

# Oracle Internet Directory

管理者ガイド

リリース 2.1.1

2000 年 11 月

部品番号 : J02325-01

ORACLE®

---

Oracle Internet Directory 管理者ガイド, リリース 2.1.1

部品番号 : J02325-01

原本名 : Oracle Internet Directory Administrator's Guide, Release 2.1.1

原本部品番号 : A86101-01

原本著者 : Richard Smith

原本協力者 : Deborah Steiner, Sandy Venning, Tridip Bhattacharya, Margaret Chou, Raj Gupta, Ashish Kolli, Stephen Lee, Michael Mesaros, Radikah Moolky, Olaf Stullich, David Saslav, Hari Sastry, Gurudat Shakshikumar, Amit Sharma, Daniel Shih, Saurabh Shrivastava, Uppili Srinivasan

Copyright © 1996, 2000, 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います。

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

はじめに .....	xix
Oracle Internet Directory の新機能 .....	xxv
<b>第 I 部 スタート・ガイド</b>	
<b>1 概要</b>	
ディレクトリとは .....	1-2
オンライン・ディレクトリ .....	1-2
オンライン・ディレクトリとリレーショナル・データベースの違い .....	1-2
問題：複数の特別な用途のディレクトリ .....	1-3
解決策：LDAP 準拠の一般的な用途のディレクトリ .....	1-4
LDAP とは .....	1-4
LDAP と単純化されたディレクトリ管理 .....	1-4
LDAP バージョン 3 .....	1-5
Oracle Internet Directory とは .....	1-6
Oracle Internet Directory と Oracle8i .....	1-6
Oracle Internet Directory のコンポーネント .....	1-7
Oracle Internet Directory の利点 .....	1-8
拡張性 .....	1-8
高い可用性 .....	1-8
セキュリティ .....	1-8

## 2 概念とアーキテクチャ

エントリ .....	2-2
属性 .....	2-3
属性情報の種類 .....	2-4
単一値と複数値の属性 .....	2-5
一般的な LDAP 属性 .....	2-5
属性の構文 .....	2-6
属性の一致規則 .....	2-6
属性オプション .....	2-7
オブジェクト・クラス .....	2-7
サブクラス、スーパー・クラスおよび継承 .....	2-8
オブジェクト・クラスの型 .....	2-8
抽象型オブジェクト・クラス .....	2-8
構造型オブジェクト・クラス .....	2-9
補助型オブジェクト・クラス .....	2-9
ネーミング・コンテキスト .....	2-10
ディレクトリ・スキーマ .....	2-10
セキュリティ .....	2-11
認証 .....	2-12
匿名認証 .....	2-12
簡易認証 .....	2-12
Secure Sockets Layer (SSL) を使用した認証 .....	2-12
アクセス制御と認可 .....	2-15
データ整合性 .....	2-16
データ・プライバシー .....	2-16
パスワード暗号化 .....	2-16
各国語サポート .....	2-17
Oracle Internet Directory のアーキテクチャ .....	2-18
Oracle Internet Directory のノード .....	2-18
Oracle Directory (LDAP) Server インスタンス .....	2-21
構成設定エントリ .....	2-21
例：Oracle Internet Directory の動作 .....	2-22
分散ディレクトリ：概要 .....	2-23
分散ディレクトリ：レプリケーション .....	2-23
ディレクトリ・レプリケーション・グループとレプリケーション承諾 .....	2-25
アドバンスト・レプリケーション .....	2-26

レプリケーション・アーキテクチャ .....	2-27
変更ログの削除 .....	2-27
レプリケーションにおける競合の解消 .....	2-28
レプリケーション競合が発生するレベル .....	2-28
競合の一般的な原因 .....	2-29
競合の自動解消 .....	2-29
レプリケーションの動作：概要 .....	2-29
レプリケーションの動作：詳細説明 .....	2-32
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 .....	2-32
レプリケーション・プロセスがエントリを削除する動作 .....	2-33
レプリケーション・プロセスがエントリを変更する動作 .....	2-34
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 .....	2-35
レプリケーション・プロセスが識別名を変更する動作 .....	2-36
分散ディレクトリ：パーティション化 .....	2-38
ナレッジ参照（参照） .....	2-39
ナレッジ参照の種類 .....	2-41
メタディレクトリ環境での他のディレクトリとの同期 .....	2-42
メタディレクトリ .....	2-42
メタディレクトリ・ソリューションでの Oracle Internet Directory の動作 .....	2-42

### 3 事前に実行する作業

タスク 1: OID モニター・デーモンの開始 .....	3-2
OID モニターの開始 .....	3-2
OID モニターの停止 .....	3-3
タスク 2: サーバー・インスタンスの起動 .....	3-3
Oracle Directory Server インスタンスの起動 .....	3-4
Oracle Directory Server インスタンスの停止 .....	3-5
Oracle Directory Replication Server インスタンスの起動 .....	3-5
Oracle Directory Replication Server インスタンスの停止 .....	3-7
Directory Server インスタンスの再起動 .....	3-7
Directory Server インスタンスの起動に関するトラブルシューティング .....	3-8
タスク 3: デフォルト・セキュリティ構成の再設定 .....	3-8
Oracle Internet Directory の以前のリリースからのアップグレード .....	3-9
単一ノード環境でのアップグレード .....	3-9
マルチノード環境でのアップグレード .....	3-9
1 ノードずつアップグレード .....	3-10

すべてのノードを同時にアップグレード .....	3-13
LDIF ベースのアップグレード .....	3-15
パスワード暗号化のためのアップグレード後の手順 .....	3-16

## 4 管理ツールの使用方法

Oracle Directory Manager の使用方法 .....	4-2
Oracle Directory Manager の起動 .....	4-2
Directory Server への接続 .....	4-3
Oracle Directory Manager のナビゲート .....	4-6
Oracle Directory Manager の概要 .....	4-6
Oracle Directory Manager のメニュー・バー .....	4-7
Oracle Directory Manager のツールバー .....	4-9
追加の Directory Server への接続 .....	4-10
Directory Server からの切断 .....	4-10
Oracle Directory Manager を使用した管理タスクの実行 .....	4-10
コマンドライン・ツールの使用方法 .....	4-11
バルク・ツールの使用方法 .....	4-12
OID 制御ユーティリティの使用方法 .....	4-13
カタログ管理ツールの使用方法 .....	4-13
OID データベース・パスワード・ユーティリティの使用方法 .....	4-13
レプリケーション・ツールの使用方法 .....	4-14
OID データベース統計収集ツールの使用方法 .....	4-14
管理タスクの一覧 .....	4-15

## 第 II 部 Oracle Internet Directory の管理

### 5 Oracle Directory Server の管理

サーバーの構成設定エントリの管理 .....	5-2
事前の考慮事項 .....	5-2
Oracle Directory Manager を使用したサーバーの構成設定エントリの管理 .....	5-4
Oracle Directory Manager を使用した構成設定エントリの表示 .....	5-4
Oracle Directory Manager を使用した構成設定エントリの追加 .....	5-4
Oracle Directory Manager を使用した構成設定エントリの変更 .....	5-8
Oracle Directory Manager を使用した構成設定エントリの削除 .....	5-10
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 .....	5-10
ldapadd を使用した構成設定エントリの追加 .....	5-10

ldapmodify を使用した構成設定エントリの変更と削除 .....	5-11
<b>システム操作属性の設定</b> .....	5-12
Oracle Directory Manager を使用したシステム操作属性の設定 .....	5-13
ldapmodify を使用したシステム操作属性の設定 .....	5-14
<b>ネーミング・コンテキストの管理</b> .....	5-15
Oracle Directory Manager を使用したネーミング・コンテキストの公開 .....	5-15
ldapmodify を使用したネーミング・コンテキストの公開 .....	5-16
<b>パスワード暗号化の管理</b> .....	5-16
Oracle Directory Manager を使用したパスワード暗号化の管理 .....	5-16
ldapmodify を使用したパスワード暗号化の管理 .....	5-17
<b>検索の構成</b> .....	5-17
Oracle Directory Manager を使用した検索の構成 .....	5-17
Oracle Directory Manager を使用した、検索で戻されるエントリの最大数の設定 .....	5-17
Oracle Directory Manager を使用した、検索の最大時間の設定 .....	5-18
ldapmodify を使用した検索の構成 .....	5-18
ldapmodify を使用した、検索で戻されるエントリの最大数の設定 .....	5-18
ldapmodify を使用した、検索の最大時間の設定 .....	5-18
<b>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</b> .....	5-19
Oracle Directory Manager を使用したユーザー名とパスワードの管理 .....	5-20
ldapmodify を使用したユーザー名とパスワードの管理 .....	5-21
<b>デバッグ・ロギング・レベルの設定</b> .....	5-22
Oracle Directory Manager を使用したデバッグ・ロギング・レベルの設定 .....	5-22
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 .....	5-22
<b>監査ログの使用方法</b> .....	5-24
監査ログ・エントリの構造 .....	5-25
DIT における監査ログ・エントリの位置 .....	5-26
監査可能なイベント .....	5-26
監査レベルの設定 .....	5-27
Oracle Directory Manager を使用した監査レベルの設定 .....	5-27
ldapmodify を使用した監査レベルの設定 .....	5-28
監査ログ・エントリの検索 .....	5-29
Oracle Directory Manager を使用した監査ログ・エントリの検索 .....	5-29
ldapssearch を使用した監査ログ・エントリの検索 .....	5-29
監査ログの削除 .....	5-29
<b>アクティブ・サーバー・インスタンスの情報の表示</b> .....	5-29
<b>Oracle データ・サーバー接続時のパスワードの変更</b> .....	5-30

## 6 ディレクトリ・スキーマの管理

ディレクトリ・スキーマの概要 .....	6-2
オブジェクト・クラス管理 .....	6-2
オブジェクト・クラスの追加のガイドライン .....	6-3
オブジェクト・クラスの変更のガイドライン .....	6-4
オブジェクト・クラスの削除のガイドライン .....	6-5
Oracle Directory Manager を使用したオブジェクト・クラスの管理 .....	6-6
Oracle Directory Manager を使用したオブジェクト・クラスの検索 .....	6-6
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 .....	6-9
Oracle Directory Manager を使用したオブジェクト・クラスの追加 .....	6-9
Oracle Directory Manager を使用したオブジェクト・クラスの変更 .....	6-11
Oracle Directory Manager を使用したオブジェクト・クラスの削除 .....	6-12
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 .....	6-12
例：新規オブジェクト・クラスの追加 .....	6-13
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 .....	6-13
属性管理の概要 .....	6-14
属性の追加に関する規則 .....	6-14
属性の変更に関する規則 .....	6-15
属性の削除に関する規則 .....	6-15
Oracle Directory Manager を使用した属性の管理 .....	6-15
Oracle Directory Manager を使用した属性の検索 .....	6-15
Oracle Directory Manager を使用した属性の追加 .....	6-18
Oracle Directory Manager を使用した新規属性の追加 .....	6-18
Oracle Directory Manager を使用した既存の属性からの新規属性の作成 .....	6-20
Oracle Directory Manager を使用した属性の変更 .....	6-21
作成時の属性の索引付け .....	6-23
Oracle Directory Manager を使用した索引付き属性の表示 .....	6-24
Oracle Directory Manager を使用した作成時の属性の索引付け .....	6-24
Oracle Directory Manager を使用した属性からの索引の削除 .....	6-24
コマンドライン・ツールを使用した属性の管理 .....	6-24
ldapmodify を使用した属性の追加と変更 .....	6-24
コマンドライン・ツールを使用した属性の索引付け .....	6-25
索引付けの概要 .....	6-25
ldapmodify を使用したディレクトリ・データが存在していない属性の索引付け .....	6-26
カタログ管理ツールを使用したディレクトリ・データが存在している属性の索引付け .....	6-26



## 7 ディレクトリ・エントリの管理

Oracle Directory Manager を使用したエントリの管理 .....	7-2
Oracle Directory Manager を使用したエントリの検索 .....	7-2
Oracle Directory Manager を使用した監査ログ・エントリの検索 .....	7-5
Oracle Directory Manager を使用した属性の表示 .....	7-5
Oracle Directory Manager を使用したエントリの追加 .....	7-6
Oracle Directory Manager を使用した新規エントリの追加 .....	7-6
Oracle Directory Manager の既存エントリを利用したエントリの追加 .....	7-7
例：Oracle Directory Manager を使用したユーザー・エントリの追加 .....	7-7
Oracle Directory Manager を使用したグループ・エントリの追加 .....	7-8
Oracle Directory Manager を使用したエントリの変更 .....	7-9
例：Oracle Directory Manager を使用したユーザー・エントリの変更 .....	7-10
コマンドライン・ツールを使用したエントリの管理 .....	7-10
エントリ管理のためのコマンドライン・ツール .....	7-11
例：ldapadd を使用したユーザー・エントリの追加 .....	7-12
例：ldapmodify を使用したユーザー・エントリの変更 .....	7-12
バルク・ツールを使用したエントリの管理 .....	7-13
bulkload を使用した LDIF ファイルのインポート .....	7-13
タスク 1: Oracle Server のバックアップ .....	7-14
タスク 2: Oracle Internet Directory のパスワードの準備 .....	7-14
タスク 3: スキーマ違反とデータ整合性違反に関する入力のチェック .....	7-14
タスク 4: SQL*Loader 用の入力ファイルの生成 .....	7-14
タスク 5: 入力ファイルのロード .....	7-15
バルク・ロードに失敗した場合 .....	7-15
ディレクトリ・データの LDIF への変換 .....	7-15
多数のエントリの変更 .....	7-15
多数のエントリの削除 .....	7-15
属性オプションのあるエントリの管理 .....	7-16
例：属性オプションの追加 .....	7-16
例：属性オプションの削除 .....	7-16
例：属性オプションのあるエントリの検索 .....	7-17
ナレッジ参照（参照）の管理 .....	7-17
スマート・ナレッジ参照の構成 .....	7-18
デフォルト・ナレッジ参照の構成 .....	7-19

## 8 Secure Sockets Layer (SSL) の管理

サポートされている Cipher Suite .....	8-2
SSL クライアントの使用例 .....	8-2
SSL パラメータの構成 .....	8-2
Oracle Directory Manager を使用した SSL パラメータの構成 .....	8-3
コマンドライン・ツールを使用した SSL パラメータの構成 .....	8-5
このリリースの Oracle Internet Directory 固有の問題 .....	8-5

## 9 ディレクトリのアクセス制御の管理

アクセス制御ポリシーの管理の概要 .....	9-2
アクセス制御管理の構造体 .....	9-2
orclACI .....	9-2
Access Control Policy Points (ACP) .....	9-3
orclEntryLevelACI .....	9-3
権限グループ .....	9-4
アクセス制御情報のコンポーネント .....	9-5
オブジェクト: アクセス権限を付与するオブジェクト .....	9-6
対象: アクセス権限を付与する対象 .....	9-7
操作: 付与するアクセス権限の種類 .....	9-8
アクセス制御リスト (ACL) の評価の動作 .....	9-10
アクセス制御リスト (ACL) の評価の概要 .....	9-10
アクセス制御リスト (ACL) の評価の優先順位規則 .....	9-11
同一オブジェクトに対する複数アクセス制御項目 (ACI) の割当て .....	9-12
オブジェクトに対する排他的アクセス権限の付与 .....	9-13
グループの場合のアクセス制御リスト (ACL) 評価 .....	9-14
LDAP 操作のアクセス・レベル要件 .....	9-14
Oracle Directory Manager を使用したアクセス制御の管理 .....	9-15
Oracle Directory Manager の Access Control Policy Points (ACP) の表示の構成 .....	9-16
Oracle Directory Manager を使用する場合の Access Control Policy Points (ACP) の 検索の構成 .....	9-16
Oracle Directory Manager を使用した Access Control Policy Points (ACP) の表示 .....	9-17
Oracle Directory Manager を使用した既存 Access Control Policy Points (ACP) と そのアクセス制御項目 (ACI) ディレクティブの変更 .....	9-19
Oracle Directory Manager を使用した既存 Access Control Policy Points (ACP) への 構造型アクセス項目の追加 .....	9-19
Oracle Directory Manager を使用した既存 Access Control Policy Points (ACP) への コンテンツ・アクセス項目の追加 .....	9-22

Oracle Directory Manager を使用した既存 Access Control Policy Points (ACP) の 構造型アクセス項目の変更 .....	9-23
Oracle Directory Manager を使用した既存 Access Control Policy Points (ACP) の コンテンツ・アクセス項目の変更 .....	9-25
Oracle Directory Manager を使用した Access Control Policy Points (ACP) の追加と アクセス項目の作成 .....	9-26
例: Oracle Directory Manager を使用した Access Control Policy Points (ACP) の管理 .....	9-27
新規 Access Control Policy Points (ACP) の作成 .....	9-27
2 番目のアクセス制御項目 (ACI) の作成 .....	9-28
3 番目のアクセス制御項目 (ACI) の作成 .....	9-29
4 番目のアクセス制御項目 (ACI) の作成 .....	9-29
Oracle Directory Manager を使用したエントリ・レベルのアクセス権限の付与 .....	9-30
コマンドライン・ツールを使用したアクセス制御の管理 .....	9-31
例: アクセス制御の管理 .....	9-31
例: ldapmodify を使用した継承可能な Access Control Policy Points (ACP) の設定 .....	9-31
例: ldapmodify を使用したエントリ・レベルのアクセス制御項目 (ACI) の設定 .....	9-32
一般的なアクセス制御ポリシー .....	9-32

## 10 ディレクトリ・レプリケーションの管理

レプリケーションのインストールと構成 .....	10-2
タスク 1: DRG の全ノードへの Oracle Internet Directory のインストール .....	10-3
タスク 2: アドバンスト・レプリケーションのマスタ定義サイト (MDS) として機能する ノードの決定 .....	10-3
タスク 3: MDS における、ディレクトリ・レプリケーション・グループ用の アドバンスト・レプリケーションの設定 .....	10-3
レプリケーション用の Net8 環境の準備 .....	10-4
ディレクトリ・レプリケーション用の Oracle アドバンスト・レプリケーションの構成 .....	10-7
タスク 4: 全ノードでの Oracle Directory Server インスタンスの起動 .....	10-10
タスク 5: レプリケーションの構成 .....	10-10
Oracle Directory Replication Server の構成パラメータの位置 .....	10-11
Oracle Directory Replication Server のパラメータ .....	10-11
Oracle Directory Manager を使用したレプリケーションの構成パラメータの表示と変更 ...	10-12
コマンドライン・ツールを使用したレプリケーションの構成パラメータの変更 .....	10-13
レプリケーション承諾のパラメータ .....	10-14
レプリケーション承諾のパラメータの位置 .....	10-15
Oracle Directory Manager を使用したレプリケーション承諾のパラメータの表示と変更 ...	10-15
ldapmodify を使用したレプリケーション承諾のパラメータの変更 .....	10-16

タスク 6: 全ノードでの Replication Server の起動 .....	10-18
変更ログ・フラグの使用 .....	10-18
マルチマスター・フラグの使用 .....	10-18
<b>レプリケーション・ノードの追加 .....</b>	<b>10-19</b>
タスク 1: すべてのノードで Oracle Directory Replication Server を停止 .....	10-20
タスク 2: 既存の全ノードで LDAP レプリケーション・グループに新規ノードを構成 .....	10-20
タスク 3: スポンサー・ノードの識別と読取り専用モードへの切替え .....	10-21
タスク 4: ldifwrite を使用したスポンサ・ノードのバックアップ .....	10-21
タスク 5: アドバンスド・レプリケーション追加ノードの設定の実行 .....	10-22
タスク 6: スポンサー・ノードの更新可能モードへの切替え .....	10-23
タスク 7: 新規ノード以外の全ノードで Oracle Directory Replication Server を起動 .....	10-24
タスク 8: bulkload を使用して新規ノードにデータをロード .....	10-24
タスク 9: 新規ノードで LDAP サーバーを起動 .....	10-24
タスク 10: 新規ノードで LDAP レプリケーション承諾を構成 .....	10-25
タスク 11: 新規ノードで Oracle Directory Replication Server を起動 .....	10-25
<b>レプリケーション・ノードの削除 .....</b>	<b>10-25</b>
タスク 1: すべてのノードでの Oracle Directory Replication Server の停止 .....	10-26
タスク 2: 削除するノード内の全プロセスの停止 .....	10-26
タスク 3: マスター定義サイトからのノードの削除 .....	10-26
タスク 4: すべてのノードでの Oracle Directory Replication Server の起動 .....	10-28
タスク 5: レプリケーション・グループからのノードの削除 .....	10-28
タスク 6: その他のノードでの Oracle Directory Replication Server の再起動 .....	10-28
<b>手動での競合の解消 .....</b>	<b>10-29</b>
レプリケーション変更の競合のモニター .....	10-29
競合解消メッセージの例 .....	10-29
例 1: 存在しないエントリを変更しようとした場合 .....	10-29
例 2: 既存のエントリを追加しようとした場合 .....	10-30
例 3: 存在しないエントリを削除しようとした場合 .....	10-30
管理者操作キュー操作ツールの使用 .....	10-30
管理者操作キューからリトライ・キューへの変更の移動 .....	10-31
管理者操作キューからパージ・キューへの変更の移動 .....	10-31
例: 管理者操作キュー操作ツールの使用 .....	10-32
OID 調停ツールの使用 .....	10-33
OID 調停ツールを使用した一貫性のないデータの調停 .....	10-33
OID 調停ツールの動作 .....	10-34

## 11 複数ディレクトリとの同期化

同期化プロセス .....	11-2
ディレクトリが Oracle Internet Directory から変更を最初に取り出す方法 .....	11-3
接続されたディレクトリが Oracle Internet Directory の orclLastAppliedChangeNumber 属性を更新する方法 .....	11-3
ディレクトリが Oracle Internet Directory から変更を取り出す方法（2 回目以降） .....	11-4
他のディレクトリと Oracle Internet Directory の同期化 .....	11-4
タスク 1: 初期ブートストラップを実行する .....	11-4
タスク 2: Oracle Internet Directory の変更サブスクリプション・オブジェクトとして ディレクトリを登録する .....	11-5
ディレクトリ登録の概要 .....	11-5
ディレクトリの登録 .....	11-5
ディレクトリの登録解除 .....	11-6
タスク 3: Oracle Internet Directory 変更ログ・オブジェクト・ストアへのアクセス権限を ディレクトリに付与する .....	11-6

## 12 各国語サポート（NLS）の管理

環境変数 NLS_LANG .....	12-2
LDIF ファイルでの NLS の使用方法 .....	12-3
ASCII 文字列のみを含む LDIF ファイル .....	12-3
UTF-8 エンコーディング文字列を含む LDIF ファイル .....	12-4
ケース 1: ネイティブ文字列（非 UTF-8） .....	12-4
ケース 2: UTF-8 文字列 .....	12-4
ケース 3: BASE64 でエンコーディングされた UTF-8 文字列 .....	12-4
ケース 4: BASE64 でエンコーディングされたネイティブ文字列 .....	12-5
コマンドライン・ツールでの NLS の使用方法 .....	12-5
各ツールを使用するときの -E 引数の指定 .....	12-5
例：コマンドライン・ツールでの -E 引数の使用方法 .....	12-6
クライアント環境における NLS_LANG の設定 .....	12-7
バルク・ツールでの NLS の使用方法 .....	12-8
bulkload での NLS の使用方法 .....	12-8
ldifwrite での NLS の使用方法 .....	12-8
bulkdelete での NLS の使用方法 .....	12-9
bulkmodify での NLS の使用方法 .....	12-9

## 第 III 部 Oracle Internet Directory の配置

### 13 配置に関する考慮事項

拡大するディレクトリの役割 .....	13-2
ディレクトリ情報の論理編成 .....	13-2
ディレクトリ・エントリのネーミング .....	13-2
DIT の階層と構造 .....	13-3
物理的な分散：パーティションとレプリカ .....	13-3
理想的な配置 .....	13-4
パーティション化に関する考慮事項 .....	13-4
レプリケーションに関する考慮事項 .....	13-5
フェイルオーバーに関する考慮事項 .....	13-6
容量計画、サイズ設定およびチューニング .....	13-6
容量計画 .....	13-7
サイズ設定に関する考慮事項 .....	13-8
チューニングに関する考慮事項 .....	13-9

### 14 容量計画

容量計画の説明 .....	14-2
ディレクトリの使用パターンの理解：事例 .....	14-3
I/O サブシステムの要件 .....	14-5
I/O サブシステムの説明 .....	14-5
ディスク領域要件の概算 .....	14-6
ディスク領域要件の詳細な計算 .....	14-7
メモリー要件 .....	14-11
ネットワーク要件 .....	14-11
CPU 要件 .....	14-12
CPU 構成 .....	14-12
CPU 要件の概算 .....	14-13
CPU 要件の詳細な計算 .....	14-13
Acme Corporation の容量計画のまとめ .....	14-15

### 15 チューニング

チューニングの概要 .....	15-2
パフォーマンス・チューニング用のツール .....	15-2

<b>CPU 使用量のチューニング</b> .....	15-3
Oracle Internet Directory のプロセスに関する CPU のチューニング .....	15-4
CPU 稼働率が 100% の場合の Oracle Internet Directory プロセスのチューニング .....	15-4
CPU が十分活用されていない場合の Oracle Internet Directory プロセスのチューニング .....	15-5
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 .....	15-5
SMP システムにおけるプロセッサ親和性の利用 .....	15-6
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 .....	15-6
<b>メモリーのチューニング</b> .....	15-7
Oracle8i 用のシステム・グローバル領域 (SGA) のチューニング .....	15-7
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 .....	15-7
<b>ディスクのチューニング</b> .....	15-8
表領域の均衡化 .....	15-8
RAID .....	15-9
<b>データベースのチューニング</b> .....	15-9
必須パラメータ .....	15-10
Oracle Internet Directory サーバーの構成に依存しているパラメータ .....	15-10
マルチスレッド・サーバー (MTS) の使用方法 .....	15-10
ハードウェア・リソースに依存している SGA パラメータ .....	15-11
<b>パフォーマンスに関するトラブルシューティング</b> .....	15-11

## 16 高い可用性とフェイルオーバー

<b>Oracle Internet Directory の高い可用性とフェイルオーバーの概要</b> .....	16-2
<b>Oracle Internet Directory および Oracle8i のテクノロジー・スタック</b> .....	16-2
<b>クライアントにおけるフェイルオーバー・オプション</b> .....	16-4
ユーザー入力からの代替サーバー・リスト .....	16-4
Oracle Internet Directory サーバーからの代替サーバー・リスト .....	16-4
<b>パブリック・ネットワーク・インフラストラクチャのフェイルオーバー・オプション</b> .....	16-5
ハードウェア・ベースの接続リダイレクション .....	16-7
ソフトウェア・ベースの接続リダイレクション .....	16-7
<b>Oracle Internet Directory の可用性とフェイルオーバー機能</b> .....	16-7
<b>プライベート・ネットワーク・インフラストラクチャのフェイルオーバー・オプション</b> .....	16-8
IP アドレス・テイクオーバー (IPAT) .....	16-8
冗長リンク .....	16-8
<b>高い可用性の配置例</b> .....	16-9

## 第 IV 部 付録

### A LDIF およびコマンドライン・ツールの構文

LDAP データ交換フォーマット (LDIF) の構文 .....	A-2
コマンドライン・ツールの構文 .....	A-4
ldapadd 構文 .....	A-4
ldapaddmt 構文 .....	A-6
ldapbind 構文 .....	A-7
ldapcompare 構文 .....	A-8
ldapdelete 構文 .....	A-10
ldapmoddn 構文 .....	A-11
ldapmodify 構文 .....	A-12
ldapmodifymt 構文 .....	A-16
ldapsearch 構文 .....	A-17
ldapsearch フィルタの例 .....	A-19
バルク・ツールの構文 .....	A-21
bulkdelete 構文 .....	A-21
bulkload 構文 .....	A-22
bulkmodify 構文 .....	A-24
ldifwrite 構文 .....	A-26
カタログ管理ツールの構文 .....	A-27
OID モニターの構文 .....	A-28
OID モニターの開始 .....	A-28
OID モニターの停止 .....	A-29
OID 制御ユーティリティの構文 .....	A-30
Oracle Directory Server インスタンスの起動と停止 .....	A-30
Oracle Directory Server インスタンスの起動 .....	A-30
Oracle Directory Server インスタンスの停止 .....	A-31
Oracle Directory Replication Server インスタンスの起動と停止 .....	A-32
Oracle Directory Replication Server インスタンスの起動 .....	A-32
Oracle Directory Replication Server インスタンスの停止 .....	A-33
Directory Server インスタンスの再起動 .....	A-33
Directory Server インスタンスの起動に関するトラブルシューティング .....	A-34
OID データベース・パスワード・ユーティリティの構文 .....	A-35



OID データベース統計収集ツールの構文 .....	A-35
構文 .....	A-35
パラメータ .....	A-36
例：OID データベース統計収集ツールの使用方法 .....	A-36

## B データベース・コピー・プロシージャを使用した DSA の追加

前提事項 .....	B-2
スポンサ・ディレクトリ・サイトの環境 .....	B-2
新規ディレクトリ・サイトの環境 .....	B-2
スポンサ・ノードで実行されるタスク .....	B-3
新規ノードで実行されるタスク .....	B-8
検証プロセス .....	B-11

## C Oracle Wallet Manager の使用方法

概要 .....	C-2
Wallet の管理 .....	C-3
Oracle Wallet Manager の起動 .....	C-4
新規 Wallet の作成 .....	C-4
既存 Wallet のオープン .....	C-5
Wallet のクローズ .....	C-5
変更の保存 .....	C-5
新しい位置へのオープン Wallet の保存 .....	C-6
システム・デフォルトへの保存 .....	C-6
Wallet の削除 .....	C-6
パスワードの変更 .....	C-7
自動ログインの使用法 .....	C-7
自動ログインの有効化 .....	C-7
自動ログインの無効化 .....	C-8
Oracle Application Server での Oracle Wallet Manager の使用法 .....	C-8
証明書の管理 .....	C-8
ユーザー証明書の管理 .....	C-8
証明書要求の作成 .....	C-9
ユーザーの証明書要求のエクスポート .....	C-10
ユーザー証明書の Wallet へのインポート .....	C-10
ユーザー証明書の Wallet からの削除 .....	C-11

信頼されている証明書の管理 .....	C-11
信頼されている証明書のインポート .....	C-12
信頼されている証明書の削除 .....	C-13
信頼されている証明書のエクスポート .....	C-13
信頼されている全証明書のエクスポート .....	C-13
Wallet のエクスポート .....	C-14

## D アクセス制御ディレクティブ書式の使用法

orclACI のスキーマ .....	D-2
orclEntryLevelACI のスキーマ .....	D-3

## E スキーマ要素

Oracle Internet Directory で施行されている IETF Requests for Comments (RFC) .....	E-2
Oracle Internet Directory で施行されている IETF Draft .....	E-2
Oracle Internet Directory 専用のスキーマ要素 .....	E-3
LDAP 構文 .....	E-6
Oracle Internet Directory で施行されている LDAP 構文 .....	E-7
Oracle Internet Directory が認識する、一般的に使用されている LDAP 構文 .....	E-7
Oracle Internet Directory が認識する、その他の LDAP 構文 .....	E-7
属性値のサイズ .....	E-8
一致規則 .....	E-9

## F 他の LDAP 準拠のディレクトリからのデータの移行

データ移行プロセスの概要 .....	F-2
データの移行 .....	F-2
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 .....	F-2
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 .....	F-3
タスク 3: Oracle Internet Directory 内のスキーマの拡張 .....	F-3
タスク 4: LDIF ファイルからの専用のディレクトリ・データの削除 .....	F-3
タスク 5: LDIF ファイルからの操作属性の削除 .....	F-3
タスク 6: LDIF ファイルからの非互換の userPassword 属性値の削除 .....	F-4
タスク 7: bulkload.sh -check モードの実行とスキーマ違反または 重複エラーが残っているかの判断 .....	F-4

## G    **トラブルシューティング**

インストール時のエラー .....	G-2
管理エラー・メッセージとその原因 .....	G-2
スキーマ変更が原因の Oracle データベース・サーバー・エラー .....	G-2
Oracle Directory Server から戻される標準エラー・メッセージ .....	G-2
その他のエラー・メッセージ .....	G-6

## **用語集**

## **索引**



---

# はじめに

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

# 対象読者

このマニュアルは、Oracle Internet Directory のシステム管理タスクを実行するすべての人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 NT オペレーティング・システムのいずれかをよく理解している必要があります。コマンドライン・モードのコマンドを使用すると、すべてのタスクを実行できます。また、大部分のタスクは、オペレーティング・システムに依存しない Oracle Directory Manager から実行できます。

# 構成

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

## 第 I 部：スタート・ガイド

第 I 部の内容は、製品と機能の概要、ディレクトリの構成と管理に必要な概念的な基礎知識、Directory Server の起動方法、および様々な管理ツールの紹介です。各章の説明は、次のとおりです。

### 第 1 章「概要」

ディレクトリ、LDAP および Oracle Internet Directory の機能の概要を提供します。

### 第 2 章「概念とアーキテクチャ」

オンライン・ディレクトリと Lightweight Directory Access Protocol (LDAP) の概要を提供します。また、ディレクトリ・エントリ、属性、オブジェクト・クラス、ネーミング・コンテキスト、スキーマ、分散ディレクトリ、セキュリティおよび各国語サポートの概念についても説明します。この章では、Oracle Internet Directory のアーキテクチャについても説明します。

### 第 3 章「事前に実行する作業」

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

#### 第4章「管理ツールの使用方法」

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

## 第II部：Oracle Internet Directory の管理

第II部では、Oracle Internet Directory の構成とメンテナンスに必要なタスクを紹介しします。各章の説明は、次のとおりです。

#### 第5章「Oracle Directory Server の管理」

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

#### 第6章「ディレクトリ・スキーマの管理」

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

#### 第7章「ディレクトリ・エントリの管理」

Oracle Directory Manager とコマンドライン・ツールを使用して、エントリを検索、表示、追加、変更および管理する方法を説明します。

#### 第8章「Secure Sockets Layer (SSL) の管理」

Secure Sockets Layer (SSL) の機能を構成する方法を紹介し説明します。

#### 第9章「ディレクトリのアクセス制御の管理」

アクセス制御方針の概要を提供し、ディレクトリ・アクセスの管理方法を説明します。

#### 第10章「ディレクトリ・レプリケーションの管理」

レプリケーションについて説明します。初めて Oracle Directory Replication Server ・ソフトウェアをインストールおよび初期化する方法、ソフトウェアがすでにインストールされている環境に新規ノードをインストールする方法を説明します。

#### 第11章「複数ディレクトリとの同期化」

Oracle Internet Directory と他のディレクトリとの間で同期がどのように起こるかを説明します。また、他のディレクトリを Oracle Internet Directory と同期化する方法を説明します。

## 第 12 章「各国語サポート (NLS) の管理」

Oracle Internet Directory で使用されている各国語サポート (National Language Support : NLS) について説明します。

## 第 III 部：Oracle Internet Directory の配置

第 III 部では、配置に関する考慮事項を説明します。各章の説明は、次のとおりです。

### 第 13 章「配置に関する考慮事項」

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。この章は企業内のディレクトリの要件を評価し、効果的な配置を選択するのに役立ちます。

### 第 14 章「容量計画」

Oracle Internet Directory の容量計画に関するガイドラインを示します。

### 第 15 章「チューニング」

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。

### 第 16 章「高い可用性とフェイルオーバー」

Oracle Internet Directory の高い可用性とフェイルオーバー機能、および配置のガイドラインを示します。

## 第 IV 部：付録

### 付録 A「LDIF およびコマンドライン・ツールの構文」

LDAP データ交換フォーマットと LDAP コマンドライン・ツールに関する構文、使用方法および例を紹介します。

### 付録 B「データベース・コピー・プロシージャを使用した DSA の追加」

ディレクトリが非常に大きい場合に、レプリケート・ディレクトリ・システムにノードを追加するための代替方法を紹介します。

### 付録 C「Oracle Wallet Manager の使用方法」

Wallet と証明書を作成および管理するために Oracle Wallet Manager を使用する方法を説明します。

### 付録 D「アクセス制御ディレクティブ書式の使用方法」

アクセス制御項目 (Access Control Information Item : ACI) の書式 (構文) を説明します。

### 付録 E「スキーマ要素」

Oracle Internet Directory でサポートされているスキーマ要素を説明します。

### 付録 F「他の LDAP 準拠のディレクトリからのデータの移行」

LDAP バージョン 3 互換のディレクトリから Oracle Internet Directory へデータを移行する手順を説明します。

### 付録 G「トラブルシューティング」

発生する可能性がある障害とエラー・コード、および考えられる原因を説明します。



# 関連文書

Oracle の関連情報は、次のドキュメントを参照してください。

- Oracle Directory Manager から使用できるオンライン・ヘルプ
- Oracle8i ドキュメント・セット

このマニュアルで説明されている概念の詳細は、次のマニュアルおよびオンライン・ドキュメントを参照してください。これらの文献の大半には、他の出版物に関する参照情報が記載されています。

『Chadwick, David, Understanding X.500 The Directory. Thomson Computer Press, 1996』この書籍は現在絶版になっていますが、次の Web サイトからオンライン版を入手できます。  
<http://www.salford.ac.uk/its024/Version.Web/Contents.htm>

Hodges, Jeff, Staff Scientist, Oblix, Inc.,  
<http://www.kingsmountain.com/ldapRoadmap.shtml>

『Howes, Tim and Mark Smith, LDAP: Programming Directory-enabled Applications with Lightweight Directory Access Protocol. Macmillan Technical Publishing, 1997』

『Howes, Tim, Mark Smith and Gordon Good, Understanding and Deploying LDAP Directory Services. Macmillan Technical Publishing, 1999』

『Kosiur, Dave, LDAP: "The next-generation directory?", SunWorld Online"SunWorldOnline ,October 1997』

『Radicati, Sara, X.500 Directory Services, Technology and Deployment, International Thomson Computer Press, 1994』

University of Michigan LDAP  
Repository,<http://www.umich.edu/~dirsvcs/ldap/index.html>

# 表記規則

このマニュアルでは、次の表記規則を使用します。

表記	意味
・	縦の省略記号が例の中で使用されている場合は、例に直接関係のない情報が省略されていることを示します。
・	
・	
...	横の省略記号が文またはコマンド内で使用されている場合は、その文またはコマンドの一部が省略されていることを示します。
太字	太字のテキストは、用語集で定義されている用語、コマンドでユーザーが入力する必要があるテキスト、または小見出しを示します。

表記	意味
イタリック	イタリック体は、コード例の中でユーザーが値を指定する必要がある変数を示します。
固定幅フォント	固定幅フォントは、ユーザーの入力例とコード例に使用されます。
構文	この字体は、コード例の中の構文説明に使用されます。
<>	山カッコは、コード例の中でユーザーが指定する必要がある名前を示します。
[]	大カッコは選択が任意の項目を示します。選択肢の中から1つ選択するか、または何も入力しなくても構いません。
{ }	中カッコは選択が必須の項目を表します。選択肢の中から1つ選択します。

---

# Oracle Internet Directory の新機能

Oracle Internet Directory リリース 2.1.1 は次の新機能を含んでいます。

機能	参照箇所
属性オプション（言語コードを含む）	概念の説明は、2-7 ページの「 <a href="#">属性オプション</a> 」を参照してください。 7-16 ページ「 <a href="#">属性オプションのあるエントリの管理</a> 」
変更ログの削除機能拡張	概念の説明は、2-27 ページの「 <a href="#">変更ログの削除</a> 」を参照してください。 10-11 ページ「 <a href="#">Oracle Directory Replication Server のパラメータ</a> 」
次の操作属性の拡張サポート <ul style="list-style-type: none"><li>■ creatorsName</li><li>■ createTimestamp</li><li>■ modifiersName</li><li>■ modifyTimestamp</li></ul>	概念の説明は、2-4 ページの「 <a href="#">属性情報の種類</a> 」を参照してください。 5-12 ページ「 <a href="#">システム操作属性の設定</a> 」 createTimestamp 属性を使用した検索操作の例は、A-20 ページの「 <a href="#">例 6: 全ユーザー属性および指定した操作属性の検索</a> 」を参照してください。
管理者操作キュー操作ツール	このツールの概要は、4-14 ページの「 <a href="#">レプリケーション・ツールの使用方法</a> 」を参照してください。 10-30 ページ「 <a href="#">管理者操作キュー操作ツールの使用</a> 」
他の LDAP 準拠のディレクトリからの移行	付録 F「 <a href="#">他の LDAP 準拠のディレクトリからのデータの移行</a> 」
オブジェクト・クラスの増加	オブジェクト・クラスを追加するときのこの機能の使用方法は、6-3 ページの「 <a href="#">オブジェクト・クラスの追加のガイドライン</a> 」を参照してください。

機能	参照箇所
OID データベース統計収集ツール	4-14 ページ「 <a href="#">OID データベース統計収集ツールの使用方法</a> 」
パスワード暗号化機能拡張	<p>概念の説明は、2-16 ページの「<a href="#">パスワード暗号化</a>」を参照してください。</p> <p>パスワード暗号化の設定方法は、5-16 ページの「<a href="#">パスワード暗号化の管理</a>」を参照してください。</p>
OID 調停ツール	<p>このツールの簡単な説明は、4-14 ページの「<a href="#">レプリケーション・ツールの使用方法</a>」を参照してください。</p> <p>10-33 ページ「<a href="#">OID 調停ツールの使用</a>」</p>
レプリケーション・ノードの削除	10-25 ページ「 <a href="#">レプリケーション・ノードの削除</a> 」
メタディレクトリ環境での複数ディレクトリとの同期	<p>概念の説明は、2-42 ページの「<a href="#">メタディレクトリ環境での他のディレクトリとの同期</a>」を参照してください。</p> <p><a href="#">第 11 章「複数ディレクトリとの同期化」</a></p>
アップグレード手順	3-9 ページ「 <a href="#">Oracle Internet Directory の以前のリリースからのアップグレード</a> 」

# 第I部

---

## スタート・ガイド

第I部の内容は、Oracle Internet Directory とその機能の概要、ディレクトリの正しい構成と管理に必要な概念的な基礎知識、起動方法の具体的な説明および管理ツールの紹介です。

第I部は次の各章から構成されています。

- [第1章「概要」](#)
- [第2章「概念とアーキテクチャ」](#)
- [第3章「事前に実行する作業」](#)
- [第4章「管理ツールの使用方法」](#)



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

この章では、次の項目について説明します。

- ディレクトリとは
- LDAP とは
- Oracle Internet Directory とは

# ディレクトリとは

ディレクトリは、情報を検索しやすいように編成します。それには、オブジェクト（たとえば、人、図書館の本、百貨店の商品など）をリストし、それぞれに詳細情報を設定します。ディレクトリの代表例には、電話帳、図書館のカード式目録、百貨店のカタログなどがあります。

この項では、次の項目について説明します。

- [オンライン・ディレクトリ](#)
- [オンライン・ディレクトリとリレーショナル・データベースの違い](#)
- [問題：複数の特別な用途のディレクトリ](#)
- [解決策：LDAP 準拠の一般的な用途のディレクトリ](#)

## オンライン・ディレクトリ

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、管理を必要とするリソースを表します。従業員名、役職、セキュリティ資格証明、E-Commerce パートナの情報または会議室やプリンタなどの共有ネットワーク・リソースの情報などが格納されます。

ディレクトリは様々なユーザーやアプリケーションによって、様々な用途で使用されます。一般的な使用例を次に示します。

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

## オンライン・ディレクトリとリレーショナル・データベースの違い

データベースはデータの構造化された集合です。オンライン・ディレクトリはデータベースですが、[リレーショナル・データベース](#)ではありません。次の表はオンライン・ディレクトリをリレーショナル・データベースと対比しています。

オンライン・ディレクトリ	リレーショナル・データベース
主に読み込みを目的としています。一般的な使用例では、データの更新が比較的少なく、検索が多い傾向があります。	主に書き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。



オンライン・ディレクトリ	リレーショナル・データベース
<p>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。</p> <p>ロケーションに依存しないように設計されています。ディレクトリ・アプリケーションは、問合せ中のサーバーに関係なく、配置環境全体にわたって常に同じ情報を参照していると想定しています。問合せ先のサーバーにローカルの情報に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、またはクライアント・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。</p> <p>情報をエントリに格納するように設計されています。これらのエントリは、従業員、E-Commerce パートナ、会議室、プリンタのような共有ネットワーク・リソースなど、管理が必要なリソースを表します。各エントリには、多数の属性が対応付けられます。それぞれの属性には1つ以上の値が割り当てられる場合があります。たとえば、person エントリの一般的な属性は、姓名、電子メール・アドレス、デフォルトのメール・サーバーのアドレス、パスワードまたは他のログイン資格証明、デジタル化された顔写真などです。</p>	<p>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。</p> <p>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。通常は特定のデータベース・サーバーに常駐します。</p> <p>リレーショナル表にレコードとして情報を格納するように設計されています。</p>

## 問題：複数の特別な用途のディレクトリ

ある見積りによると、世界規模の企業は平均 180 種類のディレクトリを作成しており、それぞれに特別な用途を指定しています。様々なエンタープライズ・アプリケーションには、ユーザー名を割り当てた個有のディレクトリがあるため、それら専用ディレクトリの実際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、3つの問題が発生する可能性があります。

- 一貫性のないデータ：1つのディレクトリで更新された情報が、他のすべてのディレクトリとの間で共有されません。
- 冗長性：同じ情報が、企業内の複数の場所に記述されます。
- 高い管理費用：管理者は、複数の場所に格納された同じ情報をメンテナンスする必要があります。

たとえば、ある企業が新しい従業員を雇用するとき、管理者は新しいユーザー ID をネットワークに作成し、新しい電子メール・アカウントを作成し、そのユーザーを従業員データベースに追加し、そして従業員が必要とするすべてのアプリケーション（開発、テストおよび本番データベース・システムのユーザー・アカウントなど）を設定する必要があります。その従業員が退社した場合は、管理者はこれらのユーザー・アカウントをすべて無効にするために逆の処理を行う必要があります。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、管理オーバーヘッドが増すだけでなく、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。

## 解決策：LDAP 準拠の一般的な用途のディレクトリ

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の共通の規格に基づいた、より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なのは明らかです。Oracle Internet Directory は、[Lightweight Directory Access Protocol \(LDAP\)](#) の使用によってこのニーズに応えます。

## LDAP とは

[Lightweight Directory Access Protocol \(LDAP\)](#) 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共通言語です。

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ク・ソフトウェアを最小限に抑えられるため、インターネット・ベースの Thin クライアント・アプリケーションには特に理想的です。

この項では、次の項目について説明します。

- [LDAP と単純化されたディレクトリ管理](#)
- [LDAP バージョン 3](#)

## LDAP と単純化されたディレクトリ管理

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

- 拡張可能な単一のディレクトリ・サービスに対し、正しく定義された単一の標準インタフェースを、企業内のすべてのユーザーとアプリケーションに提供します。これによって、ディレクトリに対応したアプリケーションの迅速な開発と配置が簡単になります。
- 企業内に散在する複数のサービスへの、冗長な情報の入力と調整の必要性を低減します。

- 正しく定義されたプロトコルと一連のプログラム・インタフェースによって、ディレクトリを活用するインターネット対応のアプリケーションの配置がより実用的になります。

## LDAP バージョン 3

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

- 各国語サポート：LDAP バージョン 3 では、世界中の言語で使用されている文字を、サーバーとクライアントの両方でサポートできます。
- ナレッジ参照（参照とも呼ばれます）：LDAP バージョン 3 の参照機能によって、サーバーは、ディレクトリ問合せの結果として、参照を他のサーバーに戻すことができます。この機能によって、[ディレクトリ情報ツリー](#)（第 2 章を参照）を複数の LDAP サーバー間に分割でき、グローバル配置が可能となります。
- セキュリティ：Simple Authentication and Security Layer（SASL）および Transport Layer Security（TLS）をサポートするための標準機能が追加され、データ・セキュリティに関する広範囲でかつ拡張可能なフレームワークが LDAP に提供されています。
- 拡張性：LDAP バージョン 3 では、ベンダーは、コントロールと呼ばれるメカニズムを使用して既存の LDAP 操作を拡張できます。
- 機能およびスキーマの開示：LDAP バージョン 3 では、他の LDAP サーバーやクライアントに役立つ情報（サポートされる LDAP プロトコルやディレクトリ・スキーマの説明など）を公開できます。

### 関連項目：

- IETF の RFC（Requests for Comments）2251 ～ 2256。次の URL で入手可能です。  
<http://www.ietf.org/rfc.html>
- LDAP に関する参考資料のその他のリストは、xxiii ページの「[関連文書](#)」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・リソースに関する情報の検索を可能にする、汎用ディレクトリ・サービスです。[LDAP](#) バージョン 3 と Oracle8i のすぐれたパフォーマンス、拡張性、耐久性および可用性を組み合わせたものです。

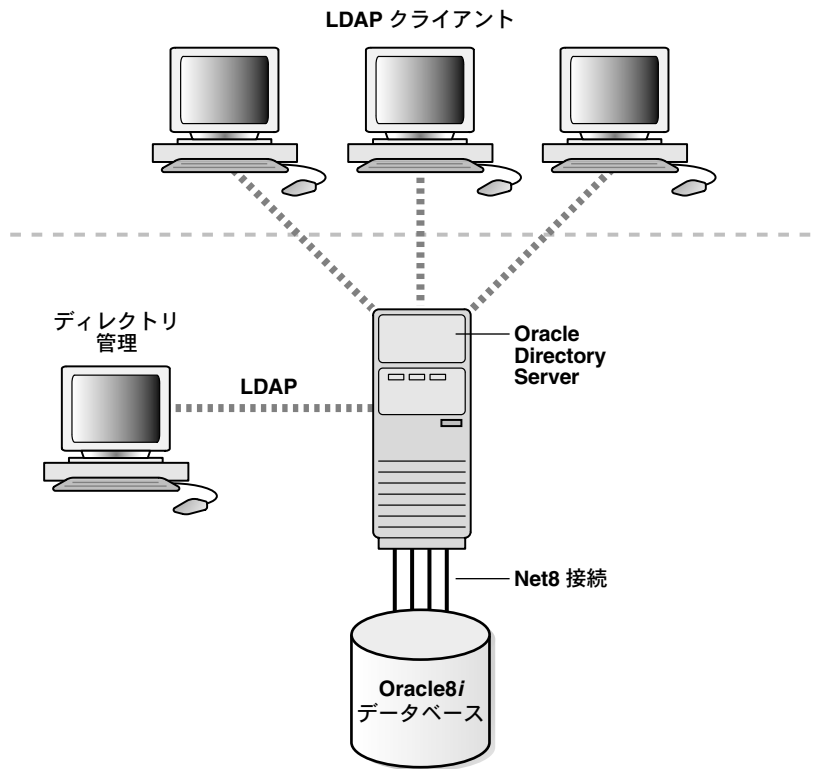
この項では、次の項目について説明します。

- [Oracle Internet Directory と Oracle8i](#)
- [Oracle Internet Directory のコンポーネント](#)
- [Oracle Internet Directory の利点](#)

## Oracle Internet Directory と Oracle8i

Oracle Internet Directory は、Oracle 8i 上のアプリケーションとして動作します。データベース（オペレーティング・システムが異なってもかまいません）と、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 [Net8](#) を使用して通信します。[図 1-1](#) はこの関係を示しています。

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



## Oracle Internet Directory のコンポーネント

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

- Oracle Directory Server。人員とリソースの情報に関するクライアントの要求に応答します。また、TCP/IP を介して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 Directory Replication Server。Oracle Directory Server 間で、LDAP データをレプリケートします。
- Oracle Directory Manager。Java ベースのグラフィカル・ユーザー・インタフェースを使用した管理ツール。
- 各種のコマンドライン管理ツールとデータ管理ツール。

## Oracle Internet Directory の利点

Oracle Internet Directory には、次のような重要な利点があります。

- [拡張性](#)
- [高い可用性](#)
- [セキュリティ](#)

### 拡張性

Oracle Internet Directory は、Oracle8i の高機能を活用して、数テラバイト (TB) に及ぶディレクトリ情報のサポートを可能にします。さらに、マルチスレッド 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ーによって、千単位の同時クライアントであっても、わずかな検索応答時間を実現します。

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

### 高い可用性

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、Oracle Internet Directory は、Directory Server 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。サーバー上のデータの変更情報は、Oracle8i データベース上の専用の表に格納されます。この表は、堅牢なレプリケーション方式である Oracle の[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、Oracle8i 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、Oracle8i データベースに安全に格納されるため、Oracle のバックアップ機能によって保護されます。また、Oracle8i データベースは、大規模なデータストアおよび高負荷で実行されていても、システム障害からすぐにリカバリできます。

### セキュリティ

Oracle Internet Directory は、広範囲にわたる柔軟なアクセス制御を提供します。管理者は、特定のディレクトリ・オブジェクトまたはディレクトリ・サブツリー全体に対するアクセス権限を付与または制御できます。さらに、Oracle Internet Directory は匿名、パスワード・ベースおよび [Secure Socket Layer \(SSL\)](#) バージョン 3 を使用した証明書ベースの 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・プライバシーが保障されています。

---

## 概念とアーキテクチャ

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

この章では、次の項目について説明します。

- [エントリ](#)
- [属性](#)
- [オブジェクト・クラス](#)
- [ネーミング・コンテキスト](#)
- [ディレクトリ・スキーマ](#)
- [セキュリティ](#)
- [各国語サポート](#)
- [Oracle Internet Directory のアーキテクチャ](#)
- [分散ディレクトリ : 概要](#)
- [分散ディレクトリ : レプリケーション](#)
- [分散ディレクトリ : パーティション化](#)
- [メタディレクトリ環境での他のディレクトリとの同期](#)

**関連項目：** LDAP 準拠のディレクトリに関する参考文献のリストは、xxiii ページの「[関連文書](#)」を参照してください。

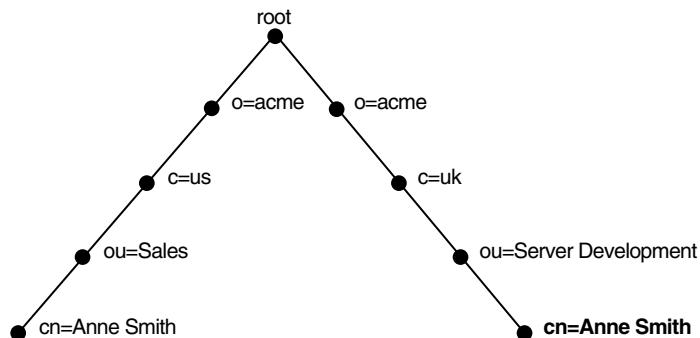
# エントリ

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

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

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

**図 2-1 ディレクトリ情報ツリー**



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

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

この Anne Smith エントリの識別名（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 DIT 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、ルートのコポーネントまで順に記述することに注意してください。

識別名内の最下位コンポーネントは**相対識別名**（RDN）と呼ばれます。たとえば、前述の Anne Smith のエントリの RDN は cn=Anne Smith です。同様に、Anne Smith の RDN のすぐ上のエントリに対応する RDN は、ou=Server Development、ou=Server



Development のすぐ上のエントリに対応する RDN は、c=uk です。DN は、このように各 RDN をカンマで区切って順に並べたものです。

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

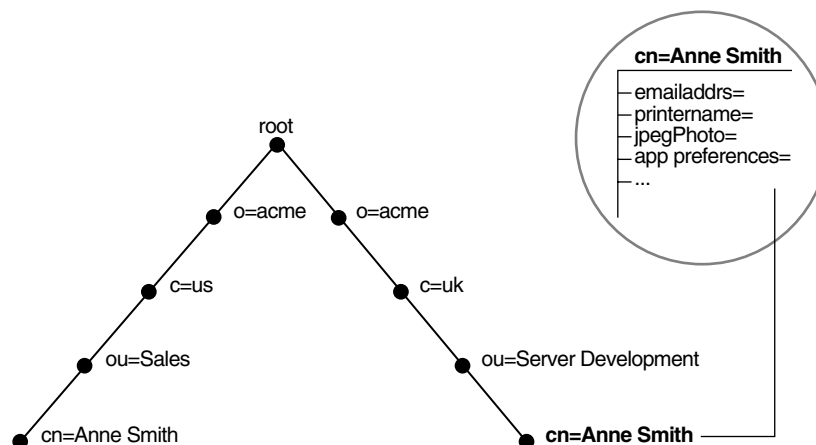
**関連項目：** 第 7 章「ディレクトリ・エントリの管理」

## 属性

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

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

図 2-2 Anne Smith のエントリの属性



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

この項では、次の項目について説明します。

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

## 属性情報の種類

属性には2種類の情報があります。

アプリケーション情報	この情報は、ディレクトリ・クライアントによってメンテナンスおよび取出しが行われ、ディレクトリの操作には影響しません。例として電話番号があります。
操作情報	この情報は、ディレクトリ自体の操作に関係します。一部の操作情報は、サーバーを制御するためにディレクトリによって指定されます。たとえば、エントリの作成や変更のタイム・スタンプ、エントリを作成または変更したユーザーの名前などです。アクセス情報など、その他の操作情報は、管理者が定義し、ディレクトリ・プログラムの処理時に、そのプログラムによって使用されます。

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

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

creatorsName	エントリ作成者の名前
createTimestamp	UTC (Coordinated Universal Time) でのエントリの作成時間
modifiersName	エントリの作成者の名前
modifyTimestamp	UTC でのエントリの作成時間

ユーザーがエントリを変更すると、Oracle Internet Directory は自動的に modifiersName 属性と modifyTimestamp 属性に対しても次のように更新します。

modifiersName      エントリを変更した人の名前  
 modifyTimestamp    UTC でのエントリの変更時間

**関連項目：** システム操作属性の構成方法は、5-12 ページの「[システム操作属性の設定](#)」を参照してください。

## 単一値と複数値の属性

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

## 一般的な LDAP 属性

Oracle Internet Directory は、標準的な LDAP 属性をすべて実装しています。表 2-1 に、一般的な LDAP 属性のいくつかを示します。

表 2-1 一般的な LDAP 属性

属性の型	属性の文字列	説明	属性値の例
commonName	cn	エントリの一般名。	cn=Anne Smith
domainComponent	dc	Domain Name System (DNS) 内のコンポーネント。	次の DN: dc=uk,dc=acme,dc=com
jpegPhoto	jpegPhoto	JPEG フォーマットの写真イメージ。エントリの属性として組み込む JPEG イメージのパスとファイル名。	/photo/audrey.jpg
organization	o	組織の名称。	o=acme
organizationalUnitName	ou	組織内の単位の名称。	ou=Server Development
owner	owner	エントリを所有している個人の識別名。	次の LDIF ファイル内の記述: owner:cn=Anne Smith, ou=Server Development, o= Acme, c=uk
surname、sn	sn	個人の姓。	Smith

表 2-1 一般的な LDAP 属性（続き）

属性の型	属性の文字列	説明	属性値の例
telephoneNumber	telephoneNumber	電話番号。	telephoneNumber= (650) 123-4567  または  telephoneNumber=65012345 67

**関連項目：** Oracle Internet Directory が用意している専用の属性のリストは、[付録 E](#) を参照してください。

属性の構文

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

Oracle Internet Directory は、RFC 2252 で指定されている構文のほとんどを認識するため、そのドキュメントに記述されている構文の大部分を属性と関連付けることができます。さらに、一部の LDAP 構文も施行します。Oracle Internet Directory ですでにサポートされているこれらの構文以外に、新規の構文を追加することはできません。

**関連項目：** E-6 ページ [「LDAP 構文」](#)

属性の一致規則

Directory Server は、クライアントの要求に応じて、検索と比較の操作を実行します。この操作時に、Directory Server 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 のいずれかと一致させるか、あるいはその両方と一致させることができます。属性を作成したときに、それを一致規則と対応付けることができます。

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

**関連項目：** E-9 ページ [「一致規則」](#)

## 属性オプション

属性の型には様々なオプションがあり、検索または比較操作でその属性の値をどのように使用できるかを指定できます。たとえば、ある従業員がロンドンとニューヨークという2つの住所を持っているとします。その従業員の `address` 属性のオプションを使用すると、両方の住所を格納できます。さらに、属性オプションは言語コードを含むことができます。たとえば、John Doe の `givenName` 属性のオプションを使用すると、彼の名前をフランス語と日本語の両方で格納できます。

1つ以上のオプションを持った属性は、そのベース属性のプロパティ（例：一致規則および構文）を持ちます。ベース属性はオプションを持ちません。たとえば、`cn` がベース属性だとします。`cn;lang-fr=Jean` がそのベース属性のフランス語の値の場合、その値は `cn` と同じ一致規則および構文を持ちます。

---

**注意：** 属性オプションは DN 内では使用できません。たとえば、次の DN は不適切です。

```
cn;lang-fr=Jean, ou=sales,o=acme,c=uk.
```

---

**関連項目：** [第6章「ディレクトリ・スキーマの管理」](#)

## オブジェクト・クラス

**オブジェクト・クラス**は**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。オブジェクト・クラスには属性が含まれており、属性には必須のものもあれば、オプションのものもあります。

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。`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、これらの属性に値を指定する必要があります。このオブジェクト・クラスには、`telephoneNumber`、`uid`、`streetAddress` および `userPassword` など、いくつかのオプション属性も含まれています。`organizationalPerson` オブジェクト・クラスの使用時に、これらオプション属性に値を提供する必要はありません。

インストール時には、いくつかの専用オブジェクト・クラスと同様に、標準的な LDAP オブジェクト・クラスを **Oracle Internet Directory** が用意します。この事前に定義されたオブジェクト・クラスに属している属性のセットには、必須属性を追加できません。エントリに必要なすべての属性が所定のオブジェクト・クラスに含まれていない場合には、次のうちのいずれかを行います。

- 既存のオブジェクト・クラスへのオプション属性の追加
- 新規の（ベース）オブジェクト・クラスの定義
- オブジェクト・サブクラスの定義

**関連項目：** Oracle Internet Directory とともにインストールされるスキーマに含まれるオブジェクト・クラスのリストは、[付録 E](#) を参照してください。

この項では、次の項目について説明します。

- [サブクラス、スーパー・クラスおよび継承](#)
- [オブジェクト・クラスの型](#)

## サブクラス、スーパー・クラスおよび継承

**サブクラス**は、別のオブジェクト・クラスから導出されたオブジェクト・クラスです。導出元のオブジェクト・クラスは、その**スーパー・クラス**と呼ばれています。たとえば、オブジェクト・クラス `organizationalPerson` は、オブジェクト・クラス `person` のサブクラスです。逆に、オブジェクト・クラス `person` は、オブジェクト・クラス `organizationalPerson` のスーパー・クラスです。

サブクラスは、そのスーパー・クラスに属している属性をすべて**継承**します。各エントリは、複数のオブジェクト・クラスによって定義された属性を継承できます。

---

---

**注意：** オブジェクト・クラス自体に値は含まれていません。値は、オブジェクト・クラスのインスタンスのみに含まれています。サブクラスがスーパー・クラスから属性を継承するときはスーパー・クラスの属性フレームワークのみ継承し、属性の値は継承しません。

---

---

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

## オブジェクト・クラスの型

オブジェクト・クラスには次の3つの型があります。

- 抽象型
- 構造型
- 補助型

### 抽象型オブジェクト・クラス

抽象型オブジェクト・クラスは仮想のオブジェクト・クラスです。これは、抽象型オブジェクト・クラスのみをエントリのオブジェクト・クラスにはできないことを意味します。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。構造型オブジェク

ト・クラスすべてに対するスーパー・クラスである必要はありますが、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。次のリストは、top 内にあるオプション属性の名前と、その説明または詳細情報の参照箇所を示しています。

- `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` — 対応する IETF ドキュメントを参照してください。
- `createTimestamp` — 対応する IETF ドキュメントを参照してください。
- `orclACI` — 9-2 ページの「[orclACI](#)」を参照してください。
- `orclEntryLevelACI` — 9-3 ページの「[orclEntryLevelACI](#)」を参照してください。

## 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な性質を表します。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、すべてのエントリが少なくとも 1 つの構造型オブジェクト・クラスに属します。構造型オブジェクト・クラスの例に `person` や `groupOfNames` があります。

これらのオブジェクト・クラスは、指定したオブジェクト・クラスの下にどのような種類のオブジェクト・クラスを作成可能にするかの制限を与えます。たとえば、体系規則では `organization (o)` オブジェクト・クラスの下にあるすべてのオブジェクトは `organizational units (ou)` であることが要求されます。この規則に従うと、`person` オブジェクトを `organization` オブジェクト・クラスの下に直接入力できません。

## 補助型オブジェクト・クラス

補助型オブジェクト・クラスは、属性をグループ化したもので、エントリ内の既存の属性リストを拡張します。たとえば、あるエントリを 2 つのオブジェクト・クラスのメンバーとして定義し、そのエントリに、これら 2 つのオブジェクト・クラスに属していない追加属性を割り当てるとします。この場合、その追加属性を含んだ補助型オブジェクト・クラスを新たに作成して、その補助型オブジェクト・クラスをエントリと関連付けることができます。これは、既存のオブジェクト・クラスを再定義せずに属性を追加する 1 つの方法です。

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

---

---

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

---

---

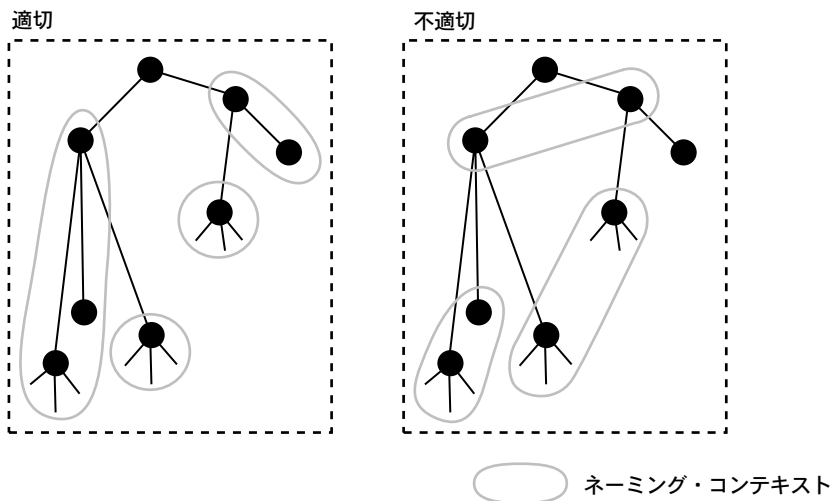
**関連項目：** [第 6 章「ディレクトリ・スキーマの管理」](#)

## ネーミング・コンテキスト

**ネーミング・コンテキスト**は、完全に1つのサーバーに常駐しているサブツリーです。サブツリーは連続している必要があります。つまり、サブツリーの最上位の役割を果たす**エントリ**から始まり、下位方向にリーフ・エントリまたは従属ネーミング・コンテキストへの参照のいずれかまでを範囲とする必要があります。単一のエントリから**ディレクトリ情報ツリー** (DIT) 全体までをその範囲とすることができます。

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

図 2-3 有効なネーミング・コンテキストと無効なネーミング・コンテキスト



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

**関連項目：** ネーミング・コンテキストの公開方法は、5-15 ページの「**ネーミング・コンテキストの管理**」を参照してください。

## ディレクトリ・スキーマ

ディレクトリ・**スキーマ**には、DIT 内のデータを組織する方法に関するすべての情報 (**オブジェクト・クラス**、**属性**、**一致規則**、構文などのメタデータ) が含まれています。ディレクトリ・スキーマはこの情報を、**サブエントリ**と呼ばれる特別なクラスのエントリに格納しま



す。Oracle Internet Directory は、LDAP バージョン 3 の規格に従って、subSchemaSubentry と呼ばれるサブエントリにスキーマ定義を保持します。

subSchemaSubentry を変更することによって新規のオブジェクト・クラスとオブジェクトを追加できます。ただし、Oracle Internet Directory ですでにサポートされているもの以外に、新規の一致規則や構文を追加することはできません。

**関連項目：**

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

## セキュリティ

Oracle Internet Directory には、不正アクセスから情報を保護する強力なメカニズムが多数用意されています。

この項では、次の項目について説明します。

- [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する方法
- [アクセス制御と認可](#)：ユーザーが権限を持つ情報のみを読み込みまたは更新することを保証する方法
- [データ整合性](#)：送信中にデータが変更されないことを保証する方法
- [データ・プライバシー](#)：送信中にデータが開示されないことを保証する方法
- [パスワード暗号化](#)：4 つの暗号化オプションのいずれかによって、ユーザー・パスワードの保護を保証する方法

認証

認証は、Directory Server が、そのディレクトリに接続しているユーザーの正確な識別情報を設定するプロセスです。LDAP セッションが ldap-bind 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。この識別情報は、認可 ID とも呼ばれます。

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認識されることを保証するために、Oracle Internet Directory には、次の 3 つの認証オプションが用意されています。それは、匿名、簡易および SSL の 3 つです。

匿名認証

ディレクトリをすべての人が使用できる場合は、ユーザーにディレクトリへの匿名ログインを許可できます。[匿名認証](#)を使用する場合、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できます。各匿名ユーザーは、匿名ユーザーに指定された権限すべてを使用できます。

簡易認証

この認証の場合、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 (DN) 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。[簡易認証](#) オプションでは、サーバーは、クライアントが送信した DN とパスワードが、ディレクトリに格納されている DN とパスワードと一致していることを検証します。

Secure Sockets Layer (SSL) を使用した認証

[SSL](#) は、ネットワーク接続を保護するための業界標準プロトコルです。信頼されている認証局によって検証された[証明書](#)を交換することによって認証を提供します。証明書は、その所有者の認証情報が正しいことを保証します。エンティティは、エンド・ユーザー、データベース、管理者、クライアントまたはサーバーになれます。[認証局](#)は、すべての関係機関によって高いレベルの信頼度を与えられた公開鍵の証明書を作成する機関です。

SSL は、3 つの認証モードで使用できます。

SSL モード	説明
認証なし	クライアントとサーバーのいずれも、他方に対して自己認証を行いません。証明書の送信または交換は行われません。この場合は、SSL 暗号化・復号化のみ使用されます。
サーバー認証	Directory Server のみ、クライアントに対して自己認証を行います。Directory Server 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。
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ます。クライアントとサーバーは、証明書を交換します。

**SSL のコンポーネント** SSL のコンポーネントは次のとおりです。

- **証明書**

証明書は、その所有者の認証情報が正しいこと、および公開鍵がその所有者に実際に属していることを保証します。証明書は、エンティティの公開鍵が信頼されている機関、つまり認証局（CA）によって署名されたときに有効となります。証明書には、所有者の名前、公開鍵、シリアル番号および有効期限が含まれています。証明書に関連付けられている権限に関する情報が含まれている場合もあります。さらに、証明書を発行した認証局の情報が含まれます。証明書は、有効期限が過ぎるまで、または取り消されるまで有効です。

- **認証局（CA）**

認証局は、他のエンティティが本物であることを証明する信頼性のある第三者機関です。認証局は、エンティティの識別情報を検証し、認証局の**秘密鍵**を使用して署名した証明書を発行します。

認証局が異なると、証明書発行時の身分証明の要件が異なる場合があります。たとえば、各認証局によって、ユーザーの運転免許証を調べる、証明書要求フォームが公証済みであることを要求する、証明書要求者の指紋を要求する、などの方法があります。認証局は、自身の公開鍵を含んだ自己証明書を公開しています。

各ネットワーク・エンティティには、信頼されている認証局の証明書リストがあります。別のエンティティと通信する前に、指定したエンティティは、このリストを使用して他のエンティティの証明書の署名が信頼されている認証局のものであることを検証します。ネットワークの各エンティティが取得する証明書は、同一の認証局のもので異なる認証局のものでかまいません。

- **Wallet**

**Wallet** は、**Trustpoint** と呼ばれる鍵、証明書および**信頼されている証明書**などで、これらは SSL で必要とされる認証データの格納と管理に使用される抽象的な概念です。Oracle 環境では、**X.509** バージョン 3 の証明書、秘密鍵および信頼されている証明書のリストを伴った Wallet が SSL を使用する各システムに用意されています。

**Oracle Wallet Manager** を使用して、セキュリティ管理者は、サーバー上のセキュリティ資格証明を管理します。Wallet の所有者は、クライアント上のセキュリティ資格証明を管理します。特に、Oracle Wallet Manager は次の内容を実行するために使用されます。

- **公開鍵と秘密鍵のペア**の生成および認証局に提出する証明書要求の作成
- エンティティ用の証明書のインストール
- エンティティ用の信頼されている証明書の構成

**関連項目：** Oracle Wallet Manager を使用した Wallet の管理方法の詳細は、**付録 C** を参照してください。

**SSL ハンドシェイク** 通信開始時に、クライアントと Directory Server は、次の 3 つの重要な手順を含んだ**ハンドシェイク**を実行します。

- クライアントとサーバーは、使用する Cipher Suite を確立します。**Cipher Suite** は、ネットワーク・ノード間でのメッセージ交換に使用される認証、暗号化およびデータ整合性アルゴリズムのセットです。SSL ハンドシェイク時に、2 つのノードは、メッセージの送受信に使用する Cipher Suite を調べるために交渉を行います。
- サーバーが、自身の証明書をクライアントに送信します。クライアントは、Directory Server の証明書が信頼されている認証局によって署名されていることを検証します。  
同様に、クライアント認証が要求された場合、クライアントは所有している証明書を Directory Server に送信します。Directory Server は、クライアントの証明書が信頼されている認証局によって署名されていることを検証します。
- クライアントと Directory Server は、**公開鍵暗号**を使用して鍵の元となるデータを交換し、この元データからそれぞれ**セッション・キー**を生成します。これ以降のすべてのクライアントと Directory Server 間の通信は、この 1 組のセッション鍵と取り決めた Cipher Suite を使用して、暗号化および復号化されます。

**関連項目：**

- データの整合性と暗号化の詳細は、2-11 ページの「**データ整合性：送信中にデータが変更されないことを保証する方法**」を参照してください。
- Oracle Internet Directory でサポートされている SSL Cipher Suite のリストは、8-2 ページの「**サポートされている Cipher Suite**」を参照してください。

**SSL と Oracle Internet Directory** クライアントと Directory Server 間の SSL 認証には、次の 3 つの基本ステップが含まれます。

1. ユーザーは、SSL ポート上の SSL を使用して、Directory Server への LDAP 接続を開始します（デフォルトの SSL ポートは 636 です）。
2. SSL は、クライアントと Directory Server 間のハンドシェイクを実行します。
3. ハンドシェイクが成功すると、Directory Server は、そのディレクトリにアクセスするために必要な認可をユーザーが所有していることを検証します。

**関連項目：**

- [第 8 章「Secure Sockets Layer \(SSL\) の管理」](#)
- アクセス制御ポリシーの設定方法は、[第 9 章「ディレクトリのアクセス制御の管理」](#)を参照してください。
- 証明書および Wallet の説明は、[付録 C「Oracle Wallet Manager の使用方法」](#)を参照してください。

## アクセス制御と認可

認可は、ユーザーが権限を持つ情報のみを読み込みまたは更新することを保証するプロセスです。ディレクトリ・セッション内でディレクトリ操作が行われると、Directory Server は、その操作の実行に必要な権限が（セッションに関連付けられた認可 ID によって識別された）ユーザーに与えられていることを確認します。権限が与えられていない場合、操作は実行できません。この方法によって、Directory Server は、ディレクトリ・ユーザーによる不正操作からディレクトリ・データを保護しています。この方法はアクセス制御と呼ばれます。

アクセス制御項目（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。

ACI は、ユーザー変更可能な操作属性として、Oracle Internet Directory に格納されています。通常、アクセス制御リスト（ACL）と呼ばれるこの ACI 属性値のリストは、ディレクトリ・オブジェクトと関連付けられています。このリストにある属性値によって、そのディレクトリ・オブジェクトに対するアクセス・ポリシーが管理されます。

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、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。これらの個々のポリシーのコンポーネントは、ACI ディレクティブまたは [ACI](#) と呼ばれ、その書式は ACI ディレクティブ書式と呼ばれます。

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](#)内の下位エントリすべてに適用されるように設定できます。このようなアクセス制御ポリシーが適用される開始地点は、[Access Control Policy Point \(ACP\)](#) と呼ばれます。

**関連項目：**

- アクセス制御ポリシーの設定方法は、[第 9 章「ディレクトリのアクセス制御の管理」](#)を参照してください。
- ACI ディレクティブを正しく書式化する方法は、[付録 D「アクセス制御ディレクティブ書式の使用法」](#)を参照してください。

## データ整合性

Oracle Internet Directory は、SSL を使用して、送信時にデータの変更、削除または再現が行われないことを保証します。この SSL 機能は、暗号方式の保護メッセージ・ダイジェストを、**MD5** アルゴリズムまたは **Secure Hash Algorithm (SHA)** を使用する暗号チェックサムを使用して生成し、ネットワークを介して送信する各パケットに組み込みます。

## データ・プライバシー

Oracle Internet Directory は、Secure Sockets Layer (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** の変形で、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、シークレット・キーを事前に処理して、40 ビットの有効**キー**を提供します。DES40 は、米国およびカナダ以外で、DES ベースの暗号化アルゴリズムの使用を希望する顧客を対象に設計されています。この機能によって、顧客は地理的条件に関係なく使用するアルゴリズムを選択できます。

- RC4\_40

Oracle は、他の Oracle 製品が使用できる事実上すべての地域に対して、鍵のサイズが、40 ビットの RC4 データ暗号化アルゴリズムを輸出するライセンスを取得しています。この結果、国際企業は、高速暗号化を使用して事業全体を保護することが可能になります。

**関連項目：** SSL の詳細は、第 8 章「[Secure Sockets Layer \(SSL\) の管理](#)」を参照してください。

## パスワード暗号化

インストール時には、パスワードの暗号化スキームを設定する必要がありました。その初期構成を変更するには、Oracle Directory Manager または ldapmodify のいずれかを使用します。パスワード暗号化のタイプを変更するには、スーパー・ユーザーである必要があります。

パスワードを暗号化するために、Oracle Internet Directory では MD4 アルゴリズムをデフォルトとして使用します。MD4 は、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。このデフォルトは、次のうちのいずれかに変更できます。

- No Encryption
- MD5 - MD4 の改善された、より複合的なバージョン。

- SHA - Secure Hash Algorithm。MD5 よりも長い 160 ビットのハッシュを生成します。このアルゴリズムは MD5 よりも若干遅くなりますが、メッセージ・ダイジェスト値が大きくなることで、総当たり攻撃や反転攻撃に対してより強力に保護できます。
- UNIX Crypt - UNIX の暗号化アルゴリズム。

指定した値は、**Root DSE** の `orclCryptoScheme` 属性に格納されます。この属性は単一値です。

Directory Server への認証時、ユーザーはパスワードをクリア・テキストで入力します。サーバーはそのパスワードを指定された暗号化アルゴリズムでハッシュし、それを `userPassword` 属性内のハッシュされたパスワードに照合して検証します。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、サーバーはユーザーに無効な資格証明というエラー・メッセージを送信します。

**関連項目：** 5-16 ページ「パスワード暗号化の管理」

## 各国語サポート

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。この規格に従って、Oracle Internet Directory は、Oracle NLS 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 **アプリケーション・プログラム・インタフェース** (API) がいくつか含まれていますが、Oracle Internet Directory 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。

NLS では、シングルスバイト文字とマルチバイト文字の両方が使用されます。シングルスバイト文字は、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ス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、中国語 (簡体字) はマルチバイト文字を使用します。中国語 (簡体字) のディレクトリ・エントリは次のようになります。

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

属性値は、中国語 (簡体字) キャラクタ・セットの文字列に相当します。

Oracle Internet Directory の主なコンポーネントである OID モニター (OIDMON)、OID 制御ユーティリティ (OIDCTL)、Oracle Directory Server (OIDLDAPD) および Oracle Directory Replication Server (OIDREPLD) は、常にデフォルトで UTF-8 キャラクタ・セットを使用します。

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 **UCS2**) を使用します。Java では、UCS2 が文字 (英文字を含む) を

処理する最も簡単な方法です。Java クライアントは、標準的な Java パッケージを使用して UCS2 と UTF-8 を相互に変換します。この変換機能によって、Oracle Directory Manager は、UTF-8 を使用する LDAP バージョン 3 のプロトコルを処理できます。

**関連項目：**

- Oracle Internet Directory の主なコンポーネントの詳細は、2-18 ページの「[Oracle Internet Directory のアーキテクチャ](#)」を参照してください。
- Oracle Internet Directory の NLS の使用方法は、[第 12 章「各国語サポート（NLS）の管理」](#)を参照してください。
- NLS の詳細は、『Oracle8i NLS ガイド』を参照してください。

## Oracle Internet Directory のアーキテクチャ

この項では、次の項目について説明します。

- [Oracle Internet Directory のノード](#)
- [Oracle Directory（LDAP）Server インスタンス](#)
- [構成設定エントリ](#)
- [例：Oracle Internet Directory の動作](#)

## Oracle Internet Directory のノード

[図 2-4](#) は、単一ノード上で稼働している様々な Directory Server コンポーネントと、それらの関連を示しています。

Oracle データベース・サーバーと次のものとの接続には、いずれも Net8 が使用されます。

- [OID 制御ユーティリティ](#)
- LDAP サーバー・インスタンス 1 非 SSL ポート 389
- LDAP サーバー・インスタンス 2 SSL 使用可能ポート 636
- [OID モニター](#)

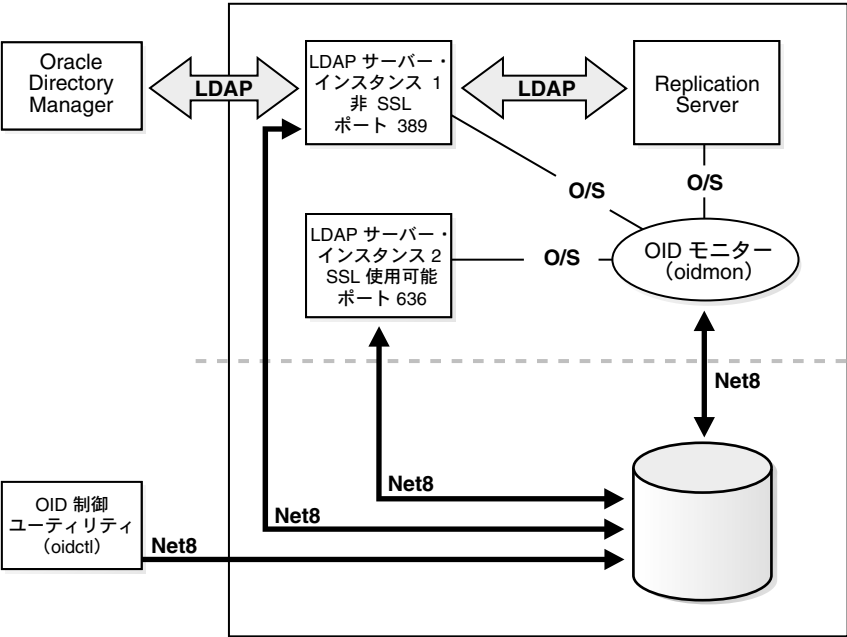
LDAP は、LDAP サーバー・インスタンス 1 非 SSL ポート 389 と次のものとの間の接続に使用されます。

- Oracle Directory Manager
- Oracle Directory Replication Server

2 つの LDAP サーバー・インスタンスと Replication Server は、オペレーティング・システム経由で OID モニターに接続します。



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



**注意：** 図 2-4 のデータベースは、Directory Server プロセスと同じノードにあります。しかし、データベースとの接続はすべて、**Oracle コール・インタフェース**と **Net8** を介するため、別のサーバー上のデータベースを使用できます。

Oracle Internet Directory のノード (図 2-4) には、次の主なコンポーネントがあります。

コンポーネント	説明
LDAP サーバー・インスタンス	Oracle Directory Server インスタンスとも呼ばれます。特定の TCP/IP ポート番号でリスニングする単一の Oracle Internet Directory ディスパッチャ・プロセスを通して、サービス・ディレクトリの要求に応答します。それぞれ異なるポートでリスニングする複数の LDAP サーバー・インスタンスが 1 つのノード上に存在する場合があるため、Oracle Internet Directory のディスパッチャ・プロセスとサーバー・プロセスは複数のスレッドを使用します。

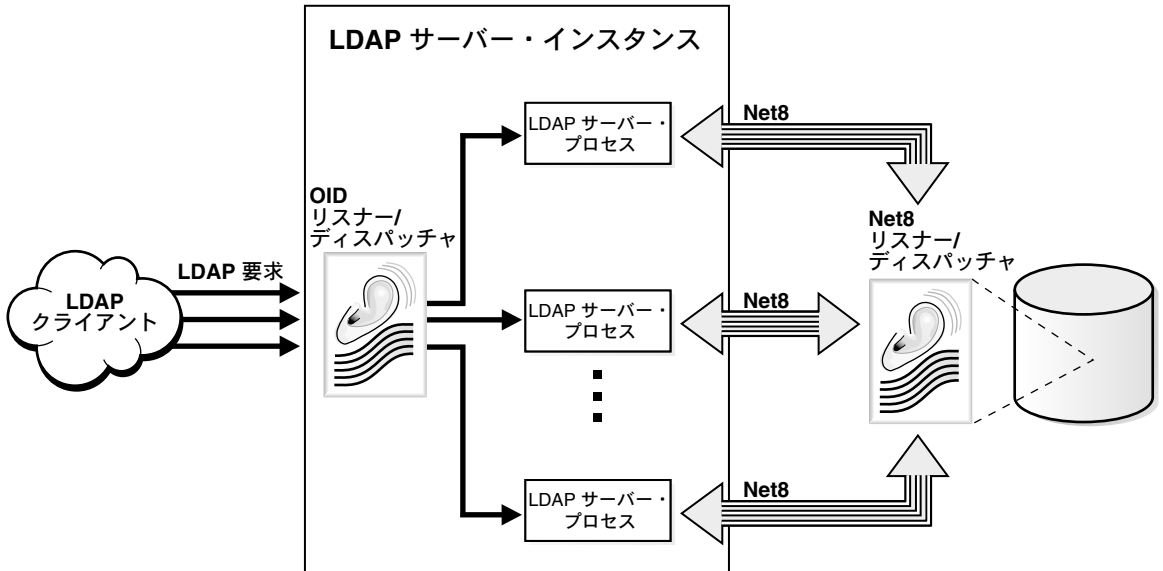
コンポーネント	説明
Replication Server	Oracle Directory Replication Server と呼ばれます。Oracle Internet Directory システム内のレプリケート・サーバーの変更を追跡し、その内容を送信します。1 つのノード上に設定できる Replication Server は 1 つのみです。Replication Server をインストールして使用するかどうかは選択できます。
Oracle8i データベース	ディレクトリ・データを格納します。データベースをこのディレクトリ専用を使用することをお勧めします。データベースは、サーバーと同じノードにも別のノードにも常駐できます。
OID モニター (OIDMON)	<p>LDAP のサーバー・プロセスを開始、モニターおよび終了します。Replication Server をインストールすると、OID モニターがこれを制御します。OID 制御ユーティリティ (OIDCTL) を使用して Directory Server インスタンスを起動または停止するコマンドを発行すると、そのコマンドはこのプロセスによって解釈されます。</p> <p>OID モニターは、管理者が OID 制御ユーティリティで行う LDAP サーバー・インスタンスの起動と停止の要求を処理します。また、サーバーをモニターし、例外的な理由で実行が停止した場合に再起動させます。</p> <p>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。Directory Server インスタンスが停止すると、レジストリ・エントリおよびその特定のサーバー・インスタンスに対応しているデータをプロセス表から削除します。OID モニターが異常終了したサーバーを再起動する場合は、そのサーバーの起動時間でレジストリ・エントリを更新します。</p> <p>OID モニターのアクティビティはすべて、ファイル <code>ORACLE_HOME/ldap/log/oidmon.log</code> に記録されます。このファイルは、Oracle Internet Directory サーバーのファイル・システムにあります。</p> <p>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。</p>
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 Directory Server 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 Directory Replication Server は LDAP を使用して、Oracle Directory (LDAP) Server 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/Net8 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 Directory (LDAP) Server と通信します。

## Oracle Directory (LDAP) Server インスタンス

各 Oracle Directory (LDAP) Server インスタンスは、[図 2-5](#) のようになります。

図 2-5 LDAP サーバー・インスタンスのアーキテクチャ



LDAP クライアントは LDAP 要求を、そのポートで LDAP コマンドをリスニングしている Oracle Internet Directory リスナー / ディスパッチャ・プロセスに送信します。

OID リスナー / ディスパッチャは LDAP Directory Server を起動し、LDAP Directory Server はサーバー・プロセスを作成します。マルチ・サーバー・プロセスによって、Oracle Internet Directory はマルチ・プロセッサ・システムを利用できます。作成されるサーバー・プロセス数は、構成パラメータ (ORCLSERVERPROCS) で決まります。デフォルトは 1 です。各操作のワーカー・スレッドが、それぞれクライアント要求を処理します。

各サーバー・プロセスからのデータベース接続数は、構成パラメータ (ORCLMAXCC) で決定された最大数まで、必要に応じて増加します。このパラメータのデフォルト値は 10 です。サーバー・プロセスはデータ・サーバーと Net8 経由で通信します。Net8 リスナー / ディスパッチャは、Oracle データ・サーバーに要求を中継します。

## 構成設定エントリ

各 Oracle Directory Server インスタンスの構成パラメータは、構成設定エントリ (configset) と呼ばれるディレクトリ・エントリに格納されます。構成設定エントリは、Directory Server の特定インスタンスに関する構成パラメータを保持しています。管理者が

OID 制御ユーティリティを使用してサーバーのインスタンスを起動すると、そのコマンドにこの configset の 1 つへの参照が含まれ、その中の情報が使用されます。

Oracle Directory Server 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、Directory Server はすぐに実行できます。特定のパラメータを変更した新しい構成設定エントリを必要に応じて追加することによって、カスタマイズされた構成設定エントリを作成できます。このエントリを表示、追加および変更するには、**Oracle Directory Manager** または該当するコマンドライン・ツールを使用します。

