のために失敗しました。これは、たとえばホストのクラッシュや、Real Application Clusters でのフェイルオーバーが原因で、発生する可能性があります。

解決方法

データベースが正常に再起動したか確認します。次に、失敗した bulkdelete または bulkmodify コマンドを再試行します。

catalog のトラブルシューティング

次の手順に進む前に、bulk ツールがスローしたすべてのエラーを調べ、修正することを強くお薦めします。

問題

catalog コマンドライン・ツールが、データベースへの接続切断のために失敗しました。これは、たとえばホストのクラッシュや、Real Application Clusters でのフェイルオーバーが原因で、発生する可能性があります。

解決方法

データベースが正常に再起動したか確認します。失敗した catalog コマンドを再試行します。最初の起動で add="TRUE" オプションを使用した場合は、最初のコマンドが部分的に完了しているため、再試行が失敗する可能性があります。再試行が失敗した場合、catalog delete="TRUE" を使用して属性索引を削除し、コマンドをもう一度再試行します。

それでも解決しない場合は

この他にも、http://metalink.oracle.com の Oracle MetaLink には様々な解決策が掲載されています。問題の解決策が見つからない場合は、オラクル社カスタマ・サポート・センターに問い合せてください。

> **関連資料：** Oracle Application Server のリリース・ノートを参照してください。この資料は Oracle Technology Network（*http://www.oracle.com/technology/documentation/index.html*）で入手できます。

用語集

3DES

「**Triple Data Encryption Standard**」を参照。

ACI

「**アクセス制御情報項目**」を参照。

ACL

「**アクセス制御リスト**」を参照。

ACP

「**アクセス制御ポリシー・ポイント**」を参照。

Advanced Encryption Standard（AES）

データ暗号化規格にかわる暗号標準として意図された**対称型暗号**アルゴリズム。商用および政府データの暗号化に対する、米国連邦情報処理標準（Federal Information Processing Standard: FIPS）となっている。

AES

「**Advanced Encryption Standard**」を参照。

API

「**Application Program Interface**」を参照。

Application Program Interface（API）

コンピュータ・アプリケーションと、下位レベルのサービスや機能（オペレーティング・システム、デバイス・ドライバ、他のソフトウェア・アプリケーションなど）との間のインタフェースとなる一連のソフトウェア・ルーチンおよび開発ツール。API は、プログラマがソフトウェア・アプリケーション間に連携を構築する際の基盤となる。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、Oracle Internet Directory 情報にアクセスする。

ASN.1

Abstract Syntax Notation One（ASN.1）は、情報データの構文定義に使用される国際電気通信連合（International Telecommunication Union: ITU）の表記規約である。ASN.1 は、構造化された情報、特に通信メディアを介して送受信される情報の記述に使用される。ASN.1 は、インターネット・プロトコルの仕様において幅広く使用されている。

ASR

「**Oracle Database アドバンスト・レプリケーション**」を参照。

Basic 認証（basic authentication）

大半のブラウザによってサポートされる**認証**プロトコル。Web サーバーでは、データ通信時に渡されたエンコード済のユーザー名とパスワードを使用してエンティティが認証される。BASE64 エンコーディングは自由に利用できるデコーディング・ユーティリティを使用して誰でもデコードできるため、Basic 認証は平文認証と呼ばれることもある。エンコーディングと**暗号化**は異なることに注意すること。

BER

「**基本エンコーディング規則**」を参照。

Blowfish

DES にかわる暗号化を迅速に導入する目的で、Bruce Schneier 氏によって 1993 年に開発された**対称型暗号**アルゴリズム。Blowfish は、64 ビット・ブロックと最大 448 ビットの鍵を使用する**ブロック暗号**である。

CA

「**認証局**」を参照。

CA 証明書（CA certificate）

認証局は、自局が発行するすべての証明書を自身の**秘密鍵**で署名する。それに対応する認証局の**公開鍵**は、CA 証明書（またはルート証明書）と呼ばれる証明書の中に含まれる。ブラウザは、CA の秘密鍵によって署名されたメッセージを信頼するには、信頼できるルート証明書リストの中に CA 証明書を保持している必要がある。

CBC

「**暗号ブロック連鎖**」を参照。

Certificate Management Protocol（CMP）

Certificate Management Protocol（CMP）は、証明書の作成と管理に関連するあらゆる局面を取り扱う。CMP では、**認証局**、**登録局**、証明書が発行されたユーザーやアプリケーションなど、**公開鍵インフラストラクチャ**の構成要素間の対話がサポートされる。

Certificate Request Message Format（CRMF）

Certificate Request Message Format（CRMF）は、**X.509** 証明書のライフサイクル管理に関連したメッセージに使用されるフォーマットで、**RFC** 2511 仕様で規定されている。

CMP

「**Certificate Management Protocol**」を参照。

CMS

「**Cryptographic Message Syntax**」を参照。

configset

「**構成設定エントリ**」を参照。

CRL

「**証明書失効リスト**」を参照。

CRMF

「**Certificate Request Message Format**」を参照。

Cryptographic Message Syntax（CMS）

デジタル・メッセージの署名、ダイジェスト、認証および暗号化に使用される構文。**RFC** 3369 で定義される。

dads.conf

データベース・アクセス記述子の構成に使用される、Oracle HTTP Server の構成ファイル。

DAS

「**Oracle Delegated Administration Services**（DAS）」を参照。

Delegated Administration Services

「**Oracle Delegated Administration Services**」を参照。

DER

「**高度なエンコーディング規則**」を参照。

DES

「**データ暗号化規格**」を参照。

DIB

「**ディレクトリ情報ベース**」を参照。

Diffie-Hellman

保護されていないチャネルで通信を行う二者間で共有シークレットを構築することを可能にする公開鍵暗号プロトコル。Diffie-Hellman は 1976 年に公開され、使用可能になった最初の公開鍵暗号システムである。

「**対称型アルゴリズム**」も参照。

Digital Signature Algorithm（DSA）

Digital Signature Standard（DSS）の一部として使用されている**非対称型アルゴリズム**。DSA は暗号化には使用できず、デジタル署名にのみ適用される。このアルゴリズムは 1 組の大きな数を生成することで、署名者の認証と、結果として添付されているデータの整合性を保証する。DSA は、デジタル署名の生成と検証の両方に使用される。

「**Elliptic Curve Digital Signature Algorithm**」も参照。

Directory Manager

「**Oracle Directory Manager**」を参照。

DIS

「**ディレクトリ統合サーバー**」を参照。

DIT

「**ディレクトリ情報ツリー**」を参照。

DN

「**識別名**」を参照。

Document Type Definition（DTD）

特定の **XML** ドキュメントで有効なタグおよびタグの順序に関する制約を指定するドキュメント。DTD は、XML の親言語である Simple Generalized Markup Language（SGML）の規則に準拠する。

DRG

「**ディレクトリ・レプリケーション・グループ**」を参照。

DSA

「**Digital Signature Algorithm（DSA）**」または「**ディレクトリ・システム・エージェント**」を参照。

DSE

「**ディレクトリ固有のエントリ**」を参照。

DTD

「**Document Type Definition**」を参照。

ECC

「**Elliptic Curve Cryptography**」を参照。

ECDSA

「**Elliptic Curve Digital Signature Algorithm**」を参照。

EJB

「**Enterprise JavaBeans**」を参照。

Elliptic Curve Cryptography（ECC）

RSA にかわる暗号化システムで、大きな数の因数分解よりも楕円曲線の離散対数問題の解決の方が困難であることに基づいている。ECC は、Certicom 社によって開発および商品化され、ワイヤレス・デバイスや PC カードのような、制限された演算能力の中で高速が要求される環境に特に適している。ECC は、同じ鍵サイズ（ビット単位）であれば、RSA よりもセキュリティが高い（鍵なしでの復号化がより困難である）。

Elliptic Curve Digital Signature Algorithm（ECDSA）

Elliptic Curve Digital Signature Algorithm（ECDSA）は、**Digital Signature Algorithm（DSA）**標準の楕円曲線版である。RSA 的な方式と比較した ECDSA の利点は、鍵の長さが短く、署名と復号化が高速なことである。たとえば、160 ビットの ECC 鍵は、1024 ビットの RSA 鍵に相当するセキュリティを実現する。210 ビットの ECC 鍵は 2048 ビットの RSA 鍵に相当し、セキュリティ・レベルが高くなるにつれて、この利点が顕著になる。

Enterprise JavaBeans（EJB）

Sun 社によって開発された Java API で、複数層からなるクライアント / サーバー・システムのコンポーネント・アーキテクチャを定義する。EJB システムは Java で記述されているため、プラットフォームに依存しない。オブジェクト指向に基づき、既存システムへの実装には、再コンパイルや構成をほとんどまたはまったく必要としない。

Enterprise Manager

「**Oracle Enterprise Manager**」を参照。

Federal Information Processing Standards（FIPS）

米国商務省の標準技術局（National Institute of Standards and Technology: NIST）によって発行されている情報処理標準。

FIM

「**フェデレーテッド ID 管理**」を参照。

FIPS

「**Federal Information Processing Standards**」を参照。

GET

ログイン資格証明がログイン URL の一部として送信される認証方式。

Global Unique Identifier（GUID）

エントリがディレクトリに追加されると、システムで生成され、エントリに挿入される識別子。マルチマスター・レプリケート環境で、DN ではなく GUID がエントリを一意に識別する。エントリの GUID をユーザーが変更することはできない。

GUID

「**Global Unique Identifier**」を参照。

Hashed Message Authentication Code（HMAC）

ハッシュ関数の 1 つの技法で、秘密のハッシュ関数結果の作成に使用される。MD5 や SHA などの既存のハッシュ関数を強化する。Transport Layer Security（TLS）で使用される。

HMAC

「**Hashed Message Authentication Code**」を参照。

HTTP

Hyper Text Transfer Protocol の略称。Web ブラウザとサーバー間で、ドキュメントのリクエストとその内容の転送に使用されるプロトコル。この仕様は、World Wide Web Consortium によって維持および開発される。

HTTP Server

「**Oracle HTTP Server**」を参照。

httpd.conf

Oracle HTTP Server の構成に使用されるファイル。

HTTP リダイレクト・プロファイル（HTTP Redirect Profile）

リクエストされたリソースが別の URL にあることを示す**フェデレーション**・プロファイル。

iASAdmins

Oracle Application Server で、ユーザーとグループの管理に責任を持つ管理グループ。OracleAS Single Sign-On 管理者は、iASAdmins グループのメンバーである。

ID 管理（identity management）

組織でネットワーク・エンティティのセキュリティ・ライフ・サイクル全体を管理するプロセス。通常、組織のアプリケーション・ユーザーの管理を指す。セキュリティ・ライフ・サイクルの手順には、アカウント作成、一時停止、権限変更およびアカウント削除が含まれる。管理されるネットワーク・エンティティには、デバイス、プロセス、アプリケーション、またはネットワーク環境で対話する必要があるその他のすべてのものが含まれる。ID 管理プロセスで管理されるエンティティには、組織外のユーザー（顧客、取引先、Web サービスなど）も含まれる。

