Oracle9*i*

Directory Service 統合および配置ガイド

リリース 2（9.2）

2002 年 7 月

部品番号：J06306-01

ORACLE®

Oracle9*i* Directory Service 統合および配置ガイド , リリース 2（9.2）

部品番号：J06306-01

原本名：Oracle9*i* Directory Service Integration and Deployment Guide, Release 2 (9.2)

原本部品番号：A96579-01

原本著者：Henry Abrecht

原本協力者：Valarie Moore, Deanna Bradshaw, Torrance Brooksfuller, Kristy Browder, Montgomery Close, Michael Cowan, Cheng Han, Marilyn Hollinger, Cynthia Kibbe, Ashish Kolli, Nina Lewis, Michael Mesaros, Janaki Narasinghanallur, David Saslav, Daniele Schechter, Richard Smith, Uppili Srinivasan, Deborah Steiner, Rama Vissapragada, Wei Wang, Rodney Ward, and Daniel Wong

Copyright © 2002 Oracle Corporation. All rights reserved.

Printed in Japan.

制限付権利の説明

プログラム（ソフトウェアおよびドキュメントを含む）の使用、複製または開示は、オラクル社との契約に記された制約条件に従うものとします。著作権、特許権およびその他の知的財産権に関する法律により保護されています。

当プログラムのリバース・エンジニアリング等は禁止されております。

このドキュメントの情報は、予告なしに変更されることがあります。オラクル社は本ドキュメントの無謬性を保証しません。

* オラクル社とは、Oracle Corporation（米国オラクル）または日本オラクル株式会社（日本オラクル）を指します。

危険な用途への使用について

オラクル社製品は、原子力、航空産業、大量輸送、医療あるいはその他の危険が伴うアプリケーションを用途として開発されておりません。オラクル社製品を上述のようなアプリケーションに使用することについての安全確保は、顧客各位の責任と費用により行ってください。万一かかる用途での使用によりクレームや損害が発生いたしましても、日本オラクル株式会社と開発元である Oracle Corporation（米国オラクル）およびその関連会社は一切責任を負いかねます。当プログラムを米国国防総省の米国政府機関に提供する際には、『Restricted Rights』と共に提供してください。この場合次の Notice が適用されます。

Restricted Rights Notice

Programs delivered subject to the DOD FAR Supplement are "commercial computer software" and use, duplication, and disclosure of the Programs, including documentation, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement. Otherwise, Programs delivered subject to the Federal Acquisition Regulations are "restricted computer software" and use, duplication, and disclosure of the Programs shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software - Restricted Rights (June, 1987). Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065.

このドキュメントに記載されているその他の会社名および製品名は、あくまでその製品および会社を識別する目的にのみ使用されており、それぞれの所有者の商標または登録商標です。

目次

3 計画と配置のガイドライン

4 Oracle 製品と Oracle Internet Directory の配置

5 ディレクトリ使用構成の完了

A Oracle 固有の LDAP スキーマ拡張機能

B LDAP コマンドライン・ツール

索引

図

表

はじめに

『Oracle9*i* Directory Service 統合および配置ガイド』は、Oracle 製品が LDAP 準拠のディレクトリ、特に Oracle Internet Directory を使用する方法を解説した入門書です。また、Oracle 製品を使用するための Oracle Internet Directory の構成方法についても説明しています。

「はじめに」の内容は次のとおりです。

対象読者

このマニュアルは、次の読者を対象としています。

- Oracle 製品用のディレクトリの構成を、最小限の作業で実行することを目的としているディレクトリ管理者。
- Oracle 製品におけるディレクトリの使用方法を理解することを目的としている、ディレクトリ管理者およびその他の読者。
- ディレクトリの概念について学習または復習することを目的としている、ディレクトリ管理者およびその他の読者。

このマニュアルでは LDAP の知識を前提とはしていませんが、LDAP プロトコルとその使用目的についての基礎的な知識があれば役に立ちます。

このマニュアルの構成

このマニュアルの構成は次のとおりです。

第 1 章「Oracle ディレクトリ環境」

ディレクトリ対応の Oracle 製品と Oracle Internet Directory を紹介します。また、Oracle 製品をサード・パーティ製ディレクトリに統合する方法についても検証します。

第 2 章「ディレクトリ・サーバーの概要」

ディレクトリの機能、LDAP プロトコルの定義、およびオンライン・ディレクトリの各コンポーネントの識別について説明します。

第 3 章「計画と配置のガイドライン」

ディレクトリを配置する前に考慮する必要のある問題について、その概要を示します。

第 4 章「Oracle 製品と Oracle Internet Directory の配置」

個々の Oracle 製品が Oracle Internet Directory を使用する方法について説明しています。各製品がエントリを格納する場所と、それらのエントリを許可のないアクセスから保護するしくみについて説明します。また、各製品の配置要因についても説明します。

第 5 章「ディレクトリ使用構成の完了」

インストール済みのディレクトリへのアクセスを構成する方法について説明します。また、第 4 章で取り上げた各 Oracle 製品のディレクトリ構成作業を説明している関連文書への参照も記載しています。

付録 A「Oracle 固有の LDAP スキーマ拡張機能」

LDAP 対応 Oracle 製品での Oracle Internet Directory のエントリの定義に使用するオブジェクト・クラスおよび属性について説明します。

付録 B「LDAP コマンドライン・ツール」

LDAP C-API を通して使用可能な 6 つの一般的なコマンドライン・ツールについて説明します。

関連文書

詳細は、次の Oracle リソースを参照してください。

- 『Oracle Advanced Security 管理者ガイド』
- 『Oracle Dynamic Services User's and Administrator's Guide』
- 『Oracle9*i* Net Services 管理者ガイド』
- 『Oracle8*i* Networking 101』（Marlene L. Theriault 著、Oracle Press、2000）
- 『Oracle9*i* アプリケーション開発者ガイド - アドバンスト・キューイング』
- 『Oracle9*i* アプリケーション開発者ガイド - 基礎編』

リリース・ノート、インストレーション・マニュアル、ホワイト・ペーパーまたはその他の関連文書は、OTN-J（Oracle Technology Network Japan）に接続すれば、無償でダウンロードできます。OTN-J を使用するには、オンラインでの登録が必要です。次の URL で登録できます。

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

OTN-J のユーザー名とパスワードを取得済みであれば、次の OTN-J Web サイトの文書セクションに直接接続できます。

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

追加情報は、次を参照してください。

- 『Understanding and Deploying LDAP Directory Services』（Timothy A. Howes、Mark C. Smith、Gordon S. Good 共著、Macmillan Technical Publishing、1999 年）
- LDAP プロトコルの詳細は、`http://www.ietf.org/` を参照してください。

表記規則

このマニュアル・セットの本文およびコード例で使用する表記規則について説明します。

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

本文の表記規則

本文には、特別な用語が一目でわかるように様々な表記規則が使用されています。次の表は、本文の表記規則と使用例をまとめたものです。

表記規則	意味	例
太字	太字は、本文内または用語集（あるいはその両方）で定義されている用語を表します。	この句を指定すると、**索引構成表**が作成されます。
固定幅フォントの大文字	固定幅フォントの大文字は、システムにより指定される要素を表します。この要素には、パラメータ、権限、データ型、Recovery Manager キーワード、SQL キーワード、SQL*Plus コマンド、ユーティリティ・コマンド、パッケージとメソッドの他、システム指定の列名、データベース・オブジェクトと構造体、ユーザー名、およびロールなどがあります。	この句は、NUMBER 列に対してのみ指定できます。 データベース・インスタンスのバックアップをとるには、BACKUP コマンドを使用します。 USER_TABLES データ・ディクショナリ・ビューの TABLE_NAME 列を問い合せます。 DBMS_STATS.GENERATE_STATS プロシージャを使用します。
固定幅フォントの小文字	固定幅フォントの小文字は、実行可能ファイル、ファイル名、ディレクトリ名およびユーザーが指定する要素のサンプルを表します。この要素には、コンピュータ名とデータベース名、ネット・サービス名、接続記述子の他、ユーザーが指定するデータベース・オブジェクトと構造体、列名、パッケージとクラス、ユーザー名とロール、プログラム・ユニット、パラメータ値などがあります。 **注意：**プログラム要素の中には、大文字と小文字が混在しているものがあります。それらの要素はそのまま入力してください。	sqlplus と入力して、SQL*Plus をオープンします。 パスワードは、orapwd ファイルで指定します。 /disk1/oracle/dbs ディレクトリに、データ・ファイルと制御ファイルのバックアップを作成します。 hr.departments 表には、department_id、department_name および location_id 列があります。 QUERY_REWRITE_ENABLED 初期化パラメータを true に設定します。 oe ユーザーで接続します。 JRepUtil クラスはこれらのメソッドを実装します。

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

コード例の表記規則

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

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

次の表は、コード例の記載上の表記規則とその使用例をまとめたものです。

表記規則	意味	例
[ ]	大カッコは 1 つ以上のオプション項目を表します。大カッコ自体は入力しません。	DECIMAL (*digits* [, *precision*])
{ }	中カッコは、2 つ以上の項目の中でいずれか 1 つが必須であることを表します。中カッコ自体は入力しません。	{ENABLE | DISABLE}
|	縦線は、大カッコまたは中カッコで囲まれた 2 つ以上のオプションを区切るために使用します。オプションの中の 1 つを入力します。縦線自体は入力しません。	{ENABLE | DISABLE} [COMPRESS | NOCOMPRESS]
...	水平の省略記号は、次のいずれかを表します。	
	■ 例に直接関係のないコードの一部が省略されていること。	CREATE TABLE ... AS *subquery*;
	■ コードの一部を繰返し可能であること。	SELECT *col1*, *col2*, ... , *coln* FROM employees;
. . .	垂直の省略記号は、例に直接関係のないコードが数行省略されていることを表します。	SQL> SELECT NAME FROM V$DATAFILE; NAME ---------- /fsl/dbs/tbs_01.dbf /fs1/dbs/tbs_02.dbf . . . /fsl/dbs/tbs_09.dbf 9 rows selected.

表記規則	意味	例
その他の表記	大カッコ、中カッコ、縦線および省略記号以外の記号はそのまま入力します。	`acctbal NUMBER(11,2);` `acct CONSTANT NUMBER(4) := 3;`
イタリック	イタリック・テキストは、特定の値を指定する必要があるプレースホルダまたは変数を表します。	`CONNECT SYSTEM/`*`system_password`* `DB_NAME =` *`database_name`*

大文字	大文字フォントは、システムにより指定される要素を表します。これらは、ユーザー定義の要素と区別するために大文字で表記しています。大カッコで囲まれている場合を除き、そのままの順序とスペルで入力してください。この要素には大 / 小文字の区別がないため、小文字でも入力できます。	`SELECT last_name, employee_id FROM employees;`
		`SELECT * FROM USER_TABLES;`
		`DROP TABLE hr.employees;`

小文字	小文字フォントは、ユーザーが指定するプログラム要素を表します。たとえば、表名、列名またはファイル名などです。
	注意 : プログラム要素の中には、大文字と小文字が混在しているものがあります。それらの要素はそのまま入力してください。
		`SELECT last_name, employee_id FROM employees;`
		`sqlplus hr/hr`
		`CREATE USER mjones IDENTIFIED BY ty3MU9;`

Windows オペレーティング・システムの表記規則

次の表は、Windows オペレーティング・システムの表記規則と使用例をまとめたものです。

表記規則	意味	例
「スタート」→ を選択	プログラムの起動方法。	Database Configuration Assistant を起動するには、「スタート」→「プログラム」→「Oracle - *HOME_NAME*」→「Configuration and Migration Tools」→「Database Configuration Assistant」を選択します。
ファイル名とディレクトリ名	ファイル名とディレクトリ名には、大 / 小文字区別はありません。特殊文字のうち、左山カッコ（<）、右山カッコ（>）、コロン（:）、二重引用符（"）、スラッシュ（/）、パイプ（|）およびハイフン（-）は使用できません。特殊文字である円記号（¥）は、二重引用符で囲まれている場合も要素セパレータとして扱われます。¥¥で始まるファイル名は、Windows では汎用命名規則を使用するものとみなされます。	`c:¥winnt"¥"system32` は `C:¥WINNT¥SYSTEM32` と同じです。

表記規則	意味	例
C:¥>	ハード・ディスクのカレント・ドライブを表す Windows のコマンド・プロンプトです。コマンド・プロンプトのエスケープ文字はカレット（^）です。プロンプトには、現在作業中のサブディレクトリが反映されます。このマニュアルでは、コマンド・プロンプトと呼ばれます。	C:¥oracle¥oradata>
特殊文字	Windows コマンド・プロンプトでは、二重引用符（"）のエスケープ文字として円記号（¥）が必要な場合があります。丸カッコと一重引用符（'）には、エスケープ文字は不要です。エスケープ文字と特殊文字の詳細は、Windows オペレーティング・システムのマニュアルを参照してください。	C:¥>exp scott/tiger TABLES=emp QUERY=¥"WHERE job='SALESMAN' and sal<1600¥" C:¥>imp SYSTEM/*password* FROMUSER=scott TABLES=(emp, dept)
HOME_NAME	Oracle ホーム名を表します。ホーム名には、16 文字までの英数文字が使用できます。ホーム名に使用できる特殊文字は、アンダースコアのみです。	C:¥> net start Oracle*HOME_NAME*TNSListener

表記規則	意味	例
ORACLE_HOME および *ORACLE_BASE*	Oracle8 リリース 8.0 以前では、Oracle コンポーネントをインストールすると、すべてのサブディレクトリはトップレベルの *ORACLE_HOME* ディレクトリの下にあります。*ORACLE_HOME* ディレクトリの名前は、デフォルトでは次のとおりです。 ■ C:¥orant（Windows NT の場合） ■ C:¥orawin98（Windows 98 の場合） このリリースは、Optimal Flexible Architecture（OFA）のガイドラインに準拠しています。すべてのサブディレクトリがトップレベルの *ORACLE_HOME* ディレクトリの下にあるわけではありません。このリリースでは、*ORACLE_BASE* というトップレベル・ディレクトリがあり、デフォルトでは C:¥oracle になります。他の Oracle ソフトウェアがインストールされていないコンピュータに最新の Oracle リリースをインストールすると、最初の Oracle ホーム・ディレクトリのデフォルト設定は C:¥oracle¥ora*nn* となります。*nn* は最新のリリース番号です。この Oracle ホーム・ディレクトリは、*ORACLE_BASE* の直下のディレクトリです。 このマニュアルでは、ディレクトリ・パスの例はすべて OFA の表記規則に従っています。	%*ORACLE_HOME*%¥rdbms¥admin ディレクトリに移動します。

1

Oracle ディレクトリ環境

この章では、ディレクトリ対応の Oracle 製品と Oracle Internet Directory について紹介します。また、テクノロジ・スタックをサード・パーティ製ディレクトリに統合する方法についても簡単に説明します。

この章の内容は次のとおりです。

Oracle 製品における LDAP の重要性

オラクル社をはじめとする各社では、情報の格納を集中的に管理するために LDAP（Lightweight Directory Access Protocol）準拠のディレクトリの使用が増えています。この情報は、ユーザー名、パスワード、電子メール・アドレス、およびプリンタなどのネットワーク・デバイスから構成され、これらの情報によって、どのユーザーがデータベースへのアクセスを許可されるかが判断されます。このような情報を集中的に管理することにより、複数のデータベースで管理する必要性が軽減します。

ディレクトリと Oracle 製品との連携

現在、Oracle 製品の多くは、Oracle Internet Directory との連携使用が認定されています。また、選択されたサード・パーティ製ディレクトリと Oracle テクノロジ・スタック全体との間で Oracle Internet Directory を使用することにより相互運用性を提供する計画も進められています。個々のコンポーネントではなくテクノロジ・スタック全体にアドレッシングすることで、相互運用性とテストを Oracle Internet Directory という 1 つのコンポーネントに独立させることが可能になります。

LDAP 対応の Oracle 製品

Oracle Internet Directory を使用している Oracle9*i* 製品は、次のとおりです。

- **Oracle Net Services**

  Oracle Net Services は、データベース・アクセス制御、ネットワーク接続、管理性および拡張性を提供する各種機能を備えています。Oracle Net Services のコンポーネントの 1 つである Oracle Net は、データベース接続識別子の格納と解決のための主要な手段として、Oracle Internet Directory を使用しています。

- **Oracle Advanced Security**

  Oracle Advanced Security は、企業ネットワークを保護するための数多くの機能を提供します。これらの機能には、暗号化、認証、シングル・サインオンおよびセキュリティ・プロトコルがあります。Oracle Advanced Security は、ユーザーの認証および認可の情報を格納する中央リポジトリとして、Oracle Internet Directory を使用しています。

- **アプリケーション・コンテキスト**

  アプリケーション・コンテキストは、ユーザーのセッション情報を基にアプリケーションを使用できるようにする、データベース・セキュリティ機能です。中央で初期化されるアプリケーション・コンテキストは、Oracle Internet Directory を使用してコンテキストの値を格納します。

- **Oracle Advanced Queuing**

  Oracle Advanced Queuing は、分散アプリケーション同士で互いにメッセージを非同期に送信できるようにする機能です。Oracle Advanced Queuing は、グローバル・トピックおよび登録のためのメタデータを格納するために Oracle Internet Directory を使用しています。

- **Oracle Dynamic Services**

  Oracle Dynamic Services は、インターネット、イントラネットおよびデータベース情報の各サービスの登録と再利用のための手段を E-Business に提供します。Oracle Dynamic Services は、ディレクトリを使用してサービス定義とアプリケーション・プロファイルを格納します。

Oracle Internet Directory

Oracle Internet Directory は、LDAP バージョン 3 に準拠した Oracle のディレクトリ・サービスです。Oracle Internet Directory は Oracle9*i* データベース上でアプリケーションとして実行されますが、両者は同じオペレーティング・システム上に常駐する場合も、異なるオペレーティング・システム上に常駐する場合もあります。データベースとの通信には、Oracle Net Services が使用されます。Oracle Net Services は、あらゆるネットワークを経由するクライアント / サーバーおよびサーバー間の通信を可能にするリモート・データ・アクセス・ソフトウェアです。

Oracle Internet Directory が企業アプリケーションのディレクトリとして選ばれている要因として、その拡張性、高可用性、そしてセキュリティ機能があります。

- **拡張性**

  Oracle Internet Directory は強力な Oracle9*i* 上で動作するため、テラバイト単位の情報を格納できます。同時に、マルチスレッドおよびデータベース接続プーリングにより、数千もの同時ユーザーを処理でき、秒以下の単位での検索応答時間を実現できます。

- **高可用性**

  Oracle Internet Directory は、クラスタ化された「論理ホスト」、Real Application Clusters、フェイルオーバー、マルチマスター・レプリケーションなどの、すべての Oracle9*i* 高可用性ソリューションおよびテクノロジをサポートしています。これらのソリューションにより、1 台のサーバーが障害を起こした場合でも、ユーザーは別のサーバーから最新の情報に確実にアクセスできます。

- **セキュリティ**

  Oracle Internet Directory は総合的で柔軟なセキュリティ機能を備えています。セキュリティ管理者は、アクセスを特定のディレクトリ・オブジェクトに制限したり、ディレクトリ・サブツリー全体に拡張できます。Secure Sockets Layer（SSL）バージョン 3 を使

用し、匿名、パスワード・ベースおよび証明書ベースの 3 つのセキュリティ・レベルが可能です。

関連項目：『Oracle Internet Directory 管理者ガイド』

Oracle 製品とサード・パーティ製ディレクトリとの統合

Oracle Internet Directory には Oracle Directory Integration Platform が含まれています。このプラットフォームは、組織内部において Oracle Internet Directory と異なるディレクトリとの間でデータを同期化します。これらの異なるディレクトリとしては、NOS ディレクトリ、グループウェア・アドレス帳、HR などのアプリケーション、メタディレクトリなどがあります。

メタディレクトリは、組織内に存在する異なるディレクトリに変更を伝播することによって、多種多様な情報を整理統合します。Oracle Directory Integration Platform を使用すると、複数のソースからの情報を収めたグローバル・ディレクトリ・エントリを持つ単一のディレクトリを構築できます。

Oracle Directory Integration Platform は次のコンポーネントで構成されます。

- ディレクトリ統合エージェント。Oracle Internet Directory、他の Oracle 製品およびサード・パーティ製ディレクトリとの間の接続を提供します。
- ディレクトリ統合サーバー。エージェントのスケジューリングと実行を制御します。
- ディレクトリ統合ツールキット。サード・パーティ製メタディレクトリのベンダーはこれを使用してエージェントを開発し、自社のメタディレクトリ・ソリューションを Oracle Internet Directory に接続できます。