**関連項目：**

- 5-2 ページ「サーバーの構成設定エントリの管理」
- 構成設定エントリの属性のリストは、E-4 ページの「構成設定エントリの属性」を参照してください。

## 例：Oracle Internet Directory の動作

すべての概念の紹介を、以上で終わります。次の例は、Oracle Internet Directory が検索要求をどのように処理するかを示しています。

1. ユーザーまたはクライアントが検索要求を入力します。検索条件は、次の 1 つ以上のオプションによって決まります。
  - SSL: クライアントとサーバーは、SSL の暗号化と認証または SSL の暗号化のみを使用するセッションを確立できます。SSL が使用されていない場合、クライアントのメッセージは平文で送信されます。
  - ユーザーのタイプ: ユーザーは、特定のユーザーまたは匿名ユーザーのいずれかでディレクトリにシーク・アクセスできます。要求する機能の実行に必要な権限を持っているかどうかによって、2 つのタイプのいずれかでアクセスします。
  - フィルタ: ユーザーは、1 つ以上の検索フィルタを使用して検索条件を絞り込むことができます。検索フィルタには、ブール条件 and、or、not の他に、greater than、equal to、less than などの演算子を使用します。
2. ユーザーまたはクライアントが Oracle Directory Manager を使用してコマンドを発行すると、Oracle Directory Manager は Java ネイティブ・インタフェースで問合せ関数を起動し、次に Java ネイティブ・インタフェースが C API で関数を起動します。ユーザーまたはクライアントがコマンドライン・ツールを使用した場合は、そのツールが直接 C API で C 関数をコールします。
3. C API は、LDAP プロトコルを使用して、ディレクトリへの接続要求を Directory Server インスタンスに送信します。
4. Directory Server がユーザーを認証します。このプロセスはバインドと呼ばれます。Directory Server は、アクセス制御リスト (ACL) もチェックして、そのユーザーが、要求した検索の実行を許可されているかどうかを検証します。

5. Directory Server は、LDAP からの検索要求を Oracle コール・インタフェース (OCI) および Net8 に変換し、Oracle8i データベースに送信します。
6. Oracle8i データベースは、情報を取得し、Directory Server、次に C API、最後にクライアントと連鎖的に戻します。

## 分散ディレクトリ：概要

オンライン・ディレクトリは論理的に集中管理されていますが、物理的にはそのデータを複数のサーバーに分散できます。データを物理的に分散すると、1 つのサーバーの作業が削減され、ディレクトリに多数のエントリを格納できるようになります。

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

### 関連項目：

- 2-23 ページ「[分散ディレクトリ：レプリケーション](#)」
- 2-38 ページ「[分散ディレクトリ：パーティション化](#)」

## 分散ディレクトリ：レプリケーション

レプリケーションはディレクトリ情報を分散する方法の 1 つです。問合せを処理するサーバーの数を増やすことによって、パフォーマンスが向上します。また、ある箇所で発生した障害から派生するリスクを排除できるため信頼性が向上します。

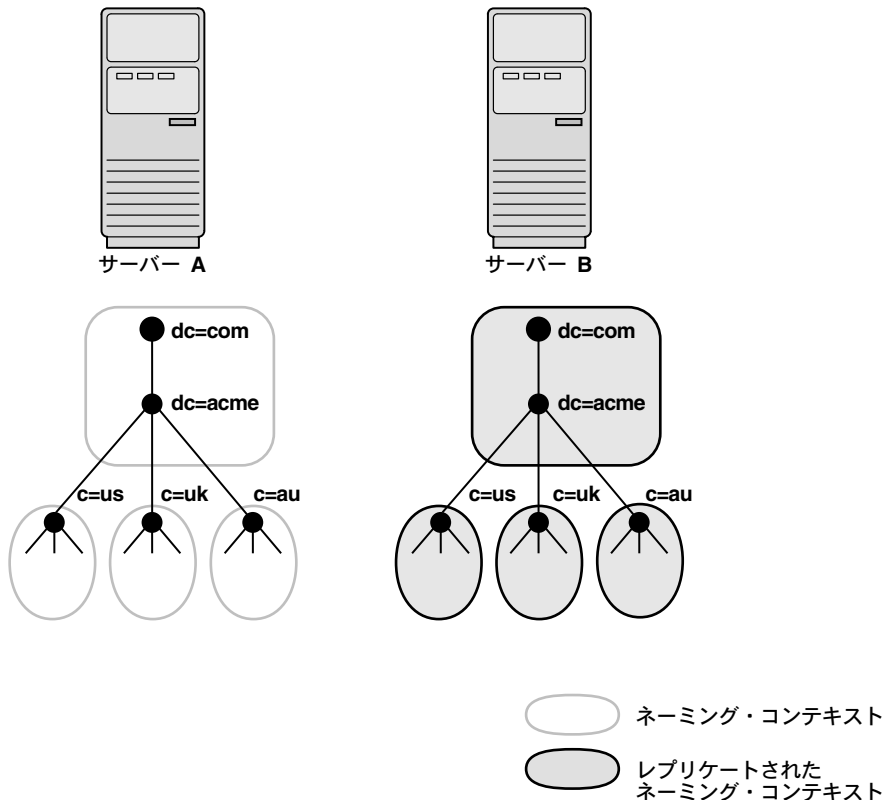
サーバー内に格納されているネーミング・コンテキストの各コピーは、レプリカと呼ばれます。Directory Server には、読取り専用レプリカと更新可能レプリカの両方を保持できます。

更新可能レプリカを保持するサーバーは、サプライヤと呼ばれます。このレプリカを変更すると、コンシューマと呼ばれる他のサーバーに伝播されます。

管理者は、Replication Server がコンシューマに対して変更内容の適用を試みる回数を指定します。指定した回数に到達すると、Replication Server 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。

図 2-6 は、レプリケート・ディレクトリを示しています。

図 2-6 レプリケート・ディレクトリ



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

また、ディレクトリ・レプリケーションのインターネット規格はまだありませんが、IETF がこれに類する規格を開発中です。Oracle Internet Directory のレプリケーションは、ディレクトリ変更情報を[変更ログ](#)に記録する IETF 規格案に準拠しています。

**関連項目：** 変更ログの詳細は、2-27 ページの「[レプリケーション・アーキテクチャ](#)」を参照してください。

この項では、次の項目について説明します。

- [ディレクトリ・レプリケーション・グループとレプリケーション承諾](#)
- [アドバンスト・レプリケーション](#)
- [レプリケーション・アーキテクチャ](#)
- [変更ログの削除](#)
- [レプリケーションにおける競合の解消](#)
- [レプリケーションの動作：概要](#)
- [レプリケーションの動作：詳細説明](#)

**関連項目：** レプリケーションの詳細は、[第 10 章「ディレクトリ・レプリケーションの管理」](#)を参照してください。

## ディレクトリ・レプリケーション・グループとレプリケーション承諾

指定したネーミング・コンテキストのレプリケーションの対象となる Directory Server のセットを、ディレクトリ・レプリケーション・グループ (DRG) と呼びます。レプリケーション承諾と呼ばれる特別なディレクトリ・エントリには、DRG 内の Directory Server 間におけるレプリケーションの関係が記述されています。

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

[図 2-7](#) に示されたディレクトリ・レプリケーション・グループでは、レプリケーション承諾内の 3 つのノードが、互に更新内容を共有しています。

図 2-7 ディレクトリ・レプリケーション・グループ

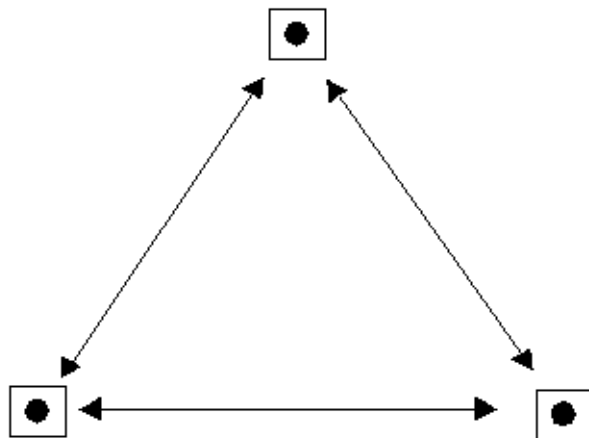


図 2-7 にある各黒丸は、Oracle Internet Directory のノードを表しています。承諾は各ノードで同一ですが、ローカル・Directory Server 上にパーティション化されたネーミング・コンテキストなどのローカル・オプションは異なります。各ノードのレプリケーション承諾には、変更内容を配布および受信する他のノードがすべてリストされています。

**関連項目：** レプリケーション承諾の構成方法は、10-10 ページの「[タスク 5: レプリケーションの構成](#)」を参照してください。

## アドバンスト・レプリケーション

レプリケーション承諾がなされたノード間における更新情報の移送は、Oracle8i で使用可能なアドバンスト・レプリケーションによって管理されます。この機能を使用すると、2 つの Oracle データベース間で、データベースの表を継続的に同期化できます。

アドバンスト・レプリケーションは、ローカルの変更内容を蓄積し、コンシューマ・サーバーに定期的にまとめて伝播します。コンシューマ Replication Server は、リモートの変更内容をローカルの Directory Server に適用し、ローカル・ストアから適用済みのリモートの変更内容を削除します。

アドバンスト・レプリケーション環境では、システム内のどこにあるディレクトリ表に対しても読み込みおよび更新アクセスが可能です。一般的なアドバンスト・レプリケーション構成では、非同期データ伝播方式の行レベル・レプリケーションが使用されます。

アドバンスト・レプリケーションは、実証済みのネットワーク・トランスを提供し、そのデータ移送は、Oracle Enterprise Manager で制御およびモニターできます。このような管理機能によって、データ移送のスケジュール方法に高度な柔軟性を与えることができます。



**関連項目:** アドバンスド・レプリケーションの詳細は、『Oracle® レプリケーション・ガイド』を参照してください。

## レプリケーション・アーキテクチャ

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

レプリケーションを構成する場合は、レプリケーション・グループ内で変更を共有するノードを指定します。レプリケーションの基本アーキテクチャは、レプリケーション環境に導入するノードの数に関係なく一定です。ローカルの変更内容はリモート・ノードに配布されてから、Replication Server 処理によって適用されます。リモート・ノード上で変更を適用するために、クライアントとして機能する Replication Server は、Directory Server にコマンドを送信し、Directory Server がそのコマンドを実行します。

**関連項目:** レプリケーションの構成方法は、10-10 ページの「[タスク 5: レプリケーションの構成](#)」を参照してください。

## 変更ログの削除

Oracle Internet Directory の変更ログの削除は、次の 2 つの方法に従って発生します。

変更番号ベース	これはデフォルトの方法です。Replication Server は、すでに DRG 内のすべてのノードに適用された変更内容を削除します。
時間ベース	この方法を実行すると、変更番号ベースの削除を補強できます。この付加的な方法を使用するには、変更ログ・オブジェクトの存続期間を時間単位で指定するパラメータを設定します。たとえば、24 時間経過した変更ログ・オブジェクトをすべて削除するように、このパラメータを設定できます。変更ログが大きくなりすぎるのを防ぐには、この方法を使用してください。

**関連項目:**

- 10-11 ページ「[Oracle Directory Replication Server のパラメータ](#)」
- 10-12 ページ「[Oracle Directory Manager を使用したレプリケーションの構成パラメータの表示と変更](#)」
- 10-13 ページ「[コマンドライン・ツールを使用したレプリケーションの構成パラメータの変更](#)」

## レプリケーションにおける競合の解消

マルチマスター・レプリケーションを使用すると、複数の Directory Server を更新できます。競合は、Oracle Directory Replication Server がサプライヤからコンシューマにリモートの変更を適用しようとしてなんらかの理由で失敗すると、必ず発生します。

次の 4 種類の LDAP 操作が競合を引き起こす可能性があります。

- 追加
- 削除
- 変更
- RDN または DN 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

**エントリ・レベルの競合** エントリ・レベルの競合は、Oracle Directory Replication Server がコンシューマに変更を適用するときに発生します。そのような変更には、コンシューマに対する次のタイプの変更のいずれかが該当します。

- すでに存在しているエントリの追加
- 存在していないエントリの削除
- 存在していないエントリの変更
- 存在していない DN に対する DN 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
- エントリの不在

存在すべきではないエントリが存在している場合は、次の理由が考えられます。

- そのエントリは以前に追加済
- そのエントリは最近 DN の変更操作あり

**属性レベルの競合** 属性レベルの競合は、2つのディレクトリが、同じ属性を異なる値で異なる時間に更新している場合に発生します。属性が単一値の場合、レプリケーション・プロセスは、競合に含まれている変更のタイムスタンプを検証して、競合を解消します。

## 競合の一般的な原因

競合は通常、広域ネットワーク上で時折発生する通信速度の低下や送信エラーが原因で生ずる変更の時間的なずれが原因です。また、過去に生じた不整合が、タイミに解消されていない場合に、引き続き競合が発生する可能性があります。

## 競合の自動解消

Oracle Directory Replication Server 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、変更競合のフラグを付け、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。Oracle Directory Replication Server 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。

---

## レプリケーションの動作：概要

図 2-8 は、サプライヤ側およびコンシューマ側のレプリケーション・プロセスの一般的な概要を表しています。この図は、次の内容を示しています。

### サプライヤ側の手順

1. LDAP クライアントがディレクトリ変更を発行すると、LDAP サーバーは変更ログ・オブジェクト・ストアに変更ログ・オブジェクトを生成します。
2. スケジュールされた時間に、Replication Server はコンシューマ側に反映する変更ログの処理スレッドを起動し、変更ログ・オブジェクトを変更ログ表の行（変更エントリなど）に変換します。

3. 変更エントリが変更ログ表に挿入され、コミットされると、アドバンスト・レプリケーションはその変更内容を遅延トランザクション・キューへ即座にコピーします。
4. スケジュールされた間隔が経過すると、アドバンスト・レプリケーションは、遅延トランザクション・キューから保留トランザクションを抽出し、ネットワークを介してコンシューマの変更ログ表に送信します。

### コンシューマ側の手順

1. Replication Server は、スケジュールされたレプリケーション・サイクルに従って、各サプライヤの変更ログの処理スレッドを起動します。
2. 変更ログの処理スレッドは、サプライヤからコンシューマに適用された最終変更を変更ステータス表で調べます。
3. 次に、変更ログ表から新規変更をすべてフェッチして、LDAP サーバーに適用します。
4. 変更ログの処理が完了すると、変更ログの処理スレッドは終了前に、変更ステータス表を更新してサプライヤから適用された最終変更を記録します。
5. アドバンスト・レプリケーションは、変更ステータスの更新内容を遅延トランザクション・キューにコピーします。
6. スケジュールされたアドバンスト・レプリケーションのレプリケーションの間隔が経過すると、アドバンスト・レプリケーションは遅延トランザクション・キューから保留変更ステータス更新を抽出し、サプライヤの変更ステータス表に送信します。

図 2-8 は、レプリケーション・プロセスを図示したものです。

図 2-8 アドバンスド・レプリケーション・ベースのレプリケーション・アーキテクチャの概要

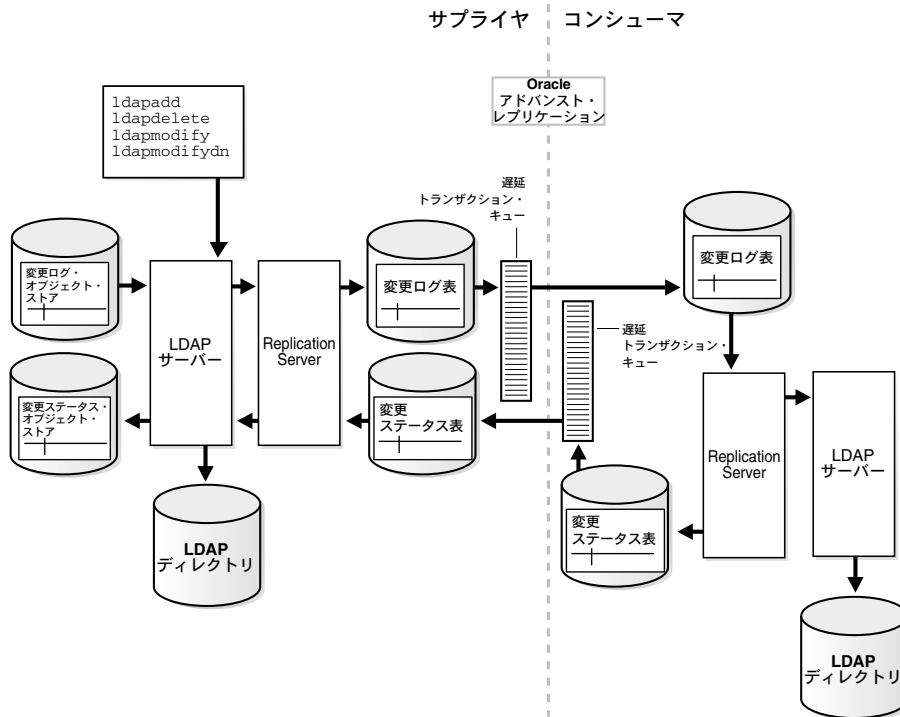


図 2-8 ではサブライヤとコンシューマの役割が分割されていますが、実際のマルチマスター・レプリケーション環境においては、各 Directory Server がサブライヤであり、コンシューマでもあります。このような環境では、適用済のエントリや候補の変更に従って削除されたエントリのページが定期的に発生します。ローカルの変更ログ表にあるリモート変更の記録は、その変更がローカルで適用されると、ガベージ・コレクション・スレッドによってページされます。ローカルの変更ログ表にあるローカル変更の記録は、その変更がすべてのコンシューマに配布されると、ガベージ・コレクション・スレッドによってページされます。

**関連項目：**

- Replication Server によるエントリの追加、削除、変更、および DN や RDN の変更方法の詳細は、2-29 ページの「[レプリケーションの動作：概要](#)」を参照してください。
- エントリを追加、削除および変更するとき、ならびに DN や RDN を変更するときの Replication Server による競合の解消方法の詳細は、2-28 ページの「[レプリケーションにおける競合の解消](#)」を参照してください。

## レプリケーションの動作：詳細説明

この項では、自動レプリケーション・プロセスによるエントリの追加、削除および変更、ならびに識別名（DN）と相対識別名（RDN）の変更方法について、さらに詳細に紹介します。

### レプリケーション・プロセスがコンシューマに新規エントリを追加する動作

Oracle Directory Replication Server は、コンシューマへの新規エントリの追加に成功すると、次の変更アプリケーション・プロセスを実行します。

1. Oracle Directory Replication Server は、コンシューマ内でターゲット・エントリの親の DN を探します。具体的には、その親の DN 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、Oracle Directory Replication Server は新規エントリの DN 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、変更エントリをページ・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

Oracle Directory Replication Server は新しい変更エントリをリトライ・キューに入れ、再試行回数を指定の最大値に設定して変更アプリケーション・プロセスを繰り返します。

#### 2 回目以降最終試行前までの試行で変更エントリが正常に適用されなかった場合

Oracle Directory Replication Server は変更エントリをリトライ・キューに保持したまま、再試行回数を減らして変更アプリケーション・プロセスを繰り返します。

#### 最終試行で変更エントリが正常に適用されなかった場合

Oracle Directory Replication Server は、新規エントリが既存エントリと同一でないかどうかをチェックします。

### 変更エントリが同一エントリの場合

Oracle Directory Replication Server は、次の競合の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ページ・キューに入ります。

ターゲット・エントリを使用すると、変更エントリがページ・キューに入ります。

### 変更エントリが同一エントリではない場合

Oracle Directory Replication Server は、変更エントリを管理者操作キューに入れ、`orclHIQSchedule` パラメータで指定した間隔で変更アプリケーション・プロセスを繰り返します。

### 変更エントリが管理者操作キューに入れられた後正常に適用されない場合

Oracle Directory Replication Server は、このキューに変更を保持したまま、指定した間隔で変更アプリケーション・プロセスを繰り返しながら管理者によるアクションを待ちます。管理者は、OID 調停ツールおよび管理者操作キュー操作ツールを使用して競合を解消できます。

## レプリケーション・プロセスがエントリを削除する動作

Oracle Directory Replication Server は、コンシューマからエントリを削除すると、次の変更アプリケーション・プロセスを実行します。

1. Oracle Directory Replication Server 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、Oracle Directory Replication Server はそのエントリを削除します。次に、変更エントリをページ・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

Oracle Directory Replication Server は変更エントリをリトライ・キューに入れ、再試行回数を指定の最大値に設定して変更アプリケーション・プロセスを繰り返します。

### 2 回目以降最終試行前までの試行で変更エントリが正常に適用されなかった場合

Oracle Directory Replication Server は変更エントリをリトライ・キューに保持したまま、再試行回数を減らして変更アプリケーション・プロセスを繰り返します。

### 最終試行で変更エントリが正常に適用されなかった場合

Oracle Directory Replication Server は、変更エントリを管理者操作キューに入れ、指定した間隔で変更アプリケーション・プロセスを繰り返します。

### 変更エントリが管理者操作キューに入れられた後正常に適用されない場合

Oracle Directory Replication Server は、このキューに変更エントリを保持したまま、指定した間隔で変更アプリケーション・プロセスを繰り返しながら、管理者によるアクションを待ちます。管理者は、OID 調停ツールおよび管理者操作キュー操作ツールを使用して競合を解消できます。

## レプリケーション・プロセスがエントリを変更する動作

Oracle Directory Replication Server は、コンシューマのエントリを変更すると、次の変更アプリケーション・プロセスを実行します。

1. Oracle Directory Replication Server 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、Oracle Directory Replication Server 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. 次に、Oracle Directory Replication Server は、次の競合の解消規則を適用します。
  - a. 変更時間が最新のエントリを使用します。
  - b. 属性のバージョンが最新のエントリを使用します。
  - 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. Oracle Directory Replication Server は、フィルタ処理済みの変更を適用し、変更エントリをページ・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

Oracle Directory Replication Server は変更エントリをリトライ・キューに入れ、再試行回数を指定の最大値に設定して変更アプリケーション・プロセスを繰り返します。

### 2 回目以降最終試行前までの試行で変更エントリが正常に適用されなかった場合

Oracle Directory Replication Server は変更エントリをリトライ・キューに保持したまま、再試行回数を減らして変更アプリケーション・プロセスを繰り返します。



**最終試行で変更エントリが正常に適用されなかった場合**

Oracle Directory Replication Server は、変更エントリを管理者操作キューに入れ、指定した間隔で変更アプリケーション・プロセスを繰り返します。

**変更エントリが管理者操作キューに入れられた後正常に適用されない場合**

Oracle Directory Replication Server は、このキューに変更エントリを保持したまま、指定した間隔で変更アプリケーション・プロセスを繰り返しながら管理者によるアクションを待ちます。管理者は、OID 調停ツールおよび管理者操作キュー操作ツールを使用して競合を解消できます。

**レプリケーション・プロセスが相対識別名を変更する動作**

Oracle Directory Replication Server は、コンシューマのエントリの RDN を変更すると、次の変更アプリケーション・プロセスを実行します。

1. Oracle Directory Replication Server 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 (DN) 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、Oracle Directory Replication Server はそのエントリの RDN を変更し、変更エントリをページ・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**

Oracle Directory Replication Server は変更エントリをリトライ・キューに入れ、再試行回数を指定の最大値に設定して変更アプリケーション・プロセスを繰り返します。

**2 回目以降最終試行前までの試行で変更エントリが正常に適用されなかった場合**

Oracle Directory Replication Server は変更エントリをリトライ・キューに保持したまま、再試行回数を減らして変更アプリケーション・プロセスを繰り返します。

**最終試行で変更エントリが正常に適用されなかった場合**

Oracle Directory Replication Server は、変更エントリを管理者操作キューに入れ、変更がそのターゲット・エントリと同一でないかどうかをチェックします。

**変更エントリが同一エントリの場合**

Oracle Directory Replication Server は、次の競合の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ページ・キューに入ります。

ターゲット・エントリを使用すると、変更エントリがページ・キューに入ります。

### 変更エントリが同一エントリではない場合

Oracle Directory Replication Server は、変更エントリを管理者操作キューに入れ、指定した間隔で変更アプリケーション・プロセスを繰り返します。

### 変更エントリが管理者操作キューに入れられた後正常に適用されない場合

Oracle Directory Replication Server は、このキューに変更エントリを保持したまま、指定した間隔で変更アプリケーション・プロセスを繰り返しながら、管理者によるアクションを待ちます。管理者は、OID 調停ツールおよび管理者操作キュー操作ツールを使用して競合を解消できます。

## レプリケーション・プロセスが識別名を変更する動作

Oracle Directory Replication Server は、コンシューマのエントリの DN を変更すると、次の変更アプリケーション・プロセスを実行します。

1. Oracle Directory Replication Server 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 (DN) を探します。

Oracle Directory Replication Server 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 DN も探します。

2. ターゲット・エントリの DN と親の DN の両方がコンシューマ内にある場合、Oracle Directory Replication Server はそのエントリの DN を変更し、変更エントリをページ・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

Oracle Directory Replication Server は変更エントリをリトライ・キューに入れ、再試行回数を指定の最大値に設定して変更アプリケーション・プロセスを繰り返します。

### 2 回目以降最終試行前までの試行で変更エントリが正常に適用されなかった場合

Oracle Directory Replication Server は変更エントリをリトライ・キューに保持したまま、再試行回数を減らして変更アプリケーション・プロセスを繰り返します。

### 最終試行で変更エントリが正常に適用されなかった場合

Oracle Directory Replication Server は、変更エントリを管理者操作キューに入れ、変更がそのターゲット・エントリと同一でないかどうかをチェックします。

### 変更エントリが同一エントリの場合

Oracle Directory Replication Server は、次の競合の解消規則を適用します。

- \* 作成タイム・スタンプが古い方のエントリを使用します。
- \* 両方のエントリの作成タイム・スタンプが同じ場合は、GUID の小さい方のエントリを使用します。

変更エントリを使用すると、ターゲット・エントリは削除されて、変更エントリが適用されパージ・キューに入ります。

ターゲット・エントリを使用すると、変更エントリがパージ・キューに入ります。

#### **変更エントリが同一エントリではない場合**

Oracle Directory Replication Server は、変更エントリを管理者操作キューに入れ、指定した間隔で変更アプリケーション・プロセスを繰り返します。

#### **変更エントリが管理者操作キューに入れられた後正常に適用されない場合**

Oracle Directory Replication Server は、このキューに変更エントリを保持したまま、指定した間隔で変更アプリケーション・プロセスを繰り返しながら管理者によるアクションを待ちます。管理者は、OID 調停ツールおよび管理者操作キュー操作ツールを使用して競合を解消できます。

## 分散ディレクトリ：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。図 2-9 は、別々のサーバーにいくつかのネーミング・コンテキストが常駐している、パーティション化されたディレクトリを示しています。

図 2-9 パーティション化されたディレクトリ

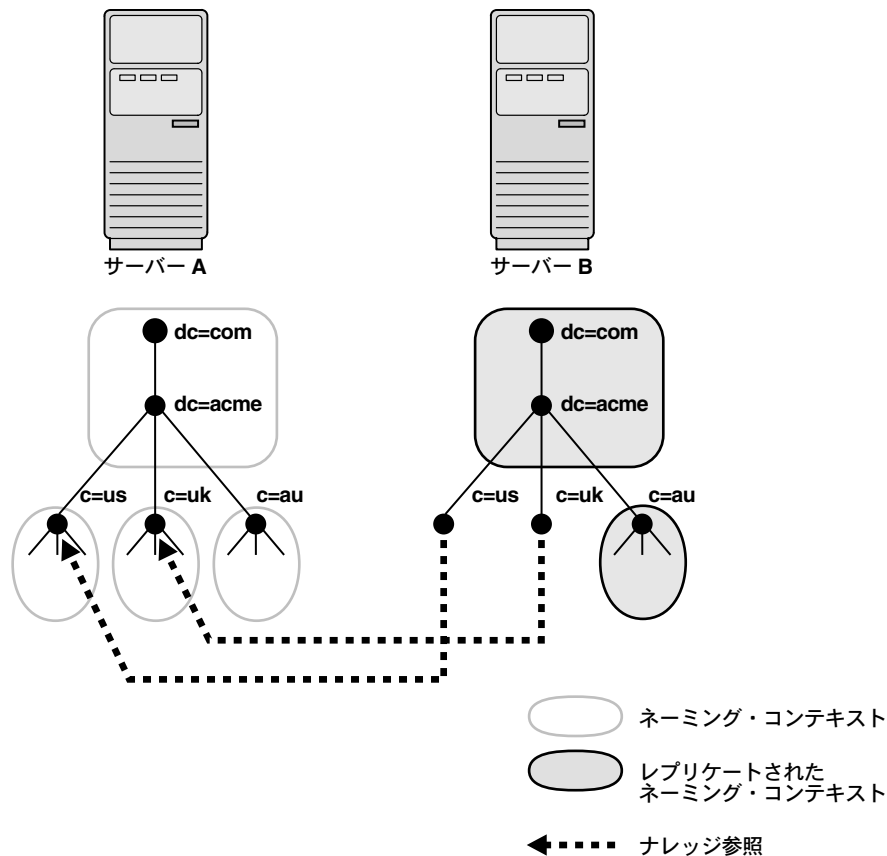


図 2-9 では、サーバー A に次の 4 つのネーミング・コンテキストが常駐しています。

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

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

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

ディレクトリは、サーバー B に要求した情報がサーバー A に常駐している場合に、**ナレッジ参照** (参照とも呼ばれます) を使用してその情報を検索します。

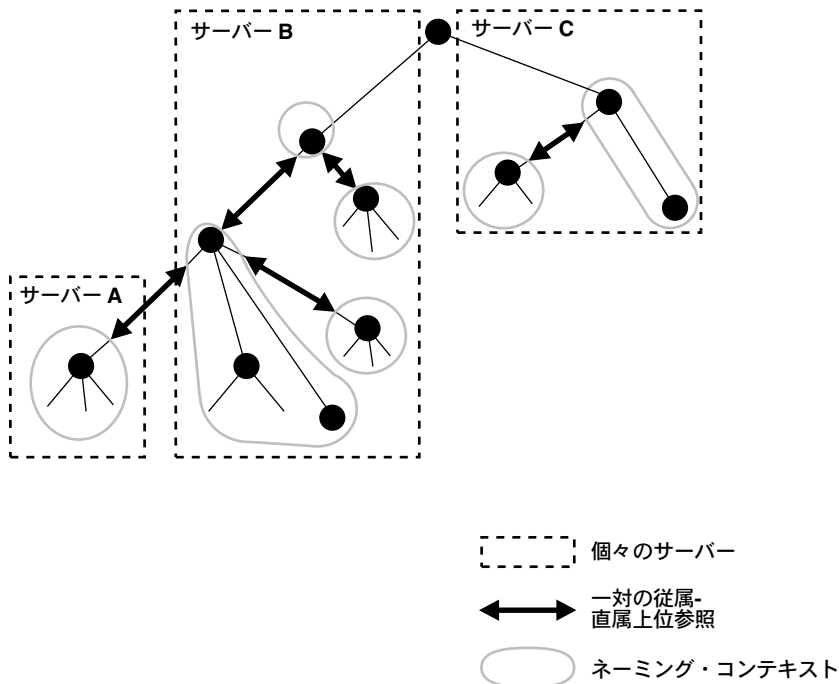
## ナレッジ参照 (参照)

ナレッジ参照は、様々なネーミング・コンテキストの名前とアドレスを提供します。図 2-9 では、サーバー B はナレッジ参照を使用して、要求された情報がサーバー A の c=us と c=uk のネーミング・コンテキストにあることをクライアントに通知します。この結果、クライアントは参照情報を使用してサーバー A と通信できます。

一般的に、各 Directory Server には、上位ナレッジ参照と従属ナレッジ参照の両方があります。上位ナレッジ参照によって、DIT 内でルートに向かう上位方向が指し示されます。この参照は、パーティション化されたネーミング・コンテキストをその親に結び付けます。従属ナレッジ参照は、DIT 内で他のパーティションへの下位方向を指し示します。

たとえば、図 2-10 では、サーバー B には他のネーミング・コンテキストの上位にある、2 つのネーミング・コンテキストがあります。この 2 つの上位ネーミング・コンテキストは、従属ナレッジ参照を使用して、その従属ネーミング・コンテキストを指し示しています。逆に、サーバー A 上のネーミング・コンテキストは、サーバー B に常駐している直属の上位ネーミング・コンテキストを持っています。したがって、サーバー A は、上位ナレッジ参照を使用してサーバー B 上の親を指し示しています。

図 2-10 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、DIT 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。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を、スキーマまたは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勧めします。

---

## ナレッジ参照の種類

ナレッジ参照には、次の 2 種類があります。

スマート・ナレッジ参照 エントリが検索の有効範囲内にある場合に戻されます。要求された情報を格納しているサーバーを示します。

たとえば、次のような場合があります。

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

ou=sales、c=us、o=acme にある情報の要求をユーザーがサーバー A に送信すると、サーバー A はサーバー B を示すナレッジ参照をそのユーザーに提供します。

デフォルト・ナレッジ参照 ベース・オブジェクトがディレクトリになく、さらに操作が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ます。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します。

たとえば、サーバー A が次のものを保持するとします。

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

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

**関連項目：** 7-17 ページ「[ナレッジ参照（参照）の管理](#)」

## メタディレクトリ環境での他のディレクトリとの同期

メタディレクトリ環境では、複数ディレクトリを Oracle Internet Directory と同期化して単一の仮想ディレクトリを構成できます。この項では、次の内容について説明します。

- [メタディレクトリ](#)
- [メタディレクトリ・ソリューションでの Oracle Internet Directory の動作](#)

## メタディレクトリ

メタディレクトリを使用すると、企業が持つ多くのディレクトリを1つの仮想ディレクトリに同期化できます。

企業では今日、ERP システム、データベース・アプリケーション、メッセージ・システムおよびネットワーク・オペレーティング・システム (NOS) など、複数のディレクトリを配置することが多くなっています。異なるディレクトリを数多く管理していると、次のような問題が発生する場合があります。

- 冗長性 - 同じ情報が、企業内の複数の場所に記述されます。
- 高い管理費用 - 管理者は、複数の場所に格納された同じ情報をメンテナンスする必要があります。
- 一貫性のない - データ1つのディレクトリで更新された情報が、他のすべてのディレクトリとの間で共有されません。

メタディレクトリは、企業のディレクトリすべてを1つの同期化されたディレクトリのディレクトリに統合することで、これらの問題に対処します。

## メタディレクトリ・ソリューションでの Oracle Internet Directory の動作

Oracle Internet Directory リリース 2.1.1 は、サポートされているサード・パーティのメタディレクトリ・ソリューションとの相互運用が可能です。これにより、様々な情報リポジトリが Oracle Internet Directory と同期化し、単一の仮想ディレクトリを構成できます。

Oracle Internet Directory を取り込むメタディレクトリ・ソリューションによって、次のことが可能となります。

- 接続ディレクトリと呼ばれる他の情報リポジトリから Oracle Internet Directory にデータをインポートできます。
- Oracle Internet Directory から接続ディレクトリにデータをエクスポートできます。

Oracle Internet Directory と接続ディレクトリとの間のデータのインポートおよびエクスポートは、メタディレクトリ・エージェントと呼ばれるソフトウェア・コンポーネントによって実行されます。メタディレクトリ・ベンダーはメタディレクトリ・エージェントを、メタディレクトリ・ソリューションの一部として提供しています。メタディレクトリ・ベンダーのフレームワークを使用して、メタディレクトリ・エージェントを設計することもできます。



たとえば、Oracle Internet Directory とメタディレクトリ・ソリューションとを相互運用すると、企業内の各従業員ごとにグローバル・ディレクトリ・エントリを作成できます。このエントリは、人材アプリケーション、電子メール・サービスまたは NOS データベースなど、異なるソースのデータを含むことができます。ユーザーは、それが最新かつすべての接続ディレクトリ間で同期化されているものとして、このエントリにアクセスできます。

さらに、同期は既存のデータ所有権方針を保持できます。たとえば、人事ディレクトリのみに従業員の給与属性を変更する権限を与えることもできます。このようにして、メタディレクトリ・ソリューションはディレクトリ・データを管理し、企業内の異なるディレクトリ間で情報を共有します。

---

**注意：** Oracle Internet Directory リリース 2.1.1 は、サポートされているバージョンの Siemens DirXMetahub との相互運用が可能です。

オラクル社は Siemens DirXMetahub 製品のライセンスを供与しておらず、この製品は CD にも収められていません。Siemens DirXMetahub を入手するには、次の Siemens の URL を参照してください。

<http://www.usa.siemens.com/>

---

サポートされているメタディレクトリ・ソリューションは、Oracle Internet Directory をそのメタディレクトリ・ストアとして使用します。つまり、Oracle Internet Directory は、他のアプリケーション固有の接続を確立済のディレクトリにとって、同期化の対象となる企業ディレクトリです。

メタディレクトリ・ソリューションによって他のディレクトリを Oracle Internet Directory に統合することには、次のような利点があります。

- ユーザーとアプリケーション双方にとっての、一貫性、データの整合性および情報の品質の向上
- Web ブラウザのような業界標準に準拠したクライアントによる、すべてのディレクトリ・データの 1 箇所でのアクセス、管理費用の削減および管理の容易さ
- Oracle Internet Directory 管理ツールを使用した 1 箇所での管理
- 環境内のすべての接続ディレクトリを最新に保つ能力

Oracle Internet Directory のメタディレクトリ・ソリューションのサポートによって、次のタイプのディレクトリ同期が可能です。

- 接続ディレクトリから Oracle Internet Directory への完全インポートおよび増分インポート（追加、変更および削除操作）
- Oracle Internet Directory から接続ディレクトリへの完全エクスポートおよび増分エクスポート（追加、変更および削除操作）

**関連項目：** [第 11 章「複数ディレクトリとの同期化」](#)



---

## 事前に行う作業

この章では、Oracle Internet Directory を構成および使用する前に実行する必要があるいくつかのタスクについて説明します。また、Oracle Internet Directory の以前のリリースからのアップグレードについても説明します。

管理ツールを実行し、ディレクトリの構成と使用を開始するには、OID モニターを開始し、Directory Server インスタンスを起動しておく必要があります。また、デフォルト・セキュリティ構成の再設定も行う必要があります。

この項では、次の項目について説明します。

- [タスク 1: OID モニター・デーモンの開始](#)
- [タスク 2: サーバー・インスタンスの起動](#)
- [タスク 3: デフォルト・セキュリティ構成の再設定](#)
- [Oracle Internet Directory の以前のリリースからのアップグレード](#)

## タスク 1: OID モニター・デーモンの開始

サーバーの起動と停止を行うコマンドを処理するためには、OID モニター・デーモンが実行中である必要があります。

この項では、次の項目について説明します。

- OID モニターの開始
- OID モニターの停止

### OID モニターの開始

OID モニターを開始する手順は、次のとおりです。

- 次の環境変数を適切な言語設定に設定します。インストール時のデフォルトの言語設定は、AMERICAN\_AMERICA です。

```

NLS_LANG=APPROPRIATE_LANGUAGE.UTF8

```

- コマンド・プロンプトで、次のコマンドを入力します。

```

oidmon [connect=net_service_name] [sleep=seconds] start

```

引数	説明
<code>connect=<i>net_service_name</i></code>	接続するデータベースのネット・サービス名を指定します。 <code>tnsnames.ora</code> ファイルに設定されているネットワーク・サービス名です。この引数はオプションです。
<code>sleep=<i>seconds</i></code>	OID モニターが、OID 制御ユーティリティからの新規要求、および停止している可能性があるサーバーの再起動要求をチェックするまでの秒数を指定します。デフォルトのスリープ・タイムは 10 秒です。この引数はオプションです。
<code>start</code>	OID モニター・プロセスを開始します。

次のようなコマンドを実行します。

```

oidmon connect=dbs1 sleep=10 start

```

## OID モニターの停止

OID モニター・デーモンを停止するには、コマンド・プロンプトで次のコマンドを入力します。

```
oidmon [connect=net_service_name] stop
```

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

次のようなコマンドを実行します。

```
oidmon connect=dbsl stop
```

## タスク 2: サーバー・インスタンスの起動

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

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

この項では、次の項目について説明します。

- [Oracle Directory Server インスタンスの起動](#)
- [Oracle Directory Server インスタンスの停止](#)
- [Oracle Directory Replication Server インスタンスの起動](#)
- [Oracle Directory Replication Server インスタンスの停止](#)
- [Directory Server インスタンスの再起動](#)
- [Directory Server インスタンスの起動に関するトラブルシューティング](#)

## Oracle Directory Server インスタンスの起動

Oracle Directory Server インスタンスを起動する構文は次のとおりです。

```
oidctl connect=net_service_name server=oidldapd instance=server_instance_number
[configset=configset_number] [flags=' -p port_number -work maximum_number_of_worker_
threads_per_server -debug debug_level -l change_logging -server n'] start
```

引数	説明
connect=net_service_name	すでに tnsnames.ora ファイルを構成している場合は、ORACLE_HOME/network/admin にある、そのファイルに指定されているネット・サービス名です。
server=oidldapd	起動するサーバーの種類（有効な値は OIDLDAPD と OIDREPLD です）。大文字と小文字は区別されません。
instance=server_instance_number	起動するサーバーのインスタンス番号。0 ～ 1000 の間の数値を設定してください。
configset=configset_number	サーバーの起動に使用される configset の番号。未設定の場合は、デフォルトで configset0 に設定されます。0 ～ 1000 の間の数値を設定してください。
-p port_number	サーバー・インスタンス起動中のポート番号を指定します。未設定の場合、デフォルト・ポートは 389 です。
-work maximum_number_of_worker_threads_per_server	このサーバーのワーカー・スレッドの最大数を指定します。
-debug debug_level	Oracle Directory Server インスタンス起動中のデバッグ・レベルを指定します。
-l change_logging	レプリケーションの変更ログを記録するかどうかを設定します。記録しない場合は -l を入力し、記録する場合はこのフラグを省略します。デフォルトは TRUE（値は TRUE と FALSE）です。（Directory Server のみ）
-server n	このポートで起動するサーバー・プロセスの数を指定します。
start	server 引数で指定したサーバーを起動します。

たとえば、ネット・サービス名が dba1 で、configset5 を使用し、ポート 12000、デバッグ・レベル 1024、インスタンス番号 3、変更ログ記録なしで Oracle Directory Server インスタンスを起動するには、コマンド・プロンプトで次のように入力します。

```
oidctl connect=dba1 server=oidldapd instance=3 configset=5 flags='-p 12000
-debug 1024 -l ' start
```

Oracle Directory Server インスタンスの起動と停止には、サーバー名とインスタンス番号が必須です。その他の引数はすべてオプションです。

フラグ引数内のペアのキーワード値はすべて、その間を1つの空白で区切る必要があります。

フラグは引用符で囲む必要があります。

configset 識別子が未設定の場合は、デフォルトで0 (configset0) に設定されます。

**注意：** デフォルト・ポート（無保護使用の場合は389、保護使用の場合は636）以外のポートを使用する場合は、Oracle Internet Directory の配置に使用するポートをクライアントに通知する必要があります。デフォルト・ポートを使用する場合、クライアントは、接続要求でポートを参照せずに Oracle Internet Directory に接続できます。

Oracle Directory Server インスタンスの停止

Oracle Directory Server インスタンスを起動または停止するときは、常に OID モニターが実行中であることが必要です。

コマンド・プロンプトで、次のコマンドを入力します。

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

次のようなコマンドを実行します。

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

Oracle Directory Replication Server インスタンスの起動

Oracle Directory Replication Server を起動する構文は、次のとおりです。

```
oidctl connect=net_service_name server=oidrepld instance=server_instance_number  
[configset=configset_number] flags=' -h hostname -p port_number  
-d debug_level -m [true | false] -z transaction_size ' start
```

引数	説明
connect=net_service_name	すでに tnsnames.ora ファイルを構成している場合は、ORACLE_HOME/network/admin にある、そのファイルに指定されている名前です。
server=oidrepld	起動するサーバーの種類（有効な値は OIDLDAPD と OIDREPLD です）。大文字と小文字は区別されません。

引数	説明
<code>instance=server_instance_number</code>	起動するサーバーのインスタンス番号。0 ～ 1000 の間の数値を設定してください。
<code>configset=configset_number</code>	サーバーの起動に使用される configset の番号。未設定の場合は、デフォルトで configset0 に設定されます。0 ～ 1000 の間の数値を設定してください。
<code>-p port_number</code>	サーバー・インスタンス起動中のポート番号を指定します。未設定の場合、デフォルト・ポートは 389 です。
<code>-d debug_level</code>	Replication Server インスタンス起動中のデバッグ・レベルを指定します。
<code>-h</code>	サーバーを実行するホスト名を指定します。(Replication Server のみ)
<code>-m [true false]</code>	競合の解消を行うかどうかを設定します。デフォルトは TRUE (値は TRUE と FALSE) です。(Replication Server のみ)
<code>-z transaction_size</code>	各レプリケーション更新サイクルで適用される変更の数を指定します。指定しない場合は、Oracle Directory Server の sizelimit パラメータの値で決まります。sizelimit パラメータのデフォルト設定は 1024 です。この設定は変更できます。
<code>start</code>	server 引数で指定したサーバーを起動します。

たとえば、インスタンスが 1、ポート 12000、デバッグ・レベル 1024 で Replication Server を起動するには、コマンド・プロンプトで次のように入力します。

```
oidctl connect=dbs1 server=oidrepld instance=1 flags='-p 12000 -h eastsun11 -d 1024' start
```

Oracle Directory Replication Server の起動と停止には、`-h` フラグ（ホスト名を指定する引数）が必須です。その他のフラグはすべてオプションです。

フラグ引数内のペアのキーワード値はすべて、その間を 1 つの空白で区切る必要があります。

フラグは引用符で囲む必要があります。

configset 識別子が未設定の場合は、デフォルトで 0 (configset0) に設定されます。

**注意：** デフォルト・ポート（無保護使用の場合は 389、保護使用の場合は 636）以外のポートを使用する場合は、Oracle Internet Directory の配置に使用するポートをクライアントに通知する必要があります。デフォルト・ポートを使用する場合、クライアントは、接続要求でポートを参照せずに Oracle Internet Directory に接続できます。



## Oracle Directory Replication Server インスタンスの停止

Oracle Directory Replication Server インスタンスを起動または停止するときは、常に OID モニターが実行中であることが必要です。

コマンド・プロンプトで、次のコマンドを入力します。

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

次のようなコマンドを実行します。

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

## Directory Server インスタンスの再起動

Directory Server インスタンスを再起動するには、コマンド・プロンプトで次のコマンドを入力します。

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

Directory Server インスタンスを起動、停止または再起動するときは、常に OID モニターが実行中の必要があります。

アクティブなサーバー・インスタンスが参照している構成設定エントリを変更する場合、構成設定エントリの変更値をそのサーバー・インスタンスで有効にするには、そのインスタンスを停止してから再起動してください。これには、STOP コマンドの後に START コマンドを発行するか、RESTART コマンドを使用します。RESTART は、サーバー・インスタンスを停止してから再起動します。

たとえば、Oracle Directory Server の instance1 が、configset3 を使用してネット・サービス名 dbs1 で起動されたとします。その後、instance1 の稼働中に configset3 内の属性の 1 つを変更したとします。configset3 の変更内容を instance1 で有効にするには、次のコマンドを入力します。

```
oidctl connect=dbs1 server=oidldapd instance=1 restart
```

configset3 を使用する複数の Oracle Directory Server のインスタンスが、そのノードで実行中の場合は、次のコマンド構文を使用して、すべてのインスタンスを一度に再起動できます。

```
oidctl connect=dbs1 server=oidldapd restart
```

このコマンドは、configset3 を使用しているかどうかに関係なく、そのノードで実行中のインスタンスをすべて再起動することに注意してください。

---

---

**重要：** 再起動プロセスの間は、クライアントが Oracle Directory Server インスタンスにアクセスできません。ただし、再起動にかかる時間は数秒です。

---

---

### Directory Server インスタンスの起動に関するトラブルシューティング

Directory Server が起動に失敗した場合は、Directory Server を起動するためにユーザーが指定した構成パラメータをすべてオーバーライドした上で、ldapmodify 操作によって構成設定を使用可能な状態に戻すことができます。

ディレクトリに格納されている構成パラメータのかわりに、ハードコードされたデフォルト・パラメータを使用して Directory Server を起動するには、コマンド・プロンプトで次のコマンドを入力します。

```
oidctl connect=net_service_name flags='-p port_number -f'
```

フラグ内に -f オプションを指定すると、定義済みの構成設定が configset0 内の値を除いてすべてオーバーライドされ、ハードコードされた構成値でサーバーが起動されます。

## タスク 3: デフォルト・セキュリティ構成の再設定

Oracle Internet Directory を初めてインストールするときは、デフォルト構成によって、ディレクトリ内のエントリすべてに対して、読み込み、ブラウズおよび検索アクセス権限がすべてのユーザーに付与されます。最初に行う必要がある作業の 1 つは、アクセス制御ポリシーを設定および実装し、適切な認証を各ユーザーに確実に付与することです。サブエントリ subSchemaSubEntry とその子のオブジェクトにはディレクトリに関する情報が格納されているため、オラクル社では、これらに対するアクセスを制御することを特にお勧めします。

また、ディレクトリ・エントリをロードすると、ディレクトリ・エントリの階層が作成されます。このため、次の項目を設定する必要があります。

- この階層にエントリをロードするための権限
- ディレクトリ・エントリに対する読み込み、変更および書き込みの各アクセス権限を必要とするクライアントを対象としたディレクトリ・アクセス権限

**関連項目：**

- アクセス制御のオプションの説明、およびセキュリティの設定方法は、[第9章「ディレクトリのアクセス制御の管理」](#)を参照してください。
- セキュリティを構成するために使用する管理ツールについては、[第4章「管理ツールの使用方法」](#)を参照してください。
- コマンドライン・ツールの構文と使用法は、[付録E「スキーマ要素」](#)を参照してください。

## Oracle Internet Directory の以前のリリースからのアップグレード

Oracle Internet Directory リリース 2.1.1 は、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 へのアップグレードは、インストール・プロセス中のプロンプトに応じて選択します。

レプリケート環境では、リリース 2.1.1 を実行するノードと Oracle Internet Directory の以前のリリースを実行するノードが共存できます。レプリケート環境では、1 つのノードをリリース 2.1.1 にアップグレードする際にネットワーク停止時間を必要としません。アップグレード・プロセス中も、他のノードは使用可能なままです。

この項では、次の項目について説明します。

- [単一ノード環境でのアップグレード](#)
- [マルチノード環境でのアップグレード](#)

### 単一ノード環境でのアップグレード

単一ノードでアップグレードするには、使用しているオペレーティング・システム用のインストール・ドキュメントの指示に従ってください。

### マルチノード環境でのアップグレード

マルチノードの Oracle Internet Directory システムをリリース 2.1.1 にアップグレードするには、特別な注意が必要です。この項では、マルチノードの Oracle Internet Directory システムをアップグレードする次の 2 つの方法について説明します。

- 1 ノードずつアップグレード
- すべてのノードを同時にアップグレード

## 1 ノードずつアップグレード

システム停止時間を発生させないためには、この方法を使用します。1つのノードでアップグレードが進行していても、他のノードはすべて使用可能なままです。しかし、この方法を使用するには、次のガイドラインを明確に理解して、必ずそれに従う必要があります。

- レプリケーション・ネットワークを1ノードずつアップグレードする場合は、すべてのノードがアップグレードされるまでアップグレードは完了しません。しかし、この間、アップグレード対象外のネットワーク・ノードはすべて使用可能なままです。これは一時的な状態とみなされます。この指定をするには、DSE ルートの属性 `orclupgradeinprogress` を `TRUE` に設定します。この属性はアップグレード手順の間に作成されます。
- レプリケートされた Oracle Internet Directory ネットワークのすべてのノードがリリース 2.1.1 にアップグレードされると、システムは一時的な状態を終ります。この時点で、すべてのノードの属性 `orclupgradeinprogress` を `FALSE` に設定してください。
- 一時的な状態、つまり DSE ルートの `orclupgradeinprogress` 属性が `TRUE` に設定されていると、リリース 2.1.1 のノードは、他のノードのために生成した変更ログ・エントリで特別な処理を実行します。これは下位互換性を保つために必須です。
- 一時的な状態では、新しいパスワード暗号化スキームを使用しないでください。これを行うと、様々なノードにまたがるパスワード値に非一貫性が発生し、以前のリリースを実行しているノードで認証が使用できなくなります。一時的な状態では、既存のパスワード暗号化スキームを使用します。ネットワーク全体がアップグレードされると、新しいパスワード暗号化スキームを使用できるようになります。
- アップグレード中に読取り / 書込みが行われるノードは1つのみです。残りのノードは読取り専用です。
- アップグレードされたノードでは、バイナリ属性変更を実行しないでください。そのような変更は、2.0.4.x および 2.0.6 ノードで失敗します。
- マスター・サイトをアップグレードする前に、必ず[マスター定義サイト](#)でアップグレードを実行してください。

### 関連項目：

- Oracle Internet Directory リリース 2.1.1 のパスワード用にサポートされている暗号化アルゴリズムのリストは、xxv ページの「[Oracle Internet Directory の新機能](#)」を参照してください。
- 3-16 ページ「[パスワード暗号化のためのアップグレード後の手順](#)」

次のタスクを最初は MDS で、次にマスター・サイトで実行してください。

#### タスク 1: アップグレードされるノードの Oracle Directory Replication Server の停止

**関連項目：** 3-7 ページ [「Oracle Directory Replication Server インスタンスの停止」](#)

#### タスク 2: アップグレードされるノードの Oracle Directory Server の停止

**関連項目：** 3-5 ページ [「Oracle Directory Server インスタンスの停止」](#)

#### タスク 3: アップグレードされるノードの OID モニターの停止

**関連項目：** 3-3 ページ [「OID モニターの停止」](#)

**タスク 4: 他のノードのジョブの削除** MDS でデータベースを停止する前に、インストール CD の /oidupgrade/ にあるスクリプト delasrjobs.sql を実行してください。このスクリプトは、MDS に変更を送信する他のマスター・サイトの [アドバンスト・レプリケーション \(ASR\)](#) ・ジョブを削除します。これらのジョブを削除すると、変更が適用されないように、MDS がレプリケーション環境から一時的に削除されます。しかし、他のノードは操作中のままで、変更をレプリケートし続けます。

**タスク 5: アップグレードされるノードのデータベースとリスナーのシャットダウン** データベースとリスナーをシャットダウンしない場合、Oracle Universal Installer がシャットダウンするように要求してきます。

**関連項目：**

- リスナーの停止については、『Oracle8i Net8 管理者ガイド』を参照してください。
- データベース・サーバーのシャットダウンについては、『Oracle8i 管理者ガイド』を参照してください。

**タスク 6: ノードの Oracle Internet Directory リリース 2.1.1 へのアップグレード** Oracle Universal Installer を実行して、Oracle Internet Directory リリース 2.1.1 へアップグレードしてください。Oracle Internet Directory リリース 2.1.1 は、Oracle8i リリース 8.1.7 を使用します。インストーラは、データベースを移行し、Oracle Internet Directory をアップグレードします。

**タスク 7: データベースとリスナーの起動** アップグレード完了後、データベースとリスナーが起動されて実行中であることを確認してください。

他のノードへの接続をテストしてください。接続が切れている場合、listener.ora、sqlnet.ora および tnsnames.ora のバックアップ・コピーを使用して、リスナーを再起

動してください。バックアップ・ファイルの名前は、`listenerdate.bak`、`sqlnetdate.bak` および `tnsnamesdate.bak` です。

**タスク 8: 他のノードでの送信ジョブの作成** ノードのアップグレード後、他のノードにジョブを作成してください。アップグレードされたノードで、`$ORACLE_HOME/ldap/admin/creasrjobs.sql` を実行します。このスクリプトによって、他のノードに、3-11 ページの「[タスク 4: 他のノードのジョブの削除](#)」で削除されたジョブが作成されます。これらのジョブは、他のノード上の既存の変更と新規の変更の、アップグレードしたノードへの送信を始めます。

**タスク 9: パスワード暗号化のためのアップグレード後の手順の実行** ノードがアップグレードされた後で、3-16 ページの「[パスワード暗号化のためのアップグレード後の手順](#)」に記述されているアップグレード後の手順を実行し、パスワード暗号化を行ってください。

#### タスク 10: OID モニターの起動

**関連項目：** 3-2 ページ「[OID モニターの開始](#)」

#### タスク 11: Oracle Directory Server の起動

**関連項目：** 3-4 ページ「[Oracle Directory Server インスタンスの起動](#)」

#### タスク 12: Oracle Directory Replication Server の起動

**関連項目：** 3-5 ページ「[Oracle Directory Replication Server インスタンスの起動](#)」

**タスク 13: 他のマスター・サイトのアップグレード** MDS のアップグレード後、他のマスター・サイトを 1 つずつアップグレードしてください。すべてのノードがアップグレードされるまで、マスター・サイトごとにタスク 1 ～ 12 を実行してください。

**タスク 14: すべてのノードの `orclupgradeinprogress` 属性の更新** すべてのノードが Oracle Internet Directory リリース 2.1.1 にアップグレードされた後、すべてのノードの `orclupgradeinprogress` 属性を `FALSE` に変更してください。この手順は、次のとおりです。

1. 入力ファイルを次のように編集します。

```
dn:
changetype:modify
replace:orclupgradeinprogress
orclupgradeinprogress:FALSE
```

2. ldapmodify を使用して、このファイルをロードします。

```
ldapmodify -D "cn=orcladmin" -w welcome -h host_name -p port_number -f input_
file.ldif
```

**関連項目：** MDS の詳細は、[第 10 章「ディレクトリ・レプリケーションの管理」](#)を参照してください。

## すべてのノードを同時にアップグレード

すべてのノードを同時にアップグレードするには、この方法を使用します。この方法を使用する場合、アップグレード処理中はシステムが使用できません。

### タスク 1: ネットワーク内のすべてのノードを読み取り専用モードに設定

1. 入力ファイルを次のように編集します。

```
dn:
changetype:modify
replace:orclservermode
orclservermode:r
```

2. レプリケーション・ネットワーク内のすべてのノードに対して、次のコマンドを実行します。

```
ldapmodify -D "cn=orcladmin" -w welcome -h host_name -p port_number -f input_
file.ldif
```

**タスク 2: 変更ログ・キューの変更がすべて適用されるまで待機** 変更ログ・キューが空になってから、次の手順に進んでください。この手順をスキップすると、変更ログ・キューにあるすべての変更は、ノードのアップグレード時に一度に適用されます。

### タスク 3: すべてのノードで Oracle Directory Replication Server を停止

**関連項目：** 3-7 ページ「[Oracle Directory Replication Server インスタンスの停止](#)」

### タスク 4: すべてのノードで Oracle Directory Server を停止

**関連項目：** 3-5 ページ「[Oracle Directory Server インスタンスの停止](#)」

### タスク 5: すべてのノードで OID モニターを停止

**関連項目：** 3-3 ページ「[OID モニターの停止](#)」

**タスク 6: すべてのノードのデータベースとリスナーのシャットダウン** データベースとリスナーをシャットダウンしない場合、Oracle Universal Installer がシャットダウンするように要求してきます。

**関連項目：**

- リスナーの停止については、『Oracle8i Net8 管理者ガイド』を参照してください。
- データベース・サーバーのシャットダウンについては、『Oracle8i 管理者ガイド』を参照してください。

**タスク 7: すべてのノードの Oracle Internet Directory リリース 2.1.1 へのアップグレード** Oracle Universal Installer を実行して、Oracle Internet Directory リリース 2.1.1 へアップグレードしてください。Oracle Internet Directory リリース 2.1.1 は、Oracle8i リリース 8.1.7 を使用します。インストーラは、データベースを移行し、Oracle Internet Directory をアップグレードします。

**タスク 8: すべてのノードのデータベースとリスナーの起動** アップグレード完了後、データベースとリスナーが起動されて実行中であることを確認してください。

他のノードへの接続をテストしてください。接続が切れている場合、listener.ora、sqlnet.ora および tnsnames.ora のバックアップ・コピーを使用して、リスナーを再起動してください。バックアップ・ファイルの名前は、listenerdate.bak、sqlnetdate.bak および tnsnamesdate.bak です。

**タスク 9: パスワード暗号化のためのアップグレード後の手順の実行** ノードがアップグレードされた後で、3-16 ページの「[パスワード暗号化のためのアップグレード後の手順](#)」に記述されているアップグレード後の手順を実行し、パスワード暗号化を行ってください。

**タスク 10: すべてのノードで OID モニターを起動**

**関連項目：** 3-2 ページ「[OID モニターの開始](#)」

**タスク 11: すべてのノードで Oracle Directory Server を起動**

**関連項目：** 3-4 ページ「[Oracle Directory Server インスタンスの起動](#)」

**タスク 12: すべてのノードで Oracle Directory Replication Server を起動**

**関連項目：** 3-5 ページ「[Oracle Directory Replication Server インスタンスの起動](#)」



**タスク 13: すべてのノードの orclupgradeinprogress 属性の更新** すべてのノードが Oracle Internet Directory リリース 2.1.1 にアップグレードされたら、すべてのノードの orclupgradeinprogress 属性を FALSE に変更してください。この手順は、次のとおりです。

1. 入力ファイルを次のように編集します。

```
dn:
changetype:modify
replace:orclupgradeinprogress
orclupgradeinprogress:FALSE
```

2. ldapmodify を使用して、このファイルをロードします。

```
ldapmodify -D "cn=orcladmin" -w welcome -h host_name -p port_number -f input_
file.ldif
```

レプリケーション環境のすべてのノードでこの変更を実行してください。

## LDIF ベースのアップグレード

オラクル社は、既存のリリースの Oracle Internet Directory のバックアップに LDIF ベースのバックアップ手順を使用することをお勧めします。この項では、その方法について説明します。

通常は、LDIF ベースのアップグレードを行う必要はありません。この方法は、データベース・ベースのアップグレード処理が正常に実行できない場合に使用してください。

LDIF ベースのアップグレード処理では、アップグレードするノードで次の手順を行う必要があります。

**タスク 1: Oracle Internet Directory の旧バージョンのバックアップ** Oracle Directory Server が実行中でないことを確認し、CD の /oidupgrade ディレクトリにあるスクリプト backup\_oid.sh を実行してください。

backup\_oid.sh を実行する構文は次のとおりです。

```
backup_oid.sh -connect net_service_name -pass password_for_DB_account_ods'
```

backup\_oid.sh スクリプトは次のことを行います。

- Oracle Internet Directory スキーマをエクスポートします。このとき、`$ORACLE_HOME/ldap/load` ディレクトリに .dmp ファイル（例: attr\_store.dmp）を生成します。
- Ldifwrite ユーティリティを使用して、OID サブツリーをバックアップします。このとき、`$ORACLE_HOME/ldap/load` に、ファイル `OID_userdata.ldif` を生成します。cn=OracleSchemaVersion の下のサブツリーも（存在する場合）、`$ORACLE_HOME/ldap/load` ディレクトリに `orcl_schemaver.ldif` としてバックアップされます。

Oracle Internet Directory リリース 2.1.1 を同じ `ORACLE_HOME` にインストールする計画の場合には、生成されたこれらのファイルを別の場所に保存してください。

## タスク 2: Oracle Internet Directory リリース 2.1.1 の新規インストールの実行

**関連項目：** 使用しているオペレーティング・システム用のインストレーション・ドキュメントを参照してください。

**タスク 3: Oracle Internet Directory の以前のバージョンの、ユーザー定義のスキーマとデータのリストア** この手順は、次のとおりです。

1. Oracle Directory Server が実行中でないことを確認します。
2. 次のファイルを `$ORACLE_HOME/ldap/load` にコピーします。
  - バックアップされた Oracle Internet Directory スキーマのダンプ・ファイル（拡張子 `.dmp` のファイル）
  - ファイル `OID_userdata.ldif`
3. `$ORACLE_HOME/ldap/install` にあるスクリプト `restore_oid.sh` を実行します。  
`restore_oid.sh` の構文は次のとおりです。

```
restore_oid.sh -connect net_service_name -pass password_for_DB_account 'ods'
```

`restore_oid.sh` スクリプトは次のことを行います。

- ダンプ・ファイルから Oracle Internet Directory スキーマをインポートします。
- 以前のリリース（2.0.6 または 2.0.4）と 2.1.1 とのスキーマの差分を挿入します。
- LDIF ファイルから `-restore` オプションで、データをバルクロードします。

**タスク 4: パスワードのアップグレード** パスワードをアップグレードするために、`$ORACLE_HOME/ldap/bin/` にある `cryptupgrd.sh` スクリプトを実行してください。

`cryptupgrd.sh` の構文は次のとおりです。

```
cryptupgrd.sh -connect net_service_name -pass password_for_DB_account 'ods'
```

## パスワード暗号化のためのアップグレード後の手順

リリース 2.0.6 とリリース 2.0.4 では、ユーザー・パスワードは 1 種類の暗号化アルゴリズムである MD4 のみを使用して暗号化されていました。ルート DSE のフラグ（`orcluseencrypt`）で、暗号化のオン / オフの切替えのみが行われていました。それに対して、Oracle Internet Directory リリース 2.1.1 では、複数のハッシュ・スキームがサポートされています。

Oracle Internet Directory リリース 2.1.1 は、パスワード値の接頭辞としてハッシュ・スキームを格納しています。アップグレード中にルート DSE に作成された新しい属性は、デフォルト

トのハッシュ・スキームを示しています。与えられたパスワードが暗号化されていない場合、Oracle Directory Server はこのデフォルト値を使用してパスワードを暗号化します。

パスワード暗号化のためのアップグレード後の手順によって、接頭辞 MD4 が、ディレクトリ内の既存のパスワード値すべてに追加されます。この手順が終了するまでにかかる時間は、ディレクトリ内のエントリ数によって変わります。

この手順を実行するには、次のコマンドを入力してください。

```
cryptupgrd.sh -connect net_service_name -pass password_for_DB_account_ 'ods'
```

**関連項目：**

- Oracle Internet Directory リリース 2.1.1 のパスワード用にサポートされている暗号化アルゴリズムのリストは、xxv ページの「[Oracle Internet Directory の新機能](#)」を参照してください。



---

## 管理ツールの使用方法

この章では、Oracle Internet Directory の様々な管理ツールを紹介します。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 Directory Server に接続する方法を説明します。また、コマンドライン・ツールとバルク・ツールについても説明します。

この章では、次の項目について説明します。

- [Oracle Directory Manager の使用方法](#)
- [コマンドライン・ツールの使用方法](#)
- [バルク・ツールの使用方法](#)
- [カタログ管理ツールの使用方法](#)
- [OID データベース・パスワード・ユーティリティの使用方法](#)
- [レプリケーション・ツールの使用方法](#)
- [OID データベース統計収集ツールの使用方法](#)
- [管理タスクの一覧](#)

# Oracle Directory Manager の使用方法

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

この項では、次の項目について説明します。

- [Oracle Directory Manager の起動](#)
- [Directory Server への接続](#)
- [Oracle Directory Manager のナビゲート](#)
- [追加の Directory Server への接続](#)
- [Directory Server からの切断](#)
- [Oracle Directory Manager を使用した管理タスクの実行](#)

## Oracle Directory Manager の起動

Oracle Directory Manager を起動するには、Directory Server [インスタンス](#)を実行しておく必要があります。

**関連項目：**

- サーバー・インスタンスの実行方法は、[第 3 章「事前に実行する作業」](#)を参照してください。
- Directory Server インスタンスの概念の説明は、2-18 ページの「[Oracle Internet Directory のアーキテクチャ](#)」を参照してください。

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

オペレーティング・システム	参照箇所
Windows NT または Windows 95	「スタート」メニューから、「プログラム」 > 「ORACLE_HOME」 > 「Oracle Internet Directory」 > 「Oracle Directory Manager」をクリックします。
Sun Solaris	パスを設定していない場合は、ORACLE_HOME/bin に移動します。  コマンド・プロンプトで次のコマンドを入力します。  oidadmin

初めて Oracle Directory Manager を起動すると、サーバーに接続する必要があることを知らせる警告が表示されます。「OK」をクリックします。

## Directory Server への接続

Directory Server に接続する手順は、次のとおりです。

1. 「Directory Server Connection」ダイアログ・ボックスに、使用可能なサーバーの名前とポート番号を入力します。

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

「OK」をクリックします。「Oracle Directory Manager Connect」ダイアログ・ボックスが表示されます。

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

フィールド	説明
User	<p>初めてログインするときは、<b>スーパー・ユーザー</b>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。</p> <p>スーパー・ユーザーでログインする場合は、「User」ボックスに <code>cn=orcladmin</code> と入力します。</p> <p>匿名でログインする場合は、「User」ボックスを空白のままにします。</p> <p>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。</p> <ul style="list-style-type: none"><li>■ 「User」フィールドの右側のボタンを使用し、そのエントリをブラウズして選択します。</li><li>■ そのユーザーのエントリに対する<b>識別名</b>を、次の例のように正しい書式で入力します。</li></ul> <p><code>cn=Susie Brown,ou=HR,o=acme,c=us</code></p>

フィールド	説明
Password	<p>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「Password」ボックスに入力します。パスワードを指定していない場合は、デフォルトのパスワード welcome を入力します。Oracle Directory Manager にログインし、Directory Server 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。</p> <p>匿名でログインする場合は、「Password」ボックスを空白のままにします。</p> <p>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。</p> <p><b>関連項目 :</b> パスワードの変更方法は、5-19 ページの「<a href="#">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</a>」を参照してください。</p>
Server	<p>「Server list」から、接続する Directory Server のあるホストを選択します。</p> <p>Directory Server にすでに接続している場合に、別のホストの Directory Server に接続する手順は、次のとおりです。</p> <ol style="list-style-type: none"><li>「Server」フィールドの右側のボタンをクリックします。使用可能なサーバーのリストが、ダイアログ・ボックスに表示されます。</li><li>サーバーを選択します。</li><li>「OK」をクリックします。</li></ol> <p>Directory Server を追加する手順は、次のとおりです。</p> <ol style="list-style-type: none"><li>「Add」をクリックします。「Directory Server Connection」ダイアログ・ボックスが表示されます。</li><li>追加する Directory Server の名前を入力します。</li><li>「OK」をクリックします。</li></ol>
Port	<p>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 Directory Server インスタンスが存在している場合、各 Directory Server インスタンスごとにポートが異なり、Directory Server 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。</p> <p>このポート番号を変更する手順は、次のとおりです。</p> <ol style="list-style-type: none"><li>「Server」フィールドの右側のボタンをクリックします。</li><li>「Select Directory Server」ダイアログ・ボックスで、Directory Server を選択します。</li><li>「Edit」をクリックします。「Directory Server Connection」ダイアログ・ボックスが表示されます。</li><li>「Directory Server Connection」ダイアログ・ボックスの「Port」フィールドにポート番号を入力して、「OK」をクリックします。</li></ol>



フィールド	説明
SSL Enabled	<p>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。</p> <p>Directory Server 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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>■ 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、接続時の認証に失敗します。</li> <li>■ 証明書と信頼されている証明書のリストを含んだ Wallet が作成済みであること。</li> </ul>

#### 関連項目：

- SSL を使用可能にする方法は、[第 8 章「Secure Sockets Layer \(SSL\) の管理」](#)を参照してください。
  - Wallet の作成方法は、[付録 C](#) を参照してください。
  - 識別名の書式に関する説明は、2-2 ページの「[エントリ](#)」を参照してください。
  - ポートの変更方法とそのセキュリティへの影響については、8-2 ページの「[SSL パラメータの構成](#)」を参照してください。
3. 「Credentials」タブの「SSL Enabled」チェック・ボックスを選択した場合は、次に「SSL」タブを選択してください。
  4. 次の表の説明に従って、各フィールドに必要なデータを入力します。

フィールド	説明
SSL Location	<p>ユーザーの 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。</p> <p style="text-align: center;"><code>file: absolute_path_name</code></p> <p>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。</p>
SSL Password	ユーザーの Wallet をオープンするパスワード。

フィールド	説明
SSL Authentication	認証レベルを次の中から選択します。 <ul style="list-style-type: none"><li>■ No SSL Authentication: 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。「Credentials」タブの「SSL Enabled」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。</li><li>■ SSL Client and Server Authentication: クライアントとサーバーの認証。クライアントとサーバーは、証明書を交換します。</li><li>■ SSL Server Authentication: サーバー認証。Directory Server がクライアントに証明書を送信することによって、Directory Server からクライアントに対してサーバー認証を行います。</li></ul>

**注意：** クライアントとサーバーの認証を必要とする場合、Oracle Directory Manager の各ユーザーは、一意の Wallet を持つ必要があります。サーバー認証を指定すると、1 つの Wallet を複数の Oracle Directory Manager ユーザーが使用できます。

5. 「Login」をクリックします。Oracle Directory Manager が表示されます。

## Oracle Directory Manager のナビゲート

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

### Oracle Directory Manager の概要

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

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

同様に、「Revert」ボタンと「Cancel」ボタンがあります。「Revert」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、ウィンドウを開いたまま作業を継続できます。

「Cancel」をクリックすると、そのウィンドウで行った変更は適用されないままウィンドウが閉じます。

## Oracle Directory Manager のメニュー・バー

次の表は、メニュー・バーからアクセスできるメニューの一覧と説明です。各メニュー項目は、表示しているペインやタブ・ページによって、使用できる場合と使用できない場合があります。

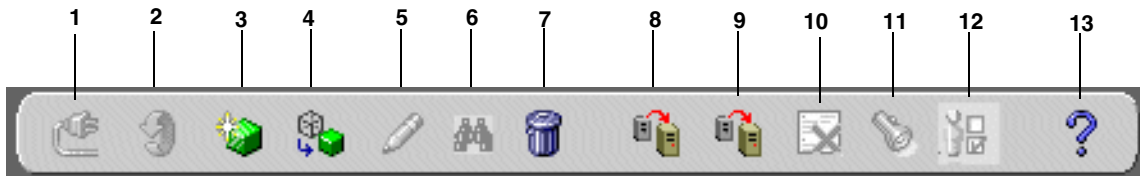
メニュー	メニュー項目
File	Create: オブジェクトを追加します。 Create Like: ナビゲータ・ペインで選択したオブジェクトをテンプレートとして使用し、新規オブジェクトを追加します。 Connect: ナビゲータ・ペインで選択した Directory Server に接続します。 Disconnect: ナビゲータ・ペインで選択した Directory Server から切断します。 Exit: Oracle Directory Manager を終了します。
Edit	Edit: オブジェクトを変更します。 Remove: 選択したオブジェクトを削除します。 Find Object Classes: オブジェクト・クラスを検索します。
View	Refresh: データベース上での変更内容を画面表示に反映するために、メモリーに格納されているデータを更新します。 Tear-Off: 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。

メニュー	メニュー項目
Operations	<p>Create Object Class: 新規オブジェクト・クラスの追加に使用する「New Object Class」ウィンドウを表示します。</p> <p>Create Attribute: エントリへの新規属性の追加に使用する「New Attribute Type」ダイアログ・ボックスを表示します。</p> <p>Create Access Ctrl Point: 新規 <b>Access Control Policy Point (ACP)</b> の追加に使用する「New Access Control Point」ダイアログ・ボックスを表示します。</p> <p>Create Entry: 新規ディレクトリ・エントリの追加に使用する「New Entry」ダイアログ・ボックスを表示します。</p> <p>Refresh Entry: 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。</p> <p>Refresh Subtree Entries: 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。</p> <p>Drop Index: 属性から索引を削除します。この項目を選択すると、削除の確認を要求する警告が表示されます。</p> <p>Search ACPs: ACP 検索の構成を可能にします。</p> <p>User Preferences: 次の操作のためのダイアログ・ボックスを表示します。</p> <ul style="list-style-type: none"><li>■ エントリ検索結果の表示の構成</li><li>■ 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</li></ul>
Help	<p>Contents: ヘルプ・ナビゲータの「Contents」タブ・ページを表示します。</p> <p>Search for Help On: オンライン・ヘルプ・ガイドのワード検索に使用する「Help Search」ダイアログ・ボックスを表示します。</p> <p>About Oracle Internet Directory: Oracle Internet Directory のバージョン情報を表示します。</p>

## Oracle Directory Manager のツールバー

図 4-1 とその下の表は、Oracle Internet Directory のツールバーの図とその説明です。各ボタンは、Oracle Directory Manager に表示しているペインやタブ・ページによって、使用できる場合と使用できない場合があります。

図 4-1 Oracle Directory Manager のツールバー



ボタン	用途
1	Connect/Disconnect: ナビゲータ・ペインで選択した Directory Server に接続、または選択した Directory Server から切断します。
2	Refresh: メモリーに格納されているエントリ以外のオブジェクトのデータを更新し、データベースに変更内容を反映します。
3	Create: 新規オブジェクトを追加します。
4	Create Like: 別のオブジェクトをテンプレートとして使用して、新規オブジェクトを追加します。
5	Edit: オブジェクトを変更します。
6	Find Object Classes: オブジェクト・クラスを検索します。
7	Delete: オブジェクトを削除します。
8	Refresh Entry: メモリーに格納されているエントリのデータを更新し、データベースに変更内容を反映します。
9	Refresh SubTree Entries: メモリーに格納されているエントリの子を更新し、データベースに変更内容を反映します。
10	Drop Index: 属性から索引を削除します。このボタンをクリックすると、削除の確認を要求する警告が表示されます。
11	Search: ACP 検索の構成を可能にします。
12	User Preferences: 検索操作のエントリと同様に、ナビゲータ・ペインの ACP の表示の構成を可能にします。
13	Help: ヘルプ・システムを表示します。

## 追加の Directory Server への接続

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

追加の Directory Server 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 Servers」を選択します。
- 2. 右側のペインの「New」をクリックします。
- 3. 4-3 ページの「[Directory Server への接続](#)」で説明している手順に従ってログインします。

## Directory Server からの切断

Oracle Directory Manager を使用して Directory Server から切断するには、「File > Disconnect」の順に選択します。また、Oracle Directory Manager を終了すると、すべての Directory Server 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、Directory Server の「Login」ダイアログ・ボックスに表示されます。

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

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

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

タスクの領域	参照箇所
スキーマの管理	6-6 ページ「 <a href="#">Oracle Directory Manager を使用したオブジェクト・クラスの管理</a> 」
	6-15 ページ「 <a href="#">Oracle Directory Manager を使用した属性の管理</a> 」
エントリの管理	7-2 ページ「 <a href="#">Oracle Directory Manager を使用したエントリの管理</a> 」
Access Control Policy Points (ACP) の管理	9-15 ページ「 <a href="#">Oracle Directory Manager を使用したアクセス制御の管理</a> 」

タスクの領域	参照箇所
パーティション化とレプリケーション	<a href="#">第 10 章「ディレクトリ・レプリケーションの管理」</a>

# 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のコマンドライン・ツールがいくつか用意されています。この項では、各ツールを使用して実行できる様々なタスクについて説明します。

コマンドライン・ツールは、LDAP データ交換フォーマット（LDIF）で記述されたテキスト・ファイルのオブジェクトに有効です。

**関連項目：** LDIF ファイルのフォーマット方法は、A-2 ページの「[LDAP データ交換フォーマット（LDIF）の構文](#)」を参照してください。

次の表は、各コマンドライン・ツールとそのツールで実行できるタスク、および構文と使用方法の参照箇所を示しています。

ツール	タスク	構文と使用方法
ldapsearch	ディレクトリ・エントリを検索します。	A-17 ページ「 <a href="#">ldapsearch 構文</a> 」
ldapbind	Directory Server に対して、ユーザーまたはクライアントを認証します。	A-7 ページ「 <a href="#">ldapbind 構文</a> 」
ldapadd	エントリを一度に 1 つずつ追加します。	A-4 ページ「 <a href="#">ldapadd 構文</a> 」
ldapaddmt	このマルチスレッド・ツールを使用して、複数のエントリを同時に追加します。	A-6 ページ「 <a href="#">ldapaddmt 構文</a> 」
ldapmodify	エントリの属性データを作成、更新および削除します。	A-12 ページ「 <a href="#">ldapmodify 構文</a> 」
ldapmodifymt	このマルチスレッド・ツールを使用して、複数のエントリを同時に変更します。	A-16 ページ「 <a href="#">ldapmodifymt 構文</a> 」
ldapdelete	エントリを削除します。	A-10 ページ「 <a href="#">ldapdelete 構文</a> 」
ldapcompare	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ます。	A-8 ページ「 <a href="#">ldapcompare 構文</a> 」
ldapmoddn	エントリの識別名（DN）または相対識別名（RDN）の変更、エントリまたはサブツリーの名前の変更、エントリまたはサブツリーの新しい親への移動を行います。	A-11 ページ「 <a href="#">ldapmoddn 構文</a> 」

**関連項目：** コマンドライン・ツールと NLS の説明は、12-5 ページの「[コマンドライン・ツールでの NLS の使用方法](#)」を参照してください。

## バルク・ツールの使用方法

バルク・ツールを使用すると、他のアプリケーションに常駐しているデータまたは他のアプリケーションで作成されたデータから、大量のディレクトリ・エントリを作成して管理できます。

**重要：** これらのツールを使用するには、Oracle Internet Directory の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。

**関連項目：**

- 4-13 ページ「[OID データベース・パスワード・ユーティリティの使用](#)  
[方法](#)」
- A-35 ページ「[OID データベース・パスワード・ユーティリティの構](#)  
[文](#)」

次の表は、各バルク・ツールとそのツールで実行できるタスク、および構文と使用方法の参照箇所を示しています。

ツール	タスク	構文と使用方法
bulkload	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ます。	A-22 ページ「 <a href="#">bulkload 構文</a> 」
ldifwrite	ディレクトリ情報ベースのデータを、LDAP 準拠の Directory Server で読み込み可能な LDIF ファイルにコピーします。ldifwrite は、bulkload と組み合わせて使用できます。ldifwrite を使用して、ディレクトリの一部またはすべての情報をバックアップすることもできます。	A-26 ページ「 <a href="#">ldifwrite 構文</a> 」
bulkmodify	大量の既存エントリを効率的に変更します。	A-24 ページ「 <a href="#">bulkmodify 構文</a> 」
bulkdelete	サブツリーを効率的に削除します。	A-21 ページ「 <a href="#">bulkdelete 構文</a> 」



## OID 制御ユーティリティの使用方法

OID 制御ユーティリティは、サーバーの起動および停止を行うためのコマンドライン・ツールです。コマンドは、OID モニターのプロセスによって解釈され、実行されます。

### 関連項目：

- A-30 ページ「[OID 制御ユーティリティの構文](#)」
- 概念の説明は、2-18 ページの「[Oracle Internet Directory のアーキテクチャ](#)」を参照してください。

## カタログ管理ツールの使用方法

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、検索で利用できる索引付けされた属性がエントリ `cn=catalogs` にリストされます。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。しかし、その属性がすでに存在している場合には、カタログ管理ツールを使用しなければ索引付けができません。

### 関連項目：

- 構文と使用方法は、A-27 ページの「[カタログ管理ツールの構文](#)」を参照してください。
- 6-25 ページ「[コマンドライン・ツールを使用した属性の索引付け](#)」
- 6-23 ページ「[作成時の属性の索引付け](#)」

## OID データベース・パスワード・ユーティリティの使用方法

Oracle Internet Directory は、Oracle データベースへの接続時にパスワードを使用します。Oracle Internet Directory をインストールした時点での、このパスワードのデフォルトは ODS です。OID データベース・パスワード・ユーティリティを使用すると、このパスワードを変更できます。

**関連項目：** 構文と使用方法は、A-35 ページの「[OID データベース・パスワード・ユーティリティの構文](#)」を参照してください。

## レプリケーション・ツールの使用方法

レプリケーション競合が発生した場合、Oracle Directory Replication Server は変更をリトライ・キューに入れ、指定した回数に応じてそれらの適用を試みます。指定した回数を超過して失敗が続いた場合、Replication Server は変更を管理者操作キューに入れます。そこから、Replication Server はより短い間隔で変更アプリケーション・プロセスを繰り返しながら管理者によるアクションを待ちます。

このとき、必要な手順は次のとおりです。

1. 管理者操作キューの変更を検証します。
2. 競合している変更を調停します。
3. 変更をリトライ・キューに戻すか、パージ・キューに入れます。

次のレプリケーション・ツールがこの処理に役立ちます。

OID 調停ツール	競合している変更の同期化を可能にします。
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・キューまたはパージ・キューへの変更の移動を可能にします。

### 関連項目：

- 10-33 ページ [「OID 調停ツールの使用」](#)
- 10-30 ページ [「管理者操作キュー操作ツールの使用」](#)

## OID データベース統計収集ツールの使用方法

`$ORACLE_HOME/ldap/admin/` にある OID データベース統計収集ツール (`oidstats.sh`) は、容量計画に役立ちます。様々なデータベース ods スキーマ・オブジェクトを分析できるため、統計の見積りに便利です。

### 関連項目： A-35 ページ [「OID データベース統計収集ツールの構文」](#)

## 管理タスクの一覧

Oracle Internet Directory の管理タスクの説明は、このマニュアル全体にわたって記述されています。表 4-1 に、一般的なタスクの一部について必要な情報を示します。

**表 4-1 一般的な管理タスクとその説明の参照箇所**

タスク	参照箇所
<b>属性の管理</b>	
コマンドライン・ツールを使用した属性の追加、変更または削除	6-24 ページ「 <a href="#">コマンドライン・ツールを使用した属性の管理</a> 」
Oracle Directory Manager を使用した属性の追加、変更または削除	6-15 ページ「 <a href="#">Oracle Directory Manager を使用した属性の管理</a> 」
<b>エントリの管理</b>	
コマンドライン・ツールを使用したディレクトリ・エントリの追加、変更または削除	7-10 ページ「 <a href="#">コマンドライン・ツールを使用したエントリの管理</a> 」
Oracle Directory Manager を使用したディレクトリ・エントリの追加、変更または削除	7-2 ページ「 <a href="#">Oracle Directory Manager を使用したエントリの管理</a> 」
大量のデータ・ファイルのインポート	A-22 ページ「 <a href="#">bulkload 構文</a> 」 A-2 ページ「 <a href="#">LDAP データ交換フォーマット (LDIF) の構文</a> 」
エントリのディレクトリ情報ツリー (DIT) 階層の表示	7-2 ページ「 <a href="#">Oracle Directory Manager を使用したエントリの管理</a> 」
<b>オブジェクト・クラスの管理</b>	
コマンドライン・ツールを使用したオブジェクト・クラスの追加、変更または削除	6-12 ページ「 <a href="#">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</a> 」
Oracle Directory Manager を使用したオブジェクト・クラスの追加、変更または削除	6-6 ページ「 <a href="#">Oracle Directory Manager を使用したオブジェクト・クラスの管理</a> 」
<b>セキュリティの管理</b>	
Access Control Policy Point (ACP) の設定	第 9 章「 <a href="#">ディレクトリのアクセス制御の管理</a> 」
セキュリティの設定	第 8 章「 <a href="#">Secure Sockets Layer (SSL) の管理</a> 」
<b>サーバーの管理</b>	
コマンドライン・ツールを使用したサーバー・インスタンス・パラメータの構成	5-10 ページ「 <a href="#">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</a> 」
Oracle Directory Manager を使用したサーバー・インスタンス・パラメータの構成	5-4 ページ「 <a href="#">Oracle Directory Manager を使用したサーバーの構成設定エントリの管理</a> 」

表 4-1 一般的な管理タスクとその説明の参照箇所 ( 続き )

タスク	参照箇所
Oracle Directory Manager を使用したディレクトリへの接続	4-3 ページ「 <a href="#">Directory Server への接続</a> 」 4-10 ページ「 <a href="#">追加の Directory Server への接続</a> 」
Directory Server プロセスの実行	第 3 章「 <a href="#">事前に実行する作業</a> 」
Directory Server プロセスの停止	第 3 章「 <a href="#">事前に実行する作業</a> 」
システム操作属性の表示	5-13 ページ「 <a href="#">Oracle Directory Manager を使用したシステム操作属性の設定</a> 」 5-14 ページ「 <a href="#">ldapmodify を使用したシステム操作属性の設定</a> 」
<b>レプリケーションの管理</b>	
レプリケーションの設定	第 10 章「 <a href="#">ディレクトリ・レプリケーションの管理</a> 」
レプリケーション変更の競合の解消	2-28 ページ「 <a href="#">レプリケーションにおける競合の解消</a> 」
レプリケーション変更の管理者操作キューからリトライ・キューかパージ・キューへの移動	10-30 ページ「 <a href="#">管理者操作キュー操作ツールの使用</a> 」

# 第II部

---

## Oracle Internet Directory の管理

第 II 部では、Oracle Internet Directory の構成とメンテナンスに必要なタスクを紹介します。  
第 II 部は次の各章から構成されています。

- 第 5 章「Oracle Directory Server の管理」
- 第 6 章「ディレクトリ・スキーマの管理」
- 第 7 章「ディレクトリ・エントリの管理」
- 第 8 章「Secure Sockets Layer (SSL) の管理」
- 第 9 章「ディレクトリのアクセス制御の管理」
- 第 10 章「ディレクトリ・レプリケーションの管理」
- 第 11 章「複数ディレクトリとの同期化」
- 第 12 章「各国語サポート (NLS) の管理」



---

# Oracle Directory Server 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 Directory Server を管理する方法を説明します。

この章では、次の項目について説明します。

- [サーバーの構成設定エントリの管理](#)
- [システム操作属性の設定](#)
- [ネーミング・コンテキストの管理](#)
- [パスワード暗号化の管理](#)
- [検索の構成](#)
- [スーパー・ユーザー、ゲスト・ユーザーおよびプロキシ・ユーザーの管理](#)
- [デバッグ・ロギング・レベルの設定](#)
- [監査ログの使用方法](#)
- [アクティブ・サーバー・インスタンスの情報の表示](#)
- [Oracle データ・サーバー接続時のパスワードの変更](#)

**関連項目：** Directory Server インスタンスの起動および停止方法は、[第 3 章「事前に実行する作業」](#)を参照してください。

## サーバーの構成設定エントリの管理

**OID 制御ユーティリティ**を使用して Oracle Directory Server 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。

### 関連項目：

- 構成設定エントリの概要は、2-21 ページの「**構成設定エントリ**」を参照してください。
- OID 制御ユーティリティを使用したサーバーの起動方法は、3-3 ページの「**タスク 2: サーバー・インスタンスの起動**」を参照してください。

この項では、次の項目について説明します。

- **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**

## 事前の考慮事項

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

実行しているサーバーのインスタンスすべてに対しては有効ではない値を変更するときは、構成設定エントリを新規に作成することをお勧めします。この方法は、リリース 2.1.1 では Oracle Directory Server インスタンスにのみ適用されます。このリリースでは、Oracle Replication Directory Server 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、Directory Server の別のインスタンスを設定できます。この値を使用するユーザーを限定する場合は、新規の構成設定エントリを設定し、特別なニーズを持つグループ用に、その構成設定エントリを示す個別のサーバー・インスタンスを実行してください。



