

Oracle Internet Directory

管理者ガイド Vol.1

リリース 9.0.2

2002 年 7 月

部品番号 : J05908-01

ORACLE®

Oracle Internet Directory 管理者ガイド Vol.1, リリース 9.0.2

部品番号 : J05908-01

原本名 : Oracle Internet Directory Administrator's Guide, Volume 1, Release 9.0.2

原本部品番号 : A97253-01

原本著者 : Jeffrey Levinger, Sheryl Edwards, Richard Smith

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

Copyright © 1999, 2002 Oracle Corporation. All rights reserved.

Printed in Japan.

制限付権利の説明

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

当プログラムのリバース・エンジニアリング等は禁止されております。

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

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

危険な用途への使用について

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

Restricted Rights Notice

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

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

目次

はじめに	xxxix
Oracle Internet Directory の新機能	xlvi
Vol.1	
第 I 部 スタート・ガイド	
1 概要	
ディレクトリとは	1-2
拡大するオンライン・ディレクトリの役割	1-2
問題: 特別な用途を指定された多数のディレクトリ	1-4
LDAP とは	1-4
LDAP と単純化されたディレクトリ管理	1-5
LDAP バージョン 3	1-5
Oracle Internet Directory とは	1-6
Oracle Internet Directory のアーキテクチャ	1-6
Oracle Internet Directory のコンポーネント	1-8
Oracle Internet Directory の利点	1-9
拡張性	1-9
高い可用性	1-9
セキュリティ	1-9
Oracle 環境との統合	1-9

Oracle 製品における Oracle Internet Directory の使用方法	1-10
簡単で対費用効果の高い管理	1-10
集中化されたセキュリティ・ポリシー管理による厳重なセキュリティ	1-10
分散ディレクトリの統合	1-12

2 概念およびアーキテクチャ

エントリ	2-2
属性	2-4
属性情報の種類	2-5
単一値と複数値の属性	2-6
一般的な LDAP 属性	2-6
属性の構文	2-6
属性の一致規則	2-7
属性オプション	2-7
オブジェクト・クラス	2-8
サブクラス、スーパークラスおよび継承	2-9
オブジェクト・クラスの型	2-9
抽象型オブジェクト・クラス	2-9
構造型オブジェクト・クラス	2-10
補助型オブジェクト・クラス	2-10
ネーミング・コンテキスト	2-11
ディレクトリ・スキーマ	2-12
セキュリティ	2-12
グローバリゼーション・サポート	2-13
Oracle Internet Directory のアーキテクチャ	2-15
Oracle Internet Directory のノード	2-15
Oracle ディレクトリ・サーバー・インスタンス	2-19
構成設定エントリ	2-20
例: Oracle Internet Directory の動作	2-20
分散ディレクトリ	2-21
レプリケーション	2-22
パーティション化	2-24

ナレッジ参照と参照	2-25
参照の種類	2-27
Delegated Administration Service	2-28
Oracle Directory Integration Platform	2-28
メタディレクトリ	2-28
Oracle Directory Integration Platform 環境	2-29

3 事前に実行するタスクと情報

タスク 1: OID モニターの開始	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 ディレクトリ・サーバー・インスタンスの起動	3-4
Oracle ディレクトリ・サーバー・インスタンスの停止	3-5
Oracle ディレクトリ・レプリケーション・サーバー・インスタンスの起動	3-6
Oracle ディレクトリ・レプリケーション・サーバー・インスタンスの停止	3-7
ディレクトリ・サーバー・インスタンスの再起動	3-7
ディレクトリ・サーバー・インスタンスの起動に関するトラブルシューティング	3-9
タスク 3: デフォルト・セキュリティ構成の再設定	3-9
デフォルトのアクセス・ポリシー	3-10
ルート DSE でのデフォルトのアクセス・ポリシー	3-10
デフォルトのサブスクライバ・ネーミング・コンテキストのユーザー・コンテナでの デフォルトのアクセス・ポリシー	3-10
デフォルトのサブスクライバ・ネーミング・コンテキストのグループ・コンテナでの デフォルトのアクセス・ポリシー	3-11
Oracle コンテキスト管理者に対するデフォルトのアクセス・ポリシー	3-11
Oracle9i Application Server 管理者に対するデフォルトのアクセス・ポリシー	3-12
タスク 4: データベースのデフォルト・パスワードの再設定	3-12
タスク 5: OID データベース統計収集ツールの実行	3-13
ログ・ファイルの位置	3-13