2

ディレクトリ・サーバーの概要

この章では、LDAP 準拠ディレクトリを理解するための基礎知識について説明します。最初に、ディレクトリ（紙ベースまたは電子）の機能について説明します。次に、LDAP プロトコル・バージョン 3 の定義について説明し、最後にオンライン・ディレクトリの基礎的なコンポーネントについて個々に説明します。

この章の内容は次のとおりです。

ディレクトリ

ディレクトリとは、情報を検索する際に役立つ索引またはリストのことです。最も身近なディレクトリはオフラインのもので、通常は、電話帳やイエローページ、商品カタログ、図書館のカード・カタログ、辞書といった、紙ベースのリソースです。

オンライン・ディレクトリ

オンライン・ディレクトリはオフライン・ディレクトリとほとんど同じ機能を果たすコンピュータ・データベースですが、それに加えて次の利点があります。

- 柔軟性

  オンライン・ディレクトリはデータを様々に編成でき、そのためユーザーは異なる検索条件を指定できます。

- セキュリティ

  オンライン・ディレクトリはデータを集中化し、その管理とデータへのアクセスの制限を容易にします。

- ダイナミズム

  オンライン・ディレクトリは頻繁に更新が可能です。

- パーソナライズ

  オンライン・ディレクトリにより、たとえばユーザー・プロファイルやパーソナル・コンピュータのカラー設定などをグローバルに格納できます。

これらの利点によって、オンライン・ディレクトリは大企業で重要な情報を格納するための理想的な手段となります。オンライン・ディレクトリの代表的なエントリには、従業員の名前、エンタープライズ・ロール、電子メール・アドレス、プリンタや会議室その他の企業リソースに関する情報などがあります。

ディレクトリとリレーショナル・データベースとの比較

ディレクトリは最終的には特殊なデータベースとみなせるため、リレーショナル・データベースと混同されることがあります。しかし、2-3 ページの表 2-1 に示すように、これら 2 つの間にはいくつかの大きな違いがあります。

表 2-1 ディレクトリとリレーショナル・データベースとの比較

ディレクトリ	リレーショナル・データベース
書込みよりも読取りのほうの頻度が多い。	読取りよりも書込みのほうの頻度が多い。
小さく単純なデータ単位を扱う。	大規模で複雑な、トランザクション指向のデータ単位を扱う。
広範囲に分散する。	広範囲には分散しない。
階層的に配置されたエントリに情報を格納する。	リレーショナル表に情報をレコードとして格納する。

読取り対書込みの比率

ディレクトリは時として書込みよりも 1,000 倍から 10,000 倍も多くの頻度で読み取られることがあります。これは、ユーザー ID、電子メール・アドレス、カタログ・データなど、更新頻度が少ないものの絶えずアクセスされるような情報を格納しているためです。これに対して、リレーショナル・データベースは受注オーダーや給与、生徒の成績など、頻繁に変更されるデータを格納するリポジトリとして機能します。その結果、書込みの頻度が多く、読取りの頻度が少なくなります。

データ単位

ディレクトリ・オブジェクトのサイズは一般に小さくなっています。これは、たとえば `surname=hay` というように属性形式で表現できる必要があるためです。この機能によって、ディレクトリが検索のために最適化されます。一方、データベースは大きなオブジェクトにも対応できます。

分散

ディレクトリ・アプリケーションでは、どのサーバーに問い合せているのかに関係なく、配置環境全体を通じていつでも同じ情報が参照されることが前提になっています。問合せ先のサーバーに情報がローカルに格納されていなければ、サーバーは必ず情報を取得するか、あるいはその情報の参照先をクライアント・アプリケーションに透過的に指し示します。リレーショナル・データベースは分散も可能ですが、通常は特定のサーバーに常駐しています。

エントリ

ディレクトリ・オブジェクトのサイズが小さいとディレクトリの検索が最適化されるのと同様に、オブジェクトの格納方法も最適化されます。個々のディレクトリ・データ・ピースはディレクトリ情報ツリー内でディスクリート・エントリとして表現されるため、すばやく取得できます。一方、データベースの検索操作には、リレーショナルなトランザクション、つまり、複数のデータ・ピースと複数の表を含むトランザクションのほうが適しています。

典型的なディレクトリ・アプリケーション

一般的なディレクトリ・アプリケーションには次のものがあります。

- オンライン電話帳

  これらは電話番号のみでなく、電子メールや従業員名といった情報のリポジトリとしても機能します。

- 電子メール・アプリケーション

  たとえば電子メール・サーバーでは、電子メール・アドレス、ユーザー名、メールボックス位置、および宛先とプロトコルの情報へのアクセスが必要です。これらのデータ分類は、すべてディレクトリへの格納に適しています。

- HR アプリケーション

  これらのアプリケーションでは人員に関する詳細情報が必要になります。これらの情報はディレクトリに容易に格納されます。人員情報は、従業員の識別番号、誕生日、給与レベル、被雇用日、役職などで構成されます。

業界標準に準拠したオンライン・ディレクトリの長所

オンライン・ディレクトリの長所としてまず挙げられるのは、情報の格納を集中化できるということです。この機能は分散データベース環境において非常に重要であり、企業アプリケーションとディレクトリとの間の対話を規定する共通の標準がなければ実現できません。このような標準がなければ、大企業では多数のアプリケーション固有のディレクトリをそれぞれ独自のプロトコルを装備して配置することが必要になります。このようなアプリケーション固有のディレクトリでは、3 つの大きな問題に直面します。

- データの非一貫性。あるディレクトリで更新された情報が他のディレクトリで更新されない場合があります。
- データの冗長性。ディレクトリ全体でエントリを複製する必要があります。
- 管理上の問題。アプリケーション固有のディレクトリでは、それらのディレクトリ・エントリを 1 回のみでなく何回も入力または修正する必要があるため、管理のための時間やコストが増大します。

このような問題は、たとえば従業員が離職したり別部門に移動したときに発生します。この場合、ネットワーク管理者は複数のデータベースで複数のアカウントを使用禁止にすること

が必要になります。この変更には時間がかかり、またデータベース全体での同期化も難しいため、管理上の負担になるのみでなく、セキュリティ上のリスクを負うことにもなります。

このような場合に、アプリケーション固有のディレクトリの管理作業を容易にするために、LDAP（Lightweight Directory Access Protocol）があります。

LDAP の概要

LDAP は、ディレクトリ・クライアントとディレクトリ・サーバーとの間で共通の言語を使用して対話ができるようにする、拡張可能な標準のディレクトリ・アクセス・プロトコルです。LDAP はその名前が示すように、1990 年に制定された X.500 Directory Access Protocol（DAP）を軽量化して実装したものです。X.500 プロトコルは、アプリケーションとオペレーティング・システムとを結び付けるディレクトリ・モデルの必要性から開発されたものです。しかし、OSI ネットワーキング・スタックを経由して実行されるなど、利用には煩雑さが伴いました。これに対して、LDAP はすでに普及している高速で単純な TCP/IP を直接経由して実行され、また実装コストも比較的安価です。

この項の内容は次のとおりです。

LDAP の利点

LDAP は次に示す方法でディレクトリの管理を簡素化します。

- 単一の拡張可能なディレクトリ・サービスに対する、詳細に定義された単一の標準インタフェースを、企業のユーザーおよびアプリケーションに提供します。
- アプリケーション固有のディレクトリを管理および調整する必要性が軽減します。
- 詳細に定義されたプロトコルと多数のプログラム・インタフェースにより、ディレクトリを有効に活用するインターネット対応アプリケーションの配置がより実用的になります。

LDAP バージョン 3

LDAP プロトコルの最新バージョンは、1997 年 12 月にインターネット標準として承認されたバージョン 3 です。バージョン 3 では、バージョン 2 と比較して次の 5 つの点で改善が図られています。

- グローバリゼーション・サポート

  LDAP バージョン 3 は Unicode のエンコーディングである UTF-8 をサポートしています。UTF-8 は、あらゆる言語での情報の格納および取得に使用されている 16 ビット・エンコーディング規格です。

- 参照

  LDAP バージョン 3 はナレッジ参照をサポートしています。ナレッジ参照は、要求された情報が問合せ先のサーバーに常駐していない場合にユーザーが他のディレクトリ・サーバーを参照できるようにする LDAP の URL です。この機能によってディレクトリのパーティション化、つまり、異なるサーバー間でのディレクトリの分散が可能になります。

- セキュリティ

  LDAP バージョン 3 は SASL（Simple Authentication and Security Layer）をサポートしています。SASL は、クライアントが必要な認証プロトコルを選択できるようにする、インターネット規格です。また、Transport Layer Security（TLS）もサポートしています。TLS は Secure Sockets Layer（SSL）の標準化版であり、クライアントとサーバー間で受け渡されるデータを暗号化します。

- 拡張性

  LDAP バージョン 3 により、新しい LDAP 操作の定義が可能になり、コントロールと呼ばれるメカニズムを使用して既存の操作を変更し、SASL を通じて新しい認証方式を許可します。

- 機能およびスキーマの検出

  LDAP バージョン 3 サーバーは、各サーバーがサポートする LDAP プロトコルの各種バージョンとスキーマを、ルート DSE（ディレクトリ・サーバー固有エントリ）と呼ばれるディレクトリ・エントリに公開します。この機能により、他の LDAP クライアントおよび LDAP サーバーとの対話が容易になります。

関連項目： IETF Web サイト `http://www.ietf.org/` の「RFC（Request for Comment）2251–2256」を参照してください。

C LDAP API

LDAP バージョン 2 で導入された C LDAP API は、コマンドラインから入力されたディレクトリ・エントリへのアクセスと変更を行うための標準 API を提供します。この API は、各 LDAP プロトコル操作に対応する機能のセットを、LDAP 対応アプリケーションのプログラマに提供します。

Java および Perl のプログラミング言語に対応した API も使用できます。

関連項目：

- IETF Web サイト `http://www.ietf.org/` の「RFC（Request for Comment）1823」。この RFC は、LDAP 対応の LDAP C API についてのドキュメントです。
- 付録 B「LDAP コマンドライン・ツール」

LDIF

Lightweight Directory Interchange Format（LDIF）は、ディレクトリ・エントリの説明と変更（変更、追加および削除）に使用する、テキストベースの書式です。ディレクトリ・エントリの変更については、コマンドライン・ユーティリティへの入力が LDIF によって提供されます。

次の 2 つの LDIF ファイルは、どちらもプリンタ用のディレクトリ・エントリを表しています。各エントリの 1 行目の文字列はエントリの名前で、識別名と呼ばれます。両者のファイルの違いを説明すると、1 つ目のファイルはエントリを説明しています。つまり、その書式はエントリに収められる情報の索引になっています。一方、2 つ目のファイルは、コマンドライン・ユーティリティ `ldapmodify` への入力として使用するときに、プリンタの処理速度に関する情報を追加します。

説明

```
dn: cn=LaserPrinter1, ou=Devices, dc=acme,dc=com
objectclass: top
objectclass: printer
objectclass: epsonPrinter
cn: LaserPrinter1
resolution: 600
description: In room 407
```

変更

```
dn: cn=LaserPrinter1, ou=Devices, dc=acme, dc=com
changetype: modify
add: pagesPerMinute
pagesPerMinute: 6
```

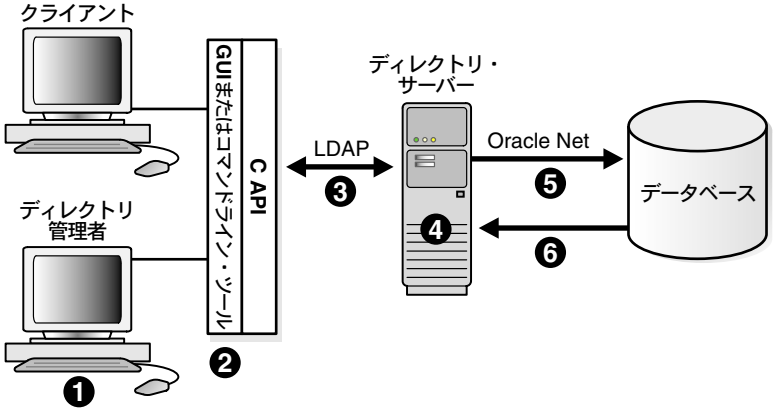
ディレクトリ情報の流れ : 例

LDAP 準拠のディレクトリから情報がどのように取得されるのかを視覚的に理解するために、Oracle Internet Directory でのこの処理のしくみについて考えてみます。

1. クライアントは、Graphical User Interface（GUI）ツールまたはコマンドライン・ツールのどちらかと、1 つ以上の認証方式を使用して、検索要求を発行します。
2. コマンドライン・ツールまたは GUI ツールが C API を起動します。コマンドライン・ツールを使用した場合は直接起動し、GUI ツールを使用した場合は java ネイティブ・インタフェースを経由して起動します。
3. LDAP プロトコルを使用して、検索要求がディレクトリ・サーバーに転送されます。
4. ディレクトリ・サーバーはクライアントを認証またはバインドし、それからアクセス制御リスト（ACL）を調べて、クライアントの要求を許可できるかどうかを判断します。
5. ディレクトリ・サーバーは、リモート・データベース・アクセス・ソフトウェアの Oracle Net を使用して要求をデータベース・サーバーに送信し、検索要求を LDAP からデータベースが認識可能な言語に変換します。
6. データベースは要求された情報を取得し、それをディレクトリ・サーバーに送り返し、さらに C API からクライアントにまで送り返します。

この過程を 2-8 ページの図 2-1 に示します。

図 2-1 Oracle Internet Directory における情報の流れ



ディレクトリの構成要素と特性

ここでは、ディレクトリに格納される情報について説明します。具体的には、情報がどのように編成されるのか、誰がアクセスできるのかについて説明します。この項の内容は次のとおりです。

エントリ

ディレクトリにおいて、オブジェクトに関する情報の個々の集まりのことをエントリと呼びます。このオブジェクトは、人物であったり、プリンタその他の共有リソースであったり、会社内部の部門であったり、あるいは会社自体であったりします。

エントリに名前を付け、ディレクトリ階層におけるその場所を識別するために、各エントリには一意な識別名（DN）が割り当てられます。エントリの DN は、相対識別名（RDN）と呼ばれるエントリ自身とその親エントリで構成され、エントリ自身からツリー内のルート（トップ）のエントリまで昇順で接続されています。これらのエントリがまとまると、2-10 ページの図 2-2 に示すディレクトリ情報ツリー（DIT）を形成します。ディレクトリ・サーバーはこのツリーを使用して、どの情報をリレーショナル、またはその他のデータベースから抽出するのかを判断します。

図 2-2 識別名を強調表示したディレクトリ情報ツリー

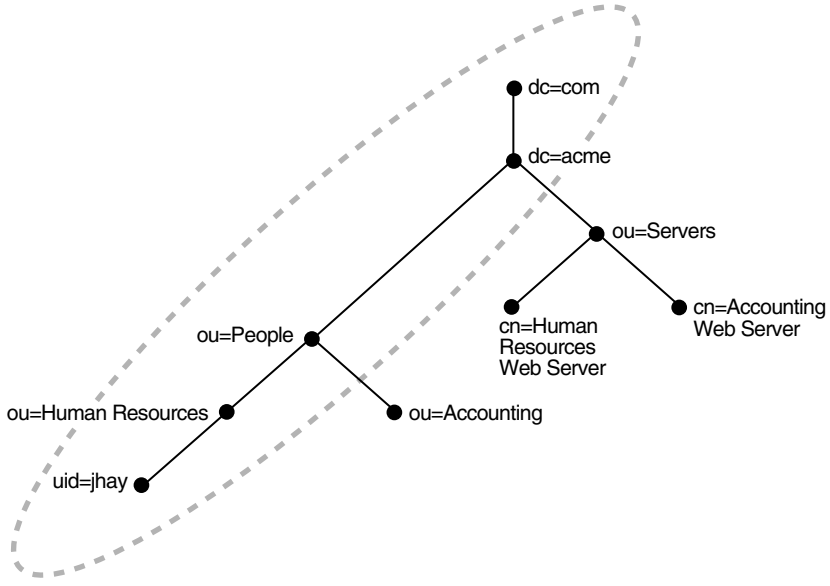


図 2-2 は、エントリ dc（ドメイン・コンポーネント）=acme, dc=com によって指定された、会社 acme に属する DIT の一部分を示したものです。強調表示された DN の `uid=jhay, ou=Human Resources, ou=People, dc=acme, dc=com` は、DIT 内のエントリです。

注意： DN では、カンマの後の空白はオプションです。

このエントリは、会社 acme の組織単位（ou）Human Resources に所属している人物のユーザー ID（uid）を表しています。

DN の形式では、名前の最下位の階層構成要素である RDN が最も左側に置かれます。この例では、この RDN は `uid=jhay` です。

属性

エントリは 1 組の属性で構成され、個々の属性がエントリの一意な特徴を表します。属性は、1 つの属性の型と、1 つ（場合によっては複数）の値の 2 つの構成要素からなります。表 2-2 は、エントリ uid=jhay, ou=Human Resources, ou=People, dc=acme, dc=com に含まれている可能性のあるいくつかの属性を LDIF 表記で示したものです。

表 2-2 典型的なディレクトリ・エントリの属性

属性の型	属性値
cn:	John Hay
cn:	Jack Hay
givenname:	John
sn:	Hay
uid:	jhay
mail:	jhay@acme.com
telephoneNumber:	+1 650 555 0167

LDAP では、この表に示した属性の一部を略記することが許されています。属性 cn は本来 commonName と記述するところを略記したものであり、同様に属性 sn は surname の略記です。

属性のタイプ

属性は、「ユーザー」および「操作」の 2 つの形式をとります。前者はアプリケーション固有であり、ユーザーが取得および変更できます。後者はディレクトリ操作の制御に使用されるもので、通常はユーザーは使用できません。ユーザー属性の例としては、commonName、surname、telephoneNumber、mail などがあります。操作属性の例としては次のようなものがあります。

- modifyTimeStamp − エントリが最後に変更された日付と時刻
- modifiersName − 最後に変更を加えた DN
- supportedLDAPVersion − ディレクトリ・サーバーがサポートしている LDAP バージョン

属性の構文と一致規則

LDAP の規則では、各属性の型は特定の構文と対応する一致規則に従う必要があります。構文は、属性値の形式を決めます。一致規則は、ディレクトリ検索において属性値がどのように比較されるのかを規定します。

X.500 規格で定義されている共通の構文と対応する一致規則は、表 2-3 のとおりです。

表 2-3 属性の構文と対応する一致規則

構文	一致規則
`DirectoryString`	`caseIgnoreMatch`
テキスト文字列	大 / 小文字の区別と、先頭、末尾および複数の空白を無視します。
	`caseExactMatch`
	大 / 小文字を区別して比較します。大 / 小文字の区別と、先頭、末尾および複数の空白を無視します。
`PrintableString`	`telephoneNumberMatch`
電話番号のテキスト文字列	caseIgnoreMatch と同じですが、空白と、ハイフンも無視します。
`Integer`	`integerMatch`
数値	整数比較の規則に従います。
`DistinguishedName`	`distinguishedNameMatch`
ディレクトリ名	DN 比較の特別な規則に従います。
`OctetString`	`octetStringMatch`
バイナリ・データ	データを 1 バイトずつ比較します。

注意： ディレクトリがエントリの記述に使用しているスキーマの形式の種類によっては、構文および一致規則に異なる名前が使用される場合もあります。

たとえば、Kit Karston という名前の従業員をディレクトリで検索するとします。X.500 の規則に従えば、この名前の表現に使用する構文は `DirectoryString` です。一致規則には、`caseIgnoreMatch` または `caseExactMatch` のどちらかを使用できます。前者を使用する場合は、名前を（`cn=kit karston`）または（`cn=kitKarston`）、あるいは（`cn= kit karston`）と入力します。どの場合でも、ディレクトリは該当する名前を返します。

属性のための外国語オプション

属性には、複数の値を格納する他に、言語コードを格納することができます。この機能は、LDAP がサポートする多数の言語のテキストにアクセスする際に便利です。たとえば、属性 cn;lang-ja は日本語における共通の名前を表します。属性の型と値はセミコロンで区切ります。

ディレクトリが指定の言語で属性を戻すように指定することもできます。たとえば、言語コード lang-en-GB は、属性値をイギリス英語で戻します。

オブジェクト・クラス

オブジェクト・クラスとは、エントリの定義に使用する属性の集まりのことです。これらの属性の一部は必須であり、その他はオプションです。

たとえば、LDAP で定義したオブジェクト・クラス organizationalPerson をエントリ uid=jhay, ou=Human Resources, ou=People, dc=acme, dc=com に割り当てた場合は、commonName（cn）および surname（sn）をエントリの属性として含める必要があります。また、オブジェクト・クラス organizationalPerson の規則により、属性 telephoneNumber、uid および userPassword を含めることもできますが、必須ではありません。