ID 管理インフラストラクチャ・データベース（identity management infrastructure database）

OracleAS Single Sign-On と Oracle Internet Directory のデータを保持するデータベース。

ID 管理レルム（identity management realm）

すべてが同じ管理ポリシーによって管理されている識別情報の集合。企業では、イントラネットへのアクセス権限を所有しているすべての従業員は 1 つのレルムに属し、企業の公開アプリケーションにアクセスするすべての外部ユーザーは別のレルムに属する。ID 管理レルムは、特別な**オブジェクト・クラス**が関連付けられた特定の**エントリ**でディレクトリ内に表される。

ID 管理レルム固有の Oracle コンテキスト（identity management realm-specific Oracle Context）

各 ID 管理レルムに含まれた Oracle コンテキスト。これには、次の情報が格納されている。

- ID 管理レルムのユーザー・ネーミング・ポリシー（ユーザーに名前を付け、配置する方法）
- 必須認証属性
- ID 管理レルム内のグループの位置
- ID 管理レルムに対する権限の割当て（レルムにユーザーを追加する権限の割当てなど）
- レルムに関するアプリケーション固有のデータ（認可など）

ID フェデレーション（identity federation）

プリンシパルが、1 つの特定の**トラスト・サークル**内で 1 つ以上の ID プロバイダまたはサービス・プロバイダと保持できる、複数アカウントのリンク。

ユーザーは、取引のある他の単独アカウント（ローカル ID）と連携するとき、2 つのエンティティで関係（任意の数のサービス・プロバイダと ID プロバイダで構成される連合）を築く。

「**ID プロバイダ**」、「**サービス・プロバイダ**」も参照。

ID プロバイダ（identity provider）

OSFS によりサポートされる **ID フェデレーション**プロトコルで定義されている 3 つの主要ロールの 1 つ。他の主要ロールは**サービス・プロバイダ**と**プリンシパル**。ID プロバイダは、特定の**トラスト・サークル**内で ID の管理および認証を担当する。

サーバー・プロバイダは、ID プロバイダのプリンシパルに対する ID 認証に基づき、プリンシパルにサービスや商品を提供する。

ID プロバイダは、ビジネスを奨励するサービス・プロバイダであり、他のサービス・プロバイダは ID プロバイダと提携する。ID プロバイダは通常、プリンシパルの認証とアサーションを行う。

Internet Directory

「**Oracle Internet Directory**」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。

J2EE

「**Java 2 Platform, Enterprise Edition**」を参照。

Java 2 Platform, Enterprise Edition（J2EE）

Sun 社によって定義された、エンタープライズ・アプリケーションを開発および配置するための環境。J2EE プラットフォームは、複数層にわたる Web ベース・アプリケーションを開発する機能を提供するサービス、Application Program Interface（API）およびプロトコルのセットで構成される。

JavaServer Pages（JSP）

JavaServer Pages（JSP）はサーバー側のテクノロジで、Sun 社によって開発された Java サーブレット・テクノロジに対する拡張である。JSP には、HTML コードと連携して動作する動的なスクリプティング機能があり、それによってページ・ロジックが静的要素（ページの設計と表示）から分離される。Java ソース・コードとその拡張機能が HTML ページに埋め込まれることで、HTML がより機能的になり、データベースへの動的な問合せなどに使用される。

JSP

「**JavaServer Pages**」を参照。

LDAP

「**Lightweight Directory Access Protocol**」を参照。

LDAP Data Interchange Format（LDIF）

システム間でディレクトリ・データを交換するためのテキストベースの共通フォーマット。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。

LDAP 接続キャッシュ（LDAP connection cache）

スループットを向上させるために、OracleAS Single Sign-On サーバーが、Oracle Internet Directory への接続をキャッシュして再利用すること。

LDIF

「**LDAP Data Interchange Format**」を参照。

Liberty Alliance

Liberty Alliance Project は、世界中の 150 を超える企業、非営利団体および政府機関からなるアライアンスである。このコンソーシアムは、現在および将来のあらゆるネットワーク・デバイスでサポートされるフェデレーテッド・ネットワーク ID のオープン・スタンダードの開発に従事する。Liberty Alliance は、**フェデレーテッド ID 管理**に関するオープンなテクノロジ標準、プライバシ保護およびビジネス・ガイドラインの定義および推進作業を行う、唯一のグローバル団体である。

Liberty ID-FF

Liberty Identity Federation Framework（Liberty ID-FF）は、フェデレーテッド ID による Web ベースの**シングル・サインオン**のアーキテクチャを提供する。

Lightweight Directory Access Protocol（LDAP）

ディレクトリ内の情報にアクセスするための 1 組のプロトコル。LDAP では、あらゆるタイプのインターネット・アクセスに必要な TCP/IP がサポートされる。また、その設計規則のフレームワークによって、Oracle Internet Directory などの業界標準のディレクトリ製品がサポートされる。これは **X.500** 標準の簡易版であるため、LDAP は X.500 Light と呼ばれることもある。

MAC

「**メッセージ認証コード**」を参照。

MD2

Message Digest Two の略称。メッセージ・ダイジェストを作成する**ハッシュ関数**。このアルゴリズムは入力テキストを処理し、元のメッセージに対して固有でデータの整合性検証に使用できる 128 ビットの**メッセージ・ダイジェスト**を作成する。MD2 は、RSA Security 社の Ron Rivest 氏によって開発され、スマート・カードなどの、メモリーが限られるシステムでの使用が意図されている。

MD4

Message Digest Four の略称。**MD2** と類似するが、ソフトウェアでの高速処理に特化して設計されている。

MD5

Message Digest Five の略称。メッセージ・ダイジェストを作成する**ハッシュ関数**。このアルゴリズムは入力テキストを処理し、元のメッセージに対して固有でデータの整合性検証に使用できる 128 ビットの**メッセージ・ダイジェスト**を作成する。MD5 は、**MD4** の潜在的な脆弱さが報告された後、Ron Rivest 氏によって開発された。MD5 は MD4 と類似するが、元のデータに対してより多くの処理を行うため速度は遅い。

MDS

「**マスター定義サイト**」を参照。

mod_osso

Oracle HTTP Server のモジュール。ユーザーが OracleAS Single Sign-On サーバーにログイン後、OracleAS Single Sign-On によって保護されたアプリケーションが、ユーザー名とパスワードのかわりに HTTP ヘッダーを受け入れることを可能にする。HTTP ヘッダーの値は **mod_osso Cookie** に格納される。

mod_osso Cookie

HTTP サーバー上に格納されるユーザー・データ。この Cookie は、ユーザー認証時に作成される。同じユーザーが別のアプリケーションをリクエストすると、Web サーバーは mod_osso Cookie にある情報を使用して、アプリケーションへのユーザーのログインを許可する。この機能によって、サーバーのレスポンス時間が速くなる。

mod_proxy

Oracle HTTP Server のモジュール。**mod_osso** を使用して、レガシー・アプリケーションまたは**外部アプリケーション**へのシングル・サインオンを可能にする。

MTS

「**共有サーバー**」を参照。

Net Services

「**Oracle Net Services**」を参照。

OASIS

Organization for the Advancement of Structured Information Standards の略称。E-Business 標準の開発、策定および採用を推進する国際的な非営利組織。

OC4J

「**Oracle Containers for J2EE**」を参照。

OCA

「**Oracle Certificate Authority**」を参照。

OCI

「**Oracle Call Interface**」を参照。

OCSP

「**Online Certificate Status Protocol**」を参照。

OEM

「**Oracle Enterprise Manager**」を参照。

OID

「**Oracle Internet Directory**」を参照。

OID 制御ユーティリティ（OID Control Utility）

サーバーの起動と停止のコマンドを発行するコマンドライン・ツール。コマンドは、**OID モニター**のプロセスによって解析され、実行される。

OID データベース・パスワード・ユーティリティ（OID Database Password Utility）

Oracle Internet Directory が Oracle Database 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 Internet Directory 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 Platform サーバーの制御も行う。

Online Certificate Status Protocol（OCSP）

デジタル証明書の有効性確認において、広く使用されている 2 つの方式のうちの 1 つ。もう 1 つの方式の**証明書失効リスト**は OCSP よりも古く、使用シナリオによっては OCSP に置き換えられている。OCSP 仕様は **RFC** 2560 で規定されている。

Oracle Application Server Single Sign-On

OracleAS Single Sign-On は、複数のアプリケーション（経費報告、メール、各種手当て申請など）に対する安全なログインを実現するプログラム・ロジックで構成される。これらのアプリケーションには、**パートナ・アプリケーション**と**外部アプリケーション**の 2 つの形態がある。どちらの場合も、ユーザーは 1 度の認証で複数のアプリケーションにアクセス可能となる。

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 Database・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 Certificate Authority

Oracle Application Server 環境内で使用される**認証局**。OracleAS Certificate Authority では、証明書の格納リポジトリとして Oracle Internet Directory が使用される。OracleAS Certificate Authority を OracleAS Single Sign-On および Oracle Internet Directory と統合することで、これらに依存するアプリケーションに対する透過的な証明書プロビジョニング・メカニズムが実現される。Oracle Internet Directory にプロビジョニングされ OracleAS Single Sign-On で認証されるユーザーは、OracleAS Certificate Authority にデジタル証明書をリクエストできる。

Oracle CMS

IETF **Cryptographic Message Syntax** プロトコルのオラクル社による実装。CMS は、セキュアなメッセージ・エンベロープを実現するデータ保護方式を定義する。

Oracle Containers for J2EE（OC4J）

Java 2 Platform, Enterprise Edition 用の軽量でスケーラブルなコンテナ。

Oracle Crypto

コアな暗号化アルゴリズムを提供する Pure Java ライブラリ。

Oracle Database アドバンスト・レプリケーション（Oracle Database Advanced Replication）

2 つの Oracle データベース間で、データベースの表を継続的に同期化できる Oracle Database の機能。

Oracle Delegated Administration Services

Oracle Delegated Administration Services ユニットと呼ばれる個々の事前定義済サービスのセットで、ユーザーのかわりにディレクトリ操作を実行する。Oracle Internet Directory セルフ・サービス・コンソールによって、Oracle Internet Directory を使用する Oracle アプリケーションおよびサード・パーティ・アプリケーションの両方の管理ソリューションを容易に開発および配布できる。

Oracle Directory Integration Platform

インタフェースとサービスの集合で、Oracle Internet Directory といくつかの関係するプラグインやコネクタを使用して複数のディレクトリを統合する。外部のユーザー・リポジトリが使用されている場合に、そこから Oracle 製品への認証を可能にする Oracle Internet Directory の機能。

Oracle Directory Integration Platform

Oracle Internet Directory のコンポーネントの 1 つ。Oracle Internet Directory のような中央 LDAP ディレクトリの周囲のアプリケーションを統合するために開発されたフレームワーク。

Oracle Directory Manager

Oracle Internet Directory を管理するための、Graphical User Interface（GUI）を備えた Java ベースのツール。

Oracle Enterprise Manager

Oracle 製品の 1 つ。グラフィカルなコンソール、エージェント、標準的なサービスおよびツールを組合せ、Oracle 製品を管理するための統合された包括的なシステム管理プラットフォームを提供する。

Oracle HTTP Server

Hypertext Transfer Protocol（HTTP）を使用する Web トランザクションを処理するソフトウェア。Apache Group によって開発された HTTP ソフトウェアが使用されている。