4 ディレクトリ管理ツール

Oracle Directory Manager の使用方法	4-2
Oracle Directory Manager の起動	4-2
ディレクトリ・サーバーへの接続	4-3
Oracle Directory Manager のナビゲート	4-7
Oracle Directory Manager の概要	4-7
Oracle Directory Manager のメニュー・バー	4-8
Oracle Directory Manager のツールバー	4-10
追加のディレクトリ・サーバーへの接続	4-11
ディレクトリ・サーバーからの切断	4-11
Oracle Directory Manager を使用した管理タスクの実行	4-11
コマンドライン・ツールの使用方法	4-12
LDAP エントリに直接影響を与えるツール	4-13
バルク・ツールの使用方法	4-13
カタログ管理ツールの使用方法	4-14
OID 制御ユーティリティの使用方法	4-15
OID データベース・パスワード・ユーティリティの使用方法	4-15
レプリケーション・ツールの使用方法	4-15
OID データベース統計収集ツールの使用方法	4-16
管理タスクの一覧	4-17

第 II 部 基本的なディレクトリ管理

5 Oracle ディレクトリ・サーバーの管理

サーバーの構成設定エントリの管理	5-2
構成設定エントリ管理のための事前の考慮事項	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	5-5
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	5-11
ldapadd を使用した構成設定エントリの追加	5-11
ldapmodify を使用した構成設定エントリの変更と削除	5-12

システム操作属性の設定	5-13
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	5-16
ネーミング・コンテキストの管理	5-17
Oracle Directory Manager を使用したネーミング・コンテキストの公開	5-17
ldapmodify を使用したネーミング・コンテキストの公開	5-18
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	5-18
Oracle Directory Manager を使用したスーパー・ユーザー、ゲスト・ユーザーおよび プロキシ・ユーザーの管理	5-19
ldapmodify を使用したスーパー・ユーザー、ゲスト・ユーザーおよび プロキシ・ユーザーの管理	5-20
検索の構成	5-21
Oracle Directory Manager を使用した検索の構成	5-21
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	5-21
Oracle Directory Manager を使用した、検索の最大時間の設定	5-21
ldapmodify を使用した検索の構成	5-22
ldapmodify を使用した、検索で戻されるエントリの最大数の設定	5-22
ldapmodify を使用した、検索の最大時間の設定	5-22
ディレクトリ・サーバーの監視、デバッグおよび監査	5-23
Oracle Internet Directory サーバー管理機能フレームワークによる Oracle Internet Directory サーバーの監視	5-23
Oracle Internet Directory サーバー管理機能のアーキテクチャとコンポーネント	5-23
Oracle Internet Directory サーバー管理機能の構成情報の位置	5-26
Oracle Internet Directory サーバー管理機能の構成	5-26
デバッグ・ロギング・レベルの設定	5-26
Oracle Directory Manager を使用したデバッグ・ロギング・レベルの設定	5-26
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	5-27
監査ログの使用方法	5-28
監査ログ・エントリの構造	5-29
ディレクトリ情報ツリーにおける監査ログ・エントリの位置	5-30
監査可能なイベント	5-30
監査レベルの設定	5-31
監査ログ・エントリの検索	5-33
監査ログの削除	5-35

アクティブ・サーバー・インスタンスの情報の表示	5-35
Oracle データベース・サーバー接続時のパスワードの変更	5-36
別名エントリの間接参照	5-36
別名エントリ間接参照の概要	5-36
別名オブジェクト・クラスの定義	5-36
別名化されたオブジェクト名の定義	5-36
別名エントリ間接参照の使用方法	5-37
別名エントリの追加	5-37
ベース検索	5-39
1 レベルの検索	5-39
サブツリーの検索	5-40
別名エントリの変更	5-41
成功メッセージとエラー・メッセージ	5-41