オプションの属性を除くと、これらのエントリは LDIF 表記では次のようになります。

```
dn: uid=jhay, ou=Human Resources, ou=People, dc=acme, dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: John Hay
cn: Jack Hay
sn: Hay
```

ここでは、3 つのオブジェクト・クラスがエントリ内に存在し、オブジェクトのサブクラスが表現されていることを示しています。この例では、organizationalPerson はオブジェクト・クラス person のサブクラスであり、person はオブジェクト・クラス top のサブクラスです。

エントリの属性を定義する他に、オブジェクト・クラスは関連するエントリ・グループの場所を調べる手段も提供します。たとえば、ディレクトリ検索の範囲を、自組織のある特定の領域に設置されているプリンタに制限するには、オブジェクト・クラス printer と属性 description（プリンタの場所に対応する値が含まれている可能性があります）とを AND 演算子を使用して結び付ける LDAP 検索フィルタを、ディレクトリ・アクセス GUI で作成します。

> **関連項目：** オブジェクト・サブクラスの詳細は、2-15 ページの「新しいオブジェクト・クラスの作成と古いオブジェクト・クラスの再定義」を参照してください。

オブジェクト・クラスのタイプ

オブジェクト・クラスは 3 つの形式をとります。

- 構造オブジェクト・クラス
- 補助オブジェクト・クラス
- 抽象オブジェクト・クラス

構造オブジェクト・クラス

ディレクトリ内のオブジェクト・クラスの大部分はエントリが何かを定義するものであるため、構造オブジェクト・クラスです。また、これらはその配下に格納されているエントリに対する規則も規定します。たとえば、オブジェクト・クラス `organization (o)` では、その配下に格納されているすべてのオブジェクトがオブジェクト・クラス `organizational units (ou)` に属する必要があります。構造オブジェクト・クラスの別の例としては、`person`、`printer`、`groupOfNames` などがあります。

補助オブジェクト・クラス

LDAP の規則では、各エントリはただ 1 つの構造クラスに属しますが、1 つまたは複数の補助クラスに属することもできます。補助クラスとはその名前が示すように、構造オブジェクト・クラスによってすでに定義済みのエントリに対して属性を追加するために使用します。補助クラスはエントリ内で単体で使用することはできません。エントリには構造オブジェクト・クラスも含まれていることが必要です。構造オブジェクト・クラスとは異なり、補助クラスにはエントリの格納場所に関する制限はありません。

抽象オブジェクト・クラス

3 番目のオブジェクト・クラス・タイプである抽象クラスは、LDAP ディレクトリの構造の決定を主な役割とするクラスです。たとえば、オブジェクト・クラス `top` は、すべての構造オブジェクト・クラスの派生元となっているルートのオブジェクト・クラスです。このオブジェクト・クラスには 1 つの必須属性 `objectClass` があり、すべてのエントリがこの属性を継承しているため、それらがオブジェクト・クラスによって定義されることが保証されます。抽象オブジェクト・クラスはエントリ内で単体で使用することはできません。エントリには構造オブジェクト・クラスも含まれていることが必要です。

注意： ディレクトリ・ベンダーによっては、オブジェクト・クラスのタイプを識別せず、そのため構造規則を規定していないものがあります。

新しいオブジェクト・クラスの作成と古いオブジェクト・クラスの再定義

LDAP では、ディレクトリ内の新しいオブジェクトに対応するためにまったく新しい構造オブジェクト・クラスおよび属性を作成することが可能です。新しいオブジェクト・クラスを作成する際に問題になるのは、一意な名前を考えることです。これは、オブジェクト・クラスと属性の名前空間がフラットであるためです。

これに対して、既存のクラスのサブクラスを作成する方法はずっと一般的で簡単です。作成されたサブクラスはその後スーパークラスになります。この方法を利用すれば、必須属性だけでなくオプションの属性を事前定義のオブジェクト・クラスに追加できます。サブクラスはスーパークラスのすべての属性を継承し、またエントリには複数のオブジェクト・クラスを格納できるため、エントリは多数の属性を継承できることになります。

たとえば、オブジェクト・クラス `printer` にオブジェクト・クラス `epsonPrinter` をサブクラスとして持たせ、組織で使用している特定の種類のプリンタに関する情報を提供することができます。

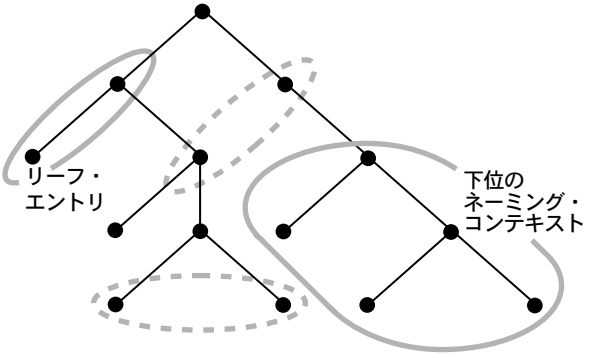
既存のディレクトリ・エントリを再定義するための最も簡単で柔軟な方法を提供するのが、補助オブジェクト・クラスです。これは、特定のオブジェクト・クラスに対してサブクラス化する必要がなく、それらの補助オブジェクト・クラスを使用して任意数のエントリに属性を追加できるためです。補助オブジェクト・クラスの便利な例としては、Uniform Resource Locator（URL）を任意のディレクトリ・エントリに追加するために使用できるオブジェクト・クラスがあります。

ネーミング・コンテキスト

ネーミング・コンテキストとは、1 台のサーバーのみに常駐している DIT のことです。ネーミング・コンテキストは、1 つのエントリ、サブツリー、あるいは DIT 全体でも構成できます。どのディレクトリ・エントリも、その配下のエントリがそのエントリに連続しているかぎり、ネーミング・コンテキストのルートとして扱うことができます。これらの従属エントリは、リーフ・エントリまたは独自の権限を持つネーミング・コンテキストになることができます。

図 2-3 では、全部ではありませんが、ネーミング・コンテキストおよび非ネーミング・コンテキストの一部を強調表示しています。ネーミング・コンテキストは実線の円で、非ネーミング・コンテキストは点線の円で、それぞれ示しています。

図 2-3 ネーミング・コンテキストと非ネーミング・コンテキスト



特定のネーミング・コンテキストを検索対象として指定できるようにするため、LDAP ではそれらのネーミング・コンテキストをディレクトリのルート DSE（ディレクトリ・サーバー固有エントリ）内で公開できます。ネーミング・コンテキストは、コンテキストのルート、つまり最上位のエントリを値として `namingContexts` という属性に割り当てることで発行します。

スキーマ

ディレクトリのスキーマは、ディレクトリにどのオブジェクトを格納できるのかを決めるメタデータで構成されます。ディレクトリのメタデータは、ディレクトリのオブジェクト・クラス、属性の型、属性構文および一致規則です。

典型的なディレクトリのスキーマは、数十のオブジェクト・クラスと数百の属性、そしていくつかの構文で成り立っています。

ディレクトリのナビゲーションと変更を容易にするため、LDAP バージョン 3 では、ディレクトリが `subschemaSubentry` と呼ばれる操作属性でそのスキーマを公開する必要があります。この属性はディレクトリ・サーバーのルート DSE（ディレクトリ・サーバー固有エントリ）にあります。この属性はリレーショナル・データベースのデータ・ディクショナリに似ています。このエントリ `subschemaSubentry` の中で、新しいオブジェクト・クラスと属性の追加や、既存のオブジェクト・クラスの再定義を行います。

関連項目： 付録 A「Oracle 固有の LDAP スキーマ拡張機能」

セキュリティ

ディレクトリへのアクセス権の取得には 2 つのプロセスを踏みます。1 つ目は、1 つ以上の認証方式を使用してディレクトリ・クライアントの認証を確立することです。2 つ目は、ACL を使用し、クライアントからどのような種類の情報にアクセスでき、アクセス後にどのような処理を実行できるのかを判断することです。

認証

LDAP バージョン 3 は 4 つの認証レベルをサポートしています。

- 匿名

  ユーザーはユーザー名やパスワードを指定せずにログインしますが、ログオン後は権限が制限される場合があります。

- 簡易

  クライアントはユーザー名（DN 形式）と保護されていないパスワード（クリア・テキストで送信されるパスワード）を指定します。

- 簡易（SSL 経由）

  ユーザーは、公開鍵暗号化テクノロジである SSL で保護されたユーザー名とパスワードを指定します。

- SSL（証明書付き）

  この方式では、公開鍵暗号化に加えて、クライアントが自身の認証に使用する証明書によって保護を補完することで、最大限の保護を実現します。証明書は認証局から発行されるため、クライアントの識別に関してかなり高い確実性が得られます。

アクセス制御リスト

ディレクトリへのアクセス権を取得すると、ACL と呼ばれるメカニズムによって、どの種類の情報を取得および変更できるのかが決まります。

ACL は、ACI（アクセス制御情報アイテム）と呼ばれる 1 つ以上の操作属性で構成されます。これらの ACI はエントリに対する権限を規定します。理論上は、ACL はディレクトリ階層のどこにでも、エントリのレベルにまで配置できます。実際には、ACL の配置はディレクトリ・ソフトウェアによる制限の影響を受けます。ACL は次の 3 つを規定します。

- アクセス制御の影響を受けるディレクトリ・オブジェクト
- アクセスを許可または拒否されるクライアント
- クライアントに付与されるアクセス権

次の例は、コマンドライン・ツール ldapmodify を使用して作成された ACL の形式を示したものです。この ACL は Oracle Internet Directory の orclEntryLevelACI 属性に基づくものです。この属性は 1 個のエントリに対してのみアクセス制御ルールを設定します。

```
dn: uid=jhay, ou=Human Resources, ou=People, dc=acme, dc=com
changetype: modify
replace: orclentrylevelaci:
orclentrylevelaci: access to entry
    by dn= "cn=directory manager, dc=acme, dc=com" (browse, add, delete)
    by *  (browse, noadd, nodelete)
orclentrylevelaci: access to attr=(*)
    by dn= "cn=directory manager, dc=acme, dc=com" (search, read, write, compare)
    by * (search, read, nowrite, nocompare)
```

この ACL は 2 つの ACI（太字で表記）で構成されています。これらはエントリ uid=jhay, ou=Human Resources, ou=People, dc=acme, dc=com に対するアクセス制御ルールを設定します。これらの ACI は、ドメイン dc=acme, dc=com 内部に所属するディレクトリ管理者に対して、エントリとその属性に対する読取りおよび変更の権限を与えます。ワイルド・カード「*」によって指定されたその他のすべてのユーザーには、書込み権限は与えられず、読取り権限のみ与えられます。権限グループだけでなく個人も、ACI によって権限が割り当てられるエンティティになることができます。

Oracle コンテキスト

ディレクトリには、Oracle ソフトウェアに関連するすべての情報が、Oracle コンテキストと呼ばれる 1 つまたは複数のエントリの下に収められます。Oracle コンテキストは cn=OracleContext という RDN を持っています。Oracle コンテキストは DIT 内の任意のエントリの配下に作成できます。ディレクトリ・アクセス構成用ツールである Oracle Net Configuration Assistant を使用すると、公開されているエントリのリストが提示場所として表示されるので便利です。Oracle Internet Directory を使用する場合は、ディレクトリのインストール時に初期設定の Oracle コンテキストが作成されます。

2-19 ページの図 2-4 に示した初期設定の Oracle コンテキストは、最上位において Products、Groups、Services、Computers の 4 つのコンテナで構成され、コンテキスト全体に適用される 3 つの管理グループに対応したエントリを持つ、ディレクトリ・サブツリーです。この段階でインストールされる製品関連のエントリのみが、エンタープライズ・ユーザー・セキュリティ用および GUI ツール Enterprise Security Manager 用のエントリです。

Oracle Net Configuration Assistant を使用してディレクトリへのアクセスを構成した後、もう 1 つのツール Database Configuration Assistant を使用してデータベースを登録できます。登録によって、データベース・サーバーとそれらに関連する Oracle Net 接続記述子に対応するエントリが追加されます。

図 2-4 データベースおよびデータベース接続記述子のエントリが追加された初期設定の Oracle コンテキスト

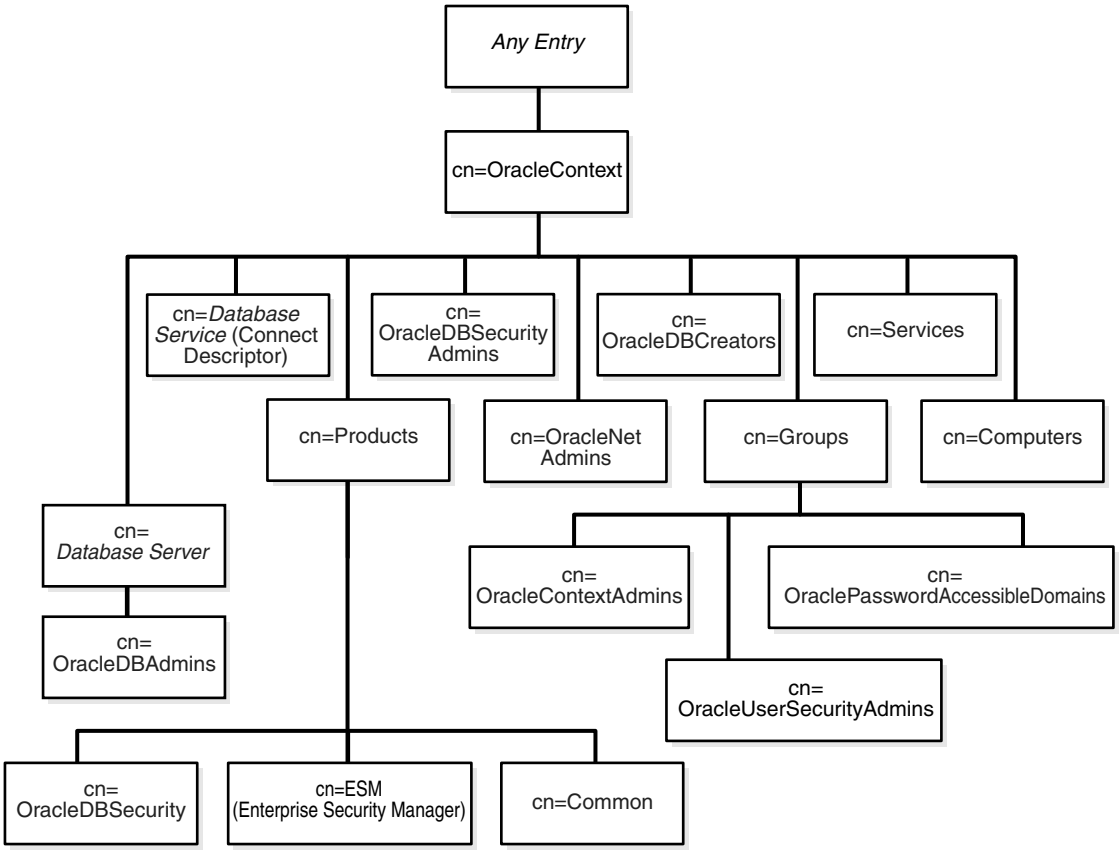


図 2-4 に示した 4 つのコンテナの内容を表 2-4 に示します。

表 2-4 Oracle コンテキスト配下のコンテナ

コンテナ	説明
Products	Products コンテナは、Oracle Net Services および Oracle Advanced Queuing を除くすべての Oracle 製品固有のエントリのためのリポジトリです。このコンテナ内のエントリは製品に関してプライベートであり、アクセス制御ポリシーによって保護される場合があります。エントリ Common（cn=Common）には、たとえばユーザーを一意に識別する属性など、すべてのオブジェクトに共通の属性が格納されます。
Groups	Groups コンテナには、Oracle コンテキスト全体に適用可能な管理グループのためのエントリが格納されます。現時点では、これらのグループは OracleContextAdmins、OracleUserSecurityAdmins および OraclePasswordAccessibleDomains です。グループ OracleNetAdmins、OracleDBCreators および OracleDBSecurityAdmins のエントリは Oracle Context のすぐ下にあります。
Services	Services コンテナには、Oracle 製品が提供するサービスに対応したエントリが格納されます。これらのエントリを別々に格納することで、必要なサービスの検出が容易になります。今後、Services はデータベース・サーバー・エントリ用のリポジトリになる予定です。
Computers	Computers コンテナには、個々のマシンに関する情報を収めたエントリが格納されます。たとえば、特定のマシン上の特定の Oracle ホームで実行されている特定のサーバーに関する構成情報などが格納されます。

関連項目：

- 『Understanding and Deploying LDAP Directory Services』（Timothy A. Howes、Mark C. Smith、Gordon S. Good 共著、Macmillan Technical Publishing、1999 年）
- 『Oracle Internet Directory 管理者ガイド』

3

計画と配置のガイドライン

この章では、ディレクトリを配置する前に考慮する必要のある問題について概要を説明します。Oracle Internet Directory の配置方法の詳細は、『Oracle Internet Directory 管理者ガイド』の第 VI 部を参照してください。

この章の内容は次のとおりです。

ディレクトリに配置する必要のあるもの

ディレクトリに何を格納するのかを決める際に最も重要なことは、「ディレクトリはデータベースのかわりにはならない」ということです。ディレクトリは読取り操作に適するように設計されているため、頻繁に変更される情報のリポジトリとして使用することは避けてください。ディレクトリ内の書込み操作を最小限に抑えることで、検索のパフォーマンスが向上します。ディレクトリは、1 つのディレクトリ・エントリに 1 つの操作が関与するような場合に最適に動作し、管理メタデータなど比較的静的なデータが関与する操作に適しています。しかし、複数のデータ項目や複数の操作が関与するトランザクション的な操作に対しては、データベースのほうがリポジトリとして適しています。

次に示すような情報がディレクトリ格納の候補として適しています。

- 電話番号、電子メール・アドレス、所在地などの連絡先情報
- 給与、役職、管理者、所属部門に関する情報からなる、従業員プロファイル
- ソフトウェア構成情報
- ソフトウェアのプリファレンス
- クレジット限度額、クレジット・カード番号、顧客連絡先情報などの、非トランザクション的な請求情報
- JPEG 画像や Java アプリケーションなど、ディレクトリ格納に適していない大規模なオブジェクトへのポインタ

効果的なディレクトリ・ツリーの設計とエントリ名の選択

効果的なディレクトリ情報ツリーを設計し、効果的な名前をエントリに割り当てるためには、慎重な計画と企業全体での調整が必要になります。効果的なディレクトリ構造によって、次のような特徴が 1 つにまとまります。

- 従業員の名前と番号を会社の人事部門から割り当てるための規則が活用されます。このような規則のポリシーは企業全体にわたって有効です。かわりに一意な名前を別途考案する方法もありますが、管理上のオーバーヘッドが増えることになります。
- エントリが会社の階層別に編成されることが回避され、そのかわりに個人の組織上の情報がその人のディレクトリ・エントリの属性として含まれます。会社の階層をディレクトリの編成方法の尺度として使用しないことで、会社の再編成の原因となる管理上の混乱が避けられます。
- データの所有権境界を反映するようにディレクトリ情報ツリーが編成されます。この結果、効果的なアクセス制御とレプリケーション・ポリシーの開発が容易になります。たとえば、世界規模のディレクトリの整理統合を必要としている多国籍企業は、ディレクトリを地域ごとに対応するネーミング・コンテキストに分割し、それぞれに独自のアクセス制御とレプリケーション・ポリシーを設けることで、目的を達成できます。

ディレクトリの物理的な分散 : パーティションとレプリカ

整理統合され集中管理されたディレクトリのモデルと、それに伴うコストの節約は、マルチマスター・レプリケーションがあって初めて達成されるものです。これらのテクノロジを利用すると、ネットワークの複数のディレクトリ・ノードにディレクトリのコピーが格納され、各ノードでディレクトリが更新されて、その変更が他のノードにレプリケートされます。レプリケーションはネーミング・コンテキストのレベルで発生するため、異なるサーバー間でディレクトリをパーティション化することに伴う管理上の負担を組織が背負うことはありません。