図 5-1 は、それぞれ異なる値を持つ、3 つの Directory Server インスタンスを示しています。

図 5-1 複数の構成設定エントリを示すディレクトリ・エントリ階層

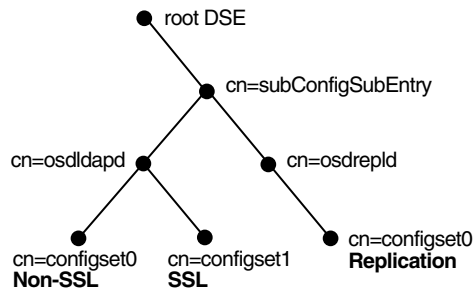


図 5-1 は、次のものを表しています。

- 次のインスタンスを含む Oracle Directory Server (cn=osdldap)
  - デフォルト・ポートでリスニングし、SSL がオフ状態の configset0 を使用している 1 つのインスタンス
  - SSL ポートでリスニングし、SSL がオン状態の configset1 を使用している 2 番目のインスタンス
- configset0 を使用している Replication Server インスタンス (cn=osdrepId)

#### 関連項目：

- SSL の構成パラメータの詳細は、第 8 章「[Secure Sockets Layer \(SSL\) の管理](#)」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 10 章「[ディレクトリ・レプリケーションの管理](#)」を参照してください。
- Directory Server の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および説明は、E-4 ページの「[構成設定エントリの属性](#)」を参照してください。

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

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

---

**重要：** アクティブ・インスタンスのパラメータを直接変更することはできません。構成設定エントリ内のパラメータを変更し、そのエントリを保存する必要があります。構成設定エントリの保存後に、OID 制御ユーティリティの `restart` コマンドを使用して現行の Oracle Directory Server インスタンスの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。

Directory Server インスタンスを再起動する方法は、3-8 ページの「[タスク 3: デフォルト・セキュリティ構成の再設定](#)」を参照してください。

---

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

構成設定エントリを表示する手順は、次のとおりです。

1. ナビゲータ・ペインで、「Oracle Internet Directory Servers」 > 「*directory server instance*」 > 「Server Management」の順に展開し、「Directory Server」または「Replication Server」を選択します。アクティブ・インスタンスのパラメータが、右側のペインに表示されます。
2. 右側のペインで、特定のインスタンスをダブル・クリックします。「Server Process」ダイアログ・ボックスが表示されます。

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

**関連項目：** 5-8 ページ「[Oracle Directory Manager を使用した構成設定エントリの変更](#)」

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

初めて構成設定エントリを追加するときには、次の操作が可能です。

- デフォルトの構成設定をテンプレートとして使用できます。以降は、作成した構成設定エントリからコピーして、別の構成設定を作成できます。
- 既存の構成設定エントリからコピーせずに、新規に追加できます。

**デフォルトの構成設定からのコピーによる構成設定エントリの追加** デフォルトの構成設定エントリのコピーで構成設定エントリを追加する手順は、次のとおりです。

1. ナビゲータ・ペインで、「Oracle Internet Directory Servers」 > 「*directory server instance*」 > 「Server Management」 > 「Directory Server」の順に展開し、「Default Configuration Set」を選択します。
2. ツールバーの「Create Like」ボタンをクリックします。「Configuration Sets」ダイアログ・ボックスに「General」タブが表示されます。
3. 次の表の説明に従って、各フィールドに情報を入力します。

フィールド	説明
Max. Number of DB Connections	1 つの Directory Server 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。
Number of Child Processes	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。
Set	構成設定エントリの番号を入力します。デフォルトの構成設定は 0 (ゼロ) です。異なる構成設定を必要な数だけ設定できます。複数のインスタンスで同じパラメータを必要とする場合は、同一の構成設定を使用できます。設定番号は変更可能です。

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

フィールド	説明
SSL Enable	SSL 認証を使用可能にするときに選択します。このチェック・ボックスを選択しない場合、SSL は使用されないため、このページの他のパラメータを設定する必要はありません。
SSL Authentication	次の中から 1 つ選択します。 <ul style="list-style-type: none"> <li>■ No SSL Authentication: 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。</li> <li>■ SSL Client and Server Authentication: 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。</li> <li>■ SSL Server Authentication: Directory Server のみ、クライアントに対して自己認証を行います。Directory Server 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。</li> </ul>

フィールド	説明
SSL Wallet URL	SSL Wallet の位置を入力します。Oracle Wallet の位置を変更する場合は、このパラメータを変更する必要があります。クライアントとサーバーの両方で Wallet の位置を設定する必要があります。たとえば Solaris では、このパラメータは次のように設定します。  orclsslwalleturl=file:/Home/my_dir/my_wallet  Windows NT では、このパラメータは次のように設定します。  file:C:¥my_dir¥my_wallet
SSL Wallet Password	サーバー側 Wallet のパスワードを入力します。このパスワードは、Wallet の作成時に設定されています。パスワードを変更する場合は、このパラメータを変更する必要があります。
SSL Wallet Confirm Password	パスワードを変更するときは、このフィールドに新規パスワードを再度入力します。
SSL Port	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。

**関連項目：** Oracle Wallet の位置と Oracle Wallet のパスワードの設定は、[付録 C](#) を参照してください。

5. 「Apply」をクリックします。

**注意：** アクティブ Directory Server 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ないことに注意してください。3-7 ページの「[Directory Server インスタンスの再起動](#)」を参照してください。

**関連項目：** 5-22 ページ「[OID 制御ユーティリティを使用したデバッグ・ロギング・レベルの設定](#)」

**既存の構成設定からのコピーによらない構成設定エントリの追加** 既存の構成設定からコピーせずに、新しい構成設定エントリを作成する手順は、次のとおりです。

1. ナビゲータ・ペインで、「Oracle Internet Directory Servers」 > 「*directory server instance*」 > 「Server Management」 > 「Directory Server」の順に展開し、「Default Configuration Set」を選択します。

2. ツールバーの「Create」ボタンをクリックします。「Configuration Sets」ダイアログ・ボックスに「General」タブ・ページが表示されます。次の表の説明に従って、フィールドに値を入力します。

フィールド	説明
Max. Number of DB Connections	1 つの Directory Server 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。
Number of Child Processes	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。
Set	構成設定エントリの番号を入力します。デフォルトの構成設定は 0 (ゼロ) です。異なる構成設定を必要な数だけ設定できます。複数のインスタンスで同じパラメータを必要とする場合は、同一の構成設定を使用できます。設定番号は変更可能です。

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

フィールド	説明
SSL Enable	SSL 認証を使用可能にするときに選択します。このチェック・ボックスを選択しない場合、SSL は使用されないため、このページの他のパラメータを設定する必要はありません。
SSL Authentication	次の中から 1 つ選択します。 <ul style="list-style-type: none"> <li>■ No SSL Authentication: 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。</li> <li>■ SSL Client and Server Authentication: 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。</li> <li>■ SSL Server Authentication: Directory Server のみ、クライアントに対して自己認証を行います。Directory Server 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。</li> </ul>
SSL Wallet URL	SSL Wallet の位置を入力します。Oracle Wallet の位置を変更する場合は、このパラメータを変更する必要があります。クライアントとサーバーの両方で Wallet の位置を設定する必要があります。たとえば Solaris では、このパラメータは次のように設定します。 <pre>orclsslwalleturl=file:/Home/my_dir/my_wallet</pre> <p>Windows NT では、このパラメータは次のように設定します。</p> <pre>file:C:¥my_dir¥my_wallet</pre>

フィールド	説明
SSL Wallet Password	サーバー側 Wallet のパスワードを入力します。このパスワードは、Wallet の作成時に設定されています。パスワードを変更する場合は、このパラメータを変更する必要があります。
SSL Wallet Confirm Password	パスワードを変更するときは、このフィールドに新規パスワードを再度入力します。
SSL Port	デフォルトの SSL ポートは 636 です。SSL ポートは変更できます。

4. 「OK」をクリックします。

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

構成設定エントリを変更する手順は、次のとおりです。

- ナビゲータ・ペインで、「Oracle Internet Directory Servers」 > 「*directory server instance*」 > 「Server Management」 > 「Directory Server」の順に展開し、変更する構成設定エントリを選択します。右側のペインのタブ・ページに、構成設定が表示されます。

次の表の説明に従って、「General」タブのフィールドの値を変更します。

フィールド	説明
Max. Number of DB Connections	1 つの Directory Server 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。
Number of Child Processes	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。
Set	構成設定エントリの番号を入力します。デフォルトの構成設定は 0（ゼロ）です。異なる構成設定を必要な数だけ設定できます。複数のインスタンスで同じパラメータを必要とする場合は、同一の構成設定を使用できます。設定番号は変更可能です。

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

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

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

フィールド	説明
SSL Authentication	<p>次の中から 1 つ選択します。</p> <ul style="list-style-type: none"> <li>■ No SSL Authentication: 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。</li> <li>■ SSL Client and Server Authentication: 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。</li> <li>■ SSL Server Authentication: Directory Server のみ、クライアントに対して自己認証を行います。Directory Server 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。</li> </ul>
SSL Wallet URL	<p>SSL Wallet の位置を入力します。Oracle Wallet の位置を変更する場合は、このパラメータを変更する必要があります。クライアントとサーバーの両方で Wallet の位置を設定する必要があります。たとえば Solaris では、このパラメータは次のように設定します。</p> <pre>orclsslwalleturl=file:/Home/my_dir/my_wallet</pre> <p>Windows NT では、このパラメータは次のように設定します。</p> <pre>file:C:¥my_dir¥my_wallet</pre>
SSL Wallet Password	<p>サーバー側 Wallet のパスワードを入力します。このパスワードは、Wallet の作成時に設定されています。パスワードを変更する場合は、このパラメータを変更する必要があります。</p>
SSL Wallet Confirm Password	<p>パスワードを変更するときは、このフィールドに新規パスワードを再度入力します。</p>
SSL Port	<p>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。</p>

3. 新規構成設定エントリ用に設定した各パラメータを確認した後、「Apply」をクリックします。
4. コマンドを有効にするために、サーバー・インスタンスを再起動します。

---

**注意：** アクティブ・Directory Server インスタンスは、再起動しなければその変更内容が適用されません。3-7 ページの「[Directory Server インスタンスの再起動](#)」を参照してください。

---

**関連項目：** Oracle Wallet の位置と Oracle Wallet のパスワードの設定は、[付録 C](#) 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、「Server Management」>「Directory Server」の順に展開します。
2. ナビゲータ・ペインで、削除する構成設定エントリを選択します。
3. ツールバーの「Delete」ボタンをクリックします。

---

**注意：** アクティブ・Directory Server インスタンスは、再起動しなければその変更内容が適用されません。3-7 ページの「[Directory Server インスタンスの再起動](#)」を参照してください。

---

## コマンドライン・ツールを使用したサーバー構成設定エントリの管理

構成設定エントリの変更には Oracle Directory Manager を使用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 Directory Server に同じ変更を加える場合などがそうです。

コマンドライン・ツールを使用して構成設定エントリを追加または変更する場合、新規構成設定エントリの追加用の入力ファイルは、[LDAP データ交換フォーマット \(LDIF\)](#) 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。Directory Server は、新規構成設定エントリに設定された属性値で、該当する属性の既存値をオーバーライドします。

**関連項目：** LDIF の詳細は、A-2 ページの「[LDAP データ交換フォーマット \(LDIF\) の構文](#)」を参照してください。

## ldapadd を使用した構成設定エントリの追加

新しい Oracle Directory Server 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、または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 形式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 RDN（ローカル名）、Wallet の位置は /HOME/test/wallet、Wallet パスワードは welcome です。

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

## 2. 入力ファイルを使用して ldapadd を実行します。

コマンド・プロンプトで、入力ファイルを追加するコマンドを入力します。前述の例のファイル名が newconfigs の場合、ldapadd コマンドは次のようになります。

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

### 関連項目：

- A-2 ページ「[LDAP データ交換フォーマット（LDIF）の構文](#)」
- このコマンドで使用できるオプションの詳細リストは、A-4 ページの「[ldapadd 構文](#)」を参照してください。
- 構成設定エントリの属性の説明は、E-4 ページの「[構成設定エントリの属性](#)」を参照してください。

## ldapmodify を使用した構成設定エントリの変更と削除

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

### 1. 入力ファイルを作成します。

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

入力ファイルは LDIF 形式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=osldlapd,cn=subconfigsubentry が、既存の構成設定エントリの DN（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=osldlapd,cn=subconfigsubentry
changetype: modify
replace: orclsslport
orclsslport: 7000
```

2. 入力ファイルを参照する ldapmodify を実行します。

コマンド・プロンプトで、入力ファイルを参照するコマンドを入力します。たとえば、入力ファイルの名前が configfile の場合、ldapmodify コマンドは次のようになります。

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

### 関連項目：

- A-2 ページ [「LDAP データ交換フォーマット \(LDIF\) の構文」](#)
- ldapmodify の詳細とそのオプションのリストは、A-12 ページの [「ldapmodify 構文」](#) を参照してください。
- 構成設定エントリの属性の説明は、E-4 ページの [「構成設定エントリの属性」](#) を参照してください。

## システム操作属性の設定

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

この項では、次の項目について説明します。

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

### 関連項目： 2-4 ページ [「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 Directory Server 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 Servers」を展開して、サーバーを選択します。右側のペインにシステム操作属性が表示されます。

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

フィールド	説明	デフォルト値	変更可能？
Configuration Set Location	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 (DN)。	cn=subconfigsubentry	いいえ
Indexed Attribute Locations	すべての索引付き属性を含むエントリの DN。	cn=catalogs	いいえ
Oracle Directory Version	使用している OID のバージョンおよびリリース。	2.1.1.0.0	いいえ
Password Encryption	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。 <ul style="list-style-type: none"> <li>■ <b>MD4</b></li> <li>■ <b>MD5</b></li> <li>■ No Encrypsion</li> <li>■ <b>SHA</b></li> <li>■ <b>UNIX Crypt</b></li> </ul>	MD4	はい
Process Instance Location	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 DN。	cn=subschemasubentry	いいえ
Query Entry Return Limit	検索で戻されるエントリの最大数。	1000	はい
Replication Agreements	レプリケーション承諾を保持しているエントリの DN。	cn=orclareplagreements	いいえ
Replication Log Location	このサーバーに変更ログを保持しているエントリの DN。	cn=changelog	いいえ
Replication Status Location	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 DN。	cn=changestatus	いいえ
Schema Definition Location	スキーマの DN。	cn=subschemasubentry	いいえ

フィールド	説明	デフォルト値	変更可能？
Server Mode	サーバーにデータを書き込むことができるかどうかを指定します。レプリケーション時はデフォルトを「Read - Only」に変更してください。	Read/Write	選択肢は「Read/Write」および「Read-Only」です。
Server Operation Time Limit	検索の最大実行時間（秒）。	3600	はい

ldapmodify を使用したシステム操作属性の設定

変更可能なシステム操作属性は、次のとおりです。

属性	説明	デフォルト
namingContexts	このサーバーに格納されているネーミング・コンテキストの最上位識別名（DN）。ネーミング・コンテキストとして DN 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。	none
orclCryptoScheme	パスワードを暗号化するハッシュ・アルゴリズム。オプションは次のとおりです。 <ul style="list-style-type: none"><li>MD4</li><li>MD5</li><li>No Encryption</li><li>SHA</li><li>UNIX Crypt</li></ul>	MD4
orclSizeLimit	検索で戻されるエントリの最大数。	1000
orclServerMode	サーバーにデータを書き込むことができるかどうかを指定します。レプリケーション時は、デフォルトを「Read-Only」に変更してください。	Read/Write
orclTimeLimit	検索の最大実行時間（秒）。	3600

**関連項目：** ldapmodify の詳細とそのオプションのリストは、A-12 ページの「[ldapmodify 構文](#)」を参照してください。

## ネーミング・コンテキストの管理

ユーザーが特定のネーミング・コンテキストを検索できるように、それらのネーミング・コンテキストを公開できます。そのためには、各ネーミング・コンテキストの最上位エントリを、ルート DSE の `namingContexts` 属性の値として指定します。

たとえば、3 つの主なネーミング・コンテキストを持った DIT 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・コンテキストに絞込むなど、検索条件を詳細に指定できます。

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

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

ネーミング・コンテキストを公開する前に、次のことを確認してください。

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

この項では、次の項目について説明します。

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

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

1. ナビゲータ・ペインで、「Oracle Internet Directory Servers」を展開して、ネーミング・コンテキストを指定する Directory Server を選択します。その Directory Server 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. 「System Operational Attributes」タブ・ページの「Naming Contexts」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 DN を入力します。「Browse」をクリックして検索ウィンドウを開くこともできます。
3. 「Apply」をクリックします。

## Idapmodify を使用したネーミング・コンテキストの公開

次の例の入力ファイルは、ネーミング・コンテキストとしてエントリ `c=uk` を指定しています。

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

## パスワード暗号化の管理

インストール時に、パスワードの暗号化スキームの設定を要求されたはずですが。その初期構成を変更するには、Oracle Directory Manager または `Idapmodify` のいずれかを使用します。パスワード暗号化のタイプを変更するには、スーパー・ユーザーである必要があります。この項では、次の項目について説明します。

- [Oracle Directory Manager を使用したパスワード暗号化の管理](#)
- [Idapmodify を使用したパスワード暗号化の管理](#)

## Oracle Directory Manager を使用したパスワード暗号化の管理

Oracle Directory Manager を使用してパスワード暗号化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 Servers」を展開して、パスワード暗号化をリセットする Directory Server インスタンスを選択します。その Directory Server 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. 「System Operational Attributes」タブ・ページの「Password Encryption」フィールドで、使用するパスワード暗号化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](#)
  - No Encryption
  - [SHA](#)
  - [UNIX Crypt](#)
3. 「Apply」をクリックします。

## ldapmodify を使用したパスワード暗号化の管理

次の例では、パスワード暗号化アルゴリズムは SHA に変更されます。

```
ldapmodify -h myhost -p 389 -v <<EOF
dn:
changetype: modify
replace: orclcryptoscheme
orclcryptoscheme: SHA
EOF
```

**関連項目：** 2-16 ページ [「パスワード暗号化」](#)

## 検索の構成

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

この項では、次の項目について説明します。

- [Oracle Directory Manager を使用した検索の構成](#)
- [ldapmodify を使用した検索の構成](#)

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

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

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

1. ナビゲータ・ペインで、「Oracle Internet Directory Servers」を展開して、Directory Server 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. 「System Operational Attributes」タブ・ページの「Query Entry Return Limit」フィールドに、検索によって戻されるエントリの最大数を入力します。デフォルトは 1000（ゼロ）です。
3. 「Apply」をクリックします。

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

1. ナビゲータ・ペインで、「Oracle Internet Directory Servers」を展開して、Directory Server 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. 「System Operational Attributes」タブ・ページの「Server Operation Time Limit」フィールドに、検索の完了までの最大秒数を入力します。デフォルトは 3600（ゼロ）です。
3. 「Apply」をクリックします。

## ldapmodify を使用した検索の構成

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

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

次の例では、検索で戻されるエントリの最大数を 500 に変更します。

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

### ldapmodify を使用した、検索の最大時間の設定

次の例では、検索の最大時間を 2400 に変更します。

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

**関連項目：** A-12 ページ [「ldapmodify 構文」](#)



## スーパー・ユーザー、ゲスト・ユーザーおよびプロキシ・ユーザーの管理

**スーパー・ユーザー**は、一般的にはディレクトリ情報へのあらゆるアクセスが可能な、特別なディレクトリ管理者です。

**ゲスト・ユーザー**は、匿名ユーザーではなく、特定のユーザー・エントリも持っていないユーザーです。

**プロキシ・ユーザー**は通常、ファイアウォールなどの中間層を備えた環境で使用されます。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います。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しますが、このログインはプロキシ・ユーザーで行われます。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 に切り替えます。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します。

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

---

---

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

---

---

**関連項目：** アクセス権限の設定方法は、第9章「ディレクトリのアクセス制御の管理」を参照してください。

この項では、次の項目について説明します。

- [Oracle Directory Manager を使用したユーザー名とパスワードの管理](#)
- [ldapmodify を使用したユーザー名とパスワードの管理](#)

## Oracle Directory Manager を使用したユーザー名とパスワードの管理

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

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 Oracle Directory Manager を使用して変更する手順は、次のとおりです。

1. ナビゲータ・ペインで「Oracle Internet Directory Servers」を展開します。
2. サーバーを選択します。そのサーバーに対応するタブ・ページが右側のペインに表示されます。
3. 「Passwords」タブを選択します。このページに、各タイプのユーザーに対するカレント・ユーザー名とパスワードが表示されます。各パスワードは、パスワードのフィールドには表示されないことに注意してください。

次の表は、「Passwords」タブ・ページのフィールドのリストと説明です。

フィールド	説明
Super User Name	スーパー・ユーザーの名前を入力します。デフォルトは cn=orcladmin です。
Super User Password	スーパー・ユーザーのパスワードを入力します。デフォルトは welcome です。このパスワードはすぐに変更してください。
Guest Login Name	ゲスト・ログイン名を入力します。ゲストには、そのディレクトリ内の <b>Access Control Policy Point (ACP) (ACP)</b> で指定されている権限が与えられます。デフォルトは cn=guest です。
Guest Login Password	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。
Proxy Login Name	プロキシ・ログイン名を入力します。プロキシ・ユーザーには、そのディレクトリ内の ACP で指定されている権限が与えられます。デフォルトは cn=proxy です。
Proxy Login Password	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。

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

# ldapmodify を使用したユーザー名とパスワードの管理

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

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

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

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

**関連項目：** ldapmodify の構文と使用方法は、A-12 ページの「[ldapmodify 構文](#)」を参照してください。

## デバッグ・ロギング・レベルの設定

**Oracle Directory Manager** または **OID 制御ユーティリティ** を使用して、デバッグ・ロギング・レベルを設定できます。

この項では、次の項目について説明します。

- **Oracle Directory Manager** を使用したデバッグ・ロギング・レベルの設定
- **OID 制御ユーティリティ** を使用したデバッグ・ロギング・レベルの設定

### Oracle Directory Manager を使用したデバッグ・ロギング・レベルの設定

1. ナビゲータ・ペインで、「Oracle Internet Directory Servers」を展開して、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. 「Debug Flags」タブを選択します。

通常、このタブ・ページのチェックボックスは選択する必要がありません。ただし、特定の問題に関するログを生成するには、このタブ・ページでデバッグ・ロギング・レベルを指定します。

### OID 制御ユーティリティを使用したデバッグ・ロギング・レベルの設定

OID 制御ユーティリティを使用してデバッグ・ロギング・レベルを設定するには、LDAP サーバーの場合は `-debug` オプションを、Replication Server の場合は `-d` フラグを使用して、Oracle Directory Server を再起動します。表 5-1 に基づいて、デバッグ・レベルの数値を設定します。

デバッグ・レベルは加算方式であるため、アクティブにする機能を表す数値を合計し、その合計値をコマンドライン・オプションに使用する必要があります。

デフォルトでは、デバッグ・ログは記録されません。デバッグ・ログを記録するには、**DSE** 属性 `orcldebugflag` を必要なレベルに変更します。デバッグ・レベルは、次のレベルのいずれかに構成できます。

OID 制御ユーティリティによって生成されたデバッグ・ログ・ファイルを見るには、`$ORACLE_HOME/ldap/log` にナビゲートします。

表 5-1 は、デバッグ・ロギング・レベルの全リストです。

**表 5-1 デバッグ・ロギング・レベル**

ロギング・レベルの値	機能
1	ファンクション・コールのトレース
2	パケット・ハンドリングのデバッグ
4	大容量トレースのデバッグ
8	接続管理
16	送受信パケットの印刷
32	検索フィルタの処理
64	構成ファイルの処理
128	アクセス制御リストの処理
256	接続 / 操作 / 結果の状態ログ
512	エントリ設定の状態ログ
1024	バックエンドでの通信の出力
2048	エントリ解析デバッグの出力
4096	スキーマ関連のデバッグ
32768	レプリケーション固有のデバッグ
65535	すべてのデバッグを使用可能にする

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

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

この例では、デバッグ・フラグを付けて、Oracle Directory Server と Oracle Directory Replication Server を再起動しています。

## 監査ログの使用法

監査ログには、Oracle Directory Server に関するセキュリティ上および操作上重要なイベントが記録されています。管理者は、`ldapsearch` コマンドを使用して監査ログを問合せできます。ログの生成はサーバーで発生するイベントに限られているため、Oracle Directory Server のみがログ・エントリを作成できます。[Oracle Directory Manager](#) またはコマンドライン・ツールのいずれかのみで監査ログ・エントリを追加できません。エントリを追加できるのはサーバーのみです。

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。各イベントごとに1つのエントリがあります。`ldapsearch` で検索基準を指定し、[Oracle Directory Manager](#) で監査ログを表示できます。

デフォルトでは、監査ログは記録されません。監査ログを記録するには、[DSE](#) 属性 `orclauditlevel` を必要なレベルに変更します。監査レベルは、選択したイベントのみを監査するように構成できます。

### 関連項目：

- 監査レベルのリストは、5-26 ページの「[監査可能なイベント](#)」を参照してください。
- 7-5 ページ「[Oracle Directory Manager を使用した監査ログ・エントリの検索](#)」
- 5-29 ページ「[ldapsearch を使用した監査ログ・エントリの検索](#)」
- A-21 ページ「[bulkdelete](#) 構文」

この項では、次の項目について説明します。

- [監査ログ・エントリの構造](#)
- [DIT における監査ログ・エントリの位置](#)
- [監査可能なイベント](#)
- [監査レベルの設定](#)
- [監査ログ・エントリの検索](#)
- [監査ログの削除](#)

## 監査ログ・エントリの構造

各監査ログ・エントリには、orclAuditoc [オブジェクト・クラス](#)が含まれています。他のすべての構造型オブジェクト・クラスと同様に、orclAuditoc は、top から属性を継承します。その属性は次のとおりです。

属性	説明
orclsequence	エントリ名の作成に使用されます。名前は、データベース順序を使用して生成されます。
orcleventtype	発生したイベントのタイプを指定します。この属性はカタログ化されています。
orcleventtime	イベントを発生させる時刻を指定します。時刻は、 <b>UTC (Coordinated Universal Time)</b> 形式です。UTC 形式であることは、値の最後の z によって示されます。たとえば、次のようになります。 orcleventtime: 199811281010z
orcluserdn	操作を実行するために Oracle Directory Server にログインしたユーザーの識別子を指定します。この属性はカタログ化されています。
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、通常の実験の結果セットには監査ログ・エントリが含まれません。たとえば、検索条件が objectclass=top の場合、監査ログ・エントリは結果として戻されません。検索のベースとして cn=auditlog を指定した場合のみ、監査ログ・エントリが検索できます。

---

**注意：** デフォルトでは、属性 orcleventtype と orcluserdn は、Oracle Internet Directory のインストール時に索引付けされています。これらの属性から索引を削除すると、この 2 つの属性の実験はできなくなります。索引を再作成するには、カタログ管理ツールを使用します。6-25 ページの「[コマンドライン・ツールを使用した属性の索引付け](#)」を参照してください。

---

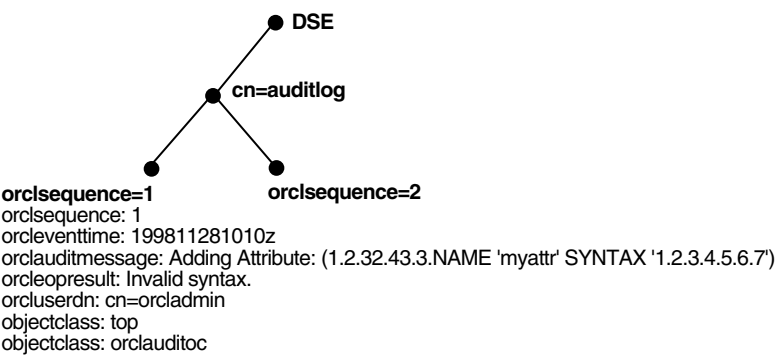
関連項目：

- カタログ化された属性については、A-27 ページの「[カタログ管理ツールの構文](#)」を参照してください。
- top の詳細は、2-8 ページの「[オブジェクト・クラスの型](#)」を参照してください。

DIT における監査ログ・エントリの位置

監査ログのコンテナは DSE の一部です。そのエントリは DSE の子として保持され、orclsequence 属性に従って構成されています。[図 5-2](#) を参照してください。

図 5-2 DSE 下のサンプル監査ログ



監査可能なイベント

次の表は、監査可能なイベントとその監査レベルを示しています。3 列目の「監査レベル」は 16 進の値です。複数のイベントを監査するには、この列のそれぞれのイベントに対応する値を加算します。

イベント	説明	監査レベル
Superuser login	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)	0 × 0001
Schema Element Add/Replace	新規スキーマ要素の追加 (成功と失敗)	0 × 0002
Schema element delete	スキーマの削除 (成功または失敗)	0 × 0004
Bind	バインドに失敗した例	0 × 0008



イベント	説明	監査レベル
Access violation	Access Control Policy Points (ACP) で否認されたアクセス	0 × 0010
DSE modification	DSE エントリに対する変更 (成功または失敗)	0 × 0020
Replication Login	Replication Server の認証 (成功または失敗)	0 × 0040
ACL Modification	ACL に対する変更	0 × 0080
User password modification	ユーザー・パスワード属性の変更	0 × 0100
Add	ldapadd 操作 (成功または失敗)	0 × 0200
Delete	ldapdelete 操作 (成功または失敗)	0 × 0400
Modify	ldapmodify 操作 (成功または失敗)	0 × 0800
ModifyDN	ldapModifyDN 操作 (成功または失敗)	0 × 1000

## 監査レベルの設定

前述の項で説明したイベントを監査するかどうかを設定できます。DSE 属性の `orclauditlevel` は、サーバーに設定されている現行の監査レベルを示します。属性の値が 0 (ゼロ) の場合は、いずれの監査も行われません。これがデフォルトです。

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。両方の使用方法について、この項で説明します。

### 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 Servers」を展開して、Directory Server インスタンスを選択します。
2. 右側のペインで、「Audit Mask Levels」タブ・ページを選択します。
3. 使用する監査レベルのチェック・ボックスを選択します。
4. 「Apply」をクリックします。

---

**注意：** アクティブ Directory Server インスタンスは、再起動しなければその変更内容が適用されません。3-7 ページの「[Directory Server インスタンスの再起動](#)」を参照してください。

---

**関連項目：** 各監査レベルの説明は、5-26 ページの「[監査可能なイベント](#)」を参照してください。

**ldapmodify を使用した監査レベルの設定**

複数のイベントを監査するには、その監査マスクの値を加算します。たとえば、次の3つのイベントを監査するとします。

イベント	監査レベル	値
Schema element delete	0 × 0004	4
DSE modification	0 × 0020	32
Add	0 × 0200	512
合計		548

監査レベルの合計値は 548 です。したがって、ldapmodify コマンドは、次のようになります。

```
ldapmodify -p port -h host << EOF
dn:
changetype:modify
replace: orclauditlevel
orclauditlevel: 548
EOF
```

orclauditlevel に変更を加えた場合は、変更内容を有効にするために Directory Server インスタンスを再起動してください。

**関連項目：** 3-8 ページ「[タスク 3: デフォルト・セキュリティ構成の再設定](#)」

## 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

参照： 7-5 ページ「[Oracle Directory Manager を使用した監査ログ・エントリの検索](#)」

### 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。

参照： A-17 ページ「[ldapsearch 構文](#)」

## 監査ログの削除

bulkdelete を使用して、コンテナ cn=auditlog の下の監査ログ・オブジェクトを削除できます。次のコマンドを実行します。

```
bulkdelete.sh -connect net_service_name -base "cn=auditlog"
```

## アクティブ・サーバー・インスタンスの情報の表示

**Oracle Directory Manager** を使用して、アクティブ・サーバー・インスタンスに関する情報を表示できます。この手順は、次のとおりです。

1. ナビゲータ・ペインで、「Oracle Internet Directory Servers」を展開して、サーバーを選択します。そのサーバー・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. 「Server Management」タブを選択すると、すべてのアクティブ・サーバー・インスタンスに対する基本的な情報（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. 特定のサーバー・インスタンスの構成パラメータを見るには、そのサーバーを選択します。
4. 「View Properties」をクリックします。「Server Process」ダイアログ・ボックスに、選択したサーバー・インスタンスの構成パラメータが表示されます。このダイアログ・ボックスでは、構成パラメータを変更できないことに注意してください。変更するには、基となっている構成設定エントリを変更する必要があります。

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

## Oracle データ・サーバー接続時のパスワードの変更

Oracle Internet Directory は、Oracle データベースへの接続時にパスワードを使用します。Oracle Internet Directory をインストールした時点では、このパスワードのデフォルトは ODS です。[OID データベース・パスワード・ユーティリティ](#)を使用すると、このパスワードを変更できます。

**関連項目：** A-35 ページ「[OID データベース・パスワード・ユーティリティの構文](#)」

---

## ディレクトリ・スキーマの管理

この章では、Oracle Internet Directory のオブジェクト・クラスと属性を管理する方法を説明します。

この章では、次の項目について説明します。

- [ディレクトリ・スキーマの概要](#)
- [オブジェクト・クラス管理](#)
- [Oracle Directory Manager を使用したオブジェクト・クラスの管理](#)
- [コマンドライン・ツールを使用したオブジェクト・クラスの管理](#)
- [属性管理の概要](#)
- [Oracle Directory Manager を使用した属性の管理](#)
- [コマンドライン・ツールを使用した属性の管理](#)

## ディレクトリ・スキーマの概要

ディレクトリ・スキーマには、次の特徴があります。

- ディレクトリに格納できるオブジェクトの種類に関する規則を含んでいます。
- 検索などの処理時に Directory Server 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、DIT 内でのデータの編成方法に関するすべての情報が含まれています。それらの情報には、属性の型、および適用される構文と一致規則が含まれます。オブジェクト・クラスと呼ばれる、属性の様々なグループ化も含まれています。

この章では、これらの各要素について説明します。

**関連項目：** 2-10 ページ「[ディレクトリ・スキーマ](#)」

## オブジェクト・クラス管理

この項では、[オブジェクト・クラス](#)の追加方法と変更方法を説明します。ディレクトリ内のベース・スキーマの追加または変更を行う前に、ディレクトリのコンポーネントの基本概念を理解しておいてください。

**関連項目：**

- オブジェクト・クラスの概要は、2-7 ページの「[オブジェクト・クラス](#)」を参照してください。
- Oracle Internet Directory とともにインストールされるスキーマ・コンポーネントのリストは、[付録 E「スキーマ要素」](#)を参照してください。

この項では、次の項目について説明します。

- [オブジェクト・クラスの追加のガイドライン](#)
- [オブジェクト・クラスの変更のガイドライン](#)
- [オブジェクト・クラスの削除のガイドライン](#)

## オブジェクト・クラスの追加のガイドライン

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

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

---

**注意：** Oracle Internet Directory のスキーマ・オブジェクトには、それぞれ特定の制限があります。たとえば、一部のオブジェクトは変更できません。これらの制限事項は、ここでは制約や規則として説明しています。

---

エントリがオブジェクト・クラスから**継承**する属性は、必須またはオプションのいずれであってもかまいません。オプション属性は、必ずしもディレクトリ・エントリに存在している必要はありません。

オブジェクト・クラスに対して、属性が必須であるか、オプションであるかを指定できます。ただし、この指定は、そのオブジェクト・クラスにのみバインドされます。同じ属性を別のオブジェクト・クラスに割り当てる場合は、そのオブジェクト・クラスに対して必須であるか、オプションであるかを指定し直すことができます。次の操作が可能です。

- 既存の標準オブジェクト・クラスからの選択
- 標準以外の新規オブジェクト・クラスの追加と既存属性の割当て
- 既存のオブジェクト・クラスの変更、異なる属性のセットへの割当て
- 既存の属性の追加と変更

**関連項目：** 6-14 ページ「[属性管理の概要](#)」

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

エントリに操作を追加または実行する場合、そのエントリに対応付けられたスーパークラスの階層全体を指定する必要はありません。オブジェクト・クラスの増加と呼ばれるこの機能によって、リーフ・オブジェクト・クラスの指定のみで済みます。Oracle Internet Directory は、リーフ・オブジェクト・クラスの階層を解決して、情報モデル制約を規定します。たとえば、inetOrgPerson オブジェクト・クラスは、そのスーパークラスとして、top、

person および organizationalPerson を持っています。ある人物のエントリを表わすエントリを作成する場合、オブジェクト・クラスとして指定する必要があるのは inetOrgPerson のみです。Oracle Internet Directory は、対応するスーパークラス、すなわち top、person および organizationalPerson によって定義されたスキーマ制約を規定します。

オブジェクト・クラスを追加するときは、次のガイドラインに注意してください。

- すべての構造型オブジェクト・クラスには、スーパー・クラスとして top を設定する必要があります。
- オブジェクト・クラスの名前とオブジェクト ID は、すべてのスキーマ・コンポーネントを通して一意であることが必要です。
- オブジェクト・クラスで参照されるスキーマ・コンポーネント（スーパー・クラスなど）は、すでに存在している必要があります。
- 抽象型オブジェクト・クラスの場合は、スーパー・クラスも抽象型であることが必要です。
- スーパー・クラスの必須属性は、新規オブジェクト・クラスでオプション属性に再定義することが可能です。同様に、スーパー・クラスのオプション属性は、新規オブジェクト・クラスで必須属性に再定義できます。

**関連項目：** これらの用語の概念の説明は、2-8 ページの「[サブクラス、スーパー・クラスおよび継承](#)」を参照してください。

## オブジェクト・クラスの変更のガイドライン

この項では、既存のオブジェクト・クラスに対して実行できる変更のタイプについて説明します。変更は、Oracle Directory Manager およびコマンドライン・ツールを使用して実行できます。

オブジェクト・クラスに対しては、次の変更を実行できます。

- 必須属性からオプション属性への変更
- オプション属性の追加
- スーパー・クラスの追加
- 抽象型オブジェクト・クラスから構造型または補助型オブジェクト・クラスへの変換（その抽象型オブジェクト・クラスが、別の抽象型オブジェクト・クラスのスーパー・クラスではない場合）



オブジェクト・クラスを変更するときは、次のガイドラインに注意してください。

- 標準の LDAP スキーマの一部であるオブジェクト・クラスは変更できません。ユーザー定義のオブジェクト・クラスは変更できます。また、必要な属性が既存のオブジェクト・クラスに設定されていない場合は、補助型オブジェクト・クラスを作成して、必要な属性を関連付けることができます。
- 既存のオブジェクト・クラスに、必須属性を追加できません。
- ベース・スキーマのオブジェクト・クラスは変更できません。
- 既存のオブジェクト・クラスから属性またはスーパー・クラスを削除できません。
- 構造型オブジェクト・クラスは、他の型のオブジェクト・クラスに変換できません。
- エントリがすでに関連付けられているオブジェクト・クラスは変更しないでください。

**関連項目：**

- 6-6 ページ「[Oracle Directory Manager を使用したオブジェクト・クラスの管理](#)」
- 6-12 ページ「[コマンドライン・ツールを使用したオブジェクト・クラスの管理](#)」

## オブジェクト・クラスの削除のガイドライン

オブジェクト・クラスの削除に関しても、いくつかの制限事項があります。

- ベース・スキーマからオブジェクト・クラスを削除できません。
- ベース・スキーマ内にないオブジェクト・クラスは、他のスキーマ・コンポーネントから直接または間接的に参照されていない限り削除できます。たとえば、このようなオブジェクト・クラスを参照するディレクトリ・エントリがいくつか存在するとします。このオブジェクト・クラスを削除すると、これらのエントリにはアクセスできなくなります。

---

**注意：** Oracle Internet Directory は、前述の規則を強制していません。ここでは、ガイドラインとして紹介します。

---

# Oracle Directory Manager を使用したオブジェクト・クラスの管理

この項では、次の項目について説明します。

- [Oracle Directory Manager を使用したオブジェクト・クラスの検索](#)
- [Oracle Directory Manager を使用したオブジェクト・クラスのプロパティの表示](#)
- [Oracle Directory Manager を使用したオブジェクト・クラスの追加](#)
- [Oracle Directory Manager を使用したオブジェクト・クラスの変更](#)
- [Oracle Directory Manager を使用したオブジェクト・クラスの削除](#)

## Oracle Directory Manager を使用したオブジェクト・クラスの検索

次の方法でオブジェクト・クラスを検索できます。

- オブジェクト・クラスのプロパティを選択する方法。たとえば、名前やオブジェクト ID 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。「Begins With」または「Exactly Matches」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「Schema Management」を選択します。「Schema Management」タブ・ページが、右側のペインに表示されます。
2. 右側のペインの右下の「Find Object Classes」ボタンをクリックするか、またはメニュー・バーから「Edit」>「Find Object Classes」をクリックします。「Find: Object Classes」ダイアログ・ボックスが表示されます。
3. 検索基準バーの一番左のメニューから、検索するオブジェクト・クラスのプロパティを選択します。オプションは次のとおりです。

オプション	説明
Name	検索するオブジェクト・クラスの名前。たとえば、「Name」「Exact Match」「subAc1」と指定すると、subAc1 オブジェクト・クラスを検索できます。
Object ID	検索するオブジェクト・クラスのオブジェクト ID。たとえば、「Object ID」「Begins With」「2.5.2」と指定すると、オブジェクト ID が 2.5.2 で始まるオブジェクト・クラスのリストが表示されます。

オプション	説明
Description	「Description」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。
Type	検索するオブジェクト・クラスの型。「Abstract」、「Structural」または「Auxiliary」のいずれかを指定します。
Super Class	検索するオブジェクト・クラスのスーパー・クラス。
Mandatory Attributes	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。
Optional Attributes	検索するオブジェクト・クラスのオプション属性。

---

**注意：** 各オブジェクト・クラスでは、すべての属性が使用されているわけではありません。指定する属性が、探しているオブジェクト・クラス内の属性と実際に一致していることを確認してください。一致する属性がない場合は、検索に失敗します。

---

4. 検索基準バーの一番右のテキスト・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。
5. 検索基準バーの中央のメニューから、検索に使用するフィルタを選択します。オプションは次のとおりです。

フィルタ	説明
Begins With	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、「Type」「Begins With」「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。
Ends With	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、「Type」「Ends With」「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。
Contains	値の位置を限定せずに、ユーザーの入力値が選択したプロパティに含まれているオブジェクト・クラスを検索します。たとえば、「Optional Attributes」「Contains」「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。

フィルタ	説明
Exact Match	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、「Super Class」「Exact Match」「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。
Greater Or Equal	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大か等しいオブジェクト・クラスを検索します。たとえば、「Name」「Greater or Equal」「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。
Less or Equal	選択したプロパティが数値順またはアルファベット順で入力値より小か等しいオブジェクト・クラスを検索します。たとえば、「Name」「Less or Equal」「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。
Not Null	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、「Mandatory Attributes」「Not Null」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。

6. 「Search Criteria」フィールドの下に、次の表で説明する 5 つのボタンがあります。これらのボタンを使用すると、検索基準をさらに詳細に指定できます。

ボタン	説明
New	「Search Criteria」フィールドに、新しい検索基準バーを作成します。このボタンは、検索基準バーが削除されている場合にのみ使用可能です。
And	「Search Criteria」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	「Search Criteria」フィールドに、別の検索基準バーを作成します。指定した 2 つの属性のいずれかを持つオブジェクト・クラスをすべて検索します。
Not	選択した検索基準バーの基準を除外し、指定した基準を満たさないオブジェクト・クラスをすべて取り出します。
Delete	選択した検索基準バーを削除します。

7. 「Search」をクリックします。検索結果が、「Find: Object Class」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「Schema Management」を展開します。「Schema Management」ペインにある各タブに、スキーマの次のコンポーネントが表示されます。

- Object Classes
- Attributes
- Syntaxes
- Matching Rules

2. 右側のペインで、「Object Classes」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、「Object Classes」タブ・ページのオブジェクト・クラスをクリックします。選択したオブジェクト・クラスのプロパティが、「Object Class」ダイアログ・ボックスに表示されます。

3. 「Object Class」ダイアログ・ボックスは、次のとおりです。

- 属性の継承元のオブジェクト・クラスが「Super Class」ボックスにリストされます。
- 必須属性が「Mandatory Attributes」ボックスにリストされます。
- オプション属性が「Optional Attributes」ボックスにリストされます。

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

## Oracle Directory Manager を使用したオブジェクト・クラスの追加

Oracle Directory Manager を使用してオブジェクト・クラスを追加する手順は、次のとおりです。

1. ナビゲータ・ペインで、「Oracle Internet Directory Servers」 > 「*directory server*」の順に展開し、「Schema Management」を選択します。

2. 次のいずれかの方法を選択します。

- 右側のペインで「Object Classes」タブを選択し、ツールバーの「Create」ボタンをクリックします。
- 右側のペインの下「Create」ボタンをクリックします。
- 「Operations」メニューから、「Create Object Class」を選択します。

「New Object Class」ダイアログ・ボックスが表示されます。

作成するオブジェクト・クラスに類似しているオブジェクト・クラスを選択して、「Create Like」をクリックする方法もあります。ダイアログ・ボックスが表示され、選択

したオブジェクト・クラスの属性が表示されます。選択したオブジェクト・クラスをテンプレートとして使用して、新規のオブジェクト・クラスを作成できます。

3. 次の表に説明されている各フィールドに、情報を入力します。

フィールド	説明
Name	作成するオブジェクト・クラスの名前を入力します。
Object ID	オブジェクト識別子を入力します。これは、IETF 規格に基づいた、標準化された数値順序です。一意、かつ組織内に設定されたシステムに準拠したものである必要があります。通常この値は、ANSI または ISO など、登録機関によって割り当てられた ID から導出されます。
Description	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。
Type	オブジェクト・クラスの型を指定します。「Abstract」、「Structural」、「Auxiliary」、「None」のいずれかを指定します。
Super Class	このオブジェクト・クラスを導出するクラスを指定します。このオブジェクト・クラスは、選択したスーパー・クラスの属性をすべて継承します。構造型オブジェクト・クラスの場合は、そのスーパー・クラスの 1 つとして必ず top を設定する必要があります。「Add」をクリックすると「Super Class Selector」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。
Mandatory Attributes	値の入力が必要な属性を指定します。「Add」をクリックすると「Mandatory Attributes Selector」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。
Optional Attributes	値が必須ではない属性を指定します。「Add」をクリックすると「Optional Attributes Selector」ダイアログ・ボックスが表示され、追加するオプション属性を選択できます。

4. 「OK」をクリックします。

**関連項目：**

- 2-8 ページ「オブジェクト・クラスの型」
- 2-8 ページ「サブクラス、スーパー・クラスおよび継承」
- オブジェクト・クラスを追加する方法の詳細は、Oracle Directory Manager のオンライン・ヘルプを参照してください。

## Oracle Directory Manager を使用したオブジェクト・クラスの変更

オブジェクト・クラスを変更する手順は、次のとおりです。

1. ナビゲータ・ペインで「Schema Management」を選択し、「Object Classes」タブを選択します。
2. 「Object Classes」タブ・ページで、変更するオブジェクト・クラスをダブルクリックします。「Object Class」ダイアログ・ボックスが表示されます。
3. 次の表に説明されている各フィールドの情報を変更または追加します。

フィールド	説明
Name	作成するオブジェクト・クラスの名前を入力します。
Object ID	オブジェクト識別子を入力します。これは、IETF 規格に基づいた、標準化された数値順序です。一意、かつ組織内に設定されたシステムに準拠したものである必要があります。通常この値は、ANSI または ISO など、登録機関によって割り当てられた ID から導出されます。
Description	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。
Type	オブジェクト・クラスの型を指定します。「Abstract」、「Structural」、「Auxiliary」、「None」のいずれかを指定します。
Super Class	このオブジェクト・クラスを導出するクラスを指定します。このオブジェクト・クラスは、選択したスーパー・クラスの属性をすべて継承します。構造型オブジェクト・クラスの場合は、そのスーパー・クラスの 1 つとして必ず top を設定する必要があります。「Add」をクリックすると「Super Class Selector」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。
Mandatory Attributes	値の入力が必要な属性を指定します。「Add」をクリックすると「Mandatory Attributes Selector」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。
Optional Attributes	値が必須ではない属性を指定します。「Add」をクリックすると「Optional Attributes Selector」ダイアログ・ボックスが表示され、追加するオプション属性を選択できます。

4. 「OK」をクリックします。

### 関連項目：

- 2-8 ページ「オブジェクト・クラスの型」
- 2-8 ページ「サブクラス、スーパー・クラスおよび継承」

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

---

**注意：** スキーマからはオブジェクト・クラスを削除しないことをお勧めします。

オブジェクト・クラスを削除する場合は、使用中または将来使用する可能性があるオブジェクト・クラスを削除しないように注意してください。エントリの参照先であるオブジェクト・クラスを削除すると、そのエントリにアクセスできなくなります。

---

---

**注意：** 属性は、補助型オブジェクト・クラスまたはユーザー定義の構造型オブジェクト・クラスに追加できます。

**関連項目：** 補助型オブジェクト・クラスへの属性の追加の例は、6-13 ページの「[例：補助型またはユーザー定義のオブジェクト・クラスへの新規属性の追加](#)」を参照してください。

---

Oracle Directory Manager を使用してオブジェクト・クラスを削除する手順は、次のとおりです。

1. ナビゲータ・ペインで「Schema Management」を選択します。
2. 右側のペインで「Object Classes」タブを選択し、削除するオブジェクト・クラスを選択します。
3. 「Delete」をクリックします。

## コマンドライン・ツールを使用したオブジェクト・クラスの管理

ディレクトリ・スキーマへのオブジェクト・クラスの追加や、既存のオブジェクト・クラスの変更にコマンドライン・ツールを使用できます。コマンドライン・ツールでは、入力ファイルが使用できます。さらに、いくつかのコマンドをスクリプトにまとめて、バッチ処理することもできます。

スキーマ・コンポーネントを追加または変更するには、ldapmodify を使用します。

**参照：** A-12 ページ「[ldapmodify 構文](#)」

この項では、次の例について説明します。

- [例：新規オブジェクト・クラスの追加](#)
- [例：補助型またはユーザー定義のオブジェクト・クラスへの新規属性の追加](#)



## 例：新規オブジェクト・クラスの追加

ldapmodify コマンドを使用して新規オブジェクト・クラスのスキーマ・コンポーネントを追加するには、コマンド・プロンプトで次の構文のコマンドを入力します。

```
ldapmodify -h host -p port -f ldif_filename
```

次のようなコマンドを実行します。

```
ldapmodify -h myhost -p 389 -f new_object_class.ldi
```

この例では、LDIF 入力ファイル new\_object\_class.ldi に、次のようなデータが含まれています。

```
dn: cn=subschemasubentry
changetype: modify
add: objectclasses
objectclasses: ( 1.2.3.4.5 NAME 'myobjclass' SUP top STRUCTURAL MUST ( cn $ sn )
MAY ( telephonenumber $ givenname $ myattr ) )
```

前述の例は、myobjclass という名前の構造型オブジェクト・クラスを、オブジェクト ID に 1.2.3.4.5、スーパー・クラスとして top、必須属性として cn と sn、オプション属性として telephonenumber、givenname および myattr を指定して追加しています。記述されている属性すべてが、コマンドの実行前に存在している必要があることに注意してください。

左右のカッコとオブジェクト ID の間に、必ず空白を残してください。

抽象型オブジェクト・クラスを作成する場合は、上の例の STRUCTURAL を ABSTRACT に置き換えてください。

## 例：補助型またはユーザー定義のオブジェクト・クラスへの新規属性の追加

補助型オブジェクト・クラスまたはユーザー定義の構造型オブジェクト・クラスに新規属性を追加するには、ldapmodify を使用します。この例では、複合変更操作で、古いオブジェクト・クラス定義を削除して新規の定義を追加します。変更は Oracle Directory Server によって 1 トランザクションでコミットされます。既存のデータは影響されません。入力ファイルには次のように指定します。

```
dn: cn=subschemasubentry
changetype: modify
delete: objectclasses
objectclasses: old value
-
add: objectclasses
objectclasses: new value
```

たとえば、既存のオブジェクト・クラス `country` に属性 `changes` を追加する場合、入力ファイルは次のようになります。

```
dn: cn=subschemasubentry
changetype: modify
delete: objectclasses
objectclasses: ( 2.5.6.2 NAME 'country' SUP top STRUCTURAL MUST c MAY
( searchGuide $ description ) )
-
add: objectclasses
objectclasses: ( 2.5.6.2 NAME 'country' SUP top STRUCTURAL MUST c MAY
( searchGuide $ description $ changes ) )
```

## 属性管理の概要

この項では、次の項目について説明します。

- [属性の追加に関する規則](#)
- [属性の変更に関する規則](#)
- [属性の削除に関する規則](#)

属性を扱う操作を実行する前に、概念的な観点から属性を理解する必要があります。

多くの場合、ベース・スキーマにある属性で、ユーザーの組織のニーズを満たすことができます。ベース・スキーマにない属性を使用する場合は、新規の属性を追加するか、または既存の属性を変更できます。

デフォルトでは、属性は複数値です。Oracle Directory Manager またはコマンドライン・ツールを使用して、属性を単一値に指定できます。

**関連項目：** 属性の概念の説明は、2-3 ページの「[属性](#)」を参照してください。

## 属性の追加に関する規則

属性の追加に関しては、次の規則があります。

- 属性の名前とオブジェクト ID 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必要があります。
- 構文と一致規則は、整合性がとれている必要があります。
- スーパー属性はすでに存在している必要があります。

## 属性の変更に関する規則

属性の変更に関しては、次の規則があります。

- 属性の名前とオブジェクト ID 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必要があります。
- 属性の構文は変更できません。
- 単一値の属性は複数値の属性に変更できますが、複数値の属性を単一値の属性に変更することはできません。
- ベース・スキーマの属性は、変更したり、削除することはできません。

## 属性の削除に関する規則

属性の削除に関しては、次の規則があります。

- ベース・スキーマから属性を削除することはできません。
- 他のスキーマ・コンポーネントから直接または間接的に参照されていない属性は、削除することができます。

エントリの参照先である属性を削除すると、そのエントリはディレクトリ操作に使用できなくなります。

## Oracle Directory Manager を使用した属性の管理

この項では、次の項目について説明します。

- [Oracle Directory Manager を使用した属性の検索](#)
- [Oracle Directory Manager を使用した属性の追加](#)
- [Oracle Directory Manager を使用した属性の変更](#)
- [作成時の属性の索引付け](#)

## 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「Schema Management」を選択します。「Schema Management」タブ・ページが、右側のペインに表示されます。
2. 「Attributes」タブ・ページを選択します。
3. 右下隅の「Find Attributes」ボタンをクリックします。「Find Attributes」ダイアログ・ボックスが表示されます。

4. 検索基準バーの一番左のメニューから、検索する属性のプロパティを選択します。オプションは次のとおりです。

フィールド	説明
Name	検索する属性の名前。
Indexed	索引付き属性のリスト。
Object ID	検索する属性のオブジェクト ID。たとえば、「Object ID」「Begins With」「2.5.2」と指定すると、オブジェクト ID が 2.5.2 で始まる属性のリストが表示されます。
Description	属性の説明列に記述されている語。
Syntax	データ・エントリに関してこの属性の型に適用される標準化規則。この規則を使用して、特定の構文を使用している属性の検索範囲を絞り込むことができます。
Size	このオブジェクトの最大サイズ。
Usage	属性の使用方法を指定する規格。userApplications、directoryOperation、distributedOperation および dSAOperation の中から 1 つ入力して、検索範囲を絞り込みます。
Ordering	値に対して設定される優先順位を指定する規格。
Equality	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。
Substring	正規表現の一致に使用されます。
Single Value	この属性の型の値が最大 1 つであることを示します。
Super	検索する属性のスーパー属性。

5. 検索基準バーの一番右のテキスト・ボックスに、検索する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、「Name」「Begins With」「orcl」という句を作成します。
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。オプションは次のとおりです。

オプション	説明
Begins With	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、「Syntax」「Begins With」「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。

オプション	説明
Ends With	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、「Name」「End with」「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。
Contains	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、「Ordering」「Contains」「time」と指定すると、順序列に time という語を含んだすべての属性のリストが表示されます。
Exact Match	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、「Equality」「Exact Match」「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。
Greater or Equal	数値順またはアルファベット順で入力値より大か等しいプロパティを持つ属性を検索します。たとえば、「Name」「Greater or Equal」「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。
Less or Equal	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プロパティを持つ属性を検索します。たとえば、「Name」「Less or Equal」「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。
Not Null	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、「Description」「Not NULL」と指定すると、「Description」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。

7. 「Search Criteria」フィールドの下に、次の表で説明する 5 つのボタンがあります。これらのボタンを使用すると、検索基準をさらに詳細に指定できます。

ボタン	説明
New	「Search Criteria」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、「Search Criteria」フィールドに何も表示されていないときのみ使用可能です。
And	「Search Criteria」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	「Search Criteria」フィールドに、別の検索基準バーを作成します。指定した 2 つのプロパティのいずれかを持つ属性をすべて検索します。
Not	選択した検索基準バーの基準を除外し、指定したプロパティがない属性をすべて検索します。
Delete	選択した検索基準バーを削除します。

- 8. 「Search」 をクリックします。検索結果が、「Find: Attributes」 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

この項では、次の項目について説明します。

- [Oracle Directory Manager を使用した新規属性の追加](#)
- [Oracle Directory Manager を使用した既存の属性からの新規属性の作成](#)

**ヒント：** 等価、構文および一致規則は数が多く複雑であるため、これらの特性は、類似の既存属性からコピーすると作業が簡単になります。

### Oracle Directory Manager を使用した新規属性の追加

新規属性を追加する手順は、次のとおりです。

1. ナビゲータ・ペインで、「Oracle Internet Directory Servers」 > 「*directory server*」 の順に展開し、「Schema Management」 を選択します。
2. 次のいずれか 1 つを行います。
  - 右側のペインで「Attributes」 タブを選択し、ツールバーの「Create」 ボタンをクリック
  - 右側のペインで「Attributes」 タブを選択し、「Attributes」 タブ・ページの下の「Create」 ボタンをクリック
  - 「Operation」 メニューから、「Create Attribute」 を選択

「New Attribute Type」 ダイアログ・ボックスが表示されます。そこには、「General」 と「Advanced」 の 2 つのタブ・ページがあります。これらの各フィールドでは、値を入力するかまたはメニューから選択します。
3. 次の表の説明に従って、「General」 タブの各フィールドに値を入力します。

フィールド	説明
Name	この属性の名前を入力します。
Object ID	この属性のオブジェクト ID を入力します。オブジェクト ID は、IETF 規格に基づいた、標準化された数値順序です。値は一意であることが必要です。通常この値は、ANSI または ISO など、登録機関によって割り当てられた ID から導出されます。  標準識別子の説明は、現行の LDAP 規格を参照してください。LDAP 規格は IETF の Web サイトで参照できます。
Description	説明を記述するオプションのフィールドです。

フィールド	説明
Syntax	この属性の型に適用されるデータ・エントリの標準化規則を入力します。
Size	このオブジェクトの最大サイズを入力します。
Single Value	この属性の型の値が最大 1 つであることを指定するには、このチェック・ボックスを選択します。

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

フィールド	説明
Indexed	このフィールドを選択するとこの属性を索引に追加され、検索で使えるようになります。等価の一致規則を持つ属性のみが索引付けできます。
Usage	属性の使用法の規格を指定します。オプションは次のとおりです。 <ul style="list-style-type: none"> <li>■ userApplications ユーザーが値を入力する必要がある属性（例：telephoneNumber）</li> <li>■ directoryOperation Directory Server によって値が入力される属性（例：creatorName または timeStamp）</li> <li>■ distributedOperation</li> <li>■ dSAOperation サーバーの内部操作に使用される属性（例：orclUpdateSchedule）</li> </ul>
Ordering	値の優先順位の設定方法に適用する規格を指定します。
Equality	比較と検索操作における等価の判断方法の規格を指定します。
Substring	正規表現の一致を指定します。
Super	この属性のスーパー属性を追加します。この手順は、次のとおりです。 <ol style="list-style-type: none"> <li>1. このフィールドの横の「Add」ボタンをクリックします。「Super Attribute Selector」が表示されます。</li> <li>2. 追加するスーパー属性を選択して、「Select」をクリックします。</li> <li>3. 必要に応じてこの処理を繰り返します。</li> </ol> 「Super」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、「Delete」をクリックします。

5. 「OK」をクリックします。

**注意：** この属性を使用するには、オブジェクト・クラスに対する属性セットの一部であることを必ず宣言してください。宣言は、ナビゲータ・ペインで「Schema Management」を選択した後、右側のペインで「Object Classes」タブ・ページを選択して行います。詳細は、6-4 ページの「[オブジェクト・クラスの変更のガイドライン](#)」を参照してください。

Oracle Directory Manager を使用した既存の属性からの新規属性の作成

既存属性を利用して属性を追加する手順は、次のとおりです。

- 1. ナビゲータ・ペインで「Schema Management」を選択します。
- 2. 右側のペインで「Attributes」タブを選択します。
- 3. 「Attributes」タブ・ページで、コピーする属性を選択します。
- 4. 右側のペインの下の「Create Like」ボタンをクリックします。その属性の「New Attribute Type」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、「General」と「Advanced」の2つのタブ・ページがあります。これらの各フィールドには値を直接入力するか、またはメニューから値を選択します。
- 5. 「General」タブを選択し、次の表の説明に従って各フィールドに値を入力します。識別名（DN）は、新規属性の DN に必ず変更する必要があります。

フィールド	説明
Name	この属性の名前を入力します。
Object ID	この属性のオブジェクト ID を入力します。オブジェクト ID は、IETF 規格に基づいた、標準化された数値順序です。値は一意であることが必要です。通常この値は、ANSI または ISO など、登録機関によって割り当てられた ID から導出されます。  標準識別子の説明は、現行の LDAP 規格を参照してください。LDAP 規格は IETF の Web サイトで参照できます。
Description	説明を記述するオプションのフィールドです。
Syntax	この属性の型に適用されるデータ・エントリの標準化規則を入力します。
Size	このオブジェクトの最大サイズを入力します。
Single Value	この属性の型の値が最大 1 つであることを指定するには、このチェック・ボックスを選択します。



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

フィールド	説明
Indexed	このフィールドを選択するとこの属性を索引に追加され、検索で使えるようになります。等価の一致規則を持つ属性のみが索引付けできます。
Usage	属性の使用方法の規格を指定します。オプションは次のとおりです。 <ul style="list-style-type: none"> <li>■ <code>userApplications</code> ユーザーが値を入力する必要がある属性（例： <code>telephoneNumber</code>）</li> <li>■ <code>directoryOperation</code> Directory Server によって値が入力される属性（例： <code>creatorName</code> または <code>timeStamp</code>）</li> <li>■ <code>distributedOperation</code></li> <li>■ <code>dsAOperation</code> サーバーの内部操作用に使用される属性（例： <code>orclUpdateSchedule</code>）</li> </ul>
Ordering	値の優先順位の設定方法に適用する規格を指定します。
Equality	比較と検索操作における等価の判断方法の規格を指定します。
Substring	正規表現の一致を指定します。
Super	この属性のスーパー属性を追加します。この手順は、次のとおりです。 <ol style="list-style-type: none"> <li>1. このフィールドの横の「Add」ボタンをクリックします。「Super Attribute Selector」が表示されます。</li> <li>2. 追加するスーパー属性を選択して、「Select」をクリックします。</li> <li>3. 必要に応じてこの処理を繰り返します。</li> </ol> 「Super」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、「Delete」をクリックします。

7. 「OK」をクリックします。

## Oracle Directory Manager を使用した属性の変更

Oracle Directory Manager を使用して属性を変更する手順は、次のとおりです。

1. ナビゲータ・ペインで「Schema Management」を選択します。
2. 右側のペインで「Attributes」タブを選択して、リストの中から編集可能な属性をダブルクリックします。「Attribute」ダイアログ・ボックスには、「General」と「Advanced」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、またはメニューから値を選択します。

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

フィールド	説明
Name	この属性の名前を入力します。
Object ID	この属性のオブジェクト ID を入力します。オブジェクト ID は、IETF 規格に基づいた、標準化された数値順序です。値は一意であることが必要です。通常この値は、ANSI または ISO など、登録機関によって割り当てられた ID から導出されます。  標準識別子の説明は、現行の LDAP 規格を参照してください。LDAP 規格は IETF の Web サイトで参照できます。
Description	説明を記述するオプションのフィールドです。
Syntax	この属性の型に適用されるデータ・エントリの標準化規則を入力します。
Size	このオブジェクトの最大サイズを入力します。
Single Value	この属性の型の値が最大 1 つであることを指定するには、このチェック・ボックスを選択します。

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

フィールド	説明
Indexed	このフィールドを選択するとこの属性を索引に追加され、検索で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。
Usage	属性の使用方法の規格を指定します。オプションは次のとおりです。 <ul style="list-style-type: none"><li>■ userApplications ユーザーが値を入力する必要がある属性（例: telephoneNumber）</li><li>■ directoryOperation Directory Server によって値が入力される属性（例: creatorName または timeStamp）</li><li>■ distributedOperation</li><li>■ dSAOperation サーバーの内部操作用に使用される属性（例: orclUpdateSchedule）</li></ul>
Ordering	値の優先順位の設定方法の規格を指定します。
Equality	比較と検索操作における等価の判断方法の規格を指定します。
Substring	正規表現の一致を指定します。

フィールド	説明
Super	<p>この属性のスーパー属性を追加します。この手順は、次のとおりです。</p> <ol style="list-style-type: none"> <li>1. このフィールドの横の「Add」ボタンをクリックします。「Super Attribute Selector」が表示されます。</li> <li>2. 追加するスーパー属性を選択して、「Select」をクリックします。</li> <li>3. 必要に応じてこの処理を繰り返します。</li> </ol> <p>「Super」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、「Delete」をクリックします。</p>

5. 「OK」をクリックします。

## 作成時の属性の索引付け

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、カタログ管理ツールを使用します。

また、等価の一致規則を持つ属性のみ索引付けできます。

---

**関連項目：** コマンドラインのカタログ管理ツールの使用方法は、6-25 ページの「[コマンドライン・ツールを使用した属性の索引付け](#)」を参照してください。

この項では、次の項目について説明します。

- [Oracle Directory Manager を使用した索引付き属性の表示](#)
- [Oracle Directory Manager を使用した作成時の属性の索引付け](#)
- [Oracle Directory Manager を使用した属性からの索引の削除](#)

## 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「Schema Management」を選択します。
2. 右側のペインで「Attributes」タブを選択します。「Attributes」タブに、スキーマ内のすべての属性が表示されます。「Indexed」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 を使用した作成時の属性の索引付け

6-18 ページの「[Oracle Directory Manager を使用した属性の追加](#)」の説明にあるように、属性を作成するときには「New Attribute Type」ダイアログ・ボックスを使用します。そのダイアログ・ボックスの「Advanced」タブ・ページで、「Indexed」チェック・ボックスを選択してください。

## Oracle Directory Manager を使用した属性からの索引の削除

属性から索引を削除する手順は、次のとおりです。

1. ナビゲータ・ペインで「Schema Management」を選択します。
2. 右側のペインで「Attributes」タブを選択します。
3. 索引付き属性を選択します。選択する属性は編集可能である必要があります。編集可能かどうかは、属性名の左にアイコンで示されています。
4. 「Drop Index」をクリックします。

# コマンドライン・ツールを使用した属性の管理

この項では、コマンドライン・ツールを使用した属性の追加、変更および索引付けについて説明します。この項では、次の内容について説明します。

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

## ldapmodify を使用した属性の追加と変更

**関連項目：** このコマンドとそのオプションの詳細は、A-12 ページの「[ldapmodify 構文](#)」を参照してください。

ldapmodify コマンドを使用して新規属性をスキーマに追加するには、コマンド・プロンプトで次のようなコマンドを入力します。

```
ldapmodify -h host -p port -f ldif_filename
```

LDIF ファイルには、次のようなデータが含まれています。

```
dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: ( 1.2.3.4.5 NAME 'myattr' SYNTAX
                  '1.3.6.1.4.1.1466.115.121.1.38' )
```

属性を単一値に指定するには、LDIF ファイルの属性定義エントリにキーワード SINGLE-VALUE を指定し、その前後を空白で囲みます。

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。

**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「Schema Management」を選択します。
2. 右側のペインで「Syntaxes」タブを選択します。

**ldapsearch を使用した構文の表示** サブエントリ cn=subSchemaSubentry で ldapsearch を使用します。

**関連項目：** A-17 ページ「[ldapsearch 構文](#)」

## コマンドライン・ツールを使用した属性の索引付け

この項では、次の項目について説明します。

- [索引付けの概要](#)
- [ldapmodify を使用したディレクトリ・データが存在していない属性の索引付け](#)
- [カタログ管理ツールを使用したディレクトリ・データが存在している属性の索引付け](#)

### 索引付けの概要

Oracle Internet Directory は、索引を使用して属性を検索できるようにしています。Oracle Internet Directory のインストール時に、エントリ cn=catalogs に、検索で使用できる属性がリストされます。

その他の属性を検索フィルタで使用する場合は、使用する属性をカタログ・エントリに追加する必要があります。等価の一致規則を持つ属性のみが索引付けできます。

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勧めします。

### **ldapmodify を使用したディレクトリ・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。次のようなコマンドを実行します。

```
dn: cn=catalogs
changetype: modify
delete: orclindexedattribute
orclindexedattribute: foo
```

**関連項目：** A-12 ページ [「ldapmodify 構文」](#)

### **カタログ管理ツールを使用したディレクトリ・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。

**参照：** A-27 ページ [「カタログ管理ツールの構文」](#)

---

# ディレクトリ・エントリの管理

この章では、エントリの表示、追加および変更方法を説明します。

この章では、次の項目について説明します。

- [Oracle Directory Manager](#) を使用したエントリの管理
- コマンドライン・ツールを使用したエントリの管理
- バルク・ツールを使用したエントリの管理
- 属性オプションのあるエントリの管理
- ナレッジ参照（参照）の管理

**関連項目：** ディレクトリ・エントリ、ディレクトリ情報ツリー、識別名および相対識別名の概要は、[第2章「概念とアーキテクチャ」](#)を参照してください。

## Oracle Directory Manager を使用したエントリの管理

この項では、次の項目について説明します。

- [Oracle Directory Manager を使用したエントリの検索](#)
- [Oracle Directory Manager を使用した監査ログ・エントリの検索](#)
- [Oracle Directory Manager を使用した属性の表示](#)
- [Oracle Directory Manager を使用したエントリの追加](#)
- [Oracle Directory Manager を使用したエントリの変更](#)

## Oracle Directory Manager を使用したエントリの検索

すべてのエントリの表示にはナビゲータ・ペインを、1 つ以上の特定のエントリの検索には Oracle Directory Manager の検索機能を使用できます。

ナビゲータ・ペインにエントリを表示するには、「Entry Management」を展開して、そのサブツリーを表示します。

ツリーのルートが最初にリストされ、次に第 2 レベル、第 3 レベルというように、左から右へ移動してリストされます。サブツリーには、各エントリの相対識別名 (**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 Servers」 > 「*directory\_server\_instance*」の順に展開し、「Entry Management」を選択します。右側のペインに「Search」フィールドが表示されます。
2. 「Root of the Search」フィールドに、検索のルートの識別名 (**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 DN は、次のようになります。

```
ou=Manufacturing,ou=Americas,o=IMC,c=US
```

この DN を「Root of the Search」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](#)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. 「Root of the Search」フィールドの右側の「Browse」をクリックします。「Select Distinguished Name (DN) Path: Tree View」ダイアログ・ボックスが表示されます。
- b. 「Tree View」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 (DN) が、右側のペインの「Root of the Search」テキスト・ボックスに表示されます。
3. 「Max Results (entries)」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 (ゼロ) です。
4. 「Max Search Time (seconds)」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。
5. 「Search Depth」のリストで、検索するレベルを選択します。  
オプションは次のとおりです。
  - Base: 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「Present」を選択します。
  - One Level: 検索のルートの 1 レベル下のすべてのエントリに検索を制限します。
  - Subtree: 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. 「Search Criteria」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。

---

**注意：** 各エントリで、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、探しているエントリ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。

---

- b. 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。
- c. 検索基準バーの中央のリストから、フィルタを選択します。オプションは次のとおりです。

フィルタ	説明
Begins With	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」「Begins With」「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。
Ends With	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」「Ends With」「son」と指定すると、Baldisson、Jacobson、Johnson などが取り出されます。

フィルタ	説明
Contains	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」「Contains」「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。
Exact Match	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」「Exact Match」「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。
Greater or Equal	指定した属性が、数値順またはアルファベット順で入力値より大か等しいエントリを検索します。たとえば、「cn」「Greater or Equal」「Frank」と指定すると、cn 属性の範囲が、Frank からアルファベットの最後の文字までのエントリがすべて取り出されます。
Less or Equal	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」「Less or Equal」「Frank」と指定すると、Frank からアルファベットの最初の文字までの cn 属性がすべて取り出されます。
Present	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」「Present」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。

7. 検索をさらに詳細に指定するには、「Search Criteria」ボックスのボタンを使用して検索基準バーを拡張します。

ボタン	説明
New	「Search Criteria」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、「Search Criteria」フィールドに何も表示されていない時のみ使用可能です。
And	「Search Criteria」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 つの属性を両方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	「Search Criteria」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。

ボタン	説明
Not	選択した検索基準バーの基準を除外し、指定した基準を満たさないエントリをすべて取り出します。たとえば、cn=Frank Not title=Laborer と指定すると、cn が Frank で、title が laborer ではない個人がすべて取り出されます。
Delete	選択した検索基準バーを削除します。

- 「Search」をクリックします。検索結果は「Distinguished Name」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および検索の時間制限の設定方法は、5-17 ページの「[検索の構成](#)」を参照してください。

## Oracle Directory Manager を使用した監査ログ・エントリの検索

Oracle Directory Manager を使用して、監査ログ・エントリも検索できます。

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。

- ナビゲータ・ペインで、「Oracle Internet Directory Servers」>「*directory\_server\_instance*」の順に展開し、「Audit Log Management」を選択します。対応する右側のペインが表示されます。
- 7-2 ページの「[Oracle Directory Manager を使用したエントリの検索](#)」の指示に従って、監査ログ内の特定の種類のエントリを検索します。検索結果は下のボックスに表示されます。
- 特定の監査ログ・エントリのプロパティを表示するには、そのプロパティを下のボックスで選択し、「View Properties」をクリックします。「Audit Log Entry」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および検索の時間制限の設定方法は、5-17 ページの「[検索の構成](#)」を参照してください。

## Oracle Directory Manager を使用した属性の表示

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。「Entry」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（DN）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 DN がある場合があります。この場合、従業員の「Entry」ダイアログ・ボックスを表示すると、「Manager」テキスト・ボックスの横に「Browse」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、「Browse」をクリックして「Directory: Entry Management」ダイアログ・ボックスを表示

し、7-2 ページの「[Oracle Directory Manager を使用したエントリの検索](#)」の手順に従って検索してください。

## Oracle Directory Manager を使用したエントリの追加

---

**注意：** このリリースの Oracle Internet Directory では、Oracle Directory Manager を使用した JPEG イメージの追加はサポートされていません。JPEG イメージを追加するには、`ldapadd` コマンドを使用します。詳細は、7-12 ページの「[例：ldapadd 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。

---

### 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き込みアクセス権限があり、新規エントリの識別名（DN）を認識している必要があります。

新規エントリを追加する手順は、次のとおりです。

1. 「Oracle Internet Directory Servers」 > 「*directory\_server\_instance*」の順に展開し、「Entry Management」を選択します。
2. ツールバーの「Create」ボタンをクリックします。「New Entry」ダイアログ・ボックスが表示されます。
3. 「Distinguished Name」フィールドに、完全な DN を入力します。「Browse」をクリックして、追加するエントリの親の DN の位置を識別して選択することもできます。選択したエントリが「Distinguished Name」フィールドに表示されます。その親の DN の左に新規エントリの RDN を入力し、その後にカンマを付けます。
4. 新規エントリの[オブジェクト・クラス](#)を指定するには、「Object Classes」ボックスの横の「Add」をクリックします。「Super Class Selector」ダイアログ・ボックスが表示されます。
5. 「Super Class Selector」ダイアログ・ボックスでオブジェクト・クラスを選択して、「Select」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、「New Entry」ダイアログ・ボックスの下半分のタブ・ページにあるウィンドウに、必須属性とオプション属性が表示されます。必須属性のフィールドには、値を入力する必要があります。オプション属性のフィールドには、値を必ずしも入力する必要はありません。
6. オブジェクト・クラスを選択して、対応する属性に値を入力した後、「OK」をクリックします。

## Oracle Directory Manager の既存エントリを利用したエントリの追加

Oracle Directory Manager では、既存エントリをコピーしてその識別名 (DN) 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 DN 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 DN 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 Servers」>「*directory\_server\_instance*」の順に展開し、「Entry Management」を選択します。検索ペインが表示されます。このペインで、テンプレートとして使用するエントリを検索します。
2. 検索結果の中からエントリを 1 つダブルクリックします。そのエントリに対応する「Entry」ダイアログ・ボックスが表示されます。このエントリが、「Create Like」ペインでテンプレートとして使用されます。
3. 「Entry」ダイアログ・ボックスで、「Create Like」をクリックします。「New Entry: Create Like」ダイアログ・ボックスが表示されます。
4. このエントリを作成するエントリに調整するために、重要なフィールドを変更します。この操作で、識別名 (DN) 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、DN の cn=Henri Latour を cn=Henri Latrobe に変更する必要があります。また、一般名属性の Henri Latour という値も Henri Latrobe に変更し、従業員番号や電話番号など、一意であることが必要なその他の属性も変更してください。
5. 「OK」をクリックして、変更内容を保存します。

**関連項目：** フィールドに情報を追加する方法は、このダイアログ・ボックスのオンライン・ヘルプを参照してください。

## 例：Oracle Directory Manager を使用したユーザー・エントリの追加

この例では、Anne Smith というユーザーを作成し、パスワードを割り当てます。

1. administrator でログインします。
2. 「Oracle Internet Directory Services」>「*directory\_server\_instance*」の順に展開し、「Entry Management」を選択します。
3. ツールバーの「Create」ボタンをクリックします。「New Entry」ダイアログ・ボックスが表示されます。

4. 「Distinguished Name」フィールドに、完全な DN を入力します。「Browse」ボタンをクリックして、このエントリの親の DN を探し、親の DN の左に相対識別名 (RDN)、つまり cn=Anne Smith を入力して、その後にカンマを付けることもできます。
5. 「Object Classes」ボックスの右側の「Add」をクリックします。「Super Class Selector」ダイアログ・ボックスが表示されます。
6. 「Super Class Selector」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、「Select」をクリックします。「New Entry」ダイアログ・ボックスに戻ります。
7. 「New Entry」ダイアログ・ボックスで「Optional Properties」タブをクリックし、「userPassword」ウィンドウまでスクロールします。
8. Anne Smith 用のパスワードを入力します。

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

グループ・エントリは、エントリのリスト（例：電子メール・リスト）を含むエントリです。グループ・エントリは、オブジェクト・クラス `orclPrivilegeGroup` をサブクラスとして持つ、`groupOfNames` または `groupOfUniqueNames` オブジェクト・クラスのいずれかと関連付けられます。

エントリが `groupOfNames` オブジェクト・クラスに属している場合は複数値の属性 `member` に、`groupOfUniqueNames` オブジェクト・クラスに属している場合は属性 `uniqueMember` に識別名 (DN) を追加して、グループのメンバーシップを決定します。

グループ・エントリを追加する手順は、次のとおりです。

1. 「Oracle Internet Directory Servers」 > 「*directory\_server\_instance*」の順に展開し、「Entry Management」を選択します。
2. ツールバーの「Create」ボタンをクリックします。「New Entry」ダイアログ・ボックスが表示されます。
3. 「Distinguished Name」フィールドに、完全な DN を入力します。「Browse」ボタンを使用して、追加するエントリの親の DN を探し、親の DN の左に新規エントリの相対識別名 (RDN) を入力して、その後にカンマを付けることもできます。
4. 新規エントリに使用するオブジェクト・クラスを指定するには、「Object Classes」ボックスの右の「Add」をクリックします。「Super Class Selector」ダイアログ・ボックスが表示されます。
5. 「Super Class Selector」ダイアログ・ボックスで、`top` オブジェクト・クラスを選択し、「Select」ボタンをクリックします。「New Entry」ダイアログ・ボックスの「Object Classes」ボックスに、`top` オブジェクト・クラスが表示されます。
6. 同様に、次の手順を実行します。
  - a. 「Object Classes」ボックスの右の「Add」をクリックします。
  - b. 「Super Class Selector」ダイアログ・ボックスから、「`groupOfNames`」または「`groupOfUniqueNames`」オブジェクト・クラスを選択します。

- c. 「Select」をクリックします。「New Entry」ダイアログ・ボックスの「Object Classes」ウィンドウに、選択したオブジェクト・クラスが表示されます。
7. グループ・エントリの必須属性とオプション属性を入力します。
- 「groupOfNames」オブジェクト・クラスを選択した場合は、いくつかのフィールド、たとえば「Mandatory Properties」タブ・ページの「member」フィールドの横に、「Browse」ボタンが表示されます。ブラウズによって必須プロパティを入力する手順は、次のとおりです。
- a. 「Browse」をクリックします。「Directory: Entry Management」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. 「Directory: Entry Management」ダイアログ・ボックスの「Distinguished Name」ウィンドウで、エントリを選択して「OK」をクリックします。「New Entry」ダイアログ・ボックスに戻ります。選択したエントリが、「member」ウィンドウのリストに追加されています。
8. 「OK」をクリックします。

#### 関連項目：

- 検索ペインの使用方法は、7-2 ページの「[Oracle Directory Manager を使用したエントリの検索](#)」を参照してください。
- グループ・エントリのアクセス制御ポリシーの設定方法は、9-4 ページの「[権限グループ](#)」を参照してください。
- アクセス権限の詳細は、2-15 ページの「[アクセス制御と認可](#)」および第 9 章「[ディレクトリのアクセス制御の管理](#)」を参照してください。

## Oracle Directory Manager を使用したエントリの変更

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

- エントリにオブジェクト・クラスを割り当て、その属性にデータを指定した後は、そのエントリが使用しているオブジェクト・クラスを変更できません。
- たとえば、オブジェクト・クラスの Person と Organizational Role を使用するエントリを構成する場合は、このエントリに後で別のオブジェクト・クラスを追加できません。
- すでにいくつかのエントリが使用しているオブジェクト・クラスには、必須属性を追加できません。オプション属性は追加できます。いくつかのエントリがすでに使用しているオブジェクト・クラスにオプション属性を追加する場合、特別な規則は適用されません。これらのエントリに対しては、オプション属性は空の属性として追加されます。

エントリを変更する手順は、次のとおりです。

1. 7-2 ページの「[Oracle Directory Manager を使用したエントリの検索](#)」の説明に従って、変更するエントリの検索を実行します。
2. 右側のペインの「Distinguished Name」ボックスで、変更するエントリを選択します。
3. 「Edit」をクリックします。「Entry」ダイアログ・ボックスが表示されます。
4. 「Properties」タブ・ページを選択します。追加または変更する属性が見つからない場合は、タブ・ページ上部の「View Properties: All」を選択します。
5. 「Properties」タブ・ページで、編集可能な属性の値を変更します。
6. 「OK」をクリックします。

### 例：Oracle Directory Manager を使用したユーザー・エントリの変更

この例では、7-7 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「Distinguished Name」ボックスで、Anne Smith のエントリを選択します。
3. 「Edit」をクリックします。
4. 「Entry」ダイアログ・ボックスで、「userPassword」ウィンドウまでスクロールしてその値を変更します。
5. 「OK」をクリックします。

## コマンドライン・ツールを使用したエントリの管理

この項では、エントリの管理に使用できるコマンドライン・ツールについて説明します。また、コマンドライン・ツールを使用したエントリ管理の例もいくつか紹介します。この項では、次の内容について説明します。

- [エントリ管理のためのコマンドライン・ツール](#)
- [例：ldapadd を使用したユーザー・エントリの追加](#)
- [例：属性オプションの追加](#)
- [例：ldapmodify を使用したユーザー・エントリの変更](#)



## エントリ管理のためのコマンドライン・ツール

次の表に、各コマンドライン・ツールと、それぞれのツールの構文と使用方法の参照箇所を示します。

ツール	タスク	構文と使用方法
ldapsearch	ディレクトリ・エントリを検索します。	A-17 ページ <a href="#">「ldapsearch 構文」</a>
ldapbind	Directory Server に対して、ユーザーまたはクライアントを認証します。 クライアントをサーバーに接続できるかどうかを検証します。	A-7 ページ <a href="#">「ldapbind 構文」</a>
ldapadd	エントリを一度に1つずつ追加します。 新規構成設定エントリを追加します。 入力ファイルを使用してサーバーを構成します。	A-4 ページ <a href="#">「ldapadd 構文」</a>
ldapaddmt	このマルチスレッド・ツールは、複数のエントリを同時に追加するときに使用します。	A-6 ページ <a href="#">「ldapaddmt 構文」</a>
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（DN）または相対識別名（RDN）を変更します。	A-12 ページ <a href="#">「ldapmodify 構文」</a>
ldapmodifymt	このマルチスレッド・ツールは、複数のエントリを同時に変更するときに使用します。	A-16 ページ <a href="#">「ldapmodifymt 構文」</a>
ldapdelete	エントリを削除します。	A-10 ページ <a href="#">「ldapdelete 構文」</a>
ldapcompare	ユーザーが指定した属性値とディレクトリ・エントリ内の属性値を比較します。	A-8 ページ <a href="#">「ldapcompare 構文」</a>
ldapmoddn	エントリの識別名（DN）または相対識別名（RDN）を変更します。 エントリまたはサブツリーを改名します。 エントリまたはサブツリーを新しい親の下に移動します。	A-11 ページ <a href="#">「ldapmoddn 構文」</a>

## 例：Idapadd を使用したユーザー・エントリの追加

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

```
dn: cn=john, c=us
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
cn: john
cn;lang-fr:Jean
cn;lang-en-us:John
sn: Doe
jpegPhoto: /photo/john.jpg
userpassword: welcome
```

このファイルには、cn、sn、jpegPhoto および userpassword の各属性が含まれています。

cn 属性では、cn;lang-fr および cn;lang-en-us という 2 つのオプションを指定しています。これらのオプションは、French（フランス語）または American English（米語）での一般名を戻します。

jpegPhoto 属性では、エントリの属性として組み込む、対応する JPEG イメージのパスとファイル名を指定しています。

## 例：Idapmodify 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 -b -f entry.ldif
```

## バルク・ツールを使用したエントリの管理

この項では、バルク・ツールで実行する一般的なタスクの一部を説明します。

この項では、次の項目について説明します。

- [bulkload](#) を使用した LDIF ファイルのインポート
- ディレクトリ・データの LDIF への変換
- 多数のエントリの変更
- 多数のエントリの削除

**関連項目：** これらのツールの概要は、4-12 ページの「[バルク・ツールの使用方法](#)」を参照してください。

### bulkload を使用した LDIF ファイルのインポート

LDIF ファイルをインポートするには、bulkload ユーティリティを使用します。この項では、bulkload で LDIF ファイルを処理するタスクについて説明します。

---

---

**注意：** バルク・ロードを実行する前に、Oracle Internet Directory プロセスを停止してください。Directory Server インスタンスの停止方法は、[第 3 章「事前に実行する作業」](#)を参照してください。

---

---

この項では、次の項目について説明します。

- [タスク 1: Oracle Server のバックアップ](#)
- [タスク 2: Oracle Internet Directory のパスワードの準備](#)
- [タスク 3: スキーマ違反とデータ整合性違反に関する入力のチェック](#)
- [タスク 4: SQL\\*Loader 用の入力ファイルの生成](#)
- [タスク 5: 入力ファイルのロード](#)
- [バルク・ロードに失敗した場合](#)

## タスク 1: Oracle Server のバックアップ

ファイルをインポートする前に、安全対策として Oracle データベース・サーバーをバックアップします。

**関連項目：**『Oracle8i バックアップおよびリカバリ・ガイド』

## タスク 2: Oracle Internet Directory のパスワードの準備

bulkload および .sh で終わるコマンドを持つ他のシェル・スクリプト・ツールを使用するには、Oracle Internet Directory のパスワードを準備する必要があります。デフォルトのパスワードは ods ですが、このパスワードは、[OID データベース・パスワード・ユーティリティ](#)を使用して、システム管理者が変更できます。

**関連項目：** 4-13 ページ「[OID データベース・パスワード・ユーティリティの使用方法](#)」

## タスク 3: スキーマ違反とデータ整合性違反に関する入力のチェック

Solaris では、bulkload.sh ファイルは通常、\$ORACLE\_HOME/ldap/bin にあります。Windows NT では通常、ORACLE\_HOME¥ldap¥bin にあります。

入力ファイルをチェックするには、次のように入力します。

```
bulkload.sh -connect net_service_name -check path_to_ldif-filename
```

すべてのスキーマ違反が

\$ORACLE\_HOME/ldap/log/schemacheck.log に記録されます。

入力ファイルに違反が検出された場合は、テキスト・ファイル・エディタを使用してその違反を修正するか、または削除してください。エントリが重複している場合、その DN は \$ORACLE\_HOME/ldap/log/duplicate.log に記録されます。

## タスク 4: SQL\*Loader 用の入力ファイルの生成

入力ファイルのエラー修正後、次の例のように -generate オプションを指定して bulkload を再実行します。このステップで、LDIF データは SQL\*Loader 固有の形式に変換されます。

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

ロード時のエラーはすべて

\$ORACLE\_HOME/ldap/log に記録されます。

このコマンドが正常に完了すると、SQL\*Loader が -load モードで使用する \*.dat ファイルが、\$ORACLE\_HOME/ldap/load ディレクトリに生成されます。このファイルは変更できません。

## タスク 5: 入力ファイルのロード

入力ファイルの生成後、`-load` オプションを指定して `bulkload` を再実行します。このステップで、Oracle SQL\*Loader 固有の形式の `*.dat` ファイルがデータベースにロードされ、属性の索引が作成されます。構文は次のとおりです。

```
bulkload.sh -connect net_service_name -load
```

## バルク・ロードに失敗した場合

ロード時のエラーはすべて、`$ORACLE_HOME/ldap/log/directory` にファイル拡張子 `.bad` で記録されます。

バルク・ロードに失敗した場合は、データベースが一貫性のない状態のままになっている可能性があります。バルク・ロードを操作する前の状態にデータベースをリストアする必要があります。