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	6-10
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	6-13
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	6-14
属性管理の概要	6-15
属性の追加に関する規則	6-15
属性の変更に関する規則	6-15
属性の削除に関する規則	6-16

Oracle Directory Manager を使用した属性の管理	6-16
Oracle Directory Manager を使用したすべてのディレクトリ属性の表示	6-17
Oracle Directory Manager を使用した属性の検索	6-18
Oracle Directory Manager を使用した属性の追加	6-20
Oracle Directory Manager を使用した新規属性の追加	6-20
Oracle Directory Manager を使用した既存の属性からの新規属性の作成	6-22
Oracle Directory Manager を使用した属性の変更	6-24
Oracle Directory Manager を使用した属性の削除	6-26
Oracle Directory Manager を使用した属性の索引付け	6-26
Oracle Directory Manager を使用した索引付き属性の表示	6-26
Oracle Directory Manager を使用した属性への索引の追加	6-27
Oracle Directory Manager を使用した属性からの索引の削除	6-27
コマンドライン・ツールを使用した属性の管理	6-27
ldapmodify を使用した属性の追加と変更	6-27
ldapmodify を使用した属性の削除	6-28
コマンドライン・ツールを使用した属性の索引付け	6-29
ldapmodify を使用した、データが存在していない属性の索引付け	6-29
ldapmodify を使用した属性からの索引の削除	6-29
カタログ管理ツールを使用した、データが存在している属性の索引付け	6-30
一致規則の表示	6-30
Oracle Directory Manager を使用した一致規則の表示	6-30
ldapsearch を使用した一致規則の表示	6-31
構文の表示	6-31
Oracle Directory Manager を使用した構文の表示	6-31
ldapsearch を使用した構文の表示	6-31

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 を使用した特定エントリの属性の表示	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	7-6

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
Oracle Directory Manager を使用した属性オプション付きエントリの管理	7-10
Oracle Directory Manager を使用した、既存エン트리への属性オプションの追加	7-10
Oracle Directory Manager を使用した属性オプションの変更	7-11
Oracle Directory Manager を使用した属性オプションの削除	7-11
コマンドライン・ツールを使用したエントリの管理	7-12
エントリ管理のためのコマンドライン・ツール	7-12
例 : ldapadd を使用したユーザー・エントリの追加	7-13
例 : ldapmodify を使用したユーザー・エントリの変更	7-14
コマンドライン・ツールを使用した属性オプション付きエントリの管理	7-14
例 : ldapmodify を使用した属性オプションの追加	7-14
例 : ldapmodify を使用した属性オプションの削除	7-14
例 : ldapsearch を使用した属性オプション付きエントリの検索	7-15
バルク・ツールを使用したエントリの管理	7-15
bulkload を使用した LDIF ファイルのインポート	7-16
タスク 1: Oracle サーバーのバックアップ	7-17
タスク 2: Oracle Internet Directory のパスワードの準備	7-17
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	7-17
タスク 4: SQL*Loader 用の入力ファイルの生成	7-17
タスク 5: 入力ファイルのロード	7-18
バルク・ロードに失敗した場合	7-18
ディレクトリ・データの LDIF への変換	7-18
多数のエントリの変更	7-18
多数のエントリの削除	7-18
ナレッジ参照と参照の管理	7-19
スマート参照の構成	7-19
デフォルト参照の構成	7-20