Oracle Identity Management

すべての企業識別情報および企業内の様々なアプリケーションへのアクセスを集中的かつ安全に管理するための配置を可能にするインフラストラクチャ。

Oracle Internet Directory

分散ユーザーやネットワーク・リソースに関する情報の検索を可能にする、一般的な用途のディレクトリ・サービス。**Lightweight Directory Access Protocol** バージョン 3 と Oracle Database のすぐれたパフォーマンス、スケーラビリティ、耐久性および可用性を組み合せたもの。

Oracle Liberty SDK

Liberty Alliance Project 仕様のオラクル社による実装。サード・パーティ製の Liberty 準拠アプリケーション間で、フェデレーテッド・シングル・サインオンを可能にする。

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 SDK

公開鍵インフラストラクチャ実装内で必要なセキュリティ・プロトコルのオラクル社による実装。

Oracle PKI 証明書使用条件（Oracle PKI certificate usages）

証明書でサポートされる Oracle アプリケーション・タイプを定義する。

Oracle S/MIME

Internet Engineering Task Force が発行するセキュアな電子メールに関する **Secure/Multipurpose Internet Mail Extension** 仕様のオラクル社による実装。

Oracle SAML

異種システムおよびアプリケーション間でセキュリティ資格証明を、XML ベースのフォーマットで交換するためのフレームワークを提供する。**Security Assertions Markup Language** に関する **OASIS** 仕様に基づく。

Oracle Security Engine

X.509 ベースの証明書管理機能を組み込んだ、Oracle Crypto の拡張。Oracle Security Engine は、Oracle Crypto のスーパーセットである。

Oracle Wallet Manager

セキュリティ管理者が、クライアントとサーバー上での公開鍵セキュリティ資格証明の管理に使用する Java ベースのアプリケーション。

『Oracle Advanced Security 管理者ガイド』も参照。

Oracle Web Services Security

既存のセキュリティ・テクノロジを使用して認証および認可を行うためのフレームワークを提供する。Web サービス・セキュリティに関する **OASIS** 仕様に基づく。

Oracle XML Security

XML 暗号化および XML 署名に関する W3C 仕様のオラクル社による実装。

OracleAS Portal

ファイル、イメージ、アプリケーションおよび Web サイトを統合するメカニズムを提供する OracleAS Single Sign-On **パートナ・アプリケーション**。External Applications ポートレットは、外部アプリケーションへのアクセスを提供する。

Oracle コンテキスト（Oracle Context）

「**ID 管理レルム固有の Oracle コンテキスト**」および「**ルート Oracle コンテキスト**」を参照。

Oracle ディレクトリ統合サーバー（Oracle Directory Integration Server）

Oracle Directory Integration Platform 環境で、Oracle Internet Directory の変更イベントを監視し、**ディレクトリ統合プロファイル**の情報に基づいてアクションを行うデーモン・プロセス。

OWM

「**Oracle Wallet Manager**」を参照。

peer-to-peer レプリケーション（peer-to-peer replication）

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

PKCS#1

公開鍵暗号規格（PKCS）とは、RSA Laboratories によって策定された仕様のこと。PKCS#1 は、RSA アルゴリズムをベースとした公開鍵暗号の実装に関する推奨事項を定めている。この内容には、暗号化の基本から、暗号化方式、署名方式、鍵の表記や各種方式の識別に使用する ASN.1 構文までが含まれる。

PKCS#10

公開鍵暗号規格（PKCS）とは、RSA Laboratories によって策定された仕様のこと。PKCS #10 は、公開鍵、名前および一連の可能な属性の証明リクエストに関する構文を定めている。

PKCS#12

公開鍵暗号規格（PKCS）とは、RSA Laboratories によって策定された仕様のこと。PKCS #12 は、個人の識別情報（秘密鍵、証明書、その他の秘密情報、拡張項目など）の伝送に関する構文を定めている。この標準をサポートするシステム（ブラウザやオペレーティング・システムなど）を使用するユーザーは、主に **Wallet** と呼ばれるフォーマットによって、1 組の個人用識別情報をインポート、エクスポートおよび利用できる。

PKCS#5

公開鍵暗号規格（PKCS）とは、RSA Laboratories によって策定された仕様のこと。PKCS#5 は、パスワードをベースとした暗号化の実装に関する推奨事項を定めている。

PKCS#7

公開鍵暗号規格（PKCS）とは、RSA Laboratories によって策定された仕様のこと。PKCS #7 は、デジタル署名やデジタル・エンベロープなどの、暗号化が適用されるデータに関する汎用構文を定めている。

PKCS#8

公開鍵暗号規格（PKCS）とは、RSA Laboratories によって策定された仕様のこと。PKCS #8 は、公開鍵と秘密鍵の対応付けアルゴリズムや一連の属性などの、秘密鍵情報に関する構文を定めている。この標準は、暗号化された秘密鍵に関する構文も定めている。

PKI

「**公開鍵インフラストラクチャ**」を参照。

point-to-point レプリケーション

ファンアウト・レプリケーション（fan-out replication）とも呼ばれる。サプライヤがコンシューマに直接レプリケートするレプリケーションのタイプ。そのコンシューマは、1 つ以上の別のコンシューマにレプリケートできます。レプリケーションには、完全レプリケーションと部分レプリケーションがあります。

policy.properties

シングル・サインオン・サーバーに必要な基本パラメータが含まれる、Oracle Application Server Single Sign-On の多目的構成ファイル。OracleAS Single Sign-On が持つマルチレベル認証などの高度な機能を構成する際にも使用される。

POSIX

Portable Operating System Interface for UNIX の略称。アプリケーションのソース・コードの記述方法を決めることで、異なるオペレーティング・システム間でのアプリケーションの移植を可能にするプログラミング・インタフェース標準のセット。この標準セットは、**Internet Engineering Task Force** によって開発されている。

POST プロファイル（POST Profile）

ログイン資格証明がログイン・フォームのボディ内で送信される**認証**方式。

Project Liberty

「**Liberty Alliance**」を参照。

RC2

Rivest Cipher Two の略称。RSA Security 社の Ronald Rivest 氏によって開発された 64 ビット**ブロック暗号**で、**データ暗号化規格**に置き換える目的で設計された。

RC4

Rivest Cipher Four の略称。RSA Security 社の Ronald Rivest 氏によって開発された**ストリーム暗号**。RC4 では、最大 1024 ビットの可変長の鍵を使用できる。RC4 は、**Secure Sockets Layer** プロトコルを使用する Web サイト間で通信を暗号化することによってデータ伝送を保護する際に、最も幅広く使用されている。

RDN

「**相対識別名**」を参照。

RFC

Internet Request For Comments とも呼ばれる。インターネット関連のプロトコルとポリシーの定義が記述されたドキュメント。Internet Engineering Task Force（IETF）が、新しい標準の討議、開発および構築を進めている。標準は、RFC という頭字語とリファレンス番号を使用して公開される。たとえば、電子メールの公式標準は RFC 822 である。

RSA

公開鍵暗号アルゴリズムの名前で、その考案者（Rivest、Shamir および Adelman の 3 氏）から名付けられた。RSA アルゴリズムは、最も幅広く使用されている暗号化 / 認証アルゴリズムで、Netscape 社および Microsoft 社の Web ブラウザや、他の多くの製品の一部として組み込まれている。

RSAES-OAEP

RSA Encryption Scheme - Optimal Asymmetric Encryption Padding の略称。**RSA** アルゴリズムと OAEP 方式を組み合せた公開鍵暗号化方式。Optimal Asymmetric Encryption Padding（OAEP）は、Mihir Bellare と Phil Rogaway の 2 氏によって開発されたメッセージ・エンコーディング方式である。

S/MIME

「**Secure/Multipurpose Internet Mail Extension**」を参照。

SAML

「**Security Assertions Markup Language**」を参照。

SASL

「**Simple Authentication and Security Layer**」を参照。

Secure Hash Algorithm（SHA）

入力に基づいて 160 ビットの**メッセージ・ダイジェスト**を生成する**ハッシュ関数**アルゴリズム。このアルゴリズムは、Digital Signature Standard（DSS）で使用されている。128、192、256 ビットの 3 通りの鍵サイズを提供する Advanced Encryption Standard（AES）の導入によって、それらに対応する同レベルのセキュリティを持つハッシュ・アルゴリズムが必要となっている。より新しい SHA-256、SHA-284 および SHA-512 ハッシュ・アルゴリズムは、これらの拡張要件を満たしている。

Secure Sockets Layer（SSL）

ネットワーク（インターネットなど）経由での暗号化および認証された通信を実現するために、Netscape 社によって設計されたプロトコル。SSL では、RSA 社の**公開鍵暗号**システムが使用され、デジタル証明書の使用も組み込まれている。SSL では、セキュアな通信の 3 要素である**機密保護**、**認証**および**整合性**が実現される。

SSL は **Transport Layer Security** へと発展している。TLS と SSL は、相互運用できない。ただし、TLS で送信されたメッセージは、SSL を処理するクライアントで処理できる。

Secure/Multipurpose Internet Mail Extension（S/MIME）

デジタル署名と**暗号化**を使用した MIME データの保護に関する Internet Engineering Task Force（IETF）の標準。

Security Assertions Markup Language（SAML）

XML ベースのフレームワーク。アクセス制御の決定を下すために使用される、サブジェクトに関するアサーションを作成することにより、サブジェクトに関するセキュリティ情報交換のメカニズムを定義する。SAML は、ID プロバイダとサービス・プロバイダ間での**認証**および**認可**情報の交換を可能にする。これがなければ、両プロバイダは相互運用できない。

SAML 2.0 は、標準の主要改訂版。SAML1 を更新したもので、Shibboleth と **Liberty ID-FF** の両仕様の入力情報がまとめられている。SAML 2.0 の重要な点は、2 つのサイトが 1 人のユーザーの識別子を、そのユーザーの協力を得て、確立および保守できる機能。その他の機能として、プライバシ・メカニズムと、グローバル・ログアウトのサポートがある。

SGA

「**システム・グローバル領域**」を参照。

SHA

「**Secure Hash Algorithm**」を参照。

Signed Public Key And Challenge（SPKAC）

Netscape Navigator ブラウザが証明書のリクエストに使用する固有のプロトコル。

Simple Authentication and Security Layer（SASL）

アプリケーション・プロトコルに**認証**および**認可**の機能を追加する方法。プロトコルと接続の間にセキュリティ・レイヤーを提供し、ユーザーのサーバーに対する認証を可能にする。セキュリティ・レイヤーは、後続のプロトコルの対話を保護するために取り決めることもできる。

Simple Object Access Protocol（SOAP）

XML ベースのプロトコルで、インターネットを介してシステム間でメッセージを送受信するためのフレームワークを定義する。Web サービス用の共通プロトコル SOAP は、HTTP や FTP などの転送プロトコルとともに使用される。SOAP メッセージは 3 つの部分からなる。1 つは、メッセージとその処理方法が記述されたエンベロープで、残りは、アプリケーションで定義されたデータ型のインスタンスを表現するための 1 組のエンコーディング規則と、リモート・プロシージャ・コールおよびレスポンスの表記規則である。

SLAPD

スタンドアロンの LDAP デーモン。レプリケーションを除くディレクトリの大半の機能を担当する LDAP ディレクトリ・サーバー・サービス。

SOAP

「**Simple Object Access Protocol**」を参照。

SPKAC

「**Signed Public Key And Challenge**」を参照。

SSL

「**Secure Sockets Layer**」を参照。

SSO

「**シングル・サインオン**」を参照。

subACLSubentry

アクセス制御リスト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**。

Time Stamp Protocol（TSP）

RFC 3161 で規定されるプロトコル。デジタル・メッセージのタイムスタンプに関する参加エンティティ、メッセージ形式および転送プロトコルが定義される。TSP システムでは、信頼できる第三者機関である時刻認証局（TSA）によって、メッセージのタイムスタンプが発行される。