集中管理された強力なディレクトリには、次のような特徴があります。

- 複数のディレクトリ・ノードのネットワークで構成され、各ノードにすべてのネーミング・コンテキストがあり、そのすべてがマルチマスター構成によって結合されています。
- ディレクトリのノードが、企業のデータ・ネットワーク接続に適合するように、各地域ごとに 1 つずつ展開されています。たとえば、ネットワークの残りの部分に低速回線を経由して接続している地域では、その地域のクライアント用に専用のディレクトリ・サーバーを設置するほうが賢明です。
- ディレクトリの地域サーバーがそれぞれフェイルオーバーとリカバリに対応するように構成されています。

レプリケートする理由

次のような状況では、ディレクトリのレプリケーションが望ましいといえます。

- 広範囲に散在しているデータ・センターからなる組織で、共通のディレクトリを必要としているものの、それらのデータ・センターが複数の中継ルーターの関与する低帯域幅回線で相互接続している場合。
- ディレクトリ・サーバーにアクセスするクライアントの数がサーバーの容量を超えていて、ロード・バランシングが必要な場合。
- 組織でディレクトリ・サーバーに障害が発生した場合でもシステムの可用性を確保する必要がある場合。

> **関連項目 :** 『Oracle Internet Directory 管理者ガイド』の第 21 章「ディレクトリ・レプリケーションの概要」および第 22 章「Oracle ディレクトリ・レプリケーション・サーバーの管理」

パーティション化する理由

複数台のサーバー間でディレクトリをパーティション化することは、各パーティションごとにバックアップ、リカバリその他のデータ管理機能の計画を独自に立てる必要が生じるため、コストがかかります。次のような条件によってディレクトリのパーティションが特長付けられる場合以外は、ディレクトリのレプリケートを計画してください。

- パーティションが管理上およびデータ所有権の境界に対応していて、独立させたままのほうが好ましい場合。
- 広範囲に散在しているデータ・センターからなる組織で、それらのデータ・センターが低帯域幅回線で相互接続しているが、ローカル・アクセスの必要性しかない場合。
- パーティションが組織全体に対して必要不可欠ではない場合。
- ディレクトリ全体のレプリカの維持に要するコストがサポート可能な範囲を超えている場合。

高可用性とフェイルオーバーのための設計

マルチマスター・レプリケーションは、ディレクトリが常時使用可能であることを保証し、フェイルオーバーに対する修復手段を提供しますが、これとは別の 2 つのバックアップおよびリカバリの方式である、Intelligent Client Failover および Intelligent Network Level Failover についても理解しておいてください。どちらも Oracle Internet Directory のインストール先でのオプションです。

Intelligent Client Failover により、Oracle Internet Directory に接続しているクライアントは、対象となるサーバー・インスタンスへの接続が失敗した場合に、Oracle Internet Directory の代替のサーバー・インスタンスに連絡できるようになります。

Intelligent Network Level Failover は、Oracle Internet Directory のホストになっているサーバーの障害を検出して接続要求を他のサーバーに再ルーティングするテクノロジです。ロード・バランシングとフェイルオーバーの機能を備えています。

> **関連項目：**『Oracle Internet Directory 管理者ガイド』の第 20 章「高可用性とフェイルオーバーに関する考慮事項」

容量計画、サイズ指定およびチューニング

対象となるディレクトリ・ノードの負荷および容量の要件を決定するには、十分な予測と慎重な計画が必要です。具体的には、容量計画、サイズ指定およびチューニングの 3 つのプロセスを踏みます。

この項の内容は次のとおりです。

容量計画

容量計画では、ディレクトリ・サーバーにかかる負荷と必要な容量を決定します。これらは次の要素をもとに決定します。

- サーバーにアクセスする LDAP クライアント・アプリケーションのタイプ
- これらのアプリケーションにアクセスするユーザーの数
- これらのアプリケーションが実行する LDAP 操作の種類
- ディレクトリ情報ツリー内のエントリの数
- ディレクトリ・サーバーが実行する操作のタイプ
- ディレクトリ・サーバーへの同時接続数
- ディレクトリ・サーバーが操作を実行する必要のあるピーク率
- ピーク負荷条件下で許容される平均待機時間

> **関連項目：**『Oracle Internet Directory 管理者ガイド』の第 18 章「容量計画に関する考慮事項」

サイズ指定

ディレクトリ・サーバーの負荷と容量の要件を決定すると、システム要件を決定できます。次の要素について検討します。

- ディレクトリ・サーバー・コンピュータの CPU のタイプと個数
- ディレクトリ・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
- ディレクトリ・サーバー・コンピュータに必要なメモリー容量
- 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

関連項目：『Oracle Internet Directory 管理者ガイド』の第 18 章「容量計画に関する考慮事項」

チューニング

ディレクトリを実際に使用する前に、アプリケーションが操作するデータをテスト・データとして使用し、ディレクトリのテストを行います。テスティングに使用するツールはどのようなものでも、チューニングをどのように実施する必要があるかを判断する際の指標として、全体のスループットと平均待機時間を使用します。

一般にチューニングされることが多いプロパティを次に示します。

- CPU 使用率

  配置されるディレクトリ・サーバーの台数と、各サーバーがオープンするデータベース接続の数によって変化します。

- メモリー使用量

  Oracle Internet Directory の場合、メモリーを最も消費するのはデータベース・キャッシュです。物理メモリーが常に使用可能になるように、データベース・キャッシュをチューニングします。キャッシュが大きすぎるとページングの原因となり、パフォーマンスが低下します。キャッシュが小さすぎるとディスク I/O が過度に多くなり、やはりパフォーマンスが低下します。

- ディスク使用量

  ディレクトリから戻されるデータがデータベース表領域に常駐する場合は、次の操作によってデータのスループットを改善できます。

  - 様々な論理ドライブおよび物理ドライブにおいて、表領域のバランスをとります。
  - 論理ボリュームを複数の物理ボリュームにストライプ化します。
  - ディスク・ボリュームを複数の I/O コントローラに分散します。

  関連項目：『Oracle Internet Directory 管理者ガイド』の第 19 章「チューニングに関する考慮事項」

ディレクトリのセキュリティの設計

ディレクトリのセキュリティを設計する際は、次の作業を実行します。

- 許可するアクセス数をできるだけ少なくします。
- ディレクトリ・ツリーのルートに配置するアクセス制御リスト（ACL）の種類について慎重に検討します。これは、ルートへの ACL の配置によって、ユーザーがツリーの他の部分に対して可能なアクセスの種類が決まるためです。
- ACL 内で、できるだけ個人ではなくグループを使用します。
- 現在の仕様では、ディレクトリ・ツリー内で上位にあるグループ権限をそれよりも下位のレベルに戻すことはできません。

関連項目：『Oracle Internet Directory 管理者ガイド』の第 10 章「ディレクトリ・セキュリティの概要」

4

Oracle 製品と Oracle Internet Directory の配置

この章では、Oracle9*i* 製品が Oracle Internet Directory と対話する方法を詳しく説明します。各製品がディレクトリを使用する方法、Oracle コンテキスト下のエントリを格納する場所、および許可されていないアクセスからこれらのオブジェクトを保護する方法について説明します。また、Oracle Internet Directory を使用する前に理解しておく必要のある配置要素についても適宜説明します。

この章では、次の製品について説明しています。

- Oracle Net Services
- Oracle Advanced Security
- アプリケーション・コンテキスト
- Oracle Advanced Queuing
- Oracle Dynamic Services

Oracle Net Services

Oracle Net Services は、分散された、異種コンピューティング環境における企業規模の接続ソリューションを提供します。Oracle Net Services によって、ネットワークの構成と管理に伴う複雑さの緩和、パフォーマンスの最大化、ネットワーク診断機能の向上が実現します。典型的なネットワーク構成に対して、Oracle Net Services は次のソリューションを提供します。

- 接続性

  ネットワーク・セッションの確立後、Oracle Net Services のコンポーネントの 1 つである Oracle Net は、クライアント・アプリケーションとデータベース・サーバーのためのデータ伝達手段として機能します。Oracle Net はクライアント・アプリケーションとデータベース・サーバー間の接続の開始と管理を担うほか、両者間のメッセージの交換も行います。Oracle Net がこれらのジョブを実行できるのは、ネットワークの各コンピュータにインストールされるためです。

- 管理性

  位置の透過性、集中化された構成、すばやい独自のインストールおよび構成といった機能により、ネットワーク・コンポーネントの構成と管理が容易に行えます。

- インターネットにおける拡張性

  Oracle Net Services により、システム・リソースの最大化とパフォーマンスの向上を実現できます。Oracle の共有サーバー・アーキテクチャによって、アプリケーションの拡張性が増し、データベースに同時に接続できるクライアントの数が増えます。

- インターネットにおけるセキュリティ

  Oracle Net Services は Oracle Advanced Security およびその他のデータベース・アクセス制御機能を使用して、ネットワークのセキュリティを強化します。

この項の内容は次のとおりです。

Oracle Net Services による Oracle Internet Directory の使用

Oracle Net Services は、接続識別子を格納し、クライアントに戻す接続記述子に解決するための主な手段として、Oracle Internet Directory を使用します。この機能のことを、ディレクトリ・ネーミングと呼びます。接続識別子を指定するには、複数の方法があります。最も一般的なのはネット・サービス名を使用する方法ですが、データベース・サービス名を使用する方法もあります。

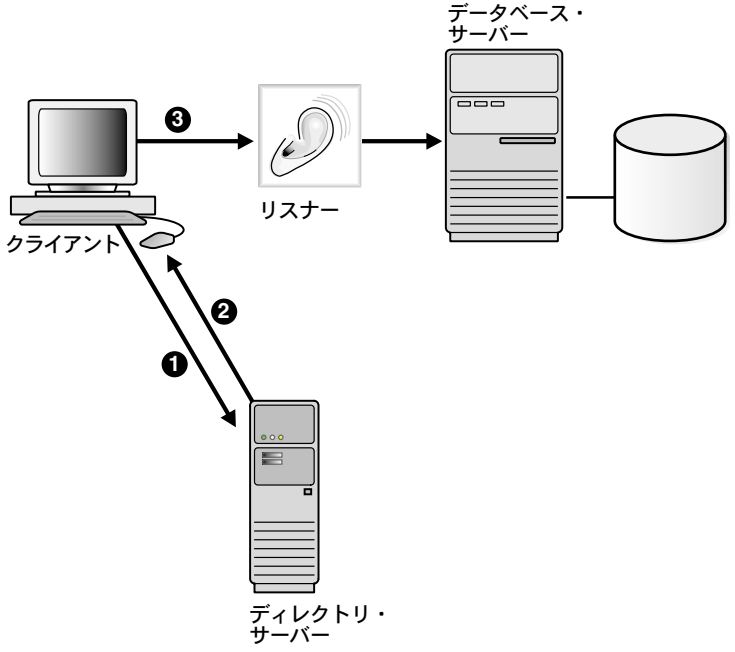
次の接続文字列では、`sales` はデータベース・サービスの単純名です。この名前は接続情報に解決され、データベースへのアクセスに使用されます。この情報を `tnsnames.ora` ファイルに格納するかわりに、ディレクトリ・サーバーに格納することができます。

```
CONNECT username/password@sales
```

4-4 ページの図 4-1 は、ディレクトリ・サーバーを通じて接続識別子を解決するクライアントを示しています。

1. クライアントはディレクトリ・サーバーに接続し、接続識別子を接続記述子に解決します。
2. ディレクトリ・サーバーは接続識別子を解決し、クライアントにかわって接続記述子を取得します。
3. クライアントは接続記述子を使用して、接続要求をリスナーに送信します。

図 4-1 ディレクトリ・サーバーを使用して接続識別子を解決するクライアント



注意： Java Database Connectivity（JDBC）ドライバでは、ディレクトリ・ネーミングがサポートされます。詳細は、『Oracle9*i* JDBC 開発者ガイドおよびリファレンス』を参照してください。

Oracle コンテキスト下の Oracle Net Services エントリ

図 4-2 は、ディレクトリ・ネーミングによってディレクトリ内で次の 3 種類の接続識別子がサポートされることを示しています。

- データベース・サービス

  データベース・サービスのエントリには、データベースの実際の名前のほか、接続記述子を構成する属性など、いくつかの属性が含まれています。データベース・サービスのエントリは、データベースの作成時に Database Configuration Assistant を使用して作成します。エントリの名前は作成時に指定したデータベース名に一致します。ディレクトリ・サーバーにアクセスするように構成されているクライアントは、クライアント自身の接続文字列でこのエントリを使用し、追加の構成を行うことなくデータベースに接続できます。

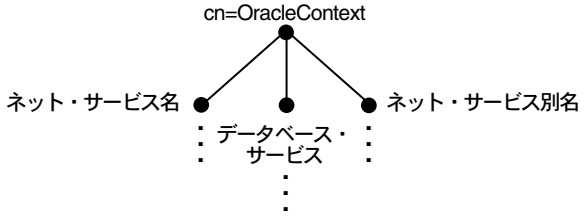
- ネット・サービス名

  ネット・サービス名はデータベースの単純名で、接続記述子に解決されます。接続記述子は、データベースの場所とデータベース・サービスの名前を指定します。ネット・サービス・エントリには、接続記述子を構成する属性が含まれています。ネット・サービス名エントリは Oracle Net Manager を使用して作成します。Oracle Net Manager は Oracle Net Services の構成と管理を行うための Graphical User Interface（GUI）ツールです。Oracle Net Manager 内部で使用可能な、ディレクトリ・サーバー移行ウィザードを使用すると、既存の `tnsnames.ora` ファイルに格納されているネット・サービス名を Oracle Internet Directory にエクスポートできます。

- ネット・サービス別名

  ネット・サービス別名は、データベース・サービス名またはネット・サービス名の代替名です。ネット・サービス別名エントリには、接続記述子情報は含まれません。かわりに、別名であるエントリの位置を参照するのみです。クライアントがネット・サービス別名のディレクトリ参照を要求すると、ディレクトリはエントリがネット・サービス別名であると判断し、参照エントリである場合と同様に参照を完了します。

図 4-2 ネットワーキング・エントリ



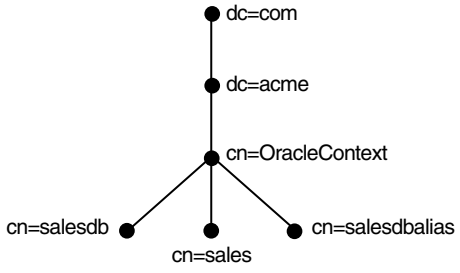
これらのエントリは、Oracle コンテキストのすぐ下に直接作成されます。

図 4-3 では、`salesdb` というデータベース・サービス・エントリ、`sales` というネット・サービス名エントリ、`salesdb` のネット・サービス別名 `salesdbalias` がディレクトリにあります。各エントリには、次の識別名（DN）があります。

- エントリ `salesdb` には `cn=salesdb,cn=OracleContext,dc=acme,dc=com` という DN があります。
- エントリ `sales` には `cn=sales,cn=OracleContext,dc=acme,dc=com` という DN があります。
- エントリ `salesdbalias` には `cn=salesdbalias,cn=OracleContext,dc=acme,dc=com` という DN があります。

`salesdbalias` を使用してデータベース・サービスに接続すると、`CONNECT` *`username`*`/`*`password`*`@salesdbalias` の場合と同様に、実際には `salesdb` に解決され、その接続記述子情報が使用されます。

図 4-3 ネットワーキング・エントリの例

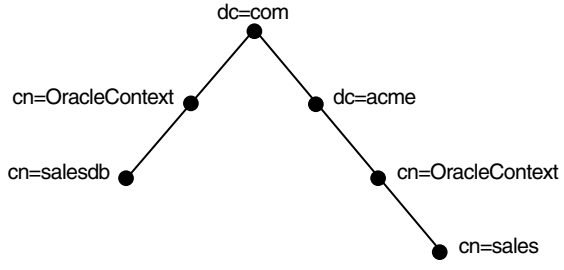


ディレクトリ・サーバーの使用構成中に、Oracle コンテキストをデフォルトの場所として含むディレクトリ・エントリを選択し、ディレクトリ・サーバー内のディレクトリ・ネーミングを検索して参照します。ディレクトリ・サーバーの使用の構成は、インストール中またはインストール後に Oracle Net Configuration Assistant を使用して行えます。

ディレクトリ・エントリがデフォルトの Oracle コンテキストの内部にある場合は、相対パス名を使用してアクセスできます。図 4-4 では、エントリ `salesdb` には `cn=salesdb,cn=OracleContext,dc=com` という DN があり、エントリ `sales` には `cn=sales,cn=OracleContext,dc=acme,dc=com` という DN があります。クライアントで `salesdb` エントリよりも頻繁に `sales` エントリにアクセスする必要がある場合は、参照実行先のデフォルトのディレクトリ・エントリとして `dc=acme,dc=com` を構成します。これにより、クライアントは次の接続文字列を使用して Oracle9*i* データベースに接続できるようになります。

```
CONNECT username/password@sales
```

図 4-4 2 つの Oracle コンテキストを持つディレクトリ構造



指定したディレクトリ・エントリがデフォルトの Oracle コンテキストの内部にない場合には、エントリの完全名か、あるいはその絶対名を、クライアント接続文字列の中で指定します。絶対名には、絶対パスを指定する場合とほぼ同様に、オブジェクトの名前とそのディレクトリ・サーバー内での場所が含まれます。salesdb を使用して Oracle9*i* データベースに接続するクライアントは、次のどちらかの接続文字列を使用します。

```
CONNECT username/password@cn=salesdb,cn=OracleContext,dc=com
CONNECT username/password@salesdb.com
```

表 4-1 に、データベース・サービス・エントリ、ネット・サービス名エントリおよびネット・サービス別名エントリのオブジェクト・クラスを示します。

表 4-1 Oracle Net Services LDAP の主要オブジェクト・クラス

オブジェクト・クラス	説明
orclDbServer	データベース・サービス・エントリの属性を定義します。
orclNetService	ネット・サービス名エントリの属性を定義します。
orclNetServiceAlias	ネット・サービス別名エントリの属性を定義します。

オブジェクト・クラス orclNetService および orclDbServer では、表 4-2 に示したオブジェクト・クラスを使用します。

表 4-2 Oracle Net LDAP の派生オブジェクト・クラス

オブジェクト・クラス	説明
orclNetAddress	リスナー・プロトコル・アドレスを定義します。
orclNetAddressList	アドレスのリストを定義します。
orclNetDescription	接続記述子を指定します。接続記述子には、データベースのリスナー・アドレスとサービスへの接続情報があります。
orclNetDescriptionList	接続記述子のリストを定義します。

これらのオブジェクト・クラスでは、接続記述子の内容を指定する属性を使用します。

関連項目： 付録 A「Oracle 固有の LDAP スキーマ拡張機能」

Oracle Net Services のエントリのためのセキュリティ保護装置

Oracle Net Services は、匿名ディレクトリ・ユーザーに対して読取りアクセス権を付与します。この権限により、どのユーザーもディレクトリ・ネーミング・エントリにアクセスし、これらのエントリを使用してデータベースに接続できます。

ネットワーキング・エントリは誰でも読み取ることができますが、これらのエントリを作成または変更できるのは、次のグループのメンバーのみです。

- OracleDBCreators グループ（`cn=OracleDBCreators,cn=OracleContext...`）または OracleContextAdmins グループ（`cn=OracleContextAdmins,cn=Groups,cn=OracleContext...`）のメンバーは、Database Configuration Assistant を使用してデータベース・サービス・エントリを作成する権限を持ちます。
- OracleNetAdmins グループ（`cn=OracleNetAdmins,cn=OracleContext...`）または OracleContextAdmins グループは、Oracle Net Manager を使用してネット・サービス名またはネット・サービス別名を作成する権限を持ちます。

Oracle Net Configuration Assistant は、前述のグループに対するこれらのアクセス権を Oracle コンテキストの作成中に設定します。

Oracle Net Services のためのディレクトリ配置要素

ディレクトリ・ネーミングを配置する前に、次のことについて検討してください。

- ディレクトリ・ネーミング・エントリは複数の Oracle コンテキストの下に格納できます。

  複数の Oracle コンテキストを使用し、所在地その他の条件別にエントリを論理的に分散できます。Oracle Net Configuration Assistant では特定の Oracle コンテキストへのデフォルトのアクセスがクライアントに提供されますが、クライアントは他の Oracle コンテキストの下にあるエントリにもアクセスできます。

- `tnsnames.ora` ファイルまたは Oracle Names Server に格納されているデータを、Oracle Internet Directory Server にエクスポートできます。

  `tnsnames.ora` ファイルに格納されているネット・サービス名をエクスポートするには、Oracle Net Manager 内で使用可能な「ディレクトリ・サーバー移行ウィザード」を使用します。Oracle Names Server に格納されているデータベース・サービスおよびネット・サービス名をディレクトリ・サーバーまたは LDIF ファイルにエクスポートするには、Oracle Names 制御ユーティリティを使用します。