## ディレクトリ・データの LDIF への変換

LDIF ライターを使用してディレクトリ・データを LDIF に変換すると、レプリケート・ディレクトリの新規ノードまたはバックアップ保管用の別のノードにロードするために使用できます。

**関連項目：** A-26 ページ [「ldifwrite 構文」](#)

## 多数のエントリの変更

`bulkmodify` ユーティリティを使用すると、多数の既存エントリを効率的に変更できます。

**関連項目：** A-24 ページ [「bulkmodify 構文」](#)

## 多数のエントリの削除

`bulkdelete` ユーティリティを使用すると、サブツリー全体を効率的に削除できます。

**関連項目：** A-21 ページ [「bulkdelete 構文」](#)

## 属性オプションのあるエントリの管理

属性オプションのあるエントリを管理するには、コマンドライン・ツールを使用します。この項では、次の内容について説明します。

- [例：属性オプションの追加](#)
- [例：属性オプションの削除](#)
- [例：属性オプションのあるエントリの検索](#)

### 例：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。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
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 -b -f entry.ldif
```

### 例：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 -b -f entry.ldif
```

## 例：属性オプションのあるエントリの検索

次の例では、言語コード属性オプションを指定するオプションのある一般名（cn）属性を持つエントリを取り出します。この例の場合には、一般名がフランス語で、R で始まるエントリを取り出します。

```
ldapsearch -p 389 -h myhost -b "c=US" -s sub "cn;lang-fr=R*"
```

John のエントリで、cn;lang-it 言語コード属性オプションに何も値が設定されていないとします。この場合、次の例は失敗します。

```
ldapsearch -p 389 -h myhost -b "c=us" -s sub "cn;lang-it=Giovanni"
```

**関連項目：** 2-7 ページ「[属性オプション](#)」

## ナレッジ参照（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 および extensibleObject **オブジェクト・クラス**にそのエントリを対応付けます。通常、ナレッジ参照エントリは、パーティションを確立する **DIT** 内の場所に作成されます。

ナレッジ参照は、ユーザーに LDAP URL を提供します。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、DIT に複数のナレッジ参照エントリがある場合もあります。

**関連項目：** ナレッジ参照の概要、[スマート・ナレッジ参照](#)および[デフォルト・ナレッジ参照](#)の説明は、2-38 ページの「[分散ディレクトリ：パーティション化](#)」を参照してください。

この項では、次の項目について説明します。

- [スマート・ナレッジ参照の構成](#)
- [デフォルト・ナレッジ参照の構成](#)

## スマート・ナレッジ参照の構成

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 はそれをクライアントに戻します。

ユーザーがナレッジ参照エントリの下に置かれたエントリに対して追加、削除または変更操作を実行すると、Oracle Internet Directory はナレッジ参照を戻します。

---

---

**注意：** 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。

---

---

たとえば、Directory Server の地理的な場所に基づいた DIT 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。

この 2 つのネーミング・コンテキストの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` で問い合わせるクライアントは、ナレッジ参照を受信します。
- サーバー C にベース `o=foo,c=us` で問い合わせるクライアントは、ナレッジ参照を受信します。
- 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 はナレッジ参照を戻します。

## デフォルト・ナレッジ参照の構成

Oracle Internet Directory は、サーバーによってローカルに保持されているすべての**ネーミング・コンテキスト**を **DSE** の `namingContext` 属性を使用して判断します。  
`namingContext` 属性には、ネーミング・コンテキスト情報を正しく反映させてください。

DSE エントリの `ref` 属性の値を入力して、デフォルト・ナレッジ参照を指定します。`ref` 属性が DSE エントリにない場合は、デフォルト・ナレッジ参照は戻されません。

デフォルト・ナレッジ参照を構成するときは、LDAP URL の DN 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・ナレッジ参照が次のとおりだとします。

```
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 DN 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 へのナレッジ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 DN 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：** ナレッジ参照の概念の説明は、2-39 ページの「**ナレッジ参照（参照）**」を参照してください。



---

## Secure Sockets Layer (SSL) の管理

この章では、Secure Sockets Layer (SSL) の機能を構成する方法を説明します。SSL を使用すると、強化認証、データ整合性およびデータ・プライバシーも構成できます。

この章では、次の項目について説明します。

- サポートされている Cipher Suite
- SSL クライアントの使用例
- SSL パラメータの構成
- このリリースの Oracle Internet Directory 固有の問題

**関連項目：** Oracle Internet Directory に関連した SSL の概要は、2-11 ページの「[セキュリティ](#)」を参照してください。

## サポートされている Cipher Suite

Cipher Suite は、ネットワーク・ノード間でのメッセージ交換に使用される認証、暗号化およびデータ整合性アルゴリズムのセットです。SSL ハンドシェイク時に、2つのノードは、メッセージの送受信に使用する Cipher Suite を調べるために交渉を行う。

Oracle Internet Directory では、次の SSL Cipher Suite がサポートされています。

表 8-1 Oracle Internet Directory でサポートされている SSL Cipher Suite

Cipher Suite	認証	暗号化	データ整合性
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	RSA	DES40	SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5	RSA	RC4_40	MD5
SSL_RSA_WITH_NULL_SHA	RSA	None	SHA
SSL_RSA_WITH_NULL_MD5	RSA	None	MD5

## 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 X509v3 デジタル証明書から必要な識別情報を取得します。

## SSL パラメータの構成

Directory Server [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このディレクトリに読み込まれます。SSL が使用可能な状態でこのディレクトリを実行する場合は、[構成設定エントリ](#)の SSL パラメータを確認する必要があります(多くの場合、再構成が必要です)。

保護モードでサーバー・インスタンスを実行するには、デフォルト・ポートの保護ポート 636 で実行するように構成設定を変更します。

管理者は、異なる値を持つ複数の構成パラメータのセットを作成および変更し、Oracle Internet Directory のインスタンスごとに異なる構成設定エントリを使用できます。これは、セキュリティ・ニーズの異なるクライアントを制御する便利な方法です。

SSL の値を変更するときは、デフォルトの構成設定にある SSL の値を変更するのではなく、別の構成設定を作成して、その SSL の値を変更する方法をお薦めします。これは、デフォルトの構成設定は、技術的な問題を診断するときにオラクル社カスタマ・サポート・センターにとって必要となる場合があるからです。

関連項目：

- これらのパラメータの設定方法は、5-2 ページの「[サーバーの構成設定エントリの管理](#)」を参照してください。
- これらのパラメータの説明は、E-4 ページの「[構成設定エントリの属性](#)」を参照してください。

Oracle Directory Manager を使用した SSL パラメータの構成

作成した各構成設定エントリおよび現在実行中の各サーバー・インスタンスの SSL 構成パラメータの値を、確認および変更できます。

**注意：** アクティブ・インスタンスのパラメータを直接変更できません。アクティブ・インスタンスのパラメータを変更する場合は、構成設定エントリ内のパラメータを変更して、それを保存してください。保存後は、現行のインスタンスを停止して、サーバーの起動メッセージ内にある新たに変更された構成設定を参照できます。

SSL 構成パラメータを表示および変更する手順は、次のとおりです。

1. Oracle Directory Manager のナビゲータ・ペインで、「Oracle Internet Directory Servers」>「*directory server*」>「Server Management」の順に展開します。
2. 「Directory Server」または「Replication Server」の適切な項目を展開します。選択した項目の下に、番号付きの構成設定が表示されます。
3. 検証する構成設定を選択します。その構成設定エントリに対応するタブ・ページが右側のペインに表示されます。
4. 「SSL Settings」タブ・ページを選択します。  
このタブ・ページでパラメータを変更して保存できます。このタブ・ページの各フィールドの説明は、次の表に記載されています。

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

フィールド	説明
SSL Authentication	<p>次の中から 1 つ選択します。</p> <ul style="list-style-type: none"><li>■ No SSL Authentication: 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。</li><li>■ SSL Client and Server Authentication: 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。</li><li>■ SSL Server Authentication: Directory Server のみ、クライアントに対して自己認証を行います。Directory Server 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。</li></ul>
SSL Wallet URL	<p>SSL Wallet の位置を入力します。Oracle Wallet の位置を変更する場合は、このパラメータを変更する必要があります。クライアントとサーバーの両方で Wallet の位置を設定する必要があります。たとえば Solaris では、このパラメータは次のように設定します。</p> <pre>orclsslwalleturl=file:/Home/my_dir/my_wallet</pre> <p>Windows NT では、このパラメータは次のように設定します。</p> <pre>file:C:¥my_dir¥my_wallet</pre>
SSL Wallet Password	<p>サーバー側 Wallet のパスワードを入力します。このパスワードは、Wallet の作成時に設定されています。パスワードを変更する場合は、このパラメータを変更する必要があります。</p>
SSL Wallet Confirm Password	<p>パスワードを変更するときは、このフィールドに新規パスワードを再度入力します。</p>
SSL Port	<p>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。</p>

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

## コマンドライン・ツールを使用した SSL パラメータの構成

**関連項目：** 5-10 ページ「[コマンドライン・ツールを使用したサーバー構成設定エントリの管理](#)」

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

Oracle Internet Directory リリース 2.1.1 での Oracle Directory Replication Server は、SSL 対応の Oracle Directory Server インスタンスとは直接通信できません。

同じホストで、SSL クライアントと非 SSL クライアントの両方をサポートする場合は、2 つの別々のサーバー・インスタンスを構成する必要があります。

**関連項目：** サーバー・インスタンスの構成方法は、[第 5 章「Oracle Directory Server の管理」](#)を参照してください。





---

# ディレクトリのアクセス制御の管理

この章では、アクセス制御ポリシーについて概説し、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を説明します。

この章では、次の項目について説明します。

- [アクセス制御ポリシーの管理の概要](#)
- [Oracle Directory Manager を使用したアクセス制御の管理](#)
- [コマンドライン・ツールを使用したアクセス制御の管理](#)

## 関連項目：

- アクセス制御ポリシーの実装と管理を始める前の概要は、2-15 ページの「[アクセス制御と認可](#)」を参照してください。
- アクセス制御項目（ACI）の書式（構文）の詳細は、[付録 D「アクセス制御ディレクティブ書式の使用法](#)」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アクセス制御項目（**ACI**）属性の値を構成して管理します。そのためには、Oracle Directory Manager または ldapmodify のいずれかを使用します。

この項では、次の項目について説明します。

- [アクセス制御管理の構造体](#)
- [アクセス制御情報のコンポーネント](#)
- [アクセス制御リスト（ACL）の評価の動作](#)
- [Oracle Directory Manager を使用した既存 Access Control Policy Points（ACP）とそのアクセス制御項目（ACI）ディレクティブの変更](#)
- [Oracle Directory Manager を使用した Access Control Policy Points（ACP）の追加とアクセス項目の作成](#)
- [例 : Oracle Directory Manager を使用した Access Control Policy Points（ACP）の管理](#)
- [Oracle Directory Manager を使用したエントリ・レベルのアクセス権限の付与](#)
- [例 : アクセス制御の管理](#)

## アクセス制御管理の構造体

この項では、次の項目について説明します。

- [orclACI](#)
- [Access Control Policy Points（ACP）](#)
- [orclEntryLevelACI](#)
- [権限グループ](#)

### orclACI

orclACI 属性には、事実上の規定である [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、そのディレクティブが、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、管理の容易さとパフォーマンス上の利点から、9-3 ページの「[orclEntryLevelACI](#)」で説明する `orclEntryLevelACI` の使用をお勧めします。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。

---

## Access Control Policy Points (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、そのエントリより上位のすべての 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 が設定されていて、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は、この 3 つのグループ内のいずれのエントリも、HR 部門のエントリに指定されているアクセス権限を継承します。

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：** 9-10 ページ「[アクセス制御リスト \(ACL\) の評価の動作](#)」

## orclEntryLevelACI

あるポリシーが特定のエンティティ（例：特別のユーザー）のみに関係するとき、単一のエントリ内で、そのエントリに固有の ACL ディレクティブをメンテナンスできます。Oracle Internet Directory では、`orclEntryLevelACI` と呼ばれるユーザーが変更可能な操作属性を使用して前述のディレクティブを管理できます。`orclEntryLevelACI` 属性には、関連付けられたエントリにのみ適用される ACL ディレクティブが含まれます。

いずれのディレクトリ・エントリにも、この属性の値をオプションで設定できます。それは、Oracle Internet Directory が抽象型クラス `top` を拡張し、オプション属性として `orclEntryLevelACI` を組み込むからです。

`orclEntryLevelACI` 属性は複数値の属性で、構造は `orclACI` と類似しています。構造の定義については、この章で後述します。

### 権限グループ

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ごとに、アクセス権限を指定できます。このようなグループは権限グループと呼ばれ、orclPrivilegeGroup オブジェクト・クラスと関連付けられます。

アクセス権限をユーザーのグループに付与するには、通常の方法でグループ・エントリを作成し、そのグループ・エントリを orclPrivilegeGroup オブジェクト・クラスと関連付けます。次に、そのグループに適用するアクセス・ポリシーを指定します。

エントリは、グループに対する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、他のグループに対する間接のメンバーとなることができます。所定のレベルで指定されたアクセス・ポリシーは、その下位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、権限グループとして指定されているグループのみをアクセス制御目的で評価するため、非権限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 (DN) とバインドされると、Oracle Internet Directory は、権限グループ内でそのユーザーの直接のメンバーシップを検出します。指定した DN 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権限グループに対するネストを検出します。この処理は、評価対象のネストされたグループがなくなるまで行われます。

アクセス制御目的で作成されたグループはすべて、ネストされるか、または orclPrivilegeGroup オブジェクト・クラスと関連付けて権限グループとして指定される必要があります。通常のグループは、権限グループのメンバーの場合でも、アクセス制御目的のグループとはみなされません。

たとえば、次のエントリのグループを仮定します。group4 以外は、それぞれ権限グループ (objectclass:orclprivilegegroup) として指定されています。管理者は、group1、group2 および group3 のメンバーに適用されるアクセス制御ポリシーを設定できます。

```
dn: cn=group1, c=us
cn: group1
objectclass: top
objectclass: groupofUniquenames
objectclass: orclprivilegegroup
uniquemember: cn=john smith, c=us
uniquemember: cn=joe smith, c=us
uniquemember: cn=bill smith, c=us
```

```
dn: cn=group2, c=us
cn: group2
objectclass: top
objectclass: groupofUniquenames
objectclass: orclprivilegegroup
uniquemember: cn=john smith, c=us
uniquemember: cn=joe smith, c=us
uniquemember: cn=bill smith, c=us
```

dn: cn=group3, c=us	dn: cn=group4, c=us
cn: group3	cn: group4
objectclass: top	objectclass: top
objectclass: groupofUniquenames	objectclass: groupofUniquenames
<b>objectclass: orclprivilegegroup</b>	uniquemember: cn=john smith, c=uk
uniquemember: cn=group2, c=us	uniquemember: cn=joe smith, c=uk
uniquemember: cn=group1, c=us	uniquemember: cn=bill smith, c=us
uniquemember: cn=group4, c=us	

グループ cn=group3, c=us には、次のネストされたグループが含まれています。

- cn=group2, c=us
- cn=group1, c=us
- cn=group4, c=us

group3 のアクセス制御ポリシーは、group3、group1 および group2 のメンバーに適用されます。これは、各グループが権限グループとして指定されているためです。この同じアクセス制御ポリシーは、group4 のメンバーには適用されません。これは、group4 は権限グループとして指定されていないためです。

たとえば、ユーザーが識別名 (DN) 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。これと比較して、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、そのアクセス権限は group1、group2 および group3 (group1 と group2 がネストされているため) のメンバーに対して設定されているアクセス・ポリシーで管理されます。これは、この3つのグループすべてがオブジェクト・クラス orclPrivilegeGroup と関連付けられているためです。

## アクセス制御情報のコンポーネント

ディレクトリ・オブジェクトに関連付けられているアクセス制御情報は、様々なディレクトリ・ユーザー・エンティティ (対象) が、指定したオブジェクトに対して所有している権限を表しています。したがって、ACI は次の3つのコンポーネントで構成されています。

- オブジェクト: アクセス権限を付与するオブジェクト
- 対象: アクセス権限を付与する対象
- 操作: 付与するアクセス権限の種類

## オブジェクト：アクセス権限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 DN コンポーネントは、暗黙的に最上位のエントリの Access Control Policy Points (ACP) から始まるサブツリー内のエントリすべての DN 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 DN 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、アクセス制御リスト (ACL) のオブジェクトのエントリ DN コンポーネントは、暗黙的にエントリ自体の DN 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 そのものです。ただし、これは暗黙的であるため、この DN コンポーネントは不要で、構文的にも許可されません。

アクセス制御リスト (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・セクタに組み込みます。

```
attr!=(attribute_list)
```

---

**注意：** エントリ自体に対するアクセス権限は、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限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限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：**

- コマンドライン・ツールの使用方法の例は、9-31 ページの「例：アクセス制御の管理」を参照してください。
- ACI の書式（構文）の詳細は、付録 D「アクセス制御ディレクティブ書式の使用法」を参照してください。

**対象：アクセス権限を付与する対象**

この項では、バインド・モードと呼ばれる認証モードについて説明します。このモードは、アクセス権限を付与する対象（エンティティとも呼ばれます）の識別情報の検証に使用します。

**バインド・モード** バインド・モードは、対象が使用する認証方式を指定します。次の 4 つのモードがあります。

- Simple: パスワードベースの簡易認証
- SSLNoauth: SSL ベースのクライアントに対する匿名またはパスワードベースの簡易認証
- SSLOneway: サーバーの自己認証をとまなう、SSL ベースのクライアントに対する匿名またはパスワードベースの認証
- SSLTwoway: SSL ベースのクライアントに対する SSL を使用した強化認証

バインド・モードは、対象の指定においてはオプションです。指定された場合は、ACI で指定されたモードと一致している必要があります。

**エンティティ** エンティティ・コンポーネントは、アクセス権限が付与されているエンティティを指定します。アクセスは、エントリではなくエンティティに対して付与されます。

エンティティは、次の方法で指定できます。

- すべてのエントリと一致する特別な "\*" 識別子
- アクセス権限によって保護されているエントリと一致するキーワード SELF
- エントリの識別名と一致する正規表現：dn=*regex*
- 権限グループ・オブジェクトのメンバー：group=*dn*
- アクセス権限が適用されるエントリ内の識別名（DN）値属性にリストされているエントリ：dnattr=(*dn-valued\_attribute\_name*)

dnattr 指定は、グループ・エントリの所有者としてリストされているグループ・エントリにアクセス権限を付与するために使用します。

操作：付与するアクセス権限の種類

付与するアクセス権限の種類は、次のいずれかです。

- None
- Compare/nocompare
- Search/nosearch
- Browse/nobrowse
- Read/noread
- Selfwrite/noselfwrite
- Write/nowrite
- Add/noadd
- Delete/nodelete

各アクセス・レベルを個々に付与または否認できることに注意してください。noxxx 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。

アクセス・レベル	説明
None	アクセス権限なし。対象 - オブジェクトの組合せにアクセス権限を付与しないことは、対象にとってオブジェクトがそのディレクトリに存在しないかのように見えるという効果があります。
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。
Browse	検索結果に識別名（DN）を戻すための権限。X.500 のリスト権限と同等です。この権限は、クライアントがエントリの DN を ldapsearch 操作でベース DN として使用するときにも必要です。
Compare	属性値で比較操作を実行する権限。
Delete	ターゲットのエントリを削除する権限。
Read	属性の値を読み込む権限。属性に対して読み込み権限が与えられている場合でも、エントリ自体にブラウズ権限がない限り値は戻されません。
Search	検索フィルタで属性を使用する権限。



アクセス・レベル	説明
Selfwrite	<p>DN のグループ・エン트리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 DN のみを追加または削除できます。</p> <p>access to attr=(member) by dnattr=(member) (selfwrite)</p> <p>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限が適用されるよう指定します。selfwrite アクセス権限セレクタは、そのメンバーが、属性上で自分自身の DN のみを追加または削除できるよう指定します。</p>
Write	エントリの属性を変更 / 追加 / 削除する権限。

エントリに関連付けられているアクセス権限と、属性に関連付けられているアクセス権限があることに注意してください。

エントリに対する権限：	属性に対する権限：
Browse/nobrowse	Compare/nocompare
Add/noadd	Search/nosearch
Delete/nodelete	Read/noread
None	Selfwrite/noselfwrite
	Write/nowrite
	None

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：** デフォルトでは、構造型アクセス項目とコンテンツ・アクセス項目の両方を対象に、すべての人に、エントリ内の全属性の「Read」、「Search」、「Write」および「Compare」の各アクセス権限が付与されており、「Selfwrite」権限は未指定です。エントリが未指定の場合、アクセス権限は、そのアクセス権限が指定されている直近の上位レベルで判断されます。

## アクセス制御リスト（ACL）の評価の動作

この項では、次の項目について説明します。

- [アクセス制御リスト（ACL）の評価の概要](#)
- [アクセス制御リスト（ACL）の評価の優先順位規則](#)
- [同一オブジェクトに対する複数アクセス制御項目（ACI）の割当て](#)
- [オブジェクトに対する排他的アクセス権限の付与](#)
- [グループの場合のアクセス制御リスト（ACL）評価](#)

### アクセス制御リスト（ACL）の評価の概要

要求を処理するときは、その要求者に付与されているアクセス・レベルを、要求に含まれている各属性ごとに評価する必要があります。この評価は、LDAP 操作に含まれている個々のエントリに関連付けられている各属性ごとに構造的に行われます。

あらゆるオブジェクト（エントリ内の属性）に対するアクセス権限の評価プロセスには、そのオブジェクトに適用されるすべてのアクセス制御項目（ACI）ディレクティブの検証が潜在的に含まれています。これは、Access Control Policy Points（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。

評価は、エントリのエントリ・レベルの ACI である `orclEntryLevelACI` の ACI ディレクティブの検証から始まります。評価の完了まで、直近の ACP から一連の上位 ACP まで、ACP ポリシーが継続的に考慮されます。

アクセス権限の評価は、エントリとその各属性に対して個々に行われます。Oracle Internet Directory は、エントリ・レベルのアクセス権限を評価して、指定された対象が、指定された操作の実行を許可されているかどうかを調べます。

アクセス制御リスト（ACL）の評価時には、属性は次のいずれかの状態になります。

状態	説明
Resolved with permission	属性に対して要求されたアクセスは、アクセス制御項目（ACI）で付与されています。
Resolved with denial	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限が否認される
- 属性のいずれかが「resolved with denial」の状態になる

この場合、操作は失敗し、エラーがクライアントに戻されます。

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。「resolved with denial」の属性は戻されません。

## アクセス制御リスト（ACL）の評価の優先順位規則

LDAP の操作では、LDAP セッションの BindDN（つまりサブジェクト）に、その操作で影響を受けるオブジェクトに対する特定の権限（エントリ自体に対する権限とそのエントリの個々の属性に対する権限を含む）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 Access Control Policy Points）までが 1 つの階層です。Access Control Policy Points（ACP）は、orclACI 属性の定義済みの値を持つあらゆるエントリです。また、単一のエントリ固有のアクセス情報をそのエントリ（orclEntryLevelACI）内で示すこともできます。

ACL の評価には、LDAP 操作の実行に必要な権限が対象にあるかどうかを判別する処理が含まれています。通常、orclentryLevelACI または orclACI には、ACL の評価に必要な情報がすべて含まれているわけではありません。したがって、評価が完全に解決されるまで、使用可能なすべての ACL 情報が、次の一定の順序で処理されます。

- エントリ・レベルのアクセス制御項目（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 Access Control Policy Points（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（DN）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、有効なアクセス権限が次のように評価されます。
  - 一致する by 句の項目内で付与された全権限の UNION
  - 次の場合の AND 検索
  - 一致する by 句の項目内で否認された全権限の UNION

**エントリ・レベルにおける優先順位** エントリ・レベルにおける ACI は、次の順序で評価されます。

1. フィルタを使用している場合。次のようなコマンドを実行します。

```
access to entry filter=(cn=p*)
by group1 (browse,add,delete)
```

2. フィルタを使用していない場合。次のようなコマンドを実行します。

```
access to entry
by group1 (browse,add,delete)
```

**属性レベルにおける優先順位** 属性レベルにおいては、属性が指定されている ACI が未指定の ACI よりも優先されます。

属性レベルにおいて、属性が指定されている 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もの。次のようなコマンドを実行します。

```
access to attr=(salary) filter=(salary >10000)
by group1 (read)
```

2. フィルタを使用していないもの。次のようなコマンドを実行します。

```
access to attr=(salary)
by group1 (search,read)
```

属性レベルにおいて、未指定のアクセス制御項目（ACI）は、次の順序で評価されます。

1. フィルタを使用している場合。次のようなコマンドを実行します。

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

2. フィルタを使用していない場合。次のようなコマンドを実行します。

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

### 同一オブジェクトに対する複数アクセス制御項目（ACI）の割当て

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

- ACI #1:

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

- ACI #2:

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

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

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

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

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

- ACI #1:

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

- ACI #2:

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

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

エントリに対するアクセス制御項目 (ACI) と同様に、解決策は、同じ Access Control Policy Points (ACP) においてこの属性に対して作成する ACI を 1 つのみにすることです。次のようなコマンドを実行します。

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

## オブジェクトに対する排他的アクセス権限の付与

指定したオブジェクトに ACI が存在しており、そのオブジェクト以外のすべてのオブジェクトにアクセス権限を指定する場合は、オブジェクトの指定が重複していないことを確認する必要があります。たとえば、次の 2 つの ACI が設定されているとします。

- ACI #1:

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

- ACI #2:

```
access to attr=(*) by group2 (read)
```

この場合、2 つの ACI でオブジェクトの指定が重複しています。つまり、両方の ACI が userpassword 属性にアクセス権限を付与しようとしています。ACI #2 は成功しません。これは、9-11 ページの「[アクセス制御リスト \(ACL\) の評価の優先順位規則](#)」で説明されているように、ACI #1 には属性が指定されていることによって評価プロセスが優先されるためです。ACI #1 が優先されると、group2 のユーザーが userpassword 属性にアクセスしようとしたときに、このレベルの階層でのアクセス権限が付与されません。解決するには、階層

を段階的に上に移動して評価する必要があります。解決されない場合は、すべてのアクセス権限が否認されます。

解決策は、ACI #1 と ACI #2 に次の構文を使用することです。

- ACI #1:  
access to attr=(userpassword)by group1 (read,write)by group2 (read)
- ACI #2:  
access to attr!=(userpassword)by group2 (read)

修正後の ACI #1 では、userpassword 属性に対する読み込みアクセス権限を group2 に付与しています。

修正後の ACI #2 では、userpassword 属性に対する group2 のアクセス権限を否認し、userpassword 属性以外のすべての属性に対する読み込みアクセス権限を付与しています。

グループの場合のアクセス制御リスト（ACL）評価

属性またはエントリ自体の操作が、DIT 内の下位の Access Control Policy Points（ACP）で明示的に否認されている場合、通常、ACL によるその属性（またはエントリ）の評価は、否認による解決とみなされます。しかし、そのセッションのユーザー（bindDN）がグループ・オブジェクトのメンバーの場合、評価はまだ解決されていないかのように継続されます。グループの対象セレクタを通して、ツリー内の上位の ACP でセッションのユーザーに権限が付与されている場合、この権限付与はツリー内の下位における否認よりも優先されます。

この例は、上位レベルの ACP における ACL ポリシーが、DIT 内の下位の ACP の ACL ポリシーよりも優先順位が高い場合にのみ発生します。

LDAP 操作のアクセス・レベル要件

次の表は、LDAP 操作と、各操作の実行に必要なアクセス権限をリストしたものです。

操作	必要なアクセス権限
オブジェクトの作成	親エントリに対する Add アクセス権限
変更	変更対象の属性に対する Write アクセス権限
識別名（DN）の変更	現行の親に対する Delete アクセス権限と新しい親に対する Add アクセス権限
相対識別名（RDN）の変更	ネーミング属性すなわち RDN 属性に対する Write アクセス権限
オブジェクトの削除	削除対象のオブジェクトに対する Delete アクセス権限

操作	必要なアクセス権限
Compare	属性に対する Compare アクセス権限
Search	<ul style="list-style-type: none"> <li>フィルタ属性での Search アクセス権限およびエントリでの Browse アクセス権限（エントリ DN が結果として戻される必要がある場合）</li> <li>フィルタ属性での Search アクセス権限、エントリでの Browse アクセス権限および属性での読取り権限（その値が結果として戻される必要があるすべての属性について）</li> </ul>

## Oracle Directory Manager を使用したアクセス制御の管理

Access Control Policy Points (ACP) 内に構成されているアクセス制御情報は、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を説明します。

---

**注意：** Oracle Internet Directory のインストール直後に、3-8 ページの「[タスク 3: デフォルト・セキュリティ構成の再設定](#)」の説明に従ってデフォルトのセキュリティ構成を必ずリセットしてください。

---

この項では、次の項目について説明します。

- [Oracle Directory Manager の Access Control Policy Points \(ACP\) の表示の構成](#)
- [Oracle Directory Manager を使用する場合の Access Control Policy Points \(ACP\) の検索の構成](#)
- [Oracle Directory Manager を使用した Access Control Policy Points \(ACP\) の表示](#)
- [Oracle Directory Manager を使用した既存 Access Control Policy Points \(ACP\) とそのアクセス制御項目 \(ACI\) ディレクティブの変更](#)
- [Oracle Directory Manager を使用した Access Control Policy Points \(ACP\) の追加とアクセス項目の作成](#)
- [例 : Oracle Directory Manager を使用した Access Control Policy Points \(ACP\) の管理](#)
- [Oracle Directory Manager を使用したエントリ・レベルのアクセス権限の付与](#)

**関連項目：** コマンドライン・ツールの説明は、[付録 A 「LDIF およびコマンドライン・ツールの構文」](#)を参照してください。

## Oracle Directory Manager の Access Control Policy Points (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 Servers」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「User Preferences」をクリックします。「User Preferences」ダイアログ・ボックスが表示されます。
3. 「Configure Access Control Policy Management」タブ・ページを選択します。
4. 「Configure Access Control Policy Management」タブ・ページで、次のいずれかを選択します。
  - 「Always display all ACPs」
  - 「Only display ACPs based on search request」
5. 「OK」をクリックします。

---

---

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

---

---

## Oracle Directory Manager を使用する場合の Access Control Policy Points (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 Servers」>「*directory\_server*」の順に展開して、「Access Control Management」を選択します。
2. ツールバーの「Configure ACPs Search」をクリックします。「Configure ACPs Search」ダイアログ・ボックスが表示されます。
3. 「Root of the Search」フィールドに検索のルートの DN を入力するか、「Browse」をクリックしてそこまでナビゲートします。



4. 「Max Results (entries)」フィールドに、ACP 検索で取り出すエントリの数を入力します。
5. 「Max Search Time (seconds)」フィールドに、検索の最大時間を秒単位で入力します。
6. 「Search Depth」のリストで、検索するレベルを選択します。オプションは次のとおりです。
  - One Level: 検索のルートの 1 レベル下のすべての ACP エントリに検索を制限する場合に選択します。
  - Subtree: 検索のルートを含め、サブツリー全体のエントリを検索する場合に選択します。
7. 「OK」をクリックします。

## Oracle Directory Manager を使用した Access Control Policy Points (ACP) の表示

9-16 ページの「[Oracle Directory Manager の Access Control Policy Points \(ACP\) の表示の構成](#)」の説明に従って検索の結果としてのみ ACP を表示するように Oracle Directory Manager を構成した場合に、ACP の位置を特定し表示する手順は次のとおりです。

1. 「Oracle Internet Directory Servers」 > 「*directory\_server*」の順に展開し、「Entry Management」を選択します。ACP として指定したエントリの検索を実行します。検索結果が右側のペインの下半分の「Distinguished Name」ボックスに表示されます。
2. 「Distinguished Name」ボックスで、エントリをダブルクリックします。対応する「Entry」ダイアログ・ボックスが表示されます。
3. この ACP のサブツリーのアクセス制御を表示するには、「Subtree Access」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、「Local Access」タブを選択します。

9-16 ページの「[Oracle Directory Manager の Access Control Policy Points \(ACP\) 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 Servers」 > 「*directory\_server*」 > 「Access Control Management」の順に展開します。ナビゲータ・ペインの「Access Control Management」の下と右側のペインに、定義済の Access Control Policy Points (ACP) がすべて表示されます。
2. ナビゲータ・ペインで「Access Control Management」の下に 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。

または右側のペインの Access Control Policy Points (ACP) をダブルクリックすると、その同じウィンドウにデータが表示されます。

「Access Control Management」 ペインには次の 3 つのフィールドがあります。

フィールド	説明
Path to the Subtree Access Control Point	Access Control Policy Points (ACP) で定義されているパスが表示されます。このポイントまでツリーを下位方向へナビゲートすると、このポイントへのパスがこのフィールドに表示されます。新しい ACP を作成する場合は、このフィールドに新規 ACP へのパスを入力する必要があります。
Structural Access Items (Entry Level Operations)	<p>エントリへのアクセス権限のリストです。「Structural Access Items」ボックスにリストされている項目は、次のカテゴリによってエントリを識別します。</p> <ul style="list-style-type: none"><li>■ By Whom: アクセス権限を付与する人またはエンティティ (対象)</li><li>■ Bind Mode: バインド・モード (認証) が使用されているかどうか</li><li>■ Access rights: 「Browse」、「Add」 および 「Delete」</li></ul> <p><b>関連項目:</b> 体系的なアクセス項目の変更方法は、9-23 ページの「<a href="#">Oracle Directory Manager を使用した既存 Access Control Policy Points (ACP) の構造型アクセス項目の変更</a>」を参照してください。</p>
Content Access Items (Attribute Level Operations)	<p>「Entry Filter」列で指定するエントリ内の属性に関連する項目のリストです。このウィンドウには次の列があります。</p> <ul style="list-style-type: none"><li>■ By Whom: アクセス権限を付与する人またはエンティティ (対象)</li><li>■ Bind Mode: バインド・モード (認証) が使用されているかどうか</li><li>■ Op: 属性に対して実行される一致操作。選択肢は「EQ」(=) と「NEQ」(!=) です。</li><li>■ Attribute: アクセス権限が付与または否認される特定の属性 (オブジェクト)。</li><li>■ Access rights: 「Read」、「Search」、「Write」、「Selfwrite」または「Compare」。</li></ul> <p><b>関連項目:</b> コンテント・アクセス項目の変更方法は、9-25 ページの「<a href="#">Oracle Directory Manager を使用した既存 Access Control Policy Points (ACP) のコンテント・アクセス項目の変更</a>」を参照してください。</p>

## Oracle Directory Manager を使用した既存 Access Control Policy Points (ACP) とそのアクセス制御項目 (ACI) ディレクティブの変更

ACP は、規定の、すなわち継承可能なアクセス制御情報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。

この項では、次の項目について説明します。

- [Oracle Directory Manager を使用した既存 Access Control Policy Points \(ACP\) への構造型アクセス項目の追加](#)
- [Oracle Directory Manager を使用した既存 Access Control Policy Points \(ACP\) へのコンテンツ・アクセス項目の追加](#)
- [Oracle Directory Manager を使用した既存 Access Control Policy Points \(ACP\) の構造型アクセス項目の変更](#)
- [Oracle Directory Manager を使用した既存 Access Control Policy Points \(ACP\) のコンテンツ・アクセス項目の変更](#)

### Oracle Directory Manager を使用した既存 Access Control Policy Points (ACP) への構造型アクセス項目の追加

9-16 ページの「[Oracle Directory Manager の Access Control Policy Points \(ACP\) 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、ナビゲートして既存 ACP に構造型アクセス項目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」 > 「*directory server*」 > 「Access Control Management」の順に展開します。「Access Control Management」を選択します。「Access Control Management」の下にリストに、定義済みのすべての Access Control Policy Points (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。
2. ナビゲータ・ペインで「Access Control Management」の下に 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。
3. 「Structural Access Items」ボックスの下に「Create」をクリックします。「Structural Access Items」ダイアログ・ボックスに、「Entry Filter」、「By Whom」および「Access Rights」の 3 つのタブが表示されます。
4. 「Entry Filter」タブ・ページを使用して、アクセス権限を付与するエントリのセットを絞り込みます。ACP の下位エントリすべてを ACP で管理する場合は、このタブ・ページを使用する必要はありません。

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 administrative assistant の個人をすべて検索したり、title が manager で organization unit が Americas の個人をすべて検索できます。

「Entry Filter」タブ・ページの「Criteria」ボックスで、検索基準バーを使用して属性を選択し、その属性の値を入力し、さらに指定した属性と入力値との一致条件を示すフィルタを指定します。この手順は、次のとおりです。

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

フィルタ	説明
Begins With	属性値の始めの数文字のみ使用して検索します。
Ends With	指定した属性値の終わりの数文字のみ使用してエントリを検索します。
Contains	値の位置を限定せずに、指定した属性に入力値が含まれているエントリを検索します。
Exact Match	指定した属性が入力値に一致するエントリを検索します。
Greater or Equal	指定した属性が、数値順またはアルファベット順で入力値より大か等しいエントリを検索します。アルファベットの先頭により近いエントリが、アルファベット順で上位とされます。
Less or Equal	指定した属性が、数値順またはアルファベット順で入力値より小か等しいエントリを検索します。アルファベットの先頭により近いエントリが、アルファベット順で下位とされます。
Present	指定した属性を持つエントリがツリーのそのレベルに存在するかどうかを判断します。この関連の使用に値の入力は不要です。たとえば、「cn」 「Present」と指定すると、ツリーのそのレベルで、cn 属性値を持つすべてのエントリが取り出されます。

- c. 検索基準バーの一番右のテキスト・フィールドに、選択した属性の値を入力します。

5. 「By Whom」タブ・ページを選択して、ACI の対象を定義します。

- a. 対象（アクセス権限を要求しているエンティティ）が使用する認証のタイプ（バインド・モードとも呼びます）を指定します。バインド・モードは、対象の指定においてはオプションです。ただし、ディレクティブを適用する場合、ノードで指定されているバインド・モードは、通信先のノードで指定されているバインド・モードと一致している必要があります。

次の 5 つのバインド・モードの中から選択します。

バインド・モード	説明
None	認証なし。
SSL No Authentication	クライアントとサーバーのいずれも、他方に対して自己認証を行いません。証明書の送信または交換は行われません。この場合は、SSL 暗号化 / 復号化のみ使用されます。
SSL One Way	Directory Server のみ、クライアントに対して自己認証を行います。Directory Server 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 Two Way	クライアントとサーバーは、相互に自己認証を行います。これは、相互に証明書を送信する方法で行われます。
Simple	クライアントは、ネットワーク上を平文で送信される識別名 (DN) とパスワードによって、サーバーに対して自己認証を行います。サーバーは、クライアントが送信した DN とパスワードが、ディレクトリに保存されている DN とパスワードに一致しているかどうかを検証します。

アクセス権限を付与するエンティティを指定します。オプションは次のとおりです。

エンティティ	説明
Everyone (*)	エントリにアクセスする人すべて。
A Specific Group	事前に定義したグループ名。
A Specific Entry	事前に定義したディレクトリ・エントリ。
A Subtree	ディレクトリ内の選択したサブツリー全体。
When Session User's Distinguished Name (DN) Is Identified by Attribute	識別名 (DN) 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み込みアクセス権限をグループのメンバーに付与する場合があります。
When Session User's Distinguished Name (DN) Matches the Accessed Entry	指定したエントリで正常にログインしている人すべて。

b. 「OK」をクリックします。

6. 「Access Rights」タブ・ページを選択します。

a. 適切なオプションを選択して、付与する権限の種類（「Browse」、「Add」または「Delete」）を指定します。

- b. 「OK」をクリックして「Structural Access Items」ダイアログ・ボックスを閉じ、Oracle Directory Manager のメイン・ウィンドウに戻ります。設定した構造型アクセス制御項目（ACI）が、Oracle Directory Manager のメイン・ダイアログ・ボックスの「Structural Access Items」ウィンドウにリストされます。

## Oracle Directory Manager を使用した既存 Access Control Policy Points (ACP) へのコンテンツ・アクセス項目の追加

9-16 ページの「[Oracle Directory Manager の Access Control Policy Points \(ACP\) 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 を構成した場合に、ナビゲートして既存 ACP へコンテンツ・アクセス項目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 Servers」>「*directory server*」>「Access Control Management」の順に展開します。「Access Control Management」を選択します。ナビゲータ・ペインの「Access Control Management」の下にリストに、定義済みのすべての Access Control Policy Points (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。
2. ナビゲータ・ペインで「Access Control Management」の下に 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。右側のペインの ACP をダブルクリックすると、その同じダイアログ・ボックスにデータが表示されます。
3. 「Content Access Items」ウィンドウで、変更するコンテンツ・アクセス項目を選択します。
4. 「Content Access Item」ボックスの下に「Create」をクリックします。「Content Access Items」ダイアログ・ボックスが表示されます。
5. 9-19 ページの「[Oracle Directory Manager を使用した既存 Access Control Policy Points \(ACP\) への構造型アクセス項目の追加](#)」の説明に従って、「Entry Filter」タブ・ページの各項目（適用可能な場合）を指定します。
6. 「By Whom」タブ・ページを選択して、9-19 ページの「[Oracle Directory Manager を使用した既存 Access Control Policy Points \(ACP\) への構造型アクセス項目の追加](#)」の説明に従って各項目を指定します。
7. 「Attribute」タブ・ページを選択します。
  - a. 右のリストから、アクセス権限を付与または否認する属性を選択します。
  - 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。
8. 「Access Rights」タブ・ページを選択して、9-19 ページの「[Oracle Directory Manager を使用した既存 Access Control Policy Points \(ACP\) への構造型アクセス項目の追加](#)」の説明に従って各項目を指定します。
9. 「OK」をクリックします。

## Oracle Directory Manager を使用した既存 Access Control Policy Points (ACP) の構造型アクセス項目の変更

9-16 ページの「[Oracle Directory Manager の Access Control Policy Points \(ACP\) 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、ナビゲートして既存 ACP の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. ナビゲータ・ペインで、「Oracle Internet Directory Servers」 > 「*directory server*」 > 「Access Control Management」の順に展開します。「Access Control Management」を選択します。ナビゲータ・ペインの「Access Control Management」の下の一覧に、定義済みのすべての Access Control Policy Points (ACP) が表示されます。同じ内容の一覧が、右側のペインにも表示されます。
2. ナビゲータ・ペインで「Access Control Management」の下の一覧の 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。
3. 「Structural Access Items」ウィンドウで変更する項目を選択し、「Structural Access Items」ウィンドウの下の一覧の「Edit」をクリックします。「Structural Access Item」ダイアログ・ボックスが表示されます。
4. 「Entry Filter」タブ・ページを使用して、アクセス権限を付与するエントリのセットを絞り込みます。ACP の下位エントリすべてを ACP で管理する場合は、次のステップに進んでください。

1 つ以上の属性に基づいてエントリを選択する場合があります。たとえば、title が secretary の個人をすべて検索したり、title が manager で organization unit が Americas の個人をすべて検索することができます。

「Entry Filter」タブ・ページの「Criteria」ウィンドウで、検索基準バーを使用して属性を選択し、その属性の値を入力し、さらに指定した属性と入力値との一致条件を示すフィルタを指定します。この手順は、次のとおりです。

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

フィルタ	説明
Begins With	属性値の始めの数文字のみ使用して検索します。
Ends With	指定した属性値の終わりの数文字のみ使用してエントリを検索します。
Contains	値の位置を限定せずに、指定した属性に入力値が含まれているエントリを検索します。
Exact Match	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。
Greater or Equal	指定した属性が、数値順またはアルファベット順で入力値より大か等しいエントリを検索します。アルファベットの先頭により近いエントリが、アルファベット順で上位です。

フィルタ	説明
Less or Equal	指定した属性が、数値順またはアルファベット順で入力値より小か等しいエントリを検索します。アルファベットの先頭により近いエントリが、アルファベット順で下位です。
Present	指定した属性を持つエントリがツリーのそのレベルに存在するかどうかを判断します。この関連の使用に値の入力は不要です。たとえば、「cn」「Present」と指定すると、ツリーのそのレベルで、cn 属性値を持つエントリがすべて取り出されます。

- c. 検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。
5. 「By Whom」タブ・ページを選択します。
- a. 対象（アクセス権限を要求しているエンティティ）が使用する認証のタイプ（バインド・モードとも呼びます）を指定します。次の 5 つのバインド・モードの中から選択します。

バインド・モード	説明
None	認証なし。
SSL No Authentication	クライアントとサーバーのいずれも、他方に対して自己認証を行いません。証明書の送信または交換は行われません。この場合は、SSL 暗号化 / 復号化のみ使用されます。
SSL One Way	Directory Server のみ、クライアントに対して自己認証を行います。Directory Server 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 Two Way	クライアントとサーバーは、相互に自己認証を行います。これは、相互に証明書を送信する方法で行われます。
Simple	クライアントは、ネットワーク上を平文で送信される識別名（DN）とパスワードによって、サーバーに対して自己認証を行います。サーバーは、クライアントが送信した DN とパスワードが、ディレクトリに保存されている DN とパスワードに一致しているかどうかを検証します。

- バインド・モードは、対象の指定においてはオプションです。ディレクティブを適用する場合、あるノードで指定されているバインド・モードは、通信先のノードで指定されているバインド・モードと一致する必要があります。
- b. アクセス権限を付与するエンティティを指定します。



エンティティ	説明
Everyone (*)	エントリにアクセスする人すべて。
A Specific Group	事前に定義したグループ名。
A Specific Entry	事前に定義したディレクトリ・エントリ。
A Subtree	ディレクトリ内の選択したサブツリー全体。
When Session User's Distinguished Name (DN) Is Identified by Attribute	識別名 (DN) 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み込みアクセス権限をグループのメンバーに付与する場合があります。
When Session User's Distinguished Name (DN) Matches the Accessed Entry	指定したエントリで正常にログインしている人すべて。

6. 「Access Rights」タブ・ページを選択します。
  - a. 付与する権限の種類（「Browse」、「Add」、「Delete」または「Unspecified」）を決定します。エントリが未指定の場合、アクセス権限は、そのアクセス権限が指定されている直近の上位レベルで判断されます。
  - b. 「OK」をクリックします。

## Oracle Directory Manager を使用した既存 Access Control Policy Points (ACP) のコンテンツ・アクセス項目の変更

9-16 ページの「[Oracle Directory Manager の Access Control Policy Points \(ACP\) 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、ナビゲートして既存 ACP のコンテンツ・アクセス項目を変更する手順は次のとおりです。

1. ナビゲータ・ペインで、「Oracle Internet Directory Servers」>「*directory server*」>「Access Control Management」の順に展開します。「Access Control Management」を選択します。ナビゲータ・ペインの「Access Control Management」の下にリストに、定義済みのすべての Access Control Policy Points (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。
2. 「Access Control Management」の下に 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。右側のペインの ACP をダブルクリックすると、その同じダイアログ・ボックスにデータが表示されます。
3. 「Content Access Items」ボックスで、変更するコンテンツ・アクセス項目を選択します。
4. 「Content Access Item」ウィンドウの下に「Edit」をクリックします。「Content Access Items」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。

5. 9-23 ページの「[Oracle Directory Manager を使用した既存 Access Control Policy Points \(ACP\) の構造型アクセス項目の変更](#)」の説明に従って、「Entry Filter」タブ・ページの各項目（適用可能な場合）を指定します。
6. 「By Whom」タブ・ページを選択して、9-23 ページの「[Oracle Directory Manager を使用した既存 Access Control Policy Points \(ACP\) の構造型アクセス項目の変更](#)」の説明に従って各項目を指定します。
7. 「Attribute」タブ・ページを選択します。
  - a. 右のメニューから、アクセス権限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。
8. 「Access Rights」タブ・ページを選択して、9-23 ページの「[Oracle Directory Manager を使用した既存 Access Control Policy Points \(ACP\) の構造型アクセス項目の変更](#)」の説明に従って各項目を指定します。
9. 「OK」をクリックします。

## Oracle Directory Manager を使用した Access Control Policy Points (ACP) の追加とアクセス項目の作成

新規 ACP 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 Servers」>「*directory server*」の順に展開します。「Access Control Management」を選択します。
2. ツールバーの「Create」ボタンをクリックします。「New Access Control Point」ダイアログ・ボックスが表示されます。
3. 「Path To Entry」フィールドで、ACP に指定するエントリの識別名 (DN) を入力します。

---

**注意：** DN を検索するには、ナビゲータ・ペインでそのエントリを探るか、または「Browse」をクリックします。

---

4. 構造型アクセス項目（エントリ）を定義するには、「Structural Access Items」ウィンドウの下「Create」をクリックします。「Structural Access Item」ダイアログ・ボックスが表示されます。9-23 ページの「[Oracle Directory Manager を使用した既存 Access Control Policy Points \(ACP\) の構造型アクセス項目の変更](#)」の説明に従って、このダイアログ・ボックスの各タブ・ページを使用します。
5. コンテント・アクセス項目（属性）を定義するには、「Content Access Items」ウィンドウの下「Create」をクリックします。「Content Access Item」ダイアログ・ボックスが表示されます。9-25 ページの「[Oracle Directory Manager を使用した既存 Access](#)

[Control Policy Points \(ACP\) のコンテンツ・アクセス項目の変更](#) の説明に従って、このダイアログ・ボックスの各タブ・ページを使用します。

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。

## 例：Oracle Directory Manager を使用した Access Control Policy Points (ACP) の管理

この例では、Oracle Directory Manager を使用して、アクセス制御項目 (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限を制限して、比較はすべての人が可能に、読み込みと変更は各パスワードの所有者 (つまり、ユーザー) のみ可能に設定する場合の例です。

この例では、新しい ACP を作成し、その ACP に次の各権限を設定する 4 つの ACI を移入します。

- すべての人による userpassword 属性に対する制限付きアクセス権限
- 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限
- すべての属性に対する開かれたアクセス権限 (すべての人による userpassword に対するアクセス権限を除く)
- 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限

### 新規 Access Control Policy Points (ACP) の作成

1. ナビゲータ・ペインで、「Oracle Internet Directory Servers」 > 「*directory server*」の順に展開し、「Access Control Management」を選択します。ACP のリストが右側のペインに表示されます。
2. 右側のペインの下の「Create」ボタンをクリックします。「New Access Control Point」ダイアログ・ボックスが表示されます。
3. 「Path To Entry」フィールドで、ACP に指定する識別名 (DN) を入力します。ACP 内の ACI は、すべての下位エントリ (その DN も含めて) に適用されます。

**構造型アクセス項目** エントリに対するアクセス権限を設定する手順は次のとおりです。

1. 「Structural Access Items」ボックスの下で「Create」をクリックします。「Structural Access Item」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、「Entry Filter」、「By Whom」および「Access Rights」の 3 つのタブがあります。  
  
Access Control Policy Points (ACP) の下位エントリすべてにアクセス制御項目 (ACI) を適用するため、「Entry Filter」タブ・ページは使用しません。
2. 「By Whom」タブ・ページを選択して、ACI の対象を定義します。「Bind Mode」リストから、使用中の環境に適した認証モードを選択します。すべての人に対するアクセス権限を作成するには、「Everyone」を選択します。「OK」をクリックします。

3. 「Access Rights」タブ・ページを選択します。デフォルトでは、すべての権限（「Browse」、「Add」および「Delete」）が付与されています。
  - a. すべての人が全エントリをブラウズでき、追加や削除はできないようにアクセス権限を変更します。
  - b. 「OK」をクリックします。

**コンテンツ・アクセス項目** この例の4つのアクセス制御項目（ACI）は、同じ体系のコンテンツ項目情報を使用します。これらは、許可するコンテンツ・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. 「Content Access Items」ボックスの下に「Create」をクリックします。「Content Access Items」ダイアログ・ボックスが表示されます。

Access Control Policy Points（ACP）のすべての下位エントリにこのアクセス制御項目（ACI）を適用するため、「Entry Filter」タブ・ページは使用しません。
  2. 「By Whom」タブ・ページを選択し、「Everyone」を選択して「OK」をクリックします。
  3. 「Attribute」タブ・ページを選択します。このページには2つのフィールドがあります。最初のフィールドの選択肢は、「EQ」（等価）と「NEQ」（非等価）です。2番目には、属性を設定します。

「EQ」を選択して、「userPassword」を選択します。
  4. 「Access Rights」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。読み込み、検索、書き込みおよび比較を否認するように権限を変更します。
  5. 「OK」をクリックします。
- これで1番目のアクセス制御項目（ACI）の設定は完了です。

## 2番目のアクセス制御項目（ACI）の作成

ユーザーに、本人のパスワードの読み込み、書き込み、検索および比較を許可する2番目のACIを作成します。

1. 「Content Access Items」ボックスの下に「Create」をクリックします。「Content Access Items」ダイアログ・ボックスが表示されます。
2. 「By Whom」タブ・ページを選択します。「When Session User's Distinguished Name (DN) Matches the Accessed Entry」をクリックし、「OK」をクリックします。
3. 「Attribute」タブ・ページを選択します。このタブ・ページには、2つのリストがあります。最初のリストの選択肢は、「EQ」（等価）と「NEQ」（非等価）です。2番目には、属性を設定します。

「EQ」と「userPassword」を選択します。

4. 「Access Rights」タブ・ページを選択します。

読み込み、検索、書き込みおよび比較の各アクセス権限を付与します。「Selfwrite」は未指定のままにします。

5. 「OK」をクリックします。

これで2つの Access Control Policy Points (ACP) が作成されました。1番目の ACP は、userPassword 属性の読み込み、検索、書き込みおよび比較の各アクセス権限をすべての人の否認しています。2番目の ACP は、パスワードの所有者に対して、その属性の読み込み、検索、書き込みおよび比較を許可しています。

### 3 番目のアクセス制御項目 (ACI) の作成

次の ACI は、userPassword を除くすべての属性の読み込み、検索および比較の各アクセス権限を、すべての人に付与します。書き込みアクセス権限は否認します。

1. 「Content Access Items」フィールドの下に「Create」をクリックして、「Content Access Items」を表示します。

2. 「By Whom」タブ・ページを選択します。

「Everyone」を選択して、「OK」をクリックします。

3. 「Attribute」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、このアクセス制御項目 (ACI) の権限の対象であることを示しています。

4. 「Access Rights」タブ・ページを選択します。

読み込み、検索および比較の各アクセス権限を付与します。「Write」アクセス権限は否認します。「Selfwrite」は未指定のままにします。

5. 「OK」をクリックしてこれらの権限を適用し、ダイアログ・ボックスを閉じます。

### 4 番目のアクセス制御項目 (ACI) の作成

次の ACI は、userpassword を除くすべての属性の読み込み、ブラウズおよび書き込みの各アクセス権限を、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限がその属性の所有者と他の人と同じになるというあいまいさを排除できます。

1. 「Content Access Items」フィールドの下に「Create」をクリックして、「Content Access Items」ダイアログ・ボックスを表示します。

2. 「By Whom」タブ・ページを選択します。

「When Session User's Distinguished Name (DN) Matches the Accessed Entry」をクリックします。「OK」をクリックします。

3. 「Attribute」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、このアクセス制御項目（ACI）の権限の対象であることを示しています。

4. 「Access Rights」タブ・ページをクリックします。

読み込み、検索および書き込みの各アクセス権限を付与します。「Selfwrite」は未指定のままにします。

5. 「OK」をクリックしてこれらの権限を適用し、ダイアログ・ボックスを閉じます。

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

## Oracle Directory Manager を使用したエントリ・レベルのアクセス権限の付与

Oracle Directory Manager を使用してエントリ・レベルのアクセス権限を付与する手順は、次のとおりです。

1. ナビゲータ・ペインで、「Oracle Internet Directory Servers」>「*directory server*」>「Entry Management」の順に展開します。次のいずれかの方法で起動できます。
  - エントリを選択して、右側のペインにそのプロパティを表示します。
  - 検索パネルを使用してエントリを検索し、エントリをダブルクリックして「Entry」ダイアログ・ボックスを開きます。
2. 「Local Access」タブ・ページを選択して、「Structural Access Item」ボックスと「Content Access Item」ボックスで、ローカル・アクセス制御項目（ACI）を作成および編集します。
3. 変更後、Oracle Directory Manager のメイン・ウィンドウで「Apply」をクリックします。

---

**注意：** 入力した情報を Directory Server に送信するには、「Apply」をクリックする必要があります。「Apply」をクリックしないと、入力した情報は、単に Oracle Directory Manager のキャッシュに入れられます。

---

## コマンドライン・ツールを使用したアクセス制御の管理

9-2 ページの「[アクセス制御ポリシーの管理の概要](#)」で説明したように、ディレクトリのアクセス制御ポリシーの情報は、ユーザーが変更可能な操作属性で表されます。したがって、`ldapmodify` コマンドでこれらの属性の値を設定および変更して、ディレクトリのアクセス制御を管理できます。`ldapmodify` や `ldapmodifymt` などのツールがこのために使用できます。

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。この項では、ACI 書式の正式な仕様を紹介し、コマンドライン・ツールで ACI を管理するために必要な構文の問題について説明します。

### 関連項目：

- コマンドライン・モードのコマンドに必須の入力フォーマットである [LDAP データ交換フォーマット \(LDIF\)](#) を使用した入力ファイルのフォーマット方法は、A-2 ページの「[LDAP データ交換フォーマット \(LDIF\) の構文](#)」を参照してください。
- `ldapmodify` の実行方法は、A-12 ページの「[ldapmodify 構文](#)」を参照してください。
- ACI の書式（構文）の詳細は、[付録 D「アクセス制御ディレクティブ書式の使用法」](#)を参照してください。

## 例：アクセス制御の管理

この項では、次の項目について説明します。

- 例：[ldapmodify](#) を使用した継承可能な Access Control Policy Points (ACP) の設定
- 例：[ldapmodify](#) を使用したエントリ・レベルのアクセス制御項目 (ACI) の設定
- 一般的なアクセス制御ポリシー

### 例：[ldapmodify](#) を使用した継承可能な Access Control Policy Points (ACP) の設定

この例では、[ルート DSE](#) で、`orclACI` にサブツリーのアクセス権限を設定します。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 DIT のエントリすべてを制御します。

<< EOF の記述があることに注意してください。

```
ldapmodify -v -h $1 -D "cn=Directory Manager, o=IMC, c=US" -w "controller" << EOF
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)

EOF
```

### 例：ldapmodify を使用したエントリ・レベルのアクセス制御項目（ACI）の設定

この例では、orclEntryLevelACI 属性にエントリ・レベルのアクセス権限を設定します。このアクセス制御リスト（ACL）は orclEntryLevelACI 属性に常駐しているため、この属性が含まれているエントリのみ制御します。<< EOF の記述があることに注意してください。

```
ldapmodify -v -h $1 -D "cn=Directory Manager, o=IMC, c=US" -w "controller" << EOF
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)

EOF
```

---

---

**注意：** この例では、DN 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。

---

---

### 一般的なアクセス制御ポリシー

この項では、次に示す一般的かつ高度なアクセス制御ポリシー・サンプルを紹介します。

- [例：ワイルド・カードの使用法](#)
- [例：識別名（DN）によるエントリの選択](#)
- [例：属性セクタと対象セクタの使用法](#)
- [例：読取り専用アクセス権限の付与](#)
- [例：グループ・エントリへの Selfwrite アクセス権限の付与](#)



**例：ワイルド・カードの使用法** この例では、オブジェクトと対象指定子にワイルド・カード (\*) を使用しています。acme.com ドメイン内のエントリすべてに対して、すべての属性の読み込みおよび検索権限の他に、すべてのエントリのブラウズ権限をすべての人に付与します。

dc=com の Access Control Policy Points (ACP) 内の orclACI 属性

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

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

**例：識別名 (DN) 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 DN を使用してエントリを選択する際の正規表現の使用法を示します。dc=acme、dc=com の下のすべての人に、address book 属性のみの読み込みアクセス権限を付与します。これにより、すべての属性に対する読み込みアクセス権限を、dc=us、dc=acme、dc=com 内の人のみに制限します。

dc=acme、dc=com の orclACI 属性

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

dc=us、dc=acme、dc=com の orclACI 属性

```
access to entry by * (browse)
access to attr=(*) by dn="*.*,dc=us,dc=acme,dc=com" (search, read)
```

**例：属性セクタと対象セクタの使用法** この例では、特定の属性に対するアクセス権限を付与する属性セクタ、および様々な対象セクタの使用法を示します。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。このアクセス制御項目 (ACI) によって実施されるポリシーは次のとおりです。

- 管理者はサブツリー内のすべてのエントリに対する追加、削除およびブラウズ権限を所有しています。dc=us サブツリー内のその他のユーザーはサブツリーのブラウズが可能ですが、サブツリー外部のユーザーはそのサブツリーにアクセスできません。
- salary 属性は、そのマネージャによる変更が可能で、本人は参照できます。その他のユーザーは salary 属性にアクセスできません。
- userPassword 属性は、パスワードの所有者と管理者による表示および変更が可能です。その他のユーザーは、この属性の比較のみ可能です。
- homePhone 属性は、本人による読み込みおよび書き込みが可能で、参照はどのユーザーも可能です。
- その他のすべての属性は、管理者のみ値の変更が可能です。その他のすべてのユーザーは、比較、検索、読み込みは可能ですが、属性の値の更新はできません。

dc=us、dc=acme、dc=com の orclACI 属性

```
access to entry
by dn="cn=admin, dc=us,dc=acme,dc=com" (browse, add, delete)
by dn=".*, dc=us,dc=acme,dc=com" (browse)
by * (none)
```

```
access to attr=(salary)
by dnattr=(manager) (read, write)
by self (read)
by * (none)
```

```
access to attr=(userPassword)
by self (search, read, write)
by dn="cn=admin, dc=us,dc=acme,dc=com" (search, read, write)
by * (compare)
```

```
access to attr=(homePhone)
by self (search, read, write)
by * (read)
```

```
access to attr != (salary, userPassword, homePhone)
by dn="cn=admin, dc=us,dc=acme,dc=com" (compare, search, read, write)
by * (compare, search, read)
```

**例：読取り専用アクセス権限の付与** この例では、dc=acme、dc=com の下のすべての人に、address book 属性の読込み専用のアクセス権限を付与します。さらに、dc=us、dc=acme、dc=com サブツリー内のすべての属性に限定した読込みアクセス権限をすべての人に付与します。

dc=acme、dc=com の orclACI 属性

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

dc=us、dc=acme、dc=com の orclACI 属性

```
access to entry by * (browse)
access to attr=(*) by dn=".*,dc=us,dc=acme,dc=com" (search, read)
```

**例：グループ・エントリへの Selfwrite アクセス権限の付与** 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（DN）の追加または削除のみを行うアクセス権限を許可します。

当該のグループ・エントリの orclEntryLevelACI 属性

```
access to attr=(member)
by dn=".*, dc=us,dc=acme,dc=com" (selfwrite)
```



---

## ディレクトリ・レプリケーションの管理

---

レプリケーションは、複数のノードで、指定したネーミング・コンテキストの完全な複製をメンテナンスする機能です。

---

**注意：** リリース 2.1.1 で、Oracle Internet Directory のレプリケーションが使用できるのは、[アドバンスト・レプリケーション](#)をインストールしている場合のみです。これは、Oracle Internet Directory のスタンドアロンでの購入および Oracle8i Enterprise Edition に付属しています。アドバンスト・レプリケーションは、Oracle8i Standard Edition には含まれません。

---

この章では、次の項目について説明します。

- [レプリケーションのインストールと構成](#)
- [レプリケーション・ノードの追加](#)
- [レプリケーション・ノードの削除](#)
- [手動での競合の解消](#)

**関連項目：** レプリケーションの概念の説明は、2-23 ページの「[分散ディレクトリ：レプリケーション](#)」を参照してください。

## レプリケーションのインストールと構成

この項では、Oracle Directory Replication Server ソフトウェアをノードにインストールおよび初期設定する方法を説明します。

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

---

**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。既存の DRG にノードを追加する方法は、10-19 ページの「**レプリケーション・ノードの追加**」を参照してください。

---

レプリケーション・グループをインストールおよび構成するには、次の一般的なタスクを実行します。

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

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

タスク 3: MDS における、ディレクトリ・レプリケーション・グループ用のアドバンスト・レプリケーションの設定

タスク 4: 全ノードでの **Oracle Directory Server** インスタンスの起動

タスク 5: レプリケーションの構成

タスク 6: 全ノードでの **Replication Server** の起動

---

**注意：** **Oracle Internet Directory** リリース 2.1.1 には、複数の DRG で構成されている環境（ディレクトリ・ネットワーク）を作成するプロシージャとツールは用意されていません。

---

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

Oracle Internet Directory に必要な Oracle8i Enterprise Edition を通常の方法でインストールすると、**アドバンスト・レプリケーション**もインストールされます。これに対して、Oracle8i Standard Edition を通常の方法でインストールしても、アドバンスト・レプリケーションはインストールされません。

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

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

**マスター定義サイト**は任意の Oracle Internet Directory データベースで、管理者はそのデータベースで構成スクリプトを実行します。リモート・マスター・サイトとは、マスター定義サイト以外のサイトで、アドバンスト・レプリケーションのメンバーであるすべてのサイトのことです。

管理者は **Net8** を使用して、DRG を構成している MDS データベースとその他の全ノードに接続することが必要です。

## タスク 3: MDS における、ディレクトリ・レプリケーション・グループ用のアドバンスト・レプリケーションの設定

次の各項では、Oracle Internet Directory のインストレーション・スクリプトを使用して、アドバンスト・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。アドバンスト・レプリケーションの上級ユーザーは、Oracle8i Replication Manager ツールを使用してアドバンスト・レプリケーションを構成することもできます。

**関連項目：** Oracle8i Replication Manager ツールでアドバンスト・レプリケーションを構成する方法は、Oracle8i Server レプリケーションのドキュメントおよび Oracle8i Replication Manager 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) を設定するためにアドバンスト・レプリケーション環境を設定するには、次のことが必要です。

- レプリケーション用の Net8 環境の準備
- ディレクトリ・レプリケーション用のアドバンスト・レプリケーションの構成

### レプリケーション用の Net8 環境の準備

Net8 環境を準備するには、ディレクトリ・レプリケーション・グループのすべてのノードで、次の各ステップを実行します。詳細は後述します。

1. `sqlnet.ora` を構成します。
2. `tnsnames.ora` を構成します。
3. ロールバック表領域とロールバック・セグメントを作成します。
4. 初期化パラメータ・ファイル `init.ora` 内のパラメータを変更します。
5. リスナーを停止して、再起動します。
6. **Oracle Internet Directory** データベースを停止して、再起動します。

Net8 環境をレプリケーション用に準備する手順は、次のとおりです。

1. `sqlnet.ora` を構成します。

`sqlnet.ora` ファイルには、少なくとも次のパラメータが記述されている必要があります。

```
names.directory_path = (TNSNAMES)
names.default_domain = domain
```

UNIX では、このファイルは `$ORACLE_HOME/network/admin` にあります。

Windows NT では、このファイルは `ORACLE_HOME¥network¥admin` にあります。

2. `tnsnames.ora` を構成します。

`tnsnames.ora` ファイルには、すべての **Oracle Internet Directory** データベースに対する [接続記述子](#) 情報が、次の書式で記述されている必要があります。

```
net_service_name =
  (DESCRIPTION =
    (ADDRESS =
      (PROTOCOL = TCP)
      (HOST = HOST_NAME_OR_IP_ADDRESS)
      (PORT = 1521))
    (CONNECT_DATA =
      (service_name = service_name))
```

UNIX では、このファイルは `$ORACLE_HOME/network/admin` にあります。

Windows NT では、このファイルは `ORACLE_HOME¥network¥admin` にあります。



---

**注意：** ネット・サービス名をドメイン修飾することもできます（例：sales.com）。これを行うかどうかにかかわらず、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. ロールバック表領域とロールバック・セグメントを作成します。

複数のロールバック・セグメントを作成することもできます。システム要件に合わせて、表領域とセグメントのサイズを増やすことができます。

a. ロールバック・セグメント用の表領域を作成します。

次のコマンドを入力して、SQL\*Plus を実行します。

```
sqlplus system/system_password@net_service_name
```

SQL\*Plus プロンプトで、次のコマンドを入力します。

```
CREATE TABLESPACE table_space_name
datafile file_name_with_full_path SIZE 50M REUSE AUTOEXTEND ON NEXT 10M
MAXSIZE max_bulk_update_transaction_size ex:500M;
```

b. ロールバック・セグメントを作成します。

SQL\*Plus プロンプトで、各ロールバック・セグメントごとに次のコマンドを入力します。

```
CREATE ROLLBACK SEGMENT rollback_segment_name
tablespace table_space_name storage (INITIAL 1M NEXT 1M OPTIMAL 2M
MAXEXTENTS UNLIMITED);
```

4. 初期化パラメータ・ファイル init.ora 内のパラメータを変更します。

初期化パラメータ・ファイルに次の行を入力します。

```
rollback_segments = (rollback_segment_name_1, rollback_segment_name_2 ...)
JOB_QUEUE_PROCESSES = a_minimum_of_total_number_of_LDAP_nodes_minus_one
SHARED_POOL_SIZE = 20000000
OPEN_LINKS = a_minimum_of_total_number_of_LDAP_nodes_minus_one
```

---

**注意：** ジョブ・キュー・プロセスの数を設定する場合、将来追加する可能性があるノードに対応できるように、十分な数のプロセスを設定するようにしてください。

---

**システム・グローバル領域**の合計が、システムの物理メモリーの 50% を超えないようにしてください。

---

**注意：** データベースを起動するたびに、システム・グローバル領域 (SGA) が割り当てられ、Oracle バックグラウンド・プロセスが開始されます。SGA は、データベース・ユーザーが共有するデータベース情報に使用されるメモリー領域です。バックグラウンド・プロセスとメモリー・バッファの組合せを、Oracle インスタンスと呼びます。

---

- 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]
```

- Oracle Internet Directory データベースを停止して、再起動します。

Oracle Internet Directory データベースを停止して再起動するには、SQL\*Plus を使用します。

### 関連項目：

- 『Oracle8i Net8 管理者ガイド』
- データベースの停止と再起動については、『Oracle8i 管理者ガイド』を参照してください。

## ディレクトリ・レプリケーション用の Oracle アドバンスド・レプリケーションの構成

レプリケーション・グループのアドバンスド・レプリケーションを構成するには、MDS から次の各ステップを実行します。

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

---

**注意：** 次のステップに進む前に、システム・ユーザーとして MDS コンソールからすべてのノード（MDS を含む）に接続します。次のことを確認してください。

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

3. MDS から、次のスクリプトを実行します。

```
ldaprepl.sh -asrsetup
```

このスクリプトは、次の多数の操作を実行します。

- MDS の構成
- リモート・マスター・サイトの構成
- すべてのサイトで、レプリケーションの送信ジョブを構成
- MDS でのレプリケーションの再開
- すべてのステップが正常に完了したことを検証

このスクリプトを実行すると、MDS、マスター・サイトの順に、次の表にある情報が要求されます。

参照箇所	定義
ホスト名	コンピュータ名
グローバル名	tnsnames.ora ファイルにリストされている、MDS データベースの ネット・サービス名
システム・パスワード	システム・パスワード

最初のマスター・サイトに関する情報の入力が終了すると、別のマスター・サイトがあるかどうかを尋ねられます。

4. 「Y」または「N」を入力します。「N」（すべてのサイトの確認が終了したことを指示します）を入力すると、指定した情報が表形式で表示され、その確認を求められます。情報に誤りがある場合は、「N」をクリックします。スクリプトは最初から起動し直し、MDS の情報を再度要求します。

すべての情報の指定が終了すると、情報が正しいことを確認するように要求されます。情報が正しい場合は「Y」をクリックします。スクリプトは、サイトの構成を開始します。

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

**注意：** 完了前に処理を中断する必要がある場合は、最初から起動し直してください。処理を中断しても、再インストールに悪影響を及ぼすことはありません。

---

**トラブルシューティングのヒント：** 処理に失敗した場合は、次の内容を実行してください。

1. `$ORACLE_HOME/ldap/admin/logs/ldaprep1.log` ファイルをチェックして、状態を調べてください。
2. ディレクトリ `$ORACLE_HOME/ldap/admin` に移動し、次のコマンドを実行してレプリケーション・ジョブの状態をチェックしてください。

```
sqlplus system/password@net_service_name @ldaplogq.sql
```

DRG のノードごとに、このコマンドを実行します。状態が正常な場合は、このコマンドの発行によって、行が選択されることはありません。行が選択され、その中に失敗のステータスとエラー・メッセージが含まれている場合は、アドバンスト・レプリケーションの設定に失敗したことを意味しています。この場合は、次のいずれかの方法で対処します。

- スクリプトを最初から実行する
- 『Oracle8i レプリケーション・ガイド』のトラブルシューティングの章を参照する
- アドバンスト・レプリケーションの専門家に問い合せて、エラー・メッセージの情報から解決策を判断する

---

**注意：** 大量の初期データが必要な場合は、`bulkload` ツールを使用して、DRG のすべてのノードに初期データをロードします。`bulkload` を使用するときは、使用前にサーバーを停止し、使用後に起動し直す必要があります。

---

#### 関連項目：

- データベースとリスナーが実行中であることを確認する方法は、『Oracle8i 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、『Oracle8i Net8 管理者ガイド』を参照してください。
- `bulkload` の構文と使用方法は、A-22 ページの「[bulkload 構文](#)」を参照してください。

## タスク 4: 全ノードでの Oracle Directory Server インスタンスの起動

全ノードで OracleDirectory Server インスタンスを起動するには、次のコマンドを実行します。

```
oidctl connect=net_service_name server=oidldapd instance=instance_number_of_ldap_server flags="-p port" start
```

---

**注意：** instance\_number\_of\_ldap\_server は、DRG 全体で一意である必要はありません。たとえば、ノード A とノード B の両方に instance=1 を指定できます。

---

**関連項目：** Oracle Directory Server [インスタンス](#)の起動方法の詳細は、[第 5 章「Oracle Directory Server の管理」](#)を参照してください。

## タスク 5: レプリケーションの構成

次のパラメータを構成する必要があります。

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

- Oracle Directory Manager を使用した承諾の表示や変更
- コマンドライン・ツール (ldapadd や ldapmodify など) での構成エントリや承諾エントリのコンテンツの変更

この項では、両方の使用方法について説明します。

レプリケーション承諾	レプリケーション承諾は、変更内容を共有するレプリケーション・グループ内のメンバー・ノードをリストするエントリです。レプリケーション承諾は、Oracle Directory Replication Server の実行時にロードされる、Oracle Directory Replication Server の構成パラメータによって参照されます。
------------	--

---

**重要：** 初めてレプリケーションをインストールして構成する場合は、レプリケーション承諾のメンバー・ノードの存在について、Oracle Directory Replication Server に通知する必要があります。メンバー・ノードを通知するには、レプリケーション承諾内の orclDirReplGroupDSAs 属性を変更します。詳細は、10-14 ページの「[レプリケーション承諾のパラメータ](#)」を参照してください。

---

## Oracle Directory Replication Server の構成パラメータの位置

Oracle Directory Replication Server の構成パラメータは、Replication Server の [構成設定エントリ](#) に格納されています。識別名 (DN) は次のとおりです。

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

このエントリには、レプリケーション処理を制御するレプリケーション属性が含まれています。この属性の一部は変更できます。orclDirReplGroupAgreement 属性にはレプリケーション承諾識別子が含まれています。このリリースでは、レプリケーション承諾は 1 つのみ設定できます。

## Oracle Directory Replication Server のパラメータ

次の表は、Oracle Directory Replication Server の構成パラメータのリストおよび説明です。

パラメータ名	説明	デフォルト値	変更可能?
modifyTimestamp	エントリの作成または変更の時間		いいえ
modifiersName	エントリを作成または変更した人の名前		いいえ
orclChangeRetryCount	単一値の属性。変更エントリを削除するまでの適用処理の再試行回数。このパラメータの値は 1 以上である必要があります。	10	はい
orclPurgeSchedule	単一値の属性。ページ（ガベージ・コレクション）間隔を分単位で指定します。適用済のエントリや候補の変更に従って削除されたエントリを除去します。このスレッドは、設定した頻度に基づいて定期的に起動されます。このパラメータの値は 1 以上である必要があります。	10 分	はい
orclThreadsPerSupplier	変更ログを処理するために、Oracle Directory Replication Server が各サプライヤに提供するワーカー・スレッドの数。このパラメータの値は 1 以上にする必要があります。	5	はい
orclDirReplGroupAgreement	複数値の属性。このサーバーに管理責任がある対称型レプリケーション承諾を識別します。	orclagreementid=000001、 cn=orclreplagreements	いいえ
orclChangeLogLife	単一値の属性。変更ログ・ストア内のエントリの存続時間を時間単位で指定します。0（ゼロ）は変更番号ベースの削除であることを示します。	0	はい
関連項目: 2-27 ページ「 <a href="#">変更ログの削除</a> 」			

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

レプリケーション構成パラメータを表示および変更する手順は、次のとおりです。

- 1. ナビゲータ・ペインで、「Oracle Internet Directory」 > 「*directory\_server\_instance*」 > 「Server Management」 > 「Replication Server」の順に展開し、パラメータを表示または変更するレプリケーションの構成設定を選択します。対応するタブ・ページが、右側のペインに表示されます。

構成パラメータが「General」タブ・ページに表示されます。このタブ・ページで、レプリケーションの構成パラメータを表示し、そのほとんどのパラメータを変更できます。次の表は、このタブ・ページのフィールドの説明です。

フィールド	説明
Modify Timestamp	エントリの作成または変更の時間 ( <b>UTC (Coordinated Universal Time)</b> )。このパラメータは変更できません。
Modifier's Name	エントリを作成または変更した人の名前。このパラメータは変更できません。
Change Retry Count	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。
Purge Schedule	ガベージ・コレクションの間隔 (分) を入力します。レプリケーションのガベージ・コレクション・スレッドは、適用済みのエントリや候補の変更に従って削除されたエントリを除去します。デフォルトは 10 です。
Number of Threads Per Supplier	変更ログを処理するために、Oracle Directory Replication Server 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。
Set	構成の識別子を入力します。
Change Log Life	変更ログ・オブジェクトの存続期間 (時間) を入力します。 <b>関連項目 :</b> 2-27 ページ「 <a href="#">変更ログの削除</a> 」



## コマンドライン・ツールを使用したレプリケーションの構成パラメータの変更

コマンドライン・ツールを使用してレプリケーションの構成パラメータを変更するには、A-12 ページの「[ldapmodify 構文](#)」で説明されている構文を使用してください。

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

1. mod.ldif を次のように編集します。

```
dn: cn=configset0,cn=osdrep1d,cn=subconfigsubentry
changetype: modify
replace: orclPurgeSchedule
orclPurgeSchedule: 30
```

2. Replication Server の configset0 パラメータの値を更新するには、次のように ldapmodify を使用します。

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

3. Oracle Directory Replication Server を再起動します。

**ldapmodify を使用した Change Log Life パラメータの変更** この例では、mod.ldif という名前の入力ファイルを使用して、Change Log Life パラメータを 10 に変更します。

1. mod.ldif を次のように編集します。

```
dn: cn=configset0,cn=oidrep1d,cn=subconfigsubentry
changetype: modify
replace: orclChangeLogLife
orclChangeLogLife: 10 hours
```

2. Replication Server の configset0 パラメータの値を更新するには、次のように ldapmodify を使用します。

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

3. Oracle Directory Replication Server を再起動します。

**ldapmodify を使用した、変更がバージ・キューに移動される前の再試行回数の変更** この例では、mod.ldif という名前の入力ファイルを使用して、再試行の回数をデフォルトの 10 回から 5 回に変更します。具体的には、更新を 5 回試行すると、その更新は削除され、レプリケーション・ログに記録されます。

1. mod.ldif を次のように編集します。

```
dn: cn=configset0,cn=osdrep1d,cn=subconfigsubentry
```

```
changetype: modify
replace: orclChangeRetryCount
orclChangeRetryCount: 5
```

2. Replication Server の configset0 パラメータの値を更新するには、次のように ldapmodify を使用します。

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

3. Oracle Directory Replication Server を再起動します。

**ldapmodify を使用した変更ログの処理に使用されるワーカー・スレッド数の変更** この例では、mod.ldif という名前の入力ファイルを使用して、変更ログの処理で使用されるワーカー・スレッドの数を変更します。

1. mod.ldif を次のように編集します。

```
dn: cn=configset0,cn=osdrep1d,cn=subconfigsubentry
changetype: modify
replace: orclthreadspersupplier
orclthreadspersupplier: new_number_of_worker_threads
```

2. Replication Server の configset0 パラメータの値を更新するには、次のように ldapmodify を使用します。

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

3. Oracle Directory Replication Server を再起動します。

**関連項目：** Oracle Directory Replication Server を再起動する方法は、3-7 ページの「[Directory Server インスタンスの再起動](#)」を参照してください。

## レプリケーション承諾のパラメータ

パラメータ DirectoryReplicationGroupDSAs に、DRG 内のディレクトリ・システム・エージェント（DSA）のホスト名をすべて入力します。この情報がすべてのノードで同じであることを確認してください。

**関連項目：**

- 10-15 ページ「[Oracle Directory Manager を使用したレプリケーション承諾のパラメータの表示と変更](#)」
- 10-16 ページ「[ldapmodify を使用したレプリケーション承諾のパラメータの変更](#)」

## レプリケーション承諾のパラメータの位置

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 (DN) は次のとおりです。

```
orclAgreementID=id number,cn=orclreplagreements
```

このエントリには、この承諾のメンバーであるノードにのみ関係する属性が含まれています。複数のレプリケーション承諾を作成し、情報交換が行われているノード間でレプリケーションを管理できますが、Oracle Directory Manager を使用してサーバーの起動メッセージで参照できるのは、その中の 1 つのみです。Oracle Internet Directory リリース 2.1.1 の場合、使用できるレプリケーション承諾は 1 つのみです。

次の表は、レプリケーション承諾のパラメータのリストおよび説明です。

**注意：** レプリケーション承諾のパラメータを変更する前に、すべてのノードで Oracle Internet Directory を起動していることを確認してください。

## Oracle Directory Manager を使用したレプリケーション承諾のパラメータの表示と変更

Oracle Directory Manager を使用してレプリケーション承諾のパラメータを表示および変更する手順は、次のとおりです。

1. ナビゲータ・ペインで、「Oracle Internet Directory Servers」 > 「*directory\_server\_instance*」 > 「Server Management」 > 「Replication Server」の順に展開し、「Default Configuration Set」を選択します。

2. 右側のペインで、「Agreement」タブを選択してレプリケーション承諾を表示します。

このタブ・ページの各フィールドの説明は、次の表に記載されています。属性をダブルクリックすると、パラメータを表示でき、その一部を変更することもできます。
- | Oracle Directory Manager のフィールド | 説明   | デフォルト値 | 変更可能？ |
|---------------------------------|--|--------|-------|
| Agreements ID                   | レプリケーション承諾の一意識別子。  | 000001 | いいえ   |
| Excluded Naming Contexts        | 複数値の属性。このレプリケーション承諾から除外されるネーミング・コンテキストを指定します。他のレプリカから送信されたこれらのネーミング・コンテキスト内のエントリへの変更は、ローカル・ノードでは適用されません。 | なし     | はい    |
- ディレクトリ・レプリケーションの管理 10-15

Oracle Directory Manager のフィールド	説明	デフォルト値	変更可能？
Replication Group Nodes	複数値の属性。対称型レプリケーション承諾のメンバーとなるノードを指定します。ここで指定したノードは、互いに更新内容を共有します。		はい
Update Schedule	新規の変更および再試行される変更のレプリケーションの更新間隔。この値は分単位です。	1	はい
Orcl HIQSchedule	管理者操作キューのレプリケーションの更新間隔。この値は分単位です。通常は orclUpdateSchedule よりも大きい値です。更新の再試行が競合の解消に失敗した場合、管理者はこの時間で DIT 構造を変更できます。	10	はい
Replication Protocol	このレプリケーション承諾で使用されるレプリケーション・プロトコルを指定します。サポートされているプロトコルは、アドバンスド・レプリケーションです。	ODS_ASR_1.0	いいえ

3. このペインをオープンした時点で表示されていた値に戻す場合は、「Revert」をクリックします。変更内容に問題がない場合は、「Apply」をクリックします。

ldapmodify を使用したレプリケーション承諾のパラメータの変更

次の表は、レプリケーション承諾のパラメータのリストおよび説明です。

パラメータ	説明	デフォルト値	変更可能？
orclAgreementID	レプリケーション承諾の一意識別子。	000001	いいえ
orclExcludedNamingcontexts	複数値の属性。このレプリケーション承諾から除外されるネーミング・コンテキストを指定します。他のレプリカから送信されたこれらのネーミング・コンテキスト内のエントリへの変更は、ローカル・ノードでは適用されません。	なし	はい

パラメータ	説明	デフォルト値	変更可能？
orclDirReplGroupDSAs	複数値の属性。対称型レプリケーション承諾のメンバーとなるノードを指定します。ここで指定したノードは、互いに更新内容を共有します。		はい
orclUpdateSchedule	新規の変更および再試行される変更のレプリケーションの更新間隔。この値は分単位です。	1	はい
OrclHIQSchedule	管理者操作キューのレプリケーションの更新間隔。この値は分単位です。通常は orclUpdateSchedule よりも大きい値です。更新の再試行が競合の解消に失敗した場合、管理者はこの時間で DIT 構造を変更できます。	10	はい
orclReplicationProtocol	このレプリケーション承諾で使用するレプリケーション・プロトコルを指定します。サポートされているプロトコルはアドバンスト・レプリケーションです。	ODS_ASR_1.0	いいえ

レプリケーション承諾エントリの値にノードを追加するには、LDIF 形式のファイルを参照して、コマンドラインで `ldapmodify` を実行します。

この例では、`mod.ldif` という名前の入力ファイルを使用して、レプリケーション承諾に 2 つのノードを追加します。

1. `mod.ldif` を次のように編集します。

```
dn: orclagreementid=000001,cn=orclreplagreements
changetype: modify
add: orcldirreplgroupdsas
orcldirreplgroupdsas: hollis
orcldirreplgroupdsas: eastsun-11
```

2. Replication Server の `configset0` パラメータの値を更新するには、次のように `ldapmodify` を使用します。

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

3. Oracle Directory Replication Server を再起動します。

このプロシージャは、識別名 (DN) に `orclagreementid=000001`、`cn=orclreplagreements` のレプリケーション承諾が含まれているエントリを変更します。入力ファイルを適用すると、`orclagreementid 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：上述の 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。

10-19 ページの「[レプリケーション・ノードの追加](#)」で、レプリケーション環境に新規ノードを追加する処理について説明します。

---

Oracle Internet Directory リリース 2.1.1 で Oracle Directory Replication Server 向け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。

## タスク 6: 全ノードでの Replication Server の起動

すべてのノードで Replication Server を起動するには、次のコマンドを入力します。

```
oidctl connect=db_connection_string server=oidrepld instance=1
      flags="-h host -p port" start
```

インスタンス番号は、DRG 全体で一意である必要はありません。

**関連項目：** Replication Server の起動方法は、[第 5 章「Oracle Directory Server の管理」](#)を参照してください。

## 変更ログ・フラグの使用

Oracle Directory Server で行われる変更ログの記録をオフにできます。オフにするには、`-l` フラグのデフォルト値を `TRUE` から `FALSE` にして Oracle Directory Server の OID 制御ユーティリティ・コマンドを実行します。この方法は、変更ログ・ファイルにログが記録されている可能性がある場合に役立ちます。ただし、指定したノードで変更ログの記録をオフにすると、そのノードにおける更新は、DRG 内の他のノードにレプリケートされません。

## マルチマスター・フラグの使用

Oracle Directory Replication Server で行われるマルチマスター・フラグをオフにできます。オフにするには、`-m` フラグのデフォルト値を `TRUE` から `FALSE` にして Oracle Directory Server の OID 制御ユーティリティ・コマンドを実行します。このフラグをオフにすると、読取り専用のレプリカ・コンシューマを持つ単一のマスターを配置している場合、パフォーマンス・オーバーヘッドの低減に効果的です。マルチマスター・オプションは、競合の解消を制御しますが、単一のマスターを配置している場合は必要ありません。

**関連項目：** 2-28 ページ「[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・ノードの追加

稼働中のレプリケーション・グループに新規ノードを追加する方法は、次の 2 通りがあります。

- `ldifwrite` を使用する方法

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

- コールド・バックアップを使用する方法

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

---

**注意：** レプリケーション・ノードを追加する前に、Net8 環境を準備してください。手順は、10-4 ページの「レプリケーション用の Net8 環境の準備」を参照してください。

---

任意の有効サイズで稼働中の DRG にレプリケーション・ノードを追加するには、次の手順に従ってください。各手順の詳細は、この章で後述します。

タスク 1: すべてのノードで Oracle Directory Replication Server を停止

タスク 2: 既存の全ノードで LDAP レプリケーション・グループに新規ノードを構成

タスク 3: スポンサ・ノードの識別と読取り専用モードへの切替え

タスク 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: アドバンスド・レプリケーション追加ノードの設定の実行

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 Oracle Directory Replication Server を起動

タスク 8: `bulkload` を使用して新規ノードにデータをロード

タスク 9: 新規ノードで LDAP サーバーを起動

タスク 10: 新規ノードで LDAP レプリケーション承諾を構成

タスク 11: 新規ノードで Oracle Directory Replication Server を起動

---

---

**注意：** 以降の各ステップで示されているコマンドを実行するには、次のファイルが対応するディレクトリに格納されている必要があります。

- バイナリ：\$ORACLE\_HOME/bin
- SQL スクリプト：\$ORACLE\_HOME/ldap/admin
- UNIX スクリプト：\$ORACLE\_HOME/ldap/bin

タスク 1 を開始する前に、これら 3 つの変数がそれぞれのパスに存在することを確認してください。

---

---

## タスク 1: すべてのノードで Oracle Directory Replication Server を停止

Oracle Directory Replication Server を停止するには、LDAP レプリケーション・グループ内の各ノードで次のコマンドを実行します。

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

---

---

**注意：** インスタンス番号が 1 ではない場合があります。実行プロセスをチェックして、そこで使用されているインスタンス番号を検出してください。

---

---

## タスク 2: 既存の全ノードで LDAP レプリケーション・グループに新規ノードを構成

次の例では、add\_node.ldif という LDIF ファイルを作成し、それを既存の全ノードのレプリケーション・グループに構成します。

```
dn: orclagreementid=000001,cn=orclreplagreements
changetype: modify
replace: orcldirreplgroupdsas
orcldirreplgroupdsas: host_name_of_the_new_node
orcldirreplgroupdsas: host_name_of_existing_node_1
orcldirreplgroupdsas: host_name_of_existing_node_2
.
.
.
orcldirreplgroupdsas: host_name_of_existing_node_n
```