TLS

「**Transport Layer Security**」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。

Triple Data Encryption Standard（3DES）

IBM 社によって 1974 年に開発された**データ暗号化規格**に基づく暗号化アルゴリズム。1977 年に米国の連邦標準として採用されている。3DES では、64 ビットの鍵が 3 つ使用される（鍵の長さは全体で 192 ビットになるが、実際の鍵長は 56 ビットである）。データは、第一の鍵で暗号化され、第二の鍵で復号化され、さらに第三の鍵で再度暗号化される。結果として、3DES は標準的な DES よりも 3 倍低速になるが、3 倍セキュアになる。

TSP

「**Time Stamp Protocol**」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。

URI

Uniform Resource Identifier の略称。Web 上にある、あらゆるコンテンツ（テキスト・ページ、ビデオ・クリップ、サウンド・クリップ、静止画、動画、プログラムなど）の位置を識別する手段。最も一般的な URI は Web ページ・アドレスで、**URL** と呼ばれる、URI の特別な形式つまりサブセットで構成される。

URL

Uniform Resource Locator の略称。インターネット上にあるアクセス可能なファイルのアドレス。テキスト・ファイル、HTML ページ、画像ファイル、プログラムなど、HTTP でサポートされるすべてのファイルが対象となる。URL には、リソースへのアクセスに必要なプロトコルの名前、インターネット上の特定のコンピュータを識別するドメイン名、およびコンピュータ上のファイル場所の階層的な記述が含まれる。

URLC トークン（URLC token）

認証済のユーザー情報を**パートナ・アプリケーション**に渡す OracleAS Single Sign-On コード。パートナ・アプリケーションは、この情報を使用してセッション Cookie を作成する。

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。

Wallet Manager

「**Oracle Wallet Manager**」を参照。

Web Services Description Language（WSDL）

XML を使用して Web サービスを定義するための標準形式。WSDL 定義には、Web サービスへのアクセス方法と、それを使用して実行できる操作が記述される。

Web サービス（Web service）

HTTP、**XML**、**SOAP** などの標準的なインターネット・プロトコルを使用してアクセスできるアプリケーションまたはビジネス・ロジック。Web サービスでは、コンポーネントベース開発と World Wide Web の両者が持つ優れた利点が結び付けられている。Web サービスは、コンポーネントと同様、サービスの実装方法を知らなくても使用または再利用できるブラックボックス機能を実現する。

WS-Federation

Web Services Federation Language のこと。Microsoft、IBM、BEA、VeriSign および RSA Security 社によって開発された仕様。WS-Federation は、異種または同種の方式を使用するエンティティ間で、**フェデレーション**を構築可能にするメカニズムを定義する。これは、公開されている **Web サービス**間で、識別情報、属性および認証の信頼性を確立および仲介することで実現される。

「**Liberty Alliance**」も参照。

WSDL

「**Web Services Description Language**」を参照。

X.500

グローバル・ディレクトリの構造化方法を定義する、国際電気通信連合（ITU）の標準。X.500 ディレクトリは、国、都道府県、市町村などの情報カテゴリごとに異なるレベルを持つ階層である。

X.509

デジタル証明書の定義において、最も幅広く使用されている標準。これは、認証サービスが備わった階層型ディレクトリに関する国際電気通信連合（ITU）の標準で、多くの**公開鍵インフラストラクチャ**実装で使用されている。

XML

eXtensible Markup Language の略称。World Wide Web Consortium（W3C）によって開発された仕様。XML は、Standard Generalized Mark-Up Language（SGML）の縮小版で、Web ドキュメントに特化して設計されている。XML はメタ言語（タグ・セットを定義する方法）で、開発者はこれによって、様々な種類のドキュメントに対して独自にカスタマイズしたマークアップ言語を定義できる。

XML 正規化（XML canonicalization: XML C14N）

論理的に同等な 2 つの XML ドキュメントを同じ物理表現に解決するプロセス。署名はデータが最初に計算処理されたときの物理表現に対してのみ検証可能なため、XML 正規化はデジタル証明において重要となる。詳細は、W3C の XML 正規化仕様を参照。

アーティファクト・プロファイル（artifact profile）

完全なアサーションを送信するかわりに、**アサーション**に対するコンパクトな参照（アーティファクト）を使用してデータを送信する**認証**メカニズム。この**プロファイル**は、限られた数の文字を処理するブラウザに対応。

アカウント・ロックアウト（account lockout）

指定された時間内にログオン試行に繰り返し失敗した場合に、セキュリティ・ポリシーの設定に基づいてユーザー・アカウントをロックするセキュリティ機能。OracleAS Single Sign-On では、ユーザーがアカウントとパスワードの組合せを、任意の数のワークステーションから Oracle Internet Directory によって許可されている回数を超えて発行するとアカウント・ロックアウトが適用される。デフォルトのロックアウト期間は 24 時間。

アクセス制御情報項目（Access Control Information Item: ACI）

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、各属性はアクセス制御情報項目（ACI）と呼ばれる。ACI は、ディレクトリ・データへのユーザー・アクセス権限を決定する。ACI には、エントリ（構造型アクセス項目）と属性（コンテンツ・アクセス項目）へのアクセス権限を制御するための一連の規則が含まれる。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）

ディレクトリ情報ツリー内のすべての下位エントリに適用されるアクセス制御ポリシー情報を含むディレクトリ・エントリ。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る。Oracle Internet Directory では、ACP を作成することで、ディレクトリ内の**サブツリー**全体にアクセス制御ポリシーを適用できる。

アクセス制御リスト（Access Control List: ACL）

コンピュータ・システム内のリソースと、それらのリソースへのアクセスを許可されたユーザーのユーザー名からなるリスト。Oracle Internet Directory では、ACL は、ディレクトリ・オブジェクトに関連付けられた**アクセス制御情報項目**の**属性値**のリストである。このリストの属性値は、様々なディレクトリ・ユーザー・エンティティ（サブジェクト）が各オブジェクトに対して所有している権限を表す。

アサーション（assertion）

プロバイダがセキュリティ・ドメインにおいて、リソースへのアクセスを求めるサブジェクトに関する情報を交換するために使用する文。サービス・プロバイダ同様、ID プロバイダも、**認証**および**認可**の決定を下し、リソースを保護するセキュリティ・ポリシーを決定し、適用するために、ID に関するアサーションを交換する。

アドバンスト・レプリケーション（Advanced Replication: AR）

「**Oracle Database アドバンスト・レプリケーション**」を参照。

アプリケーション・サービス・プロバイダ（application service provider）

ソフトウェアベースのサービスやソリューションの管理および配信を、中央のデータ・センターから Wide Area Network を通じて顧客に提供するサード・パーティ・エンティティ。つまり、アプリケーション・サービス・プロバイダ（ASP）は、企業が必要とする情報技術の一部またはすべてをアウトソースする手段となる。

暗号（cipher）

「暗号化アルゴリズム」を参照。

暗号化（cryptography）

情報を判読できない形式に変換することによって保護する処理。情報は、データを判読不能にする**鍵**を使用して暗号化され、情報が再度必要になったときに復号化される。「**公開鍵暗号**」および「**対称型暗号**」も参照。

暗号化（encryption）

暗号化アルゴリズムを適用することで、平文を暗号文に変換する処理。

暗号化アルゴリズム（cryptographic algorithm）

判読可能なデータ（平文）を判読できないデータ（暗号文）に変換する、またはその逆を行うために定義された一連の処理手順。これらの変換には特別なシークレット情報が必要で、通常、それらは**鍵**に含まれる。暗号化アルゴリズムには、**DES**、**AES**、**Blowfish**、**RSA** などがある。

暗号化証明書（encryption certificate）

電子メッセージ、ファイル、ドキュメントまたはデータ伝送の暗号化や、同じ目的のセッション鍵の交換または確立に使用される**公開鍵**を含む**証明書**。

暗号スイート（cipher suite）

Secure Sockets Layer 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暗号スイートを確認する。

暗号ブロック連鎖（Cipher Block Chaining: CBC）

ブロック暗号の操作モードの 1 つ。CBC では、初期設定ベクトル（IV）と呼ばれる特定長のベクトル値が使用される。CBC の最も重要な特性の 1 つは、連鎖メカニズムによって、特定の暗号文ブロックの復号化が、それよりも前のすべての暗号文ブロックに依存することにある。結果として、1 つ前の暗号文ブロックには、それよりも前のすべてのブロックの全体としての妥当性が含まれることになる。

暗号文（ciphertext）

判読可能なデータ（平文）に**暗号化アルゴリズム**を適用することで、適切な**鍵**の所有者以外は誰も判読できないデータに変換したもの。

一方向関数（one-way function）

一方向への計算は容易だが、逆の計算（反対方向への計算）は非常に難しい関数。

一方向ハッシュ関数（one-way hash function）

可変サイズの入力を取得して、固定サイズの出力を作成する**一方向関数**。

「**ハッシュ関数**」も参照。

一致規則（matching rule）

検索または比較操作における、検索対象の属性値と格納されている属性値との間の等価性の判断。たとえば、`telephoneNumber` 属性に関連付けられた一致規則では、(650) 123-4567 を (650) 123-4567 または 6501234567 のいずれか、あるいはその両方と一致させることができる。**属性**の作成時に、その属性を一致規則と対応付けることができる。

委任管理者（delegated administrator）

ホスティングされた環境では、アプリケーション・サービス・プロバイダなどの 1 企業が、他の複数の企業に Oracle コンポーネントを使用可能にして、その情報を格納する。この種の環境では、グローバル管理者はディレクトリ全体にまたがるアクティビティを実行する。委任管理者と呼ばれる他の管理者は、特定の ID 管理レルムでのロール、または特定のアプリケーションに対してのロールを持つ。

インスタンス（instance）

「**ディレクトリ・サーバー・インスタンス**」を参照。

インフラストラクチャ層（infrastructure tier）

ID 管理を担当する Oracle Application Server コンポーネント。OracleAS Single Sign-On、Oracle Delegated Administration Services および Oracle Internet Directory が、このコンポーネントに該当する。

インポート・エージェント（import agent）

Oracle Directory Integration Platform 環境で、Oracle Internet Directory にデータをインポートするエージェント。

インポート・データ・ファイル（import data file）

Oracle Directory Integration Platform 環境で、**インポート・エージェント**によってインポートされたデータを格納するファイル。

エクスポート・エージェント（export agent）

Oracle Directory Integration Platform 環境で、Oracle Internet Directory からデータをエクスポートするエージェント。

エクスポート・データ・ファイル（export data file）

Oracle Directory Integration Platform 環境で、**エクスポート・エージェント**によってエクスポートされたデータを格納するファイル。

エクスポート・ファイル（export file）

「**エクスポート・データ・ファイル**」を参照。

エンドツーエンド・セキュリティ（end-to-end security）

メッセージレベルのセキュリティによって実現される特性。ビジネス・エンティティ内およびビジネス・エンティティ間の複数のアプリケーションでメッセージが伝送処理されるときに、それらのあらゆる経路でメッセージがセキュアである場合に確立される。