  データをエクスポートすると、ディレクトリ・ネーミングを使用するようにクライアントを構成できます。または必要に応じて、Oracle Names Server を Oracle Names LDAP プロキシ・サーバーに変換し、ディレクトリ・ネーミングをサポートしていないクライアントをサポートできます。Oracle Names LDAP プロキシ・サーバーは、ディレクトリ・サーバーのプロキシ（代理）として機能するように構成されている Oracle Names Server です。Oracle Names LDAP プロキシ・サーバーは、起動と同時にネットワーク・オブジェクト情報をディレクトリ・サーバーから取得します。これにより、ディレ

クトリ・サーバー内のすべてのデータが一点で集中的に定義できるようになり、Oracle Names Server とディレクトリ・サーバーの両方を個々に、かつ同時にメンテナンスする必要がなくなります。

ドメイン・ツリーを持つ Oracle Names Server からそれと等価なディレクトリ情報ツリー（DIT）構造にデータをエクスポートしようとする場合は、DIT 内のサブドメインごとに Oracle コンテキストを作成する必要があります。

- 現在 Oracle Names で使用しているドメイン構造をレプリケートするか、あるいはまったく異なる構造を作成できます。まったく異なる構造を導入すると、クライアントが接続文字列で接続識別子を入力する方法が変わります。したがって、構造を変更する場合はその前に相対ネーミングおよび絶対ネーミングについて考慮することをお薦めします。

  複数の管理リージョンをサポートする Oracle Names LDAP プロキシ・サーバーの使用を計画している場合は、現在の Oracle Names 構造を DIT 構造にミラー化することをお薦めします。異なる構造を使用する場合、Oracle Names LDAP プロキシ・サーバー用に定義されているトポロジの変更が必要な場合があります。Oracle Net Services のツールはトポロジの変更をサポートしていません。

- ディレクトリ・ネーミングに対して管理上のセキュリティを確立します。

  ディレクトリ・ネーミング・エントリに対して、Oracle コンテキストごとに管理権限を設定します。たとえば、異なるディレクトリ・ネーミング・エントリに対する権限を 2 組の管理者に持たせる場合は、2 つの Oracle コンテキストを作成します。

- Oracle Net Configuration Assistant を使用してディレクトリの使用を構成する必要がありますが、このツールを使用してディレクトリ・ネーミング・エントリを作成することはできません。

  ネット・サービス名エントリとネット・サービス別名エントリの作成には Oracle Net Manager を使用し、データベース・サービス・エントリの作成には Database Configuration Assistant を使用します。

  関連項目：『Oracle9*i* Net Services 管理者ガイド』

Oracle Advanced Security

Oracle Advanced Security は、Oracle の数多くの機能を表現するために使用される用語です。これらの機能は、様々な異なるデータベースに複数のユーザー・アカウントが存在することによって起きる管理上およびセキュリティ上の課題に対処するためのものです。すべての機能において、エンタープライズ・ロールなどのユーザー関連情報の集中的な格納および管理を Oracle Internet Directory で行っています。たとえば、従業員が作業を変更するとき、管理者はディレクトリという 1 つの場所で情報を変更するだけで済みます。このような集中管理によって、管理コストが低減されるとともに、企業のセキュリティも向上します。

この項の内容は次のとおりです。

Oracle Advanced Security による Oracle Internet Directory の使用

Oracle Advanced Security は次の目的でディレクトリを使用します。

ユーザー資格証明の集中管理

ユーザーのデータベース・パスワードは、そのユーザーのユーザー・エントリの属性として、個々のデータベースにではなくディレクトリに格納されます。

ユーザー認証の集中管理

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、対象のエンタープライズ・ユーザーが与えられた共有スキーマまたは所有スキーマの中でどの権限を持つのかを判断します。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・ロールを収めたコンテナです。たとえば、Claire Stevens というユーザーにエンタープライズ・ロール `clerk` を割り当て、それにグローバル・ロール `hrclerk` と `human resources` データベースに対する付随権限、さらにグローバル・ロール `analyst` と `payroll` 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 はマッピングを使用します。マッピングとは、エンタープライズ・ユーザーを個々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・スキーマを指すように指定するディレクトリ・エントリのことです。たとえば、複数のエンタープライズ・ユーザーについて、ユーザー名で個別のアカウントにマップするのではなく、スキーマ `sales_application` にマップできます。

単一パスワード認証

Oracle9*i* では、Oracle Advanced Security のオプションにより、エンタープライズ・ユーザーが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認証できます。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によって保護されます。この機能により、クライアントでの Secure Sockets Layer（SSL）の設定に伴うオーバーヘッドがなくなり、ユーザーが複数のパスワードを覚える必要がなくなります。

シングル・サインオン

集中管理された単一のパスワードを使用して認証するかわりに、SSL を通じて PKI ベースのシングル・サインオンを使用することもできます。この機能でも、単一パスワード認証と同様にディレクトリ内にユーザー・エントリを必要とします。また、ユーザーの Wallet を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 資格証明の集中的な格納

Oracle9*i* では、ユーザー Wallet をユーザーのエントリの属性としてディレクトリに格納できます。この機能により、モバイル・ユーザーは Enterprise Login Assistant を使用して自分の Wallet を取得してオープンできます。Wallet がオープンの間、認証は透過的になります。つまり、ユーザーは再度認証をする必要なく、自分がスキーマを所有または共有しているどのデータベースにもアクセスできます。

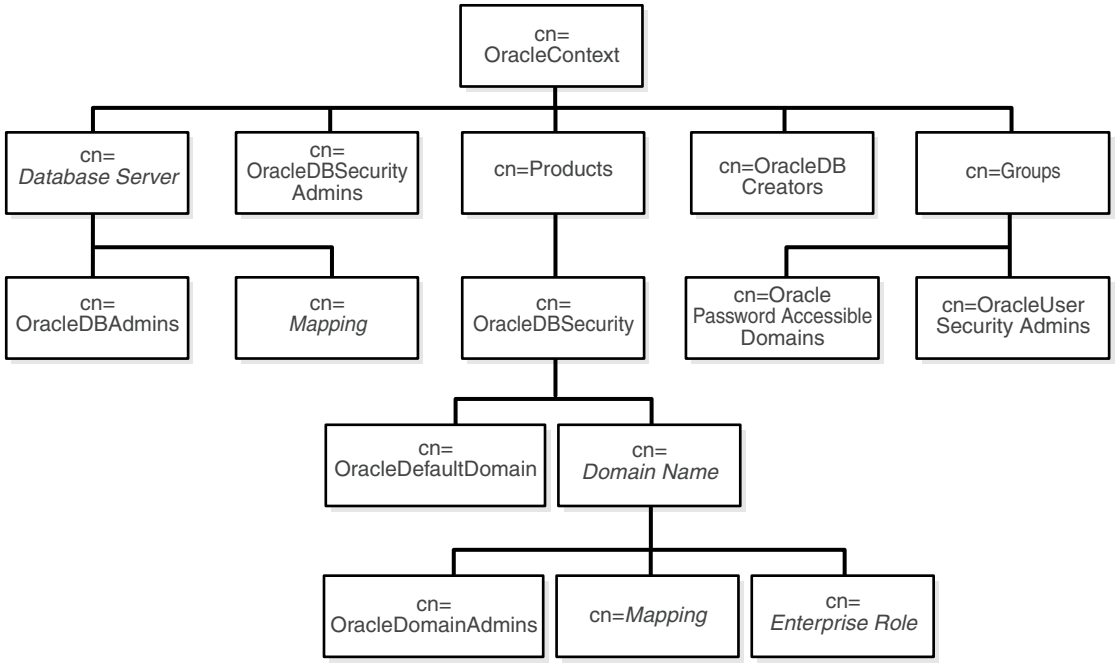
Oracle コンテキスト下の Oracle Advanced Security エントリ

Oracle Advanced Security の製品サブツリーでは、コンテナ `cn=OracleDBSecurity` を使用して、エンタープライズ・ロール、ユーザーからスキーマへのマッピング、およびエンタープライズ・ドメインのための各エントリを格納します。各ドメインの下にはドメインの管理者を指定するエントリ `cn=OracleDomainAdmins` があります。

エンタープライズ・ドメインは、本質的にはデータベースとエンタープライズ・ロール、そしてユーザーからスキーマへのマッピングが集まったものです。これらのドメインの 1 つには、Oracle コンテキストの作成時に作成される `cn=OracleDefaultDomain` があります。このドメインは管理者定義ドメインの代用として使用できます。

Oracle Advanced Security に関連するすべてのエントリを図 4-5 に示します。

図 4-5 Oracle Advanced Security に関連するディレクトリ・エントリ



Oracle Advanced Security のエントリのためのセキュリティ保護装置

Oracle Advanced Security は、ディレクトリ内の多数の点で ACL を使用し、データベース・セキュリティに関連するエントリを保護しています。これらの ACL のほとんどは、表 4-3 で説明している機能を持つグループのメンバーに対して権限を付与します。

表 4-3 Oracle Advanced Security のための管理グループ

管理グループ	機能
OracleDBSecurityAdmins	コンテナ `OracleDBSecurity` 内のオブジェクトに対する完全な権限。このグループの初期メンバーは、コンテキスト作成者です。
OracleDomainAdmins	対象ドメインに対する完全な権限。初期メンバーは、ドメインの作成者または更新者です。新しい Oracle コンテキストと `OracleDefaultDomain` が作成されている場合、初期メンバーはコンテキスト作成者になります。

表 4-3 Oracle Advanced Security のための管理グループ（続き）

管理グループ	機能
OracleUserSecurityAdmins	ユーザー・エントリに対する特殊な権限。このグループは、Wallet のパスワード・ヒントおよびパスワードに対する読取りおよび書込みの権限を持っています。初期メンバーは、Oracle コンテキストの作成者です。
OraclePasswordAccessibleDomains	ユーザーのデータベース・パスワード・ベリファイアを読み取るように信頼されたエンタープライズ・ドメイン。したがって、ユーザーはパスワード認証済みのグローバル・ユーザーとしてログインできます。初期メンバー（ダミー）は OracleDBSecurityAdmins です。
OracleDBCreators	Oracle コンテキストの下に新しいデータベース・エントリを追加するための権限。このグループの初期メンバーは、コンテキスト作成者です。
OracleDBAdmins	与えられたデータベースおよびそのサブツリーに対する完全な権限。

Oracle Advanced Security のためのディレクトリ配置要素

Oracle Advanced Security 機能を Oracle Internet Directory とともに配置する際は、必ず次のことを実行してください。

- 管理者がユーザーを 1 箇所で削除するだけで済むように、認証を集中化します。

  この機能により、ユーザーのすべての権限が取り消され、意図しない権限が残る危険性が少なくなります。

- セキュリティの専任者を集中化できるように、セキュリティ情報を集中化します。

  セキュリティに関する知識を持つディレクトリ管理者が、ディレクトリのセキュリティと、ユーザーのロールおよび権限を管理します。これにより、DBA が同じ機能を実行する負担から解放されます。その結果、実質的にセキュリティが向上します。

- エンタープライズ・ドメインにおけるメンバーシップの計画は慎重に行います。

  現行ユーザー・データベース・リンクが必ず単一のエンタープライズ・ドメイン内のドメイン間でのみ動作するようにします。データベースをドメインに割り当てるときは注意が必要です。これは、エンタープライズ・ユーザーのパスワード認証がドメイン・レベルで定義されるためです。エンタープライズ・ロールもまたドメイン・レベルで定義されます。データベース間でエンタープライズ・ロールを共有する場合は、必ずそれらのデータベースを同じドメインのメンバーにしてください。

  関連項目：『Oracle Advanced Security 管理者ガイド』の第 15 章「エンタープライズ・ユーザー・セキュリティの管理」

アプリケーション・コンテキスト

アプリケーション・コンテキストは、ユーザーのセッション情報を土台としたアプリケーションを開発できるようにする、データベース・セキュリティ機能です。アプリケーション・コンテキストは、アプリケーションがアクセス制御の施行に使用できる属性について、それらの定義、設定およびアクセスのための手段を提供します。アプリケーション・コンテキストの 4 つのタイプであるグローバル、ローカル、外部および集中化のうち、グローバルに初期化された（initialized globally）句を使用して作成される集中化コンテキストは、Oracle Internet Directory を使用します。

この項の内容は次のとおりです。

アプリケーション・コンテキストによる Oracle Internet Directory の使用

アプリケーション・コンテキストのユーザーは、Oracle Internet Directory 内でユーザー用に設定された初期コンテキストの属性を、エントリの形式で持つことができます。ユーザーが Oracle Advanced Security を使用して正常に認証されると、ユーザーのグローバル・ロールがディレクトリから取得され、それからユーザーのグローバル・アプリケーション・コンテキストが取得されます。ユーザーがデータベースにログオンするまでに、ユーザーのグローバル・ロールと初期アプリケーション・コンテキストが設定されます。

アプリケーション・コンテキストが Oracle Internet Directory をどのように使用するのかを理解するために、HR という仮想のアプリケーション・コンテキストの設定に関わる手順について考えてみます。ここでは、アプリケーション管理者がこのコンテキストを使用して、人員表が含まれている HR という名前のアプリケーション・モジュールにユーザーがアクセスできるようにする必要があるとします。このユーザーの情報は人員表にではなくディレクトリに格納されています。しかし、管理者は、GetPersonnelData という PL/SQL プロシージャを使用して HR コンテキストをコールすることで、ユーザーに対して人員表への制限付きアクセスを許可します。

1. 管理者は、ユーザーをディレクトリ内のエンタープライズ・ユーザーとして識別する DN を使用して、user1 というグローバル・ユーザーをデータベースに作成します。
2. 管理者は、PL/SQL を使用して作成されたコンテキスト・パッケージを実装する SQL コマンドを使用して、アプリケーション HR のためのアプリケーション・コンテキストをデータベースに作成します。
3. 管理者は LDIF スクリプトを使用して、ディレクトリ・エントリ HR を作成します。そして、サブエントリ Title および Manager をエントリ HR に割り当てます。管理者はこれらすべてのエントリをドメイン MyDomain 内に格納します。このドメインはコンテナ OracleDBAppContext 内にあります。

4. 管理者は、エントリ Manager への属性として、グローバル・ユーザー名 user1 を割り当てます。
5. 管理者は PL/SQL プロシージャ（この場合は GetPersonnelData）を書き込みます。このプロシージャはアプリケーション・コンテキストを使用して、コンテキストと一致する値を持つレコードのみを取得します。

user1 がドメイン myDomain に属するデータベースに接続すると、ユーザーの役職が Manager に設定され、ユーザーに関するその他の情報は LDAP ディレクトリから取得されます。たとえば、ユーザーのユーザー・エントリにオブジェクト・クラス inetOrgPerson があれば、このオブジェクトの属性が取得されます。

ユーザーがコマンド GetPersonnelData を実行すると、ユーザーは役職が Manager である人物のレコードのみを取得します。

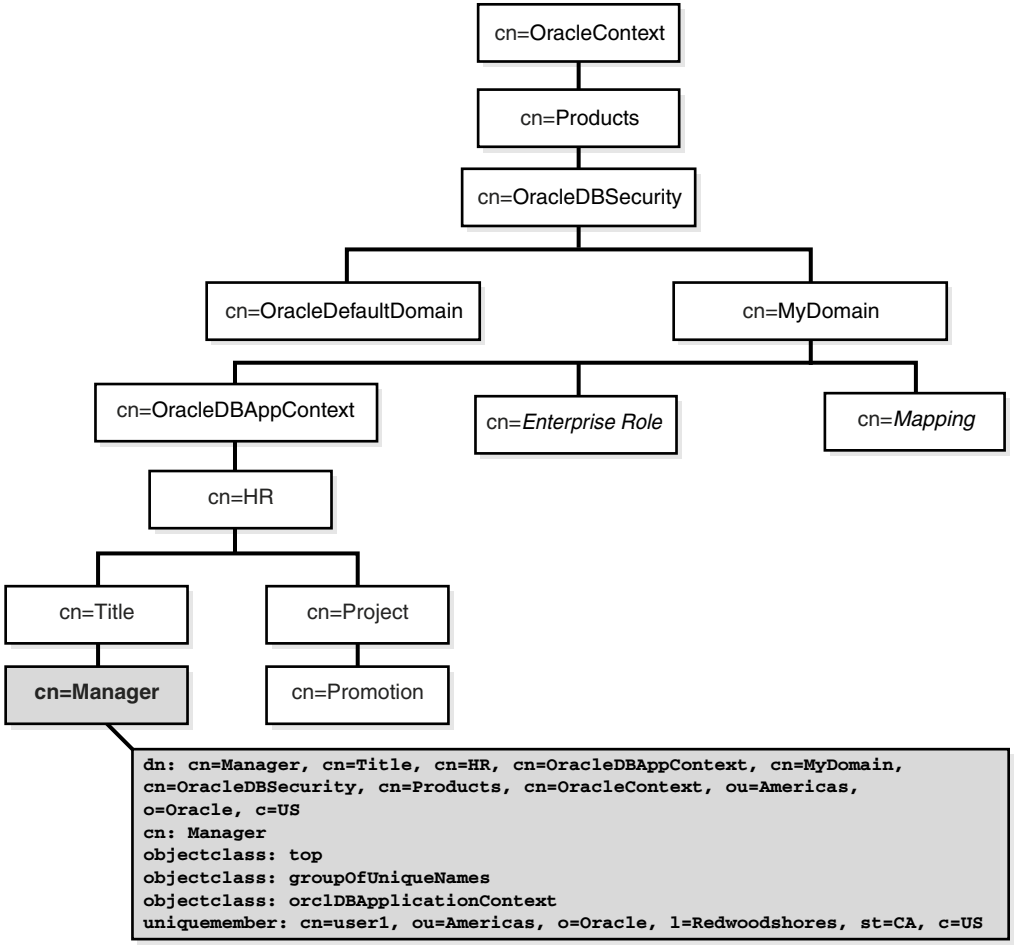
Oracle コンテキスト下のアプリケーション・コンテキスト・エントリ

4-16 ページの図 4-6 に示すように、集中的に初期化されたアプリケーション・コンテキストでは 4 つのタイプのエントリがディレクトリに格納されます。

- コンテキスト・コンテナ ― OracleDBAppContext
- コンテキスト名前空間 ― この場合は HR
- コンテキスト属性 ― この場合は Title
- コンテキスト値 ― この場合は Manager

アプリケーション・コンテキストの値はオブジェクト・クラス orclDBApplicationContext に属します。このオブジェクト・クラスは groupOfUniqueNames のサブクラスです。アプリケーション・コンテキストのエントリは、そのアプリケーション・コンテキストが適用されるエンタープライズ・ドメイン（この場合は MyDomain）の下にあるコンテナ OracleDBSecurity の中にあります。

図 4-6 コンテキスト値に対応する属性を示したアプリケーション・コンテキストのディレクトリ情報ツリー



アプリケーション・コンテキストのエントリのためのセキュリティ保護装置

集中的に初期化されるアプリケーション・コンテキストのディレクトリ・エントリは、アクセス制御リスト（ACL）により、コンテナ `OracleDBSecurity` およびエンタープライズ・ドメインの 2 つのレベルで保護されます。前者のレベルでは、OracleDBSecurityAdmins がすべてのエンタープライズ・ドメインとそれらのサブツリーへの完全なアクセス権を持ちます。後者のレベルでは、OracleDomainAdmins が各自のドメインに対するアプリケーション・コンテキスト値への完全なアクセス権を持ちます。コンテキストが正しく動作するためには、ドメインに属するすべてのデータベースにおいて、そのドメイン内のコンテキストに属する値をデータベースが読み取ることができる必要があります。

関連項目：『Oracle9*i* アプリケーション開発者ガイド - 基礎編』

Oracle Advanced Queuing

Oracle Advanced Queuing はメッセージ・キューイング・システムと Oracle データベースとを組み合せた機能で、キュー表を使用してメッセージに関する情報を格納します。このようなモデルにより、異なるマシンおよびデータベースのキューどうしで一貫した格納とメッセージ伝達の実現が容易になります。

Oracle Advanced Queuing は様々なプログラム環境を使用して、Point-to-Point およびパブリッシュ・サブスクライブという 2 つのメッセージ送信モードを提供します。前者のモードでは、送信側と受信側で共通のキューを使用し、ただ 1 つの受信先を持つメッセージを交換します。後者のモードでは、メッセージがサブスクライバと呼ばれる複数の受信者によって受信される場合があり、サブスクライバは異なるデータベース上に設置された複数のキューにサブスクライブできます。このようなマルチ・コンシューマ・キューのことを、グローバル・トピックと呼びます。