LDAP レプリケーション・グループ内の各ノードに対して、次のコマンドを実行します。

```
ldapmodify -h host_name_of_the_node -p port -f add_node.ldif
```



---

**注意：** このコマンドは、1 台のワークステーションから全ノードに実行できます。

---

### タスク 3: スポンサー・ノードの識別と読取り専用モードへの切替え

スポンサ・ノードは、新規ノードにデータを供給するノードです。スポンサ・ノードを識別し、それを読取り専用モードへ切り替える手順は次のとおりです。

1. 次の記述を含んだ新規ファイル `change_mode.ldif` を作成します。

```
dn:
changetype: modify
replace: orclservermode
orclservermode: r
```

2. 識別されたスポンサ・ノードに対して、次のコマンドを実行します。

```
ldapmodify -D "cn=orcladmin" -w welcome -h host_name_of_sponsor_node
-p port -f change_mode.ldif

oidctl connect=net_service_name server=oidldapd restart
```

このコマンドは、スポンサ・ノードで実行中の全 Oracle Directory Server を読取り専用モードで再起動します。Directory Server の再起動には、約 15 秒を要します。

---

**注意：** スポンサー・ノードが読取り専用モードの間は、そのノードを更新できません。他のノードは更新できますが、その更新内容はすぐにはレプリケートされません。

さらに、スポンサ・ノードと **MDS** が同じノードの可能性もあります。

---

### タスク 4: `ldifwrite` を使用したスポンサ・ノードのバックアップ

この処理には長時間を要する場合がありますため、バックアップ処理中に「[タスク 5: アドバンスド・レプリケーション追加ノードの設定の実行](#)」を開始してもかまいません。

バックアップを実行するには、次のコマンドを入力します。

```
ldifwrite -c db_connect_string -b "" -f output_ldif_file
```

## タスク 5: アドバンスド・レプリケーション追加ノードの設定の実行

このタスクは、「[タスク 4: ldifwrite を使用したスポンサ・ノードのバックアップ](#)」の実行中にも実行できます。

スポンサ・ノードから、次のスクリプトを実行します。

```
ldaprepl.sh -addnode
```

このスクリプトは、次の複数の操作を実行します。

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

スクリプトを実行すると、[表 10-1](#) にリストされている情報を、最初にスポンサ・ノード、次に既存のマスター・サイトについて要求されます。

**表 10-1 アドバンスド・レプリケーションの設定情報**

参照箇所	説明
スポンサ・ノードのホスト名	コンピュータ名
グローバル名	tnsnames.ora にリストされている、MDS またはマスター・サイトのデータベースのネット・サービス名
システム・パスワード	システム・パスワード

既存のマスター・サイトをすべて確認して、「N」を入力します。スクリプトが新規ノードに関する情報を尋ねます。情報の指定が終了すると、指定した情報を表で示し、確認を要求します。

情報に誤りがある場合は、「N」をクリックします。スクリプトは最初から起動し直し、同じ情報を要求します。情報が正しい場合は「Y」を入力します。スクリプトは、サイトの構成を開始します。

この処理は、システム・リソースと DRG のサイズによって、長時間を要する場合があります。処理の経過は、継続的に通知されます。

---

**注意：** なんらかの理由で完了前に処理を中断する必要がある場合は、最初から起動し直す必要があります。

---

---

**トラブルシューティングのヒント：** 処理に失敗した場合は、次の内容を実行してください。

1. 次のチェックを行います。  
\$ORACLE\_HOME/ldap/admin/logs/ldaprep1.log ファイルをチェックして、状態を調べてください。
2. ディレクトリ \$ORACLE\_HOME/ldap/admin に移動し、次のコマンドを実行してレプリケーション・ジョブの状態をチェックしてください。

```
sqlplus system/password@net_service_name @ldaplogq.sql
```

DRG のノードごとにこのコマンドを実行します。状態が正常な場合は、このコマンドの発行によって、行が選択されることはありません。行が選択され、その中に状態 [failed] とエラー・メッセージが含まれている場合は、アドバンスト・レプリケーションの設定に失敗したことを意味しています。この場合は、次のいずれかの方法で対処します。

- スクリプトを最初から実行する
  - 『Oracle8i レプリケーション・ガイド』のトラブルシューティングの章を参照する
  - アドバンスト・レプリケーションの専門家に問い合せて、エラー・メッセージの情報から解決策を判断する
- 

## 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. スポンサー・ノードで次のコマンドを実行します。

```
ldapmodify -D "cn=orcladmin" -w welcome -h host_name_of_sponsor_node
-p port -f change_mode.ldif

oidctl connect=net_service_name server=oidldapd restart
```

---

**注意：** タスク 6 は、タスク 3 に極めて類似しています。唯一異なるのは、このステップでは `change_mode.ldif` の `orclservermode` パラメータが、`rw`（すなわち読取り / 書込み）に設定されることです。

---

## タスク 7: 新規ノード以外の全ノードで Oracle Directory Replication Server を起動

Oracle Directory Replication Server を起動するには、次のコマンドを入力します。

```
oidctl connect=db_connection_string server=oidrepld instance=1
flags="-h host -p port" start
```

新規ノードでディレクトリまたはレプリケーション処理が何も実行されていないことを検証します。

## タスク 8: bulkload を使用して新規ノードにデータをロード

データをロードするには、次のコマンドを入力します。

```
bulkload.sh -connect db_connect_string_of_new_node -generate -load
-restore absolute_path_to_the_ldif_file_generated_by_ldifwrite
```

## タスク 9: 新規ノードで LDAP サーバーを起動

LDAP サーバーを起動するには、次のコマンドを入力します。

```
oidctl connect=db_connect_string_of_new_node server=oidldapd
instance=1 flags="-p port" start
```

## タスク 10: 新規ノードで LDAP レプリケーション承諾を構成

新規ノードに対して次のコマンドを実行します。

```
ldapmodify -h host_name_of_the_new_node -p port -f add_node.ldif
```

## タスク 11: 新規ノードで Oracle Directory Replication Server を起動

Oracle Directory Replication Server を起動するには、次のコマンドを入力します。

```
oidctl connect=db_connect_string_of_new_node server=oidrepld instance=1  
flags="-h host_name_of_new_node -p port" start
```

## レプリケーション・ノードの削除

**DRG** からレプリケーション・ノードを削除できるのは、DRG に 3 つ以上のノードがある場合のみです。

エントリが 100 万個未満のディレクトリからレプリケーション・ノードを削除するには、次のステップに従ってください。各ステップの詳細は、後述します。

タスク 1: すべてのノードでの Oracle Directory Replication Server の停止

タスク 2: 削除するノード内の全プロセスの停止

タスク 3: マスター定義サイトからのノードの削除

タスク 4: すべてのノードでの Oracle Directory Replication Server の起動

タスク 5: レプリケーション・グループからのノードの削除

タスク 6: その他のノードでの Oracle Directory Replication Server の再起動

---

**注意：** 次の各ステップで示されているコマンドを実行するには、次のファイルが対応するディレクトリに格納されている必要があります。

- パイナリ: `$ORACLE_HOME/bin`
- SQL スクリプト: `$ORACLE_HOME/ldap/admin`
- UNIX スクリプト: `$ORACLE_HOME/ldap/bin`

タスク 1 を開始する前に、3 つの変数がそれぞれのパスに存在することを確認してください。

---

タスク 1: すべてのノードでの Oracle Directory Replication Server の停止

Oracle Directory Replication Server を停止するには、DRG 内の各ノードで次のコマンドを実行します。

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

注意： インスタンス番号は違う場合があります。

タスク 2: 削除するノード内の全プロセスの停止

OID 制御ユーティリティおよび OID モニターを停止します。

関連項目：

- OID 制御ユーティリティの停止方法は、3-5 ページの「Oracle Directory Server インスタンスの停止」を参照してください。
- OID モニターの停止方法は、3-3 ページの「OID モニターの停止」を参照してください。

タスク 3: マスター定義サイトからのノードの削除

MDS から、次のスクリプトを実行します。

```
ldaprepl.sh -delnode
```

このスクリプトは次の操作を実行します。

- MDS およびその他の既存マスター・サイトでアドバンスト・レプリケーションを停止
- orclDirReplGroupDSAs パラメータからノードを削除
- すべてのステップが正常に完了したことを検証

このスクリプトを実行すると、表 10-2 にある情報が、最初にマスター定義サイト、次に削除するノードについて要求されます。

表 10-2 アドバンスト・レプリケーションの設定情報

参照箇所	説明
MDS またはマスター・サイトのホスト名	コンピュータ名
グローバル名	tnsnames.ora にリストされている、MDS またはマスター・サイトのデータベースのネット・サービス名

情報の指定が終了すると、指定した情報を表で示し、確認を要求します。情報に誤りがある場合は、「N」をクリックします。スクリプトは最初から起動し直し、同じ情報を要求します。情報が正しい場合は「Y」を入力します。スクリプトは、サイトの構成を開始します。

この処理は、システム・リソースと DRG のサイズによって、長時間を要する場合があります。処理の経過は、継続的に通知されます。

---

---

**注意：** なんらかの理由で完了前に処理を中断する必要がある場合は、最初から起動し直す必要があります。

---

---

---

---

**トラブルシューティングのヒント：** 処理に失敗した場合は、次の内容を実行してください。

1. `$ORACLE_HOME/ldap/admin/logs/ldaprepl.log` ファイルをチェックして、状態を調べてください。
2. ディレクトリ `$ORACLE_HOME/ldap/admin` に移動し、次のコマンドを実行してレプリケーション・ジョブの状態をチェックしてください。

```
sqlplus system/password@net_service_name @ldaplogq.sql
```

DRG のノードごとにこのコマンドを実行します。状態が正常な場合は、このコマンドの発行によって、行が選択されることはありません。行が選択され、その中に状態 [failed] とエラー・メッセージが含まれている場合は、アドバンスト・レプリケーションの設定に失敗したことを意味しています。この場合は、次のいずれかの方法で対処します。

- スクリプトを最初から実行する
  - 『Oracle8i レプリケーション・ガイド』のトラブルシューティングの章を参照する
  - アドバンスト・レプリケーションの専門家に問い合せて、エラー・メッセージの情報から解決策を判断する
- 
-

## タスク 4: すべてのノードでの Oracle Directory Replication Server の起動

Oracle Directory Replication Server を起動するには、次のコマンドを入力します。

```
oidctl connect=net_service_name server=oidrepld instance=1  
flags="-h host -p port" start
```

## タスク 5: レプリケーション・グループからのノードの削除

レプリケーション・グループからノードを削除する前に、その変更内容のすべてが他のノードに適用されていることを確認してください。

次の例では、`delete_node.ldif` という LDIF ファイルを作成し、それを既存の全ノードのレプリケーション・グループに構成します。この LDIF ファイルには、削除するノードのホスト名が含まれていません。

```
dn: orclagreementid=000001,cn=orclreplagreements  
changetype: modify  
replace: orcldirreplgroupdsas  
orcldirreplgroupdsas: host_name_of_existing_node1  
orcldirreplgroupdsas: host_name_of_existing_node2  
.  
.  
.  
orcldirreplgroupdsas: host_name_of_existing_node_n
```

LDAP レプリケーション・グループ内のノードごとに、次のコマンドを実行します。

```
ldapmodify -h host_name_of_the_node -p port -f delete_node.ldif
```

## タスク 6: その他のノードでの Oracle Directory Replication Server の再起動

ノードの削除後、効率を高めるためにその他のノードの Oracle Directory Replication Server を再起動します。そのためには、次のコマンドを入力します。

```
oidctl connect=db_connection_string server=oidrepld instance=1  
flags="-h host -p port" restart
```



## 手動での競合の解消

この項では、次の項目について説明します。

- レプリケーション変更の競合のモニター
- 競合解消メッセージの例
- 管理者操作キュー操作ツールの使用
- OID 調停ツールの使用

### レプリケーション変更の競合のモニター

競合がログに書き込まれた場合、それは、システムに備わった解消手順では競合を解消できないということを意味します。以前に適用されなかった変更によって新たなレプリケーション変更の競合が発生することを防止するために、ログを定期的にモニターすることが重要です。

レプリケーション変更の競合をモニターするには、レプリケーション・ログの内容を検証します。それぞれに付加されているタイムスタンプによって、各メッセージを識別できます。

### 競合解消メッセージの例

競合解消メッセージは、ファイル `oidrep1d00.log` に記録されます。次にメッセージの例を示します。このファイルのパスは、`ORACLE_HOME/ldap/log` です。レプリケーション競合の解消を試みた結果は、各競合解消メッセージの最後に記述されています。

#### 例 1: 存在しないエントリを変更しようとした場合

```
2000/08/03::10:59:05: ***** Conflict Resolution Message *****
2000/08/03::10:59:05: Conflict reason: Attempted to modify a non-existent entry.
2000/08/03::10:59:05: Change number:1306.
2000/08/03::10:59:05: Supplier:eastlab-sun.
2000/08/03::10:59:05: Change type:Modify.
2000/08/03::10:59:05: Target DN:cn=ccc,ou=Recruiting,ou=HR,ou=Americas,o=IMC,c=US.
2000/08/03::10:59:05: Result: Change moved to low priority queue after failing on
10th retry.
```

### 例 2: 既存のエントリを追加しようとした場合

```
2000/08/03::10:59:05: ***** Conflict Resolution Message *****
2000/08/03::10:59:05: Conflict reason: Attempted to add an existing entry.
2000/08/03::10:59:05: Change number:1209.
2000/08/03::10:59:05: Supplier:eastlab-sun.
2000/08/03::10:59:05: Change type:Add.
2000/08/03::10:59:05: Target DN:cn=Lou Smith, ou=Recruiting, ou=HR, ou=Americas,
o=IMC, c=US.
2000/08/03::10:59:05: Result: Deleted duplicated target entry which was created
later than the change entry. Apply the change entry again.
```

### 例 3: 存在しないエントリを削除しようとした場合

```
2000/08/03::10:59:06: ***** Conflict Resolution Message *****
2000/08/03::10:59:06: Conflict reason: Attempted to delete a non-existent entry.
2000/08/03::10:59:06: Change number:1365.
2000/08/03::10:59:06: Supplier:eastlab-sun.
2000/08/03::10:59:06: Change type:Delete.
2000/08/03::10:59:06: Target DN:cn=Lou
Smith,ou=recruiting,ou=hr,ou=americas,o=imc,c=us.
2000/08/03::10:59:06: Result: Change moved to low priority queue after failing on
10th retry.
```

## 管理者操作キュー操作ツールの使用

管理者操作キュー操作ツールによって、変更を管理者操作キューからリトライ・キューまたはパージ・キューへ移動できます。パージ・キューへの変更の移動は、ログ・エントリに対する変更の再適用を以降は試みないということを意味します。次の一般的なステップを実行して、管理者操作キューの変更を移動してください。

1. Oracle Directory Replication Server 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。

## 管理者操作キューからリトライ・キューへの変更の移動

変更をリトライ・キューへ戻すには、次の構文を使用します。

```
higretry.sh -connect net_service_name [-start change_number]
[-end change_number] [-equal change_number] -supplier supplier_node
```

引数は、次のとおりです。

引数	説明
-connect <i>net_service_name</i>	tnsnames.ora ファイルに定義されているネット・サービス名を使用してデータベースに接続します。
-start <i>change_number</i>	再試行操作の開始変更番号を指定します。このオプションをスキップすると、コマンドは、指定した終了変更番号より小か等しいすべての変更をリトライ・キューに戻します。
-end <i>change_number</i>	再試行操作の終了変更番号を指定します。このオプションをスキップすると、コマンドは、指定した開始変更番号より大か等しいすべての変更をリトライ・キューに戻します。
-equal <i>change_number</i>	変更番号を指定します。コマンドは、その変更の競合のみをリトライ・キューに戻します。このオプションは、-start または -end を使用している場合は指定できません。
-supplier <i>supplier_node</i>	変更が発生したサプライヤのノードを指定します。

## 管理者操作キューからパージ・キューへの変更の移動

変更をパージ・キューへ戻すには、次の構文を使用します。

```
higpurge.sh -connect net_service_name [-start change_number] [-end change_number]
[-equal change_number] -supplier supplier_node
```

引数は、次のとおりです。

引数	説明
-connect <i>net_service_name</i>	tnsnames.ora ファイルに定義されているネット・サービス名を使用してデータベースに接続します。
-start <i>change_number</i>	削除操作の開始変更番号を指定します。このオプションをスキップすると、コマンドは、指定した終了変更番号より小か等しいすべての変更をパージ・キューに戻します。
-end <i>change_number</i>	削除操作の終了変更番号を指定します。このオプションをスキップすると、コマンドは、指定した開始変更番号より大か等しいすべての変更をパージ・キューに戻します。

引数	説明
-equal <i>change_number</i>	変更番号を指定します。コマンドは、その変更の競合のみをページ・キューに戻します。このオプションは、-start または -end を使用している場合は指定できません。
-supplier <i>supplier_node</i>	変更が発生したサプライヤのノードを指定します。

**注意：** hiqretry.sh または hiqpurge.sh を使用する場合、変更のすべてを移動しないときには、-equal フラグ、または -start フラグと -end フラグの組合せを指定する必要があります。

**例：管理者操作キュー操作ツールの使用**

次の例は、管理者操作キュー操作ツールの使用方法を示しています。

**例：変更の再試行と廃棄** レプリケーション・ログを分析した結果、次のように決定したとします。

- サプライヤ・ノード ldap\_rep1 からの変更のうち、変更番号 10324 ～ 10579 のものを再試行する
- 変更番号 10581 ～ 10623 の変更を廃棄する

これらを行うために、次の 2 つのコマンドを発行します。

```
hiqretry.sh -connect oiddb1 -start 10324 -end 10579 -supplier ldap_rep1
hiqpurge.sh -connect oiddb1 -start 10581 -end 10623 -supplier ldap_rep1
```

最初のコマンドは、ldap\_rep1 で発生した変更番号 10324 ～ 10579 の変更をリトライ・キューに戻します。2 番目のコマンドは、サプライヤ ldap\_rep1 で発生した変更番号 10581 ～ 10623 の変更を削除します。

**例：管理者操作キューからリトライ・キューへの単一の変更の移動** 次のコマンドは、変更番号 10519 の変更をリトライ・キューに戻します。

```
hiqretry.sh -connect oiddb1 -equal 10519 -supplier ldap_rep1
```

**例：管理者操作キューからリトライ・キューへの複数の変更の移動** 次のコマンドは、変更番号が 10324 より大か等しいすべての変更をリトライ・キューに戻します。

```
hiqretry.sh -connect oiddb1 -start 10324 -supplier ldap_rep1
```

次のコマンドは、変更番号が 1057 より小か等しいすべての変更をリトライ・キューに戻します。

```
hiqretry.sh -connect oiddb1 -end 10579 -supplier ldap_rep1
```

**例：管理者操作キューからリトライ・キューへのすべての変更の移動** 次のコマンドには、オプションがありません。このコマンドは、サプライヤ ldap\_repl で発生したすべての変更を管理者操作キューからリトライ・キューへ移動します。

```
hiqretry.sh -connect oiddb1 -supplier ldap_repl
```

## OID 調停ツールの使用

Oracle Directory Replication Server が一貫性のないデータを検出した場合、OID 調停ツールを使用して、コンシューマのエントリをサプライヤのエントリに同期化させることができます。その場合、次の一般的なステップを実行します。

1. サプライヤとコンシューマを、読取り専用モードに設定します。
2. サプライヤとコンシューマが安定した状態にあることを確認します。安定した状態にならない場合は、更新が完了するまで待ちます。
3. コンシューマ上の一貫性のないエントリまたはサブツリーを識別します。
4. OID 調停ツールを使用して、コンシューマ上の一貫性のないエントリまたはサブツリーを修正します。
5. サプライヤとコンシューマを、読取り / 書き込みモードに戻します。

### OID 調停ツールを使用した一貫性のないデータの調停

OID 調停ツールは、次の構文を使用します。

```
oidreconcile -h supplier_host -c consumer_host [-P supplier_port] [-p consumer_port]
[-s scope] -b basedn -W supplier_password -w consumer_password [-T thread]
```

引数	説明
-h <i>supplier_host</i>	サプライヤ・ホスト。コンピュータ名または IP アドレスです。
-c <i>consumer_host</i>	コンシューマ・ホスト。コンピュータ名または IP アドレスです。
-P <i>supplier_port</i>	サプライヤの TCP ポート。このオプションを指定しない場合は、デフォルト・ポート（389）に接続されます。
-p <i>consumer_port</i>	コンシューマの TCP ポート。このオプションを指定しない場合は、デフォルト・ポート（389）に接続されます。
-s <i>scope</i>	調停の適用範囲：サブツリー。
-b <i>basedn</i>	調停を実行するエントリの識別名を指定します。
-W <i>supplier_password</i>	サプライヤ・ノードの cn=orcladmin のパスワード。

引数	説明
-w consumer_password	コンシューマ・ノードの cn=orcladmin のパスワード。
-T thread	ワーカー・スレッド。

### OID 調停ツールの動作

OID 調停ツールは指定された DN を受け取ると、サプライヤとコンシューマ両方の親の DN の orclGuid を比較します。

両方の親のグローバル識別子 (orclGuid) が一致し、オプション -s subtree が設定されている場合、OID 調停ツールは、次のことを行います。

1. コンシューマ・ノードのサブツリー内のエントリをすべて削除します。
2. サプライヤ・ノードからのエントリでそれらを置換します。

たとえば次のコマンドは、コンシューマの "ou=hr,o=acme,c=us" から始まるサブツリー全体を対応するサプライヤのサブツリーと置換します。

```
oidreconcile -h supplier_host -P 389 -c consumer_host -p 389 -b "ou=hr,o=acme,c=us"
-s subtree -W supplier_password -w consumer_password
```

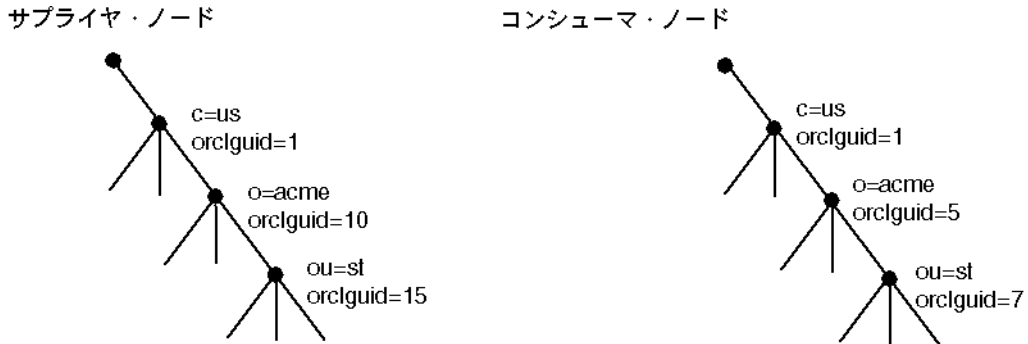
両方の親 ("o=acme,c=us") のグローバル識別子 (orclGuid) が一致し、-s subtree が設定されていない場合、OID 調停ツールはコンシューマ・ノードのエントリ自身のみをサプライヤ・ノードからの指定されたエントリと置換します。

たとえば、オプション "-s subtree" が設定されていない次のコマンドは、指定されたエントリ "ou=hr,o=acme,c=us" のみを置換します。

```
oidreconcile -h supplier -P 389 -c consumer -p 389 -b "ou=hr, o=acme, c=us"
-W supplier_password -w consumer_password
```

図 10-1 は、この処理の動作の説明に役立ちます。

図 10-1 例：OID 調停ツールの処理



この図は2つの **DIT**、一方はサプライヤ・ノード、もう一方はコンシューマ・ノードを表しています。サプライヤ・ノードの DIT では、c=us の orclGuid は 1、o=acme の orclGuid は 10、ou=st の orclGuid は 15 です。コンシューマ・ノードでは、o=acme の orclGuid は 5、ou=st の orclGuid は 7 です。

o=acme、c=us の親の orclGuid、つまり c=us は、サプライヤとコンシューマで一致します。したがって、次のコマンドは、コンシューマの o=acme、c=us の下のすべてのエントリを、サプライヤの対応するエントリと置換します。

```
oidreconcile -h supplier -c consumer -b "o=acme, c=us" -s subtree -W supplier_password -w consumer_password
```

両方の親の orclGuid が一致しない場合、OID 調停ツールは調停を実行しません。かわりに、orclGuid がサプライヤの同じ祖先クラスのものとも一致する、コンシューマの最初の祖先クラスを表示します。

たとえば、図 10-1 で、次のコマンドを実行するとします。

```
oidreconcile -h supplier -c consumer -b "ou=st, o=acme, c=us" -s subtree -W supplier_password -w consumer_password
```

このコマンドの結果として、orclGuid が一致する ou=st の最初の祖先クラスは o=acme、c=us であるというメッセージを管理者が受け取ります。このメッセージは、oidreconcile の basedn 引数として o=acme、c=us を使用する必要があるということを意味します。





---

## 複数ディレクトリとの同期化

Oracle Internet Directory リリース 2.1.1 では、サポートされているサード・パーティのメタディレクトリ・ソリューションとの同期化が可能です。これらのメタディレクトリ・ソリューションとの同期化は、変更ログの使用によって発生します。この章では、サポートするソリューションによって変更ログ情報がどのように生成および使用されるかを説明します。さらに、他のディレクトリを Oracle Internet Directory と同期化する方法についても説明します。

この章では、次の項目について説明します。

- [同期化プロセス](#)
- [他のディレクトリと Oracle Internet Directory の同期化](#)

## 同期化プロセス

Oracle Internet Directory での変更は、変更ログ・オブジェクト・ストアにエントリとして記録されます。他のディレクトリが Oracle Internet Directory に同期化しようとする場合は、そのストアにアクセスする必要があります。このアクセス権限は、ディレクトリを Oracle Internet Directory に登録することで付与されます。

変更ログ・ストアの各エントリは、変更番号を持っています。他のディレクトリは、最後に取り出した変更より大か等しい変更番号のエントリのみを Oracle Internet Directory から取り出します。たとえば、あるディレクトリが最後に取り出したエントリの変更番号が 250 だったとします。このディレクトリが次に取り出すエントリの変更番号は、250 以上となります。

---

**注意：** 最後に取り出した変更に一致する変更番号のエントリが戻された検索結果の中にある場合は、Oracle Internet Directory 変更ログのエントリのいくつかが削除されていることを意味します。その場合、ディレクトリは、Oracle Internet Directory 変更ログ全体を読み込んで、変更ログのコピーを Oracle Internet Directory に同期化する必要があります。

---

他のディレクトリを Oracle Internet Directory に登録すると、そのディレクトリは Oracle Internet Directory への認証を行い、そこから更新を取り出せるようになります。この処理は、次のプロセスに従って行われます。

**関連項目：** ディレクトリの Oracle Internet Directory への登録方法は、11-4 ページの「[他のディレクトリと Oracle Internet Directory の同期化](#)」を参照してください。

この項では、次の項目について説明します。

- ディレクトリが Oracle Internet Directory から変更を最初に取り出す方法
- 接続されたディレクトリが Oracle Internet Directory の `orclLastAppliedChangeNumber` 属性を更新する方法
- ディレクトリが Oracle Internet Directory から変更を取り出す方法（2 回目以降）

## ディレクトリが Oracle Internet Directory から変更を最初に取り出す方法

この例では、my\_other\_directory が ldapsearch によって次のコマンドを発行し、Oracle Internet Directory から変更を取得します。

```
ldapsearch -h host -p port -b "cn=changeLog" -s one
(&(objectclass=changeLogEntry)
(changeNumber >= orclLastAppliedChangeNumber )
( ! (modifiersname =cn=my_other_directory,cn=Subscriber Profile,
cn=ChangeLog Subscriber,cn=Oracle Internet Directory ) ) )
```

ディレクトリが初めて変更を取り出す場合、orclLastAppliedChangeNumber の値は、11-5 ページの「[タスク 2: Oracle Internet Directory の変更サブスクリプション・オブジェクトとしてディレクトリを登録する](#)」で設定した番号です。

フィルタの引数 ( ! (modifiersname=client\_bind\_dn) ) は、Oracle Internet Directory が他のディレクトリ自身によって行われた変更を戻さないようにします。

## 接続されたディレクトリが Oracle Internet Directory の orclLastAppliedChangeNumber 属性を更新する方法

接続されたディレクトリは、Oracle Internet Directory から変更を取り出すと、その変更サブスクリプション・オブジェクトの orclLastAppliedChangeNumber 属性を更新します。これにより、Oracle Internet Directory は、接続されたディレクトリによって適用済の変更を削除できます。さらに、接続されたディレクトリは、適用済の変更を無視して最新の変更のみを取り出すことができるようになります。

この例では、最後に適用された変更番号が 121 で、mod.ldif という名前の入力ファイルを使用します。接続されたディレクトリは、その変更サブスクリプション・オブジェクトの orclLastAppliedChangeNumber を次のように更新します。

1. mod.ldif を編集します。

```
dn: cn=my_other_directory,cn=Subscriber Profile,
cn=ChangeLog Subscriber,cn=Oracle Internet Directory
changetype:modify
replace: orclLastAppliedChangeNumber
orclLastAppliedChangeNumber: 121
```

2. ldapmodify を使用して、編集された mod.ldif ファイルをロードします。

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

**関連項目：** 変更番号による変更の削除については、2-27 ページの「[変更ログの削除](#)」を参照してください。

## ディレクトリが Oracle Internet Directory から変更を取り出す方法（2 回目以降）

2 回目以降に変更を取り出す場合、他のディレクトリは `ldapsearch` を使用してコマンドを発行します。次の例では、他のディレクトリ自身によって実行された操作に関連するものを除いて、`changeNumber` が 121 より大か等しいすべての変更が戻されます。

```
ldapsearch -h my_host> -p my_port_number -b "cn=changeLog" -s one"
(&(objectclass=changeLogEntry) (changeNumber >= 122 )
( ! (modifiersname = cn=my_other_directory,cn=Subscriber Profile,
cn=ChangeLog Subscriber,cn=Oracle Internet Directory ) ) )
```

## 他のディレクトリと Oracle Internet Directory の同期化

他のディレクトリが Oracle Internet Directory に格納された変更を取り出せるようにするためには、この項で説明する次のタスクを実行します。この項では、次の内容について説明します。

- **タスク 1: 初期ブートストラップを実行する**
- **タスク 2: Oracle Internet Directory の変更サブスクリプション・オブジェクトとしてディレクトリを登録する**
- **タスク 3: Oracle Internet Directory 変更ログ・オブジェクト・ストアへのアクセス権限をディレクトリに付与する**

### タスク 1: 初期ブートストラップを実行する

ディレクトリをブートストラップしてローカル・ディレクトリと Oracle Internet Directory の間でデータを同期化するには、次のステップを実行します。

1. 次のコマンドを実行して、Oracle Internet Directory から最新の変更番号を取り出します。

```
oidcurrentchange.sh -connect net_service_name
```

最新の変更番号が表示されます。後でディレクトリを登録するときは、`orclLastAppliedChangeNumber` フィールドにこの番号を入力します。

2. `ldifwrite` を使用して、データを Oracle Internet Directory から LDIF ファイルにエクスポートします。
3. LDIF ファイルをクライアント・ディレクトリに適した形式に変換して、クライアント・ディレクトリにロードします。

---

**注意：** 初期ブートストラップは、新規にインストールされた Oracle Internet Directory の場合には不要です。この場合、新規にインストールされた Oracle Internet Directory の最新の変更番号は 0（ゼロ）です。

---

**関連項目：** `ldifwrite` の使用方法は、A-26 ページの「[ldifwrite 構文](#)」を参照してください。

## タスク 2: Oracle Internet Directory の変更サブスクリプション・オブジェクトとしてディレクトリを登録する

他のディレクトリを Oracle Internet Directory と同期化させるには、それらのディレクトリを Oracle Internet Directory に登録する必要があります。それによって、Oracle Internet Directory に格納されている変更ログ・オブジェクトにディレクトリがアクセスできるようになります。

### ディレクトリ登録の概要

ディレクトリを登録するには、Oracle Internet Directory 内にそのエントリを作成します。このエントリは変更サブスクリプション・オブジェクトと呼ばれ、Oracle Internet Directory スキーマの、次のコンテナの下に配置されます。

```
cn=Subscriber Profile,cn=ChangeLog Subscriber,cn=Oracle Internet Directory
```

この変更サブスクリプション・オブジェクトは、ディレクトリが Oracle Internet Directory にバインドしてそこから変更を取り出すための、一意の資格証明を提供します。

変更サブスクリプション・オブジェクトを補助型オブジェクト・クラス `orclChangeSubscriber` に関連付けます。`orclChangeSubscriber` にはいくつかの属性があり、その中の 2 つは必須です。2 つの必須属性は、次のとおりです。

`userPassword`

Oracle Internet Directory の変更ログ・オブジェクトにアクセスするときにディレクトリが使用するパスワード。

`orclLastAppliedChangeNumber`

最後の同期化で適用された変更の番号。この属性によって、ディレクトリは適用前の Oracle Internet Directory の変更のみを取り出せます。

### ディレクトリの登録

ディレクトリの登録には、`ldapadd` を使用します。次の例では、`add.ldif` という名前の入力ファイルを使用して、次のコンテナの下に、変更サブスクリプション・オブジェクト `my_other_directory` を作成します。

```
cn=Subscriber Profile,cn=ChangeLog Subscriber,cn=Oracle Internet Directory
```

- ファイル `add.ldif` を編集します。

```
dn: cn=my_other_directory,cn=Subscriber Profile,cn=ChangeLog Subscriber,
cn=Oracle Internet Directory
userpassword:my_secret_code
```

```
orclLastAppliedChangeNumber: current_change_number_in_directory_before_  
                             initial_boot_strapping  
objectclass: orclChangeSubscriber  
objectclass: top
```

- エントリを追加します。

```
ldapadd -h <host> -p <port> -f add.ldif
```

### ディレクトリの登録解除

ディレクトリの登録解除には、`ldapdelete` を使用します。次のコマンドを入力します。

```
ldapdelete -h host -p port cn=directory_name,cn=Subscriber Profile,  
cn=ChangeLog Subscriber,cn=Oracle Internet Directory
```

## タスク 3: Oracle Internet Directory 変更ログ・オブジェクト・ストアへのアクセス権限をディレクトリに付与する

ディレクトリには、Oracle Internet Directory に登録した後に Oracle Internet Directory の `cn=changeLog` エントリへの読み込みアクセス権限を付与する必要があります。

**関連項目：** アクセス制御ポリシーの設定方法は、[第 9 章「ディレクトリのアクセス制御の管理」](#)を参照してください。

---

## 各国語サポート（NLS）の管理

Oracle Internet Directory の各国語サポート（NLS）によって、データの格納、処理および取出しをネイティブ言語で行うことができます。NLS は、Oracle Internet Directory のユーティリティとエラー・メッセージを、ネイティブ言語と地域に自動的に調整します。

この章では、Oracle Internet Directory で使用される NLS について説明し、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 を紹介します。

**関連項目：** NLS の構成の前に、2-17 ページの「[各国語サポート](#)」を参照してください。

この章では、次の項目について説明します。

- [環境変数 NLS\\_LANG](#)
- [LDIF ファイルでの NLS の使用方法](#)
- [コマンドライン・ツールでの NLS 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 NLS の使用方法](#)

## 環境変数 NLS\_LANG

NLS\_LANG パラメータには、language、territory および charset の 3 つのコンポーネントがあります。形式は次のとおりです。

```
NLS_LANG = language_territory.charset
```

各コンポーネントは、NLS 機能のサブセットの作用を制御します。

コンポーネント 説明	
language	<p>Oracle メッセージ、曜日および月の名前に使用する言語などの規則を指定します。サポートしているそれぞれの言語には、American English（米語）、French（フランス語）または German（ドイツ語）などの固有の名前があります。言語引数によって、地域およびキャラクタ・セットの引数のデフォルト値が指定され、その結果、territory または charset のいずれか（あるいはその両方）を省略できます。</p> <p>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。</p> <p><b>関連項目：</b>言語の全リストについては、『Oracle8i NLS ガイド』を参照してください。</p>
territory	<p>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。</p> <p>territory を指定しない場合、デフォルト値では America になります。</p> <p><b>関連項目：</b>地域の全リストについては、『Oracle8i NLS ガイド』を参照してください。</p>
charset	<p>クライアント・アプリケーションが使用するキャラクタ・セット（通常はユーザー端末で使用するキャラクタ・セット）を指定します。サポートしているそれぞれのキャラクタ・セットには、US7ASCII、WE8ISO8859P1、WE8DEC、WE8EBCDIC500、JA16EUC などの一意の頭字語があります。それぞれの言語には、デフォルトのキャラクタ・セットが対応付けられています。システムで使用可能な言語のデフォルト値については、オペレーティング・システムのインストール・ガイドまたは管理者ガイドを参照してください。</p> <p>Oracle Internet Directory では、全データが UTF-8 で格納されている必要があります。</p> <p><b>関連項目：</b>キャラクタ・セットの全リストについては、『Oracle8i NLS ガイド』を参照してください。</p>



---

**注意：** NLS\_LANG 定義のコンポーネントは、すべてオプションです。特に指定しない項目はデフォルト値になります。

territory または charset を指定する場合、先行デリミタを入力する必要があります。先行デリミタは、territory の場合はアンダースコア ( \_ ) で、charset の場合はピリオド ( . ) です。先行デリミタがないと、値全体が言語名として解析されます。

---

コマンドラインで、NLS\_LANG を環境変数として設定できます。次は、NLS\_LANG の適切な値の例です。

- AMERICAN\_AMERICA.UTF8
- JAPANESE\_JAPAN.UTF8

## LDIF ファイルでの NLS の使用方法

**関連項目：** A-2 ページ「LDAP データ交換フォーマット (LDIF) の構文」

属性の型は必ず ASCII 文字列で、マルチバイト文字は使用できません。Oracle Internet Directory は、属性の型名にマルチバイト文字をサポートしていません。ただし、Oracle Internet Directory は、属性の値にマルチバイト文字の使用をサポートしています。たとえば、中国語（簡体字）(.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。

属性の値は、異なる方法でエンコーディングできます。この方法でエンコーディングされた値は、Oracle Internet Directory のツールで正しく解釈できます。次の 2 つの例があります。

- [ASCII 文字列のみを含む LDIF ファイル](#)
- [UTF-8 エンコーディング文字列を含む LDIF ファイル](#)

### ASCII 文字列のみを含む LDIF ファイル

この例では、属性値の文字列も ASCII 文字列です。

すべてのツールがデフォルトで UTF-8 キャラクタ・セットを使用しており、ASCII は UTF-8 の正しいサブセットであるため、いずれのツールもこのファイルを解釈できます。キーボードで ASCII 文字列の値をそのまま入力する場合も同様です。

## UTF-8 エンコーディング文字列を含む LDIF ファイル

この例では、属性値の文字列も UTF-8 文字列です。

ツールはすべてデフォルトで UTF-8 キャラクタ・セットを使用するため、すべてのツールがこのファイルを解釈できます。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・キャラクタの文字列は、属性値として LDIF ファイルで使用したり、キーボードで入力できます。それらの文字列は、ネイティブ・キャラクタ・セットまたは UTF-8 でエンコーディングできます。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 でエンコーディングされた UTF-8 文字列
- ケース 4: BASE64 でエンコーディングされたネイティブ文字列

LDAP サーバーは UTF-8 エンコーディング文字列のみを理解し、UTF-8 エンコーディング文字列を受信することを想定しているため、ケース 1、3 および 4 は、LDAP サーバーに送信する前に、UTF-8 文字列に変換しておく必要があります。

### ケース 1: ネイティブ文字列（非 UTF-8）

コマンドライン・ツール、ldifwrite および bulkmodify で、-E 引数を使用します。bulkload と bulkdelete の各ツールでは -encode 引数を使用します。

この例では、中国語（簡体字）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（DN）は、中国語（簡体字）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 でエンコーディングされた UTF-8 文字列

コマンドライン・ツール ldifwrite および bulkmodify で -E 引数を使用したり、bulkload や bulkdelete で -encode 引数を使用する必要はありません。Oracle Internet Directory のツールは、BASE64 でエンコーディングされた 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 でエンコーディングされたネイティブ文字列

コマンドライン・ツール、ldifwrite および bulkmodify で、-E 引数を使用します。bulkload および bulkdelete ツールでは、-encode 引数を使用します。

Oracle Internet Directory のツールは、BASE64 でエンコーディング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利用できる言語セットは1つのみです。

---

---

## コマンドライン・ツールでの NLS の使用方法

Oracle Internet Directory のコマンドライン・ツールは、キーボード入力または LDIF ファイル入力を次の方法で読み込みます。

- ASCII 文字のみ
- 非 ASCII 入力（ネイティブ言語キャラクタ・セット）
- UTF-8 またはネイティブ文字列の BASE64 でエンコーディングされた値（LDIF ファイル入力のみ）

LDIF ファイルまたはキーボードからの入力として使用されているキャラクタ・セットが UTF-8 以外の場合、コマンドライン・ツールは、LDAP サーバーに送信する前に、その入力を UTF-8 形式に変換する必要があります。

コマンドライン・ツールで入力を UTF-8 に変換するには、各ツールの使用時に -E 引数を指定します。

この項では、次の項目について説明します。

- [各ツールを使用するときの -E 引数の指定](#)
- [例: コマンドライン・ツールでの -E 引数の使用方法](#)

## 各ツールを使用するときの -E 引数の指定

クライアント・ツールは、-E 引数で指定されていない限り、常に UTF-8 がキャラクタ・セットであるとみなします。-E が指定されていると、BASE64 でエンコーディングされた値はデコードされ、次にデコードされたバッファが UTF-8 に変換されます。たとえば、-E ".ZHS16GBK" と指定すると、デコードされたバッファは、LDAP サーバーに送信される前に、中国語（簡体字）から UTF-8 に変換されます。

-E 引数を指定すると、-E 引数で指定したキャラクタ・セット（-E ".character\_set"）が UTF-8 キャラクタ・セットに正しく変換されます。

コマンドライン・ツールは、`-E` 引数を使用して、`-E` 引数に指定されたキャラクタ・セットで入力を処理します。出力は、環境変数 `NLS_LANG` で指定されたキャラクタ・セットで表示します。

たとえば、中国語（簡体字）のキャラクタ・セット（`.ZHS16GBK`）でエンコーディングされた LDIF ファイルからのエントリを `ldapadd` を使用して追加するには、次のように入力します。

```
ldapadd -h myhost -p 389 -E ".ZHS16GBK" -f my_ldif_file
```

この例では、LDAP サーバーに送信される前に、文字が `ldapadd` ツールによって `".ZHS16GBK"`（中国語（簡体字）のキャラクタ・セット）から `".UTF8"`（UTF-8 キャラクタ・セット）に変換されます。

例：コマンドライン・ツールでの `-E` 引数の使用方法

次の表は、`-E` 引数を各コマンドライン・ツールで正しく使用方法の補足例を示したものです。各例のコマンドは、値 `".ZHS16GBK"` で指定されている中国語（簡体字）から UTF-8 にデータを変換します。たとえば、各コマンドの `-D` オプションと `-w` オプションの値が中国語（簡体字）で記述されます。`-E` 引数を指定すると、これらの値が UTF-8 に変換されます。

次の表の例には、`.ZHS16GBK` キャラクタ・セットに属している実際のキャラクタは含まれていないことに注意してください。したがって、これらの例は `-E` 引数の指定なしで動作します。ただし、引数の値に `.ZHS16GBK` キャラクタ・セット内の実際のキャラクタが含まれる場合は、`-E` 引数を使用する必要があります。

**関連項目：** 各コマンドライン・ツールの構文と使用方法は、[付録 A「LDIF およびコマンドライン・ツールの構文」](#)を参照してください。

ツール	例
ldapbind	ldapbind -h my_host -p 389 -E ".ZHS16GBK" -D o=acme,c=us -w my_password
ldapsearch	ldapsearch -h my_host -p 389 -E ".ZHS16GBK" -D o=acme,c=us -w my_password
ldapadd	ldapadd -h my_host -p 389 -E ".ZHS16GBK" -D o=acme,c=us -w my_password
ldapaddmt	ldapaddmt -h my_host -p 389 -E ".ZHS16GBK" -D o=acme,c=us -w my_password
ldapmodify	ldapmodify -h my_host -p 389 -E ".ZHS16GBK" -D o=acme,c=us -w my_password
ldapmodifymt	ldapmodifymt -h my_host -p 389 -E ".ZHS16GBK" -D o=acme,c=us -w my_password

ツール	例
ldapdelete	ldapdelete -h my_host -p 389 -E ".ZHS16GBK" -D o=acme,c=us -w my_password
ldapcompare	ldapcompare -h my_host -p 389 -E ".ZHS16GBK" -D o=acme,c=us -w my_password -b ou=Construction,ou=Manufacturing,o=acme,c=us -a title -v manager
ldapmoddn	ldapmoddn -h my_host -p 389 -E ".ZHS16GBK" -D o=acme,c=us -w my_password -b "cn=Franklin Badlwins,ou=Construction,ou=Manufacturing,c=us,o=acme" -N ou=Contracting,ou=Manufacturing,o=acme,c=us -r

## クライアント環境における NLS\_LANG の設定

クライアントで必要な出力が UTF-8 の場合は、環境変数 NLS\_LANG を設定する必要はありません。この場合、環境変数 NLS\_LANG はデフォルトで .UTF8 に設定され、クライアントからサーバーへの入力の過程、およびサーバーからクライアントへの出力の過程で、キャラクタ・セット変換の必要はありません。

クライアントで必要な出力が UTF-8 以外の場合は、環境変数 NLS\_LANG を設定する必要があります。この設定によって、UTF-8 キャラクタ・セットからクライアントが要求したキャラクタ・セットに正しく変換されます。

たとえば、環境変数 NLS\_LANG が中国語（簡体字）のキャラクタ・セットに設定されている場合、コマンドライン・ツールは、そのキャラクタ・セットで出力を表示します。環境変数が設定されていない場合、出力にはデフォルトで UTF-8 キャラクタ・セットが使用されます。

---

**注意：** Windows NT を使用している場合、サーバーの起動後にコマンドライン・ツールを使用するには、MS-DOS ウィンドウで NLS\_LANG を再設定する必要があります。MS-DOS セッションのコード・ページに一致するキャラクタ・セットを設定してください。（UTF-8 は使用できません。）MS-DOS セッションでコマンドライン・ツールに使用するキャラクタ・セットの詳細は、『Oracle8i インストレーション・ガイド for Windows NT』を参照してください。

Oracle Internet Directory とともに、事前インストールされた Oracle8i リリース 8.1.7 データベースを使用している場合、データベースのキャラクタ・セットも UTF-8 に設定する必要があります。Windows NT に関する詳細は、『Oracle8i NLS ガイド』と『Oracle8i インストレーション・ガイド for Windows NT』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 NLS の使用方法

Oracle Internet Directory は、LDIF ファイルのテキスト・データの読み込み / 書き込みを、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 NLS の使用方法](#)
- [ldifwrite での NLS の使用方法](#)
- [bulkdelete での NLS の使用方法](#)
- [bulkmodify での NLS の使用方法](#)

**関連項目：** 各バルク・ツールの引数のリストは、「[バルク・ツールの構文](#)」を参照してください。

### bulkload での NLS 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 of LDIF ファイルは `"character_set"` でエンコーディングされています。

次のようなコマンドを実行します。

```
bulkload.sh -connect net_service_name -encode ".ZHS16GBK" my_ldif_file
```

### ldifwrite での NLS 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 でエンコーディングされた値を書き出します。

BASE64 エンコーディングは、Directory Server に格納されている UTF-8 文字列、または ldifwrite の実行時に環境変数 NLS\_LANG の設定で指定されたネイティブ文字列にも使用できます。

次のようなコマンドを実行します。

```
ldifwrite -c net_service_name -b baseDN -f output_file
```

環境変数 NLS\_LANG が未設定の場合または `language_territory.UTF8` 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 でエンコーディングされた 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 host -p port -f output_file
```

この場合、デコードされた BASE64 文字列はすでに UTF-8 でエンコーディングされていて、サーバーに送信できる状態であるため、`-E` 引数は不要です。

環境変数 `NLS_LANG` が UTF-8 以外のキャラクタ・セット（たとえば、`".ZHS16GBK"`）に設定されている場合は、出力の LDIF ファイルには、中国語（簡体字）（`.ZHS16GBK`）文字列の BASE64 でエンコーディング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 文字列は中国語（簡体字）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 NLS の使用方法

引数 `-encode ".character_set"` をコマンドに追加します。

次のようなコマンドを実行します。

```
bulkdelete.sh -connect net_service_name -encode ".ZHS16GBK" -base  
"ou=manufacturing,o=acme,c=us"
```

この例では、`-base` オプションの値に、ZHS16GBK ネイティブ・キャラクタ・セット（中国語（簡体字））を使用できます。

## bulkmodify での NLS の使用方法

引数 `-E ".character_set"` をコマンドに追加します。

次のようなコマンドを実行します。

```
bulkmodify.sh -c net_service_name -E ".ZHS16GBK" -b ou=manufacturing,o=acme,c=us -r  
title -v Foreman -f filter
```

この例では、`-b`、`-v` および `-f` の各引数の値を中国語（簡体字）キャラクタ・セットを使用して指定できます。





# 第III部

---

## Oracle Internet Directory の配置

第 III 部では、配置に関する考慮事項を説明します。第 III 部は次の各章から構成されています。

- [第 13 章「配置に関する考慮事項」](#)
- [第 14 章「容量計画」](#)
- [第 15 章「チューニング」](#)
- [第 16 章「高い可用性とフェイルオーバー」](#)



---

## 配置に関する考慮事項

この章では、Oracle Internet Directory を配置するときに考慮する必要がある問題について説明します。企業のディレクトリの要件を評価し、効果的な配置を選択するのに役立ちます。この章の推奨事項は、主に中規模および大規模の企業やインターネット・サービス・プロバイダ（ISP）のディレクトリに対するものですが、基本的な考え方は他の環境でも同様に適用できます。

この章では、次の項目について説明します。

- 拡大するディレクトリの役割
- ディレクトリ情報の論理編成
- 物理的な分散：パーティションとレプリカ
- フェイルオーバーに関する考慮事項
- 容量計画、サイズ設定およびチューニング

## 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

企業のバックボーンとして機能するディレクトリ製品を選択することは、重要です。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、配置の選択も重要となります。

## ディレクトリ情報の論理編成

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

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

この項では、次の項目について説明します。

- **ディレクトリ・エントリのネーミング**
- **DIT の階層と構造**

## ディレクトリ・エントリのネーミング

通常、ほとんどの企業には、従業員に一意の名前と番号を割り当てる規則を定める人事部門があります。ディレクトリ・エントリに対して一意のネーミング・コンポーネントを選択する場合、この管理インフラストラクチャを活用し、その方針を使用するのが有効です。それに対して、必要となる管理方針が増加することにより、DN をよりわかりやすくするという利点が軽減します。

## DIT の階層と構造

DIT は、DNS (Domain Name System) と同様に、構造の中で階層になっています。企業に対応付けられた論理階層を反映するように、DIT を編成できます。その選択は、次のものに対応する必要があります。

- 企業全体の DIT 構造とネーミング・ポリシーは、部門単位のものに規則および制限と互換性を持つ必要があります。たとえば、ディレクトリ製品には、最初にドメインを定義して、組織単位と地域が論理的にそれらのドメインに従属することが必要な場合があります。また、**兄弟**ではないエントリに対しても、ドメイン内でディレクトリ名が一意であることを必須とするディレクトリ製品もあります。
- ディレクトリ編成は、明確で効果的なアクセス制御とレプリケーション・ポリシーを促進する必要があります。**ACL** 管理の委任が必須の企業では、データ所有権の境界を反映するように DIT を編成すると便利です。

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

- 企業の部門構造または組織階層を反映するようにディレクトリ階層を編成するのがよい場合があります。ほとんどの企業は頻繁に組織の再編成や部門の再構成を行うので、通常はこの方法はお勧めできません。個人のディレクトリ・エントリの属性として個人の組織情報を捉えると、管理しやすくなります。

## 物理的な分散：パーティションとレプリカ

ディレクトリ・データを分散するには、次の2つの方法があります。

- サーバーのディレクトリ全体のメンテナンス
- 別のサーバーの別のネーミング・コンテキストへのデータ提供と、両者の間の**ナレッジ参照**（参照とも呼ばれます）のメンテナンス

**関連項目：** 2-23 ページ「分散ディレクトリ：概要」

この項では、次の項目について説明します。

- **理想的な配置**
- **パーティション化に関する考慮事項**
- **レプリケーションに関する考慮事項**

## 理想的な配置

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

単純な解決策は、冗長な LDAP サーバーとそれに対応付けられたデータベースを実装することです。しかし、冗長性を持たせても、ほとんどのグローバルな組織がその地域やサイトすべてで必要とする、接続性、アクセス可能性およびパフォーマンスが提供されない場合があります。これらの要件を満たすには、企業の地理的な広がりに応じて、様々な地域にレプリカを物理的に配置する必要があります。

Oracle Internet Directory が単一のマスターによる構成しかサポートしない場合、ディレクトリの論理的な統合は困難なものとなります。各地域またはグループは、信頼できるネーミング・コンテキストのマスター・レプリカを格納することが必要となります。このことは、パーティション間での管理方針の統一性の欠如を意味します。管理者は、各パーティションに対して異なるデータ管理手順を使用する必要があります。

しかし、Oracle Internet Directory のマルチマスター・レプリケーションでは、ディレクトリの論理的な統合は容易です。どこでも更新可能な構成ができるので、ディレクトリの統合は、複数のパーティションをメンテナンスするよりも、より効率的で費用がかからなくなりました。

堅牢で集中化された企業ディレクトリにするための、単純で実用的な推奨事項は次のとおりです。

- それぞれがすべてのネーミング・コンテキストを保持した、2つ以上のディレクトリ・ノードを持つネットワークを確立します。これらのノードはマルチマスター構成で設定します。
- これらのノードをそれぞれ各地域に1つずつ、企業のデータ・ネットワーク接続に合うように配置します。たとえば、ある地域が遅いリンク方法でネットワークの他の地域と接続されている場合、その地域のクライアントが使用するための専用の Directory Server を設置する必要があります。
- フェイルオーバーとリカバリのために、各地域のサーバーを個々に構成します。

すべてのネーミング・コンテキストは整理統合されていますが、今までどおり様々な論理ネーミング・コンテキストに対して管理の自律性を実現できます。そのためには、適切なアクセス制御ポリシーを各ネーミング・コンテキストのルートで設定してください。

**関連項目：** 冗長性の説明は、13-6 ページの「[フェイルオーバーに関する考慮事項](#)」を参照してください。

## パーティション化に関する考慮事項

**パーティション**が多すぎるディレクトリは、一般的に利点よりも管理上のオーバーヘッドのほうが大きくなります。これは、各パーティションごとに、バックアップ、リカバリおよびその他のデータ管理機能の計画が必要になるためです。

通常、パーティションをメンテナンスする理由は次のようなものです。

- パーティションが、独立したままのほうがよい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。

パーティション化を使用するときは、各パーティションを[ナレッジ参照](#)で相互接続します。

---

**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一般的に増加します。クライアントは相互接続されたすべてのノードが使用可能でなくても、データを変更できるためです。たとえば、1つのノードが使用不能か、あるいは負荷が高いとします。マルチマスター・レプリケーションでは、操作は代替のノードで実行され、後に相互接続されたすべてのノードが同期化します。

レプリケート・ネットワークを実装する理由の多くは、次のようなものです。

- ローカルなアクセス可能性とパフォーマンス要件

多くの企業は世界中の様々な地域で活動しており、それらの活動には共通ディレクトリが必要です。複数の中継ルーターを含む、低帯域幅のリンクで各地域が相互接続されているとします。地域の外部から Directory Server にアクセスしているクライアントは、長い[待機時間](#)および不十分な[スループット](#)を体験します。

このような場合には、地域レプリカ（更新を受信するために、マルチマスター・レプリケーションによって使用可能にされています）が必要です。さらに、基礎となる[アドバンスド・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ほうが、費用がかからない場合があります。ロード・バランシングに加えて、そのような構成も、システムの可用性を高めることに貢献します。

- 障害許容度とシステム全体の高い可用性

ディレクトリ・レプリケーションを実装する最も重要な理由の1つは、システム全体の可用性を増すことです。1つのサーバーが使用できない場合、通信量は他の使用可能なサーバーに送られます。これはクライアントには透過的です。

## フェイルオーバーに関する考慮事項

ディレクトリ・サービスは企業内で重要な機能を持っているので、配置する際に障害リカバリと高可用性を考慮する必要があります。各ノードのバックアップおよびリカバリ計画を作成することが必要です。

マルチマスター・レプリケーションに加えて、Oracle Internet Directory のインストール時に可能な配置について、次のフェイルオーバーおよび高可用性オプションを考慮します。

- インテリジェント・クライアントのフェイルオーバー

Oracle Internet Directory に接続しているすべての LDAP クライアントは、指定したサーバー・インスタンスとの接続が突然切断された場合に接続する、Oracle Internet Directory の代替サーバー・インスタンスのリストをメンテナンスできます。

- インテリジェント・ネットワーク・レベルのフェイルオーバー

Oracle Internet Directory を稼働させるシステムの障害を検出できる、ハードウェアおよびソフトウェアのソリューションがいくつかあります。これらのソリューションでは、以降の接続要求を代替サーバーにインテリジェントに変更できます。この中には、必要なフェイルオーバー機能も提供しながら、受信した接続要求の負荷を代替サーバーと調整するソリューションもあります。

Oracle Internet Directory は Oracle8i のクライアントなので、Oracle Parallel Server などの他のフェイルオーバー・テクノロジーも使用可能です。

**関連項目：** Oracle Internet Directory で使用可能な、高可用性およびフェイルオーバーのオプションの詳細は、[第 16 章「高い可用性とフェイルオーバー」](#)を参照してください。

## 容量計画、サイズ設定およびチューニング

ディレクトリの使用に際し、企業全体および地域の要件を見積るときは、将来の必要性を計画します。レプリケーションとフェイルオーバーは他の構成の選択に依存するため、それぞれ独自の負荷と容量の要件を持つ複数のディレクトリ・ノードを必要とする場合があります。この場合、各ディレクトリ・ノードに対し個々にサイズを決める必要があります。



企業ではディレクトリの使用が増加しているので、Oracle Internet Directory を使用して要求を適時に処理する必要があるアプリケーションも増えています。Oracle Internet Directory のインストールが、それらのアプリケーションのパフォーマンスと容量の期待値にこたえられるかを確認します。

配置プロセスの2つのフェーズで、指定した Oracle Internet Directory のインストールの容量とパフォーマンスに影響を与えることができます。

- 計画フェーズ

このフェーズで、ディレクトリのユーザーすべての要件を集めて、統一したパフォーマンスと容量の要件を確立します。これは、容量計画とシステム・サイズ設定で構成されます。

- 実装フェーズ

ハードウェアの入手後、ハードウェア資源を最大限使用できるように、Oracle Internet Directory ソフトウェア・スタックをチューニングします。Oracle Internet Directory と LDAP クライアント・アプリケーションのパフォーマンスが改善されます。

この項では、次の項目について説明します。

- [容量計画](#)
- [サイズ設定に関する考慮事項](#)
- [チューニングに関する考慮事項](#)

## 容量計画

容量計画は、パフォーマンスと容量の要件を決定するプロセスです。企業のディレクトリ使用の一般的なモデルに基づいて行われます。

Oracle Internet Directory のインストールに必要な容量を見積る場合の考慮事項は、次のとおりです。

- LDAP クライアント・アプリケーションのタイプ
- アプリケーションにアクセスするユーザー数
- アプリケーションが実行する LDAP 処理の特性
- DIT 内のエントリ数
- Oracle Directory Server に対して実行される操作のタイプ
- Oracle Directory Server への同時接続数
- Oracle Directory Server 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

これらの詳細を見積るときには、ディレクトリの使用が将来増加したときのための空間を考慮してください。

サイズ設定に関する考慮事項

基本となる容量とパフォーマンスの要件を確立した後、それをシステム要件に変換します。これはシステム・サイズ設定と呼ばれます。このフェーズでの考慮事項の詳細は次のとおりです。

- Oracle Internet Directory サーバー・コンピュータの CPU のタイプと数
- Oracle Internet Directory サーバー・コンピュータのディスク・サブシステムのタイプとサイズ
- Oracle Internet Directory サーバー・コンピュータに必要なメモリーの量
- クライアントからの LDAP メッセージに使用されるネットワークのタイプ

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

使用方法	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)

Oracle Internet Directory のインストールに必要なディスク領域の量は、DIT に格納されるエントリ数に正比例します。次の表は、様々なサイズの DIT に必要な概算のディスク領域要件を示しています。

DIT 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・キャッシュの量によってほぼ決まります。多くの場合、データベース・キャッシュのサイズは、DIT 内のエントリ数に正比例します。次の表は、様々な DIT サイズのメモリー要件の見積りを示しています。

ディレクトリのタイプ	エントリ数	最低メモリー
小	600,000 未満	512MB
標準	600,000 ～ 2,000,000	1GB
大	2,000,001 以上	2GB

**関連項目：** [第 14 章「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勧めします。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す。必要な場合があります。

- 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 Directory Server 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 Directory Server 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 Directory Server 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・キャッシュです。大規模なデータベース・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・キャッシュを小さくすると、ディスク I/O が多く発生して、パフォーマンスに悪影響を及ぼします。システム内のメモリーのコンシューマすべてが、ページングの使用を必要とせずに物理メモリーを取得できるように、システムのメモリー使用量をチューニングします。

### ■ ディスク使用量

Oracle Internet Directory によって処理されるデータはすべてデータベースの表領域に常駐しているので、I/O スループットを増加させるようなチューニングには注意してください。一般的なディスクのチューニング・テクニックは、次のようなものです。

- 異なる論理ドライブおよび物理ドライブにある表領域の均衡化
- 論理ボリュームの複数の物理ボリュームへのストライプ化
- ディスク・ボリュームの複数の I/O 制御装置への分散

**関連項目：** 様々なチューニングのヒントとテクニックの詳細は、[第 15 章「チューニング」](#)を参照してください。

容量計画は、アプリケーションのディレクトリ・アクセス要件を評価し、許容速度で要求を処理するための十分なコンピュータ・リソースが Oracle Internet Directory にあることを確認するプロセスです。この章では、容量計画を行うときに考慮する必要がある項目について説明します。Acme Corporation という架空の会社における、電子メール・メッセージ・アプリケーションのディレクトリ配置例を使用して説明します。

この章では、次の項目について説明します。

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

## 容量計画の説明

Oracle Internet Directory とそれに対応する Oracle8i データベースが同じコンピュータ上で実行されている場合、容量計画の担当者が考慮する必要がある設定可能なリソースは次のとおりです。

- I/O サブシステム（タイプとサイズ）
- メモリー
- ネットワーク接続性
- CPU（スピードと数量）

Oracle Internet Directory 用のハードウェアを調達する場合は、すべてのコンポーネント（CPU、メモリー、I/O など）が、効果的に使用されることを確認してください。一般的に、適切なメモリーの使用と堅固な I/O サブシステムによって、CPU をビジー状態に保つことができます。

Oracle Internet Directory の新規インストール時には、次の 2 つの事項が整っている必要があります。

- インストールされたシステムに、負荷率のピーク時にユーザーの要求を満たすための十分なハードウェア・リソースが用意されていること。
- 使用可能なリソースを最大限に活用し、使用可能なハードウェアから最大のパフォーマンスを引き出すために適切にチューニングされたシステム（ハードウェアおよびソフトウェア）が用意されていること。

Acme Corporation という架空の会社における、電子メール・メッセージング・アプリケーションのディレクトリ配置例を考察します。容量計画の各コンポーネントを検証し、Acme Corporation の例に対して推奨事項を適用していきます。

### この章で使用される用語

スループット	Oracle Internet Directory がディレクトリ操作を完了する包括的な率。通常、操作 / 秒（1 秒当りの操作件数）で表されます。
待機時間	指定したディレクトリ操作が完了するまでのクライアントの待機時間。
同時クライアント	Oracle Internet Directory とのセッションを確立しているクライアントの総数。
同時操作	すべての同時クライアントの要求に基づいてディレクトリで実行されている同時操作の数。一部のクライアントではセッションがアイドル状態の可能性があるので、この数は同時クライアントの数と必ずしも同じではありません。

## ディレクトリの使用パターンの理解：事例

Oracle Internet Directory の潜在的な負荷を評価することは、正確な容量計画を作成するために非常に重要です。Acme Corporation という架空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。Mail Transfer Agent (MTA) とも呼ばれます。ディレクトリを調べて、社内メールを会社全体の配布リストに送信し、外部からのメールを社内のメールボックスに送信します。

個々のユーザーのプライベート・エイリアスとプライベート配布リストもディレクトリに格納されていると仮定します。さらに、次の仮定を設けて、ディレクトリのサイズを推測できるようにします。

ユーザー数の合計	40,000
1 ユーザー当りのプライベート・エイリアスの平均数	10
1 ユーザー当りのプライベート配布リストの平均数	10
パブリック配布リストの合計数	4000
社内におけるパブリック・エイリアスの合計数	1000
このアプリケーションに関連しているディレクトリ内の各エントリにある属性数	20
カタログ化属性の数	10

前述の仮定に基づくと、Oracle Internet Directory における全体的なエントリ件数は、次のように算出できます。

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	$40,000 \times 10 = 400,000$ エントリ
ユーザーのプライベート配布リスト	$40,000 \times 10 = 400,000$ 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

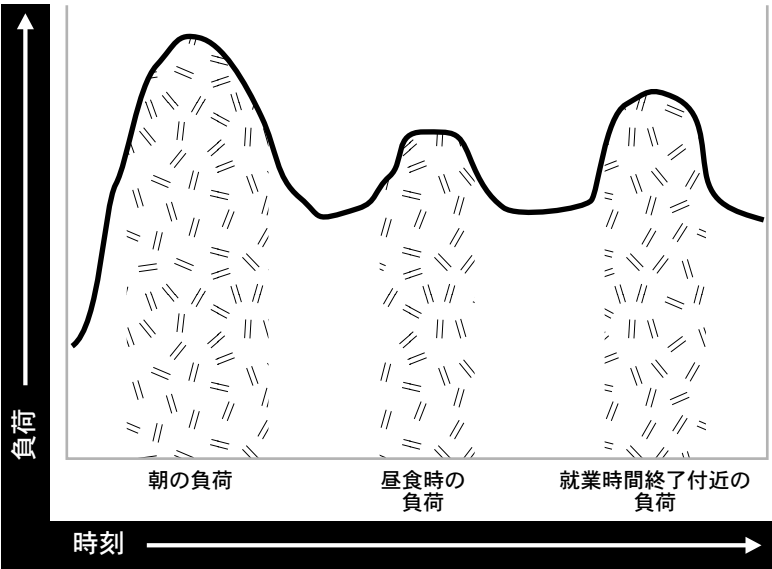
前述の仮定から、ディレクトリに存在するエントリは約 100 万件であることがわかります。ユーザー数とディレクトリに存在するエントリ数が与えられたとして、パフォーマンス要件を導出するために、使用パターンを分析してみます。一般的なユーザーは、1 日に平均 10 通の電子メールを送信し、外部から 1 日に平均 10 通の電子メールを受信します。ユーザーが送信する各メールに対して、平均 5 人の受信者がいると仮定すると、各メールごとに 5 回ずつディレクトリ参照が行われます。

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

ディレクトリ参照のタイプ	1 日のディレクトリ参照の数
各ユーザーからの送信メールを処理する Mail Transfer Agent (MTA)	$5 \times 10 \times 40,000 = 2,000,000$
外部からのメールを処理する MTA	$10 \times 40,000 = 400,000$
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、1 日のディレクトリ参照の総数は約 3,200,000 (320 万) となります。このディレクトリ参照が 1 日の範囲内で均一に分配されたとすると、毎秒約 37 ディレクトリ参照 (毎時約 133,333 参照) が行われる必要があります。ただし、このように均一に分配されることは実際にはありません。現行の電子メール・システムの使用状況を 24 時間にわたって分析すると、そのパターンは図 14-1 のようになります。

図 14-1 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）には、朝のピーク時に負荷がかかります。その他に、昼食時と就業時間終了付近にもピークがあります。しかし、Oracle Internet Directory に最も負荷がかかるのは朝の時間帯です。

全ディレクトリ参照の 90 パーセントが通常の勤務時間内に発生すると仮定します。次に、勤務時間内の負荷を次のカテゴリに分割します（勤務時間は 1 日 8 時間と仮定します）。

朝の負荷	65%: $0.90 \times 0.65 \times 3,200,000 = 1,872,000$ 参照 / 2 時間（936,000 参照 / 時）
昼食時の負荷	10%: $0.90 \times 0.10 \times 3,200,000 = 288,000$ 参照 / 1 時間（288,000 参照 / 時）
就業時間終了付近の負荷	20%: $0.90 \times 0.20 \times 3,200,000 = 576,000$ 参照 / 2 時間（288,000 参照 / 時）

これらの計算結果より、この場合の Oracle Internet Directory は、ピーク時の負荷である 1 時間当たり 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、インストレーションの個々のコンポーネントを調べ、それぞれについて適切な値を見積ることができます。

## I/O サブシステムの要件

この項では、次の項目について説明します。

- [I/O サブシステムの説明](#)
- [ディスク領域要件の概算](#)
- [ディスク領域要件の詳細な計算](#)

## I/O サブシステムの説明

I/O サブシステムは、CPU が負荷となる作業を実行できるように、CPU にデータを送り出すポンプにたとえることができます。I/O サブシステムには、データ記憶域を管理する役割もあります。I/O サブシステムの主なコンポーネントは、ディスク制御装置によって制御される一連のディスク・ドライブです。

I/O サブシステムのサイズを決めるときは、記憶要件のみに基づいたサイズではなく、パフォーマンス要件を考慮することが重要です。ディスク・ドライブのサイズは増加していますが、スループット（ディスク・ドライブがデータを送り出す速度）は、比例して増加していません。I/O サブシステムのサイズを計算するときには、情報として次の要因を考慮する必要があります。

- データベースのサイズ
- システム上の CPU の数
- Oracle Internet Directory の作業負荷の初期見積り

- ディスクがデータを送出できる速度
- ロード前のデータ準備に必要な領域
- 索引作成とソート作業に必要な領域

様々な I/O サブシステムがある場合は、常にスループットが最大のドライブを選択してください。一般的に、次の技術を 1 つ以上使用すると、I/O スループットを最大にできます。

- I/O 操作で複数のディスク・スピンドルを使用するために、論理ボリュームをストライプ化
- 異なる表領域を、異なる論理ディスク・ボリュームと物理ディスク・ボリュームに格納
- ディスク・ボリュームを複数の I/O 制御装置に分散

Oracle Internet Directory 固有のデータ・ファイルを組織化する方法のガイドラインは、[第 15 章「チューニング」](#)に記載されています。ディスク障害の許容度によっては、異なるレベルの Redundant Arrays of Inexpensive Disks (RAID) を考慮することもできます。

可能な限り最良の I/O サブシステムを用意する決定が行われたと仮定して、次にディスク自体のサイズ設定を見積ります。

## ディスク領域要件の概算

次の表を使用すると、全般的なディスク要件を概算で見積ることができます。

DIT 内のエントリ数	ディスク要件
100,000	450MB ～ 650MB
200,000	850MB ～ 1.5GB
500,000	2.5GB ～ 3.5GB
1,000,000	4.5GB ～ 6.5GB
1,500,000	6.5GB ～ 10GB
2,000,000	9GB ～ 13GB

この表のデータから、次の仮定が導出されます。

- カタログ化属性が約 20 個であること
- エントリごとの属性の数が約 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、アクセス制御項目（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 Oracle8i データベースに格納するため、ディスク領域のサイズ設定では、主に基礎となるデータベースのサイズを設定します。Oracle Internet Directory は、データを次の表領域に格納します。

OLTS_ATTR_STORE	DIT 内にある全エントリのすべての属性を格納。
OLTS_IND_ATTRSTORE	ディレクトリ内の属性に関連する索引を格納。
OLTS_CT_DN	識別名カタログを格納。
OLTS_IND_CT_DN	DN カタログに関連する索引を格納。
OLTS_CT_CN	一般名カタログを格納。
OLTS_CT_OBJCL	オブジェクト・クラス・カタログを格納。
OLTS_CT_STORE	その他のすべてのカタログ（ユーザー定義カタログを含む）を格納。
OLTS_IND_CT_STORE	ユーザー定義カタログに関連する索引を格納。
OLTS_DEFAULT	Oracle Internet Directory の管理に関連するデータとレプリケーション・サポートに使用するデータをすべて格納。
OLTS_TEMP	表の各種索引の作成に使用。すべての索引作成が正常に行われるように、十分な大きさに設定してください。
SYSTEM	各種の記録保持の目的で、Oracle8i データベースに必要。通常、このサイズは約 300MB で一定です。

この項では、前述の表に示した各表領域のサイズ要件を決定するための簡単な計算方法を提示します。すべてのサイズの計算は、次の変数に基づいて行われます。

変数名	説明
<i>num_entries</i>	ディレクトリ内のエントリの合計数。
<i>attrs_per_entry</i>	ディレクトリ・エントリごとの属性の平均数。
<i>avg_attr_size</i>	属性の平均サイズ（バイト）。
<i>avg_dn_size</i>	属性の識別名（DN）の平均サイズ（バイト）。
<i>objectclass_per_entry</i>	エントリが属しているオブジェクト・クラスの平均数。
<i>objectclass_size</i>	各オブジェクト・クラス名の平均サイズ（バイト）。
<i>num_cataloged_attrs</i>	エントリ内で使用されているカタログ化属性の数。
<i>entries_per_catalog</i>	カタログ表ごとのエントリの平均数。DIT 内の全エントリにカタログ化属性が存在しているとは限らないため、この変数は必須です。
<i>change_log_capacity</i>	レプリケーション目的のためにバッファする変更の数。
<i>num_acis</i>	ディレクトリ内のアクセス制御項目（ACI）の全体数。
<i>num_auditlog_entries</i>	ディレクトリに格納する監査ログ・エントリの数。
<i>db_storage_ovhd</i>	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。
<i>db_index_ovhd</i>	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。
<i>factor_of_safety</i>	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。

この表の変数を使用すると、個々の表領域のサイズを次のように計算できます。

表領域名	サイズ
OLTS_ATTR_STORE	$num\_entries \times attrs\_per\_entry \times avg\_attr\_size \times db\_storage\_ovhd$
OLTS_IND_ATTRSTORE	$num\_entries \times attrs\_per\_entry \times 30$

表領域名	サイズ
OLTS_CT_DN	$num\_entries \times 2 \times avg\_dn\_size$
OLTS_IND_CT_DN	$num\_entries \times 2 \times (avg\_dn\_size + 30)$
OLTS_CT_CN	$num\_entries \times avg\_dn\_size \times db\_storage\_ovhd$
OLTS_CT_OBJCL	$(num\_entries \times objectclass\_per\_entry \times objectclass\_size \times db\_storage\_ovhd) + (num\_auditlog\_entries \times 2 \times avg\_dn\_size \times db\_storage\_ovhd)$
OLTS_CT_STORE	$(entries\_per\_catalog \times num\_cataloged\_attrs \times avg\_attr\_size \times db\_storage\_ovhd) + (num\_entries \times objectclass\_per\_entry \times objectclass\_size \times db\_storage\_ovhd)$
OLTS_IND_CT_STORE	$(entries\_per\_catalog \times num\_cataloged\_attrs \times avg\_attr\_size \times db\_index\_ovhd) + (num\_entries \times objectclass\_per\_entry \times objectclass\_size \times db\_index\_ovhd) + (num\_acis \times 1.5 \times avg\_dn\_size \times db\_index\_ovhd) + (num\_auditlog\_entries \times 2 \times avg\_dn\_size \times db\_index\_ovhd)$
OLTS_DEFAULT	$(change\_log\_capacity \times 4 \times avg\_attr\_size \times db\_storage\_ovhd \times db\_index\_ovhd) + (num\_entries \times 5)$
OLTS_TEMP	(OLTS_IND_ATTR_STORE のサイズ) + (OLTS_IND_CT_STORE のサイズ)
SYSTEM	300MB

この表の計算式を使用すると、Oracle Internet Directory の広範囲にわたる様々な配置例に対して、正確な領域要件を計算できます。各表領域のサイズを合計すると、データベース全体のディスク要件がわかります。オプションで、その値に `factor_of_safety` 変数を乗算すると、予期せぬ事態にも対処可能な数値を算出できます。

Acme Corporation の例に戻り、前項に記述されている要件に基づいて各変数に値を代入します。次の表は、この項で紹介した各変数に、Acme Corporation の値を代入したものです。

変数名	値
<code>num_entries</code>	1,000,000
<code>attrs_per_entry</code>	20
<code>avg_attr_size</code>	32 バイト
<code>avg_dn_size</code>	40 バイト
<code>objectclass_per_entry</code>	5 (各エントリが平均 5 つのオブジェクト・クラスに所属)
<code>objectclass_size</code>	10 バイト
<code>num_cataloged_attrs</code>	10

変数名	値
<i>entries_per_catalog</i>	1,000,000
<i>change_log_capacity</i>	80,000 の変更（1 ユーザー当たり 2 つの変更）
<i>num_acis</i>	80,000 のアクセス制御項目（ACI）1 ユーザー当たり 2 つの ACI）
<i>num_auditlog_entries</i>	1000
<i>db_storage_ovhd</i>	1.4（40% のオーバーヘッド）
<i>db_index_ovhd</i>	5.0（400% のオーバーヘッド）
<i>factor_of_safety</i>	1.5（50% の安全係数）

これらの値を前述の等式に代入すると、次の値が得られます。

表領域名	サイズ（バイト）	サイズ（MB）	サイズ (MB: 安全係数を乗算)
OLTS_ATTRSTORE	896000000	875	1313
OLTS_IND_ATTRSTORE	600000000	586	879
OLTS_CT_DN	80000000	78	117
OLTS_IND_CT_DN	140000000	137	205
OLTS_CT_CN	56000000	55	82
OLTS_CT_OBJCL	70112000	68	103
OLTS_CT_STORE	518000000	506	759
OLTS_IND_CT_STORE	1874400000	1830	2746
OLTS_DEFAULT	76680000	75	112
OLTS_TEMP	2474400000	2416	3625
SYSTEM	307200000	300	450
合計サイズ	7092792000	6927	10390

この表は、Acme Corporation のデータベースの見積りサイズが約 6.9GBであることを示しています。安全係数の 50% を乗算すると、見積りサイズは 10.4GB まで増加します。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、テンポラリ・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 50% 必要です。Acme Corporation の場合は、領域要件の合計に約 2.25GB ～ 3.35GB を追加します。

## メモリー要件

メモリーは、Oracle Internet Directory などのあらゆるデータベース・アプリケーションが、多数の個別のタスク用に使用します。いずれかのタスクに対するメモリー・リソースが不十分な場合は、ボトルネックによって CPU の稼働率が低くなり、システム・パフォーマンスが低下します。また、メモリー使用量はデータベースへの同時接続数とディレクトリの同時ユーザー数に比例して増加します。

処理に使用できるメモリーは、システム上の仮想メモリーから供給されます。これは、使用可能な物理メモリーよりもやや大きいメモリーです。全アクティブ・メモリー使用量の合計が、そのシステムで使用可能な物理メモリーを超えると、オペレーティング・システムは、ある程度のメモリー・ページをディスク上に格納する必要があります。この作業をページングと呼びます。使用可能な物理メモリーをはるかに超えるメモリーを使用すると、ページングによってパフォーマンスが低下することがあります。一般的に、物理メモリーの 20% を超えたメモリーは使用しないでください。ページングが発生した場合は、プロセスごとのメモリー使用量を減らすか、または物理メモリーを追加する必要があります。ただし、トレードオフに注意してください。追加できるメモリーには物理的な制限があり、プロセスごとのメモリー使用量を減らすとパフォーマンスが大幅に低下します。

メモリーを主に消費するのは、**システム・グローバル領域**内のデータベース・バッファ・キャッシュです。これに割り当てるメモリーを増やすと、バッファ・キャッシュ・ヒット率が高くなります。バッファ・キャッシュ・ヒット率が高いと、データベース・パフォーマンスが向上するため、Oracle Internet Directory のパフォーマンスも向上します。

**関連項目：** SGA のチューニングの詳細は、第 15 章「チューニング」を参照してください。

次の表は、異なるディレクトリ構成別に最低メモリー要件を示したものです。

ディレクトリのタイプ	エントリ件数	最低メモリー
小	600,000 未満	512MB
標準	600,000 ～ 2,000,000	1GB
大	2,000,001 以上	2GB

Acme Corporation の例では、ディレクトリ内のエントリ数は約 1,000,000（100 万）です。パフォーマンスを最大にするには、2GB を選択してください。

## ネットワーク要件

ほとんどの場合、ネットワークがボトルネックとなることはありません。ただし、容量計画の段階では、慎重に考慮する必要があります。クライアントが Oracle Internet Directory とのメッセージ送受信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、1 秒間に 800 の検索を処理するように Oracle Internet Directory を構成しても、Oracle Directory Server 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）。

クライアントから Oracle Directory Server 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です。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ます。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勧めします。

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で転送されると仮定すると、100Mbps のネットワークを使用するか、または 10Mbps のネットワークで最低 60 パーセントの帯域幅を使用する必要があります。100Mbps のネットワークの方が通常待機時間が短いため、10Mbps のネットワークより優先して選択することになります。

## CPU 要件

この項では、次の項目について説明します。

- [CPU 構成](#)
- [CPU 要件の概算](#)
- [CPU 要件の詳細な計算](#)

## CPU 構成

Oracle Internet Directory に関する CPU のサイズ設定は、ユーザーの作業負荷に直接影響を与えます。CPU 構成は、次の要因によって決まります。

- サポートする同時操作の数。この数は、操作を同時に実行しているユーザー数に直接依存します。
- 各操作の許容待機時間。たとえば、電子メール・アプリケーションの場合、1 操作ごとの待機時間が 100 ミリ秒であることが理想ですが、多くの場合、500 ミリ秒でも許容範囲内です。

作業負荷の増加に従って、システムに CPU リソースを追加できますが、CPU リソースを追加しても、すべての操作にそのまま拡張性がもたらされることはほとんどありません。これは、多くの操作が純粋に CPU バウンドではないためです。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出され、すべてのシステム・ベンダーおよび SPEC の Web サイト（[www.spec.org](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、通常の状態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 Oracle8i データベースと同じマシンに常駐しているため、少なくとも 2CPU のシステムをお勧めします。Oracle Internet Directory の使用レベルに基づいて、次のように概算で見積ることがができます。

使用方法	CPU の数	SPECint_rate95 ベースライン	システム
部門単位	2	60 ～ 200	Compaq AlphaServer 8400 5/300 (300MHz × 2)
組織単位	4	200 ～ 350	IBM RS/6000 J50 (200MHz × 4)
会社単位	4+	350+	Sun Ultra 450 (296 MHz × 4)

## CPU 要件の詳細な計算

CPU の消費量はいくつかの要因によって変化するため、所定の配置サイトですべての操作に対する CPU 要件を判断することは困難です。次のような要因があります。

- 操作の種類。ベース検索、サブツリー検索、変更、追加など。
- SSL モードを使用可能にしているかどうか。SSL を使用すると、15 ～ 20% 多く CPU リソースが消費されます。
- 検索で戻されるエントリの数。
- 検索操作中にチェックする必要があるアクセス制御ポリシーの数。

SSL を除くほとんどの場合、Oracle Internet Directory サーバー・プロセスとデータベースとの間にかなりの待機時間があることが予想されます。Oracle Internet Directory サーバー・プロセスのスレッドがデータベースの応答を待機しているときは、Oracle Internet Directory サーバー・プロセス内のその他のスレッドを、LDAP サーバー固有の処理が必要なその他の

クライアント要求の作業に充てることができます。この結果、操作のいかなる組合せでも、同時クライアントと Oracle Internet Directory サーバー・プロセスの組合せが常に実現でき、CPU 使用率が 100% になります。この場合は、CPU がボトルネックとなります。

この事実を考慮し、最小値の CPU サイクルを消費する操作であるベース検索を選び、様々なコンピュータで CPU 使用量がピークとなる同時操作件数を見積ります。次に、この結果とそのコンピュータの SPECint\_rate95 ベースラインとの相関関係を調べます。この相関関係から、ユーザー負荷にある程度の並行性があれば、Oracle Internet Directory に必要な処理能力の下限を知ることができます。次の計算式によって、SPECint\_rate95 ベースライン数値に対するこのリリースの Oracle Internet Directory に関する並行性が示されます。

$$\text{SPECint\_rate95 baseline} = 6.0 * (\text{同時ベース検索操作})$$

たとえば、CPU の稼働率を 100% にせずに、50 のベース検索操作を同時に処理できるコンピュータが必要な場合は、SPECint\_rate95 のベースライン評価が約 300 のコンピュータが必要です。

この数値を基準として、その他の操作をベース検索操作の一定の係数として表すと、その操作の CPU 要件を知ることができます。次の係数は、他の要因に加えて使用できます。

- SSL モードを使用している場合は、CPU 要件に係数 1.2 を乗算します。
- 各検索で多数のエントリをフェッチする場合は、CPU 要件に係数  $(1 + 0.2 \times \text{num\_entries\_per\_search})$  を乗算します。
- 安全係数 20 ~ 30% を組み込みます (1.2 ~ 1.3 を乗算します)。

Acme Corporation の例に戻り、約 100 件の同時操作をサポートするために十分な CPU リソースを算出するとします。各検索でエントリが 1.5 件戻されると仮定し、安全係数 20% を付加すると、CPU 要件の仮見積りは次のようになります。

$$\text{SPECint\_rate95 baseline} = 6.0 * 100 * (1 + 0.2 * 1.5) * 1.2 = 600 * 1.3 * 1.2 = 936$$

SPEC の Web サイト (<http://www.spec.org>) で使用可能なシステムを調べると、次のコンピュータ構成が、考慮する最小構成であることがわかります。

次の表は、Acme Corporation が Oracle Internet Directory を使用する場合に検討対象となるコンピュータの一部を示したものです。

会社	モデル	CPU の数	CPU のタイプ	SPECint95_rate ベースライン
Sun Microsystems	ES 4002	12	250MHz UltraSPARC II	943
Siemens Nixdorf	RM600 Model E60	8	250MHz R10000	970
Hewlett-Packard	HP SPP1600	32	120MHz PA-RISC 7200	996
SGI	Origin2000	8	250MHz MIPS R10000	1001
Data General Corporation	AViiON AV 20000	16	Pentium Pro (200MHz)	1007

会社	モデル	CPU の数	CPU のタイプ	SPECint95_rate ベースライン
Sun Microsystems	Sun Enterprise 3500	8	400MHz UltraSPARC II	1011
Sun Microsystems	Sun Enterprise 3500	8	400MHz UltraSPARC II	1030
Hewlett-Packard	HP 9000 Model N4000	4	440MHz PA-RISC 8500	1093
Hewlett-Packard	HP 9000 Model T600	12	180MHz PA-RISC 8000	1099
Siemens AG	RM600 Model E80	8	285MHz R12000	1103
Compaq Corporation	AlphaServer 8400 5/440	12	437MHz 21164	1146
Compaq Corporation	AlphaServer 8400 5/625	8	612MHz 21164	1153
SGI	origin2000	16	195MHz MIPS R10000	1182
Sun Microsystems	Sun Enterprise 4000	12	336MHz UltraSPARC II	1211

## 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 という架空の会社における 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：260 検索 / 秒
- CPU 使用率を最大にするための同時使用率：100

この要件とその他の仮定に基づいて、次の推奨事項を提示しました。

- ディスク領域：7GB ～ 11GB
- メモリー：2GB
- ネットワーク：100 Base-T
- CPU: SPECint\_rate95 の数値が 936 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。



# 15

## チューニング

第 14 章「容量計画」で説明した容量計画を完了し、必要なハードウェアを用意した後にいくつかテストを実行し、現在の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かどうかを算定することが重要です。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。

この章では、次の項目について説明します。

- [チューニングの概要](#)
- [パフォーマンス・チューニング用のツール](#)
- [CPU 使用量のチューニング](#)
- [メモリーのチューニング](#)
- [ディスクのチューニング](#)
- [データベースのチューニング](#)
- [パフォーマンスに関するトラブルシューティング](#)

# チューニングの概要

Oracle Internet Directory に関するパフォーマンスの主な測定方法は次の 2 つです。

- 最大負荷時における個々の操作の平均待機時間。  
この時間は、各操作が完了するまでの時間です。
- 最大負荷時における Oracle Internet Directory の包括的なスループット。1 秒当りの操作件数で表されます。  
このスループットは、Oracle Internet Directory のインスタンスがクライアントの操作を完了できる率です。

パフォーマンス・テストの結果がよくない場合は、以降の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勧めします。

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 間に分割して示します。このユーティリティは Solaris でのみ使用可能です。
iostat	各種ディスク・コントローラからのディスク I/O 統計を示します。

Windows NT を使用している場合は、次のツールを理解しておくことをお勧めします。

ツール	説明
Windows NT パフォーマンス モニタ	システム内のイベントのカスタマイズされたビューを表示します。
Windows NT タスク マネジャ	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。

Oracle8i 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勧めします。

- utlbstat.sql および utlestat.sql
- DBMS\_STATS パッケージの ANALYZE ファンクション

**関連項目：**

- utlbbstat.sql および utlestat.sql の詳細は、『Oracle8i リファレンス・マニュアル』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、『Oracle8i 概要』を参照してください。

オペレーティング・システム・ツール以外に、カスタマ環境で使用されている LDAP アプリケーションも待機時間やスループットの測定方法を提供しています。

さらに、様々なデータベース ods スキーマ・オブジェクトを分析して統計を見積るために、`$ORACLE_HOME/ldap/admin` にあるデータベース統計収集ツール (`oidstats.sh`) が提供されています。

**関連項目：** A-35 ページ「OID データベース統計収集ツールの構文」

## CPU 使用量のチューニング

CPU はおそらく、すべてのソフトウェアが使用する最も重要なリソースです。第 14 章では、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る場合。

内部的なベンチマークでは、CPU リソースの約 70 ～ 75% が Oracle Internet Directory のプロセスで消費され、残りの約 25 ～ 30% がデータベース接続に対応する Oracle のフォアグラウンド・プロセスで消費されている場合に、Oracle Internet Directory が最も効率よく実行されることが示されています。CPU 使用量を監視すると同時に、システム領域で使用されている時間とユーザー領域で使用されている時間の割合を監視することも重要です。内部的なベンチマークでは、約 85% がユーザー時間、約 15% がシステム時間の場合にスループット値が最大であることが示されています。

この項では、次の項目について説明します。

- Oracle Internet Directory のプロセスに関する CPU のチューニング
- Oracle のフォアグラウンド・プロセスに関する CPU のチューニング
- SMP システムにおけるプロセッサ親和性の利用
- CPU がボトルネックとなっているシステムに関するその他の方法

Oracle Internet Directory のプロセスに関する CPU のチューニング

CPU に対する Oracle Internet Directory プロセスの需要は、ORCLSERVERPROCS および ORCLMAXCC の各パラメータで制御できます。次の表に、様々なクライアント負荷に対応したパラメータの推奨値を示します。

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
サーバー・プロセス ORCLSERVERPROCS	10 ～ 15	20 ～ 30	30 ～ 40	40 ～ 60
データベース接続 ORCLMAXCC	10 ～ 15	15 ～ 20	15 ～ 20	15 ～ 20

同時クライアントの数が 500 で、ORCLSERVERPROCS の値が 10、ORCLMAXCC の値が 15 の場合を例にとると、次のような構成になります。

- 10 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 15 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 (15+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。

CPU 稼働率が 100% の場合の Oracle Internet Directory プロセスのチューニング

システムの CPU 使用量が 100% のとき、次の条件の両方に該当する場合は、Oracle Internet Directory のプロセスをさらにチューニングすることを考慮してください。

- 最大負荷時に、Oracle Internet Directory のプロセスが、使用可能な全 CPU リソースの 70% 以上を消費している場合
- 最大負荷時に、システムまたはカーネルの領域で使用されている時間の全般的な割合が 20% 以上で、ユーザー用に使用されている時間の割合が 80% 未満の場合

この条件は、構成されている Oracle Internet Directory のサーバー・プロセスやデータベース接続がシステムに対して多すぎることを示しています。このため、いくつかのプロセスまたはスレッドが同じ CPU リソースを取り合うことになります。結果として、コンピュータは、実行可能なタスク間のコンテキスト切替えにかなりの時間を費やします。このような状況を防ぐには、ORCLSERVERPROCS と ORCLMAXCC の値を計画的に減らして、最大負荷時にパフォーマンスが最大になり、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する必要があります。

- ユーザー時間：85% 以上
- システム時間：15% 以下



## CPU が十分活用されていない場合の Oracle Internet Directory プロセスのチューニング

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。
- 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
- Oracle Internet Directory のプロセスが CPU リソースの約 70 ～ 75% を消費している場合
- データベース・プロセスが CPU リソースの約 25 ～ 30% を消費している場合

このような状況では、データベース・フォアグラウンド・プロセスをどの CPU でも実行できるようにすると、その他のタスクに対して多数のハードウェア・キャッシュ・ミスが発生する潜在的な原因となる場合があります。これは、データベース・プロセスでは通常の実行の一部として大量のデータを参照する必要があり、ほとんどのシステムにおいて、使用可能な L2 キャッシュの制限を超えることがあるためです。この結果、データベース・プロセスが CPU で実行されると、大部分の L2 キャッシュに**システム・グローバル領域**からのページが含まれます。タスク切替えが発生し、Oracle Internet Directory のプロセスがアクティブ化すると、メモリーからのフェッチがすべて低速になります。これは、そのプロセッサ上の先行タスクが L2 キャッシュを使用したためです。

Oracle のフォアグラウンド・プロセスをすべて 1 つのプロセッサで実行するように制限すると、Oracle Internet Directory のプロセスに関するキャッシュ・ミスの多くを回避できます。この結果、全般的なパフォーマンスが向上します。

## 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 Directory Server と Oracle8i データベースを別々のコンピュータに配置する方法。

## メモリーのチューニング

CPU の次に、メモリーのチューニングが重要です。Oracle Internet Directory においてメモリーを主に消費しているのは、Oracle8i データベースです。バックエンド・データベースの SGA は、Oracle Internet Directory と Oracle プロセスがそのプライベート・スタックとヒープを操作するために必要な領域を残し、できる限り大きいサイズで作成する必要があります。この項では、SGA の様々なコンポーネントの判別に関して詳細に説明します。

この項では、次の項目について説明します。

- [Oracle8i 用のシステム・グローバル領域 \(SGA\) のチューニング](#)
- [メモリーがボトルネックとなっているシステムに関するその他の方法](#)

### Oracle8i 用のシステム・グローバル領域 (SGA) のチューニング

SGA は、Oracle8i を実行しているシステムの使用可能な物理メモリーに基づいてサイズ設定してください。

**関連項目：** SGA を適切なサイズに設定する方法の詳細は、『Oracle8i パフォーマンスのための設計およびチューニング』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
- パッファ・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 5MB です。

この見積りで、SGA 合計の 30% を超える領域を消費する場合は、SGA 合計の 30% を使用してください。

残りの使用可能な SGA サイズの 60% を、データベースに対するブロック・サイズで除算し、DB\_BLOCK\_BUFFERS の数にこの値を使用します。この 2 つの値は初期見積りであり、BSTAT/ESTAT やその他の RDBMS 監視ツールを使用してさらに詳細に見積ると、最大のパフォーマンスを得るための正確なサイズを設定できます。

### メモリーがボトルネックとなっているシステムに関するその他の方法

データベースと Oracle Directory Server を同じコンピュータ上で実行するためのメモリーが不足している場合は、データベースを別のコンピュータに配置できます。

## ディスクのチューニング

ディスク I/O の均衡化は、RDBMS 全般、つまり Oracle Internet Directory のパフォーマンスにおいて重要な考慮事項です。一般的に、次の技術を 1 つ以上使用すると、I/O スループットを最大にできます。

- I/O 操作で複数のディスク・スピンドルを使用するために、論理ボリュームをストライプ化
- 異なる表領域を、異なる論理ディスク・ボリュームと物理ディスク・ボリュームに格納
- ディスク・ボリュームを複数の I/O 制御装置に分散

**関連項目：** ディスク I/O の均衡化とチューニングの概要は、『Oracle8i パフォーマンスのための設計およびチューニング』を参照してください。

この項では、次の項目について説明します。

- [表領域の均衡化](#)
- [RAID](#)

## 表領域の均衡化

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

**関連項目：** 論理ディスクの詳細は、15-9 ページの「[RAID](#)」を参照してください。

次の表領域を分離してください。

- OLTS\_ATTRSTORE と OLTS\_IND\_ATTRSTORE  
属性格納表とその索引を分離します。
- OLTS\_CT\_DN と OLTS\_IND\_CT\_DN  
DN カタログとその索引を分離します。
- OLTS\_xxxx と OLTS\_IND\_xxxx  
(経験に基づいて、格納表領域と関連する索引を分離します。)
- OLTS\_IND\_ATTRSTORE と OLTS\_IND\_CT\_DN

属性格納表と DN カタログ索引を交換します。交換すると、使用可能な論理ディスクが 2 つのみの場合にも有効です（一方の論理ディスクに OLTS\_CT\_DN と OLTS\_IND\_ATTRSTORE、他方の論理ディスクに OLTS\_IND\_CT\_DN と OLTS\_ATTRSTORE が格納されます）。

RAID

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

データベースのチューニング

この項では、Oracle Internet Directory のインストールに有効な、その他のチューニング可能なパラメータについて説明します。

次の表は、様々なクライアント負荷に対する RDBMS パラメータの推奨値を一覧にしたものです。これらのパラメータは、初期化パラメータ・ファイルで設定可能です。

パラメータ	同時 LDAP クライアントの 数が 500 の場合	同時 LDAP クライアントの 数が 1000 の場合	同時 LDAP クライアントの 数が 1500 の場合	同時 LDAP クライアントの 数が 2000 の場合
オープン・カーソル	100	100	100	100
セッション	225	600	800	1200
データベース・ブロック・バッファ	200 ～ 250MB	200 ～ 250MB	200 ～ 250MB	200 ～ 250MB
データベース・ブロック・サイズ	8192	8192	8192	8192
共有プール・サイズ	30 ～ 40MB	30 ～ 40MB	30 ～ 40MB	30 ～ 40MB
プロセス	400	800	1000	1500

この項では、チューニング可能な各 RDBMS パラメータについての詳細を説明します。この項では、次の内容について説明します。

- 必須パラメータ
- Oracle Internet Directory サーバーの構成に依存しているパラメータ
- ハードウェア・リソースに依存している SGA パラメータ

## 必須パラメータ

OPEN\_CURSORS パラメータを次のように設定します。