エントリ（entry）

ユーザーなどのオブジェクトを表す、ディレクトリ内の一意なレコード。エントリは**属性**とそれに関連付けられた**属性値**で構成され、それらはエントリ・オブジェクトを定義する**オブジェクト・クラス**によって規定される。LDAP ディレクトリ構造内のすべてのエントリは、その**識別名**によって一意に識別される。

オブジェクト・クラス（object class）

LDAP において、情報のグループ化に使用される。通常、オブジェクト・クラスは、従業員やサーバーなどの実社会の事物をモデル化する。各ディレクトリ・エントリは、1 つ以上のオブジェクト・クラスに属する。オブジェクト・クラスは、エントリを構成する属性を決定する。オブジェクト・クラスは別のオブジェクト・クラスから導出でき、結果として、他のクラスの特性が継承される。

介在者（man-in-the-middle）

第三者によるメッセージの不正傍受などのセキュリティ攻撃。第三者、つまり介在者は、メッセージを復号化して再暗号化し（元のメッセージを変更する場合と変更しない場合がある）、元のメッセージの宛先である受信者に転送する。これらの処理はすべて、正当な送受信者が気付かないうちに行われる。この種のセキュリティ攻撃は、**認証**が行われていない場合にのみ発生する。

外部アプリケーション（external application）

OracleAS Single Sign-On サーバーに認証を委任しないアプリケーション。かわりに、アプリケーション・ユーザー名とパスワードの入力を求める HTML ログイン・フォームが表示される。ユーザーは、最初のログイン時に OracleAS Single Sign-On サーバーで自身の資格証明を取得するように選択できる。以降は、それらのアプリケーションに透過的にログインできる。

外部エージェント（external agent）

Oracle Directory Integration Platform サーバーに依存しないディレクトリ統合エージェント。Oracle Directory Integration Platform サーバー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）

特定のデータ・ブロックの暗号化と復号化の成功に必要なシークレット情報を含むデータ構造。鍵のサイズが大きくなるにつれて、暗号化されたデータ・ブロックのクラッキングは困難になる。たとえば、256 ビットの鍵は 128 ビットの鍵よりも安全である。

鍵のペア（key pair）

公開鍵とそれに対応する**秘密鍵**のペア。

「**公開鍵と秘密鍵のペア**」も参照。

仮想 IP アドレス（virtual IP address）

Oracle Application Server Cold Failover Cluster（Identity Management）では、各物理ノードに独自の物理 IP アドレスと物理ホスト名がある。単一のシステムであるというイメージを外部に示すために、クラスタは、クラスタ内のどの物理ノードにも変更できる動的 IP アドレスを使用する。これは、仮想 IP アドレスと呼ばれる。

仮想ホスト（virtual host）

1 つ以上の Web サイトまたはドメインをホスティングする 1 台の物理的な Web サーバー・マシン、または他のマシンに対するプロキシ（受信リクエストを受け取り、それらを適切なサーバーにルーティングする）としての機能を持つサーバー。

OracleAS Single Sign-On では、仮想ホストは、2 つ以上の OracleAS Single Sign-On サーバー間でのロード・バランシングに使用される。仮想ホストは、セキュリティ対策用の追加層ともなる。

仮想ホスト名（virtual host name）

Oracle Application Server Cold Failover Cluster（Identity Management）で、特定の仮想 IP アドレスに対応するホスト名。

簡易認証（simple authentication）

ネットワークでの送信時に暗号化されない識別名とパスワードを使用して、クライアントがサーバーに対して自己認証を行うプロセス。簡易認証オプションでは、クライアントが送信した識別名とパスワードと、ディレクトリに格納されている識別名とパスワードが一致していることをサーバーが検証する。

管理領域（administrative area）

ディレクトリ・サーバー上の 1 つの**サブツリー**。そのエントリは、1 つの管理認可レベルで制御される。指定された管理者が、管理領域内の各**エントリ**に加えて、ディレクトリ・**スキーマ**、**アクセス制御リスト**およびそれらのエントリの**属性**を制御する。

基本エンコーディング規則（Basic Encoding Rules: BER）

ASN.1 に示されているデータ・ユニットをエンコーディングするための標準規則。BER は ASN.1 と間違って組み合されることがある。ASN.1 は抽象的な構文定義言語で、エンコーディング規則には適用できない。

機密保護（confidentiality）

暗号化では、機密保護（またはプライバシ保護）は、認可されていないエンティティがデータを読み取ることを防止する機能を意味する。通常、これは**暗号化**によって実現される。

キャッシュ（cache）

通常は、コンピュータ内部にある、高速にアクセス可能な一定量のメモリー領域のことを指す。ただし、Web では、ブラウザがダウンロードしたファイルや画像を格納するコンピュータ上の場所を指すことが多い。

競合（contention）

リソースの競合。

強制認証（forced authentication）

事前定義された一定時間アイドル状態が続いた場合に、ユーザーに再認証を強制すること。Oracle Application Server Single Sign-On では、グローバル・ユーザーの非アクティブ・タイムアウトを指定できる。この機能は、セキュリティに敏感なアプリケーションがインストールされている場合に使用する。

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・リクエスト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リクエストを取り出す。これは、サーバー・プロセスの小規模プールで大量のクライアントを処理できることを意味する。専用サーバーと対比。

クライアント SSL 証明書（client SSL certificates）

Secure Sockets Layer で、サーバーに対するクライアント・マシンの身元確認（クライアント認証）に使用される**証明書**。

クラスタ（cluster）

単一のコンピューティング・リソースとして使用される、相互接続された使用可能なすべてのコンピュータの集合。ハードウェア・クラスタによって、高可用性およびスケーラビリティが実現する。

グループ検索ベース（group search base）

Oracle Internet Directory のデフォルトの**ディレクトリ情報ツリー**で、すべてのグループを検索できる ID 管理レルムのノード。

グローバリゼーション・サポート（globalization support）

GUI で複数言語がサポートされること。Oracle Application Server Single Sign-On では、29 言語がサポートされる。

グローバル管理者（global administrator）

ホスティングされた環境では、アプリケーション・サービス・プロバイダなどの 1 企業が、他の複数の企業に Oracle コンポーネントを使用可能にして、その情報を格納する。この種の環境では、グローバル管理者はディレクトリ全体にまたがるアクティビティを実行する。

グローバルに一意なユーザー ID（globally unique user ID）

ユーザーを一意に識別する数値文字列。ユーザー名、パスワードおよび識別名は変更または追加されることがあるが、グローバルに一意なユーザー ID は常に同じである。

グローバル・ユーザーの非アクティブ・タイムアウト（global user inactivity timeout）

Oracle Application Server Single Sign-On のオプション機能。事前定義された一定時間アイドル状態が続いた場合に、ユーザーに再認証を強制する。グローバル・ユーザーの非アクティブ・タイムアウト時間は、シングル・サインアウトのセッション・タイムアウト時間よりもはるかに短い。

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。

検証（verification）

署名とその署名の意図的な適用先となるデータ・ブロックを作成する目的で、**公開鍵**とそれに対応する**秘密鍵**が与えられているときに、特定の**デジタル署名**が有効であることを確認するプロセス。

コード署名証明書（code signing certificates）

Java プログラム、JavaScript またはその他の署名ファイルに署名したエンティティの身元確認に使用される**証明書**。

コールド・バックアップ（cold backup）

Oracle Internet Directory では、データベース・コピー・プロシージャを使用して、新規**ディレクトリ・システム・エージェント**・ノードを既存のレプリケート・システムに追加する手順を表す。

公開鍵（public key）

公開鍵暗号で使用される**公開鍵と秘密鍵のペア**において、一般に公開される鍵。エンティティは、公開鍵を使用してデータを暗号化する。そのデータは、公開鍵の所有者のみが、対応する**秘密鍵**を使用して復号化できる。公開鍵は、対応する秘密鍵で作成されたデジタル署名の検証にも使用できる。

公開鍵暗号（public key cryptography）

公開鍵暗号（非対称型暗号とも呼ばれる）では、公開鍵と秘密鍵の 2 つの鍵が使用される。これらの鍵は、鍵のペアと呼ばれる。秘密鍵は秘密にしておく必要があるが、公開鍵は任意のパーティに送信できる。秘密鍵と公開鍵は、数学的に関連付けられている。秘密鍵によって署名されたメッセージは、対応する公開鍵によって検証できる。同様に、公開鍵によって暗号化されたメッセージは、対応する秘密鍵によって復号化できる。秘密鍵の所有者のみがメッセージを復号化できるため、この方式によって機密保護が保証される。

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。

公開鍵インフラストラクチャ（Public Key Infrastructure: PKI）

公開鍵と**秘密鍵**の発行、配布および証明を管理するシステム。通常、PKI は次のコンポーネントによって構成される。

- **認証局**：デジタル証明書の生成、発行、公開および失効に責任を持つ。
- **登録局**：CA に対する証明書リクエストに記載されている情報の検証に責任を持つ。
- ディレクトリ・サービス：CA によって**証明書**または**証明書失効リスト**が公開される場所。このシステムに依存する第三者は、ここでそれらを取得できる。
- 依存する第三者：**デジタル署名**の検証とデータの暗号化に、CA によって発行された証明書と、それに含まれる**公開鍵**を使用するエンティティ。

公開鍵証明書（public key certificate）

「**証明書**」を参照。

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 Oracle Internet Directory 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、**ディレクトリ固有のエントリ**の `subConfigsubEntry` 属性で指定されているサブツリー内でメンテナンスされる。DSE 自体は、サーバーの起動対象である関連の**ディレクトリ情報ベース**に常駐している。

高度なエンコーディング規則（Distinguished Encoding Rules: DER）

ASN.1 オブジェクトをバイト・シーケンスにエンコーディングするための 1 組の規則。DER は**基本エンコーディング規則**の特殊な形式である。

コンシューマ（consumer）

レプリケーション更新の宛先となるディレクトリ・サーバー。スレーブと呼ばれることもある。

コンテキスト接頭辞（context prefix）

ネーミング・コンテキストのルートの**識別名**。

サード・パーティ製アクセス管理システム（third-party access management system）

OracleAS Single Sign-On を使用して Oracle Application Server アプリケーションにアクセスできるように変更可能な非 Oracle シングル・サインオン・システム。

サーバー証明書（server certificate）

セキュアな Web サーバーを使用してデータを提供する組織の ID が真正であることを証明する**証明書**。サーバー証明書は、相互に信頼できる**認証局**によって発行された**公開鍵と秘密鍵のペア**に関連付けられる必要がある。サーバー証明書は、ブラウザと Web サーバー間のセキュアな通信に必須である。

サービス時間（service time）

リクエストの開始から、そのリクエストに対するレスポンスの完了までの時間。

サービス・プロバイダ（service provider）

トラスト・サークルのメンバーによって、Web ベースのサービスをユーザーに提供するエンティティとして認識されている組織。サービス・プロバイダは他のサービス・プロバイダおよび ID プロバイダと連携して、関連するユーザーに**フェデレーション**内の全パーティに対するセキュアなシングル・サインオンを提供するという目標を実現する。