8 ディレクトリにおけるグローバリゼーション・サポート

環境変数 NLS_LANG	8-2
非 UTF-8 データベースの使用方法	8-3
LDIF ファイルでのグローバリゼーション・サポートの使用方法	8-4
ASCII 文字列のみを含む LDIF ファイル	8-4
UTF-8 エンコーディング文字列を含む LDIF ファイル	8-4
ケース 1: ネイティブ文字列（非 UTF-8）	8-5
ケース 2: UTF-8 文字列	8-5
ケース 3: BASE64 でエンコーディングされた UTF-8 文字列	8-5
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	8-5
コマンドライン・ツールでのグローバリゼーション・サポートの使用方法	8-6
各ツールを使用するときの -E 引数の指定	8-6
例: コマンドライン・ツールでの -E 引数の使用方法	8-7
クライアント環境における NLS_LANG の設定	8-8
バルク・ツールでのグローバリゼーション・サポートの使用方法	8-9
bulkload でのグローバリゼーション・サポートの使用方法	8-9
ldifwrite でのグローバリゼーション・サポートの使用方法	8-10
bulkdelete でのグローバリゼーション・サポートの使用方法	8-11
bulkmodify でのグローバリゼーション・サポートの使用方法	8-11

9 Delegated Administration Service

Delegated Administration Service の概要	9-2
Delegated Administration Service ユニット	9-2
Oracle Internet Directory セルフ・サービス・コンソール	9-2
Delegated Administration Service と Oracle Internet Directory セルフ・サービス・コンソールの利点	9-3
Delegated Administration Service の概念とアーキテクチャ	9-4
Delegated Administration Service の動作	9-4
Delegated Administration Service と Oracle9iAS Single Sign-On	9-5
Delegated Administration Service の起動と停止	9-7
Delegated Administration Service のインストールと構成	9-7
Delegated Administration Service 環境でのコンポーネントのログ・ファイル	9-7

タスク 1: Delegated Administration Service のインストール	9-8
タスク 2: Delegated Administration Service が稼働していることの検証	9-8
手順 1: Oracle HTTP Server が稼働していることの検証	9-8
手順 2: Java (OC4J JVM) が稼働していることの検証	9-8
手順 3: Delegated Administration Service が稼働していることの検証	9-9
タスク 3: デフォルト・サブスクリバ・コンテキストの構成	9-9
タスク 4: ユーザー・エントリの構成	9-10
Delegated Administration Service を使用したユーザー・エントリとグループ・エントリの検索	9-13
Delegated Administration Service を使用したユーザー・エントリの検索	9-13
Delegated Administration Service を使用したグループ・エントリの検索	9-13
Delegated Administration Service を使用したユーザー、グループおよびサブスクリバの管理	9-14
Delegated Administration Service を使用したユーザー・エントリの作成	9-14
Delegated Administration Service を使用したユーザー・エントリの変更	9-14
Delegated Administration Service を使用したユーザー・エントリの削除	9-15
Delegated Administration Service を使用したユーザー権限の割当て	9-15
Delegated Administration Service を使用したグループ・エントリの作成	9-16
Delegated Administration Service を使用したグループ・エントリの変更	9-17
Delegated Administration Service を使用したグループ・エントリの削除	9-17
Delegated Administration Service を使用したグループ権限の割当て	9-18
Delegated Administration Service を使用したパスワードの変更	9-19
ユーザー自身のパスワード変更	9-19
別のユーザーのパスワード変更	9-20

10 属性一意性

概要	10-2
概念	10-2
要件	10-3
属性一意性の作成	10-4
ディレクトリ全体での属性一意性の作成	10-4
1 つのサブツリー内での属性一意性の作成	10-4
1 つのオブジェクト・クラス内での属性一意性の作成	10-4

属性一意性の有効化と無効化	10-5
属性一意性の有効化	10-5
属性一意性の無効化	10-5
サブツリーの指定	10-5
属性一意性ポリシーの削除	10-5
構成インタフェース	10-6
定義されたポリシーの位置およびモデル	10-6
ポリシー有効範囲決定規則	10-7
属性一意性機能の適用	10-8
既知の制限事項	10-8
単純なレプリケーション使用例	10-8
マルチマスター・レプリケーション使用例	10-9

第 III 部 ディレクトリのセキュリティ

11 ディレクトリ・セキュリティの概要

データ整合性	11-2
データ・プライバシ	11-2
認可	11-3
認証	11-4
直接認証	11-4
間接認証	11-5
ディレクトリ認証用ユーザー・パスワードの保護	11-7
パスワード・ポリシー	11-7