```
OPEN_CURSORS=100
```

Oracle Internet Directory サーバーのカーソル・キャッシュを処理するには、Oracle8i 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 100 に設定すると、どのようなサイズの DIT にも対応できます。

## Oracle Internet Directory サーバーの構成に依存しているパラメータ

SESSIONS パラメータを次のように設定します。

```
PROCESSES = (# OID server processes per instance) x  
            (# DB Connections per server + 1) x  
            (# of OID instances) + 20  
SESSIONS = 1.1 *PROCESSES + 5
```

各 Oracle Internet Directory サーバー・プロセスには、そのサーバーに構成されているワーカー・スレッドの数と等しい同時データベース接続数に 1 を加算した数が必要です。したがって、許容される同時データベース接続の合計数は、インスタンスごとのサーバー当りのこの数値になる必要があります。パラメータ値に追加されている 20 の接続数には、Oracle バックグラウンド・プロセスとその他の Oracle Internet Directory プロセス（OID モニター、OID 制御、Oracle Directory Replication Server およびバルク・ツールなど）が考慮されています。

## マルチスレッド・サーバー（MTS）の使用方法

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、MTS 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、MTS 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。MTS の構成の詳細は、『Oracle8i Net8 管理者ガイド』および『Oracle8i 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、15-7 ページの「[メモリーのチューニング](#)」に記載されています。その他のチューニング可能なパラメータを次にいくつか示します。

- ソート領域

ディスク上でソートが行われないように、十分なソート領域を確保するために、262144 (256K) に設定してください。

- REDO ログ・バッファ

初期見積りとして 32768 (32K) に設定してください。ログの書込みパフォーマンスがパフォーマンスの問題となる場合は、(REDO ログ領域要求 / REDO エントリ) > 1/5000 となるように十分に大きい値を使用して、LGWR プロセスが遅延しないようにしてください。この数値は全体でも、可変の SGA サイズにほとんど影響しないサイズであるため、この値の多少の増加が問題となることはありません。

## パフォーマンスに関するトラブルシューティング

この項では、一般的なパフォーマンス関連の問題を解決するための簡単な説明を示します。

LDAP 検索のパフォーマンスが悪い場合、次のことを確認してください。

- 検索対象の属性が索引付けされていること
- ODS ユーザーに関連付けられているスキーマが ANALYZED であること

複数のフィルタ・オペランドを含む検索の場合は、フィルタの指定順序が、最も特殊な条件から最も一般的な条件の順であることを確認します。たとえば、

&(l=Chicago) (state=Illinois) (c=US) は、  
&(c=US) (state=Illinois) (l=Chicago) と指定した方が効率的です。

LDAP 追加または変更のパフォーマンスが悪い場合、次のことを確認してください。

- データベースに十分な数の REDO ログ・ファイルがあること
- データベースに十分な数のロールバック・セグメントがあること
- 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





---

## 高い可用性とフェイルオーバー

この章では、Oracle Internet Directory の高い可用性とフェイルオーバー機能、および配置のガイドラインを示します。この項では、次の項目について説明します。

- [Oracle Internet Directory の高い可用性とフェイルオーバーの概要](#)
- [Oracle Internet Directory および Oracle8i のテクノロジ・スタック](#)
- [クライアントにおけるフェイルオーバー・オプション](#)
- [パブリック・ネットワーク・インフラストラクチャのフェイルオーバー・オプション](#)
- [Oracle Internet Directory の可用性とフェイルオーバー機能](#)
- [プライベート・ネットワーク・インフラストラクチャのフェイルオーバー・オプション](#)
- [高い可用性の配置例](#)

## Oracle Internet Directory の高い可用性とフェイルオーバーの概要

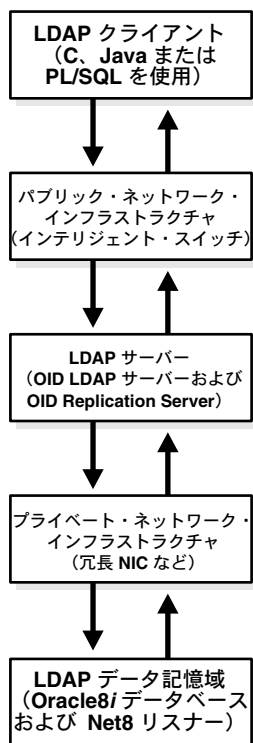
Oracle Internet Directory は、高度なシステム可用性を必要とするミッション・クリティカルなアプリケーションの配置ニーズに対処できるように設計されています。高度な可用性の実現には、システムのすべてのコンポーネントにおける冗長性の促進とすべてのインタフェースにおける障害検出とリカバリ（**フェイルオーバー**と呼ばれます）の促進が必要です。さらに、システム全体の可用性目標を達成するには、配置システム全体におけるアプリケーションに依存しない、ネットワーク・フェイルオーバー機能の統合が重要です。

Oracle 製品は通常、高可用性環境を目標として設計されており、必要な機能は Oracle テクノロジ・スタック（16-2 ページを参照）のすべての層に組み込まれています。通常、すべてのコンポーネントでフェイルオーバー機能を使用する必要はありません。この章では、Oracle Internet Directory のテクノロジ・スタックにおける様々なコンポーネントの可用性とフェイルオーバー機能について説明し、一般的なディレクトリ配置に関してこれらの製品を最適な状態で活用する方法を示します。

## Oracle Internet Directory および Oracle8i のテクノロジ・スタック

図 16-1 は、Oracle Internet Directory スタックの様々なコンポーネントの概要を示したものです。別々のコンピュータ間のスタック通信は、いくつかのコードのレイヤーを使用して、一方のノードから他方のノードへ情報を送ることによって発生します。情報はクライアント側でレイヤーを下降します。また、ネットワーク・メディアによる移送のためにパッケージされます。情報はその後サーバー側のスタックを上昇し、対応するレイヤーによって変換および解釈されます。

図 16-1 Oracle Internet Directory および Oracle8i のテクノロジー・スタック



製品の可用性を最大限にするために、十分なフォールト・トレランス機能を各層に組み込むことができます。以降の項では、図に示した各層で使用可能な可用性の高いオプションについて説明します。

## クライアントにおけるフェイルオーバー・オプション

クライアントに十分なインテリジェント機能を取り込み、プライマリ Oracle Directory Server で障害が発生した場合に、代替の Oracle Directory Server にフェイルオーバーするオプションが有効な場合があります。このためには、クライアントに代替のサーバー情報をキャッシュし、接続障害の検出時にその情報を使用する必要があります。可用性を保証する方法は、ディレクトリにアクセスするクライアントのタイプを、完全に制御できる配置システムに対してのみ実行可能です。

この項では、次の項目について説明します。

- ユーザー入力からの代替サーバー・リスト
- Oracle Internet Directory サーバーからの代替サーバー・リスト

### ユーザー入力からの代替サーバー・リスト

クライアントは、プライマリ・サーバーで障害が発生した場合に自動的にフェイルオーバーできるように、代替の Oracle Directory Server のリストをユーザーからの入力として受け取るように設計できます。ただし、このオプションは、クライアントの数が増加すると、クライアント・インストールの管理という面で負荷が高くなります。

### Oracle Internet Directory サーバーからの代替サーバー・リスト

Oracle Internet Directory は、AlternateServers と呼ばれる DSE ルート属性をサポートしています。これは、LDAP バージョン 3 規格の属性で、ディレクトリ管理者がメンテナンスします。この属性は、ローカル・サーバーと同じネーミング・コンテキストのセットを持つ、システム内の他の Oracle Directory Server に対する参照を所有することを想定しています。ローカル・サーバーとの接続が失われた場合に、クライアントは、この属性にリストされているサーバーの 1 つにアクセスすることができます。このオプションを使用する場合は、この属性をメンテナンスする十分な管理活動が必要です。

#### 関連項目：

- AlternateServers 属性の設定は、6-15 ページの「[Oracle Directory Manager を使用した属性の管理](#)」および 6-24 ページの「[コマンドライン・ツールを使用した属性の管理](#)」を参照してください。

## パブリック・ネットワーク・インフラストラクチャのフェイルオーバー・オプション

Oracle Internet Directory サービスへのアクセスに使用されるネットワークは、パブリック・ネットワーク・インフラストラクチャと呼ばれます。パブリック・ネットワーク・インフラストラクチャでネットワークレベルのロード・バランシングとフェイルオーバー対策（接続のリダイレクション）を準備することをお勧めします。これらの対策はアプリケーション・クライアントに対して、高度な柔軟性と透過性を提供します。

Oracle Internet Directory サービスが、インターネットからアクセスされる場合、このアクセスには、いくつかの高速リンク（T1 ～ T3）とインテリジェント TCP/IP レベルの接続リダイレクタが使用されます。Oracle Internet Directory サービスが、イントラネットからアクセスされる場合は、Oracle Directory Server を実行しているサーバー・コンピュータへの高速 LAN 接続と、インテリジェント TCP/IP レベルの接続リダイレクタが使用されます。いずれの場合も、1 つの Oracle Directory Server コンピュータの障害が可用性に影響を与えないように、LDAP 要求を処理するコンピュータが複数存在しています。

図 16-2 は、ネットワークレベルのフェイルオーバーが使用可能な Oracle Internet Directory の一般的なインターネット配置を示したものです。

図 16-2 ネットワークレベルのフェイルオーバー

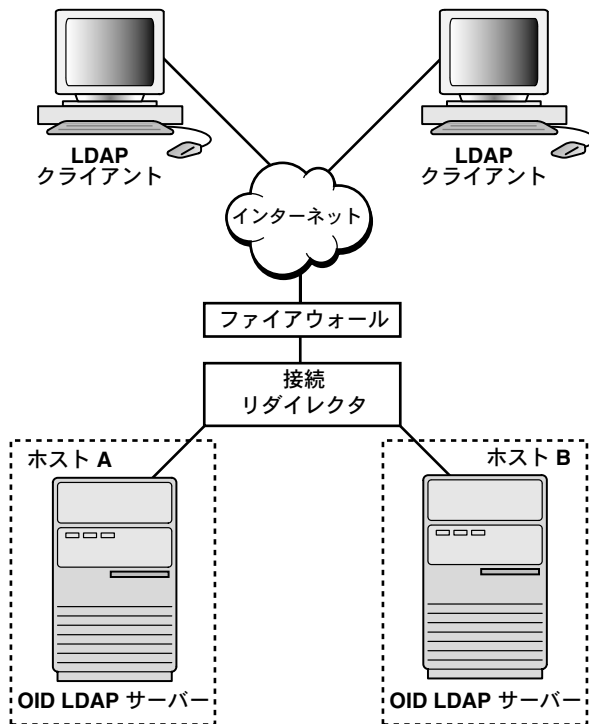


図 16-2 では、Oracle Directory Server (OID LDAP サーバー) は、同じバックエンドのデータベースまたは異なるバックエンドのデータベースのいずれにも接続できます。この配置システムの場合、ネットワークレベルの接続リダイレクションは、ハードウェアとソフトウェア両方のソリューションによって実施できます。

この項では、次の項目について説明します。

- ハードウェア・ベースの接続リダイレクション
- ソフトウェア・ベースの接続リダイレクション

## ハードウェア・ベースの接続リダイレクション

ハードウェア・ベースの接続リダイレクション技術は、複数のベンダーが提供しています。このリダイレクション・デバイスを使用すると、インターネットに直接接続し、複数のサーバー・コンピュータ間で要求の経路を指定できます。また、コンピュータ障害を検出し、障害が発生したコンピュータへの要求の送信を停止できます。この機能によって、クライアントからの新規接続が障害が発生したコンピュータに経路指定されないことが保証されます。コンピュータが回復すると、デバイスはそれを検出し、そのマシンへの新規要求の送信を開始します。また、このデバイスは、クライアント要求が均一に配布されるように、ある程度のロード・バランシングも実行します。

ハードウェア・ベースのリダイレクション技術を提供しているベンダーの例は、次のとおりです。

- Nortel Networks 社の Accelar Server Switches
- Cisco 社の Local Director
- F5 Labs Inc. 社の BIG/ip
- HydraWEB Technologies 社の Hydra
- Coyote Point Systems 社の Equalizer

## ソフトウェア・ベースの接続リダイレクション

ソフトウェア・ベースのソリューションは、本質的に、対応するハードウェアと同様の方法で機能します。現在使用可能なソリューションの例に、Resonate 社の Dispatch および IBM 社の Network Dispatcher などがあります。

## Oracle Internet Directory の可用性とフェイルオーバー機能

マルチマスター・レプリケーション機能によって、ディレクトリ・システムは、そのシステム内のノードが少なくとも 1 つ使用可能である限り、アクセスと更新のいずれにも常時使用できます。一定時間、非稼働状態のノードがオンラインに復旧すると、既存のノードからのレプリケーションが自動的に再開し、その内容は透過的に同期化されます。

高い可用性が必要とされるディレクトリ・システムでは、常にマルチマスター構成でレプリケート・ノードのネットワークを使用する必要があります。レプリカ・ノードは、相対的に低速または帯域幅の狭いネットワーク・セグメントが原因になることがあるため、他のリージョンから分離されている各リージョンごとに作成することをお勧めします。このような構成は、同一リージョンではクライアントへのディレクトリ・アクセスを迅速に処理しながら、他の場所でリージョン障害が発生したとき、フェイルオーバー対策としても機能します。

## プライベート・ネットワーク・インフラストラクチャのフェイルオーバー・オプション

プライベート・ネットワーク・インフラストラクチャは、Oracle Internet Directory とそのバックエンド・コンポーネントが相互通信に使用するネットワークです。Oracle Internet Directory がインターネット上に配置される場合、このネットワークとクライアント要求の処理に使用するネットワークを物理的に分離することをお勧めします。Oracle Internet Directory がイントラネットを介して配置される場合は、同一の LAN を使用できますが、ネットワーク・スイッチを利用して、Oracle Internet Directory のコンポーネント専用の帯域幅を確保してください。Oracle Internet Directory は、その通信に関してプライベート・ネットワーク・インフラストラクチャに依存するため、プライベート・ネットワークにおける障害発生時の可用性を保証するために、十分な予防措置を講じる必要があります。この領域で使用可能なオプションの例は、次のとおりです。

- [IP アドレス・テイクオーバー \(IPAT\)](#)
- [冗長リンク](#)

### IP アドレス・テイクオーバー (IPAT)

IP アドレス・テイクオーバー機能は、多数の商用クラスタで使用可能です。この機能は、ネットワーク・インタフェース・カード (NIC) の障害から装置を保護します。このメカニズムを使用するには、装置に 2 つの NIC があり、各 IP アドレスが 1 つのサーバーに割り当てられている必要があります。2 つの NIC は、いずれも同じ物理ネットワークに接続されている必要があります。一方の NIC は常にアクティブで、他方の NIC はスタンバイ・モードです。システムは、メイン・アダプタに問題を検出するとすぐに、スタンバイ NIC にフェイルオーバーします。継続中の TCP/IP 接続には影響しないため、クライアントが、そのサーバーの故障に気づくことはありません。

### 冗長リンク

すべてのネットワーク（ワイヤレス・ネットワークは除く）は、ある場所から別の場所まで配線されたケーブルで構成されているため、クライアント・コンピュータとサーバー・コンピュータを接続しているケーブルが誤って切断される可能性があります。これに対する予防措置を講じるには、リンク・レベルの障害時に冗長リンクを使用する機能を持つ、NIC とハブまたはスイッチを使用してください。



## 高い可用性の配置例

図 16-3 では、データベースと Oracle Directory Server (OID LDAP サーバー) は、同じコンピュータに共存しています。一方の Oracle Directory Server インスタンスに加えられた変更は、マルチマスター・レプリケーション機能によってもう一方の Oracle Directory Server インスタンスに反映されます。特定のノードで Oracle Directory Server またはデータベース・サーバーに障害が発生すると、その障害はコンピュータ障害とみなされ、接続リダイレクタは、障害が発生したコンピュータへの接続の送信を停止します。

図 16-3 配置例 (レプリケーションにおける Oracle Internet Directory の 2 つのノード)

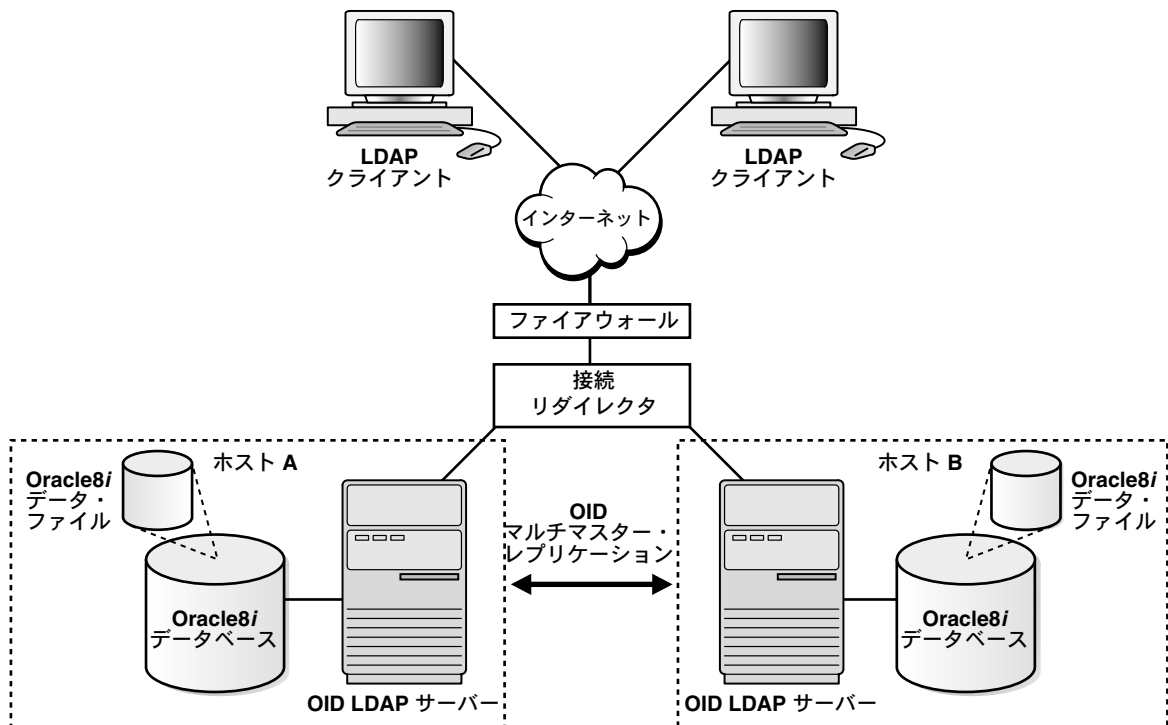
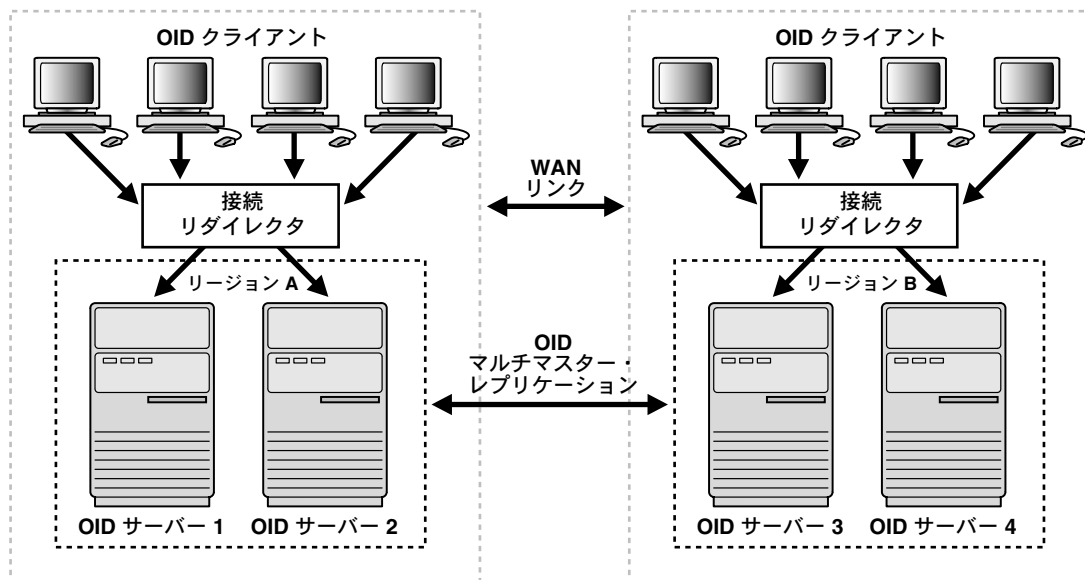


図 16-4 が示すように、相互にレプリケートする 2 つの Oracle Internet Directory ノードを各リージョンに設定できます。この構成は、大企業が配置しているグローバル・ディレクトリ・ネットワークの典型的な例で、前述のリージョンがそれぞれ、大陸または国に対応する場合などがあります。

図 16-4 配置例 2



# 第IV部

---

## 付録

第 IV 部は次の付録で構成されています。

- [付録 A「LDIF およびコマンドライン・ツールの構文」](#)
- [付録 B「データベース・コピー・プロシージャを使用した DSA の追加」](#)
- [付録 C「Oracle Wallet Manager の使用方法」](#)
- [付録 D「アクセス制御ディレクティブ書式の使用法」](#)
- [付録 E「スキーマ要素」](#)
- [付録 F「他の LDAP 準拠のディレクトリからのデータの移行」](#)
- [付録 G「トラブルシューティング」](#)



---

# LDIF およびコマンドライン・ツールの構文

この付録では、**LDAP データ交換フォーマット (LDIF)** と LDAP コマンドライン・ツールに関する構文、使用方法および例を紹介します。この付録では、次の項目について説明します。

- **LDAP データ交換フォーマット (LDIF) の構文**
- **コマンドライン・ツールの構文**
- **バルク・ツールの構文**
- **カタログ管理ツールの構文**
- **OID モニターの構文**
- **OID 制御ユーティリティの構文**
- **OID データベース・パスワード・ユーティリティの構文**
- **OID データベース統計収集ツールの構文**

# LDAP データ交換フォーマット (LDIF) の構文

ディレクトリ・エントリの標準ファイル形式は、次のとおりです。

```
dn: distinguished_name
attribute_type: attribute_value
.
.
.
objectClass: object_class_value
.
.
.
```

プロパティ	値	説明
dn:	RDN,RDN,RDN, ...	相対識別名 (RDN) をカンマで区切ります。
attribute:	attribute_value	この行は、エントリの各属性、および複数値属性の各属性値ごとに繰り返します。
objectClass:	object_class_value	この行は、各オブジェクト・クラスごとに繰り返します。

次の例は、ある従業員のファイル・エントリを示しています。1 行目は識別名 (DN) です。DN に続く各行は、属性のニーモニックで始まり、その属性の値が続きます。各エントリが、そのエントリのオブジェクト・クラスを定義する行で終了していることに注意してください。

```
dn: cn=Suzie Smith,ou=Server Technology,o=Acme, c=US
cn: Suzie Smith
cn: SuzieS
sn: Smith
email: ssmith@us.Acme.com
telephoneNumber: 69332
photo:/ORACLE_HOME/empdir/photog/ssmith.jpg
objectClass: organizational person
objectClass: person
objectClass: top
```

次の例は、ある組織のファイル・エントリを示しています。

```
dn: o=Acme,c=US
o: Acme
ou: Financial Applications
objectClass: organization
objectClass: top
```

## LDIF 形式化の注意事項

次に示すのは、形式化規則のリストです。このリストは、全規則ではありません。

- 追加対象のエントリに属しているすべての必須属性は、非 NULL 値で LDIF ファイルに記述する必要があります。

**ヒント：** オブジェクト・クラスの必須属性とオプション属性のタイプを調べるには、Oracle Directory Manager を使用します。6-9 ページの「[Oracle Directory Manager を使用したオブジェクト・クラスのプロパティの表示](#)」を参照してください。

- 非表示文字やタブは、ベース 64 エンコーディングによる属性値で記述します。
- ファイル内のエントリの間は、空白行で区切る必要があります。
- ファイルには、少なくとも 1 つのエントリが含まれている必要があります。
- 次の行に継続する場合は、継続行を空白またはタブで開始します。
- 個々のエントリの間には空白行を追加してください。
- 写真などのバイナリ・ファイルは、スラッシュ (/) で始まるファイルの絶対アドレスで参照を付けます。
- 識別名 (DN) には、オブジェクトに対する一意の完全なディレクトリ・アドレスが含まれます。
- DN の後にリストされる行には、属性とその値が含まれます。入力ファイルで使用する DN と属性は、DIT の既存の構造と一致している必要があります。DIT 内で実装していない属性は、入力ファイルで使わないでください。
- LDIF ファイル内のエントリは、DIT が上位から下位へ作成されるように順に記述します。エントリがその DN の上位のエントリに依存している場合は、その子エントリの前に上位エントリを必ず追加してください。
- LDIF ファイル内にスキーマを定義するときは、左カッコと最初のテキストの間、および最後のテキストと右カッコの間に空白を挿入してください。

### 関連項目：

- LDIF 形式化規則の全リストは、xxiii ページの「[関連文書](#)」の各種資料を参照してください。
- 12-3 ページ「[LDIF ファイルでの NLS の使用方法](#)」

## コマンドライン・ツールの構文

この項では、次のツールの使用方法を説明します。

- [ldapadd 構文](#)
- [ldapaddmt 構文](#)
- [ldapbind 構文](#)
- [ldapcompare 構文](#)
- [ldapdelete 構文](#)
- [ldapmoddn 構文](#)
- [ldapmodify 構文](#)
- [ldapmodifymt 構文](#)
- [ldapsearch 構文](#)

### ldapadd 構文

ldapadd コマンドライン・ツールを使用すると、エントリ、そのオブジェクト・クラス、属性および値をディレクトリに追加できます。既存のエントリに属性を追加するには、ldapmodify コマンドを使用します。ldapmodify コマンドは、A-12 ページの「[ldapmodify 構文](#)」を参照してください。

**関連項目：** 入力ファイルを使用してサーバーを構成するために ldapadd を使用する方法は、5-10 ページの「[ldapadd を使用した構成設定エントリの追加](#)」を参照してください。

ldapadd は次の構文を使用します。

```
ldapadd [arguments] -f filename
```

*filename* は、A-2 ページの「[LDAP データ交換フォーマット \(LDIF\) の構文](#)」で説明されている仕様に従って作成された LDIF ファイルの名前です。

次の例は、LDIF ファイル `my_ldif_file.ldi` に指定されているエントリを追加します。

```
ldapadd -p 389 -h myhost -f my_ldif_file.ldi
```



オプションの引数	説明
-b	ファイルにバイナリ・ファイル名が含まれていることを指定します。バイナリ・ファイル名はスラッシュで始まります。ツールは、参照先のファイルから実際の値を取り出します。
-c	エラーが発生しても処理を継続する場合に指定します。エラーはレポートされます。(このオプションを使用しない場合、エラーが発生すると <code>ldapadd</code> は停止します。)
-D <i>binddn</i>	ディレクトリに対して認証するときに、 <i>binddn</i> に指定されているエントリとして認証することを指定します。この引数は、 <i>-w password</i> オプションとともに使用します。
-E " <i>character_set</i> "	ネイティブ・キャラクタ・セット・エンコーディングを指定します。 <a href="#">第 12 章「各国語サポート (NLS) の管理」</a> を参照してください。
-f <i>filename</i>	LDIF 形式のインポート・データ・ファイルの入力名を指定します。LDIF ファイルのフォーマット方法の詳細は、A-2 ページの「 <a href="#">LDAP データ交換フォーマット (LDIF) の構文</a> 」を参照してください。
-h <i>ldaphost</i>	デフォルトのホスト（ローカル・コンピュータ）ではなく、 <i>ldaphost</i> に接続します。 <i>ldaphost</i> には、コンピュータ名または IP アドレスを指定します。
-K	-k と同様ですが、Kerberos バインドの最初のステップのみ実行します。
-k	簡易認証のかわりに、Kerberos 認証を使用して認証します。このオプションを使用可能にするには、定義済みの Kerberos でコンパイルする必要があります。  証明書を付与する有効なチケットをすでに所有している必要があります。
-n	操作を実際には実行せずに、予測結果を示します。
-p <i>ldapport</i>	TCP ポート <i>ldapport</i> 上のディレクトリに接続します。このオプションを指定しない場合は、デフォルト・ポート（389）に接続されます。
-P <i>wallet_password</i>	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet のパスワードを指定します。
-U <i>SSLAuth</i>	SSL 認証モードを指定します。 <ul style="list-style-type: none"><li>■ 1: SSL 認証なし</li><li>■ 2: サーバー認証</li><li>■ 3: クライアントとサーバーの認証</li></ul>
-v	冗長モードを指定します。
-w <i>password</i>	接続に必要なパスワードを指定します。

オプションの引数	説明
-W <i>wallet_location</i>	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet の位置を指定します。

ldapaddmt 構文

ldapaddmt は ldapadd と似ています。これを使用すると、エントリ、そのオブジェクト・クラス、属性および値をディレクトリに追加できます。ldapadd と異なるのは、複数のエントリを同時に追加するために複数のスレッドをサポートしている点です。

LDIF エントリの処理中に、ldapaddmt は、現行のディレクトリ内の add.log ファイルにエラー・ログを記録します。

ldapaddmt は次の構文を使用します。

```
ldapaddmt -T number_of_threads -h host -p port -f filename
```

*filename* は、A-2 ページの「LDAP データ交換フォーマット (LDIF) の構文」で説明されている仕様に従って作成された LDIF ファイルの名前です。

次の例は、5 つの同時スレッドを使用して、ファイル myentries.ldif 内のエントリを処理しています。

```
ldapaddmt -T 5 -h node1 -p 3000 -f myentries.ldif
```

**注意：** 同時スレッドの数が増加すると、LDIF エントリの作成は速くなりますが、システム・リソースはより多く消費されます。

オプションの引数	説明
-b	データ・ファイルにバイナリ・ファイル名が含まれていることを指定します。バイナリ・ファイル名はスラッシュで始まります。ツールは、参照先のファイルから実際の値を取り出します。
-c	エラーが発生しても処理を継続する場合に指定します。エラーはレポートされます。(このオプションを使用しない場合、エラーが発生するとツールは停止します。)
-D <i>binddn</i>	ディレクトリに対して認証するとき、 <i>binddn</i> に指定されているエントリとして認証することを指定します。この引数は、 <i>-w password</i> オプションとともに使用します。
-E " <i>character_set</i> "	ネイティブ・キャラクタ・セット・エンコーディングを指定します。 第 12 章「各国語サポート (NLS) の管理」を参照してください。

オプションの引数	説明
-h <i>ldaphost</i>	デフォルトのホスト（ローカル・コンピュータ）ではなく、 <i>ldaphost</i> に接続します。 <i>ldaphost</i> には、コンピュータ名または IP アドレスを指定します。
-K	-k と同様ですが、Kerberos バインドの最初のステップのみ実行します。
-k	簡易認証のかわりに、Kerberos 認証を使用して認証します。このオプションを使用可能にするには、定義済みの Kerberos でコンパイルする必要があります。  証明書を付与する有効なチケットをすでに所有している必要があります。
-n	操作を実際には実行せずに、予測結果を示します。
-p <i>ldappport</i>	TCP ポート <i>ldappport</i> 上のディレクトリに接続します。このオプションを指定しない場合は、デフォルト・ポート（389）に接続されます。
-P <i>wallet_password</i>	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet のパスワードを指定します。
-T	エントリを同時に処理するスレッドの数を設定します。
-U <i>SSLAuth</i>	SSL 認証モードを指定します。  <ul style="list-style-type: none"> <li>■ 1: SSL 認証なし</li> <li>■ 2: サーバー認証</li> <li>■ 3: クライアントとサーバーの認証</li> </ul>
-v	冗長モードを指定します。
-w <i>password</i>	接続に必要なパスワードを指定します。
-W <i>wallet_location</i>	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet の位置を指定します。

## ldapbind 構文

ldapbind コマンドライン・ツールを使用すると、サーバーに対してクライアントを認証できるかどうかを調べることができます。

ldapbind は次の構文を使用します。

```
ldapbind [arguments]
```

オプションの引数	説明
-D <i>binddn</i>	ディレクトリに対して認証するときに、 <i>binddn</i> に指定されているエントリとして認証することを指定します。この引数は、 <i>-w password</i> オプションとともに使用します。
-E ". <i>character_set</i> "	ネイティブ・キャラクタ・セット・エンコーディングを指定します。 <a href="#">第 12 章「各国語サポート（NLS）の管理」</a> を参照してください。
-h <i>ldaphost</i>	デフォルトのホスト（ローカル・コンピュータ）ではなく、 <i>ldaphost</i> に接続します。 <i>ldaphost</i> には、コンピュータ名または IP アドレスを指定します。
-n	操作を実際には実行せずに、予測結果を示します。
-p <i>ldapport</i>	TCP ポート <i>ldapport</i> 上のディレクトリに接続します。このオプションを指定しない場合は、デフォルト・ポート（389）に接続されます。
-P <i>wallet_password</i>	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet のパスワードを指定します。
-U <i>SSLAuth</i>	SSL 認証モードを指定します。 <ul style="list-style-type: none"><li>■ 1: SSL 認証なし</li><li>■ 2: サーバー認証</li><li>■ 3: クライアントとサーバーの認証</li></ul>
-w <i>password</i>	接続に必要なパスワードを指定します。
-W <i>wallet_location</i>	Wallet の位置を指定します（サーバー、またはクライアントとサーバーの SSL 接続の場合は必須）。

ldapcompare 構文

ldapcompare コマンドライン・ツールを使用すると、コマンドラインで指定した属性値と、ディレクトリ・エントリの属性値を比較できます。

ldapcompare は次の構文を使用します。

```
ldapcompare [arguments]
```

次の例は、Person Nine の title が associate であるかどうかを通知します。

```
ldapcompare -p 389 -h myhost -b "cn=Person Nine, ou=EuroSinet Suite, o=IMC, c=US" -a title -v associate
```

必須の引数	説明
-a <i>attribute name</i>	比較を実行する属性を指定します。
-b <i>basedn</i>	比較を実行するエントリの識別名を指定します。
-v <i>attribute value</i>	比較する属性値を指定します。

オプションの引数	説明
-D <i>binddn</i>	ディレクトリに対して認証するとき、 <i>binddn</i> に指定されているエントリとして認証することを指定します。この引数は、 <i>-w password</i> オプションとともに使用します。
-d <i>debug level</i>	デバッグ・レベルを設定します。5-22 ページの「 <a href="#">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</a> 」を参照してください。
-E " <i>character_set</i> "	ネイティブ・キャラクタ・セット・エンコーディングを指定します。 <a href="#">第 12 章「各国語サポート (NLS) の管理</a> 」を参照してください。
-f <i>filename</i>	入力ファイル名を指定します。
-h <i>ldaphost</i>	デフォルトのホスト（ローカル・コンピュータ）ではなく、 <i>ldaphost</i> に接続します。 <i>ldaphost</i> には、コンピュータ名または IP アドレスを指定します。
-p <i>ldapport</i>	TCP ポート <i>ldapport</i> 上のディレクトリに接続します。このオプションを指定しない場合は、デフォルト・ポート（389）に接続されます。
-P <i>wallet_password</i>	Wallet のパスワードを指定します（サーバー、またはクライアントとサーバーの SSL 接続の場合は必須）。
-U <i>SSLAuth</i>	SSL 認証モードを指定します。 <ul style="list-style-type: none"> <li>■ 1: SSL 認証なし</li> <li>■ 2: サーバー認証</li> <li>■ 3: クライアントとサーバーの認証</li> </ul>
-w <i>password</i>	接続に必要なパスワードを指定します。
-W <i>wallet_location</i>	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet の位置を指定します。

ldapdelete 構文

ldapdelete コマンドライン・ツールを使用すると、コマンドラインに指定したディレクトリからエントリ全体を削除できます。

ldapdelete は次の構文を使用します。

```
ldapdelete [arguments] "entry_DN"
```

次の例では、myhost という名前のホストでポート 389 を使用しています。

```
ldapdelete -p 389 -h myhost ou=EuroSInet Suite, o=IMC, c=US"
```

オプションの引数	説明
-D binddn	ディレクトリに対して認証するときに、binddn パラメータに完全識別名 (DN) を使用します。通常、-w password オプションとともに使用されます。
-d debug level	デバッグ・レベルを設定します。5-22 ページの「OID 制御ユーティリティを使用したデバッグ・ロギング・レベルの設定」を参照してください。
-E "character_set"	ネイティブ・キャラクタ・セット・エンコーディングを指定します。第 12 章「各国語サポート (NLS) の管理」を参照してください。
-f filename	入力ファイル名を指定します。
-h ldaphost	デフォルトのホスト (ローカル・コンピュータ) ではなく、ldaphost に接続します。ldaphost には、コンピュータ名または IP アドレスを指定します。
-k	簡易認証のかわりに、Kerberos 認証を使用して認証します。このオプションを使用可能にするには、定義済みの Kerberos でコンパイルする必要があります。  証明書を付与する有効なチケットをすでに所有している必要があります。
-n	削除を実際には実行せずに、予測結果を示します。
-p ldapport	TCP ポート ldapport 上のディレクトリに接続します。このオプションを指定しない場合は、デフォルト・ポート (389) に接続されます。
-P wallet_password	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet のパスワードを指定します。
-U SSLAuth	SSL 認証モードを指定します。 <ul style="list-style-type: none"><li>■ 1: SSL 認証なし</li><li>■ 2: サーバー認証</li><li>■ 3: クライアントとサーバーの認証</li></ul>

オプションの引数	説明
<code>-v</code>	冗長モードを指定します。
<code>-w password</code>	接続に必要なパスワードを指定します。
<code>-W wallet_location</code>	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet の位置を指定します。

## ldapmoddn 構文

ldapmoddn コマンドライン・ツールを使用すると、エントリの識別名 (DN) または相対識別名 (RDN) を変更できます。

ldapmoddn は次の構文を使用します。

```
ldapmoddn [arguments]
```

次の例では、ldapmoddn を使用して、DN の RDN コンポーネントを "cn=dcpl" から "cn=thanh mai" に変更しています。ポートは 389、myhost という名前のホストを使用しています。

```
ldapmoddn -p 389 -h myhost -b "cn=dcpl,dc=Americas,dc=imc,dc=com" -R "cn=thanh mai"
```

必須の引数	説明
<code>-b basedn</code>	変更されるエントリの識別名 (DN) を指定します。

オプションの引数	説明
<code>-D binddn</code>	ディレクトリに対して認証するときは、そのエントリが <code>binddn</code> に指定されている場合に認証します。この引数は、 <code>-w password</code> オプションとともに使用します。
<code>-E "character_set"</code>	ネイティブ・キャラクタ・セット・エンコーディングを指定します。第 12 章「各国語サポート (NLS) の管理」を参照してください。
<code>-f filename</code>	入力ファイル名を指定します。
<code>-h ldaphost</code>	デフォルトのホスト (ローカル・コンピュータ) ではなく、 <code>ldaphost</code> に接続します。 <code>ldaphost</code> には、コンピュータ名または IP アドレスを指定します。
<code>-N newparent</code>	RDN の新しい親を指定します。

オプションの引数	説明
-p <i>ldapport</i>	TCP ポート <i>ldapport</i> 上のディレクトリに接続します。このオプションを指定しない場合は、デフォルト・ポート（389）に接続されます。
-P <i>wallet_password</i>	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet のパスワードを指定します。
-r	旧 RDN を変更エントリ内に値として保持しないことを指定します。この引数が指定されない場合、旧 RDN は変更エントリ内に属性として保持されます。
-R <i>newrdn</i>	新規 RDN を指定します。
-U <i>SSLAuth</i>	SSL 認証モードを指定します。 <ul style="list-style-type: none"><li>1: SSL 認証なし</li><li>2: サーバー認証</li><li>3: クライアントとサーバーの認証</li></ul>
-w <i>password</i>	接続に必要なパスワードを指定します。
-W <i>wallet_location</i>	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet の位置を指定します。

ldapmodify 構文

ldapmodify ツールは、属性で作用します。

ldapmodify は次の構文を使用します。

```
ldapmodify [arguments] -f filename
```

*filename* は、A-2 ページの「LDAP データ交換フォーマット (LDIF) の構文」で説明されている仕様に従って作成された LDIF ファイルの名前です。

次の表の引数リストは、すべての引数ではありません。

オプションの引数	説明
-a	エントリが追加対象で、入力ファイルが LDIF 形式であることを示します。
-b	データ・ファイルにバイナリ・ファイル名が含まれていることを指定します。バイナリ・ファイル名はスラッシュで始まります。
-c	エラーが発生しても処理を継続する場合に指定します。エラーはレポートされます。（このオプションを使用しない場合、エラーが発生すると ldapmodify は停止します。）



オプションの引数	説明
-D <i>binddn</i>	ディレクトリに対して認証するときに、 <i>binddn</i> に指定されているエントリとして認証することを指定します。この引数は、-w <i>password</i> オプションとともに使用します。
-E " <i>character_set</i> "	ネイティブ・キャラクタ・セット・エンコーディングを指定します。 <a href="#">第 12 章「各国語サポート (NLS) の管理」</a> を参照してください。
-h <i>ldaphost</i>	デフォルトのホスト（ローカル・コンピュータ）ではなく、 <i>ldaphost</i> に接続します。 <i>ldaphost</i> には、コンピュータ名または IP アドレスを指定します。
-n	操作を実際には実行せずに、予測結果を示します。
-p <i>ldapport</i>	TCP ポート <i>ldapport</i> 上のディレクトリに接続します。このオプションを指定しない場合は、デフォルト・ポート（389）に接続されます。
-P <i>wallet_password</i>	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet のパスワードを指定します。
-U <i>SSLAuth</i>	SSL 認証モードを指定します。 <ul style="list-style-type: none"> <li>■ 1: SSL 認証なし</li> <li>■ 2: サーバー認証</li> <li>■ 3: クライアントとサーバーの認証</li> </ul>
-v	冗長モードを指定します。
-w <i>password</i>	デフォルトの非認証の NULL バインドをオーバーライドします。認証を強制するには、このオプションを -D オプションとともに使用します。
-W <i>wallet_location</i>	Wallet の位置を指定します（サーバー、またはクライアントとサーバーの SSL 接続の場合は必須）。

-f フラグを使用して modify、delete および modifyrdn 操作を実行するには、入力ファイル形式に LDIF を使用します（A-2 ページの「[LDAP データ交換フォーマット \(LDIF\) の構文](#)」を参照してください）。仕様は次のとおりです。

エントリは常に空白行で区切ります。

属性値の後の空白など、LDIF 入力ファイルにおける不要な空白は、LDAP 操作が失敗する原因となります。

**第 1 行:** 変更レコードの場合は、その 1 行目にリテラル dn:、その後にエントリの識別名 (DN) 値を記述します。たとえば、次のように記述します。

```
dn:cn=Barbara Fritchey,ou=Sales,o=Oracle,c=US
```

**第2行:** 変更レコードの場合は、その2行目にリテラル `changetype:`、その後に変更の種類 (`add`、`delete`、`modify`、`modrdn` など) を記述します。たとえば、次のように記述します。

```
changetype:modify
```

または

```
changetype:modrdn
```

変更の種類に応じて、次の要件に従って各レコードの残りの部分をフォーマットします。

- `changetype:add`

LDIF 形式を使用します (A-2 ページの「[LDAP データ交換フォーマット \(LDIF\) の構文](#)」を参照してください)。

- `changetype:modify`

この `changetype` に続く行には、前述の第1行で指定したエントリに属する属性に対する変更内容を記述します。属性を変更する場合は、3種類の変更タイプ (`add`、`delete` および `replace`) を指定できます。変更タイプについて次に説明します。

- **属性値の追加。** `changetype modify` のこのオプションは、既存の複数値の属性にさらに値を追加します。属性が存在しない場合は、指定した値で新規属性を追加します。

```
add: attribute name
attribute name: value1
attribute name: value2...
```

次のようなコマンドを実行します。

```
dn:cn=Barbara Fritchey,ou=Sales,o=Oracle,c=US
changetype:modify
add: work-phone
work-phone:510/506-7000
work-phone:510/506-7001
```

- **値の削除。** `delete` 行のみ記述すると、指定した属性のすべての値が削除されます。属性行を指定した場合は、その属性から特定の値を削除できます。

```
delete: attribute name
[attribute name: value1]
```

次のようなコマンドを実行します。

```
dn:cn=Barbara Fritchey,ou=Sales,o=Oracle,c=US
changetype:delete
delete: home-fax
```

- **値の置換。**このオプションを使用すると、新しく指定した設定で、属性の値をすべて置換できます。

```
replace:attribute name  
[attribute name:value1 ...]
```

replace に属性を指定しない場合、ディレクトリは空のセットを追加します。次に、ディレクトリはその空のセットを削除要求と解釈し、エントリから属性を削除することによって対応します。この方法は、存在するかどうかわからない属性を削除する場合に便利です。

次のようなコマンドを実行します。

```
dn:cn=Barbara Fritchey,ou=Sales,o=Oracle,c=US  
changetype:modify  
replace: work-phone  
work-phone:510/506-7002
```

\* changetype:delete

この変更タイプは、エントリを削除するときに使用します。第1行でエントリを指定し、第2行で changetype に delete を指定しているため、それ以上の入力はありません。

次のようなコマンドを実行します。

```
dn:cn=Barbara Fritchey,ou=Sales,o=Oracle,c=US  
changetype:delete
```

\* changetype:modrdn

変更タイプに続く行に、次の形式で新規の相対識別名 (RDN) を指定します。

```
newrdn: RDN
```

次のようなコマンドを実行します。

```
dn:cn=Barbara Fritchey,ou=Sales,o=Oracle,c=US  
changetype:modrdn  
newrdn: cn=Barbara Fritchey-Blomberg
```

ldapmodifymt 構文

ldapmodifymt コマンドライン・ツールを使用すると、複数のエントリを同時に変更できます。

ldapmodifymt は次の構文を使用します。

```
ldapmodifymt -T number_of_threads [arguments] -f filename
```

filename は、A-2 ページの「LDAP データ交換フォーマット (LDIF) の構文」で説明されている仕様に従って作成された LDIF ファイルの名前です。

**関連項目：** ldapmodifymt で使用されるその他の形式化仕様は、A-12 ページの「ldapmodify 構文」を参照してください。

次の例は、5 つの同時スレッドを使用して、ファイル myentries.ldif 内のエントリを変更しています。

```
ldapmodifymt -T 5 -h node1 -p 3000 -f myentries.ldif
```

オプションの引数	説明
-a	エントリが追加対象で、入力ファイルが LDIF 形式であることを示します。(ldapadd を実行している場合、このフラグは必要ありません。)
-b	データ・ファイルにバイナリ・ファイル名が含まれていることを指定します。バイナリ・ファイル名はスラッシュで始まります。
-c	エラーが発生しても処理を継続する場合に指定します。エラーはレポートされます。(このオプションを使用しない場合、エラーが発生すると ldapmodify は停止します。)
-D binddn	ディレクトリに対して認証するとき、binddn に指定されているエントリとして認証することを指定します。この引数は、-w password オプションとともに使用します。
-E "character_set"	ネイティブ・キャラクタ・セット・エンコーディングを指定します。第 12 章「各国語サポート (NLS) の管理」を参照してください。
-h ldaphost	デフォルトのホスト (ローカル・コンピュータ) ではなく、ldaphost に接続します。ldaphost には、コンピュータ名または IP アドレスを指定します。
-n	操作を実際には実行せずに、予測結果を示します。
-p ldapport	TCP ポート ldapport 上のディレクトリに接続します。このオプションを指定しない場合は、デフォルト・ポート (389) に接続されます。
-P wallet_password	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet のパスワードを指定します。

オプションの引数	説明
-T	エントリを同時に処理するスレッドの数を設定します。
-U <i>SSLAUTH</i>	SSL 認証モードを指定します。 <ul style="list-style-type: none"> <li>1: SSL 認証なし</li> <li>2: サーバー認証</li> <li>3: クライアントとサーバーの認証</li> </ul>
-v	冗長モードを指定します。
-w <i>password</i>	デフォルトの非認証の NULL バインドをオーバーライドします。認証を強制するには、このオプションを -D オプションとともに使用します。
-W <i>wallet_location</i>	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet の位置を指定します。

## ldapsearch 構文

ldapsearch コマンドライン・ツールを使用すると、ディレクトリ内の特定のエントリを検索および取得できます。

ldapsearch は次の構文を使用します。

```
ldapsearch [arguments] filter [attributes]
```

*filter* の書式は RFC-2254 に準拠している必要があります。この規格の詳細は、次の Web サイトを検索してください。 <http://www.ietf.org/rfc/rfc2254.txt>

属性は空白で区切ります。属性を何も入力しないと、すべての属性が取り出されます。

必須の引数	説明
-b <i>basedn</i>	検索するベース識別名 (DN) を指定します。
-s <i>scope</i>	検索有効範囲を指定します。base、one または sub。

オプションの引数	説明
-A	属性名のみ取り出します (値は取り出しません)。
-a <i>deref</i>	別名参照解除を指定します。never、always、search または find。
-B	非 ASCII 値を出力します。

オプションの引数	説明
-D <i>binddn</i>	ディレクトリに対して認証するときに、 <i>binddn</i> に指定されているエントリとして認証することを指定します。この引数は、 <i>-w password</i> オプションとともに使用します。
-d <i>debug level</i>	指定したレベルにデバッグ・レベルを設定します (5-23 ページの表 5-1 を参照してください)。
-E " <i>character_set</i> "	ネイティブ・キャラクタ・セット・エンコーディングを指定します。第 12 章「各国語サポート (NLS) の管理」を参照してください。
-f <i>file</i>	<i>file</i> にリストされている検索順を実行します。
-F <i>sep</i>	属性名と値の間に、「=」ではなく「 <i>sep</i> 」を出力します。
-h <i>ldaphost</i>	デフォルトのホスト（ローカル・コンピュータ）ではなく、 <i>ldaphost</i> に接続します。 <i>ldaphost</i> には、コンピュータ名または IP アドレスを指定します。
-L	エントリを LDIF 形式で出力します (引数 <i>-B</i> の内容も含まれます)。
-l <i>timelimit</i>	<i>ldapsearch</i> コマンドが完了するまでの最大待機時間 (秒) を指定します。
-n	検索を実際には実行せずに、予測結果を示します。
-p <i>ldappport</i>	TCP ポート <i>ldappport</i> 上のディレクトリに接続します。このオプションを指定しない場合は、デフォルト・ポート (389) に接続されます。
-P <i>wallet_password</i>	Wallet のパスワードを指定します (サーバー、またはクライアントとサーバーの SSL 接続の場合は必須)。
-S <i>attr</i>	検索結果を属性 <i>attr</i> でソートします。
-t	/tmp のファイルに書き込みます。
-u	わかりやすいエントリ名で出力します。
-U <i>SSLAuth</i>	SSL 認証モードを指定します。 <ul style="list-style-type: none"> <li>■ 1: SSL 認証なし</li> <li>■ 2: サーバー認証</li> <li>■ 3: クライアントとサーバーの認証</li> </ul>
-v	冗長モードを指定します。
-w <i>bindpassword</i>	簡易認証の場合にバインド・パスワードを指定します。
-W <i>wallet_location</i>	サーバー、またはクライアントとサーバーの SSL 接続の場合は必須の、Wallet の位置を指定します。
-z <i>sizelimit</i>	エントリの最大検索数を指定します。

## ldapsearch フィルタの例

検索コマンドの作成方法を理解するには、次の例を参考にしてください。

**例 1: ベース・オブジェクト検索** 次の例は、ディレクトリ上でルートからベース・レベルの検索を実行します。

```
ldapsearch -p 389 -h myhost -b "" -s base -v "objectclass=*"
```

- `-b` で、検索するベース DN（この場合はルート）を指定します。
- `-s` で、ベース検索（base）、1 レベルの検索（one）またはサブツリー検索（sub）のうちの、いずれの検索かを指定します。
- `"objectclass=*"` で、検索のフィルタを指定します。

**例 2: 1 レベルの検索** 次の例は、`"ou=HR, ou=Americas, o=IMC, c=US"` で開始される 1 レベルの検索を実行します。

```
ldapsearch -p 389 -h myhost -b "ou=HR, ou=Americas, o=IMC, c=US" -s one -v "objectclass=*"
```

**例 3: サブツリー検索** 次の例は、サブツリー検索を実行して、`"cn=Person"` で始まる DN を持つすべてのエントリを戻します。

```
ldapsearch -p 389 -h myhost -b "c=US" -s sub -v "cn=Person*"
```

**例 4: サイズ制限を使用する検索** 次の例では、一致するエントリが 3 つ以上あっても、実際に取り出すエントリは 2 つのみです。

```
ldapsearch -h myhost -p 389 -z 2 -b "ou=Benefits,ou=HR,ou=Americas,o=IMC,c=US" -s one "objectclass=*"
```

**例 5: 必須の属性と属性オプションでの検索** 次の例は、一致したエントリの DN 属性値のみを戻します。

```
ldapsearch -p 389 -h myhost -b "c=US" -s sub -v "objectclass=*" dn
```

次の例は、姓（sn）および説明（description）属性値とともに、識別名（dn）を取り出します。

```
ldapsearch -p 389 -h myhost -b "c=US" -s sub -v "cn=Person*" dn sn description
```

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を持った一般名（cn）属性を持つエントリを取り出します。この例の場合には、一般名がフランス語で、R で始まるエントリを取り出します。

```
ldapsearch -p 389 -h myhost -b "c=US" -s sub "cn;lang-fr=R*"
```

John のエントリで、cn;lang-it 言語コード属性オプションに値が設定されていないと想定します。この場合、次の例は失敗します。

```
ldapsearch -p 389 -h myhost -b "c=us" -s sub "cn;lang-it=Giovanni"
```

**例 6: 全ユーザー属性および指定した操作属性の検索** 次の例は、全ユーザー属性と、createtimestamp および orclguid 操作属性を取り出します。

```
ldapsearch -p 389 -h myhost -b "ou=Benefits,ou=HR,ou=Americas,o=IMC,c=US" -s sub "cn=Person*" * createtimestamp orclguid
```

次の例は、Anne Smith によって変更されたエントリを取り出します。

```
ldapsearch -h sun1 -b "" "(&(objectclass=*)(modifiersname=cn=Anne Smith))"
```

次の例は、2000 年 4 月 1 日から 2000 年 4 月 6 日までの間に変更されたエントリを取り出します。

```
ldapsearch -h sun1 -b "" "(&(objectclass=*)(modifytimestamp>=20000401000000)(modifytimestamp<= 20000406235959))"
```

---

---

**注意：** modifiersname と modifytimestamp は索引付き属性ではないので、catalog.sh を使用してこれら 2 つの属性に索引を付けてください。前述の 2 つの ldapsearch コマンドを発行する前に、Oracle Directory Server を再起動してください。

---

---

**その他の例：** 次の各例は、ホスト sun1 のポート 389 で、識別名 (DN) "ou=hr,o=acme,c=us" から開始してサブツリー全体を検索します。

次の例は、objectclass 属性の値を持つすべてのエントリを検索します。

```
ldapsearch -p 389 -h sun1 -b "ou=hr, o=acme, c=us" -s subtree "objectclass=*"
```

次の例は、objectclass 属性の値が orcle で始まるすべてのエントリを検索します。

```
ldapsearch -p 389 -h sun1 -b "ou=hr, o=acme, c=us" -s subtree "objectclass=orcle*"
```

次の例は、objectclass 属性が orcle で始まり、cn が foo で始まるエントリを検索します。

```
ldapsearch -p 389 -h sun1 -b "ou=hr, o=acme, c=us" -s subtree "(&(objectclass=orcle*)(cn=foo*))"
```

次の例は、一般名 (cn) が foo ではないエントリを検索します。

```
ldapsearch -p 389 -h sun1 -b "ou=hr, o=acme, c=us" -s subtree "(!(cn=foo))"
```



次の例は、cn が foo で始まるか、あるいは sn が bar で始まるエントリを検索します。

```
ldapsearch -p 389 -h sun1 -b "ou=hr, o=acme, c=us" -s subtree
"(| (cn=foo*) (sn=bar*))"
```

次の例は、employeenumber が 10000 より小か等しいエントリを検索します。

```
ldapsearch -p 389 -h sun1 -b "ou=hr, o=acme, c=us" -s subtree
"employeenumber<=10000"
```

# バルク・ツールの構文

この項では、次の項目について説明します。

- [bulkdelete 構文](#)
- [bulkload 構文](#)
- [bulkmodify 構文](#)
- [ldifwrite 構文](#)

## bulkdelete 構文

bulkdelete コマンドライン・ツールを使用すると、サブツリーを効率的に削除できます。このツールは、Oracle Directory Server と Oracle Directory Replication Server がともに稼働しているときに使用できます。また、パフォーマンス向上のために、SQL インタフェースを使用します。このリリースでは、bulkdelete ツールは一度に 1 つのノードでのみ動作します。

このツールは、フィルタベースの削除はサポートしていません。つまり、サブツリーのルート下にあるサブツリー全体が削除されます。ベース識別名 (DN) が、ディレクトリのインストール時に作成された DN ではなく、ユーザーが追加した DN の場合でも削除の対象となります。削除中はサブツリーに対する LDAP アクティビティを制限する必要があります。

bulkdelete ツールは次の構文を使用します。

```
bulkdelete.sh -connect net_service_name -base "base_dn" -size number_of_entries
-encode "character_set"
```

必須の引数	説明
-connect net_service_name	ディレクトリ・データベースに接続するためのネット・サービス名を指定します。  関連項目：『Oracle8i Net8 管理者ガイド』
-base "base_dn"	削除するサブツリーのベース DN を指定します。

オプションの引数	説明
-size <i>number_of_entries</i>	1 トランザクションとしてコミットされるエントリの数を指定します。
-encode "character_set"	ネイティブ・キャラクタ・セット・エンコーディング。

bulkload 構文

bulkload コマンドライン・ツールは、Oracle SQL\*Loader を使用して、他のアプリケーションに常駐しているデータまたは他のアプリケーションで作成されたデータからディレクトリ・エントリを作成します。bulkload を使用するときは、オプションと入力ファイル名を指定します。bulkload ツールの入力ファイルは、LDIF であることが必要です。

**関連項目：** A-2 ページ「[LDAP データ交換フォーマット \(LDIF\) の構文](#)」

bulkload ツールは次の構文を使用します。

```
bulkload.sh -connect net_service_name [-check] [-generate] [-load]
           [-restore] absolute_path_to_ldif.file
```

必須の引数	説明
connect <i>net_service_name</i>	tnsnames.ora ファイルに定義されているネット・サービス名を指定します。  関連項目：『Oracle8i Net8 管理者ガイド』

オプションの引数	説明
check	ファイル内の不整合と重複している識別名 (DN) の存在に関して LDAP スキーマをチェックします。
-encode "character_set"	ネイティブ・キャラクタ・セット・エンコーディングを指定します。第 12 章「 <a href="#">各国語サポート (NLS) の管理</a> 」を参照してください。
generate	Oracle Internet Directory へのロードに適したファイルを作成します。
load	generate で作成されたファイルを、指定したデータベースにロードします。

オプションの引数	説明
restore	orclguid、creatorname および createtimestamp などの操作属性を、新たに生成するかわりに LDIF ファイルから取得します。この引数は、LDIF ファイルに操作属性が含まれている場合にのみ使用してください。また、generate および check 引数と組み合わせて使用してください。

バルク・ロードは、Oracle Internet Directory インスタンスを実行していないときに実行する必要があります。

**関連項目：** Directory Server インスタンスの停止方法は、[第 5 章「Oracle Directory Server の管理」](#)を参照してください。

LDIF データ・ファイルのパスは、check または generate 操作時にはフルパスを指定する必要があります。

## レプリケート環境における複数ノードのバルク・ロード

generate オプションでファイルを生成した後、その同じ SQL\*Loader ファイルを、load オプションを使用して複数のコンピュータにロードできます。この処理は、新規のレプリカ・ノードを作成するときのみ実行してください。

**関連項目：** 10-18 ページ [「タスク 6: 全ノードでの Replication Server の起動」](#)

bulkload の現行バージョンでは、すべてのノードに対する接続情報を 1 つのコマンドで指定できません。

レプリケート・ネットワークにおいて、同一データを複数ノードにロードするときは、orclGUID パラメータ（グローバル ID）がノード全体で一貫していることを確認してください。これは、bulkload のデータ・ファイルを 1 回のみ生成（-generate オプションを使用）し、生成した同じデータ・ファイルを他のノードにロード（-load オプションを使用）することによって処理できます。

## bulkmodify 構文

bulkmodify コマンドライン・ツールを使用すると、多数の既存エントリを効率的に変更できます。bulkmodify ツールは、次の機能をサポートしています。

- サブツリー・ベースの変更。
- 単一属性フィルタ。たとえば、objectclass=\*、objectclass=oneclass または telephonenumber=\* などのフィルタを設定できます。
- 属性値の追加と置換。一致するエントリを一括変更します。

bulkmodify ツールは、指定した属性名と値に対して、初期化時にスキーマ・チェックを実行します。次の基準を満たすすべてのエントリが変更されます。

- 指定したサブツリーの下にあること
- 単一のフィルタ条件を満たしていること
- 変更対象の属性を、必須またはオプションとして含んでいること

一括変更処理時に、Oracle Directory Server と Oracle Directory Replication Server が同時に稼働している可能性があります。一括変更は Replication Server には影響しません。一括変更は、すべてのレプリカに対して実行する必要があります。

---

---

**注意：** LDIF ファイル・ベースの変更は、bulkmodify ではサポートされていません。このタイプの変更では、エントリごとにスキーマ・チェックを行う必要があるため、既存の ldapmodify ツールを上回るパフォーマンスの向上はありません。

---

---

一括変更中はサブツリーへのユーザー・アクセスを制限する必要があります。必要に応じて、bulkmodify の更新対象のサブツリーに、アクセス制御項目 ([ACI](#)) 制限を適用できます。

bulkmodify は、すでに値が1つ存在する単一値の属性に値を追加するためには使用できません。2つ目の値を追加する場合は、ディレクトリ・スキーマを変更して、その属性を複数値の属性にする必要があります。

bulkmodify ツールは次の構文を使用します。

```
bulkmodify -c net_service_name -b base_dn {-a|-r} attr_name -v att_value [-f filter]
[-s size]
```

必須の引数	説明
<code>-c net_service_name</code>	ディレクトリ・データベースのネット・サービス名を指定します。 <b>関連項目:</b> 『Oracle8i Net8 管理者ガイド』
<code>-b base_dn</code>	変更するサブツリーのベース識別名 (DN) を指定します。
<code>-a attr_name</code>	追加する場合に属性名を指定します。
<code>-r attr_name</code>	置換する場合に属性名を指定します。
<code>-v att_value</code>	追加または置換する場合に属性値を指定します。

オプションの引数	説明
<code>-f filter</code>	使用するフィルタを指定します。
<code>-s number_of_entries</code>	1 トランザクションとしてコミットされるエントリの数を指定します。指定しない場合、デフォルトは 100 です。
<code>-E "character_set"</code>	ネイティブ・キャラクタ・セット・エンコーディング。第 12 章「 <a href="#">各国語サポート (NLS) の管理</a> 」を参照してください。

`-f` オプションで指定したフィルタには、単一の属性が含まれている必要があります。

フィルタを指定しないと、デフォルトのフィルタ `objectclass=*` が使用されます。

各実行時に、`-a` または `-r` オプションに指定できる属性名は 1 つのみです。

各実行時に、`-v` オプションに指定できる値は 1 つのみです。たとえば、次の `bulkmodify` コマンドは、マネージャが Anne Smith の全従業員のエントリに、電話番号 408-123-4567 を追加します。

```
-c my_database -b "c=US" -a telephoneNumber -v "408-123-4567 -f "manager=Anne Smith"
```

`bulkmodify` プロシージャの完了後、変更されたエントリが確実に読み込まれるように、Oracle Internet Directory サーバーを再起動してください。

ldifwrite 構文

ldifwrite コマンドライン・ツールを使用すると、Oracle Internet Directory に常駐している情報の一部またはすべてを LDIF に変換できます。変換した情報は、レプリケート・ディレクトリの新規ノード、またはバックアップ保管用の別のノードへのロードに使用できます。ldifwrite ツールは、指定した識別名 (DN) を含めその下の全エントリを処理対象とするサブツリー検索を実行します。

ldifwrite ツールは次の構文を使用します。

```
ldifwrite -c net_service_name -b base_DN -f filename
```

必須の引数	説明
-c net_service_name	データの取得元であるディレクトリのネット・サービス名を指定します。ネット・サービス名は、tnsnames.ora ファイルに定義されています。 <b>関連項目:</b> 『Oracle8i Net8 管理者ガイド』
-b base_DN	LDIF 形式で書き出すサブツリーのベース識別名 (DN) を指定します。
-f filename	作成する LDIF ファイルの名前を指定します。

オプションの引数	説明
-E "character_set"	ネイティブ・キャラクタ・セット・エンコーディングを指定します。 <b>関連項目:</b> 12-8 ページ <a href="#">「ldifwrite での NLS の使用方法」</a>

次の例は、ou=Europe、o=imc、c=us の下の全エントリを output1.ldi ファイルに書き出します。

```
ldifwrite -c nldap -b "ou=Europe, o=imc, c=us" -f output1.ldi
```

引数はすべて必須です。

LDIF ファイルと中間ファイルは、常に現行のディレクトリに書き込まれます。

ldifwrite ツールには、createtimestamp、creatorsname および orclguid など、ディレクトリ内の各エントリの操作属性が含まれます。

# カタログ管理ツールの構文

Oracle Internet Directory では、索引を使用して属性を検索できます。Oracle Internet Directory のインストール時に、エントリ cn=catalogs に、検索で使用できる属性がリストされます。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。Oracle Directory Manager を使用して属性を作成するときに追加できます。しかし、その属性がすでに存在している場合は、カタログ管理ツールの使用によってのみ索引付けできます。

カタログ管理ツールを実行する前に、LANG 変数の設定を解除してください。カタログ管理ツールの実行終了後、LANG 変数を元の値に設定してください。

LANG の設定を解除する方法は、次のとおりです。

- Korn シェルを使用している場合

```
unset LANG
```

- C シェルを使用している場合

```
unsetenv LANG
```

カタログ管理ツールは次の構文を使用します。

```
catalog.sh -connect net_service_name {add|delete} {-attr attr_name|-file filename}
```

必須の引数	説明
-connect net_service_name	ディレクトリ・データベースに接続するためのネット・サービス名を指定します。
関連項目：『Oracle8i Net8 管理者ガイド』	

オプションの引数	説明
-add -attr attr_name	指定した属性を索引付けします。
-delete -attr attr_name	指定した属性から索引を削除します。
-add -file filename	指定したファイル内の属性（1 行に 1 つずつ）を索引付けします。
-delete -file filename	指定したファイル内の属性から索引を削除します。

catalog.sh コマンドを入力すると、次のメッセージが表示されます。

```
This tool can only be executed if you know the OiD user password.
Enter OiD password:
```

正しいパスワードを入力すると、コマンドが実行されます。パスワードに誤りがあると、次のメッセージが表示されます。

```
Cannot execute this tool
```

カタログ管理ツールの実行終了後、LANG 変数を元の値に設定してください。

LANG を設定する方法は、次のとおりです。

- Korn シェルを使用している場合

```
SET LANG=appropriate_language; EXPORT LANG
```

- C シェルを使用している場合

```
SETENV LANG appropriate_language
```

カタログ管理ツールの実行後にその変更内容を有効にするには、Oracle Directory Server を停止して再起動してください。

**関連項目：** Directory Server の起動と再起動については、[第 5 章「Oracle Directory Server の管理」](#)を参照してください。

## OID モニターの構文

この項では、次の項目について説明します。

- [OID モニターの開始](#)
- [OID モニターの停止](#)

## OID モニターの開始

OID モニターを開始する手順は、次のとおりです。

1. 次の環境変数を適切な言語設定に設定します。インストール時のデフォルトの言語設定は、AMERICAN\_AMERICA です。

```
NLS_LANG=APPROPRIATE_LANGUAGE.UTF8
```

2. コマンド・プロンプトで、次のコマンドを入力します。

```
oidmon [connect=net_service_name] [sleep=seconds] start
```



引数	説明
<code>connect=net_service_name</code>	接続するデータベースのネット・サービス名を指定します。 <code>tnsnames.ora</code> ファイルに設定されているネットワーク・サービス名です。この引数はオプションです。
<code>sleep=seconds</code>	OID モニターが、OID 制御ユーティリティからの新規要求および停止している可能性があるサーバーの再起動要求をチェックするまでの秒数を指定します。デフォルトのスリープ・タイムは 10 秒です。この引数はオプションです。
<code>start</code>	OID モニター・プロセスを開始します。

次のようなコマンドを実行します。

```
oidmon connect=dbsl sleep=10 start
```

## OID モニターの停止

OID モニター・デーモンを停止するには、コマンド・プロンプトで次のコマンドを入力します。

```
oidmon [connect=net_service_name] stop
```

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

次のようなコマンドを実行します。

```
oidmon connect=dbsl stop
```

# OID 制御ユーティリティの構文

**注意：** Directory Server インスタンスを起動、停止または再起動するときは、常に OID モニターが実行中である必要があります。

この項では、次の項目について説明します。

- [Oracle Directory Server インスタンスの起動と停止](#)
- [Oracle Directory Replication Server インスタンスの起動と停止](#)
- [Directory Server インスタンスの再起動](#)
- [Directory Server インスタンスの起動に関するトラブルシューティング](#)

## Oracle Directory Server インスタンスの起動と停止

[OID 制御ユーティリティ](#)を使用して、Oracle Directory Server インスタンスの起動と停止を行います。

### Oracle Directory Server インスタンスの起動

Oracle Directory Server インスタンスを起動する構文は、次のとおりです。

```
oidctl connect=net_service_name server=oidldapd instance=server_instance_number
[configset=configset_number] [flags=' -p port_number -work maximum_number_of_worker_
threads_per_server -debug debug_level -l change-logging -server n'] start
```

引数	説明
connect	すでに tnsnames.ora ファイルを構成している場合は、ORACLE_HOME/network/admin にある、そのファイルに指定されているネット・サービス名です。
server	起動するサーバーの種類（有効な値は OIDLDAPD と OIDREPLD です）。大文字と小文字は区別されません。
instance	起動するサーバーのインスタンス番号。0 ～ 1000 の間の数値を設定してください。
configset	サーバーの起動に使用される configset の番号。未設定の場合は、デフォルトで configset0 に設定されます。0 ～ 1000 の間の数値を設定してください。
-p	サーバー・インスタンス起動中のポート番号を指定します。未設定の場合、デフォルト・ポートは 389 です。
-work	このサーバーのワーカー・スレッドの最大数を指定します。

引数	説明
-debug	Oracle Directory Server インスタンス起動中のデバッグ・レベルを指定します。
-l	レプリケーションの変更ログを記録するかどうかを設定します。記録しない場合は -l を入力し、記録する場合はこのフラグを省略します。デフォルトは TRUE（値は TRUE と FALSE）です。（Directory Server のみ）
-server	このポートで起動するサーバー・プロセスの数を指定します。
start	server 引数で指定したサーバーを起動します。

たとえば、ネット・サービス名が dba1 で、configset5 を使用し、ポート 12000、デバッグ・レベル 1024、インスタンス番号 3、変更ログ記録なしで Oracle Directory Server インスタンスを起動するには、コマンド・プロンプトで次のように入力します。

```
oidctl connect=dba1 server=oidldapd instance=3 configset=5 flags='-p 12000
-debug 1024 -l ' start
```

Oracle Directory Server インスタンスの起動と停止では、サーバー名とインスタンス番号が必須です。その他の引数はすべてオプションです。

フラグ引数内のペアのキーワード値はすべて、その間を 1 つの空白で区切る必要があります。

フラグは引用符で囲む必要があります。

configset 識別子が未設定の場合は、デフォルトで 0（configset0）に設定されます。

---

**注意：** デフォルト・ポート（無保護使用の場合は 389、保護使用の場合は 636）以外のポートを使用する場合は、Oracle Internet Directory の配置に使用するポートをクライアントに通知する必要があります。デフォルト・ポートを使用する場合、クライアントは、接続要求でポートを参照せずに Oracle Internet Directory に接続できます。

---

## Oracle Directory Server インスタンスの停止

コマンド・プロンプトで、次のコマンドを入力します。

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

次のようなコマンドを実行します。

```
oidctl connect=dba1 server=oidldapd instance=3 stop
```

## Oracle Directory Replication Server インスタンスの起動と停止

OID 制御ユーティリティを使用して、Oracle Directory Replication Server インスタンスの起動と停止を行います。

### Oracle Directory Replication Server インスタンスの起動

Oracle Directory Replication Server を起動する構文は、次のとおりです。

```
oidctl connect=net_service_name server=oidrepld instance=server_instance_number
[configset=configset_number] flags=' -h hostname -p port_number
-d debug_level -z transaction_size ' start
```

引数	説明
connect	すでに tnsnames.ora ファイルを構成している場合は、ORACLE_HOME/network/admin にある、そのファイルに指定されている名前です。
server	起動するサーバーの種類（有効な値は OIDLDAPD と OIDREPLD です）。大文字と小文字は区別されません。
instance	起動するサーバーのインスタンス番号。0 ～ 1000 の間の数値を設定してください。
configset	サーバーの起動に使用される configset の番号。未設定の場合は、デフォルトで configset0 に設定されます。0 ～ 1000 の間の数値を設定してください。
-p	サーバー・インスタンス起動中のポート番号を指定します。未設定の場合、デフォルト・ポートは 389 です。
-d	Replication Server インスタンス起動中のデバッグ・レベルを指定します。
-h	サーバーを実行するホスト名を指定します。（Replication Server のみ）
-m [true false]	競合の解消を行うかどうかを設定します。デフォルトは TRUE（値は TRUE と FALSE）です。（Replication Server のみ）
-z	各レプリケーション更新サイクルで適用される変更の数を指定します。指定しない場合は、Oracle Directory Server の sizelimit パラメータの値で決まります。sizelimit パラメータのデフォルト設定は 1024 です。この設定は変更できます。
start	server 引数で指定したサーバーを起動します。

たとえば、インスタンスが 1、ポート 12000、デバッグ・レベル 1024 で Replication Server を起動するには、コマンド・プロンプトで次のように入力します。

```
oidctl connect=dbs1 server=oidrepld instance=1 flags='-p 12000 -h eastsun11 -d 1024' start
```

Oracle Directory Replication Server の起動と停止では、`-h` フラグ（ホスト名を指定する引数）が必須です。その他のフラグはすべてオプションです。

フラグ引数内のペアのキーワード値はすべて、その間を 1 つの空白で区切る必要があります。

フラグは引用符で囲む必要があります。

`configset` 識別子が未設定の場合は、デフォルトで 0 (`configset0`) に設定されます。

---

**注意：** デフォルト・ポート（無保護使用の場合は 389、保護使用の場合は 636）以外のポートを使用する場合は、Oracle Internet Directory の配置に使用するポートをクライアントに通知する必要があります。デフォルト・ポートを使用する場合、クライアントは、接続要求でポートを参照せずに Oracle Internet Directory に接続できます。

---

## Oracle Directory Replication Server インスタンスの停止

コマンド・プロンプトで、次のコマンドを入力します。

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

次のようなコマンドを実行します。

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

## Directory Server インスタンスの再起動

Directory Server インスタンスを再起動するには、コマンド・プロンプトで次のコマンドを入力します。

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

Directory Server インスタンスを起動、停止または再起動するときは、常に OID モニターが実行中であることが必要です。

ダウンしているサーバーに接続しようとすると、SDK からエラー・メッセージ「81: LDAP サーバーと通信できません。」を受け取ります。

アクティブなサーバー・インスタンスが参照している構成設定エントリを変更する場合、構成設定エントリの変更値をそのサーバー・インスタンスで有効にするには、そのインスタン

スを停止して、再起動してください。STOP コマンドと START コマンドを続けて発行するか、RESTART コマンドを使用します。RESTART は、サーバー・インスタンスを停止して、再起動します。

たとえば、Oracle Directory Server の instance1 が、configset3 を使用してネット・サービス名 dbs1 で起動されたとします。その後、instance1 の稼働中に、configset3 内の属性の 1 つを変更したとします。configset3 の変更内容を instance1 で有効にするには、次のコマンドを入力します。

```
oidctl connect=dbs1 server=oidldapd instance=1 restart
```

configset3 を使用する Oracle Directory Server のインスタンスが、そのノードで複数実行中の場合は、次のコマンド構文を使用して、すべてのインスタンスを一度に再起動できます。

```
oidctl connect=dbs1 server=oidldapd restart
```

このコマンドは、configset3 を使用しているかどうかに関係なく、そのノードで実行中のインスタンスをすべて再起動することに注意してください。

---

---

**重要：** 再起動を実行中、クライアントは Oracle Directory Server インスタンスにアクセスできません。ただし、再起動にかかる時間は数秒です。

---

---

## Directory Server インスタンスの起動に関するトラブルシューティング

Directory Server が起動に失敗した場合は、Directory Server を起動するためにユーザー指定の構成パラメータをすべてオーバーライドし、サーバー起動後に ldapmodify 操作を使用して、構成設定を使用可能な状態に戻すことができます。

ディレクトリに格納されている構成パラメータのかわりに、ハードコードされたデフォルト・パラメータを使用して Directory Server を起動するには、コマンド・プロンプトで次のコマンドを入力します。

```
oidctl connect=net_service_name flags='-p port_number -f'
```

フラグ内に -f オプションを指定すると、定義済みの構成設定が configset0 内の値を除いてすべてオーバーライドされ、ハードコードされた構成値でサーバーが起動されます。

## OID データベース・パスワード・ユーティリティの構文

OID データベース・パスワード・ユーティリティの構文は、次のとおりです。

```
oidpasswd [connect=net_service_name]
```

OID データベース・パスワード・ユーティリティは、現行のパスワードの入力を要求します。現行のパスワードの次に新規パスワードを入力し、続いて確認のため新規パスワードを再入力します。

OID データベース・パスワード・ユーティリティは、変更されるパスワードはローカル・データベース（`ORACLE_HOME` と `ORACLE_SID` で定義）のものであるとデフォルトでみなされています。リモート・データベースのパスワードを変更する場合は、`connect=net_service_name` オプションを使用する必要があります。

次のようなコマンドを実行します。

```
$ oidpasswd
current password: ods
new password: newsupersecret
confirm password: newsupersecret
password set.$
```

---

---

**注意：** ユーザーの入力値は画面に表示されません。

---

---

## OID データベース統計収集ツールの構文

様々なデータベース `ods` スキーマ・オブジェクトを分析して統計を見積るために、`$ORACLE_HOME/ldap/admin/oidstats.sh` ツールが提供されています。

### 構文

```
oidstats.sh [ -connect database_connect_string ]
             [ -login database_account_login ]
             [ -pass database_account_password ]
             [ -all ]
             [ -cat catalog_name ]
             [ -pct percent ]
             [ -help | -usage ]
```

パラメータ

パラメータ	説明	デフォルト
connect	DB 接続文字列	ORACLE_SID
login	DB ユーザー名	ods
pass	DB アカウントのパスワード	ods
all	すべてのカタログ表と DN カタログに関する統計の見積り	すべてのカタログ
cat	すべてのカタログ（all）または特定のカタログ（例：ct_cn）に関する統計の見積り	なし
pct	サンプルとして抽出するデータの割合（パーセント）	100

例：OID データベース統計収集ツールの使用方法

次の各例では、ORACLE\_SID とデフォルトのユーザー名およびパスワードが有効であるとみなします。

この例では、すべての表の 100% のサンプル・データに基づいて統計を見積ります。

```
oidstats.sh -all -pct 100
```

この例では、すべての表の 50% のサンプル・データに基づいて統計を見積ります。

```
oidstats.sh -all -pct 50
```

この例では、CT\_CN 表の 50% のサンプル・データに基づいて統計を見積ります。

```
oidstats.sh -cat ct_cn -pct 50
```

この例では、カタログ表の 40% のサンプル・データに基づいて統計を見積ります。

```
oidstats.sh -cat all -pct 40
```



---

# データベース・コピー・プロシージャを使用した DSA の追加

この付録では、データベース・コピー・プロシージャ（**コールド・バックアップ**とも呼ばれます）を使用して、既存のレプリケート・システムに新しい **DSA** を追加する方法を説明します。

---

**注意：** このプロシージャには、Oracle のデータ・ファイルをコピーする処理が含まれているため、パフォーマンスは基礎となるネットワークに依存します。基礎となるネットワークが弱い場合は、[第 10 章「ディレクトリ・レプリケーションの管理」](#)に記載されている方法を実施するか、またはテープやディスクなどのメディアに、圧縮した Oracle データ・ファイルを物理的にコピーする方法をお薦めします。ネットワークに関する詳細は、ローカル・システムの管理者またはネットワーク管理者に相談してください。

このプロシージャは、Oracle データベースをよく理解している人のみ実施してください。

---

この付録では、次の項目について説明します。

- [前提事項](#)
- [スポンサ・ディレクトリ・サイトの環境](#)
- [新規ディレクトリ・サイトの環境](#)
- [スポンサ・ノードで実行されるタスク](#)
- [新規ノードで実行されるタスク](#)
- [検証プロセス](#)

## 前提事項

このマニュアルは、Optimal Flexible Architecture (OFA) に従って UNIX ディレクトリが作成されていることを前提としています。Optimal Flexible Architecture (OFA) は、効率的で信頼性のある Oracle データベースを構築するための一連の構成ガイドラインです。

**関連項目：** OFA の詳細は、使用しているオペレーティング・システム用の Oracle インストレーション・ガイドを参照してください。

## スポンサ・ディレクトリ・サイトの環境

スポンサ・サイトの環境を設定します。この章で使用される例では、ホスト名は `rst-sun` です。