サブエントリ（subentry）

サブツリー内のエントリ・グループに適用可能な情報が含まれているエントリのタイプ。情報には次の 3 つのタイプがある。

- アクセス制御ポリシー・ポイント
- スキーマ規則
- 共通属性

サブエントリは、管理領域のルートのすぐ下に位置している。

サブクラス（subclass）

別のオブジェクト・クラスから導出されたオブジェクト・クラス。導出元のオブジェクト・クラスは、その**スーパークラス**と呼ばれる。

サブスキーマ DN（subschema DN）

独立した**スキーマ**定義を持つ**ディレクトリ情報ツリー**領域のリスト。

サブタイプ（subtype）

オプションを持たない同じ属性に対して、1 つ以上のオプションを持つ属性。たとえば、American English をオプションとして持つ commonName（cn）属性は、そのオプションを持たない commonName（cn）属性のサブタイプである。逆に、オプションを持たない commonName（cn）属性は、オプションを持つ同じ属性の**スーパータイプ**である。

サブツリー（subtree）

ディレクトリ階層（**ディレクトリ情報ツリー**とも呼ばれる）の中の 1 つのセクション。通常、サブツリーは特定のディレクトリ・ノードから始まり、ディレクトリ階層内でそのノードよりも下位にあるすべてのサブディレクトリとオブジェクトが含まれる。

サプライヤ（supplier）

レプリケーションにおいて、**ネーミング・コンテキスト**のマスター・コピーを保持しているサーバー。マスター・コピーから**コンシューマ**・サーバーに更新を供給する。

参照（referral）

ディレクトリ・サーバーがクライアントに提供する情報。リクエストする情報を見つけるためにクライアントが接続する必要がある他のサーバーを示す。

「**ナレッジ参照**」も参照。

識別名（Distinguished Name: DN）

X.500 識別名（DN）は、ディレクトリ・ツリー内のノードの一意名である。DN は、ユーザーまたはそれ以外のディレクトリ・エントリの一意名の作成に使用される。DN は、ルート・ノードから特定のエントリのノードまでのパス上にある、ツリー内の各ノードから選択された**属性**の連結である。たとえば、LDAP 表記規則では、米国のオラクル社に勤務する John Smith という名前のユーザーの DN は、cn=John Smith, ou=People, o=Oracle, c=us となる。

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、**ディレクトリ統合サーバー**の制御下で実行されるエージェント。**外部エージェント**と対比。

システム操作属性（system operational attribute）

ディレクトリ自体の操作に関係する情報を保持する属性。一部の操作情報は、サーバーを制御するためにディレクトリによって指定される（例 : エントリのタイムスタンプ）。アクセス情報などのその他の操作情報は、管理者が定義し、ディレクトリ・プログラムで処理時に使用される。

従属 CA（subordinate CA）

従属**認証局**のこと。階層構造を持つ**公開鍵インフラストラクチャ**において、その証明書署名鍵が別の CA によって証明され、その役割が他の CA によって制約される CA。

従属参照（subordinate reference）

エントリのすぐ下から始まる**ネーミング・コンテキスト**の参照位置を、**ディレクトリ情報ツリー**内の下位方向に指し示す**ナレッジ参照**。

上位参照（superior reference）

ディレクトリ情報ツリー内で、参照先の**ディレクトリ・システム・エージェント**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**。

条件（predicates）

Oracle Application Server Certificate Authority（OCA）において、ポリシーに適用可能な論理式のこと。ポリシー条件式は、受信する証明書リクエストまたは証明書失効化に対してポリシーを適用する方法を制限する。たとえば、次の条件式は、DN に ou=sales,o=acme,c=us が含まれるクライアントからのリクエストまたは失効化には、表示されているポリシーが異なる効力を持つことを指定している。

```
Type=="client" AND DN=="ou=sales,o=acme,c=us"
```

証明書（certificate）

公開鍵とその所有者の識別情報を関連付ける特別な形式のデータ構造。証明書は、**認証局**によって発行される。証明書には、特定のエンティティの名前、シリアル番号、有効期限および公開鍵が含まれる。証明書は、それが本物であることを受信側が検証できるように、発行元のCA によってデジタル署名される。大半のデジタル証明書は、**X.509** 標準に準拠する。

証明書失効リスト（Certificate Revocation List: CRL）

発行元の**認証局**によって失効されたデジタル**証明書**のリスト。

証明連鎖（certificate chain）

ユーザー**証明書**とそれに関連付けられた **CA 証明書**の 1 つ以上のペアを含む、順序付けられた証明書のリスト。

シングル・サインオフ（single sign-off）

OracleAS Single Sign-On セッションを終了して、すべてのアクティブなパートナ・アプリケーションから同時にログアウトするプロセス。シングル・サインオフは、操作中のアプリケーションからログアウトすることで実行できる。

シングル・サインオン（Single Sign-On: SSO）

一度の認証で、ユーザーが複数のコンピュータ・プラットフォームやアプリケーション・システムにアクセスすることを可能にするプロセスまたはシステム。

シングル・サインオン SDK（single sign-on SDK）

OracleAS Single Sign-On パートナ・アプリケーションをシングル・サインオン対応にするためのレガシー API。SDK は、PL/SQL API と Java API、さらにはこれらの API の実装方法を例示するサンプル・コードで構成される。この SDK は現在は使用不可で、かわりに **mod_osso** が使用される。

シングル・サインオン・サーバー（single sign-on server）

ユーザーが複数のシングル・サインオン・アプリケーション（経費報告、メール、各種手当て申請など）に安全にログインできるようにするプログラム・ロジック。

申告（claim）

エンティティによって行われる宣言内容（名前、ID、鍵、グループなど）。

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。通常、信頼できる証明書は、ユーザー証明書の発行業務を行う、信頼された**認証局**によって発行される。

スーパークラス（superclass）

別のオブジェクト・クラスの導出元の**オブジェクト・クラス**。たとえば、オブジェクト・クラス person は、オブジェクト・クラス organizationalPerson のスーパークラスである。後者の organizationalPerson は、person の**サブクラス**であり、person に含まれている属性を継承する。

スーパータイプ（supertype）

1 つ以上のオプションを持つ同じ属性に対して、オプションを持たない属性。たとえば、オプションを持たない commonName（cn）属性は、オプションを持つ同じ属性のスーパータイプである。逆に、American English をオプションとして持つ commonName（cn）属性は、そのオプションを持たない commonName（cn）属性の**サブタイプ**である。

スーパーユーザー（super user）

一般的には、ディレクトリ情報へのあらゆるアクセスが可能な特別なディレクトリ管理者。

スキーマ（schema）

属性、**オブジェクト・クラス**およびそれらに関連付けられた**一致規則**の集合。

スケーラビリティ（scalability）

使用可能なハードウェア・リソースに応じて、そのハードウェア・リソースによってのみ制限されるシステムの機能。

ストリーム暗号（stream cipher）

対称型アルゴリズムの一種。ストリーム暗号では、一度に 1 ビットや 1 バイトという小さな単位で暗号化され、特定形式のフィードバック・メカニズムの実装によって鍵が絶えず変更される。**RC4** はストリーム暗号の例である。

「**ブロック暗号**」も参照。

スポンサ・ノード（sponsor node）

レプリケーションにおいて、新規ノードに初期データを設定するために使用されるノード。

スマート・ナレッジ参照（smart knowledge reference）

ナレッジ参照エントリが検索の有効範囲内にあるときに戻される**ナレッジ参照**。リクエスト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リクエストの数。通常、「操作 / 秒」（1 秒当たりの操作件数）で表される。

スレーブ（slave）

「**コンシューマ**」を参照。

成功 URL（success URL）

Oracle Application Server Single Sign-On の使用時に、アプリケーションとのセッションおよびセッション Cookie を構築する役割を持つルーチンへの URL。

整合性（integrity）

暗号化では、権限のないエンティティによってデータが変更されていないかどうかを検出する機能を表す。

セカンダリ・ノード（secondary node）

Oracle Application Server Cold Failover Cluster（Identity Management）で、フェイルオーバー中にアプリケーションの移動先となるクラスタ・ノード。

「**プライマリ・ノード**」も参照。

セキュリティ・トークン（security token）

Liberty プロトコルでは、クレームを示し、立証する一連のセキュリティ情報を指す。

セッション鍵（session key）

メッセージまたは通信の 1 セッション期間内でのみ使用される**秘密鍵**。

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 Oracle Database 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）

ディレクトリの属性には、名前、電話番号、役職名などの具体的なデータ要素が保持される。各**エントリ**は 1 組の属性から構成され、それぞれが**オブジェクト・クラス**に所属する。さらに、各属性には型と値があり、型は属性の情報の種類を説明するものであり、値には実際のデータが格納されている。

属性一意性（attribute uniqueness）

指定した 2 つの**属性**に同じ値が含まれていないようにする Oracle Internet Directory 機能。企業ディレクトリと同期しているアプリケーションで、属性を一意キーとして使用することを可能にする。

属性構成ファイル（attribute configuration file）

Oracle Directory Integration Platform 環境で、接続ディレクトリに関係のある属性を指定するファイル。

属性値（attribute value）

特定の**エントリ**の**属性**内に保持される実際のデータ。たとえば、属性の型が `email` であれば、属性値は `sally.jones@oracle.com` のようになる。

属性の型（attribute type）

属性の型は、データ型、最大長、単一値か複数値かなど、データ要素に関する情報を指定する。属性の型は、名前や電子メール・アドレスなど、値が実社会で持つ意味を表し、特定のデータ断片の作成と格納に適用するルールを指定する。

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**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）

リクエストの発行からレスポンスの開始までの時間。

ダイジェスト（digest）

「**メッセージ・ダイジェスト**」を参照。

対称鍵（symmetric key）

「**秘密鍵**」を参照。

対称型アルゴリズム（symmetric algorithm）

暗号化と復号化に同じ鍵を使用する暗号アルゴリズム。主要な対称型（秘密鍵）アルゴリズムには、**ストリーム暗号**と**ブロック暗号**の 2 つのタイプがある。

対称型暗号（symmetric cryptography）

共有秘密暗号とも呼ばれる、データの暗号化と復号化に同じ鍵を使用するシステム。対称型暗号の課題は、送信者と受信者が秘密鍵を合意する手段の安全性を保証することである。転送中の秘密鍵が第三者によって傍受された場合、傍受者はその秘密鍵を使用することで、その鍵によって暗号化されたすべてのデータを復号できるようになる。通常、対称型暗号は非対称型暗号よりも高速で、大量のデータ交換が必要なときに使用されることが多い。対称型暗号には、**DES**、**RC2**、**RC4** などがある。

単一鍵ペア Wallet（single key-pair wallet）

単一のユーザー**証明書**とその関連する**秘密鍵**が含まれる **PKCS#12** 形式の Wallet。**公開鍵**は証明書に埋め込まれている。

中央ディレクトリ（central directory）

Oracle Directory Integration Platform 環境で、中央リポジトリとして機能するディレクトリ。Oracle Directory Integration Platform 環境では、Oracle Internet Directory が中央ディレクトリになる。

中間層（middle tier）

Oracle HTTP Server と OC4J で構成される、OracleAS Single Sign-On インスタンスの一部。OracleAS Single Sign-On 中間層は、ID 管理インフラストラクチャ・データベースとそのクライアントの間に位置する。

データ暗号化規格（Data Encryption Standard: DES）

幅広く使用されている**対称型暗号**アルゴリズムで、1974 年に IBM 社によって開発された。DES では、64 ビットのデータ・ブロックごとに 56 ビットの鍵が適用される。DES および 3DES は、主に **S/MIME** の暗号化アルゴリズムとして使用される。