この項の内容は次のとおりです。

Oracle Advanced Queuing による Oracle Internet Directory の使用

Oracle Advanced Queuing は、Oracle Internet Directory をグローバル・トピックのメタデータ用のリポジトリとして使用し、データベース・イベント通知用のレジストリとしても使用します。前者の場合、Java メッセージ・サービスのためのコネクション・ファクトリおよび宛先を、Java Native Directory Interface（JNDI）からアクセス可能な名前空間に格納できます。後者の場合、クライアントは「オープン登録」を実行できます。つまり、クライアントは単一ディレクトリ・エントリを使用して複数のデータベースに対する登録を実行できます。

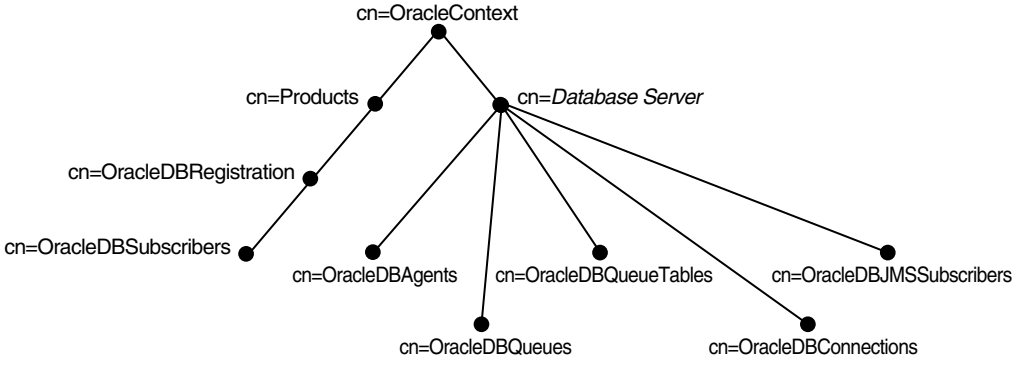
キュー、キュー表またはサブスクライバがデータベースに作成されるとき、データベースはオブジェクト・メタデータを収めるディレクトリ・エントリを自動的に作成します。たとえば、キュー用のディレクトリ・エントリには、特定のキュー表を参照する情報と、対応するキューが複数の（マルチ）コンシューマ・キューであるかどうかを示す情報が格納されます。

PL/SQL または Java のインタフェースを使用すると、別名用および JMS コネクション・ファクトリ用のディレクトリ・エントリを追加することもできます。後者は、データベースとの接続の確立に必要な構成パラメータからなります。

Oracle コンテキスト下の Oracle Advanced Queuing エントリ

図 4-7 に示すように、Oracle Advanced Queuing はグローバル・トピックのためのエントリを、それらの適用対象のデータベース・サーバーのすぐ下に格納します。

図 4-7 Oracle Advanced Queuing のディレクトリ情報ツリー



Oracle Advanced Queuing はこの目的のために 5 つのコンテナを使用します。そのうちの 1 つには、グローバル・サブスクリプションのサポートに必要な各オブジェクト型が格納されます。また、別名もデータベース・サーバー・エントリのすぐ下に格納されます。これら 5 つのコンテナの内容を表 4-4 に示します。

表 4-4 グローバル・トピック・エントリ用のコンテナ

コンテナ	内容
cn=OracleDBAgents	データベース・エージェント。
cn=OracleDBQueues	キュー。キューのサブスクライバは対応するキュー・エントリの下に置かれます。
cn=OracleDBQueueTables	キュー表。
cn=OracleDBConnections	コネクション・ファクトリ。
cn=OracleDBJMSSubscribers	JMS サブスクライバ。キュー・サブスクライバに関する詳細情報のほか、サブスクライバ・エントリへのリンクが格納されます。

データベース・イベント通知のためのクライアント登録には、それぞれ独自の cn=OracleDBRegistration というコンテナがあります。このコンテナは製品コンテナのすぐ下にあります。cn=OracleDBRegistration の下にはエントリ cn=OracleDBSubscribers があります。このエントリは、登録エントリを追加、変更および削除することを許可された LDAP ユーザーを定義します。

Oracle Advanced Queuing のエントリのためのセキュリティ保護装置

グローバル・トピックに関連するエントリは誰でも読取りが可能ですが、それらのエントリを変更できるのは作成元のデータベース・サーバーのみです。イベント通知の LDAP 登録の場合は、グローバル・ロール global_aq_user_role の権限を付与されたユーザーが登録エントリを追加、変更および削除できます。

グローバル・ロールは Oracle9*i* では権限グループとして実装されているため、グローバル・ロール global_aq_user_role を含むエンタープライズ・ロールを付与された人物は、すべて権限グループ cn=OracleDBSubscribers に含まれます。各データベース・サーバーもまた cn=OracleDBSubscribers のメンバーです。

登録エントリには、その作成者とデータベース・サーバーのみそのエントリを変更できることを保証する ACI が含まれることがあります。

Oracle Advanced Queuing のためのディレクトリ配置要素

Oracle Internet Directory を Oracle Advanced Queuing とともに使用する前に、必ず次のことを実行してください。

- 各エンタープライズ・ドメインにエンタープライズ・ロール `enterprise_aq_user_role` が含まれていることを確認します。
- 権限グループ `cn=orclDBSubscribers` が適切に設定されていることを確認します。これには、データベースと `enterprise_aq_user_role` がこのエントリの属性であることを調べます。
- グローバル・ロール `global_aq_user_role` が `enterprise_aq_user_role` の属性であることを確認します。
- `enterprise_aq_user_role` が `cn=OracleDBAQUsers` の属性であることを確認します。
- エンタープライズ・ドメイン間でデータベースを移動する場合は、`global_aq_user_role` を古いドメインの `enterprise_aq_user_role` から削除します。そして、それを新しいドメインの `enterprise_aq_user_role` に追加します。

関連項目：『Oracle9*i* アプリケーション開発者ガイド - アドバンスト・キューイング』

Oracle Dynamic Services

Oracle Dynamic Services は、E-Business において既存のインターネット、イントラネットおよびデータベースの各情報サービスを登録および再利用するためのプログラム・フレームワークを提供します。Oracle Dynamic Services により、E-Business はこれらのサービスを各自の要件に対応するように変換し適合させることが可能になります。

注意： Oracle9*i* データベース リリース 2（9.2）以降は、Oracle Dynamic Services は使用されなくなります。

Oracle9*i* Application Server リリース 2（9.0.2）以降の Oracle では、統合された J2EE 準拠の Web サービス・プラットフォームが提供されます。Oracle Dynamic Services は、Oracle9*i*AS Web Services に XML/HTML Stream Processing Tool として統合されました。このツールを使用すると、Web サービス開発者は HTML/XML ソース（静的 Web ページや HTML フォームなど）を Enterprise JavaBeans（EJB）として表現し、J2EE クライアント・アプリケーション開発者が使用できるように Oracle9*i*AS に配置できます。また、開発者は J2EE アプリケーションを SOAP 準拠の Web サービスとして公開し、外部クライアントが検出できるように、対応する Web サービス記述（WSDL）を提供される UDDI リポジトリに登録できます。

これらの機能の詳細は、『Oracle9*i*AS Web Services 開発者ガイド』を参照してください。Oracle9*i*AS リリース 2（9.0.2）では、業界標準に準拠した、完全に統合された J2EE および Web サービス配置プラットフォームが提供されます。現行の Dynamic Services の機能は、Oracle9*i*AS プラットフォームに統合されており、Dynamic Services 端末リリースは Oracle9*i* データベース リリース 2（9.2）で提供されます。

Oracle Dynamic Services フレームワークを使用すると、インターネット上の様々なコンテンツ・ソースからサービスを作成および集約できます。Oracle Dynamic Services は次のソースからのコンテンツ・アクセスをサポートしています。

- SQL および PL/SQL を使用しているデータベース。
- Simple Object Access Protocol（SOAP）を使用しているリモートのサービス・リポジトリ。
- HTTP/HTTPS を使用しているインターネット・アプリケーション・リポジトリ。
- アプリケーション開発者またはその他の拡張可能アダプタによって拡張または強化された、サポート対象のプロトコルを使用している、その他のアプリケーション・リポジトリ。

Oracle Dynamic Services フレームワークは、次のものを含むあらゆるプロトコルを経由した任意の場所へのサービスの配置をサポートしています。

- Simple Mail Transfer Protocol（SMTP）

  Oracle Dynamic Services フレームワークの内部では、SMTP を使用してシステム・メッセージやビジネス・メッセージを生成できます。

- Wireless Application Protocol（WAP）

  サービスの実行結果を任意のモバイル・デバイスに配信できます。

E-Business では、自社のデータベース・アプリケーション、ホスト・アプリケーション、オンライン交換およびポータル（B2B、B2C、B2M）の中で、Oracle Dynamic Services を使用できます。

この項の内容は次のとおりです。

Oracle Dynamic Services による Oracle Internet Directory の使用

Oracle Dynamic Services フレームワークには 2 つのレジストリがあり、どちらもディレクトリ・ベースです。

- Oracle Dynamic Services サービス・レジストリ（SR）

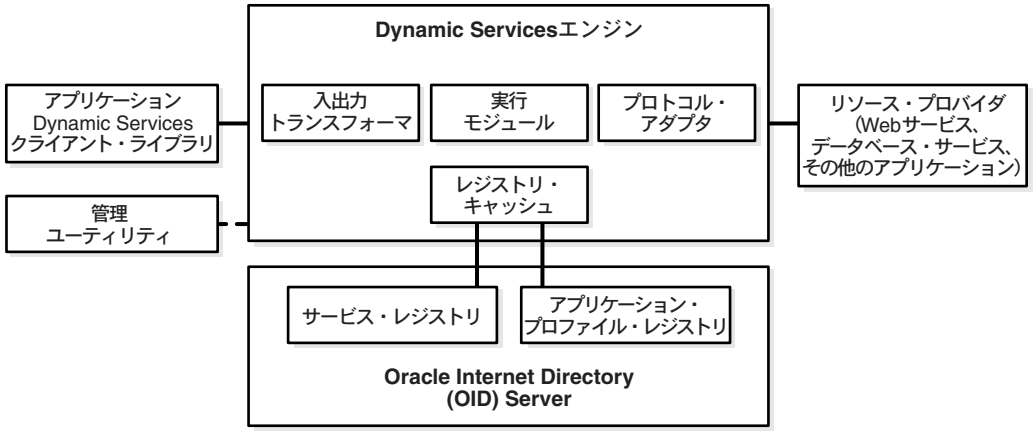
  サービス・レジストリは、すべてのサービスを定義するためのプレースホルダです。コンシューマはクライアント・ライブラリを使用してサービス・レジストリの問合せと更新ができます。

- Oracle Dynamic Services アプリケーション・プロファイル・レジストリ（UPR）

  アプリケーション・プロファイル・レジストリは、すべての検証済み Dynamic Services エンジン（DSE）・アプリケーションのためのプレースホルダです。これらの DSE アプリケーションは DS コンシューマとみなされます。レジストリにはアクセス・ポリシーとアプリケーション・プロパティが格納されます。

図 4-8 は、これら 2 つのレジストリが Oracle Dynamic Services フレームワーク内の他のコンポーネントとどのように対話するのかを示したものです。

図 4-8 Oracle Dynamic Services フレームワーク・アーキテクチャ内部の LDAP サーバー



Oracle Dynamic Services フレームワークは、サービス定義とコンシューマ・プロファイルの格納と管理を行うために Oracle Internet Directory を使用します。

ディレクトリのボトルネック化の回避とパフォーマンスの向上を図るために、DSE インスタンスはローカル・レジストリ・キャッシュ上の操作を先に処理します。DSE インスタンスは、これらの操作によってレジストリが変更される場合にのみ、ディレクトリ・サーバーに通知します。そのような変更では、たとえばサービス・エントリの削除が伴うことがあります。

レジストリ・キャッシュとディレクトリ内の中央のレジストリとの間で整合性を保つために、DSE インスタンスはディレクトリが同じ処理を実行した後にのみ、キャッシュを更新します。この機能によって DSE インスタンスどうしの整合性も保たれます。

4-24 ページの図 4-9 は、管理者が Oracle Dynamic Services 対応の新しいサービスである YahooQuote サービスを 1 つの DSE インスタンスを通じて登録するときに発生する同期プロセスを示したものです。

1. 管理者は 1 つの DSE インスタンスに接続して YahooQuote サービスを登録します。このサービスは「`urn:com.yahoo:quote`」という一意なサービス ID を持ち、「business, finance, stock」というサービス・カテゴリに属します。
2. DSE インスタンスはサービス登録要求を処理し、サービス・パッケージを自身のローカル・サービス・レジストリに事前登録します。事前登録プロセスでエラーがなければ、DSE インスタンスは YahooQuote サービス・パッケージを登録のためにディレクトリ・サーバーに送ります。

3. Oracle Internet Directory は YahooQuote パッケージを登録します。
4. ディレクトリは、YahooQuote サービスを登録した後 DSE インスタンスにその旨を通知します。DSE インスタンスはローカル・レジストリ・キャッシュを更新し、登録が完了したことを管理者に知らせます。

図 4-9 YahooQuote サービスの登録

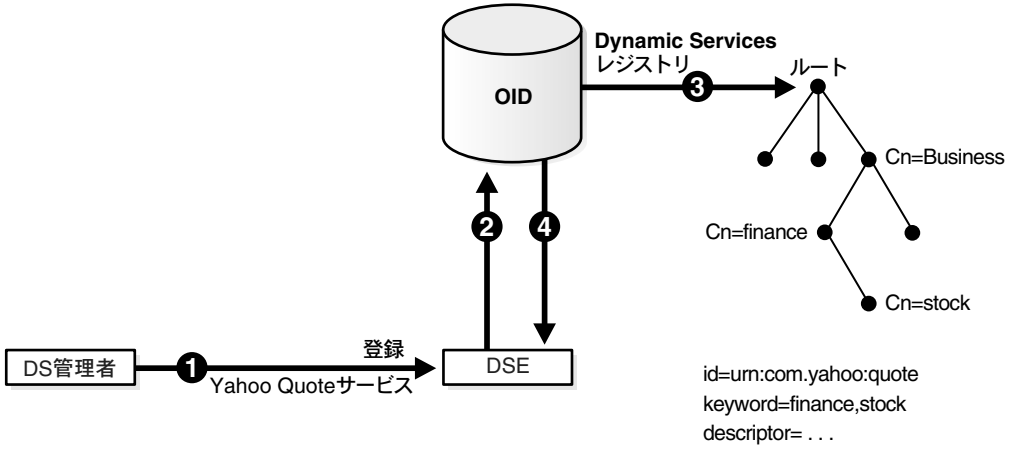
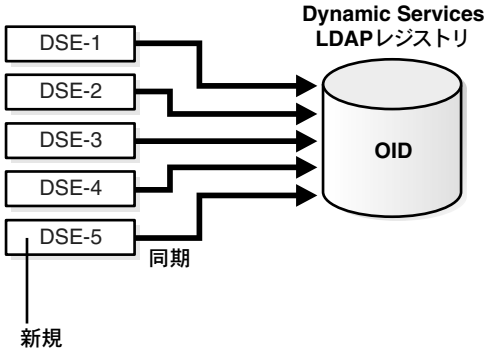


図 4-10 は、管理者が新しい DSE インスタンスを起動したときに発生する同期プロセスを示したものです。起動処理中、このインスタンスはディレクトリに接続して中央のレジストリと同期をとります。

図 4-10 新しい Dynamic Services エンジン・インスタンスのためのレジストリ同期プロセス



Oracle コンテキスト下の Oracle Dynamic Services エントリ

Oracle Dynamic Services は次のエントリを Oracle Internet Directory に格納します。

- `cn=OracleDynamicServicesSR`

  Oracle Dynamic Services 用サービス・レジストリ。Oracle Dynamic Services フレームワーク内部で作成されたすべてのサービス・カテゴリと登録済みサービスがこのエントリの下に格納されます。

- `cn=OracleDynamicServicesUPR`

  Oracle Dynamic Services 用アプリケーション・プロファイル・レジストリ。個々の有効な Dynamic Services アプリケーションのプロファイルがこのエントリの下に格納されます。これらのプロファイルには、サービス固有のプロパティやサービスのアクセス権限に関する情報があります。

- `cn=OracleDynamicServicesDomain`

  1 組の DSE インスタンスの適用範囲を定義するエントリ。各 DSE がこのエントリの下で表現されます。エントリには、個々のエンジン・インスタンスの接続やセキュリティなどのプロパティを表す詳細な属性セットが格納されます。

- `cn=OracleDynsDocument`

  サービス関連文書（サービスの入力スキーマや出力スキーマなど）のためのサブツリー。サービス登録プロセスの間、一意な文書 ID が文書に割り当てられます。実行時には、文書が文書 ID によって取得されます。

- `cn=OracleDynsBinObject`

  サービス関連のすべてのバイナリ・ファイルが格納されるエントリ。これらのファイルの 1 つはサービス・パッケージに含まれている jar ファイルです。

- `cn=OracleDynsSPOrganization`

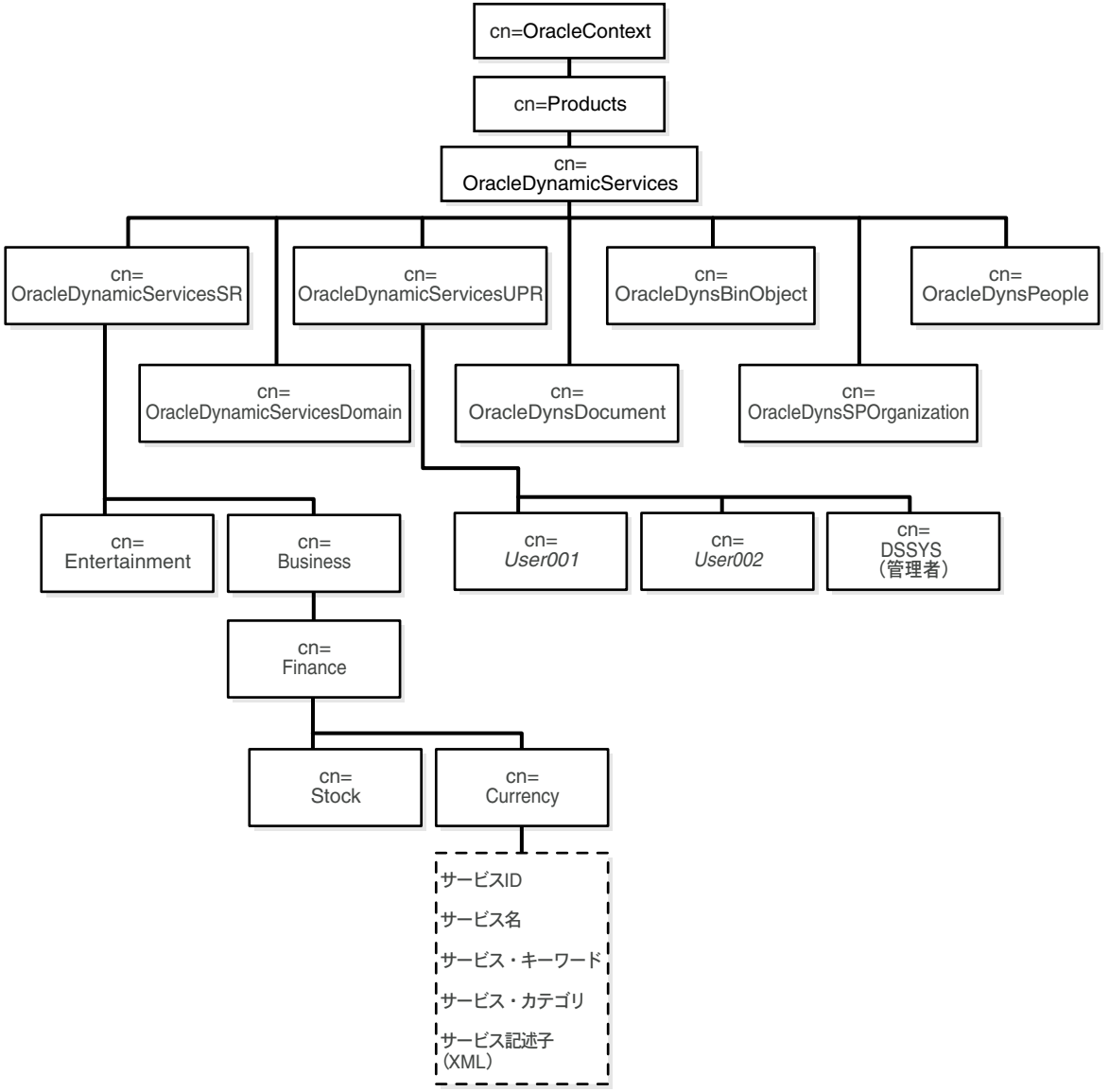
  サービス・プロバイダの組織プロファイルの格納に使用されるサブツリー。プロファイルにはそれぞれ会社名のエントリ、会社のロゴ URL、会社の Web サイト URL などが含まれます。