```
Hostname      = rst-sun
ORACLE_BASE   = /private/oracle/app/oracle
ORACLE_HOME   = /private/oracle/app/oracle/product/8.1.6
ORACLE_SID    = LDAP
LD_LIBRARY_PATH = $ORACLE_HOME/lib
NLS_LANG      = AMERICAN_AMERICA.UTF8
datafile location = /private/oracle/oradata/LDAP
Dump destination = /private1/oracle/app/oracle/admin/LDAP/pfile,
                  /private1/oracle/app/oracle/admin/LDAP/bdump,
                  /private1/oracle/app/oracle/admin/LDAP/cdump,
                  /private1/oracle/app/oracle/admin/LDAP/udump,
                  /private1/oracle/app/oracle/admin/LDAP/create
```

## 新規ディレクトリ・サイトの環境

新規ディレクトリ・サイトの環境を設定します。この章で使用される例では、新規サイトは、`dsm-sun` というノード上にあります。

```
Hostname = dsm-sun
ORACLE_BASE = /private1/oracle/app/oracle
ORACLE_HOME = /private1/oracle/app/oracle/product/8.1.6
ORACLE_SID = NLDAP
LD_LIBRARY_PATH = $ORACLE_HOME/lib
NLS_LANG = AMERICAN_AMERICA.UTF8
datafile location = /private1/oracle/oradata/NLDAP
Dump destination = /private1/oracle/app/oracle/admin/NLDAP/pfile,
                  /private1/oracle/app/oracle/admin/NLDAP/bdump,
                  /private1/oracle/app/oracle/admin/NLDAP/cdump,
                  /private1/oracle/app/oracle/admin/NLDAP/udump,
                  /private1/oracle/app/oracle/admin/NLDAP/create
```

---

**注意：** Oracle データベースまたは Oracle ディレクトリのインストール後、Oracle Database Configuration Assistant を使用して、データ・ファイルのディレクトリを作成します。OFA の定義に従って、様々な UNIX パーティション下の新規ノードに、新規ディレクトリを作成してください。

---

## スポンサ・ノードで実行されるタスク

スポンサ・ノードで次の各ステップを実行します。

1. コマンドライン・プロンプトで、SQL\*Plus を実行します。

```
$ sqlplus
SQL> connect internal
SQL> ALTER DATABASE BACKUP CONTROLFILE TO TRACE;
```

このコマンドは、ユーザー・ダンプ出力先ディレクトリ (/private1/oracle/app/oracle/admin/LDAP/udump) にトレース・ファイルを作成します。

ファイルは次の書式で作成されます。

```
$ORACLE_SID_<ora_processid>.trc
```

次のようなコマンドを実行します。

```
ldap_ora_4765.trc
```

2. LDAP サーバーと Replication Server および OID モニター・プロセスを停止します。OID モニター・プロセスを停止する前に、LDAP サーバーと Replication Server が停止していることを確認してください。

```
$ oidctl connect=<net_service_name> server=oidrepld instance=<inst_#> stop
$ oidctl connect=<net_service_name> server=oidldapd instance=<inst_#> stop
$ oidmon connect=<net_service_name> stop
```

これらのコマンドで、*net\_service\_name* はそのノードの *tnsnames.ora* ファイル内に記述されているネット・サービス名です。

3. その他のノードで、LDAP Replication Server のみ停止します。

```
$ oidctl connect=<net_service_name> server=oidrepld instance=<inst_#> stop
```

スポンサ・ノードを除くすべてのノードで、この手順を繰り返します。対応するノードの適切なネット・サービス名を指定してください。

4. **マスター定義サイト**で次のスクリプトを実行して、**アドバンスド・レプリケーション**を停止します。

```
ldaprepl.sh -quiesce
```

要求された場合は、MDS の Oracle グローバル名を入力します。

---

**注意：** この手順は、マスター定義サイトでのみ実施できます。

---

この時点で、他のノードは LDAP 編集のみ使用可能で、レプリケーションは行われません。

5. 環境の停止後、スポンサ・ノードでのみデータベースと Net8 リスナーを停止します。

```
$ lsnrctl [listener name] stop   (デフォルトのリスナー名は LISTENER です)
$ sqlplus /nolog
SQL> connect / as sysdba
SQL> shutdown normal
SQL> exit
```

6. ステップ 1 で作成されたトレース・ファイルを、同じディレクトリ内の新規ファイル newdb.sql にコピーします。

```
$ cd $ORACLE_BASE/admin/LDAP/udump
$ cp ldap_ora_4765.trc newdb.sql
```

7. テキスト・エディタを使用して newdb.sql を編集し、START NOMOUNT までの行を削除します。

```
CREATE CONTROLFILE REUSE SET DATABASE <database_name> RESETLOG
```

8. データベースやログ・ファイルなどの UNIX ディレクトリの位置を、新規ノードのディレクトリを指すように変更します。次のサンプル・ファイル newdb.sql を参考にしてください。

```
Begin newdb.sql
CREATE CONTROLFILE REUSE SET DATABASE "LDAP" RESETLOGS
MAXLOGFILES 16
MAXLOGMEMBERS 2
MAXDATAFILES 255
MAXINSTANCES 1
MAXLOGHISTORY 100
LOGFILE
GROUP 1 '/private2/oracle/oradata/NLDAP1/log1_NLDAP.dbf'   SIZE 1M,
GROUP 2 '/private2/oracle/oradata/NLDAP1/log2_NLDAP.dbf'   SIZE 1M
```

```

DATAFILE
'/private2/oracle/oradata/NLDAP1/sys0_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/rbs1_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/attrs1_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/dncat1_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/cncat1_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/objcl1_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/cats1_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/default1_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/temp1_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/iattrs1_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/idncat1_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/icncat1_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/iobjcl1_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/icats1_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/temp2_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/cats2_NLDAP.dbf',
'/private2/oracle/oradata/NLDAP1/attrs2_NLDAP.dbf'
;
End newdb.sql

```

9. \$ORACLE\_HOME/dbs の initLDAP.ora ファイルと configLDAP.ora ファイルを、それぞれ initNLDAP.ora と configNLDAP.ora にコピーします。

```

$cd $ORACLE_HOME/dbs
$cp initLDAP.ora initNLDAP.ora
$cp configLDAP.ora configNLDAP.ora

```

10. コピーしたファイル (initNLDAP.ora) を編集し、パラメータ JOB\_QUEUE\_PROCESS をコメント化します。次のパラメータを変更します。

```

db_name = LDAP      (ファイル initNLDAP.ora にパラメーターが存在しない場合、ファイル
configNLDAP.ora を変更します)
ifile = UNIX_directory_location_of_the_new_config_file/ configNLDAP.ora

```

11. コピーしたファイル configNLDAP.ora を編集し、次のパラメータを変更します。

```

cdump = UNIX_directory_location_of_the_new_node
udump = UNIX_directory_location_of_the_new_node
bdump = UNIX_directory_location_of_the_new_node
control_files = UNIX_directory_location_of_the_new_node

```

12. tnsnames.ora ファイルを編集して、新規ノードに関連する情報を記述します。次のサンプル・ファイルを参考にしてください。

```

Begin tnsnames.ora

ldap1.world =

```

```

        (description=
          (address=(protocol=tcp) (host=rst-sun) (port=1521))
          (connect_data=(sid=LDAP))
        )
ldap2.world =
  (description=
    (address=(protocol=tcp) (host=eas-sun10) (port=1521))
    (connect_data=(sid=LDAP))
  )
ldap3.world =
  (description=
    (address=(protocol=tcp) (host=dsm-sun) (port=1521))
    (connect_data=(sid=NLDAP))
  )

End tnsnames.ora

```

13. listener.ora ファイルを list.bak にコピーします。コピーしたファイル list.bak を編集して、新規ノードに関連する情報を記述します。次のサンプル・ファイルを参考にしてください。

```

Begin listener.ora

# The KEY value for the IPC protocol may be anything, and
# is not related to either the TCP hostname or database SID.

LISTENER =
  (ADDRESS_LIST =
    (ADDRESS= (PROTOCOL= IPC) (KEY= LDAP))
    (ADDRESS= (PROTOCOL= IPC) (KEY= PNPKEY))
    (ADDRESS= (PROTOCOL= TCP) (Host= dsm-sun) (Port= 1521))
  )
SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (GLOBAL_DBNAME= dsm-sun.us.oracle.com)
      (ORACLE_HOME= /private1/oracle/app/oracle/product/8.1.6)
      (SID_NAME = NLDAP)
    )
    (SID_DESC =
      (SID_NAME = extproc)
      (ORACLE_HOME = /private1/oracle/app/oracle/product/8.1.6)
      (PROGRAM = extproc)
    )
  )
STARTUP_WAIT_TIME_LISTENER = 0
CONNECT_TIMEOUT_LISTENER = 10

```

```
TRACE_LEVEL_LISTENER = OFF
```

```
End listener.ora
```

tnsnames.ora ファイルと listener.ora ファイルは、  
\$ORACLE\_HOME/network/admin または /var/opt/oracle、あるいは環境変数  
TNS\_ADMIN が指し示すディレクトリ内にあります。

14. 更新した tnsnames.ora ファイルをすべてのノードにコピーします。各ノードの現行の tnsnames.ora の位置にコピーするように注意してください。tnsnames.ora ファイルは、FTP を使用して他のノードにコピーできます。ファイルは、必ず ASCII モードで転送してください。

tnsnames.ora ファイルを新規ノードにコピーする前に、新規ノードに Oracle データベース・ソフトウェアをインストールします。また、listener.ora ファイルのかわりの list.bak ファイルと sqlnet.ora ファイルを、スポンサ・ノードから新規ノードにコピーします。

15. すべてのデータ・ファイルのアーカイブを作成し、アーカイブしたファイルを圧縮します。次のようなコマンドを実行します。

```
$ >oradb.tar
```

このコマンドは、ディレクトリ内に空のファイルを作成します。アーカイブが作成されるパーティションに、十分な領域があることを確認してください。

```
$ find / -name *.dbf -print -exec tar rvf <absolute_path_of_the_directory_which_contains_oradb.tar> {} \;
```

次のようなコマンドは、拡張子が .dbf のすべてのファイルを、ルート・ディレクトリから検索します。ノードにインストールされているデータベース・サーバーのインスタンスが 1 つのみで、データ・ファイルが \*.dbf 拡張子で終わっていることを前提としています。

```
$ find / -name *.log -print -exec tar rvf <absolute_path_of_the_directory_which_contains_oradb.tar>  
$ compress oradb.tar
```

このプロシージャは、ファイルのバックアップ方式を示す 1 つの例です。Oracle データ・ファイルは、この方法で絶対パス内でバックアップされます。データ・ファイルをリストアするときに、柔軟に対応できるように、現行のディレクトリからファイルをバックアップすることをお勧めします。データベースをバックアップする前に、システム管理者と相談してください。

## 新規ノードで実行されるタスク

新規ノードで次の各ステップを実行します。

1. 新規ノード (dsm-sun) にログインします。
2. すべてのデータベース・ノードで、新規インスタンス用に oratab ファイルを適切に編集します。構文はサンプル・ファイルを参照してください。

```
Begin oratab
```

```
NLDAP:/private1/oracle/app/oracle/product/8.1.6:N  
*:/private1/oracle/app/oracle/product/8.1.6:N
```

```
End oratab
```

3. 新規ディレクトリ・サイトに環境変数が設定されていることを確認します。
4. Oracle データベースと Oracle Directory Server をインストールします。Oracle データベースと Oracle Directory Server のインストールのみソフトウェアを実行します。データベース・ファイルが新しいマシンにコピーされる前であれば、いつでも新規ノードで Oracle データベースと Oracle Directory Server のソフトウェアのインストールを実行できます。データベースと Directory Server に、インストール後のアクティビティ (root.sh) を実行してください。

### 関連項目： Oracle8i インストール

新規ノードに Oracle データベースと Oracle Directory Server のインストールがすでに実行されている場合は、ステップ 5 に進んでください。

5. initNLDAP.ora ファイルと configNLDAP.ora ファイルをスポンサ・ノード (rst-sun) から UNIX ディレクトリ \$ORACLE\_BASE/ADMIN/NLDAP/PFILE の新規ノードにコピーします。新規マシンへのファイルのコピーには、FTP などのツールを使用します。転送モードが ASCII であることを確認してください。
6. \$ORACLE\_HOME/DBS から \$ORACLE\_BASE/ADMIN/NLDAP/PFILE へのシンボリック・リンクを作成します。

```
$ ln -s $ORACLE_BASE/admin/NLDAP/pfile/initNLDAP.ora  
$ORACLE_HOME/dbs/initNLDAP.ora  
$ ln -s $ORACLE_BASE/admin/NLDAP/pfile/configNLDAP.ora  
$ORACLE_HOME/dbs/configNLDAP.ora
```



7. スポンサ・ノードの手順で作成したアーカイブ・ファイルを、FTP などのツールを使用してコピーします（このファイルは、B-7 ページのステップ 15 で作成しています）。転送モードをバイナリに設定します。

```
ftp> open rst-sun
Connected to rst-sun.us.oracle.com.
220 rst-sun FTP server (UNIX(r) System V Release 4.0) ready.
Name (rst-sun:oracle):
331 Password required for oracle.
Password:
230 User oracle logged in.
ftp> cd /private1/oracle/oradata/LDAP
250 CWD command successful.
ftp> binary
200 Type set to I.
ftp> mget oradb.tar.Z
```

データ・ファイルが非常に大きく（数 GB または数 TB）、ネットワーク帯域幅が狭い場合は、スポンサ・ノードから新規ノードにコピーするとき、テープやディスクなどのメディアに、圧縮したファイルを物理的にコピーする方法をお勧めします。

8. スポンサ・ノードの設定のステップ 6 で作成した newdb.sql ファイルを、バックグラウンドのユーザー・ダンプ出力先ディレクトリにコピーします。newdb.sql ファイルのみ ASCII モードで転送する必要があります。次のようなコマンドを実行します。

```
$ cd /private1/oracle/app/oracle/admin/NLDAP/udump
      (つまり、$ORACLE_BASE/admin/<SID>/udump です)
$ ftp
ftp> open rst-sun
ftp> cd /private1/oracle/app/oracle/admin/LDAP/udump
ftp> mget newdb.sql
```

9. UNIX シェル・プロンプトで、次のコマンドを実行します。

```
$ sqlplus /nolog
SQL> connect / as sysdba
SQL> startup nomount
SQL> @newdb.sql
SQL> shutdown normal
SQL> startup （開始する前にパラメータ job_queue_process をコメント化しません）
SQL> exit
$ lsnrctl start
```

10. スポンサ・ノードにログインして、スポンサ・ノード（例：rst-sun）でデータベースとリスナーを起動します。

```
$ telnet rst-sun
$ sqlplus /nolog
SQL> connect / as sysdba
SQL> startup
SQL> exit
$ lsnrctl start （デフォルトのリスナー名は LISTENER です）
$ exit
```

11. スポンサ・ノードがマスター・サイトの場合は、ステップ 12 に進んでください。

新規ノードが MDS のバックアップ・データベース・コピーを使用して作成されている場合は、マスター定義カタログを削除して、基礎となるアドバンスト・レプリケーション・カタログを作成する必要があります。新規ノードでアドバンスト・レプリケーション・カタログから MDS の定義を削除してアドバンスト・レプリケーション・カタログを追加するには、次のスクリプトを実行します。

```
$ cd $ORACLE_HOME/ldap/admin
$ sqlplus repadmin/repadmin
SQL> @ldapdropmds.sql
SQL> @ldapcreindex.sql
```

要求された場合は、新規ノードのグローバル名を指定してください。

12. 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。

```
$ ldaprepl.sh -addnode
```

13. LDAP レプリケーション承諾を更新して、新規ノードを組み込みます。

LDIF ファイルのサンプルは次のとおりです。

```
dn: orclagreementid=000001, cn=orclreplagreements
changetype: modify
add: orcldirreplgroupdsas
orcldirreplgroupdsas: dsm-sun
```

14. すべてのノード（新規ノードとスポンサ・ノードを含む）で、LDAP Replication Server を起動します。

## 検証プロセス

SQL\*Plus を使用して Oracle データベースにログインし、ユーザー名 ods を指定し、要求に従ってパスワード ods を指定します。

すべてのノードで ods\_chg\_stat 表をチェックし、同一の正しい行が含まれているかどうかをチェックします。ods\_chg\_stat 表には、(ノード数) × (ノード数) 行が含まれている必要があります。たとえば、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メンバー・ノードが 2 つあり、3 番目のノードを追加した場合、ods\_chg\_stat の行は各ノードで 9 (3 × 3) 行です。各行の内容を次の表で示します。

サプライヤ	コンシューマ	変更番号
ノード 1	ノード 2	< 番号 1>
ノード 1	ノード 3	< 番号 2>
ノード 1	ノード 1	< 番号 3>
ノード 2	ノード 1	< 番号 4>
ノード 2	ノード 2	< 番号 5>
ノード 2	ノード 2	< 番号 6>
ノード 3	ノード 1	0
ノード 3	ノード 2	0
ノード 3	ノード 3	0

コンシューマ名とサプライヤ名が同じ行には、サプライヤ側でアウトバウンド変更ログの処理スレッドが処理した最終変更が含まれています。サプライヤ名とコンシューマ名が異なる行には、サプライヤからそのコンシューマに対して、すでに処理された最終変更番号が含まれています。

ノード 3 は新規ノードであるため、ノード 3 による変更はまだありません。したがって、サプライヤとしてのノード 3 の変更番号は 0 (ゼロ) です。

すべてのノードの行が同一になるまでに時間的な遅延が生じることがありますが、この遅延は 2 ～ 3 分ほどです。



---

# Oracle Wallet Manager の使用方法

セキュリティ管理者は、Oracle Wallet Manager を使用して、Oracle クライアントとサーバーにおける公開鍵のセキュリティ資格証明を管理します。作成された Wallet は、Oracle Enterprise Login Assistant または Oracle Wallet Manager のいずれかを使用してオープンできます。

この章では、Oracle Wallet Manager について次の各項で説明します。

- [概要](#)
- [Wallet の管理](#)
- [証明書の管理](#)

**関連項目：** Oracle Enterprise Login Assistant を使用して保護 SSL 通信の Wallet をオープンおよびクローズする方法については、『Oracle8i Advanced Security 管理者ガイド』を参照してください。

## 概要

従来の秘密鍵または対称鍵暗号化では、保護通信を確立するエンティティとしてお互いのみが知っている単一のシークレット・キーを持つ必要があります。たとえば、Harriet と Dick が、プライベートなメッセージの中の各文字を 2 文字ずらし、メッセージのテキストを暗号化することを取り決めます（A は C, B は D になります）。この方法を使用すると、HELLO という Harriet から Dick へのメッセージは、JGNNQ と読めるようになります。現在使用されている実際の暗号化方式はさらに複雑で厳重に保護されていますが、根本的な問題は残されたままです。つまり、この方法では単一のキーで暗号化されたメッセージを送信する前に、各関係者に安全にキーを配布しておく必要があります。そうでなければ、不正な第三者がキーを取得して、通信を途中で傍受し、セキュリティを危険にさらすことになります。公開鍵暗号では、安全なキーの配布方法を提供することでこの問題に対応しています。

公開鍵暗号では、**公開鍵と秘密鍵のペア**が必要になります。**秘密鍵**は秘密にされており、その関係者のみが知っています。**公開鍵**は、その名前が示すように自由に使用できます。秘密のメッセージを送信する場合、第三者である送信者はメッセージを公開鍵で暗号化する必要があります。暗号化されたメッセージは、対応する秘密鍵を持った関係者のみが復号化できます。

たとえば、Dick が保護メッセージを Harriet に送信するとき、最初に Harriet に公開鍵を教えてください（あるいは、別の公的な情報源から取得します）。Harriet は Dick に自分の公開鍵を教えますが、不正な盗聴者である Tom もその公開鍵を取得します。しかし、Dick が Harriet に公開鍵で暗号化したメッセージを送信しても、Tom はそれを復号化できません。そのメッセージは Harriet の秘密鍵でのみ復号化できます。

公開鍵アルゴリズムは、このようにしてメッセージの秘密性を保証しますが、保護通信は保証しません。公開鍵アルゴリズムでは、通信している相手の識別情報を検証しないからです。保護通信を確立するには、メッセージの暗号化に使用される公開鍵が実際にターゲットとなる受信者のものであることを検証することが重要です。そうしなければ、第三者が通信を盗聴して公開鍵の要求を傍受し、自分の公開鍵を本物の鍵のかわりに使用する可能性があります。

たとえば、Tom が自分の公開鍵を Harriet の公開鍵のかわりに Dick に送信できた場合、Dick は（Harriet の公開鍵を使用しているつもりで）Tom の公開鍵で暗号化したメッセージを Harriet に送信してしまう可能性があります。その場合、Tom は次に傍受した Dick からのメッセージを自分の秘密鍵を使用して復号化し、それを Harriet の公開鍵で再び暗号化して Harriet に再送信できます。Harriet は受信したメッセージを自分の秘密鍵を使用して復号化し、Tom に傍受されたことにまったく気づきません。

このような介入者からの攻撃を回避するには、公開鍵の所有者を検証することが必要です。このプロセスを**認証**と呼びます。この認証は、**認証局**によって実現できます。

認証局とは、保護通信を試みる両方の側から信頼される第三者機関です。認証局は、公開鍵証明書を発行します。公開鍵証明書には、エンティティの名前、公開鍵およびその他のセキュリティ資格証明が含まれています。その資格証明には、一般的に認証局の名前、認証局の署名および証明書の有効期間（開始日付と終了日付）などがあります。

認証局は秘密鍵を使用してメッセージを暗号化し、公開鍵はそれを復号化するために使用されます。このようにして、そのメッセージが認証局によって暗号化されたことが検証されます。認証局の公開鍵は一般に知られており、アクセスのたびに認証する必要はありません。そのような認証局の公開鍵は、**Wallet** に格納されます。

Oracle Wallet Manager はスタンドアロンの Java アプリケーションで、Wallet の所有者が、それぞれの Oracle Wallet におけるセキュリティ資格証明を管理および編集するために使用します。次のようなタスクを実行します。

- 公開鍵と秘密鍵のペアの生成および認証局への証明書発行要求の作成。
- エンティティ用の証明書のインストール。
- エンティティ用の**信頼されている証明書**の構成。
- Wallet のオープン。PKI ベースのサービスへのアクセスを可能にします。
- Wallet の作成。Wallet は、Oracle Enterprise Login Assistant または Oracle Wallet Manager のいずれかを使用してアクセスできます。

## Wallet の管理

この項では、次の各サブセクションで、新規 Wallet の作成方法および関連する Wallet 管理タスク（証明書要求の生成、証明書要求のエクスポート、証明書の Wallet へのインポートなど）の実行方法を説明します。

- **Oracle Wallet Manager の起動**
- **新規 Wallet の作成**
- **既存 Wallet のオープン**
- **Wallet のクローズ**
- **変更の保存**
- **新しい位置へのオープン Wallet の保存**
- **システム・デフォルトへの保存**
- **Wallet の削除**
- **パスワードの変更**
- **自動ログインの使用法**
- **Oracle Application Server での Oracle Wallet Manager の使用法**

## Oracle Wallet Manager の起動

Oracle Wallet Manager を起動する手順は、次のとおりです。

UNIX: コマンドラインで `owm` と入力します。

Windows NT: 「スタート」>「ORACLE\_HOME」>「Network Administration」>「Wallet Manager」の順にクリックします。

## 新規 Wallet の作成

新規 Wallet を作成する手順は、次のとおりです。

1. メニュー・バーから、「Wallet」>「New」の順に選択します。「New Wallet」ダイアログ・ボックスが表示されます。
2. パスワードの作成に関する推奨ガイドラインを読み、「Wallet Password」フィールドにパスワードを入力します。

Oracle Wallet には、複数のデータベースに対してユーザーを認証するために使用される資格証明が含まれているため、Wallet 用には特別安全なパスワードを選択することが特に重要です。別のユーザーの Wallet のパスワードを探し当てた不正なユーザーは、そのユーザーがアクセスできるすべてのデータベースにアクセスすることが可能です。

パスワードは、短すぎず、簡単に推測できず、ある程度複雑なものを使用することをお勧めします。ある程度複雑なパスワードにするには、最低 6 文字で、(辞書で探すことができないように) 記号や数字を少なくとも 1 つ使用する必要があります。

例: `gol8fer`

また、毎月 1 回または 3 か月に 1 回など、定期的にパスワードを変更することをお勧めします。

3. 「Confirm Password」フィールドに同じパスワードを再度入力します。
4. 継続するには「OK」を選択します。
5. 警告が表示され、空の新規 Wallet が作成されたことが通知されます。証明書要求を作成するかどうかを尋ねられます。C-9 ページの「[証明書要求の作成](#)」を参照してください。

「Cancel」を選択すると、Oracle Wallet Manager のメイン・ウィンドウに戻ります。作成した新規 Wallet が左側のウィンドウ・ペインに表示されます。証明書の状態は「Empty」で、Wallet にはそのデフォルトの信頼されている証明書が表示されます。

6. 「Wallet」>「Save In System Default」の順に選択して、新規 Wallet を保存します。

その Wallet をシステム・デフォルトに保存する権限が与えられていない場合は、別の位置に保存できます。

ウィンドウ下部に、Wallet が正常に保存されたことを通知するメッセージが表示されます。



## 既存 Wallet のオープン

ファイル・システム・ディレクトリにすでに存在している Wallet をオープンする手順は、次のとおりです。

1. メニュー・バーから、「Wallet」 > 「Open」の順に選択します。「Select Directory」ダイアログ・ボックスが表示されます。
2. Wallet が格納されているディレクトリ位置に移動し、ディレクトリを選択します。
3. 「OK」を選択します。「Open Wallet」ダイアログ・ボックスが表示されます。
4. 「Wallet Password」フィールドに Wallet のパスワードを入力します。
5. 「OK」を選択します。
6. 「Wallet opened successfully」というメッセージがウィンドウ下部に表示され、Oracle Wallet Manager のメイン・ウィンドウに戻ります。Wallet の証明書とその信頼されている証明書が、左側のウィンドウ・ペインに表示されます。

## Wallet のクローズ

現在選択しているディレクトリのオープン Wallet をクローズする手順は、次のとおりです。

- 「Wallet」 > 「Close」の順に選択します。
- 「Wallet closed successfully」というメッセージがウィンドウ下部に表示され、Wallet がクローズされたことを通知します。

## 変更の保存

現行のオープン Wallet に加えた変更を保存する手順は、次のとおりです。

- 「Wallet」 > 「Save」の順に選択します。
- ウィンドウ下部に、変更内容が選択したディレクトリ位置にある Wallet に正常に保存されたことを通知するメッセージが表示されます。

## 新しい位置へのオープン Wallet の保存

現行のオープン Wallet を新しいディレクトリ位置に保存するには、「Save As」オプションを使用します。

1. 「Wallet」> 「Save As」の順に選択します。「Select Directory」ダイアログ・ボックスが表示されます。
2. Wallet を保存するディレクトリ位置を選択します。
3. 「OK」を選択します。

選択したディレクトリ内に Wallet がすでに存在している場合は、次のメッセージが表示されます。

「A wallet already exists in the selected path. Do you want to overwrite it?」

既存の Wallet を上書きする場合は「Yes」、Wallet を別のディレクトリに保存する場合は「No」を選択してください。

ウィンドウ下部に、Wallet が選択したディレクトリ位置に正常に保存されたことを通知するメッセージが表示されます。

## システム・デフォルトへの保存

現行のオープン Wallet をシステム・デフォルト・ディレクトリ位置に保存するには、「Save in System Default」メニュー・オプションを使用します。この位置に保存すると、現行のオープン Wallet を SSL で使用される Wallet にできます。

- 「Wallet」> 「Save in System Default」の順に選択します。
- ウィンドウ下部に、Wallet がシステム・デフォルトの Wallet 位置に正常に保存されたことを通知するメッセージが表示されます。

## Wallet の削除

現行のオープン Wallet を削除する手順は、次のとおりです。

1. 「Wallet」> 「Delete」の順に選択します。「Delete Wallet」ダイアログ・ボックスが表示されます。
2. 表示されている Wallet 位置を確認して、削除する Wallet が正しいことを検証します。
3. Wallet のパスワードを入力します。
4. 「OK」を選択します。Wallet が正常に削除されたことを通知するダイアログ・パネルが表示されます。

---

---

**注意：** アプリケーション・メモリー内のオープン Wallet は、そのアプリケーションを終了するまでメモリー内に残ります。このため、現在使用中の Wallet を削除しても、システム操作にはすぐには影響しません。

---

---

## パスワードの変更

パスワードを変更すると、すぐに有効になります。Wallet は、現在選択されているディレクトリに、暗号化された新規パスワードで保存されます。現行のオープン Wallet のパスワードを変更する手順は、次のとおりです。

1. 「Wallet」> 「Change Password」の順に選択します。「Change Wallet Password」ダイアログ・ボックスが表示されます。
2. Wallet の既存のパスワードを入力します。
3. 新しいパスワードを入力します。
4. 新しいパスワードを再度入力します。
5. 「OK」を選択します。

ウィンドウ下部に、パスワードが正常に変更されたことを通知するメッセージが表示されます。

## 自動ログインの使用方法

Oracle Wallet Manager の自動ログイン機能は、Wallet のコピーをオープンして、保護サービスへの PKI ベースのアクセスを可能にします。これは、指定されたディレクトリの Wallet がメモリー内でオープン状態のときに可能です。

複数の Oracle データベースへの Single Sign-on アクセスを行うには、自動ログインを有効にする必要があります。

### 自動ログインの有効化

自動ログインを有効化する手順は、次のとおりです。

1. メニュー・バーから「Wallet」を選択します。
2. 「Auto Login」メニュー項目の横のチェック・ボックスを選択します。ウィンドウ下部に、「Autologin enabled」というメッセージが表示されます。

### 自動ログインの無効化

自動ログインを無効化する手順は、次のとおりです。

1. メニュー・バーから「Wallet」を選択します。
2. 「Auto Login」メニュー項目の横のチェック・ボックスを選択します。ウィンドウ下部に、「Autologin disabled」というメッセージが表示されます。

## Oracle Application Server での Oracle Wallet Manager の使用方法

Oracle Application Server (OAS) を使用するときには、Oracle Wallet Manager を 1 次ノードとマルチノード構成の各リモート・ノードにインストールする必要があります。各ノードにインストールした後、1 次ノードから各リモート・ノードに Wallet をコピーする必要があります。

## 証明書の管理

Oracle Wallet Manager は、ユーザー証明書と信頼されている証明書の 2 種類の証明書を使用します。この項では、次のサブセクションで、両方の種類の証明書を管理する方法を説明します。

- [ユーザー証明書の管理](#)
- [信頼されている証明書の管理](#)

---

**注意：** 最初に認証局からの信頼されている証明書をインストールする必要があります。その後、その認証局が発行するユーザー証明書をインストールできます。新規 Wallet の作成時に、信頼されている証明書がいくつかデフォルトでインストールされています。

---

## ユーザー証明書の管理

ユーザー証明書の管理には、次の作業が含まれます。

- [証明書要求の作成](#)
- [ユーザーの証明書要求のエクスポート](#)
- [ユーザー証明書の Wallet へのインポート](#)
- [ユーザー証明書の Wallet からの削除](#)

## 証明書要求の作成

実際の証明書要求は、Wallet の一部になります。証明書要求は、新しい証明書を取得するために再利用できます。ただし、既存の証明書要求は編集できません。正しく記述された証明書要求のみ Wallet に格納してください。

PKCS #10 証明書要求を作成する手順は、次のとおりです。

1. 「Operations」 > 「Create Certificate Request」の順に選択します。「Create Certificate Request」ダイアログ・ボックスが表示されます。
2. 次の情報（表 C-1）を入力します。

**表 C-1 証明書要求：フィールドと説明**

フィールド名	説明
Common Name	必須。ユーザーまたはサービスのアイデンティティの名前を入力します。ユーザーの名前は、名（First name） / 姓（Last name）の形式で入力してください。
Organizational Unit	オプション。アイデンティティの組織単位の名前を入力します。 例：Finance
Organization	オプション。アイデンティティの組織の名前を入力します。 例：XYZ Corp
Locality/City	オプション。アイデンティティの所在地域または市区町村の名前を入力します。
State/Province	オプション。アイデンティティの所在州または都道府県の完全な名前を入力します。  州名は省略せずに入力してください。これは、2 文字の略称を受け入れない認証局があるためです。
Country	必須。ドロップ・ダウン・リストを選択して、国の略称を表示します。組織が置かれている国を選択します。
Key Size	必須。ドロップ・ダウン・ボックスを選択して、公開鍵と秘密鍵のペアの作成時に使用するキー・サイズのリストを表示します。
Advanced	オプション。「Advanced」を選択して、「Advanced Certificate Request」ダイアログ・パネルを表示します。このフィールドを使用して、アイデンティティの識別名（DN）を編集またはカスタマイズします。たとえば、完全な州名および地域を編集できます。

3. 「OK」を選択します。「Oracle Wallet Manager」ダイアログ・ボックスで、証明書要求が正常に作成されたことが通知されます。このダイアログ・パネルの本文から証明書要求のテキストをコピーして、認証局に送信するために電子メール・メッセージにペーストするか、または証明書要求をファイルにエクスポートできます。

4. 「OK」を選択します。Oracle Wallet Manager のメイン・ウィンドウに戻ります。証明書の状態が「Requested」に変更されます。

### ユーザーの証明書要求のエクスポート

証明書要求をエクスポートする場合は、ファイル・システム・ディレクトリに証明書要求を保存します。

1. メニュー・バーから、「Operations」>「Export Certificate Request」の順に選択します。「Export Certificate Request」ダイアログ・ボックスが表示されます。
2. 証明書要求を保存するファイル・システム・ディレクトリを入力するか、または「Folders」の下のディレクトリ構造に移動します。
3. 「Enter File Name」フィールドにファイル名を入力して、証明書要求を保存します。
4. 「OK」を選択します。ウィンドウ下部に、証明書要求がファイルに正常にエクスポートされたことを通知するメッセージが表示されます。Oracle Wallet Manager のメイン・ウィンドウに戻ります。

### ユーザー証明書の Wallet へのインポート

ユーザーは、証明書要求が完了したことを知らせる電子メール通知を認証局から受け取ります。証明書を Wallet にインポートするには、認証局から受信した電子メールから証明書をコピーしてペーストする方法とファイルからユーザー証明書をインポートする方法があります。

#### 証明書のペースト

証明書をペーストする手順は、次のとおりです。

1. 認証局から受信した電子メール・メッセージまたはファイルから証明書のテキストをコピーします。「Begin Certificate」と「End Certificate」の間の行をコピーしてください。
2. メニュー・バーから、「Operations」>「Import User Certificate」の順に選択します。「Import Certificate」ダイアログ・ボックスが表示されます。
3. 「Paste the Certificate」ボタンを選択し、「OK」を選択します。「Import Certificate」ダイアログ・ボックスが、次のメッセージとともに表示されます。  
「Please provide a base64 format certificate and paste it below.」
4. ダイアログ・ボックスに証明書をペーストして、「OK」を選択します。ウィンドウ下部に、証明書が正常にインストールされたことを通知するメッセージが表示されます。Oracle Wallet Manager のメイン・パネルに戻ります。Wallet の状態は「Ready」に変更されます。

### 証明書を含んだファイルの選択

ファイルを選択する手順は、次のとおりです。

1. メニュー・バーから「Operations」>「Import User Certificate」の順に選択します。
2. 「Select a file... certificate」ボタンを選択して、「OK」を選択します。「Import Certificate」ダイアログ・ボックスが表示されます。
3. 証明書の位置のパスまたはフォルダ名を入力します。
4. 証明書ファイルの名前（例：cert.txt）を選択します。
5. 「OK」を選択します。ウィンドウ下部に、証明書が正常にインストールされたことを通知するメッセージが表示されます。Oracle Wallet Manager のメイン・パネルに戻ります。Wallet の状態は「Ready」に変更されます。

### ユーザー証明書の Wallet からの削除

1. 「Operations」>「Remove User Certificate」の順に選択します。Wallet からユーザー証明書を削除することを確認するダイアログ・パネルが表示されます。
2. 「Yes」を選択します。Oracle Wallet Manager のメイン・パネルに戻ります。証明書は「Requested」の状態が表示されます。

## 信頼されている証明書の管理

信頼されている証明書の管理には、次の作業が含まれます。

- [信頼されている証明書のインポート](#)
- [信頼されている証明書の削除](#)
- [信頼されている証明書のエクスポート](#)
- [信頼されている全証明書のエクスポート](#)
- [Wallet のエクスポート](#)

## 信頼されている証明書のインポート

信頼されている証明書を Wallet にインポートするには、認証局から受信した電子メールからペーストする方法とファイルからインポートする方法があります。

Oracle Wallet Manager では、新規 Wallet の作成時に、VeriSign、RSA および GTE CyberTrust Entrust からの信頼されている証明書が自動的にインストールされます。

**信頼されている証明書のペースト** 信頼されている証明書をペーストする手順は、次のとおりです。

1. メニュー・バーから、「Operations」> 「Import Trusted Certificate」の順に選択します。「Import Trusted Certificate」ダイアログ・パネルが表示されます。
2. 「Paste the Certificate」ボタンを選択し、「OK」を選択します。「Import Trusted Certificate」ダイアログ・パネルが、次のメッセージとともに表示されます。  
「Please provide a base64 format certificate and paste it below.」
3. 受信した電子メール・メッセージの本文から信頼されている証明書をコピーします。この電子メールには、ユーザー証明書が含まれています。「Begin Certificate」と「End Certificate」の間の行をコピーしてください。
4. 証明書をウィンドウにペーストして、「OK」を選択します。ウィンドウ下部に、信頼されている証明書が正常にインストールされたことを通知するメッセージが表示されます。
5. 「OK」を選択します。Oracle Wallet Manager のメイン・パネルに戻ります。信頼されている証明書は、Trusted Certificates ツリーの下に表示されます。

## 信頼されている証明書を含んだファイルの選択

ファイルを選択する手順は、次のとおりです。

1. メニュー・バーから「Operations」> 「Import Trusted Certificate」の順に選択します。「Import Trusted Certificate」ダイアログ・パネルが表示されます。
2. 信頼されている証明書の位置のパスまたはフォルダ名を入力します。
3. 信頼されている証明書ファイルの名前（例：cert.txt）を選択します。
4. 「OK」を選択します。ウィンドウ下部のメッセージで、信頼されている証明書が Wallet に正常にインポートされたことが通知されます。
5. 「OK」を選択して、ダイアログ・パネルを終了します。Oracle Wallet Manager のメイン・パネルに戻ります。信頼されている証明書は、Trusted Certificates ツリーの下に表示されます。



## 信頼されている証明書の削除

信頼されている証明書を Wallet から削除する手順は、次のとおりです。

1. Trusted Certificates ツリーにリストされている信頼されている証明書を選択します。
2. メニュー・バーから「Operations」> 「Remove Trusted Certificate」の順に選択します。  
ダイアログ・パネルによって、署名に使用されている信頼されている証明書を削除すると、ユーザー証明書をその受信者が検証できなくなることが警告されます。
3. 「Yes」を選択します。選択した信頼されている証明書が、Trusted Certificates ツリーから削除されます。

---

**注意：** 信頼されている証明書を Wallet から削除すると、その信頼されている証明書で署名されている証明書はそれ以降検証できなくなります。

また、Wallet にまだ存在しているユーザー証明書の署名に使用されている信頼されている証明書は削除できません。このような信頼されている証明書を削除するには、その証明書が署名している証明書を先に削除する必要があります。

---

## 信頼されている証明書のエクスポート

信頼されている証明書を別のファイル・システム位置にエクスポートする手順は、次のとおりです。

1. 「Operations」> 「Export Trusted Certificate」の順に選択します。「Export Trusted Certificate」ダイアログ・ボックスが表示されます。
2. 信頼されている証明書を保存するファイル・システム・ディレクトリを選択するか、または「Browse」を選択してディレクトリ構造を表示します。
3. ファイル名を入力して、信頼されている証明書を保存します。
4. 「OK」を選択します。Oracle Wallet Manager のメイン・ウィンドウに戻ります。

## 信頼されている全証明書のエクスポート

すべての信頼されている証明書を別のファイル・システム位置にエクスポートする手順は、次のとおりです。

1. 「Operations」> 「Export All Trusted Certificates」の順に選択します。「Export Trusted Certificate」ダイアログ・ボックスが表示されます。
2. 信頼されている証明書を保存するファイル・システム・ディレクトリを選択するか、または「Browse」を選択してディレクトリ構造を表示します。

- 3. ファイル名を入力して、信頼されている証明書を保存します。
- 4. 「OK」を選択します。Oracle Wallet Manager のメイン・ウィンドウに戻ります。

Wallet のエクスポート

Wallet をテキストベースの PKI フォーマットにエクスポートします。個々のコンポーネントは、次の規格に準じてフォーマットされます (表 C-2)。

表 C-2 PKI Wallet エンコーディング規格

コンポーネント	エンコーディング規格
証明連鎖	X509v3
信頼されている証明書	X509v3
秘密鍵	PKCS5

---

# アクセス制御ディレクティブ書式の使用方法

この付録では、[アクセス制御項目](#)の書式（構文）について説明します。

この付録では、次の項目について説明します。

- [orclACI](#) のスキーマ
- [orclEntryLevelACI](#) のスキーマ

## orclACI のスキーマ

ユーザー属性 orclACI で定義されているアクセス制御ディレクティブのスキーマは、次のとおりです。

```
OrclACI:
{ object_identifier NAME 'orclACI' DESC 'Stores an inheritable ACI' EQUALITY
accessDirectiveMatch SYNTAX 'accessDirectiveDescription' USAGE
'directoryOperation' }
```

accessDirectiveDescription をバックスラッシュ正規形で記述すると、次のようになります。

```
<accessDirectiveDescription>
    ::= access to <object> [by <subject> ( <accessList> ) ]+

<object> ::= [attr <EQ-OR-NEQ> (<attrList>) | entry] [filter=(<ldapFilter>)]

<subject> ::= <entity> [<BindMode>]

<entity> ::= * | self | dn="<regex>" | dnAttr=(<dn_attribute>) | group="<dn>"

<BindMode> ::= | BindMode = Simple
               | BindMode = SSLNoauth
               | BindMode = SSLOneway
               | BindMode = SSLTwoway

<accessList> ::= <access> | <access>, <accessList>

<access> ::= none | compare | search | browse | read | selfwrite | write | add
            | delete | nocompare | nosearch | nobrowse | noread | noselfwrite | nowrite | noadd |
            nodelete

<attrList> ::= * | <attribute name> | <attribute name>,<attrList>

<EQ-OR-NEQ> ::= = | !=

<regex> ::= <dn> | *,<dn_of_any_subtree_root>
```

---

---

**注意：** 前述の正規表現は、任意の式に合せるためのものではありません。構文で許可されているのは、ワイルド・カードの後にカンマと有効な DN が続く式のみです。<dn\_of\_any\_subtree\_root> で示されている DN 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> )]+
```



---

## スキーマ要素

この付録では、Oracle Internet Directory でサポートされている各種スキーマ要素を簡単に説明します。これらの要素の大部分は、Internet Engineering Task Force (IETF) の ldapext および ASID ワーキング・グループによる定義に従って使用されています。

**関連項目：** 次の URL を参照してください。

- <http://www.ietf.org> (IETF のホームページ)
- <http://www.ietf.org/html.charters/ldapext-charter.html> (ldapext の Charter と LDAP Draft)
- <http://www.ietf.org/html.charters/asid-charter.html> (ASID の Charter と LDAP Draft)
- <http://www.ietf.org/html.charters/ldup-charter.html> (LDUP の Charter と Draft)
- <http://www.iana.org> (Internet Assigned Numbers Authority のホームページ。オブジェクト識別子に関する情報)

この付録では、次の項目について説明します。

- [Oracle Internet Directory で施行されている IETF Requests for Comments \(RFC\)](#)
- [Oracle Internet Directory で施行されている IETF Draft](#)
- [Oracle Internet Directory 専用のスキーマ要素](#)
- [LDAP 構文](#)
- [一致規則](#)

## Oracle Internet Directory で施行されている IETF Requests for Comments (RFC)

Oracle Internet Directory では、Internet Engineering Task Force (IETF) の次の Requests for Comments (RFC) が施行されています。

RFC	タイトル	URL
1777	Lightweight Directory Access Protocol	<a href="http://www.ietf.org/rfc/rfc1777.txt">http://www.ietf.org/rfc/rfc1777.txt</a>
1778	The String Representation of Standard Attribute Syntaxes	<a href="http://www.ietf.org/rfc/rfc1778.txt">http://www.ietf.org/rfc/rfc1778.txt</a>
1779	A String Representation of Distinguished Names	<a href="http://www.ietf.org/rfc/rfc1779.txt">http://www.ietf.org/rfc/rfc1779.txt</a>
1960	A String Representation of LDAP Search Filters	<a href="http://www.ietf.org/rfc/rfc1960">http://www.ietf.org/rfc/rfc1960</a>
2079	Definition of an X.500 Attribute Type and an Object Class to Hold Uniform Resource Identifiers (URIs)	<a href="http://www.ietf.org/rfc/rfc2079.txt">http://www.ietf.org/rfc/rfc2079.txt</a>
2247	Using Domains in LDAP/X.500 Distinguished Names	<a href="http://www.ietf.org/rfc/rfc2247.txt">http://www.ietf.org/rfc/rfc2247.txt</a>
2251	Lightweight Directory Access Protocol (v3)	<a href="http://www.ietf.org/rfc/rfc2251.txt">http://www.ietf.org/rfc/rfc2251.txt</a>
2252	Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions	<a href="http://www.ietf.org/rfc/rfc2252.txt">http://www.ietf.org/rfc/rfc2252.txt</a>
2253	Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names	<a href="http://www.ietf.org/rfc/rfc2253.txt">http://www.ietf.org/rfc/rfc2253.txt</a>
2254	The String Representation of LDAP Search Filters	<a href="http://www.ietf.org/rfc/rfc2254.txt">http://www.ietf.org/rfc/rfc2254.txt</a>
2255	The LDAP URL Format	<a href="http://www.ietf.org/rfc/rfc2255.txt">http://www.ietf.org/rfc/rfc2255.txt</a>
2256	A Summary of the X.500(96) User Schema for use with LDAPv3	<a href="http://www.ietf.org/rfc/rfc2256.txt">http://www.ietf.org/rfc/rfc2256.txt</a>

## Oracle Internet Directory で施行されている IETF Draft

Oracle Internet Directory では、次の 2 つの IETF Draft が施行されています。

IETF "Definition of the inetOrgPerson LDAP Object Class"  
Draft:  
URL: <http://ietf.org/internet-drafts/draft-smith-ldap-inetorgperson-03.txt>

IETF "Referrals and Knowledge References in LDAP Directories"  
Draft:  
URL: <http://www.ietf.org/internet-drafts/draft-ietf-ldapext-knowledge-00.txt>



## Oracle Internet Directory 専用のスキーマ要素

Oracle Internet Directory の専用スキーマには、次のカテゴリの属性とオブジェクト・クラスがあります。

- [アクセス制御](#)
- [レプリケーション](#)
- [Oracle Internet Directory の構成](#)
- [SSL](#)
- [監査ログ](#)
- [構成設定エントリの属性](#)

この他に、Oracle Internet Directory のインストールには、特定の Oracle 製品で Oracle Internet Directory を使用できるようにするスキーマ要素も含まれています。これらのスキーマ要素の詳細は、各 Oracle 製品のドキュメントを参照してください。

### アクセス制御

Attributes      orclEntryLevelACI, orclACI

オブジェクト・クラス      orclPrivilegeGroup

### レプリケーション

Attributes      orclGUID, changeNumber, changeType, changes, orclParentGUID, server, supplier, consumer, orclReplBindDN, orclReplBindPassword, changeLog, changeStatus, orclChangeRetryCount, orclPurgeSchedule, orclDirReplGroupAgreement, orclAgreementId, orclSupplierReference, orclConsumerReference, orclReplicationProtocol, orclUpdateSchedule, targetDN, orclExcludedNamingcontexts, orclDirReplGroupDSAs

オブジェクト・クラス      changeLogEntry, changeStatusEntry, orclReplAgreementEntry

Oracle Internet Directory の構成

Attributes	orclDebugLevel, orclMaxCC, orclDBType, orclSuffix, orclDITRoot, orclSuName, orclSuPassword, orclSizeLimit, orclTimeLimit, orclGuName, orclGuPassword, orclServerProcs, orclconfigsetnumber, orclhostname, orclIndexedAttribute, orclCatalogEntryDN, orclServerMode, orclPrName, orclPrPassword, orclUseEncrypt, orclDirectoryVersion
オブジェクト・クラス	subconfig, orclConfigSet, orclLDAPSubConfig, orclREPLSubConfig, orclcontainerOC, subregistry, orclLDAPInstance, orclREPLInstance, orclIndexOC, orcleventLog, orclEvents

SSL

---

---

**注意：** これらの属性の値は、構成エントリの一部として格納されています。

---

---

Attributes	orclsslAuthentication, orclsslEnable, orclsslWalletURL, orclsslWalletPasswd, orclsslPort, orclsslVersion
------------	--

監査ログ

Attributes	orclServerEvent, orcleventtype, orclauditattribute, orclauditmessage, orcleventtime, orcluserdn, orclSequence, orclAuditLevel, orclOpResult
オブジェクト・クラス	OrclAuditOC

構成設定エントリの属性

次の表は、Directory Server のインスタンスの構成に使用される構成設定エントリの属性の全セットをリストし、説明したものです。

パラメータ	説明
orcldebuglevel	このサーバー・インスタンスに関連付けられているデバッグ・レベル。configset0 のデフォルトは 0（ゼロ）です。値の範囲は 0（ゼロ）～ 65535 までです。

パラメータ	説明
orclmaxcc	データベースの最大同時接続数。configset0 のデフォルトは 10 です。この属性に負数は使用できません。
orclserverprocs	起動するサーバー・プロセスの数。configset0 のデフォルトは 1 です。この属性に負数は使用できません。
orclsslport	SSL モードのデフォルト・ポート（デフォルトは 636）。ディレクトリを保護モードで実行すると、デフォルト・ポート 636 でリスニングし、SSL ベースの TCP/IP 接続のみ受け入れます（ディレクトリを通常モードで実行すると、デフォルト・ポート 389 でリスニングし、通常の TCP/IP 接続を受け入れます）。複数の LDAP サーバー・インスタンスを追加するときは、このポートを変更することもできます。
orclnonsslport	非 SSL モードのデフォルト・ポート（デフォルトは 389）。
orclsslenable	SSL を使用可能にするかどうかを切り替えるフラグ。同じサーバーの異なるインスタンスを SSL 用または非 SSL 用に使用するときは、このフラグを切り替えることができます。次の 2 つの値のいずれかを使用できます。 <ul style="list-style-type: none"> <li>■ 0 = SSL 使用不可（構成設定 0 のデフォルト）</li> <li>■ 1 = SSL 使用可能</li> </ul> デフォルトは 0（ゼロ）です。
orclsslauthentication	フラグの値は、1、32 または 64 で、Oracle Directory Server の各インスタンスに使用する認証のタイプを指定します。デフォルト値の 1 は、認証なしを意味します。異なるインスタンスに対しては、異なる値を同時に実行できます。サーバー認証、およびクライアントとサーバーの認証の値を指定する場合は、Wallet が必要です。次の 3 つの値のいずれかを使用できます。 <ul style="list-style-type: none"> <li>■ 1 = SSL 認証なし</li> <li>■ 32 = SSL サーバー認証（サーバーがクライアントに証明書を送信します）</li> <li>■ 64 = SSL クライアントとサーバーの認証（クライアントとサーバーは、証明書を交換します）</li> </ul>

パラメータ	説明
orclsslwalleturl	Oracle Wallet の位置を設定します。この値は、Wallet の作成時に設定済みです。Oracle Wallet の位置を変更する場合は、このパラメータを変更する必要があります。クライアントとサーバーの両方で Wallet の位置を設定する必要があります。たとえば Solaris では、このパラメータは次のように設定します。  orclsslwalleturl=file:///Home/my_dir/  Windows NT では、このパラメータは次のように設定します。  file:C:¥Home¥my_dir¥
orclsslwalletpasswd	Wallet をオープンするためにサーバーが使用するパスワード。この値は、Wallet の作成時に設定済みです。Wallet のパスワードを変更する場合は、このパラメータを変更する必要があります。クライアントとサーバーの両方で Wallet のパスワードを設定する必要があります。
orclsslversion	SSL のバージョン。デフォルトは 3 です。

関連項目：

- デバッグ・レベルの詳細は、5-22 ページの「OID 制御ユーティリティを使用したデバッグ・ロギング・レベルの設定」を参照してください。
- Oracle Wallet の位置と Oracle Wallet のパスワードの設定に関する情報は、付録 C「Oracle Wallet Manager の使用方法」を参照してください。

LDAP 構文

構文は、属性が保持できる値の型を定義します。Oracle Internet Directory は、RFC 2252 で指定されている構文の大部分を認識するため、そのドキュメントに記述されている構文の大部分を属性と関連付けることができます。Oracle Internet Directory は、ほとんどの LDAP 構文を認識した上で、一部の LDAP 構文を施行します。

この項では、次のサブセクションについて説明します。

- [Oracle Internet Directory で施行されている LDAP 構文](#)
- [Oracle Internet Directory が認識する、一般的に使用されている LDAP 構文](#)
- [Oracle Internet Directory が認識する、その他の LDAP 構文](#)
- [属性値のサイズ](#)

## Oracle Internet Directory で施行されている LDAP 構文

Oracle Internet Directory では、次の LDAP 構文が施行されています。

- DN
- Facsimile Telephone Number
- OID（オブジェクト識別子）
- Telephone Number

---

---

**注意：** これらの属性に指定する値は、RFC 2252 で指定されている構文に準拠している必要があります。

---

---

## Oracle Internet Directory が認識する、一般的に使用されている LDAP 構文

次の LDAP 構文は、一般的に使用されている構文です。

Attribute Type Description	Numeric String
Boolean	Object Class Description
Certificate	Octet String
Directory String	OID
DN	Presentation Address
Facsimile Telephone Number	Printable String
INTEGER	Telephone Number
JPEG	UTC Time
Name And Optional UID	

## Oracle Internet Directory が認識する、その他の LDAP 構文

前述の一般的に使用されている LDAP 構文以外に、Oracle Internet Directory では次の LDAP 構文が認識されます。

Access Point	LDAP Schema Description
ACI Item	LDAP Syntax Description
Audio	Mail Preference
Binary	Master And Shadow Access Points
Bit String	Matching Rule
Certificate List	Matching Rule Use Description

Certificate Pair	MHS OR Address
Country String	Modify Rights
Data Quality Syntax	Name Form Description
Delivery Method	Object Class Description
DIT Content Rule Description	Octet String
DIT Structure Rule Description	Other Mailbox
DL Submit Permission	Postal Address
DSA Quality Syntax	Protocol Information
DSE Type	Substring Assertion
Enhanced Guide	Subtree Specification
Fax	Supplier And Consumer
Generalized Time	Supplier Information
Guide	Supplier Or Consumer
IA5 String	Supported Algorithm
LDAP Schema Definition	Teletex TerminalIdentifier
	Telex Number

## 属性値のサイズ

構文では、属性値に対して特定のサイズ制約が定義されていません。ただし、構文を使用すると、属性値のサイズを指定できます。Oracle Internet Directory が属性に 'len' 特性を指定することはありません。

たとえば、属性 foo のサイズを 64 に制限するには、属性を次のように定義します。

```
(object_identifier_of_attribute NAME 'foo' EQUALITY caseIgnoreMatch SYNTAX 'object_
identifier_of_syntax{64}')
```

**関連項目：** 属性値の詳細は、RFC2251 の 4.1.6 f 項を参照してください。  
この RFC は、URL: <http://www.ietf.org/rfc/rfc2251.txt> にあります。

## 一致規則

Oracle Internet Directory では、スキーマで次の一致規則定義が認識されます。

accessDirectiveMatch	IntegerMatch
bitStringMatch	numericStringMatch
caseExactMatch	objectIdentifierFirstComponentMatch
caseExactIA5Match	ObjectIdentifierMatch
caseIgnoreIA5Match	OctetStringMatch
caseIgnoreListMatch	presentationAddressMatch
caseIgnoreMatch	protocolInformationMatch
caseIgnoreOrderingMatch	telephoneNumberMatch
distinguishedNameMatch	uniqueMemberMatch
generalizedTimeMatch	
generalizedTimeOrderingMatch	

このリストの一致規則の中で、Oracle Internet Directory では属性値を比較するときに、次の一致規則が実際に実行されています。

DistinguishedNameMatch  
caseExactMatch  
caseIgnoreMatch  
numericStringMatch  
IntegerMatch  
telephoneNumberMatch





---

## 他の LDAP 準拠のディレクトリからのデータの移行

この付録では、LDAP バージョン 3 互換のディレクトリから Oracle Internet Directory へデータを移行する手順を説明します。

この付録では、次の項目について説明します。

- [データ移行プロセスの概要](#)
- [データの移行](#)

## データ移行プロセスの概要

この方法では、アプリケーション・データとメタデータの LDAP バージョン 3 フラット・ファイル表現用に設定された LDIF ファイル形式を使用します。LDIF は、IETF が承認した、LDAP バージョン 3 ディレクトリ・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す。すべての LDAP バージョン 3 互換のサーバーでは、エクスポート時に、ディレクトリ情報ツリーを表す 1 つ以上の LDIF ファイルにその内容をエクスポートできます。しかし、LDIF ファイルがすべて同じように作成されるわけではありません。ある専用の属性またはメタデータが、特定の製品の LDIF 出力に含まれるかどうかわかりません。その結果、`bulkload` または `ldapadd` を使用するときには、LDIF ファイルを Oracle Internet Directory にインポートする前に、いくつかの追加ステップが必要です。

**関連項目：** <http://ftp.isi.edu/in-notes/rfc2849.txt> (LDIF の技術的な仕様に関する詳細)

## データの移行

この項では、次の項目について説明します。

- **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 ファイルからの専用のディレクトリ・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.sh -check` モードの実行とスキーマ違反または重複エラーが残っているかの判断

### 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

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。

- 含まれる専用情報が最少の LDIF 出力を生成する方法
- F-2 ページに記載した IETF Request for Comments 2849 に対して最大の規格合致性を提供する方法

## 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 ("conf") 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」](#)での Oracle Internet Directory 内のベース・スキーマの拡張のためのガイドラインとして使用できます。

## タスク 3: Oracle Internet Directory 内のスキーマの拡張

Oracle Internet Directory 内のディレクトリ・スキーマの拡張方法についてのヒントは、このマニュアルのディレクトリ・スキーマの管理に関する章を参照してください。この作業は、Oracle Directory Manager またはコマンドライン・ツールを使用して実行できます。

## タスク 4: LDIF ファイルからの専用のディレクトリ・データの削除

アクセス制御情報 (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なものになっていません。その結果、様々なディレクトリ・ベンダーがベンダー間で移植できない方法で、ACI ポリシー・オブジェクトを実装しています。

正常と思われる LDIF ファイルから基本エントリ・データがインポートされた後、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、必要なアクセス制御ポリシー情報を含んだ LDIF ファイルを使用して実行できます。

他にもアクセス制御のエリア外を表す専用のメタデータがある場合があります。それらも同様に削除する必要があります。様々な IETF RFC を十分に理解することで、どのディレクトリ・メタデータが特定のベンダーに専用か、どれが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

標準の LDAP バージョン 3 操作属性、すなわち `creatorsName`、`createTimestamp`、`modifiersName` および `modifyTimestamp` の中の 2 つが、Oracle Internet Directory によって、エントリが作成またはインポートされるたびに自動的に生成されます。たとえば LDIF ファイルのインポートを使用して、既存のディレクトリ・データからこれらの値をインスタンス化することはできません。したがって、インポートする前にこれらの属性をファイルから削除する必要があります。

## タスク 6: LDIF ファイルからの非互換の userPassword 属性値の削除

Oracle Internet Directory リリース 2.1.1 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。

- MD4
- MD5
- No encryption
- SHA
- UNIX Crypt

一部のベンダー製品で使用されている userPassword 属性のハッシュ値は、Oracle Internet Directory と互換性はありません。その結果、userPassword 属性と値に対応するすべての行は、プレーン・テキストで表されている、あるいは値を含んでいない場合以外は、LDIF データ・ファイルから取り除く必要があります。LDIF データをインポートした後、手動で再入力するか、ハッシュされた userPassword 情報を別途ディレクトリにアップロードする必要があります。

## タスク 7: bulkload.sh -check モードの実行とスキーマ違反または重複エラーが残っているかの判断

LDIF ファイルの生成とロードの前には、常に bulkload ユーティリティを使用してチェック・モードを LDIF ファイルで実行してください。bulkload の出力が、データの非一貫性をレポートします。

---

# 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。

この付録では、次の項目について説明します。

- [インストール時のエラー](#)
- [管理エラー・メッセージとその原因](#)

## インストール時のエラー

Oracle8i データベース・サーバーをインストールおよび構成するときには、キャラクタ・セット UTF-8 を選択する必要があります。他のキャラクタ・セットを選択すると、Directory Server が正しく機能しません。

## 管理エラー・メッセージとその原因

この項では、発生する可能性のある Oracle Directory Server のすべてのエラー・メッセージをリストします。各メッセージに続いて、そのエラーに関して最も考えられる原因が記述されています。

この項では、次の項目について説明します。

- スキーマ変更が原因の Oracle データベース・サーバー・エラー
- Oracle Directory Server から戻される標準エラー・メッセージ
- その他のエラー・メッセージ

## スキーマ変更が原因の Oracle データベース・サーバー・エラー

### ORA-1562

**原因：** ロールバック・セグメント領域に収まらないスキーマ・コンポーネントを追加しようとする、このエラーが発生し、変更はコミットされません。この問題を解決するには、データベース・サーバーのロールバック・セグメントのサイズを増やします。

## Oracle Directory Server から戻される標準エラー・メッセージ

次にリストされているメッセージは、標準のエラー・メッセージです。Oracle Internet Directory では、これ以外のメッセージも戻されます。標準以外のメッセージは、G-6 ページの「[その他のエラー・メッセージ](#)」にリストし、説明しています。

### 00: 成功しました

**原因：** 操作が正常に完了しました。

### 01: 操作エラー

**原因：** 要求の処理時に、サーバーで一般的なエラーが発生しました。

### 02: プロトコル・エラー

**原因：** クライアント要求が、LDAP プロトコル要件（書式や構文など）を満たしていません。このエラーは、次の状況で発生する可能性があります。

- サーバーで、受信した要求の解析時にデコード・エラーが発生した場合
- エントリに属性の型を追加する追加または変更の要求で、値が指定されていない場合

- SSL 資格証明の読み込みでエラーが発生した場合
- 変更操作で指定されたタイプが不明な場合 (LDAP\_MOD\_ADD、LDAP\_MOD\_DELETE および LDAP\_MOD\_REPLACE 以外)
- 検索範囲が不明です。

**03: 時間制限を超えました。**

**原因:** 検索時間が指定した制限時間を超えました。検索の制限時間が未指定の場合、Oracle Internet Directory では、デフォルトの制限時間である 1 時間が使用されます。

**04: サイズ制限を超えました。**

**原因:** 検索の問合せに一致するエントリが、指定したサイズ制限を超えました。検索のサイズ制限が未指定の場合、Oracle Internet Directory では、デフォルトのサイズ制限が使用されます。

**05: 比較結果は FALSE です。**

**原因:** 指定した値は、エントリ内の値と同一ではありません。

**06: 比較結果は TRUE です。**

**原因:** 指定した値は、エントリ内の値と同一です。

**07: 厳密認証はサポートされていません。**

**原因:** バインド方法がサーバーでサポートされていません。

**08: 厳密認証が必要です。**

**原因:** 強化認証が必要です。この時点で、Oracle Internet Directory はこのメッセージを戻しません。

**09: 受信した結果と参照は一部分です。**

**原因:** サーバーから参照が戻されました。

**10: LDAP 参照エラー**

**原因:** サーバーから参照が戻されました。

**11: LDAP 管理制限エラー**

**原因:** この時点で、Oracle Internet Directory はこのメッセージを戻しません。

**12: 最大拡張機能はサポートされていません。**

**原因:** 指定した要求はサポートされていません。

**16: 該当する属性がありません。**

**原因:** 要求で指定したエントリ内に、該当する属性は存在していません。

**17: 属性タイプが未定義です。**

**原因:** 指定した属性の型が、スキーマ内で定義されていません。

**18: 一致しません。**

**原因:** 指定した一致規則は、その属性型に適合しません。この時点で、Oracle Internet Directory はこのメッセージを戻しません。

- 19: **制約違反です。**  
原因: 要求内の値が、特定の制約に違反しています。
- 20: **タイプまたは値が存在しています。**  
原因: 属性に指定した値が重複しています。
- 21: **構文に誤りがあります。**  
原因: 指定した属性の構文に誤りがあります。検索の場合は、フィルタの構文に誤りがあります。
- 32: **該当するオブジェクトがありません。**  
原因: 操作用に指定したベースが存在していません。
- 33: **別名に問題があります。**  
原因: この時点で、Oracle Internet Directory はこのメッセージを戻しません。
- 34: **識別名の構文に誤りがあります。**  
原因: 識別名 (DN) 構文にエラーがあります。
- 35: **オブジェクトはリーフです。**  
原因: そのエントリはリーフ (終端エントリ) です。この時点で、Oracle Internet Directory はこのメッセージを戻しません。
- 36: **別名の参照解除に問題があります。**  
原因: この時点で、Oracle Internet Directory はこのメッセージを戻しません。
- 48: **認証が正しくありません。**  
原因: この時点で、Oracle Internet Directory はこのメッセージを戻しません。
- 49: **資格証明が無効です。**  
原因: 資格証明が正しくないため、バインドに失敗しました。
- 50: **アクセス権限が不十分です。**  
原因: クライアントに、この操作を実行するためのアクセス権限がありません。
- 51: **ディレクトリ・サービス・エージェントがビジー状態です。**  
原因: サーバーは、これ以上のクライアント接続を受け入れることができません。この時点で、Oracle Internet Directory はこのメッセージを戻しません。
- 52: **ディレクトリ・サービス・エージェントが利用不可です。**  
原因: サーバーと通信できません。この時点で、Oracle Internet Directory はこのメッセージを戻しません。
- 53: **ディレクトリ・サービス・エージェントが実行不可の状態です。**  
原因: 一般的なエラーか、またはサーバーが読み取り専用モードです。
- 54: **ループが検出されました。**  
原因: この時点で、Oracle Internet Directory はこのメッセージを戻しません。
- 64: **命名違反です。**  
原因: この時点で、Oracle Internet Directory はこのメッセージを戻しません。



- 65: **オブジェクト・クラス違反です。**  
原因: エントリに対する変更が、オブジェクト・クラスの定義に違反しています。
- 66: **リーフ以外での操作は許可されていません。**  
原因: 削除対象のエントリに子エントリがあります。
- 67: **相対識別名での操作は許可されていません。**  
原因: 相対識別名 (RDN) 属性でこの操作は実行できません。たとえば、エントリの RDN 属性を削除することはできません。
- 68: **すでに存在しています。**  
原因: 追加条件が重複しています。
- 69: **オブジェクト・クラスを変更できません。**  
原因: この時点で、Oracle Internet Directory はこのメッセージを戻しません。
- 70: **結果が大きすぎます。**  
原因: この時点で、Oracle Internet Directory はこのメッセージを戻しません。
- 80: **不明なエラー**  
原因: この時点で、Oracle Internet Directory はこのメッセージを戻しません。
- 81: **LDAP サーバーと通信できません。**  
原因: LDAP サーバーと通信できません。このメッセージは SDK から戻されます。
- 82: **ローカル・エラー**  
原因: クライアントで内部エラーが発生しました。このメッセージはクライアントの SDK から戻されます。
- 83: **コード化エラー**  
原因: クライアントで、要求をエンコーディングするときにエラーが発生しました。このメッセージは SDK から戻されます。
- 84: **デコード・エラー**  
原因: クライアントで、要求をデコードするときにエラーが発生しました。このメッセージは SDK から戻されます。
- 85: **時間切れです。**  
原因: クライアントが、その操作に指定したタイムアウトに達しました。このメッセージは SDK から戻されます。
- 86: **認証方式が不明です。**  
原因: 認証方式が、クライアントの SDK で理解されません。
- 87: **検索フィルタが正しくありません。**  
原因: 検索フィルタが正しくありません。
- 88: **ユーザーが操作を取り消しました。**  
原因: ユーザーが操作を取り消しました。

**89: LDAP ルーチンのパラメータが正しくありません。**

**原因:** LDAP ルーチンに対するパラメータが正しくありません。

**90: メモリー不足です。**

**原因:** メモリー不足です。

## その他のエラー・メッセージ

これらのメッセージには、エラー・コードは表示されません。

後述のメッセージの一部で使用されているパラメータタグは、Oracle Internet Directory アプリケーションによって、対応する実行時の値に置換されます。

**string 属性が見つかりません (string には文字列が入ります)。**

**原因:** 特定の属性型が、スキーマに定義されていません。

**<パラメータ> が属性 <パラメータ> に見つかりません。**

**原因:** 値がその属性に見つかりません。(ldapmodify)

**オブジェクト・クラス <パラメータ> のスキーマ情報が管理ドメインに含まれていません。**

**原因:** 要求で指定したオブジェクト・クラスが、スキーマに存在していません。

**クラスの追加に使用した oid<パラメータ> は別のクラスで使用されています。**

**原因:** 指定したオブジェクト識別子が重複しています。(スキーマ変更)

**属性 <パラメータ> はすでに使用されています。**

**原因:** 属性名が重複しています。(スキーマ変更)

**属性 <パラメータ> に構文エラーがあります。**

**原因:** 属性名の定義に構文エラーがあります。(スキーマ変更)

**属性 <パラメータ> はスキーマでサポートされていません。**

**原因:** 属性が定義されていません。(すべての操作)

**属性 <パラメータ> は単一の値です。**

**原因:** 属性は単一値です。(ldappadd および ldapmodify)

**属性 <パラメータ> がエントリに存在していません。**

**原因:** エントリに、この属性は存在していません。(ldapmodify)

**属性の定義が正しくありません。**

**原因:** 属性の定義に構文エラーがあります。(スキーマ変更)

**現在はサポートされていません。**

**原因:** このバージョンの LDAP 要求は、このサーバーではサポートされていません。

**削除対象のエントリが見つかりません。**

**原因:** 削除操作に指定した識別名 (DN) が見つかりません。

**変更対象のエントリが見つかりません。**

**原因:** 要求で指定したエントリが見つかりません。

**<パラメータ> をエントリに追加中にエラーが発生しました。**

**原因:** modify の add 操作が呼び出されたときに戻されました。システム・リソースが使用できないことが原因と考えられます。

**属性値の暗号化時にエラーが発生しました。**

**原因:** ユーザー・パスワードの暗号化時にエラーが発生しました。(すべての操作)

**DN の正規化でエラーが発生しました。**

**原因:** 指定された識別名 (DN) が無効です。DN の解析時に構文エラーが見つかりました。(すべての操作)

**<パラメータ> 属性のハッシングでエラーが発生しました。**

**原因:** 属性に対するハッシュ・エントリの作成時にエラーが発生しました。(スキーマ変更)

**<パラメータ> オブジェクト・クラスのアッシングでエラーが発生しました。**

**原因:** オブジェクト・クラスに対するハッシュ・エントリの作成時にエラーが発生しました。(スキーマ変更)

**スキーマ・ハッシュの作成でエラーが発生しました。**

**原因:** スキーマに対するハッシュ表作成時にエラーが発生しました。(スキーマ変更)

**<パラメータ> の置換でエラーが発生しました。**

**原因:** この属性の置換でエラーが発生しました。(ldapmodify)

**属性<パラメータ> に対する値の正規化時にエラーが発生しました。**

**原因:** 属性に対する値の正規化時にエラーが発生しました。(すべての操作)

**<パラメータ> が必須またはオプションの属性リストで見つかりません。**

**原因:** 指定した属性が、オブジェクト・クラスの要件どおりに、必須属性またはオプション属性のリストに存在していません。

**この機能は組み込まれていません。**

**原因:** その機能または要求が現在はサポートされていません。

**INVALID 非同期通信インタフェースは<パラメータ> です。**

**原因:** 要求で指定した特定のアクセス制御項目 (ACI) が無効です。

**必須属性<パラメータ> が管理ドメイン<パラメータ> に定義されていません。**

**原因:** 未定義の属性を参照しています。(スキーマ変更)

**必須属性が不足しています。**

**原因:** 特定のエントリに対する必須属性が、特定のオブジェクト・クラスの要件どおりに存在していません。

**一致規則<パラメータ> が定義されていません。**

**原因:** サーバーに一致規則が定義されていません。(スキーマ変更)

**MaxConnReached**

**原因:** LDAP サーバーへの最大同時接続数に達しました。

**DN を変更せずにエントリの命名属性を変更しようとしています。**

原因: ldap\_modify を使用して、命名属性を変更することはできません。cn などの命名属性は識別名 (DN) の要素です。

**新しい親が見つかりません。**

原因: DN の変更操作で指定した新しい親が存在していません。(ldapmodifydn)

**オブジェクトはすでに存在しています。**

原因: エントリが重複しています。(ldapadd および ldapmodifydn)

**オブジェクト ID<パラメータ> はすでに使用されています。**

原因: 指定したオブジェクト識別子が重複しています。(スキーマ変更)

**オブジェクト・クラス<パラメータ> はすでに使用されています。**

原因: オブジェクト・クラス名が重複しています。(スキーマ変更)

**オブジェクト・クラスの属性が不足しています。**

原因: この特定のエントリに対するオブジェクト・クラスの属性が不足しています。

**OID<パラメータ> に構文エラーがあります。**

原因: オブジェクト識別子の定義に構文エラーがあります。(スキーマ変更)

**エントリ内の属性の 1 つに重複した値があります。**

原因: 作成中のエントリで、同じ属性に対して値を 2 つ入力しました。

**<パラメータ> での操作は許可されていません。**

原因: このエントリでの操作は許可されていません。(変更、追加および削除)

**Directory Server エントリでの操作は許可されていません。**

原因: Directory Server エントリで、この操作を行うことはできません。(削除)

**オプション属性<パラメータ> が管理ドメイン<パラメータ> に定義されていません。**

原因: 未定義の属性を参照している可能性があります。(スキーマ変更)

**ディレクトリ内に親のエントリが見つかりません。**

原因: 親エントリが存在していません。(ldapadd および ldapmodifydn)

**スーパー・オブジェクト<パラメータ> が管理ドメイン<パラメータ> に定義されていません。**

原因: スーパー・タイプが、存在していないクラスを参照しています。(スキーマ変更)

**スーパー・タイプが未定義です。**

原因: スーパー・タイプが存在していません。(スキーマ変更)

**スーパー・ユーザーの追加は許可されていません。**

原因: スーパー・ユーザーのエントリを作成することはできません。(ldapadd)

**構文<パラメータ> が未定義です。**

原因: 構文がサーバーに定義されていません。(スキーマ変更)

**RDN で指定された属性または値がエントリ内に存在していません。**

**原因：** 相対識別名 (RDN) として指定した属性値がエントリ内に存在していません。  
(ldapadd)

**検索範囲が不明です。**

**原因：** LDAP 要求で指定した検索範囲が認識されません。

**このバージョンはサポートされていません。**

**原因：** このバージョンの LDAP 要求は、このサーバーではサポートされていません。



---

# 用語集

## Access Control Policy Point (ACP)

セキュリティ・ディレクティブを含んだエントリ。このディレクティブは、[ディレクトリ情報ツリー](#)内の下位エントリすべてに適用される。

## ACI

「[アクセス制御項目](#)」を参照。

## ACL

「[アクセス制御リスト](#)」を参照。

## ACP

「[Access Control Policy Point \(ACP\)](#)」を参照。

## API

「[アプリケーション・プログラム・インタフェース](#)」を参照。

## ASR

「[アドバンスト・レプリケーション](#)」を参照。

## Cipher Suite

SSL において、ネットワーク・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つのノードは、メッセージの送受信に使用する Cipher Suite を調べるために交渉を行う。

## configset

「[構成設定エントリ](#)」を参照。

## **DES**

データ暗号化規格。1970 年代に IBM と米国政府によって公式規格として開発されたブロック暗号。

## **DIB**

「[ディレクトリ情報ベース](#)」を参照。

## **DIT**

「[ディレクトリ情報ツリー](#)」を参照。

## **DN**

「[識別名](#)」を参照。

## **DRG**

「[ディレクトリ・レプリケーション・グループ](#)」を参照。

## **DSA**

「[ディレクトリ・システム・エージェント](#)」を参照。

## **DSE**

DSA 固有のエントリ。異なる DSA に、同じ DIT 名を保持できるが、内容は異なる必要がある。つまり、内容はそれを保持している DSA に固有のものである。DSE は、それを保持している DSA に固有の内容を含むエントリである。

## **Global Unique Identifier (GUID)**

マルチマスター・レプリケーション環境では、複数のノードでレプリケートされるエントリは、各ノードで同じ識別名 (DN) を持つ。ただし、DN が同じでも、各ノードで異なる GUID が割り当てられる。たとえば、同じ DN を node1 と node2 の両方でレプリケートできるが、node1 に常駐しているときのその DN に対する GUID は、node2 におけるその DN に対する GUID とは異なる。

## **GUID**

「[Global Unique Identifier \(GUID\)](#)」を参照。

## **Internet Message Access Protocol (IMAP)**

プロトコルの 1 種。クライアントは、このプロトコルを使用して、サーバー上の電子メール・メッセージに対するアクセスおよび操作を行う。リモートのメッセージ・フォルダ (メールボックスとも呼ばれる) を、ローカルのメールボックスと機能的に同じ方法で操作できる。

## **LDAP**

「[Lightweight Directory Access Protocol \(LDAP\)](#)」を参照。



## LDAP データ交換フォーマット (LDIF)

LDAP コマンドライン・ユーティリティに使用する入力ファイルをフォーマットするための一連の規格。

## Lightweight Directory Access Protocol (LDAP)

標準的で拡張可能なディレクトリ・アクセス・プロトコル。LDAP クライアントとサーバーが通信で使用する共通言語。業界標準のディレクトリ製品 (Oracle Internet Directory など) をサポートする設計規則の枠組み。

## 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方向ハッシュ関数。1 ビットでもファイルの値が変更された場合、そのファイルの MD4 チェックサムは変更される。MD4 が元のファイルと同じ結果を生成するようなファイルの偽造は、非常に難しいと考えられている。

## MD5

MD4 の改善されたバージョン。

## MDS

「[マスター定義サイト](#)」を参照。

## MTS

「[マルチスレッド・サーバー](#)」を参照。

## Net8

Oracle のネットワーク製品ファミリの基礎。Net8 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。Net8 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。Net8 は、ネットワーク上の各コンピュータに配置される。一度ネットワーク・セッションが確立されると、Net8 は、クライアントとサーバーに対するデータ転送手段として機能する。

## 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釈され、実行される。

## OID データベース・パスワード・ユーティリティ (OID Database Password Utility)

Oracle Internet Directory が Oracle データベースに接続するときのパスワードの変更に使用されるユーティリティ。

## **OID モニター (OID Monitor)**

Oracle Directory Server プロセスの開始、モニターおよび終了を実行する Oracle Internet Directory のコンポーネント。Replication Server がインストールされている場合は、その制御も行う。

## **Oracle Directory Manager**

Oracle Internet Directory を管理するための、グラフィカル・ユーザー・インタフェースを備えた Java ベースのツール。

## **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 (LDAP) バージョン 3 と Oracle8i の高パフォーマンス、拡張性、耐久性および可用性を組み合わせたもの。

## **Oracle Wallet Manager**

セキュリティ管理者が、クライアントとサーバーにおける公開鍵のセキュリティ資格証明の管理に使用する Java ベースのアプリケーション。

## **Oracle コール・インタフェース (Oracle Call Interface: OCI)**

Oracle データベース・サーバーにアクセスして SQL 文実行のすべてのフェーズを制御するために、第三世代言語のネイティブ・プロシージャまたはファンクション・コールを使用するアプリケーションを作成することを可能にする、アプリケーション・プログラミング・インタフェース (API)。

## **RDN**

「[相対識別名](#)」を参照。

## **Secure Hash Algorithm (SHA)**

長さが 264 ビット未満のメッセージを取得して、160 ビットのメッセージ・ダイジェスト値を生成するアルゴリズム。アルゴリズムは MD5 よりも若干遅いが、メッセージ・ダイジェスト値が大きくなることで、激しい衝突や反転攻撃に対してより強力に保護できる。

## **Secure Socket Layer (SSL)**

Netscape Communications Corporation によって設計された、ネットワーク接続を保護するための業界標準プロトコル。SSL では公開鍵方式 (PKI) の使用によって、認証、暗号化およびデータの整合性が提供される。

## **SGA**

「[システム・グローバル領域](#)」を参照。

## **SHA**

「[Secure Hash Algorithm \(SHA\)](#)」を参照。

## SLAPD

スタンドアロンの LDAP デーモン。

## SSL

「[Secure Socket Layer \(SSL\)](#)」を参照。

## subACLSubentry

ACL 情報を含んだ特定のタイプのサブエントリ。

## subSchemaSubentry

スキーマ情報を含んだ特定タイプの[サブエントリ](#)。

## Trustpoint

「[信頼されている証明書](#)」を参照。

## UCS2

固定幅 16 ビットの [Unicode](#)。各文字は 16 ビットの領域を持つ。Latin-1 文字はこの規格の最初の 256 コード・ポイントであり、Latin-1 の 16 ビット拡張と見なすことができる。

## Unicode

汎用キャラクタ・セットのタイプ。16 ビットの領域にコード化された 64K 個の文字の集合。既存のほとんどのすべてのキャラクタ・セット規格の文字をすべてコード化する。世界中で使用されているほとんどの書き言葉を含む。Unicode は Unicode Inc. によって所有および定義される。Unicode は標準的なコード化であり、異なるロケールで値を伝達できることを意味する。しかし、Unicode とすべての Oracle キャラクタ・セットとの間で、情報の損失なしにラウンドトリップ変換が行われることは保証されない。

## UNIX Crypt

UNIX 暗号化アルゴリズム。

## UTC (Coordinated Universal Time)

世界中のあらゆる場所で共通の標準時間。以前から現在に至るまで広くグリニッジ時 (GMT) または世界時と呼ばれており、UTC は名目上は地球の本初子午線に関する平均太陽時を表す。UTC 形式である場合、値の最後に z が示される (例: 200011281010z)。

## UTF-8

文字ごとに連続した 1、2 または 3 バイトを使用する [UCS2](#) の可変幅コード化。0 ~ 127 の文字 (7 ビット ASCII 文字) は 1 バイトでコード化され、128 ~ 2047 の文字では 2 バイト、2048 ~ 65535 の文字では 3 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 UTF-8 (Unicode 2.1 規格用) となる。規格は、文字ごとに連続した 4、5 または 6 バイトを使用する UCS4 文字をサポートする拡張の余地を残している。

## 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します。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します。

## X.509

公開鍵の署名に使用される ISO の一般的な書式。

## アクセス制御項目 (Access Control Information Item: ACI)

どのディレクトリ・データに対して、誰がどのタイプのアクセス権限を持っているかを判断する属性。この属性には、エントリに関係する構造型アクセス項目と、属性に関係するコンテンツ・アクセス項目に関する 1 組の規則が含まれている。両方のアクセス項目に対するアクセス権限を、1 つ以上のユーザーまたはグループに付与できる。

## アクセス制御リスト (Access Control List: ACL)

アクセス・ディレクティブのグループ。管理者が定義する。ディレクティブは、特定のクライアントまたはクライアントのグループ、あるいはその両方に対して、特定データへのアクセスのレベルを付与する。

## アドバンスト・レプリケーション (Advanced Symmetric Replication: ASR)

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 Oracle8i の機能。

## アプリケーション・プログラム・インタフェース (Application Program Interface: API)

指定したアプリケーションのサービスにアクセスするための一連のプログラム。たとえば、LDAP 対応のクライアントは、LDAP API で使用可能なプログラム・コールを通して、ディレクトリ情報にアクセスする。

## 暗号化 (encryption)

メッセージの内容を、宛先の受信者以外の第三者が読むことのできない形式 (暗号文) に変換するプロセス。

## 一方向関数 (one-way function)

一方向への計算は容易だが、逆の計算、すなわち反対方向への計算は非常に難しい関数。

## 一方向ハッシュ関数 (one-way hash function)

可変サイズの入力を取得して、固定サイズの出力を作成する [一方向関数](#)。

## 一致規則 (matching rule)

検索または比較操作での、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 のいずれかと一致させるか、あるいはその両方と一致させることができます。属性を作成したときに、それを一致規則と対応付けることができます。

### **インスタンス (instance)**

「[サーバー・インスタンス](#)」を参照。

### **エントリ (entry)**

ディレクトリの基本単位で、ディレクトリ・ユーザーに関係のあるオブジェクトに関する情報が含まれている。

### **オブジェクト・クラス (object class)**

名前を持った属性のグループ。属性をエントリに割り当てるときは、その属性を保持しているオブジェクト・クラスをそのエントリに割り当てる。

同じオブジェクト・クラスに関連するオブジェクトはすべて、同じ属性を共有する。

### **簡易認証 (simple authentication)**

ネットワークで送信された暗号化されていない識別名 (DN) とパスワードによって、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 DN とパスワードとディレクトリに格納されている DN 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)**

Directory Server 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 (スキーマ、ACL および共通属性) される。

### **キー (key)**

暗号化において広く使用されているビット列。データの暗号化と復号化を可能にする。キーは別の数学的な操作にも使用される。暗号が与えられると、キーは平文の暗号文へのマッピングを判断する。

### **兄弟 (sibling)**

1 つ以上の他のエントリと同じ親を持ったエントリ。

### **継承 (inherit)**

オブジェクト・クラスが別のクラスから導出されたときに、導出元のオブジェクト・クラスの多数の特性も導出 (継承) されること。同様に、属性のサブタイプも、そのスーパータイプの特性を継承する。

### **ゲスト・ユーザー (guest user)**

匿名ユーザーではなく、特定のユーザー・エントリも持っていないユーザー。

### コールド・バックアップ (cold backup)

データベース・コピー・プロシージャを使用して、新規 **DSA** を既存のレプリケート・システムに追加する手順。

### 公開鍵 (public key)

公開鍵暗号における一般に公開されるキー。主に暗号化に使用されるが、署名の検証にも使用される。

### 公開鍵暗号 (public-key cryptography)

公開鍵と秘密鍵を使用する方法に基づいた暗号化。

### 公開鍵暗号 (public-key encryption)

メッセージの送信側が、受信側の公開鍵でメッセージを暗号化するプロセス。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そのメッセージを復号化します。

### 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)

Directory Server の特定インスタンスに関する構成パラメータを保持しているディレクトリ・エントリ。複数の構成設定エントリを格納でき、実行時に参照できる。構成設定エントリは、DSE の subConfigsubEntry 属性で指定されているサブツリー内でメンテナンスされる。DSE 自体は、サーバーの起動対象である関連の**ディレクトリ情報ベース**に常駐している。

### コンシューマ (consumer)

レプリケーション更新の宛先となる Directory Server。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)

**ディレクトリ・ネーミング・コンテキスト**のルートの **DN**。

### サーバー・インスタンス (server instance)

Directory Server の個々の起動のこと。異なる Directory Server 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、異なるサーバー・インスタンスと呼ばれる。

### 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。

- **Access Control Policy Point (ACP)**
- 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ของ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 DIT 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。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**。

### サブライヤ (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。**コンシューマ**・サーバーに、マスター・コピーから更新を供給する。

### 参照 (referral)

「**ナレッジ参照**」を参照。

### 識別名 (distinguished name: DN)

ディレクトリ・エントリの一意名。親エントリの個々の名前が、下からルート方向へすべて順に結合されて構成されている。

### システム・グローバル領域 (System Global Area: SGA)

共有メモリ構造の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。

### 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、その他の操作情報は、管理者が定義し、ディレクトリ・プログラムの処理時に、そのプログラムによって使用される。

### 従属参照 (subordinate reference)

エントリのすぐ下から始まるネーミング・コンテキストの参照位置を、DIT 内で下位方向に指し示すナレッジ参照。

### 上位参照 (superior reference)

DIT 内で、参照先の DSA が保持しているすべてのネーミング・コンテキストより上位のネーミング・コンテキストを保持している DSA を上位方向に指し示すナレッジ参照。

### 証明書 (certificate)

アイデンティティを公開鍵に安全にバインドする ITU X.509 バージョン 3 規格のデータ構造。証明書は、エンティティの公開鍵が、信頼されている機関（**認証局**）によって署名されたときに有効となる。この証明書は、そのエンティティの情報が正しいこと、および公開鍵がそのエンティティに実際に属していることを保証します。

### 証明連鎖 (certificate chain)

エンド・ユーザーまたはサブスクライバの証明書とその認証局の証明書を含む、順序付けられた証明書のリスト。

### 信頼されている証明書 (trusted certificate)

一定の信頼度を有すると認定された第三者のアイデンティティ。信頼されている証明書は、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ます。一般的に、信頼されている認証局によってユーザーの証明書が発行されます。

### 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。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。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**。



### スーパー・ユーザー (superuser)

一般的にはディレクトリ情報へのあらゆるアクセスが可能な、特別なディレクトリ管理者。

### スキーマ (schema)

**属性、オブジェクト・クラス**、およびそれらに対応する一致規則の集合体。

### スポンサ・ノード (sponsor node)

レプリケーションにおいて、新規ノードに初期データを供給するために使用されるノード。

### スマート・ナレッジ参照 (smart knowledge reference)

ナレッジ参照エントリが検索の有効範囲内にあるときに戻される**ナレッジ参照**。要求された情報を格納しているサーバーを示す。

### スループット (throughput)

Oracle Internet Directory がディレクトリ操作を完了する包括的な率。通常、操作 / 秒 (1 秒当りの操作件数) で表されます。

### スレーブ (slave)

「**コンシューマ**」を参照。

### セッション・キー (session key)

1 つのメッセージまたは通信セッションの継続時間に使用される、対称鍵暗号方式のキー。

### 整合性 (integrity)

受信メッセージの内容が、送信時の元のメッセージの内容から変更されていないことを保証すること。

### 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ための宛先の説明。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。

宛先サービスは、その Oracle8i リリース 8.1 データベースのサービス名またはその Oracle リリース 8.0 またはバージョン 7 データベースの Oracle システム識別子 (Oracle System Identifier: SID) を使用して示される。ネットワーク・ルートは、ネットワーク・アドレスを使用して、少なくともリスナーの位置を示す。