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。

「**整合性**」も参照。

データベース・アクセス記述子（Database Access Descriptor: DAD）

OracleAS Single Sign-On スキーマなど、特定の Oracle Application Server コンポーネントに対するデータベース接続情報。

ディレクトリ（directory）

「**Oracle Internet Directory**」、「**Lightweight Directory Access Protocol**」および「**X.500**」を参照。

ディレクトリ固有のエントリ（Directory-specific Entry: DSE）

ディレクトリ・サーバー固有のエントリ。異なるディレクトリ・サーバーに同じ**ディレクトリ情報ツリー**名を保持できるが、内容は異なる必要がある。つまり、DSE を保持しているディレクトリに固有の内容を保持できる。DSE は、それを保持しているディレクトリ・サーバーに固有の内容を含むエントリである。

ディレクトリ・サーバー・インスタンス（directory server instance）

ディレクトリ・サーバーの個々の起動のこと。異なるディレクトリ・サーバーの起動（それぞれ、同じまたは異なる構成設定エントリと起動フラグで起動）は、異なるディレクトリ・サーバー・インスタンスと呼ばれる。

ディレクトリ・システム・エージェント（Directory System Agent: DSA）

ディレクトリ・サーバーを表す **X.500** の用語。

ディレクトリ情報ツリー（Directory Information Tree: DIT）

エントリの **DN** で構成されるツリー形式の階層構造。

ディレクトリ情報ベース（Directory Information Base: DIB）

ディレクトリに保持されているすべての情報の完全なセット。DIB は、**ディレクトリ情報ツリー**内で、階層的に相互に関連するエントリで構成されている。

ディレクトリ同期プロファイル（directory synchronization profile）

Oracle Internet Directory と外部システム間の同期の実現方法を記述した特殊な**ディレクトリ統合プロファイル**。

ディレクトリ統合サーバー（directory integration server）

Oracle Directory Integration Platform 環境で、Oracle Internet Directory と**接続ディレクトリ**との間でデータの同期化を実行するサーバー。

ディレクトリ統合プロファイル（directory integration profile）

Oracle Directory Integration Platform 環境での、Oracle Directory Integration Platform による外部システムとの通信方法および通信内容を示す Oracle Internet Directory のエントリ。

ディレクトリ・ネーミング・コンテキスト（directory naming context）

「**ネーミング・コンテキスト**」を参照。

ディレクトリ・プロビジョニング・プロファイル（directory provisioning profile）

Oracle Directory Integration Platform がディレクトリ対応アプリケーションに送信するプロビジョニング関連通知の性質を記述した特殊な**ディレクトリ統合プロファイル**。

ディレクトリ・ユーザー・エージェント（Directory User Agent: DUA）

ディレクトリ・ユーザーのかわりにディレクトリ・サービスにアクセスするソフトウェア。ディレクトリ・ユーザーは人の場合もあれば、別のソフトウェア・コンポーネントの場合もある。

ディレクトリ・レプリケーション・グループ（Directory Replication Group: DRG）

レプリケーション承諾のメンバーであるディレクトリ・サーバーの集合。

デジタル証明（digital certificate）

「**証明書**」を参照。

デジタル署名（digital signature）

デジタル署名は、特定のデータ・ブロックに対して 2 ステップのプロセスを適用して得られる。最初に、データに**ハッシュ関数**を適用して結果を生成する。次に、その結果を署名者の**秘密鍵**を使用して暗号化する。デジタル署名は、データの整合性、メッセージ認証および否認防止を保証する目的で使用できる。デジタル署名アルゴリズムには、**DSA**、**RSA**、**ECDSA** などがある。

デフォルト ID 管理レルム（default identity management realm）

ホスティングされた環境では、アプリケーション・サービス・プロバイダなどの 1 企業が、他の複数の企業に Oracle コンポーネントを使用可能にして、その情報を格納する。このようなホスティングされた環境では、ホスティングしている企業はデフォルト ID 管理レルムと呼ばれ、ホスティングされている企業はそれぞれ**ディレクトリ情報ツリー**内のその企業独自の ID 管理レルムに関連付けられる。

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**。デフォルト・ナレッジ参照は、一般的にディレクトリ・パーティション化対策についてより多くのナレッジを持つサーバーに送信する。

デフォルト・レルム位置（default realm location）

デフォルト ID 管理レルムのルートを識別する**ルート Oracle コンテキスト**での属性。

同時クライアント数（concurrent clients）

Oracle Internet Directory とのセッションを確立しているクライアントの総数。

同時実行性（concurrency）

複数のリクエストを同時に処理できる機能。同時実行性メカニズムの例には、スレッドおよびプロセスなどがある。

同時操作数（concurrent operations）

すべての**同時クライアント数**のリクエストに基づいて Oracle Internet Directory 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。

登録局（Registration Authority: RA）

登録局（RA）は、**認証局**によって証明書が発行される前のユーザーの検証と登録に責任を持つ。RA は、各申請者に対して、新しく適用される証明書の相対識別値または相対識別名を割り当てる。RA は、証明書の署名および発行は行わない。

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。

ドメイン（domain）

ドメインには、Web サイトと、**プリンシパル**がリソースを利用できるようにするアプリケーションが含まれる。1 つのフェデレーテッド・サイトが、**ID プロバイダ**（ソース・ドメイン）、**サービス・プロバイダ**（宛先とメイン）、あるいはその両方の役割を果す。

ドメイン・コンポーネント属性（domain component attribute）

ドメイン・コンポーネント（dc）属性は、ドメイン名から**識別名**を構築する際に使用できる。たとえば、oracle.com などのドメイン名が使用されている場合は、dc=oracle, dc=com で始まる DN を構築して、この DN をディレクトリ情報の該当サブツリーのルートとして使用する。

トラスト・サークル（circle of trust）

一連の ID プロバイダおよびサービス・プロバイダ間の信頼関係で、**プリンシパル**は、その連合内のプロバイダとビジネス・トランザクションを行う場合に、単一のフェデレーテッド ID と**シングル・サインオン**を使用できる。

企業は、Liberty 対応の技術と、企業間の信頼関係を定義する運用協定に基づいたトラスト・サークルのフェデレーションを組むか、またはそれらに加入する。

「**フェデレーテッド ID 管理**」、「**Liberty Alliance**」も参照。

トラスト・ポイント（trustpoint）

「**信頼できる証明書**」を参照。

名前 ID プロファイル（name identifier profile）

プロバイダがピア・プロバイダに、共通ユーザーの 1 人の名前 ID の割当てまたは更新時に通知できる**フェデレーション**プロファイル。

ナレッジ参照（knowledge reference）

リモート・**ディレクトリ・システム・エージェント**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**ディレクトリ情報ツリー**のサブツリーの名前。ナレッジ参照は、参照とも呼ばれる。

ニックネーム属性（nickname attribute）

ディレクトリ全体のユーザーを一意に識別するために使用する属性。この属性のデフォルト値は `uid`。アプリケーションでは、この属性を使用して単純なユーザー名が完全な識別名に変換される。ユーザー・ニックネーム属性を複数値にはできない。つまり、ユーザーは同じ属性名で格納される複数のニックネームを所有できない。

認可（authorization）

サービスまたはネットワーク・リソースへのアクセスを許可または拒否するプロセス。大半のセキュリティ・システムは、2 ステップのプロセスを基本としている。最初のステップは認証で、ここでユーザーは自身の ID を証明する。2 番目のステップは認可で、ここでユーザーは、各自の ID と定義済の**認可ポリシー**に基づいて各種リソースへのアクセスが許可される。

認可ポリシー（authorization policy）

認可ポリシーは、保護されたリソースに対するアクセスを制御する方法を決定する。ポリシーによって、ID およびオブジェクトが、特定のシステム・モデルに従って一連の権限に対応付けられる。たとえば、認可ポリシーによって、営業部に属しているユーザーのみが販売レポートにアクセスできるなどが規定される。

認証（authentication）

エンティティが主張している ID を、その資格証明に基づいて検証するプロセス。ユーザーの認証は、一般的に、ユーザーが知っているか所持しているもの（パスワードや証明書など）に基づいて行われる。

電子メッセージの認証の場合は、特定のシステム（**公開鍵暗号**など）を使用して、ファイルまたはメッセージが主張しているとおりの個人または企業から間違いなく発信されたものであることを検証するプロセスや、メッセージの内容に基づくチェックを使用して、メッセージが配信中に変更されていないことを検証するプロセスが含まれる。

認証局（Certificate Authority: CA）

デジタル**証明書**の発行、更新および失効を行う、信頼できる第三者機関。CA の基本的な役割はエンティティの識別情報を保証することで、申請者の検証を**登録局**に委任する場合もある。広く一般に知られている認証局（CA）には、Digital Signature Trust、Thawte、VeriSign などがある。

認証プラグイン（authentication plugin）

特定の認証方式を実装したもの。OracleAS Single Sign-On には、パスワード認証、デジタル証明書、Windows ネイティブ認証およびサード・パーティ製アクセス管理それぞれの Java プラグインが組み込まれている。

認証レベル（authentication level）

アプリケーションに対して特定の認証動作を指定可能にする、OracleAS Single Sign-On のパラメータ。このパラメータを特定の**認証プラグイン**にリンクできる。

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すエントリから始まり、下位方向にリーフ・エントリまたは従属ネーミング・コンテキストへの**ナレッジ参照**（参照とも呼ばれる）のいずれかまでを範囲とする必要がある。単一のエントリから**ディレクトリ情報ツリー**全体までをその範囲とすることができます。

ネーミング属性（naming attribute）

Oracle Delegated Administration Services または Oracle Internet Directory Java API を使用して作成した新規ユーザー・エントリの相対識別名を構成するために使用する属性。この属性のデフォルト値は cn。

ネット・サービス名（net service name）

接続記述子に変換されるサービスの単純な名前。ユーザーは、接続するサービスに対する接続文字列内のネット・サービス名に従ってユーザー名とパスワードを渡すことによって、接続リクエストを開始する。次に例を示す。

```
CONNECT username/password@net_service_name
```

必要に応じて、ネット・サービス名は次のような様々な場所に格納できる。

- 各クライアントのローカル構成ファイル（tnsnames.ora）
- ディレクトリ・サーバー
- Oracle Names Server
- NDS、NIS、CDS などの外部ネーミング・サービス

パーティション（partition）

一意の重複していないディレクトリ・ネーミング・コンテキスト。1 つのディレクトリ・サーバーに格納されている。

パートナ・アプリケーション（partner application）

認証機能を OracleAS Single Sign-On サーバーに委任する Oracle Application Server アプリケーションまたは非 Oracle アプリケーション。このタイプのアプリケーションでは、**mod_osso** ヘッダーが受け入れられるため、ユーザーは再認証が不要になる。

バインド（binding）

ネットワークの場合は、通信エンティティ間の論理的な接続の確立を意味する。

Oracle Internet Directory では、バインドはディレクトリに対して認証を行うプロセスを表す。

SOAP メッセージを、相互に交換する目的で他のプロトコル（基礎となるプロトコル）内またはその上で伝送する、一定の形式に従った規則の組合せもバインドと呼ばれる。

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。

「**ハッシュ関数**」も参照。

ハッシュ関数（hash function）

暗号化におけるハッシュ関数または一方向ハッシュ関数は、特定のデータ・ブロックに適用されるアルゴリズムを意味する。ハッシュ関数の結果は、特定のデータ・ブロックの整合性を保証する目的で使用できる。ハッシュ関数が安全であるためには、既知のデータ・ブロックと既知の結果を与えられたときに、同じ結果となる別のデータ・ブロックを作成することが極めて困難である必要がある。