- `cn=OracleDynsPeople`

  電子メール・アドレスや電話番号などのすべての連絡先情報が格納されるエントリ。

4-26 ページの図 4-11 は、Oracle Dynamic Services のディレクトリ・サブツリーの構造を示したものです。

図 4-11 サービスの 1 つである通貨の属性の型を示した Oracle Dynamic Services のディレクトリ情報ツリー



Oracle Dynamic Services のエントリのためのセキュリティ保護装置

Oracle Dynamic Services は、管理権限を持つユーザーである DSAdmin グループに対して、完全な（読取り / 書込み）アクセス権を付与します。匿名ディレクトリ・ユーザーは、サービス・レジストリおよびアプリケーション・プロファイル・レジストリにはアクセスできません。

Oracle Dynamic Services のためのディレクトリ配置要素

Oracle Internet Directory を Oracle Dynamic Services とともに使用する前に、次の要素について考慮してください。

- Oracle Dynamic Services のレジストリ・エントリは汎用目的で設計されたものではありません。これらは Oracle Dynamic Services 専用であり、DSAdmin グループのみから、標準の Java LDAP インタフェースを使用してアクセスできます。
- ディレクトリ・サーバーのロード・バランシングを行うことが Oracle Dynamic Services にとって非常に重要です。ディレクトリ・サーバー・インスタンスを設定する前に、サーバーの通信量のレベルについて十分な見積りを立ててください。ディレクトリ・サーバーへのアクセス頻度が高くなるにつれて、ディレクトリ・サーバー・インスタンスのレプリケートが必要になることがあります。
- Oracle Dynamic Services のレジストリ・データを移行する場合は特に注意が必要です。移行の際はディレクトリの設計に関する注意事項を考慮してください。
- Oracle Dynamic Services のインストール時にルートの Oracle コンテキストがディレクトリに存在しない場合は、エントリ `cn=US` がデフォルトのルートとして指定されます。

Oracle Dynamic Services は Oracle Internet Directory を使用するように認定されています。つまり、Oracle Dynamic Services のレジストリ構造は Oracle Internet Directory のディレクトリ・サービスと互換性があります。オラクルの LDAP Schema Council では、この製品のオブジェクト・クラスと属性について十分なレビューを実施しています。

関連項目：『Oracle Dynamic Services User's and Administrator's Guide』

5

ディレクトリ使用構成の完了

この章では、Oracle ホームで Oracle Internet Directory Server を使用できるようにするための構成手順について説明します。最初に、すべての Oracle 製品に共通の構成手順について説明し、次に、個々の Oracle 製品に固有のディレクトリ構成作業を説明しているリソースへの参照を示します。

この章の内容は次のとおりです。

ディレクトリ使用の前提条件

概念上、Oracle RDBMS でディレクトリとの通信を行うには、次の 5 つの主要前提条件があります。

- ディレクトリには、現行バージョンの Oracle スキーマをインストールする必要があります。Oracle スキーマには、Oracle 固有のオブジェクト・クラスと属性がすべて含まれており、Oracle Internet Directory に事前にインストールされます。
- ディレクトリには、現行バージョンの Oracle コンテキストをインストールする必要があります。これは、Oracle 固有のオブジェクトがすべて格納されるサブツリーです。Oracle Internet Directory は、Oracle コンテキストがディレクトリのルートに事前にインストールされた状態で出荷されます。他の Oracle コンテキストを他の場所に作成することもできますが、ルート・コンテキストは削除しないでください。
- Oracle ホームをディレクトリ使用のために構成する必要があります。Oracle ホームを構成するには、Oracle プログラムでディレクトリに接続できるように、ldap.ora ファイル内でパラメータを設定する必要があります。これらのパラメータは、ディレクトリのホスト、ポートおよびタイプの値と、Oracle コンテキストの場所の値で構成されます。
- ディレクトリには、データベースをディレクトリにバインド（ログイン）できるように、データベース・エントリを含める必要があります。
- Oracle Advanced Security など、一部のディレクトリ対応機能の場合は、ディレクトリを Secure Sockets Layer（SSL）による 2 方向認証に使用可能にする必要があります。この機能を使用するには、ディレクトリ内に Oracle Wallet が必要です。

最新バージョンの Oracle Internet Directory を使用していれば、最初の 2 つの前提条件はデフォルトで満たされます。最新バージョンを使用していない場合は、Oracle Net Configuration Assistant によって Oracle スキーマと Oracle コンテキストの両方が更新されます。また、このツールでは ldap.ora ファイルも作成されます。Database Configuration Assistant は、4 番目の前提条件を満たします。つまり、Database Configuration Assistant によって、データベース登録と呼ばれるプロセスでディレクトリ内にデータベース・エントリが作成されます。ディレクトリ使用構成を完了するには、両方のツールを実行する必要があります。次の項では、それぞれのツールの実行方法について説明します。

Wallet の作成方法およびディレクトリとの間のアップロードおよびダウンロードの方法は、『Oracle Advanced Security 管理者ガイド』の第 17 章「Oracle Wallet Manager の使用方法」を参照してください。ディレクトリが Oracle Internet Directory の場合に、SSL インスタンスを作成して起動する方法は、『Oracle Internet Directory 管理者ガイド』の第 3 章の「タスク 2: サーバー・インスタンスの起動」を参照してください。

ディレクトリ使用構成のオプション

ディレクトリ使用構成を完了するには、次の 3 つの方法があります。

1. データベースのインストール後にディレクトリ使用を構成します。この方法では、Oracle ホームでディレクトリを使用できます。
2. データベースをインストールして登録するときに、ディレクトリ使用を構成します。この方法は、カスタム・データベース・インストールの一部であり、第 1 の方法の代替案です。
3. ディレクトリを使用してデータベースに接続するように、クライアントを構成します。この方法は、クライアント・インストールの一部です。

データベースのインストール後のディレクトリ使用の構成

Oracle Net Configuration Assistant と Database Configuration Assistant を使用すると、いつでもディレクトリ使用構成を完了できます。このオプションを選択した場合は、両方のツールをスタンドアロン・モードで実行する必要があります。最初のツールでは、ディレクトリ・サーバーを選択できます。2 番目のツールでは、データベースを登録します。つまり、ディレクトリにデータベース・エントリを作成します。このエントリがなければ、Oracle ホームからはディレクトリにアクセスできません。

この項の内容は次のとおりです。

Oracle Net Configuration Assistant を使用したディレクトリ使用の構成

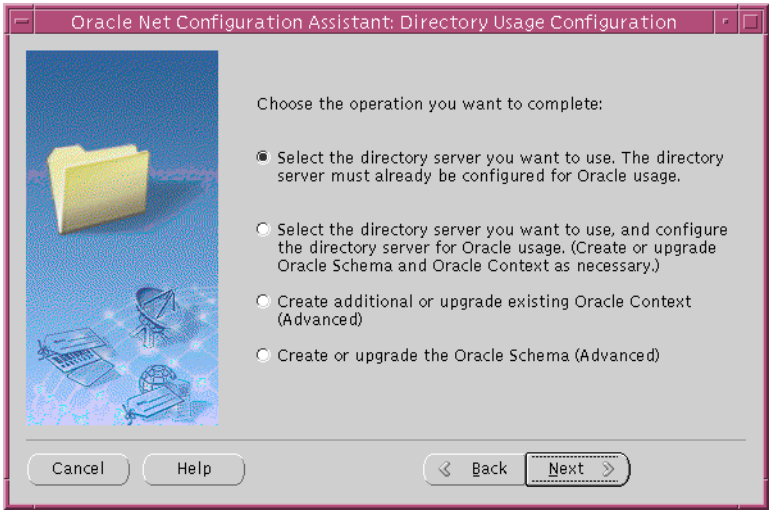
ディレクトリ・サーバーの使用を構成するには、次を実行します。

1. Oracle Net Configuration Assistant を起動します。
   - UNIX の場合は、`$ORACLE_HOME/bin` に移動してコマンド `netca` を入力します。
   - Windows NT の場合は、**「スタート」→「プログラム」→「Oracle - *HOME_NAME*」→「Configuration and Migration Tools」→「Net Configuration Assistant」**を選択します。

   「Welcome」ページが表示されます。
2. 「Directory Service Usage Configuration」を選択して**「Next」**を選択します。

   5-4 ページの図 5-1 に、「Directory Usage Configuration」ページを示します。

図 5-1 Oracle Net Configuration Assistant: 「Directory Usage Configuration」ページ



3. このページで 4 つのオプションのうち 1 つを選択し、ウィザードの指示に従って作業を進め、ディレクトリ使用構成を完了します。

オプションは、次のとおりです。

オプション 1: 「Select the directory server you want to use」

すでにディレクトリ対応機能を使用するように構成してあるディレクトリ・サーバーを自分の Oracle ホームで使用できるようにするには、このオプションを選択します。

構成が完了すると、このオプションによってコンピュータからディレクトリ内のエントリを参照できるようになります。次のプロンプトが表示されます。

- ディレクトリ・サーバーのタイプを選択します。
- ディレクトリ・サーバーのホスト名とポートを特定します。デフォルトの非 SSL ポート番号は 389、デフォルトの SSL ポート番号は 636 です。
- このサーバーから Oracle エントリにアクセスできる、Oracle コンテキストのあるディレクトリ・エントリを選択します。

オプション 2:「Select the directory server you want to use, and configure the directory server for Oracle usage」

ディレクトリ・サーバーをディレクトリ対応機能のために構成し、自分の Oracle ホームでそのディレクトリを使用できるようにするには、このオプションを選択します。このオプションは、これらの機能を初めて構成する管理者のために用意されています。

構成が完了すると、Oracle ホームからディレクトリ内のエントリを参照できるようになります。

このオプションはオプション 1 と同じですが、Oracle スキーマが存在しない場合や旧バージョンの場合に、その作成またはアップグレードを求めるプロンプトが表示されます。Oracle コンテキストを作成または指定するためには、スキーマ・バージョンが適切であることが前提条件になります。Oracle コンテキストの選択では 3 つのオプションがあります。

1. ルートの Oracle コンテキストをデフォルトとして受け入れます。ルートの Oracle コンテキストは、ディレクトリのルート・エントリ（最上位エントリ）にあります。
2. Oracle コンテキストのドロップダウン・リストから選択します。
3. Oracle コンテキストが存在しない場合は、選択したディレクトリ・エントリの下に作成します。Oracle コンテキストを追加するには、オプション 3 を使用する必要があります。一部の Oracle 機能では、ルート Oracle コンテキスト（ディレクトリのルート・エントリにある Oracle コンテキスト）が必要であるため注意してください。ルート Oracle コンテキストが見つからない場合は、Oracle Net Configuration Assistant で表示されるディレクトリ・エントリのドロップダウン・リストから「root entry」を選択して作成できます。

オプション 3:「Create additional or upgrade existing Oracle Context」

既存の Oracle コンテキストが存在する場合に、新規の Oracle コンテキストをディレクトリに追加するには、このオプションを選択する必要があります。また、このオプションを選択すると、旧バージョンのコンテキストをアップグレードできます。

Oracle コンテキストを作成するためには、次のものがディレクトリ・サーバーに存在する必要があります。

- Oracle コンテキストを作成するディレクトリ・エントリ
- 現行の Oracle スキーマ

Oracle コンテキストが古いバージョンである場合は、それをアップグレードするようプロンプトされます。アップグレードが重要なのは、Oracle9*i* データベースは Oracle8*i* 以前の Oracle コンテキストでは動作しないためです。アップグレードした Oracle コンテキストを使用すると、将来作成する Oracle8*i* データベースを登録できます。

オプション 4:「Create or upgrade the Oracle Schema」

Oracle Internet Directory に Oracle スキーマが含まれていない場合は、オプション 4 を使用すると、オプション 1 および 2 で説明したディレクトリ使用構成全体を行わなくてもスキーマを作成できます。また、オプション 4 を使用すると、Oracle スキーマをアップグレードできます。

注意：

- Oracle コンテキストを作成するには、新規コンテキスト用に選択したエントリの下に新規サブツリーを作成するための資格証明が必要です。つまり、ディレクトリ管理者であるか、ディレクトリ内のどこかの ACL によってエントリの変更が許可されている必要があります。
- Oracle スキーマを更新するには、ディレクトリ管理者の資格証明が必要です。
- 後で異なる Oracle コンテキストを選択したり、新しい Oracle コンテキストを作成した場合は、必ず自分のデータベースをこのコンテキストの下に登録してください。
- ディレクトリ使用構成を、サーバーでの Enterprise Edition または Standard Edition のインストールの一部として完了することはできません。これらのインストール・オプションを選択した場合は、Oracle Net Configuration Assistant をスタンドアロン・モードで実行する必要があります。

Database Configuration Assistant を使用したデータベースの登録

Oracle Net Configuration Assistant の実行後に、Database Configuration Assistant を実行してデータベースをディレクトリに登録します。データベースを登録するには、Database Registration グループまたは OracleContextAdmins グループのメンバーであるか、ディレクトリのスーパー・ユーザーである必要があります。この 2 つのグループに管理者を追加するには、Oracle Enterprise Security Manager を使用します。このツールの使用方法は、『Oracle Advanced Security 管理者ガイド』の第 19 章「Oracle Enterprise Security Manager の使用方法」を参照してください。エンタープライズ・ユーザー・セキュリティを使用している場合は、Enterprise Security Manager を使用してデータベースを登録できることに注意してください。

データベースをディレクトリに登録するには、次のように Database Configuration Assistant をスタンドアロン・モードで使用します。

1. 次のように Database Configuration Assistant を起動します。
   - Windows NT の場合は、**「スタート」→「プログラム」→「Oracle-<Oracle-HOME_NAME>」→「Database Administration」→「Database Configuration Assistant」**を選択します。
   - UNIX の場合は、**「$ORACLE_HOME/bin/dbca」**を選択します。
2. **「Configure database options in a database」**を選択し、**「Next」**を選択します。
3. データベースを選択し、**「Next」**を選択します。

   「Database Configuration Assistant」ウィンドウが表示されます。
4. **「Yes, Register the Database」**を選択し、Database Registration グループのユーザー用のディレクトリ資格証明を入力します。
5. データベースの登録を完了する場合は**「Finish」**、他のデータベース機能を追加選択する場合は**「Next」**を選択します。
6. **「Finish」**を選択すると、「File」ウィンドウが表示されます。
7. 適切な初期化ファイルを選択し、**「OK」**を選択します。

前述の手順を正しく実行すると、Database Configuration Assistant で次の操作が実行されます。

- ディレクトリ内で、選択した Oracle コンテキストの下に新規のデータベース・サービス・オブジェクトとサブツリーが作成されます。
- データベースをデフォルトのエンタープライズ・ドメインに追加します（エンタープライズ・ドメインの詳細は、第 4 章の「Oracle コンテキスト下の Oracle Advanced Security エントリ」を参照）。
- データベースの識別名を、データベース・サーバー・パラメータ・ファイル spfile.ora に `RDBMS_SERVER_DN` 初期化パラメータ値として追加します。
- 新規の初期化パラメータが有効になるようにデータベースを再起動します。

カスタム・データベースのインストール中のディレクトリ使用の構成

データベース・サーバー・ソフトウェアをインストールした後、Oracle Universal Installer は Oracle Net Configuration Assistant を起動します。Oracle Net Configuration Assistant ではディレクトリ使用構成の完了のオプションを選択できます。構成の完了は次の作業からなります。

- ディレクトリ・タイプの選択。
- ディレクトリのホスト名とポートの指定。デフォルト・ポート番号は、非 SSL 接続の場合は 389、SSL 接続の場合は 636 です。
- Oracle コンテキストのあるディレクトリ・エントリの選択。

必要な Oracle スキーマがすでにインストール済みであれば、Oracle Net Configuration Assistant はディレクトリ・エントリのドロップダウン・リストから Oracle コンテキストを選択するようプロンプトします。Oracle コンテキストをディレクトリのセットアップ中に作成している場合は、リスト内のエントリの 1 つがルートの Oracle コンテキストになっています。ルートの Oracle コンテキストは、ディレクトリのルート・エントリ（最上位エントリ）にあります。

ルート・コンテキストのみ存在する場合は、このコンテキストを使用するか、あるいは Oracle Net Configuration Assistant をスタンドアロン・モードで実行して新しい Oracle コンテキストを作成できます（「オプション 3:「Create additional or upgrade existing Oracle Context」」を参照）。

ルート Oracle コンテキストが存在しない場合は、ディレクトリ・エントリのドロップダウン・リストから「root entry」を選択して作成できます。一部の Oracle 機能では、ルート Oracle コンテキストが存在する必要があるため注意してください。

必要な Oracle スキーマがまだインストールされていなければ、Oracle Net Configuration Assistant は適切なスキーマをインストールするか、ディレクトリ構成を後回しにするかを選ぶオプションを提示します。

カスタム・データベースのインストールを実行すると、Oracle Net Configuration Assistant の後に Database Configuration Assistant が自動的に実行され、データベースの登録を確認するプロンプトが表示されます。**「Yes, Register the Database」**を選択し、「Database Configuration Assistant を使用したデータベースの登録」の手順 4 ～ 7 に従います。

管理グループ

ディレクトリ構成の完了作業中に Oracle コンテキストを正常に作成または更新した管理者は、次の 5 つの管理グループに自動的に追加されます。

- OracleContextAdmins (`cn=OracleContextAdmins,cn=Groups,cn=OracleContext`)

  このグループは、Oracle コンテキスト全体に対するすべての権限を持ちます。

- OracleDBCreators (`cn=OracleDBCreators,cn=OracleContext`)

  このグループでは、Database Configuration Assistant を使用してデータベース・サービス・エントリをその接続記述子といっしょにディレクトリに登録できます。

- OracleNetAdmins (`cn=OracleNetAdmins,cn=OracleContext`)

  このグループでは、Oracle Net Manager を使用して、ネット・サービス名の作成、変更および削除を実行できる他、データベース・サービスの Oracle Net 属性を変更できます。

- OracleDBSecurityAdmins (`cn=OracleDBSecurityAdmins,cn=OracleContext`)

  このグループは、コンテナ `OracleDBSecurity` 内のディレクトリ・オブジェクトに対するすべての権限を持ちます。これらのオブジェクトは、エンタープライズ・ドメイン、エンタープライズ・ロール、および、ユーザー・データベース・スキーマと共有データベース・スキーマとの間のマッピングで構成されます。

- OracleUserSecurityAdmins (`cn=OracleUserSecurityAdmins,cn=Groups,cn=OracleContext`)

  このグループは、Wallet のパスワード・ヒントおよびパスワードに対する読取りおよび書込みの権限を持っています。

クライアント・インストール中のディレクトリ使用の構成

クライアントのインストール中には、オプションを選択して、データベースへの接続にディレクトリに格納されているデータベース・サービス、ネット・サービス名またはネット・サービス別名を使用するように指定できます。この機能のことを、ディレクトリ・ネーミングと呼びます。データベースへの接続にディレクトリを使用するように選択すると、Oracle Net Configuration Assistant で次のプロンプトが表示されます。

- ディレクトリ・タイプの選択。
- ディレクトリのホスト名またはポートの指定。デフォルト・ポート番号は、非 SSL 接続の場合は 389、SSL 接続の場合は 636 です。

- Oracle コンテキストのあるディレクトリ・エントリの選択。

Oracle スキーマが不適切かまたはインストールされていない場合、あるいは Oracle コンテキストが存在しない場合は、クライアントでのディレクトリ使用構成を完了できません。構成を完了するためには、データベースのインストール後に Oracle Net Configuration Assistant をスタンドアロン・モードで実行してください。

データベース・サービス、ネット・サービス名およびネット・サービス別名の詳細は、第 4 章「Oracle 製品と Oracle Internet Directory の配置」の「Oracle コンテキスト下の Oracle Net Services エントリ」を参照してください。