### 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 RDN である。

**属性 (attribute)**

エントリの性質を表す断片的な情報項目。エントリは属性のセットで構成され、属性はそれぞれ、[オブジェクト・クラス](#)に属している。さらに、各属性には型と値があり、型で属性内の情報の種類が表され、値には実際のデータが含まれる。

**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。

**データ整合性 (data integrity)**

受信メッセージの内容が、送信時の元のメッセージの内容から変更されていないことを保証すること。

**ディレクトリ・システム・エージェント (directory system agent: DSA)**

Directory Server を表す X.500 の用語。

**ディレクトリ情報ツリー (directory information tree: DIT)**

エントリの識別名 (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・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・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 Directory Server の集まり。

**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。

**同時クライアント (concurrent clients)**

Oracle Internet Directory とのセッションを確立しているクライアントの総数。

**同時操作 (concurrent operations)**

すべての同時クライアントの要求に基づいてディレクトリで実行されている操作の数。一部のクライアントではセッションがアイドル状態の可能性があるため、この数は同時クライアントの数と必ずしも同じではありません。

### 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

1 つの特定管理領域は、この 3 つの管理面の 1 つを制御する。特定管理領域は、自律型管理領域の一部である。

### 匿名認証 (anonymous authentication)

ディレクトリがユーザー名とパスワードの組合せを要求せずにユーザーを認証するプロセス。各匿名ユーザーは、匿名ユーザー用に指定された権限を行使する。

### ナレッジ参照 (knowledge reference)

リモート **DSA** に関するアクセス情報（名前とアドレス）およびそのリモート DSA が保持している **DIT** サブツリーの名前。ナレッジ参照は、参照とも呼ばれる。

### 認可 (authorization)

オブジェクトまたはオブジェクトのセットへのアクセスのためにユーザー、プログラムまたはプロセスに与えられる許可。

### 認証 (authentication)

コンピュータ・システム内のユーザー、デバイスまたはその他のエンティティの識別情報を検証するプロセス。多くの場合、システム内のリソースへのアクセスを許可する前提条件として使用される。

### 認証局 (certificate authority: CA)

他のエンティティ（ユーザー、データベース、管理者、クライアント、サーバーなど）が本物であることを証明する信頼性のある第三者機関。認証局は、ユーザーの識別情報を検証し、認証局の秘密鍵を使用して署名した証明書を発行します。

### ネーミング・コンテキスト (naming context)

完全に 1 つのサーバーに常駐しているサブツリー。サブツリーは連続している必要がある。つまり、サブツリーの最上位の役割を果たすエントリから始まり、下位方向にリーフ・エントリまたは従属ネーミング・コンテキストへの**ナレッジ参照**（参照とも呼ばれる）のいずれかまでを範囲とする必要がある。単一のエントリから DIT 全体までを範囲とすることができず。

### ネーミング属性 (naming attribute)

異なるタイプの相対識別名 (**RDN**) の値を保持する特別な属性。ネーミング属性は、そのニーモニック・ラベル（通常 cn、sn、ou、o、c など）で識別できる。たとえば、ネーミン

グ属性「c」は、ネーミング属性「国」(country) のニーモニックで、特定の国の値に対応する RDN が保持されている。

### **ネット・サービス名 (net service name)**

接続記述子へ解決されるサービスの簡易名。ユーザーは、ユーザー名とパスワードを、接続するサービスの接続文字列内のネット・サービス名とともに送ることによって、接続要求を開始する。

```
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)
- Directory Server
- Oracle Names server
- NDS、NIS または CDS などの外部ネーミング・サービス

### **パーティション (partition)**

一意の重複していないディレクトリ・ネーミング・コンテキスト。1 つの Directory Server に格納されている。

### **バインド (binding)**

ディレクトリに対して認証を行うプロセス。

### **ハンドシェイク (handshake)**

2 台のコンピュータが通信セッションを開始するために使用するプロトコル。

### **秘密鍵 (private key)**

公開鍵暗号におけるシークレット・キー。主に復号化に使用されるが、デジタル署名とともに暗号化にも使用される。

### **フィルタ (filter)**

データ (通常、検索対象のデータ) を限定する方法。フィルタは、常に DN で表される (例: cn=susie smith, o=acme, c=us)。

### **フェイルオーバー (failover)**

障害の認識とリカバリのプロセス。

### **復号化 (decryption)**

暗号化されたメッセージ (暗号文) の内容を、元の可読書式 (プレーン・テキスト) に変換する処理。

### プロキシ・ユーザー (proxy user)

通常、ファイアウォールなどの中間層を備えた環境で利用される一種のユーザー。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しますが、このログインはプロキシ・ユーザーで行われます。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 に切り替えます。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します。

### 変更ログ (change logs)

Directory Server に加えられた変更を記録するデータベース。

### マスター・サイト (master site)

レプリケーションにおいて、マスター定義サイト以外のサイトで、LDAP レプリケーションのメンバーであるサイト。

### マスター定義サイト (master definition site: MDS)

レプリケーションにおいて、管理者が構成スクリプトを実行する Oracle Internet Directory のデータベース。

### マルチスレッド・サーバー (multi-threaded server: MTS)

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の数が増える。MTS 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、受信した複数のネットワーク・セッション要求を共通キューに送信する。サーバー・プロセスの共有プールにあるアイドル状態の共有サーバー・プロセスが、キューから要求を取り出す。これは、サーバー・プロセスの小さいプールで大量のクライアントを処理できるということを意味する。専用サーバーとは対照的である。

### リレーショナル・データベース (relational database)

データベースはデータの構造化された集合。リレーショナル・システムでは、データは、それぞれ同じ列のセットを持つ 1 つ以上の行で構成された表に格納される。Oracle では、複数の表のデータを容易にリンクできる。このため、Oracle はリレーショナル・データベース管理システム、すなわち RDBMS と呼ばれる。Oracle はデータを複数の表に格納し、さらに表間の関係を定義できる。このリンクは両方の表に共通の、1 つ以上のフィールドに基づいて行われる。

### ルート DSE (Root DSE)

「[ルート・ディレクトリ固有のエントリ](#)」を参照。

### ルート・ディレクトリ固有のエントリ (Root Directory Specific Entry)

ディレクトリに関する操作情報を格納するエントリ。情報は複数の属性に格納されている。

**レジストリ・エントリ (registry entries)**

**サーバー・インスタンス**と呼ばれる Oracle Internet Directory サーバーの起動に関連する実行時情報を含むエントリ。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 Directory Server・インスタンスが停止するまで保持される。

**レプリカ (replica)**

ネーミング・コンテキストの個々のコピー。1 つのサーバー内に格納されている。

**レプリケーション承諾 (replication agreement)**

**ディレクトリ・レプリケーション・グループ**内の Directory Server 間におけるレプリケーションの関係を記述する特別なディレクトリ・エントリ。

---

# 索引

## 数字

---

1 レベルの検索, 7-3

389 ポート, 3-5, 3-6, A-31, A-33, E-5

636 ポート, 3-5, 3-6, A-31, A-33, E-5

## A

---

Access Control List (ACL), 2-15, 2-22

Modification, 5-27

評価, 9-10

グループ, 9-14

優先順位規則, 9-11

Access Control Policy Points (ACP), 9-3, 9-19

管理、Oracle Directory Manager を使用, 4-10

構造型アクセス項目, 9-18

コンテンツ・アクセス項目, 9-18

作成、Oracle Directory Manager を使用, 4-8

追加

ldapmodify を使用, 9-31

Oracle Directory Manager を使用, 9-26

表示、Oracle Directory Manager を使用, 9-17

複数, 9-3

ACI 項目、「アクセス制御項目 (ACI)」を参照

ACI ディレクティブ, 2-15

ACI ディレクティブ書式, 2-15

ACI, 「アクセス制御項目 (ACI)」を参照

ACL ディレクティブ

エントリ, 9-3

サブツリー, 9-2

ACL, 「アクセス制御リスト (ACL)」を参照

ACP, 「Access Control Policy Points (ACP)」を参照

add.log, A-6

AlternateServers 属性、フェイルオーバー, 16-4

ANALYZE, 15-5

「Apply」ボタン、Oracle Directory Manager, 4-6

ASR, 「アドバンスト・レプリケーション」を参照

## B

---

Begins With、Oracle Directory Manager のフィルタ,  
6-7

Bind イベント, 5-26

BSTAT/ESTAT, 15-7

bulkdelete, 4-12, 7-15, A-21

NLS, 12-9

構文, A-21

bulkload, 4-12, 7-14, 7-15, A-22

.dat ファイル, 7-14

-load オプション, 7-15

NLS, 12-8

構文, A-22

索引の作成, 7-15

入力ファイルの生成, 7-14

bulkmodify, 4-12

LDIF ファイルベースの変更, A-24

NLS, 12-9

構文, A-24

## C

---

C API, 2-22

「Cancel」ボタン、Oracle Directory Manager, 4-7

catalog.sh, 「カタログ管理ツール」を参照

CA, 「認証局」を参照

Chadwick, David, xxiii

Change Retry Count、設定, 10-12

changeLog, E-3

changeLogEntry, E-3

changeNumber, E-3

- changeStatus, E-3
- changeStatusEntry, E-3
- changetype, E-3
  - add, A-14
  - delete, A-15
  - modify, A-14
  - modrdn, A-15
- Cipher Suite, 2-14
  - SSL, 8-2
    - SSL\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA, 8-2
    - SSL\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5, 8-2
    - SSL\_RSA\_WITH\_NULL\_MD5, 8-2
    - SSL\_RSA\_WITH\_NULL\_SHA, 8-2
- cn 属性, 2-5
- commonName 属性, 2-5
- configNLDAP.ora, B-8
- Configuration Set Location, 5-13
- CPU の数
  - Oracle のフォアグラウンド・プロセスに関するチューニング, 15-5
  - 様々な配置の使用例に必要な能力, 13-8
  - 使用量, 13-9
  - 処理能力, 14-12
  - チューニング, 15-3
  - チューニングが必要な場合, 15-3
  - 要件
    - 見積り, 14-13
    - 容量計画, 14-12
  - 容量計画, 14-2
- CPU の処理能力, 14-12
- CPU 要件の見積り, 14-13
- 「Create Entry」メニュー項目、Oracle Directory Manager, 4-8
- createTimestamp 属性, 2-4, F-3
  - top 内のオプション, 2-9
- 「Create」ボタン、Oracle Directory Manager, 4-9
- creatorsName 属性, 2-4, F-3
- creatorsName、top 内のオプション属性, 2-9

## D

---

- .dat ファイル、bulkload により生成, 7-14
- DB\_BLOCK\_BUFFERS, 15-7
- DBMS\_STATS パッケージ, 15-2
- DBMS\_STATS パッケージの ANALYZE ファンクション, 15-2
- 「Delete」ボタン、Oracle Directory Manager, 4-9

- DES40 暗号化, 2-16
- Directory Server, 1-7
  - アクティブ・インスタンスのパラメータの変更, 5-4
  - 起動, 3-5, 4-16, A-31
    - 構成設定なし, 3-8
    - デフォルトの構成を使用, 3-8, A-34
  - 起動失敗, 3-8
  - 構成設定エントリ, 5-2
  - 構成設定エントリの変更, 5-11
  - 異なる構成設定エントリを使用, 5-2
  - 再起動, 3-7, 5-4, A-33
  - サプライヤとコンシューマ両方の役割, 2-31
  - 実行方法, 3-3
  - 接続, 2-22, 4-3, 4-4, 4-10, 4-16
    - Oracle Directory Manager を使用, 4-7, 4-9
  - 切断、Oracle Directory Manager を使用, 4-7, 4-10
  - 通常モード, E-5
  - 停止, 3-5, 4-16, A-31
  - デバッグ・レベル, E-4
  - プロセス, E-5
  - 保護モード, E-5
  - マルチスレッド, 1-8
  - マルチマスター・レプリケーション, 1-8, 2-31
  - レプリケート環境, 2-31
- Directory Server インスタンス, 2-21
- Directory Server からの切断, 4-10
  - Oracle Directory Manager を使用, 4-7
- Directory Server の停止, 4-16
- DirectoryReplicationGroupDSAs, 10-14
- DIT, 「ディレクトリ情報ツリー (DIT)」を参照
- DNS (Domain Name System), 13-3
- DN, 「識別名」を参照
- 「Drop Index」ボタン, 4-9
- 「Drop Index」メニュー項目, 4-8
- DSA、環境の設定, B-2
- 「DSE Modification」イベント, 5-27

## E

---

- 「Edit」ボタン、Oracle Directory Manager, 4-9
- 「Edit」メニュー項目、Oracle Directory Manager, 4-7
- 「Ends With」フィルタ、Oracle Directory Manager, 6-7
- 「Exact Match」フィルタ、Oracle Directory Manager, 6-8, 7-4, 9-20, 9-23



「Exit」メニュー項目、Oracle Directory Manager, 4-7  
extensibleObject オブジェクト・クラス, 7-17

## F

---

「File」メニュー、Oracle Directory Manager, 4-7  
「Find Attributes」ボタン、Oracle Directory Manager, 6-15  
「Find Objects」ボタン、Oracle Directory Manager, 4-9, 6-6

## G

---

「Greater or Equal」フィルタ、Oracle Directory Manager, 6-8, 7-4, 9-20, 9-23  
groupOfNames オブジェクト・クラス, 7-8  
groupOfUniqueNames, 7-8  
groupOfUniqueNames オブジェクト・クラス, 7-8

## H

---

「Help」ボタン、Oracle Directory Manager, 4-9  
「Help」メニュー項目、Oracle Directory Manager, 4-8  
Hodges, Jeff, xxiii  
Howes, Tim and Mark Smith, xxiii

## I

---

### IETF

Draft, Oracle Internet Directory で施行, E-2  
LDAP 承認, 1-5  
Oracle Internet Directory で施行されている RFC, E-2  
initNLDAP.ora, B-8  
Internet Engineering Task Force (IETF), 「IETF」を参照  
iostat ユーティリティ, 15-2  
I/O サブシステム  
    サイズ設定, 14-5  
    容量計画, 14-2, 14-5  
I/O スループット、最大, 14-6  
IP アドレス・テイクオーバー (IPAT), 16-8

## J

---

Java クライアント、NLS, 2-18  
Java ネイティブ・インタフェース, 2-22  
jpegPhoto 属性, 2-5, 7-12  
JPEG イメージ、ldapadd を使用した追加, A-6

## K

---

Kerberos 認証, A-5, A-7, A-10  
Kosiur, Dave, xxiii

## L

---

### LDAP

IETF 承認, 1-5  
Transport Layer Security, 1-5  
拡張性, 1-5  
規則、エントリの変更, 7-9  
検索フィルタ、IETF 準拠, A-17  
構文, E-6  
    Oracle Internet Directory で施行, E-7  
    Oracle Internet Directory で認識, E-7  
国際化対応, 2-17  
サーバー・インスタンス, 2-19, 2-20, 2-21  
    起動, 3-4, A-30  
サーバー、マルチスレッド, 1-8  
セキュリティ, 1-5  
追加または変更のパフォーマンス, 15-11  
バージョン 3, 1-5, 用語集 -4  
ldapadd, 4-11, 7-11, A-4  
    JPEG イメージの追加, A-6  
    NLS, 12-6  
    エントリの追加, A-4  
    構文, A-4  
ldapaddmt, 4-11, 7-11, A-6  
    NLS, 12-6  
    構文, A-6  
    複数エントリを同時に追加, A-6  
    ログ, A-6  
ldapbind, A-7  
    NLS, 12-6  
    構文, A-7  
ldap-bind 操作, 2-12  
ldapcompare, 4-11, 7-11, A-8  
    NLS, 12-7  
    構文, A-8

- ldapdelete, 4-11, 7-11, A-10
  - NLS, 12-7
  - エントリの削除, A-10
  - 構文, A-10
- ldapmoddn, 4-11, 7-11, A-11
  - NLS, 12-7
  - 構文, A-11
- ldapmodify, 4-11, 7-11, A-12
  - ACP の追加, 9-31
  - LDIF ファイル, A-4, A-6, A-12, A-16
  - NLS, 12-6
  - エントリの削除, A-15
  - エントリ・レベルの ACI の追加, 9-32
  - オブジェクト・クラスの追加, 6-12
  - オブジェクト・クラスの変更, 6-12
  - 監査レベルの変更, 5-28
  - グループ・エントリの作成, A-14
  - 構文, A-12
  - 属性値の置換, A-15
  - 属性の追加, 6-24
  - 属性の変更, 6-24
  - 複数値の属性への値の追加, A-14
  - 変更の種類, A-14
- ldapmodifymt, 4-11, 7-11, A-16
  - NLS, 12-6
  - 構文, A-16
  - 使用方法, A-16
  - マルチスレッド処理, A-17
- ldaprepl.sh, 10-7
- ldapsearch, A-17
  - NLS, 12-6
  - 監査ログの間合せ, 5-24
  - 構文, A-17
  - フィルタ, A-19
- LDAP 検索のパフォーマンス, 15-11
- LDAP 交換フォーマット (LDIF), 4-11
- LDAP データ交換フォーマット (LDIF), A-2
  - bulkload 使用時, A-22
- LDIF
  - 形式化規則, A-3
  - 形式化の注意事項, A-3
  - 構文, A-2
  - 使用方法, 4-11, A-2
  - ファイルベースの変更、bulkmodify では未サポート, A-24
  - ファイル、ldapmodify コマンド, A-4, A-6, A-12, A-16

- ldifwrite, 4-12, A-26
  - NLS, 12-8
  - 構文, A-26
- LDIF ファイル
  - 移行での専用のデータの削除, F-3
  - 構成設定エントリの追加, 5-10
  - コマンドでの参照, 5-12
- 「Less or Equal」フィルタ, 6-8, 7-4, 9-20, 9-24
- listener.ora, 10-6, B-7
- load オプション、bulkload, 7-15
- LSNRCTL ユーティリティ, 10-6

---

## M

- maxextents, 10-5
- MD4, 5-13, 5-14, 5-16
  - パスワード暗号化, 2-16
- MD5, 5-13, 5-14, 5-16, F-4
  - パスワード暗号化, 2-16
- member 属性, 7-8
- Microsoft Active Directory, 13-2
- modifiersName, 2-5
- modifiersName 属性, 2-4, F-3
- modifyDN、監査ログのイベント, 5-27
- modifyTimestamp 属性, 2-4, F-3
- mpstat ユーティリティ, 15-2

---

## N

- namingContexts 属性, 5-14, 5-15
  - 複数値, 5-15
- Net8, 2-20, 2-23
  - レプリケーションの準備, 10-4
- newdb.sql, B-9
- NLS\_LANG 環境変数, 12-2
  - 指定, 12-3
- NLS, 「各国語サポート (NLS)」を参照
- 「no SSL authentication」オプション, 4-6
- NOS ディレクトリ, 13-2, 13-3
- 「Not Null」フィルタ、Oracle Directory Manager, 6-8
- Novell の eDirectory ソリューション, 13-2
- NULL 値、属性, 6-3

## O

- objectclass 属性, 5-25
- OCI, 「Oracle コールインタフェース」を参照
- OFA, 「Optimal Flexible Architecture (OFA)」を参照
- oidctl, 「OID 制御ユーティリティ」を参照
- OIDLDAPD, 3-5, A-31
- oidmon, 「OID モニター」を参照
- OIDREPLD, 3-7, A-33
- OID 制御ユーティリティ, 3-2, 4-13
  - restart コマンド, 5-4
  - 構文, A-30
  - サーバー・インスタンスの起動と停止, 3-3
  - サーバーの起動コマンド, 4-13
  - サーバーの停止コマンド, 4-13
- OID 調停ツール, 4-14, 10-33
- OID データベース統計収集ツール, 4-14
  - 構文, A-35
- OID データベース・パスワード・ユーティリティ, 4-13, 5-30
- OID パスワード・ユーティリティ, 4-13
- OID モニター, 2-20, 4-13
  - 起動, 3-2, 3-3, A-28, A-29
  - 構文, A-28
  - スリープ・タイム, 3-2, A-29
- OLTS\_ATTRSTORE 表領域, 14-10, 15-8
- OLTS\_CT\_CN 表領域, 14-10
- OLTS\_CT\_DN 表領域, 14-10, 15-8
- OLTS\_CT\_OBJCL 表領域, 14-10
- OLTS\_CT\_STORE 表領域, 14-10
- OLTS\_DEFAULT 表領域, 14-10
- OLTS\_IND\_ATTRSTORE, 15-8
- OLTS\_IND\_ATTRSTORE 表領域, 14-10
- OLTS\_IND\_CT\_DN, 15-8
- OLTS\_IND\_CT\_DN 表領域, 14-10
- OLTS\_IND\_CT\_STORE 表領域, 14-10
- OPEN\_CURSORS, 15-10
- 「Operations」メニュー項目、Oracle Directory Manager, 4-8
- Optimal Flexible Architecture (OFA), B-2
- Oracle Directory Manager, 1-7, 7-2
  - 「Apply」ボタンと「OK」ボタンの比較, 4-6
  - 「Cancel」ボタン, 4-7
  - 「Create Access Control Policy Point」メニュー, 4-8
  - 「Create Entry」メニュー項目, 4-8
  - 「Create Like」ボタン, 4-9, 7-7
  - 「Create」ボタン, 4-9
  - 「Delete」ボタン, 4-9
  - Directory Server からの切断, 4-7
  - Directory Server への接続, 4-7, 4-9
  - 「Edit」ボタン, 4-9
  - 「Edit」メニュー, 4-7
  - 「Ends With」フィルタ, 6-7
  - 「Exact Match」フィルタ, 6-8, 7-4, 9-20, 9-23
  - 「Exit」メニュー項目, 4-7
  - 「File」メニュー, 4-7
  - 「Find Attributes」ボタン, 6-15
  - 「Find Objects」ボタン, 4-9, 6-6
  - 「Greater or Equal」フィルタ, 6-8, 7-4, 9-20, 9-23
  - 「Help」ボタン, 4-9
  - 「Help」メニュー項目, 4-8
  - 「Less or Equal」フィルタ, 6-8, 7-4, 9-20, 9-24
  - 「Not Null」フィルタ, 6-8
  - 「Operations」メニュー, 4-8
  - 「Present」フィルタ, 7-4
  - Purge Schedule, 設定, 10-12
  - 「Refresh Entry」ボタン, 4-9
  - 「Refresh Subtree Entries」ボタン, 4-9
  - 「Refresh」ボタン, 4-9
  - 「Revert」ボタン, 4-7
  - Sun Solaris での起動, 4-2
  - 「Tear-Off」メニュー項目, 4-7
  - 「View」メニュー, 4-7
  - アクセス権限の付与, 9-15
  - エントリの管理, 4-10
  - エントリの変更, 7-9
  - オブジェクト・クラスの作成, 4-8
  - オブジェクトの削除, 4-7, 4-9
  - 概要, 4-2
  - 管理
    - ACP, 4-10
    - エントリ, 4-10
    - オブジェクト・クラス, 6-6
    - 構成設定エントリ, 5-4
  - 起動, 4-2
  - 検索
    - エントリ, 7-2
    - オブジェクト, 4-9
    - 属性, 6-15
  - 検索基準バー, 7-3
  - 検索のルート, 7-2
  - 検索フィルタ, 6-7
  - 更新, 4-7
    - サブツリー・エントリ・データ, 4-9

- 構成設定エントリの削除, 5-4
- 構成設定エントリの変更, 5-4
- 実行方法, 4-2
- スキーマの管理, 4-10
- 属性構文の型の選択, 6-25
- 属性の型のリスト, A-3
- 属性の検索, 6-15
- 属性の作成, 4-8
- 追加
  - ACP, 9-26
  - エントリ, 7-6
  - オブジェクト, 4-7
  - オブジェクト・クラス, 6-9
  - グループ・エントリ, 7-8
  - 構成設定エントリ, 5-4
  - 属性, 6-18
- ツールバー, 4-9
- ナビゲート, 4-6
- 表示
  - エントリの属性, 7-5
- ヘルプ・ナビゲータの表示, 4-8
- 変更
  - オブジェクト, 4-7, 4-9
  - オブジェクト・クラス, 6-11
  - 構成設定エントリ, 2-22
  - レプリケーション承諾, 10-15
  - メニュー・バー, 4-7
  - 類似項目の作成操作, 4-7
- Oracle Directory Manager の「Connect/Disconnect」ボタン, 4-9
- Oracle Directory Manager の起動, 4-2
- Oracle Directory Manager のナビゲート, 4-6
- Oracle Directory Replication Server, 1-7, 2-20
  - 起動, 3-6, 10-18, A-32, A-33
  - 停止, 3-7, A-33
- Oracle Directory Server, 1-7, 2-19, 2-20
- Oracle Directory Server インスタンス, 2-21
  - 起動, 3-5, A-31
  - 停止, 3-5, A-31
- Oracle Directory Version, 5-13
- Oracle Internet Directory で施行されている RFC, E-2
- Oracle Internet Directory のノード, 2-18
- Oracle NLS, 2-17
- Oracle SQL\*Loader, bulkload で使用, A-22
- Oracle Wallet, E-6
  - 位置の変更, 5-6, 5-7, 5-9, 8-4, E-6
- Oracle Wallet Manager, 2-13
- Oracle8i, 2-23
  - アドバンスト・レプリケーション, 2-26
  - データベース, 2-20
- Oracle8i Replication Manager, アドバンスト・レプリケーションの構成, 10-3
- Oracle インスタンス, 10-6
- Oracle コール・インタフェース, 2-23
- Oracle データ・サーバー
  - エラー, G-2
  - パスワードの変更, 4-13
- Oracle データベース・サーバー, パスワードの変更, 5-30
- Oracle のフォアグラウンド・プロセス
  - CPU のチューニング, 15-5
  - 制限, 15-6
- Oracle バックグラウンド・プロセス, 15-10
- orclACI, 9-2, E-3
  - top 内のオプション属性, 2-9
  - アクセス, 9-2
- orclAgreementID, 10-15, 10-16
- orclAgreementId, E-3
- orclauditattribute, E-4
- orclAuditLevel, E-4
- orclauditlevel 操作属性, 5-22, 5-24
- orclauditlevel 属性, 5-27
- orclauditmessage, E-4
- orclauditmessage 属性, 5-25
- OrclAuditOC, E-4
- orclauditoc オブジェクト・クラス, 5-25
- orclauditoc 属性, 5-25
- orclCatalogEntryDN, E-4
- orclChangeLogLife, 10-11
- orclChangeRetryCount, 10-11, 10-14, E-3
- orclConfigSet, E-4
- orclconfigsetnumber, E-4
- orclConsumerReference, E-3
- orclcontainerOC, E-4
- orclCryptoScheme 属性, 5-14
- orclDBType, E-4
- orclDebugLevel, E-4
- orcldebuglevel 構成設定エントリ, E-4
- orclDirReplGroupAgreement, 10-11, E-3
- orclDirReplGroupDSAs, 10-10, 10-17, 10-18, E-3
- orclDITRoot, E-4
- orclEntryLevelACI, 9-3, E-3
  - top 内のオプション属性, 2-9
- orcleventLog, E-4

orclEvents, E-4  
orcleventtime, E-4  
orcleventtime 属性, 5-25  
orcleventtype, E-4  
orcleventtype 属性, 5-25  
orclExcludedNamingcontexts, 10-16, E-3  
orclGuid, E-3  
    top 内のオプション属性, 2-9  
orclGuName, E-4  
orclguname 属性, 5-21  
orclGuPassword, E-4  
orclgupassword 属性, 5-21  
orclhostname, E-4  
orclIndexedAttribute, E-4  
orclIndexOC, E-4  
orclLDAPInstance, E-4  
orclLDAPSubConfig, E-4  
ORCLMAXCC, 15-4  
orclMaxCC, E-4  
orclmaxcc, 2-21  
orclmaxcc 構成設定エントリ, E-5  
orclOpResult, E-4  
orclopresult 属性, 5-25  
orclParentGUID, E-3  
orclPrivilegeGroup, 7-8  
orclPrName, E-4  
orclprname 属性, 5-21  
orclPrPassword, E-4  
orclprpassword 属性, 5-21  
orclPurgeSchedule, 10-11, 10-13, E-3  
orclReplAgreementEntry, E-3  
orclReplBindDN, E-3  
orclReplBindPassword, E-3  
orclReplicationProtocol, 10-17, E-3  
orclREPLInstance, E-4  
orclREPLSubConfig, E-4  
orclSequence, E-4  
orclsequence 属性, 5-25, 5-26  
orclServerEvent, E-4  
orclServerMode, E-4  
orclServerMode 属性, 5-14  
ORCLSERVERPROCS, 15-4  
orclServerProcs, E-4  
orclserverprocs, 2-21  
orclserverprocs 構成設定エントリ, E-5  
orclSizeLimit, E-4  
orclSizeLimit 属性, 5-14

orclssl authentication 構成設定エントリ, E-5  
orclsslAuthentication, E-4  
orclsslEnable, E-4  
orclsslenable, E-5  
orclsslenable 構成設定エントリ, E-5  
orclsslPort, E-4  
orclsslport 構成設定エントリ, E-5  
orclsslVersion, E-4  
orclsslWalletPasswd, E-4  
orclsslwalletpasswd 構成設定エントリ, E-6  
orclsslWalletURL, E-4  
orclsslwalleturl 構成設定エントリ, E-6  
orclSuffix, E-4  
orclSuName, E-4  
orclsuname 属性, 5-21  
orclSuPassword, E-4  
orclsupassword 属性, 5-21  
orclSupplierReference, E-3  
orclThreadsPerSupplier, 10-11  
orclTimeLimit, E-4  
orclTimeLimit 属性, 5-14  
orclUpdateSchedule, 10-17, E-3  
orclUseEncrypt, E-4  
orcluserdn, E-4  
orcluserdn 属性, 5-25  
organizationalUnitName, 2-5  
organization 属性, 2-5  
o 属性, 2-5

---

## P

PKI 認証, 2-16  
「Present」フィルタ、Oracle Directory Manager, 7-4  
Process Instance Location, 5-13  
Purge Schedule、Oracle Directory Manager を使用した設定, 10-12

---

## Q

Query Entry Return Limit, 5-13

---

## R

Radicati, Sara, xxiii  
RAID, 15-9  
RC4\_40 暗号化, 2-16  
RDN, 「相対識別名 (RDN)」を参照

REDO ログ・バッファ・パラメータ, 15-11  
referral オブジェクト・クラス, 7-17  
「Refresh Entry」ボタン、Oracle Directory Manager, 4-9  
「Refresh Entry」メニュー項目, 4-8  
「Refresh Subtree Entries」ボタン、Oracle Directory Manager, 4-9  
「Refresh Subtree Entries」メニュー項目, 4-8  
「Refresh」ボタン、Oracle Directory Manager, 4-9  
ref 属性, 7-17  
「Revert」ボタン、Oracle Directory Manager, 4-7

## S

SASL, 「Simple Authentication and Security Layer (SASL)」を参照  
「Schema Management」ペイン、Oracle Directory Manager, 6-9  
「Search ACPs」ボタン, 4-9  
「Search ACPs」メニュー項目, 4-8  
Secure Hash Algorithm (SHA), 5-13, 5-14, 5-16  
Secure Sockets Layer (SSL)  
    Oracle Directory Manager で使用可能にする方法, 4-5  
    構成, 4-3  
server mode, 5-14  
Server Operation Time Limit, 5-14  
SGA, 「システム・グローバル領域 (SGA)」を参照  
SHA, 5-13, 5-14, 5-16, F-4  
SHA (Secure Hash Algorithm)、パスワード暗号化, 2-17  
Siemens DirXMetahub, 2-43  
Simple Authentication and Security Layer (SASL)、LDAP バージョン 3, 1-5  
sn 属性, 2-5  
SPECint\_rate95 ベースライン, 14-12, 14-13  
sqlnet.ora、レプリケーション用の構成, 10-4  
SSL, 4-5  
    Cipher Suite, 8-2  
        Oracle Internet Directory でサポート, 8-2  
        SSL\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA, 8-2  
        SSL\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5, 8-2  
        SSL\_RSA\_WITH\_NULL\_MD5, 8-2  
        SSL\_RSA\_WITH\_NULL\_SHA, 8-2  
    orclsslwalleturl パラメータの変更, 5-6, 5-7, 5-9, 8-4, E-6

Wallet, 2-13, E-5, E-6  
    位置の変更, 5-6, 5-7, 5-9, 8-4, E-6  
    パスワードの変更, 5-6, 5-8, 5-9, 8-4, E-6  
オン・オフの切替え, E-5  
強化認証, 2-16  
クライアントとサーバーの認証, 2-12, E-5  
    アクセス制御の対象, 9-21, 9-24  
クライアントの使用例, 8-2  
構成, 4-3  
構成パラメータ, 8-2  
    変更, 8-3  
コンポーネント, 2-13  
サーバー認証, 2-12  
    アクセス制御の対象, 9-21, 9-24  
使用可能, 8-2, A-5, A-7, A-8, A-13, A-17, E-5  
使用不可, E-5  
属性値, E-4  
データ・プライバシー, 1-8  
デフォルト・ポート, 2-14, E-5  
動作, 2-14  
認証, 9-7  
    Oracle Directory Manager, 4-6  
    サーバー, 4-6  
    サーバーのみ, 4-6  
認証アクセス, 1-8  
認証なし, 2-12, 4-6, E-5  
    アクセス制御の対象, 9-21, 9-24  
バージョン 2, 8-2  
バージョン 3, 8-2  
パスワード, 4-5  
パラメータ, 8-2  
    ハンドシェイク, 2-14, 8-2  
    ポート 636, 8-2  
SSL 使用不可, E-5  
SSL を使用可能にする, 8-2  
subconfig, E-4  
subregistry, E-4  
subSchemaSubentry  
    オブジェクト・クラスの追加, 2-11  
    スキーマ定義の保持, 2-11  
    変更, 2-11  
Sun Solaris、Oracle Directory Manager の起動, 4-2  
「Super User Login」イベント, 5-26  
surname 属性, 2-5  
SYSTEM システム, 14-10

## T

---

targetDN, E-3  
TCP/IP 接続, 16-5, 16-8, E-5  
Tear-Off, Oracle Directory Manager, 4-7  
tnsnames.ora  
    コールド・バックアップ, B-7  
    レプリケーション用の構成, 10-4  
top オブジェクト・クラス, 2-8  
    オプション属性, 2-9  
top ユーティリティ, 15-2  
Transport Layer Security (TLS)、LDAP バージョン 3,  
    1-5  
「tree view」  
    検索のルートの選択, 7-2  
    ブラウズ, 7-2

## U

---

Unicode Transformation Format 8-bit (UTF-8), 2-17  
UNIX Crypt, 5-13, 5-14, 5-16, F-4  
    パスワード暗号化, 2-17  
UNIX、Oracle Directory Manager の起動, 4-2  
「User password modification」イベント, 5-27  
「User Preferences」ボタン, 4-9  
「User Preferences」メニュー項目, 4-8  
userPassword 属性、ハッシュ値, F-4  
「User」フィールド、Oracle Directory Manager, 4-3  
UTF-8, 「Unicode Transformation Format 8-bit」を  
    参照  
UTLBSTAT.SQL, 15-2  
UTLESTAT.SQL, 15-2

## V

---

「View」メニュー、Oracle Directory Manager, 4-7  
vmstat ユーティリティ, 15-2

## W

---

Wallet  
    SSL, E-6  
    位置, E-6  
    位置の変更, 5-6, 5-7, 5-9, 8-4, E-6  
    オープン, C-5  
    管理, C-3  
    クローズ, C-5

削除, C-6  
作成, 5-6, 5-8, 5-9, 8-4, C-4, E-6  
自動ログイン, C-7  
証明書の管理, C-8  
信頼されている証明書の管理, C-11  
定義, 2-13  
パスワード, 4-5  
    変更, 5-6, 5-8, 5-9, 8-4, E-6  
    パスワードの変更, C-7  
    保存, C-5  
Windows NT タスク マネージャ, 15-2  
Windows NT パフォーマンス モニタ, 15-2  
Windows NT、Oracle Directory Manager の起動, 4-2

## X

---

X.509 バージョン 3、証明書, 2-13

## あ

---

アーキテクチャ  
    Oracle Internet Directory, 2-1  
アクセス  
    violation イベント, 5-27  
    オブジェクト, 9-6  
    権限、Oracle Directory Manager を使用して設定,  
        9-21, 9-25  
    種類, 9-8  
    選択、DN による, 9-33  
    操作, 9-8  
    対象, 9-7  
    付与  
        Oracle Directory Manager を使用, 9-15  
        エントリ・レベル、Oracle Directory Manager を  
            使用, 9-30  
        エントリ・レベル、コマンドライン・ツールを  
            使用, 9-32  
        コマンドライン・ツールを使用, 9-31  
        サブツリー, 9-21, 9-25  
        すべての人、Oracle Directory Manager を使用,  
            9-21, 9-25  
        特定のグループ、Oracle Directory Manager を  
            使用, 9-21, 9-25  
未指定, 9-9, 9-25  
レベル、LDAP 操作に必要, 9-14

- アクセス項目
  - 構造型, 9-18
  - コンテンツ, 9-18
- アクセス制御, 1-8, 2-11, 2-15, 9-1
  - SSL クライアントとサーバーの認証, 9-21, 9-24
  - SSL サーバー認証, 9-21, 9-24
  - SSL 認証なし, 9-21, 9-24
  - 簡易, 9-21, 9-24
  - 管理
    - Oracle Directory Manager を使用, 9-15
    - コマンドライン・ツールを使用, 9-31
  - 設定、ワイルド・カードを使用, 9-33
  - 認証なし, 9-21, 9-24
  - ポリシー
    - 競合, 9-3
    - 継承, 9-3
- アクセス制御項目 (ACI)
  - 構文, D-1
  - コンポーネント, 9-5
  - 書式, D-1
  - 属性, 2-15
  - ディレクティブのオブジェクト, 9-6
  - ディレクティブの対象, 9-7
- アクセス制御ディレクティブ書式, 「ACI ディレクティブ書式」を参照
- アクセス制御の規定, 9-2
- アクセス制御ポリシーの競合, 9-3
  - 解消するための優先順位規則, 9-3
- アクセス制御リストの処理, 5-23
- アクティブ・サーバー・インスタンス
  - 構成設定エントリの変更, 5-4
  - 表示, 5-4
- アドバンスト・レプリケーション, 2-26
  - Oracle8i とともにインストール, 10-3
  - インストール, 10-3
  - 構成, 10-7
    - Oracle8i Replication Manager を使用, 10-3
  - 設定, 10-3
- アプリケーション情報、属性, 2-4
- 暗号化, 2-14
  - DES40, 2-16
  - Oracle Internet Directory で使用可能なレベル, 2-16
  - RC4\_40, 2-16
  - パスワード, 2-16, 5-16
    - MD4, 2-16
    - MD5, 2-16
    - SHA, 2-17

- UNIX Crypt, 2-17
- デフォルト, 2-16
- パスワードのオプション, 2-16

## い

---

- 移行、他の LDAP ディレクトリから, F-2
- 以前のリリースからのアップグレード, 3-9
  - 単一ノード環境, 3-9
  - マルチノード環境, 3-9
- 位置の識別
  - 識別名を使用したディレクトリ・エントリの位置の識別, 2-3
- 一致規則
  - Oracle Directory Manager のタブ, 6-9
  - Oracle Internet Directory で認識, E-9
  - subSchemaSubentry への追加不可, 2-11
  - スキーマ内のメタデータとして, 2-11
  - スキーマに格納, 2-11
  - 属性, 2-6
- イベント、監査可能, 5-26
- インストール
  - アドバンスト・レプリケーション, 10-3
  - ディレクトリ・レプリケーション・グループ (DRG), 10-2
- インストール時のエラー, G-2
- インテリジェント・クライアントのフェイルオーバー, 13-6
- 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, 13-6

## え

---

- エージェント、メタディレクトリ, 2-42
- エラー
  - インストールेशन, G-2
  - データベース・サーバー, G-2
- エラー・メッセージ
  - その他, G-6
  - 標準, G-2
- エンティティ、アクセス権限の付与, 9-21, 9-24
- エントリ
  - ACI に関連付けられているオブジェクト, 9-6
  - DN による選択, 9-33
  - 位置の識別, 2-3
  - オブジェクト・クラスの割当て, 6-3
  - 親, 6-3



- 概念の説明, 2-2
- 監査ログ, 5-24
  - 検索, 5-25
- 管理
  - Oracle Directory Manager を使用, 4-10
  - コマンドライン・ツールを使用, 7-10
- グループ, 2-5
- 検索
  - 1 レベル, 7-3
  - ldapsearch を使用, A-17
  - Oracle Directory Manager を使用, 7-2
  - 検索の深さの指定, 7-3
  - サブツリー・レベル, 7-3
  - ベース・レベル, 7-3
- 削除
  - ldapdelete を使用, 4-11, 7-11, A-10
  - ldapmodify を使用, A-15
- 識別名, 2-2
- スーパー・クラス、選択, 7-6
- 属性の継承, 6-3
- 属性の表示, 7-5
- 追加
  - bulkload を使用, A-22
  - ldapaddmt を使用, 4-11, 7-11, A-6
  - ldapadd を使用, 4-11, 7-11, A-4
  - Oracle Directory Manager を使用, 7-6
  - オプション属性, 7-6
  - 親に対する書き込みアクセス権限が必要, 7-6
  - 既存エントリをコピー, 7-7
  - 同時, 4-11, 7-11
  - 必須属性, 7-6
  - 他のアプリケーション, A-22
- 特定、アクセス権限の付与, 9-21, 9-25
- ネーミング, 2-2, 13-2
- 比較、ldapcompare を使用, 4-11, 7-11
- 表示, 7-2
- フィルタ, 9-19, 9-23
- 変更
  - LDAP 規則, 7-9
  - 規則, 7-9
  - 多数, A-24
  - 同時、ldapmodifymt を使用, A-16
- 変更規則, 7-9
- ユーザー
  - 追加、ldapadd を使用, 7-12
  - 追加、Oracle Directory Manager を使用, 7-7

- 変更、ldapmodify を使用, 7-12
- 変更、Oracle Directory Manager を使用, 7-10
- ロード, 6-3
- エントリへのオブジェクト・クラスの割当て, 6-3
- エントリ・レベルの競合、レプリケーション, 2-28

## お

---

- オープン・カーソル・パラメータ, 15-9
- オブジェクト
  - ACI ディレクティブ, 9-6
  - 検索、Oracle Directory Manager を使用, 4-9
  - 追加、Oracle Directory Manager を使用, 4-9
  - 比較, 4-7
- オブジェクト ID、オブジェクト・クラス, 6-6
- オブジェクト・クラス, 2-7
  - extensibleObject, 7-17
  - groupOfNames, 7-8
  - LDIF ファイル, A-2
  - Oracle Directory Manager のタブ, 6-9
  - orclauditoc, 5-25
  - top, 2-8
  - 一意のオブジェクト ID, 6-4
  - 一意名, 6-4
  - エントリへの割当て, 6-2, 6-3
- 管理
  - コマンドライン・ツールを使用, 6-12
- 規則, 2-9
- 検索, 6-6
- 構造型の変換, 6-5
- 削除、Oracle Directory Manager を使用, 6-12
- 作成、Oracle Directory Manager を使用, 4-8
- サブクラス, 2-8
  - 定義, 2-7
- 参照 (referral), 7-17
- スーパー・クラス, 2-8, 6-9
- スーパー・クラスの削除, 6-5
- スキーマ内のメタデータとして, 2-11
- 増加, 6-4
- 属性の削除, 6-5
- タイプ, 2-8
- 追加, 6-2, 6-3
  - Oracle Directory Manager を使用, 6-9
  - コマンドライン・ツールを使用, 6-12
  - 同時、ldapaddmt を使用, A-6
- 定義, 2-7
- 必須属性の再定義, 6-4

- 表示, 6-9
- ベース・スキーマ, 6-5
- 変更, 6-4
  - Oracle Directory Manager を使用, 6-11
  - コマンドライン・ツールを使用, 6-12
- 補助型の変換, 6-4
- オブジェクト・クラス型
  - 構造型, 2-8, 2-9
  - 抽象型, 2-8
  - 補助型, 2-9
- オブジェクト・クラスの説明, 6-7
- オブジェクト・クラスの増加, 6-4
- オブジェクト・クラスの定義, 2-7
- オプション
  - 属性, 2-7
- オプション属性, 2-7, 6-3
  - 値の入力, 7-6
  - オブジェクト・クラス, 6-7
  - 事前定義オブジェクト・クラスへの追加, 2-7
- オンライン管理ツール, 「Oracle Directory Manager」を参照

## か

---

- ガイドライン
  - 属性の削除, 6-15
  - 属性の追加, 6-14
  - 属性の変更, 6-15
- 概念、LDAP, 2-1
- 各国語サポート (NLS)
  - bulkdelete, 12-9
  - bulkload, 12-8
  - bulkmodify, 12-9
- Java クライアント, 2-18
- ldapadd, 12-6
- ldapaddmt, 12-6
- ldapbind, 12-6
- ldapcompare, 12-7
- ldapdelete, 12-7
- ldapmoddn, 12-7
- ldapmodify, 12-6
- ldapmodifymt, 12-6
- ldapsearch, 12-6
- ldifwrite, 12-8
- Oracle Internet Directory の設定, 12-2
- コマンドライン・ツール, 12-5
- 拡張性
  - LDAP バージョン 3, 1-5
  - Oracle Internet Directory, 1-8
- 仮想ディレクトリ, 2-42
- 仮想メモリー, 14-11
- 型
  - オブジェクト・クラス, 6-7
  - 属性, 2-4
- カタログ化属性
  - orcleventtype, 5-25
  - orcluserdn, 5-25
- カタログ管理ツール, 4-13, 6-23, 6-26
- ガベージ・コレクション, 2-27
  - レプリケーション, 10-11
- 可用性, 高い, 16-7
- 簡易認証, 1-8, 2-12
  - アクセス制御の対象, 9-21, 9-24
- 環境変数 NLS\_LANG
  - 設定, 12-2
- 環境変数、NLS\_LANG, 12-2
- 監査可能なイベント, 5-26
- 監査レベル, 5-26
- 監査ログ, 5-24
  - エントリ
    - DIT における位置, 5-26
    - 検索, 5-24, 5-25
    - 表示, 5-24
  - エントリの構造, 5-25
  - コンテナ・オブジェクト, 5-29
  - サンプル, 5-26
  - 使用方法, 5-24
  - スキーマ要素, E-4
  - デフォルトの構成, 5-24
  - 問合せ, 5-24
- 監査ログのイベント
  - Access violation, 5-27
  - ACL Modification, 5-27
  - add, 5-27
  - Bind, 5-26
  - DSE modification, 5-27
  - modify, 5-27
  - ModifyDN, 5-27
  - Replication Login, 5-27
  - Schema element
    - Add/Replace, 5-26
    - delete, 5-26
  - User password modification, 5-27

- 削除, 5-27
- スーパー・ユーザー
  - ログイン, 5-26
- 選択, 5-27
- 管理
  - エントリ
    - Oracle Directory Manager を使用, 4-10, 7-2
    - コマンドライン・ツールを使用, 7-10
  - オブジェクト・クラス
    - コマンドライン・ツールを使用, 6-12
  - 構成設定エントリ, 5-2
  - 属性
    - Oracle Directory Manager を使用, 6-15
    - 概要, 6-14
    - コマンドライン・ツールを使用, 6-24
  - ディレクトリ・スキーマ, 6-1
  - ナレッジ参照、権限の制限, 2-40
- 管理者操作キュー操作ツール, 4-14, 10-30
- 管理ツール, 4-11, 7-11
  - bulkdelete, A-21
  - bulkload, A-22
  - bulkmodify, A-24
  - ldapadd, 4-11, 7-11, A-4
  - ldapaddmt, A-6
  - ldapbind, A-7
  - ldapcompare, A-8
  - ldapdelete, 4-11, 7-11, A-10
  - ldapmoddn, 4-11, 7-11, A-11
  - ldapmodify, 4-11, 7-11, A-12
  - ldapmodifymt, 4-11, 7-11, A-16
  - ldapsearch, A-17
  - ldifwrite, A-26
  - OID データベース・パスワード・ユーティリティ, 4-13
  - Oracle Directory Manager, 4-2
  - カタログ管理, 4-13
  - コマンドライン, 1-7, 4-11
  - バルク・ツール, 4-12

## き

---

- 規則、LDIF, A-3
- 規定のアクセス制御, 9-2
- 起動
  - Directory Server, 3-4, 4-16, A-30
  - デフォルトの構成を使用, 3-8, A-34
  - LDAP サーバー・インスタンス, 3-4

- OID モニター, 3-2, 3-3, A-28, A-29
- Oracle Directory Manager, 4-2
  - Sun Solaris, 4-2
  - UNIX, 4-2
  - Windows 95, 4-2
  - Windows NT, 4-2
- Oracle Directory Replication Server, 3-6, 10-18, A-33
- Oracle Directory Server, 3-4
- Oracle Directory Server インスタンス, 10-10, A-30
- Replication Server インスタンス, A-32
- 機能、新, xxv
  - Oracle Wallet Manager, C-1
- 強化認証, 2-12
- 競合の手動解消, 10-29
- 競合、レプリケーション
  - 一般的な原因, 2-29
- エントリ・レベル, 2-28
- 解消, 2-28, 9-11
  - 手動, 10-29
  - メッセージ, 10-29
- 自動解消, 2-29
- 手動解消, 10-29
- 属性レベル, 2-29
- 共有ルール・サイズ, 15-7
- パラメータ, 15-9

## く

---

- クライアントとサーバーの認証、SSL, E-5
- クライアントのフェイルオーバー・オプション, 16-4
- グループ
  - Oracle Directory Manager を使用したアクセス権限の付与, 9-21, 9-25
  - 権限, 9-4
- グループ・エントリ, 2-5
- 作成
  - ldapmodify を使用, A-14
  - Oracle Directory Manager を使用, 7-8
- 追加, 7-8

## け

---

- 継承, 2-8
  - アクセス制御ポリシー, 9-3
- スーパー・クラス, 6-3, 6-9
- 属性, 6-9

- ゲスト・ユーザー
  - 定義, 5-19
  - ユーザー名とパスワードの管理, 5-19
- 権限, 2-11, 2-13, 2-15
  - 付与
    - Oracle Directory Manager を使用, 9-15
    - コマンドライン・ツールを使用, 9-31
- 権限グループ, 9-4
- 検索
  - エントリ, 7-2
    - 1 レベル, 7-3
    - ldapsearch を使用, A-17
    - 検索の深さ, 7-3
    - 検索のルート, 7-2
    - サブツリー・レベル, 7-3
    - ベース・レベル, 7-3
  - エントリの最大数の指定, 7-3
- オブジェクト
  - Oracle Directory Manager を使用, 4-9
- オブジェクト・クラス, 6-6
- 監査ログ・エントリ, 5-24, 5-25
- 構成
  - ldapmodify を使用, 5-18
  - Oracle Directory Manager を使用, 5-17
- 最大時間, 7-3
- 最大時間の設定
  - ldapmodify を使用, 5-18
  - Oracle Directory Manager を使用, 5-18
- 属性
  - Oracle Directory Manager を使用, 6-15
  - 属性を使用可能にする方法, 6-23
- フィルタを使用, 6-7
- 戻されるエントリの最大数の設定
  - ldapmodify を使用, 5-18
  - Oracle Directory Manager を使用, 5-17
- 検索および比較操作, 2-6
- 検索基準バー, Oracle Directory Manager, 7-3
- 検索結果, エントリの最大数の指定, 7-3
- 検索の最大時間、指定, 7-3
- 検索の深さ、指定, 7-3
- 検索のルート
  - 選択, 7-2
  - 入力, 7-2
- 検索のルートの選択, 7-2

- 検索フィルタ
  - IETF 準拠, A-17
  - ldapsearch, A-19
- 検索フィルタの処理, 5-23

## こ

- 公開鍵, 2-13
- 公開鍵インフラストラクチャ, 2-16
- 更新
  - Oracle Directory Manager, 4-7
  - エントリ・データ, Oracle Directory Manager を使用, 4-9
  - サブツリー・エントリ・データ, Oracle Directory Manager を使用, 4-9
  - 属性、ldapmodify を使用, 4-11, 7-11
  - データ, 4-9
- 構成
  - SSL, 4-3, 8-2
  - アドバンスド・レプリケーション, 10-3
    - Oracle8i Replication Manager を使用, 10-3
  - サーバー・パラメータ
    - Oracle Directory Manager を使用, 4-15
    - コマンドライン・ツールを使用, 4-15
  - サーバー、入力ファイルを使用, 7-11
  - ディレクトリ・レプリケーション・グループ (DRG), 10-2
  - レプリケーション, 10-10
    - 承認, 10-10, 10-14
- 構成設定エントリ, 2-22
  - Directory Server プロセス, E-5
  - LDIF ファイル, 5-10
  - orcldebuglevel, E-4
  - orclmaxcc, E-5
  - orclserverprocs, E-5
  - orclssl authentication, E-5
  - orclsslenable, E-5
  - orclsslport, E-5
  - orclsslwalletpasswd, E-6
  - orclsslwalleturl, E-6
  - Replication Server, 10-11
  - SSL 使用不可, E-5
  - SSL パラメータ, 8-2
  - 管理, 4-15, 5-2
    - Oracle Directory Manager を使用, 5-4
    - コマンドライン・ツールを使用, 5-10
  - 異なるものを使用, 5-2

- 削除, 5-2
  - Oracle Directory Manager を使用, 5-4
- 使用せずに Directory Server を起動, 3-8
- 追加, 2-22, 5-2
  - Oracle Directory Manager を使用, 5-4
  - コマンドライン・ツールを使用, 7-11
- データベース接続, E-5
- デバッグ・レベル, E-4
- 複数使用, 8-2
- 変更, 3-7, 5-2, 5-11, A-34
  - Oracle Directory Manager を使用, 5-4, 5-8
  - アクティブ・サーバー・インスタンス, 5-4
  - コマンドライン・ツールを使用, 7-11
- ユーザー指定のオーバーライド, 3-8, A-34
- 構成設定, 「構成設定エントリ」を参照
- 構成ファイルの処理, 5-23
- 構造型アクセス項目, 9-18
  - アクセス制御ポイント, 9-18
- 構造型オブジェクト・クラス型, 2-8, 2-9
- 構造型オブジェクト・クラス, 変換, 6-5
- 構造、監査ログ・エントリ, 5-25
- 構文
  - bulkdelete, A-21
  - bulkload, A-22
  - bulkmodify, A-24
  - LDAP, E-6
  - ldapadd, A-4
  - ldapaddmt, A-6
  - ldapbind, A-7
  - ldapcompare, A-8
  - ldapdelete, A-10
  - ldapmoddn, A-11
  - ldapmodify, A-12
  - ldapmodifymt, A-16
  - ldapsearch, A-17
  - LDIF, A-2
  - ldifwrite, A-26
  - oidctl, A-30
  - OID 制御ユーティリティ, A-30
  - OID モニター, A-28
  - Oracle Directory Manager のタブ, 6-9
  - subSchemaSubentry への追加不可, 2-11
  - カタログ管理ツール, A-27
  - コマンドライン・ツール, A-4
  - スキーマに格納, 2-11
  - バルク・ツール, A-21
- 構文、属性, 2-6

- コールド・バックアップ, B-1
- 国際化対応、LDAP, 12-1
- コマンドライン・ツール, 1-7
  - ldapadd, 4-11, 7-11, A-4
  - ldapaddmt, 4-11, 7-11, A-6
  - ldapbind, A-7
  - ldapcompare, A-8
  - ldapdelete, 4-11, 7-11, A-10
  - ldapmoddn, 4-11, 7-11, A-11
  - ldapmodify, 4-11, 7-11, A-12
  - ldapmodifymt, 4-11, 7-11, A-16
  - ldapsearch, A-17
- NLS を設定, 12-5
- 概要, 4-11
- カタログ管理, 6-23
- 管理
  - エントリ, 7-10
  - 属性, 6-24
- 構文, A-4
- 索引付け, 6-23, 6-26
- 属性値の比較, 7-11
- 追加
  - 構成設定エントリ, 2-22, 7-11
- 変更
  - 構成設定エントリ, 7-11
- コマンドライン・モードのコマンドのバッチ処理, 6-12
- コンシューマ・サーバー, 2-23, 2-27, 2-30
- コンテンツ・アクセス項目, 9-18
  - アクセス制御ポイント, 9-18
- コンポーネント
  - Directory Server, 2-18
  - SSL, 2-13

## さ

---

- サーバー
  - 構成、入力ファイルを使用, 7-11
  - 接続, 4-4
  - ディレクトリ, 1-7
    - 接続, 4-3
  - パラメータ、構成, 4-15
  - プロセス, 2-21
    - 複数, 2-21
  - レプリケーション, 1-7

- サーバー・インスタンス
  - 実行方法, 4-2
  - 保護モードで実行, 8-2
- サーバー認証、SSL, 2-12, 4-6, E-5
- サーバーの起動コマンド, 5-2
  - OID 制御ユーティリティを使用, 4-13
- サーバーの停止コマンド, 4-13
- サーバー・プロセス
  - 数, E-5
  - 過多, 15-4
- 再起動
  - Directory Server, 3-7, 5-4, A-33
  - ディレクトリ・データベースのリスナー, 10-6
- サイズ
  - 属性値, E-8
  - データベース・キャッシュ, 13-9
- サイズ設定, 13-6, 13-8
  - I/O サブシステム, 14-5
  - 表領域, 14-8
- 索引
  - bulkload により作成, 7-15
  - 属性からの削除
    - Oracle Directory Manager を使用, 6-24
- 索引付き属性, 6-24
  - Oracle Directory Manager で表示, 6-9
  - orcleventtype, 5-25
  - orcluserdn, 5-25
  - 場所, 5-13
- 索引付け
  - カタログ管理ツールを使用, 6-26
  - 属性, 6-23, 6-26
    - Oracle Directory Manager を使用, 6-23
    - カタログ管理ツールを使用, 6-23
    - コマンドライン・ツールを使用, 6-25
- 削除
  - エントリ, 4-11, 7-11
    - ldapdelete を使用, A-10
    - ldapmodify を使用, A-15
  - オブジェクト
    - Oracle Directory Manager を使用, 4-7, 4-9
    - コマンドライン・ツールを使用, A-10, A-12
  - オブジェクト・クラス
    - Oracle Directory Manager を使用, 6-12
    - ベース・スキーマ, 6-5
    - ベース・スキーマ内外, 6-5
  - オブジェクト・クラスから属性を削除, 6-5
  - 監査ログのイベント, 5-27

- 構成設定エントリ, 5-2
  - Oracle Directory Manager を使用, 5-4
- 属性, 6-15
  - ldapmodify を使用, A-15
  - ガイドライン, 6-15
- 属性からの値の削除、ldapmodify を使用, A-14
- ベース・スキーマの属性, 6-15
- 変更ログ, 2-27
  - 時間ベース, 2-27
  - 変更番号ベース, 2-27
- 作成
  - Access Control Policy Points、Oracle Directory Manager を使用, 4-8
  - LDIF 入力ファイル, 5-10
  - Wallet, 5-6, 5-8, 5-9, 8-4, E-6
  - オブジェクト・クラス、Oracle Directory Manager を使用, 4-8
  - 新規エントリ
    - Oracle Directory Manager を使用, 4-8, 7-6
  - 属性
    - ldapmodify を使用, 4-11, 7-11
    - Oracle Directory Manager を使用, 4-8
  - 表領域, 10-5
  - 類似項目の作成操作を使用した類似エントリの作成, 7-7
  - ロールバック・セグメント, 10-5
- サブエントリ、定義, 2-11
- サブクラス, 2-8
- サブツリー
  - アクセス権限の付与, 9-21, 9-25
- サブツリーの表示, 7-2
- サブツリー・レベルの検索, 7-3
- サブライヤ, 2-23, 2-29
- 参照
  - 「ナレッジ参照」を参照

## し

---

- 時間ベースの変更ログの削除, 2-27
- 識別名, 2-2
  - LDIF ファイル, A-2
  - コンポーネント, 2-3
  - 書式, 2-2
  - 属性, 7-6
  - 変更, 4-11, 7-11
    - ldapmoddn を使用, 4-11, 7-11
    - コマンドライン・ツールを使用, 7-11

- 識別名 (DN) を変更
  - ldapmoddn を使用, 7-11
- システム・グローバル領域 (SGA), 10-6, 14-11, 15-6, 15-7
  - Oracle8i 用のチューニング, 15-7
  - サイズ設定, 15-7
  - チューニング・パラメータ, 15-11
- システム操作属性, 5-12
  - 設定
    - ldapmodify を使用, 5-14
    - Oracle Directory Manager を使用, 5-13
- 従属ネーミング・コンテキスト, 2-39
- 上位参照, 2-39
- 上位ナレッジ参照, 2-39
- 障害許容度、レプリケーション, 13-6
- 障害の認識とリカバリ、「フェイルオーバー」を参照
- 状態
  - ログ結果, 5-23
- 状態ログ
  - エントリ設定, 5-23
  - 接続, 5-23
  - 操作, 5-23
- 承諾、レプリケーション, 2-25
- 冗長構成, 16-2
  - フェイルオーバー, 13-4
- 冗長リンク, 16-8
- 証明書, 2-12, E-5
  - X.509 バージョン 3, 2-13
  - 管理, C-8
  - 信頼, 2-13
  - 定義, 2-13
  - ユーザー, C-8
  - 要求, 2-13
- 証明書ベースの認証, 2-12
- 書式、識別名, 2-2
- 新規構文、追加, 2-6
- 新機能, xxv
  - Oracle Wallet Manager, C-1
- 信頼されている証明書, 2-13
- 信頼性、レプリケーション, 2-23

## す

---

- スーパー・クラス, 2-8
  - オブジェクト・クラス, 6-7
  - 継承, 6-3
  - 属性, 6-9

- スーパー・クラス・セクタ, 7-6
- スーパー・ユーザー
  - 定義, 5-19
  - ユーザー名とパスワードの管理, 5-19
  - ログイン, 4-3
- スキーマ
  - Definition Location, 5-13
  - subSchemaSubentry 内の定義, 2-11
  - オブジェクト・クラスの追加と変更 (オンライン), 6-2
  - 管理, 6-1
    - Oracle Directory Manager を使用, 4-10
  - 複数の表領域に分散, 15-8
  - 要素, E-1
    - Add/Replace イベント, 5-26
    - delete イベント, 5-26
    - 特定の Oracle 製品, E-3
- スキーマ・オブジェクトの管理、Oracle Directory Manager を使用, 4-10
- スキーマ関連のデバッグ, 5-23
- スクリプト、バッチ処理するコマンドライン・モードのコマンド, 6-12
- スタック、テクノロジー, 16-2
- ステータス変更ログ, 2-30
- ストライプ化, 15-8, 15-9
- すべてのデバッグを使用可能にする, 5-23
- すべての人、アクセス権限の付与, 9-21, 9-25
- スポンサ・ノード, 10-21
  - コールド・バックアップ・プロシージャ, B-3
- スマート・ナレッジ参照, 2-41
  - 構成, 7-18
- スリープ・タイム、OID モニター, 3-2, A-29
- スループット (throughput), 14-5

## せ

---

- 制御、アクセス, 1-8, 9-1
- 制約、オブジェクト・クラス, 2-9
- セキュリティ, 2-11
  - LDAP バージョン 3, 1-5
  - Oracle Internet Directory 環境, 2-11
  - 異なるクライアント, 8-2
  - 異なるクライアントごとの SSL パラメータ, 8-2
- セッション固有のユーザー ID, 2-12
- セッション・パラメータ, 15-9

## 接続

- Directory Server, 2-22, 4-3, 4-4, 4-16
  - Oracle Directory Manager を使用, 4-9

- 管理, 5-23

- 追加の Directory Server, 4-10

- プーリング, 1-8

- 複数の Directory Server, 4-10

- リダイレクション, 16-9

- ソフトウェア・ベース, 16-7

- ネットワークレベル, 16-6

- ハードウェア・ベース, 16-7

- 接続ディレクトリ, 2-42

## 切断

- ボタン, Oracle Directory Manager, 4-7

- メニュー項目, Oracle Directory Manager, 4-7

## 設定

- システム操作属性, 5-12

- デバッグ・ロギング・レベル, 5-22

- OID 制御ユーティリティを使用, 5-22

## 選択

- エントリのスーパー・クラス, 7-6

- 属性構文の型, 6-25

- 選択したイベントの監査, 5-27

- 選択した監査ログのイベント, 5-27

# そ

---

- 操作属性, 5-12

- ACI, 2-15

- 送受信パケットの印刷, 5-23

- 相対識別名 (RDN), 2-3

- 各エントリごとの表示, 7-2

- 変更

- ldapmoddn を使用, 4-11, 7-11

- ldapmodify を使用, A-15

- コマンドライン・ツールを使用, 7-11

- ソート領域パラメータ, 15-11

## 属性

- ACI に関連付けられているオブジェクト, 9-6

- AlternateServers、フェイルオーバー, 16-4

- commonName, 2-5

- DN, 7-6

- jpegPhoto, 2-5, 7-12

- LDIF ファイル, A-2

- NULL 値, 6-3

- objectclass, 5-25

- Oracle Directory Manager のタブ・ページ, 6-9

- orclauditlevel, 5-27

- orclauditmessage, 5-25

- orclauditoc, 5-25

- orcleventtime, 5-25

- orcleventtype, 5-25

- orclopresult, 5-25

- orclsequence, 5-25, 5-26

- orcluserdn, 5-25

- organization, 2-5

- organizationalUnitName, 2-5

- ref, 7-17

- sn, 2-5

- surname, 2-5

## 構文

- 選択, 6-25

- 変更不可, 6-15

- top 内, 2-9

- 値, 2-4

- 変更規則, 7-9

- 値のサイズ, E-8

- 一致規則, 2-6

- オブジェクト・クラスにより判別, 6-3

- オプション, 2-7, 6-3

- 管理, 7-16

- 言語コード, 2-7

- 型, 2-4

## 管理

- Oracle Directory Manager を使用, 6-15

- 概要, 6-14

- コマンドライン・ツールを使用, 6-24

- 継承, 6-3, 6-9

- 検索で使用可能にする方法, 6-23

- 検索, Oracle Directory Manager を使用, 6-15

- 構文, 2-6

- サイズ、値, E-8

- 索引付け, 6-9, 6-24, 6-26

- Oracle Directory Manager を使用, 6-23

- コマンドライン・ツールを使用, 6-25

- 索引の削除, 6-24

- 索引、bulkload により作成, 7-15

- 削除, 6-15, A-15

- 値、ldapmodify を使用, A-14

- ガイドライン, 6-15

- システム操作, 5-12

- 情報の種類, 2-4

- スキーマ内のメタデータとして, 2-11

- 操作, 5-12



- 単一値, 2-5
  - 複数値への変換, 6-15
- 追加, 6-14
  - ldapadd を使用, A-4
  - ldapmodify を使用, 6-24
  - Oracle Directory Manager を使用, 6-18, 6-20
  - ガイドライン, 6-14
  - 既存のエントリ, A-4
  - 同時、ldapaddmt を使用, A-6
- 必須, 2-7, 6-3, 7-9
- 必須の再定義, 6-4
- 必須またはオプションの指定, 6-3
- 表示, 7-5
- 複数値, 2-5, 9-3
  - 単一値への変換, 6-15
- ベース・スキーマ, 6-14
  - 削除, 6-15
  - 変更, 6-15
- 変更
  - ldapmodify を使用, 6-24
  - ガイドライン, 6-15
  - 規則, 6-15
- 属性オプション、管理, 7-16
- 属性からの索引の削除, 5-25, 6-24
- 属性値の置換、ldapmodify を使用, A-15
- 属性の指定、必須またはオプション, 6-3
- 属性レベルの競合, 2-29
- ソフトウェア・ベースの接続リダイレクション, 16-7

## た

---

- 体系規則、Oracle Internet Directory では非強制, 2-9
- 対称型マルチプロセッサ (SMP) システム, 15-6
- 大容量トレースのデバッグ, 5-23
- 高い可用性, 13-6
  - Oracle Internet Directory, 16-1
  - Oracle Internet Directory の機能, 16-7
  - マルチマスター・レプリケーション, 16-7
- 単一値の属性, 2-5
  - 複数値への変換, 6-15

## ち

---

- チェック・モード、LDIF ファイルで実行, F-4
- 蓄積転送、Oracle8i, 2-26
- 中間層
  - プロキシ・ユーザーを使用, 5-19

- 抽象型オブジェクト・クラス, 2-8
  - top, 2-8
  - スーパー・クラス, 6-4
- チューニング, 13-6, 15-1
  - CPU 使用量, 15-3
  - SGA パラメータ, 15-11
  - ツール, 15-2
  - ディスク, 15-8
  - 配置に関する考慮事項, 13-9
  - メモリー, 15-7
- チューニング可能、データベース, 15-9

## つ

---

- 追加
  - ACP, 9-26
    - ldapmodify を使用, 9-31
    - Oracle Directory Manager を使用, 9-26
  - エントリ, 7-6
    - ldapaddmt を使用, A-6
    - ldapadd を使用, 4-11, 7-11, A-4
    - Oracle Directory Manager を使用, 7-6
    - 親に対する書き込みアクセス権限が必要, 7-6, 7-7
    - 既存エントリをコピー, 7-7
    - 同時, 4-11, 7-11, A-6
  - エントリ・レベルの ACI、ldapmodify を使用, 9-32
- オブジェクト
  - Oracle Directory Manager を使用, 4-7, 4-9
  - テンプレートを、使用, 4-9
- オブジェクト・クラス, 6-2, 6-3
  - Oracle Directory Manager を使用, 6-9
  - コマンドライン・ツールを使用, 6-12
- 監査ログ・エントリ, 5-24
- 監査ログのイベント, 5-27
- 既存のエントリへの属性の追加, A-4
- グループ・エントリ、Oracle Directory Manager を使用, 7-8
- 構成設定エントリ, 2-22, 5-2, 5-10
  - Oracle Directory Manager を使用, 2-22, 5-4
  - コマンドライン・ツールを使用, 2-22, 7-11
- 属性
  - Oracle Directory Manager を使用, 6-18
  - ガイドライン, 6-14
  - 既存属性をコピー, 6-20
- 入力ファイル, 5-11

- 必須属性
  - 既存のオブジェクト・クラス, 6-5
  - 使用中のオブジェクト・クラス, 7-9
- ユーザー・エントリ、Oracle Directory Manager を使用, 7-7
- レプリケーション・ノード, 10-19
- レプリケート・システムへの DSA の追加, B-1
- 追加の Directory Server、接続, 4-10
- 通常モード、Directory Server の実行, E-5
- ツール、チューニング, 15-2

## て

---

- 停止
  - Oracle Directory Replication Server, 3-7, A-33
  - Replication Server インスタンス, 3-7, A-33
  - ディレクトリ・データベースのリスナー, 10-6
- ディスク使用量, 13-10
- ディスクのチューニング, 15-8
- ディスク領域要件、見積り, 14-6
- ディレクトリ
  - NOS, 13-2, 13-3
  - 概念的な概要, 1-2
  - 仮想, 2-42
  - 接続, 2-42
  - パーティション化, 2-38
  - 分散, 2-23
  - 読み込み目的, 1-2
  - ロケーション非依存, 1-3
- ディレクトリ・アクセス制御, 1-8, 9-1
- ディレクトリ・エントリの表示, 7-2
- ディレクトリ使用パターン、習得, 14-3
- ディレクトリ情報ツリー
  - 階層と構造, 13-3
  - データ所有権の境界を反映するように編成, 13-3
  - 編成, 13-3
- ディレクトリ情報ツリー (DIT)、2-2
  - 監査ログ・エントリ, 5-26
- ディレクトリ・スキーマ, 2-11
  - 管理, 6-1
- ディレクトリ・ツリー, 7-2
- ディレクトリ・データベースのリスナー, 10-6
- ディレクトリと対比したりレーショナル・データベース, 1-2
- ディレクトリ・パスワード、変更, 5-19

- ディレクトリ・レプリケーション・グループ (DRG), 2-25, 10-2
  - インストールと構成, 10-2
  - 設定, 10-2
- データ
  - 整合性, 2-11, 2-14, 2-16
  - プライバシー, 2-11, 2-16
- データ移行プロセス, F-2
- データ・サーバー
  - パスワードの変更, 5-30
- データ・プライバシー
  - SSL を使用, 1-8
- データベース・キャッシュ
  - サイズ, 13-9
- データベース・サーバー・エラー, G-2
- データベース接続, 2-21
  - 同時, 15-10, E-5
  - プーリング, 1-8
- データベース・ブロック・サイズ・パラメータ, 15-9
- データベース・ブロック・バッファ・パラメータ, 15-9
- データベース、ディレクトリ専用, 2-20
- データを移行、他の LDAP ディレクトリから, F-2
- デーモン, 3-2
- テクノロジ・スタック, 16-2
- デバッグ・レベル, E-4
- デバッグ・ロギング・レベル, 5-23
  - 設定, 5-22
  - OID 制御ユーティリティを使用, 5-22
  - Oracle Directory Manager を使用, 5-22
- デフォルト・ナレッジ参照, 2-41
  - 構成, 7-19
- デフォルト・ポート, 4-3
- デフォルト・ポート以外、実行方法, 4-3
- デフォルト・ポート番号, 3-5, 3-6, A-31, A-33
- テンプレート、エントリの作成, 7-7

## と

---

- 間合せ
  - 監査ログ, 5-24
  - 重要なイベント, 5-24
- 同時データベース接続, 15-10, E-5
- 匿名
  - 認証, 2-12, 4-4
  - アクセス制御, 9-21, 9-24
  - ログイン, 4-3

トラブルシューティング, G-1  
    Directory Server, 3-8  
    パフォーマンス, 15-11  
トレース、ファンクション・コール, 5-23

## な

---

ナビゲータ・ペイン、Oracle Directory Manager, 4-6  
名前、オブジェクト・クラス, 6-6  
ナレッジ参照, 2-39, 13-3, 13-5  
    概要, 2-39  
    管理権限の制限, 2-40  
    構成, 7-17  
    種類, 2-41  
    上位, 2-39  
    スマート, 2-41  
        構成, 7-18  
    デフォルト, 2-41  
        構成, 7-19

## に

---

入力ファイル、作成, 5-10  
認可, 2-11, 2-15  
認可 ID, 2-12  
認証, 2-11, 2-12, 2-22  
    Kerberos, A-5, A-7, A-10  
    Oracle Internet Directory, 1-8  
    PKI, 2-16  
    SSL, 2-12, A-5, A-7, A-8, A-13, A-17  
        Oracle Directory Manager, 4-6  
        サーバー, E-5  
        サーバーのみ, 4-6  
    SSL クライアントとサーバー, 2-12, E-5  
    SSL サーバー, 2-12  
    SSL なし, 4-6  
    SSL なしの指定, E-5  
    アクセス制御の対象の指定, 9-20, 9-24  
    オプション, 2-12  
    簡易, 1-8, 4-4  
        アクセス制御の対象, 9-21, 9-24  
    強化, 2-12  
    証明書ベース, 2-12  
    匿名, 2-12, 4-4  
        アクセス制御, 9-21, 9-24  
    パスワード・ベース, 2-12, 4-4  
    パラメータ, E-5

認証アクセス、SSL を使用, 1-8  
認証局, 2-12, 2-13  
    定義, 2-13  
認証なし、アクセス制御, 9-21, 9-24

## ね

---

ネーミング・エントリ, 2-2, 13-2  
ネーミング・コンテキスト  
    管理, 5-15  
    検索, 2-10  
    公開, 2-10, 5-15  
        ldapmodify を使用, 5-16  
        Oracle Directory Manager を使用, 5-15  
    公開を検索, 5-15  
    従属, 2-39  
    定義, 2-10  
    パーティション化されたディレクトリ, 2-38  
    レプリケーション, 2-24, 10-2  
ネット・サービス名, 3-2, 3-3, A-29  
ネットワーク  
    接続性、容量計画, 14-2  
    帯域幅, 14-12  
    要件, 14-12  
    容量計画, 14-12  
ネットワーク・インタフェース・カード (NIC)、  
    障害, 16-8  
ネットワークレベルの接続リダイレクション, 16-6  
ネットワークレベルのフェイルオーバー, 16-6

## は

---

バージョン  
    Oracle ディレクトリ, 5-13  
パーティション化, 2-23, 2-38  
    配置に関する考慮事項, 13-4  
ハードウェア・ベースの接続リダイレクション, 16-7  
配置  
    考慮事項, 13-1  
    パーティション化, 13-4  
配置に関する考慮事項  
    CPU の能力, 13-8  
    チューニング, 13-9  
    フェイルオーバー, 13-6  
    レプリケーション, 13-5  
配置例, 16-9  
バインド, 2-22

バインド・モード

アクセス制御の対象の指定, 9-20, 9-24

パケット・ハンドリングのデバッグ, 5-23

パスワード

Oracle データ・サーバー, 4-13

変更, 5-30

SSLWallet 用, 4-5

設定, E-6

変更, 5-6, 5-8, 5-9, 8-4, E-6

暗号化, 2-16

MD4, 2-16

MD5, 2-16

SHA, 2-17

UNIX Crypt, 2-17

デフォルト, 2-16

暗号化オプション, 2-16

シェル・ツール, 4-12, 7-14

ディレクトリ, 変更, 5-19

バルク・ツールを使用, 4-12

パスワード暗号化, 2-11

ldapmodify を使用した変更, 5-17

Oracle Directory Manager を使用した変更, 5-16

スキームを変更, 5-16

設定

Oracle Directory Manager を使用, 5-13

パスワード・ベースの認証, 2-12, 4-4

バックアップおよびリカバリの計画, 13-6

バックエンドでの通信の出力, 5-23

バッチ処理

コマンドライン・モードのコマンド, 6-12

バッファ・キャッシュ・サイズ, 15-7

パフォーマンス

orclEntryLevelACI を使用, 9-3

検索, 15-11

測定, 15-2

追加または変更, 15-11

トラブルシューティング, 15-11

複数のスレッドの使用, A-6

レプリケーション, 2-23, 13-5

バルク・ツール, 4-12

構文, A-21

## ひ

---

比較

2つのオブジェクト, 4-7

エントリ, 4-11, 7-11

属性値, 7-11

必須属性, 2-7, 6-3

値の入力, 7-6

オブジェクト・クラス, 6-7

既存のオブジェクト・クラスへの追加, 6-5

再定義, 6-4

使用中のオブジェクト・クラスへの追加, 7-9

必須属性の再定義, 6-4

秘密鍵, 2-13

評価、ACL, 9-10

優先順位規則, 9-11

表記規則, xxiii

表示

ACP、Oracle Directory Manager を使用, 9-17

エントリの属性, 7-5

オブジェクト・クラス, 6-9

監査ログ・エントリ, 5-24

索引付き属性, 6-24

サブツリー, 7-2

システム操作属性, 5-12

表領域, 14-7

OLTS\_ATTRSTORE, 14-10

OLTS\_CT\_CN, 14-10

OLTS\_CT\_DN, 14-10

OLTS\_CT\_OBJCL, 14-10

OLTS\_CT\_STORE, 14-10

OLTS\_DEFAULT, 14-10

OLTS\_IND\_ATTRSTORE, 14-10

OLTS\_IND\_CT\_DN, 14-10

OLTS\_IND\_CT\_STORE, 14-10

SYSTEM, 14-10

均衡化, 15-8

サイズ設定, 14-8

作成, 10-5

レプリケーション, 10-5

## ふ

---

ファンクション・コールのトレース, 5-23

フィルタ

Begins With, 6-7

Ends With, 6-7

- Exact Match, 6-8, 7-4, 9-20, 9-23
- Greater or Equal, 6-8, 7-4, 9-20, 9-23
- IETF 準拠, A-17
- ldapsearch, A-19
- Less or Equal, 6-8, 7-4, 9-20, 9-24
- Not Null, 6-8
- Present, Oracle Directory Manager, 7-4
- 検索, 2-22
  - Oracle Directory Manager, 6-7
  - 属性の検索, 6-16
- プーリング、接続, 1-8
- フェイルオーバー, 1-8, 16-1
  - AlternateServers 属性, 16-4
  - Oracle Internet Directory の機能, 16-7
  - クライアントにおけるオプション, 16-4
  - 配置での考慮事項, 13-6
  - パブリック・ネットワーク・インフラストラクチャのオプション, 16-5
  - プライベート・ネットワーク・インフラストラクチャのオプション, 16-8
- フォールト・トレランス機能, 16-3
- 複数値の属性, 2-5
  - member, 7-8
  - orclEntryLevelACI, 9-3
  - 値の追加、ldapmodify を使用, A-14
  - 単一値への変換, 6-15
- 複数ディレクトリ、Oracle Internet Directory と同期化, 2-42
- 複数の構成設定エントリ, 8-2
- 複数のスレッド, A-17
  - ldapaddmt, A-6
  - 数の増加, A-6
- 物理的な分散
  - パーティションとレプリカ, 13-3
- 物理メモリー, 14-11
- 付与
  - Access, 9-21, 9-24
  - エントリ・レベルのアクセス権限
    - Oracle Directory Manager を使用, 9-30
- プライバシー、データ, 2-11, 2-16
  - SSL を使用, 1-8
- プロキシ・ユーザー
  - 定義, 5-19
  - ユーザー名とパスワードの管理, 5-19
- プロセス, 2-20
  - Oracle バックグラウンド, 15-10

- Oracle フォアグラウンド
  - 制限, 15-6
- プロセッサ親和性、SMP システム, 15-6
- 分散ディレクトリ, 2-23, 2-38
  - パーティション化, 2-23
  - パーティションとレプリカ, 13-3
  - レプリケート, 2-23



- 平均待機時間, 15-2
- ページング, 14-11
- ベース検索, 7-3
- ベース・スキーマ
  - オブジェクト・クラス, 6-5
  - 属性, 6-14
  - 削除, 6-15
  - 変更, 6-15
- 変換
  - 構造型オブジェクト・クラス, 6-5
  - 補助型オブジェクト・クラス, 6-4
- 変更
  - ACI ディレクティブ、Oracle Directory Manager を使用, 9-19
  - ACP、Oracle Directory Manager を使用, 9-19
- DN
  - ldapmoddn を使用, 4-11
  - コマンドライン・ツールを使用, 7-11
- Oracle Wallet の位置, 5-6, 5-7, 5-9, 8-4, E-6
- Oracle Wallet パラメータ, 5-6, 5-7, 5-9, 8-4, E-6
- RDN、コマンドライン・ツールを使用, 7-11
- SSL 構成パラメータ, 8-3
- Wallet パスワード, 5-6, 5-8, 5-9, 8-4, E-6
- アクティブ・インスタンスのパラメータ, 8-3
- アクティブ・サーバー・インスタンスのパラメータ, 5-4
- エントリ
  - ldapmodify を使用, A-12
  - LDAP 規則, 7-9
  - Oracle Directory Manager を使用, 7-9
  - 規則, 7-9
  - 同時、ldapmodifymt を使用, A-16
- オブジェクト
  - ldapmodify を使用, 4-11, 7-11
  - Oracle Directory Manager を使用, 4-7, 4-9

- オブジェクト・クラス, 6-4
  - Oracle Directory Manager を使用, 6-11
  - コマンドライン・ツールを使用, 6-12
  - ベース・スキーマ, 6-5
- 監査レベル, 5-28
- 監査ログのイベント, 5-27
- 構成設定エントリ, 2-22, 3-7, 5-2, A-34
  - ldapmodify を使用, 5-11
  - Oracle Directory Manager を使用, 5-4, 5-8
  - コマンドライン・ツールを使用, 7-11
- 構成設定エントリの値, 5-2
- 構成パラメータ, 2-22
- 属性
  - ldapmodifymt を使用, 4-11, 7-11
  - ldapmodify を使用, 4-11, 7-11
  - ガイドライン, 6-15
  - 同時, 4-11, 7-11
- 属性値, 7-9
- 属性の構文, 6-15
- 多数のエントリ, A-24
- パスワード
  - Oracle データ・サーバー, 4-13
  - ディレクトリ, 5-19
- ベース・スキーマの属性, 6-15
- ユーザー・エントリ, 7-10
- レプリケーション承諾のパラメータ, 10-15
- 変更の種類、ldapmodify 入力ファイル, A-14
- 変更番号ベースの削除, 2-27
- 変更ログ, 2-24, 2-25, 2-29
  - オブジェクト・ストア、Oracle メタディレクトリ・ソリューション, 11-2
- 削除
  - 方法, 2-27
- 時間ベースの削除, 2-27
- 処理スレッド, 2-29
- 変更番号ベースの削除, 2-27
- レプリケーション, 1-8, 2-31
- 変更ログ記録, 3-4, A-31
- 変更ログの削除
  - 時間ベース, 2-27, 10-11, 10-12
  - 変更番号ベース, 2-27, 10-11
- 変更ログの処理スレッド, 2-30
- 変更ログ・フラグ, 10-18
  - 切替え, 10-18

## ほ

---

- 包括的なスループット, 15-2
- ポート, 4-4
  - デフォルト, 3-5, 3-6, 4-3, A-31, A-33
- ポート 389, 3-5, 3-6, A-31, A-33, E-5
- ポート 636, 3-5, 3-6, A-31, A-33, E-5
- 他のディレクトリとの同期, 2-42
- 他のディレクトリとの同期化, 11-1
- 保護
  - ポート 636, 8-2
- モード
  - Directory Server の実行, E-5
  - サーバー・インスタンスの実行, 8-2
- 補助型
  - オブジェクト・クラス, 6-4
  - オブジェクト・クラス型, 2-9
- ポリシー
  - ネーミング、既存のものを活用, 13-2

## ま

---

- マスター定義サイト (MDS), 10-3
  - 指定, 10-3
- マルチ・サーバー・プロセス, 2-21
- マルチスレッド LDAP サーバー, 1-8
- マルチスレッド・コマンドライン・ツール
  - ldapaddmt, 4-11, 7-11, A-6
  - ldapmodifymt, 4-11, 7-11, A-17
- マルチマスター・フラグ, 10-18
  - 切替え, 10-18
- マルチマスター・レプリケーション, 1-8, 2-25, 13-4, 13-5
  - 高い可用性, 16-7

## み

---

- 未指定のアクセス権限, 9-9, 9-25

## め

---

- メタディレクトリ
  - エージェント, 2-42
  - 概要, 2-42
- メタディレクトリ環境、Oracle Internet Directory と同期化, 2-42, 11-1
- メタディレクトリ・ソリューション、利点, 2-43

メタデータ、スキーマに格納, 2-11  
メニュー・バー、Oracle Directory Manager, 4-7  
メモリー  
  仮想, 14-11  
  使用量, 13-10  
  チューニング, 15-7  
  必須, 13-9  
  不足, 15-7  
  物理, 14-11  
  要件, 14-11  
  容量計画, 14-2  
メモリー不足, 15-7

## ゆ

---

ユーザー・エントリ  
  追加、ldapadd を使用, 7-12  
  追加、Oracle Directory Manager を使用, 7-7  
  変更、ldapmodify を使用, 7-12  
  変更、Oracle Directory Manager を使用, 7-10  
ユーザー指定の構成設定のオーバーライド, 3-8, A-34  
ユーザー名とパスワード  
  管理  
    ldapmodify を使用, 5-21  
    Oracle Directory Manager を使用, 5-20  
ユーザー・ログイン, 4-3  
優先順位規則  
  ACL の評価, 9-11  
  アクセス・ポリシーの競合, 9-3

## よ

---

容量計画, 13-6, 13-7  
  I/O サブシステム, 14-5  
  ネットワーク要件, 14-12  
読み込み目的、ディレクトリ, 1-2

## り

---

リカバリ機能、Oracle8i, 1-8  
リスナー、ディレクトリ・データベース, 2-19, 2-21  
  再起動, 10-6  
  停止, 10-6  
リレーショナル・データベースと対比したディレク  
  トリ, 1-2

## る

---

類似項目の作成

  操作、Oracle Directory Manager を使用, 4-7  
  テンプレートをを使用したエントリの追加, 7-7  
  ボタン、Oracle Directory Manager, 4-9, 7-7

## れ

---

レプリカ, 2-23  
  配置, 13-4  
レプリケーション, 2-23  
  Log Location, 5-13  
  Login イベント, 5-27  
  Net8 環境の準備, 10-4  
  Status Location, 5-13  
  アドバンスト・レプリケーション, 2-26  
  移送方法, 2-26  
  インストール, 10-2  
  概要, 2-29  
  ガベージ・コレクション, 10-11  
  競合  
    手動での解消, 10-29  
構成, 10-10  
  sqlnet.ora, 10-4  
  tnsnames.ora, 10-4  
  アドバンスト・レプリケーション, 10-7  
コールド・バックアップ, B-1  
サーバー, 1-7, 2-20  
  起動, 3-6, A-32, A-33  
  構成設定エントリ, 10-11  
  停止, 3-7, A-33  
実装する理由, 13-5  
障害許容度, 13-6  
詳細プロセス, 2-32  
承諾, 2-25, 5-13, 10-15  
  構成, 10-10  
  ノードの追加, 10-17  
承諾のパラメータ, 10-14  
  表示, 10-15  
  変更, 10-15  
新規ノードの追加, 10-19, 10-25  
信頼性, 2-23  
スポンサ・ノード, B-3  
データベース・コピー・プロシージャ, B-1  
ネーミング・コンテキスト, 10-2

- ノード
  - 削除, 10-25
  - 追加, 10-19
- ノードを削除, 10-25
- 配置, 13-5
- パフォーマンス, 2-23
- 変更ログ, 1-8, 2-31
- マルチマスター, 1-8, 2-25, 13-4
- ゆるやかな一貫性モデル, 13-5
- ロード・バランシング, 13-5
- ワーカー・スレッドの数を指定, 10-12
- レプリケーション固有のデバッグ, 5-23
- レプリケーションのゆるやかな一貫性モデル, 13-5
- レプリケート・ディレクトリ、概念の説明, 2-23

## ろ

---

- ロード・バランシング
  - ネットワークレベル, 16-5
  - レプリケーション, 13-5
- ロールバック・セグメント, 10-5
  - 作成, 10-5
- ログイン
  - スーパー・ユーザー, 4-3
  - 匿名, 4-3
  - ユーザー, 4-3
- ロケーション非依存、ディレクトリ, 1-3
- 論理ディスク, 15-8

## わ

---

- ワーカー・スレッド, 2-21, 15-10
  - レプリケーションで指定, 10-12
- ワイルド・カード、アクセス制御ポリシーの設定,  
9-33