判読可能データ（readable data）

暗号化によって暗号文に変換される前のデータ、または復号化によって暗号文から変換された結果のデータ。

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。

非対称型アルゴリズム（asymmetric algorithm）

暗号化と**復号化**に異なる**鍵**を使用する**暗号化アルゴリズム**。

「**公開鍵暗号**」も参照。

非対称型暗号（asymmetric cryptography）

「**公開鍵暗号**」を参照。

否認防止（non-repudiation）

暗号化において、特定の**デジタル署名**が特定のエンティティの**秘密鍵**によって生成されていることと、メッセージが特定の時点で改ざんされずに伝送されていることを保証する機能。

秘密鍵（private key）

公開鍵暗号で使用される**公開鍵と秘密鍵のペア**において、秘密にされる鍵。エンティティは自身の秘密鍵を使用して、**公開鍵**によって暗号化されたデータを復号化する。また、エンティティは秘密鍵を使用して、**デジタル署名**を作成することもできる。エンティティの公開鍵によって暗号化されたデータと、秘密鍵によって作成された署名のセキュリティは、秘密鍵の秘密が維持されていることに依存する。

秘密鍵（secret key）

対称型アルゴリズムで使用される**鍵**。秘密鍵は暗号化と復号化の両方に使用されるため、暗号文を相互に送受信するパーティ間で共有される必要があるが、許可されていないすべてのエンティティに対しては秘密が維持される必要がある。

秘密鍵暗号（private key cryptography）

「**対称型暗号**」を参照。

秘密鍵暗号（secret key cryptography）

「**対称型暗号**」を参照。

平文（plaintext）

暗号化によって暗号文に変換される前の判読可能データ、または復号化によって暗号文から変換された結果の判読可能データ。

ファンアウト・レプリケーション（fan-out replication）

point-to-point レプリケーションとも呼ばれる。サプライヤがコンシューマに直接レプリケートするレプリケーションのタイプ。そのコンシューマは、1 つ以上の別のコンシューマにレプリケートできます。レプリケーションには、完全レプリケーションと部分レプリケーションがあります。

フィルタ（filter）

ディレクトリに対するリクエストまたは検索結果として返されるエントリを定義する式。フィルタは、多くの場合、`cn=susie smith,o=acme,c=us` のような識別名で表される。

フェイルオーバー（failover）

障害を認識し、リカバリする処理。Oracle Application Server Cold Failover Cluster（Identity Management）で、1 つのクラスタ・ノード上で実行されているアプリケーションは、他のクラスタ・ノードに透過的に移行される。この移行時に、クラスタ上のサービスにアクセスするクライアントは一時的に接続できず、フェイルオーバーが完了した後、再接続する必要がある場合がある。

フェデレーション（federation）

「**ID フェデレーション**」を参照。

フェデレーション解除（defederation）

ユーザーのアカウントを **ID プロバイダ**または**サービス・プロバイダ**から外す行為。

フェデレーテッド ID 管理（Federated Identity Management: FIM）

自律型ドメイン内で ID と資格をポータブルにするための協定、標準およびテクノロジ。FIM によって、複数ドメイン全体でユーザー認証が認識可能になり、認証済ユーザーが複数ドメイン内のパーソナライズされたサービスに参加可能になる。FIM は、複数のアカウント間で ID 情報をリンク可能にすることで、個人情報が 1 箇所に格納されることの危険性を回避する。フェデレーテッド ID には、トラストと標準という 2 つの主要なコンポーネントが必要である。フェデレーテッド ID 管理のトラスト・モデルは、**トラスト・サークル**に基づく。標準は、**Liberty Alliance** Project によって定義される。

復号化（decryption）

暗号化されたメッセージ（暗号文）の内容を、元の判読可能な形式（平文）に変換する処理。

プライマリ・ノード（primary node）

Oracle Application Server Cold Failover Cluster（Identity Management）で、指定した時間にアプリケーションが実行されるクラスタ・ノード。

「**セカンダリ・ノード**」も参照。

プリンシパル（principal）

OSFS によりサポートされる **ID フェデレーション**プロトコルで定義されている 3 つの主要ロールの 1 つ。他のロールは **ID プロバイダ**と**サービス・プロバイダ**。

プリンシパルは、サービスを使用でき、フェデレーテッド ID を取得できるエンティティ。通常、プリンシパルは、ID を認証できる人物（ユーザー）またはシステム・エンティティ。

プロキシ・サーバー（proxy server）

Web ブラウザなどのクライアント・アプリケーションと実サーバーの間にあるサーバー。プロキシ・サーバーは、実サーバーに対するすべてのリクエストを代理受信して、自分がそのリクエストを処理できるかどうかを調べる。処理できない場合、リクエストは実サーバーに転送される。OracleAS Single Sign-On では、プロキシは、ロード・バランシング目的とセキュリティ対策用の追加層として使用される。

「**ロード・バランサ**」も参照。

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。

ブロック暗号（block cipher）

対称型アルゴリズムの一種。ブロック暗号では、メッセージを固定サイズのブロック（一般的には 64 ビット）に分割し、各ブロックを鍵によって暗号化する方法でメッセージが暗号化される。広く一般に知られているブロック暗号には、**Blowfish**、**DES** および **AES** などがある。

「**ストリーム暗号**」も参照。

プロビジョニング（provisioning）

エンタープライズ環境で使用可能なアプリケーションおよびその他のリソースへのアクセスをユーザーに付与するプロセス。

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。

プロビジョニング統合プロファイル（provisioning integration 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**。

プロファイル（profile）

「**ディレクトリ統合プロファイル**」を参照。

変更ログ（change log）

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。

ポリシーの優先順位（policy precedence）

Oracle Application Server Certificate Authority（OCA）では、メイン・ポリシー・ページに表示されている順番で、ポリシーが受信リクエストに適用される。OCA ポリシー・プロセッサ・モジュールがポリシーを解析する際、ポリシー・リストの上部にあるポリシーが最初にリクエストに適用される。ポリシー・リストの下部にあるポリシーは最後に適用され、他のポリシーよりも優先される。有効なポリシーのみが受信リクエストに適用される。

マスター・サイト（master site）

レプリケーションにおいて、**マスター定義サイト**以外のサイトで、LDAP レプリケーションのメンバーであるサイト。

マスター定義サイト（Master Definition Site: MDS）

レプリケーションにおいて、管理者が構成スクリプトを実行する Oracle Internet Directory のデータベース。

マッピング・ルール・ファイル（mapping rules file）

Oracle Directory Integration Platform 環境で、Oracle Internet Directory 属性と**接続ディレクトリ**の属性との間のマッピングを指定するファイル。

マルチマスター・レプリケーション（multimaster replication）

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

メタディレクトリ（metadirectory）

企業のすべてのディレクトリ間で情報を共有するディレクトリ・ソリューション。すべてのディレクトリを 1 つの仮想ディレクトリに統合する。集中的に管理できるため、管理コストを削減できる。ディレクトリ間でデータが同期化されるため、企業内のデータに一貫性があり最新であることが保証される。

メッセージ・ダイジェスト（message digest）

ハッシュ関数の結果。

「**ハッシュ**」も参照。

メッセージ認証（message authentication）

特定のメッセージが特定のエンティティから発信されたことを検証するプロセス。

「**認証**」も参照。

メッセージ認証コード（Message Authentication Code: MAC）

メッセージ認証コード（MAC）は、特定のデータ・ブロックに対して 2 ステップのプロセスを適用して得られる。最初に、**ハッシュ関数**の結果を取得する。次に、その結果を**秘密鍵**を使用して暗号化する。MAC は、特定のデータ・ブロックのソースの認証に使用できる。

ユーザー検索ベース（user search base）

Oracle Internet Directory のデフォルトの**ディレクトリ情報ツリー**で、すべてのユーザーが配置される ID 管理レルムのノード。

ユーザー名マッピング・モジュール（user name mapping module）

ユーザー**証明書**とユーザーのニックネームを対応付ける OracleAS Single Sign-On の Java モジュール。ニックネームは認証モジュールに渡され、認証モジュールはこのニックネームを使用して、ユーザーの証明書をディレクトリから取得する。

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**以外のサイトで、**Oracle Database アドバンスト・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 CA（root CA）

ルート**認証局**のこと。階層構造を持つ**公開鍵インフラストラクチャ**において、その**公開鍵**がセキュリティ・ドメイン全体の最も信頼できるデータとして機能する CA。

ルート DSE（root DSE）

「**ルート・ディレクトリ固有のエントリ**」を参照。

ルート Oracle コンテキスト（root Oracle Context）

Oracle Identity Management インフラストラクチャでは、ルート Oracle コンテキストは、インフラストラクチャのデフォルト ID 管理レルムへのポインタを含む Oracle Internet Directory のエントリである。単純な名前を指定して ID 管理レルムの位置を特定する方法の詳細も含まれる。

ルート・ディレクトリ固有のエントリ（Root Directory Specific Entry: root DSE）

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。

レガシー・アプリケーション（legacy application）

認証を OracleAS Single Sign-On サーバーに委任するように変更できない古いアプリケーション。**外部アプリケーション**と呼ばれることもある。

レジストリ・エントリ（registry entry）

Oracle Internet Directory サーバーの起動（**ディレクトリ・サーバー・インスタンス**と呼ばれる）に関連する実行時情報が含まれているエントリ。レジストリ・エントリはディレクトリ自体に格納され、対応するディレクトリ・サーバー・インスタンスが停止するまで保持される。

レスポンス時間（response time）

リクエストの発行からレスポンスの完了までの時間。

レプリカ（replica）

ネーミング・コンテキストの個々のコピー。1 つのサーバー内に格納されている。

レプリケーション承諾（replication agreement）

ディレクトリ・レプリケーション・グループ内のディレクトリ・サーバー間におけるレプリケーションの関係を記述する特別なディレクトリ・エントリ。

レルム（realm）

「**ID 管理レルム**」を参照。

レルム検索ベース（realm search base）

すべての **ID 管理レルム**を含む**ディレクトリ情報ツリー**内のエントリを識別する**ルート Oracle コンテキスト**での属性。この属性は、単純なレルム名をディレクトリ内の対応するエントリにマッピングする際に使用される。

ロード・バランサ（load balancer）

高い負荷やフェイルオーバーが生じた際に、2 つ以上のサーバー間で接続リクエストを負荷分散するハードウェア・デバイスおよびソフトウェア。広く一般に知られているハードウェア・デバイスには、BigIP、Alteon、Local Director などがある。Oracle Application Server Web Cache はロード・バランシング・ソフトウェアの例である。

論理ホスト（logical host）

Oracle Application Server Cold Failover Cluster（Identity Management）で、1 つ以上のディスク・グループおよびホスト名と IP アドレスのペア。論理ホストは、クラスタ内の物理ホストにマップされる。この物理ホストは、論理ホストのホスト名と IP アドレスを使用することになる。

索引

数字

A

B

C

D

E

G

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