製品固有の構成作業

Oracle Net Configuration Assistant は、大部分の Oracle 製品に必要な最小限のディレクトリ構成作業のみ実行します。そのため、多くのディレクトリ対応の Oracle 製品では追加の構成が必要になる場合があります。表 5-1 は、このマニュアルで説明している各製品と、それらの製品に固有の構成作業を説明しているマニュアルへの参照先を示したものです。

表 5-1 製品固有の構成に関する情報の参照先

製品	マニュアル
Oracle Net Services	『Oracle9*i* Net Services 管理者ガイド』の第 8 章「ディレクトリ・サーバー使用の設定」
Oracle Advanced Security	『Oracle Advanced Security 管理者ガイド』の第 15 章「エンタープライズ・ユーザー・セキュリティの管理」
アプリケーション・コンテキスト	『Oracle9*i* アプリケーション開発者ガイド - 基礎編』の第 12 章「アプリケーション・セキュリティ・ポリシーの実装」
Oracle Advanced Queuing	『Oracle9*i* アプリケーション開発者ガイド - アドバンスト・キューイング』の第 12 章「JMS を使用したアプリケーションの作成」
Oracle Dynamic Services	『Oracle Dynamic Services User's and Aministrator's Guide』の第 4 章「Advanced Installation Options」の「Using Lightweight Directory Access Protocol（LDAP）as a Central Master Registry」

A

Oracle 固有の LDAP スキーマ拡張機能

この付録では、LDAP 対応の Oracle 製品が Oracle Internet Directory のエントリを定義するために使用する、構造オブジェクト・クラスおよび属性の一覧を記載しています。補助オブジェクト・クラスを使用する Oracle9*i*AS Email の場合を除き、記載されている各属性はそれぞれのオブジェクト・クラスと相互参照になっており、複数のオブジェクト・クラスに属するものについてはそれぞれのオブジェクト・クラスと相互参照になっています。オブジェクト・クラスと属性は、製品別に分類されています。

この付録では、次の製品を対象としています。

- Oracle Net Services
- Oracle Advanced Security
- アプリケーション・コンテキスト
- Oracle Advanced Queuing
- Oracle Dynamic Services

Oracle Net Services

ここでは、Oracle Net Services 用の構造オブジェクト・クラスと属性を示し、それぞれについて説明します。

構造オブジェクト・クラス

- `orclDBServer`

  データベース・サービス・エントリの属性を定義します。

- `orclNetService`

  ネット・サービス名エントリの属性を定義します。

- `orclNetServiceAlias`

  ネット・サービス別名エントリの属性を定義します。

- `orclNetDescription`

  接続記述子を指定します。接続記述子には、リスナー・プロトコル・アドレスとサービスへの接続情報があります。

- `orclNetDescriptionList`

  接続記述子のリストを指定します。

- `orclNetAddress`

  リスナー・プロトコル・アドレスを指定します。

- `orclNetAddressList`

  アドレスのリストを指定します。

属性

- `orclNetAddrList` (`orclNetAddressList`, `orclNetDescription`)

  1 つ以上のリスナー・プロトコル・アドレスを識別します。

- `orclNetAddressString` (`orclNetAddress`)

  リスナー・プロトコル・アドレスを定義します。

- `orclNetConnParamList` (`orclNetDescription`)

  将来の接続データ・パラメータ用のプレースホルダです。

- `orclNetDescList` (`orclNetDescriptionList`)

  1 つ以上の接続記述子を識別します。

- orclNetDescName (orclDBServer, orclNetService)

  接続記述子または接続記述子のリストを識別します。

- orclNetFailover (orclNetDescription, orclNetAddressList)

  アドレス・リストに対して接続時フェイルオーバーをオンにします。

- orclNetInstanceName (orclNetDescription)

  アクセスするインスタンス名を指定します。

- orclNetLoadBalance (orclNetDescription, orclNetAddressList)

  アドレス・リストに対してクライアント・ロード・バランシングをオンにします。

- orclNetProtocol (orclNetAddress)

  orclAddressString 属性で使用するプロトコルを識別します。

- orclNetSdu (orclNetDescription)

  セッション・データ・ユニット（SDU）のサイズを指定します。

- orclNetServiceName (orclNetDescription)

  CONNECT_DATA 部分の Oracle9*i* または Oracle8*i* データベース・サービス名を指定します。

- orclNetSourceRoute (orclNetDescription, orclNetAddressList)

  接続先に達するまで各アドレスを順番に使用するよう Oracle Net に指示します。

- orclSid (orclNetDescription)

  接続記述子の CONNECT_DATA 部分の Oracle システム識別子（Oracle System Identifier: SID）を指定します。

- orclVersion （すべてのオブジェクト・クラス）

  エントリの作成に使用するソフトウェアのバージョンを指定します。

Oracle Advanced Security

ここでは、Oracle Advanced Security 用の構造オブジェクト・クラスと属性を示し、それぞれについて説明します。

構造オブジェクト・クラス

- `orclDBEnterpriseDomain`

  ドメインのデータベース・メンバーを識別するグループ・オブジェクト・クラス。ドメインの構成データが含まれています。たとえば、許可可能な認証タイプを指定し、カレントのユーザー・データベース・リンクが有効にされているかどうかを示します。

- `orclDBEnterpriseRole`

  ドメイン内のエンタープライズ・ロールに加えて、このエンタープライズ・ロールに割り当てられるユーザーおよびデータベースのグローバル・ロールを定義する、グループ・オブジェクト・クラス。

- `orclDBEntryLevelMapping`

  ユーザーとデータベース・スキーマとの間の単一のマッピングを定義します。

- `orclDBSubtreeLevelMapping`

  ユーザー・サブツリーとデータベース・スキーマとの間のマッピングを定義します。

属性

- `uniquemember`[1] (`orclDBEnterpriseDomain`, `orclDBEnterpriseRole`)

  ドメインのメンバーであるデータベースのリストを格納します。エンタープライズ・ロールに割り当てられるユーザーのリストを格納します。

- `orclDBAuthTypes` (`orclDBEnterpriseDomain`)

  データベースが承認する必要のあるユーザー認証のタイプを示します。

- `orclDBTrustedDomain` (`orclDBEnterpriseDomain`)

  カレントのユーザー・データベース・リンクがドメイン内のデータベース間で機能するかどうかを示します。

- `orclDBServerRole` (`orclDBEnterpriseRole`)

  ドメイン内のデータベースのグローバル・ロールのリストを定義します。

[1] Oracle9*i* データベースのみ。Oracle8*i* データベースは `OracleDBServerMember` および `orclDBRoleOccupant` を使用します。

- orclDBDistinguishedName (orclDBEntryLevelMapping, orclDBSubtreeLevelMapping)

  エンタープライズ・ユーザーの完全な識別名を指定します。

- orclDBNativeUser (orclDBEntryLevelMapping, orclDBSubtreeLevelMapping)

  データベース共有スキーマ名を指定します。

アプリケーション・コンテキスト

アプリケーション・コンテキストは orclDBApplicationContext という 1 個の構造オブジェクト・クラスを使用してコンテキスト値を定義します。このオブジェクト・クラスは uniquemember という 1 個の属性を使用してコンテキスト・ユーザーを定義します。orclDBApplicationContext は GroupOfUniqueNames のサブクラスです。

Oracle Advanced Queuing

ここでは、Oracle Advanced Queuing 用の構造オブジェクト・クラスと属性を示し、それぞれについて説明します。

構造オブジェクト・クラス

- orclDBAQConnection

  アドバンスト・キューイングの JMS コネクション・ファクトリ・オブジェクトを格納します。

- orclDBAQObject

  キュー、キュー表、別名、サブスクライバ、JMS サブスクライバおよびエージェントを格納します。

- orclDBAQRegistration

  エンタープライズ・ユーザーからの登録要求を格納します。

属性

- orclDBAQGeneric (OrclDBAQConnection)

  その他の名前と値のペアを格納します。

- orclDBAQObjName (orclDBAQObject)

  アドバンスト・キューイング・オブジェクトの名前を格納します。

- orclDBAQObjOwner (orclDBAQObject)

  アドバンスト・キューイング・オブジェクトを所有しているデータベース・ユーザーの名前を格納します。

- orclDBAQObjType (orclDBAQObject)

  アドバンスト・キューイング・オブジェクトのタイプを格納します。

- orclDBAQPointerAttr (orclDBAQObject)

  ― キュー・オブジェクトの基になるキュー表の識別名

  ― エージェントのデジタル証明を収めた LDAP エントリ

  ― 対応するキュー・サブスクライバに対するエージェントの識別名

  ― 対応する JMS サブスクライバに対するキュー・サブスクライバの識別名

  ― 別名化されたオブジェクトの識別名

- orclDBAQRegNamespace (orclDBAQRegistration)

  AQ や anonymous などの登録名前空間を格納します。

- orclDBAQRegSubscription (orclDBAQRegistration)

  登録のサブスクリプション名を格納します。

- orclDBAQRegLocation (orclDBAQRegistration)

  サーバーが通知を送信する場所を格納します。

- orclDBAQRegUser (orclDBAQRegistration)

  登録中のエンタープライズ・ユーザーの名前を格納します。

- orclDBAQRegUserContext (orclDBAQRegistration)

  通知発生時にユーザーに返されるユーザー・コンテキストを指定します。

- orclDBAQRegServers (orclDBAQRegistration)

  エンタープライズ・ユーザーが登録しているデータベース・サーバーの識別名を指定します。

- orclDBAQRegUnreachable (orclDBAQRegistration)

  クライアントに到達できなかったデータベース・サーバーの識別名を指定します。この値は Oracle データベース・サーバーにより与えられます。

- orclDBAQRegRejected (orclDBAQRegistration)

  この登録要求を拒否したデータベース・サーバーの識別名を指定します。この値は Oracle データベース・サーバーにより与えられます。

Oracle Dynamic Services

ここでは、Oracle Dynamic Services 用の構造オブジェクト・クラスと属性を示し、それぞれについて説明します。

構造オブジェクト・クラス

- orclDynsAccessibleService

  アプリケーションで使用可能なサービスを指定します。サブツリー OracleDynamicServicesUPR 内で使用されます。

- orclDynsServiceModProperty

  アプリケーションのプロパティを指定します。サブツリー OracleDynamicServicesUPR 内で使用されます。

- orclDynsTxtObject

  OracleDynsDocument サブツリーの下のテキスト文書のプレースホルダを指定します。

- orclDynsBinObject

  サービスのバイナリ・ファイルのプレースホルダを指定します。DSBBinObject サブツリーの下で使用されます。

- orclDynsServiceCat

  「Business」や「Finance」などの特定のサービス・カテゴリを指定します。サブツリー OracleDynamicServicesSR 内で使用されます。

- orclDynsServiceRegistryEntry

  実際のサービス・エンティティを指定します。OracleDynamicServicesSR サブツリー内で使用されます。サービス検索をサポートするために、サービス ID、キーワードおよびインタフェースが抽出されます。

- orclDynsEnterpriseDomain

  ドメイン内のすべての DSE インスタンスを管理する DSE ドメイン管理者を指定します。このオブジェクト・クラスは将来の実装のために拡張が可能です。

- orclDynsEnterpriseInstance

  DSE インスタンスを指定します。DSE インスタンスへの接続がどのようになされるのかを指定します。

- orclDynsPerson

  サービスの連絡先である人物を指定します。

- orclDynsSPOrganization

  サービス・プロバイダである組織を指定します。登録商標を持つ組織名がそれぞれ一意な ID です。

属性

- orclDynsBinaryHolder (orclDynsBinObject)

  バイナリ・オブジェクトを格納します。

- orclDynsTextHolder (orclDynsTxtObject, orclDynsServiceRegistryEntry)

  テキスト文書を格納します。

- orclDynsObjRefCnt (orclDynsTxtObject, orclDynsBinObject, orclDynsSPOrganization)

  オブジェクト参照の追跡に使用するカウンタ。

- orclDynsPropertyName (orclDynsServiceModProperty)

  アプリケーションがサービスに対して使用するプロパティ名を指定します。

- orclDynsPropertyValue (orclDynsPropertyValue)

  プロパティ値を識別します。

- orclDynsInternalObjectID (orclDynsTxtObject, orclDynsBinObject)

  バイナリ・オブジェクトなどの内部オブジェクトへの参照に対する一意な ID を指定します。

- orclDynsInternalObjectType (orclDynsTxtObject, orclDynsBinObject)

  拡張性の目的に使用されます。

- orclDynsKeywords (orclDynsServiceRegistryEntry)

  サービスのキーワードを指定します。

- orclDynsServiceID (orclDynsAccessibleService, orclDynsServiceRegistryEntry)

  サービス ID を指定します。

- orclDynsServiceName (orclDynsServiceRegistryEntry)

  サービス名を指定します。

- orclDynsModifier (orclDynsServiceModProperty)

  OracleDynamicServicesUPR サブツリー内で <mod, pn, pv> として使用されます。

- orclDynsURL (orclDynssPOrganization)
  企業の URL を指定します。サービス・プロバイダのプロパティの 1 つです。
- orclDynsLogoURL (orclDynssPOrganization)
  サービス・プロバイダである企業のロゴを指定します。
- orclDynsCopyright (orclDynssPOrganization)
  サービスの著作権を指定します。サービス・プロバイダのプロパティの 1 つです。
- orclDynsDomainAdminPassword (orclDynsEnterpriseDomain)
  ドメイン管理者のパスワードを指定します。
- orclDynsConnection (orclDynsEnterpriseInstance)
  DSE の接続文字列。
- orclDynsInterface (orclDynsServiceRegistryEntry)
  特定のサービスのインタフェースを指定します。

B

LDAP コマンドライン・ツール

LDAP プロトコル操作は、認証、問合せ、および更新と制御の、3 つのカテゴリに分けられます。LDAP C-API には、これら 3 つのカテゴリに対応する簡単なコマンドライン・ツールがいくつか付属しています。

この付録の内容は次のとおりです。

LDAP コマンドライン・ツール

ここでは、頻繁に使用する 6 つのコマンドライン・ツールを紹介します。この後の「コマンドライン・ツールのオプションの引数」では、コマンドの説明と例で使用されているオプションの引数について説明します。

次の 6 つのコマンドについて説明します。

- ldapbind
- ldapsearch
- ldapadd
- ldapdelete
- ldapmodify
- ldapmoddn

ldapbind

コマンドライン・ツール ldapbind は、ディレクトリ・サーバーへの認証に使用します。ldapbind はサーバーが実行中かどうかを調べるために使用することもできます。

構文

```
ldapbind [options]
```

例

```
ldapbind -h myhost -p 389 -D "cn=orcladmin" -w welcome
```

このコマンドは、ポート 389 にあるディレクトリ・サーバー myhost に対して、パスワード welcome を使用してユーザー orcladmin を認証します。

ldapsearch

コマンドライン・ツール ldapsearch は、ディレクトリ内の特定のエントリを検索するために使用します。ldapsearch は、ディレクトリへの接続をオープンし、操作を実行するユーザーを認証して、指定されたエントリを検索し、その結果をユーザーが指定した書式で出力します。

構文

```
ldapsearch [options] filter [attributes]
```

例

```
ldapsearch -h myhost -p 389 -s base -b "ou=people,dc=acme,dc=com" \ "objectclass=*"
```

このコマンドは、ポート 389 にあるディレクトリ・サーバー myhost を検索します。検索の有効範囲（-s）はベースであり、検索対象のディレクトリの部分は指定されたベース DN（-b）です。検索フィルタ "objectclass=*" は、エントリのすべてのオブジェクト・クラスの値が戻されることを意味します。属性は指定していないため戻されません。この例では認証オプションを指定していないため、匿名認証を想定しています。

ldapadd

コマンドライン・ツール ldapadd は、ディレクトリにエントリを追加するために使用します。ldapadd は、ディレクトリへの接続をオープンしてユーザーを認証します。そして、引数に指定された LDIF ファイルをオープンし、ファイル内の各エントリを連続して追加します。

構文

```
ldapadd [options] [-f LDIF-filename]
```

例

```
ldapadd -h myhost -p 389 -D "cn=orcladmin" -w welcome -f jhay.ldif
```

このコマンドを使用し、ポート 389 にあるディレクトリ myhost に対してユーザー orcladmin を認証します。次に、コマンドはファイル jhay.ldif をオープンし、その内容をディレクトリに追加します。このファイルは、たとえば uid=jhay,cn=Human Resources,cn=acme,dc=com などのエントリと、そのオブジェクト・クラスおよび属性を追加します。

> **関連項目：** LDIF ファイルの構文の詳細は、2-7 ページの「LDIF」を参照してください。

ldapdelete

コマンドライン・ツール ldapdelete は、ディレクトリからリーフ・エントリを削除するために使用します。ldapdelete は、ディレクトリ・サーバーへの接続をオープンしてユーザーを認証します。そして、指定されたエントリを削除します。

構文

```
ldapdelete [options] "entry DN"
```

例

```
ldapdelete -h myhost -p 389 -D "cn=orcladmin" -w welcome \
"uid=hricard,ou=sales,ou=people,dc=acme,dc=com"
```

このコマンドは、ディレクトリ myhost に対して、パスワード welcome を使用してユーザー orcladmin を認証します。そして、エントリ uid=hricard,ou=sales,ou=people,dc=acme,dc=com を削除します。

ldapmodify

コマンドライン・ツール ldapmodify は、既存のエントリを変更するために使用します。ldapmodify は、ディレクトリへの接続をオープンしてユーザーを認証します。そして、引数に指定された LDIF ファイルをオープンし、ファイルで指定された LDAP エントリを変更します。

ldapmodify は、LDIF ファイルの変更された形式を使用します。ファイルそれ自体の中で、属性 changetype を使用して変更のタイプを指定します。たとえば、changetype: add などとします。

4 種類の変更を指定できます。

- add ー 新しいエントリを追加します。
- modify ー 既存のエントリを変更します。つまり、エントリの属性を追加、削除または置換します。
- delete ー 既存のエントリを削除します。
- modrdn ー 既存のエントリの RDN を変更します。

構文

```
ldapmodify [options] [-f LDIF-filename]
```

例

```
ldapmodify -h myhost -p 389 -D "cn=orcladmin" -w welcome -f hricard.ldif
```

このコマンドを使用し、ポート 389 にあるディレクトリ myhost に対してユーザー orcladmin を認証します。次に、コマンドはファイル hricard.ldif をオープンし、ファイルで指定されたディレクトリ・エントリを変更します。このファイルは、たとえばエントリ uid=hricard,cn=sales,cn=acme,dc=com の電話番号属性を変更します。

注意： ldapadd および ldapdelete を使用してエントリを追加または削除するかわりに、ldapmodify を使用できます。

---

ldapmoddn

コマンドライン・ツール ldapmoddn は次の用途に使用します。

- エントリの RDN を変更します。
- エントリまたはサブツリーをディレクトリ内の他の位置に移動します。

構文

```
ldapmoddn [options] -b "current DN" -R "new RDN" -N "new Parent"
```

例

```
ldapmoddn -h myhost -p 389 -D "cn=orcladmin" -w welcome \
-b "uid=oball,ou=sales,ou=people,dc=acme,dc=com" \
-N "ou=marketing,ou=people,dc=acme,dc=com"
```

このコマンドは、ディレクトリ myhost に対して、パスワード welcome を使用してユーザー orcladmin を認証します。そして、エントリ uid=oball,ou=sales,ou=people,dc=acme,dc=com に新しい親エントリ ou=marketing,ou=people,dc=acme,dc=com を割り当てます。

コマンドライン・ツールのオプションの引数

表 B-1 は、コマンドの説明と例で使用されているオプションの引数の定義です。

表 B-1 一般に使用されるコマンドライン・オプション

オプション	説明
-h	ディレクトリ・サーバーのホスト名
-p	ディレクトリ・サーバーのポート番号
-D	バインド DN ーディレクトリへの認証を行っているユーザー
-w	簡易認証におけるバインド・パスワード
-W	一方向または双方向の SSL 認証における Wallet の位置
-P	Wallet パスワード
-U	SSL 認証モード ■ 1 は認証なし ■ 2 は一方向認証 ■ 3 は双方向認証
-b[1]	検索のベース DN
-s[2]	検索有効範囲 ■ base ー 要求されたエントリ ■ one ー 要求されたエントリのすぐ下にあるエントリ ■ sub ー サブツリー全体
-f	追加、削除または変更のある LDIF ファイル
-R	新しい RDN
-N	移動されるエントリまたはサブツリーの新しい親

[1] ldapsearch で必須。
[2] ldapsearch で必須。

関連項目：『Oracle Internet Directory アプリケーション開発者ガイド』の付録 A「コマンドライン・ツールの構文」

索引

A

C

D

I

J

L

O

R

S

な

に

ね

は

ふ

ほ

ま

め

る

れ