12 Secure Sockets Layer (SSL) とディレクトリ

サポートされている Cipher Suite	12-2
SSL クライアントの使用例	12-3
SSL パラメータの構成	12-3
Oracle Directory Manager を使用した SSL パラメータの構成	12-4
コマンドライン・ツールを使用した SSL パラメータの構成	12-5
このリリースの Oracle Internet Directory 固有の問題	12-5

13 ディレクトリ・アクセス制御

アクセス制御ポリシー・ポイントの管理の概要	13-2
アクセス制御管理の構造体	13-2
アクセス制御ポリシー・ポイント (ACP)	13-2
規定のアクセス制御のための orclACI 属性	13-2
エントリ・レベルのアクセス制御のための orclEntryLevelACI 属性	13-3
アクセス制御グループ	13-3
アクセス制御情報アイテム (ACI) のコンポーネント	13-7
オブジェクト: アクセス権を付与するオブジェクト	13-7
対象: アクセス権を付与する対象	13-8
操作: 付与するアクセス権の種類	13-10
Oracle Directory Manager を使用したアクセス制御の管理	13-12
アクセス制御管理のための Oracle Directory Manager の構成	13-12
Oracle Directory Manager の ACP の表示の構成	13-12
Oracle Directory Manager を使用する場合の ACP の検索の構成	13-13
Oracle Directory Manager を使用した ACP の表示	13-13
Oracle Directory Manager を使用した ACP の追加	13-15
タスク 1: ACP にするエントリの指定	13-15
タスク 2: 構造型アクセス項目の構成	13-16
タスク 3: コンテンツ・アクセス項目の構成	13-19
Oracle Directory Manager の ACP 作成ウィザードを使用した ACP の追加	13-22
タスク 1: ACP にするエントリの指定	13-22
タスク 2: ACP 作成ウィザードを使用した構造型アクセス項目の構成	13-23
タスク 3: ACP 作成ウィザードを使用したコンテンツ・アクセス項目の構成	13-26
Oracle Directory Manager を使用した ACP の変更	13-29
タスク 1: 変更するエントリの指定	13-29
タスク 2: 構造型アクセス項目の変更	13-29
タスク 3: コンテンツ・アクセス項目の変更	13-33
Oracle Directory Manager を使用したエントリ・レベルのアクセス権の付与	13-36
例: Oracle Directory Manager を使用した ACP の管理	13-37
新規 ACP の作成	13-37
3 番目の ACI の作成	13-39
4 番目の ACI の作成	13-39

コマンドライン・ツールを使用したアクセス制御の管理	13-40
例：ユーザーが追加できるエントリの種類の制限	13-40
例：ldapmodify を使用した継承可能な ACP の設定	13-41
例：ldapmodify を使用したエントリ・レベルの ACI の設定	13-41
例：ワイルド・カードの使用方法	13-42
例：識別名によるエントリの選択	13-42
例：属性セクタと対象セクタの使用方法	13-43
例：読取り専用アクセス権の付与	13-44
例：グループ・エントリへの自己書き込みアクセス権の付与	13-44
ACL 評価の動作	13-44
ACL の評価の優先順位規則	13-45
同一オブジェクトに対する複数 ACI	13-47
オブジェクトに対する排他的アクセス権の付与	13-48
グループの場合の ACL 評価	13-48
LDAP 操作のアクセス・レベル要件	13-48

Vol.2

第 IV 部 ディレクトリの配置

14 一般的な配置の考慮事項

拡大するディレクトリの役割	14-2
ディレクトリ情報の論理編成	14-2
ディレクトリ・エントリのネーミング	14-2
ディレクトリ情報ツリーの階層と構造	14-3
物理的な分散：パーティションとレプリカ	14-4
理想的な配置	14-4
パーティション化に関する考慮事項	14-5
レプリケーションに関する考慮事項	14-6
フェイルオーバーに関する考慮事項	14-7

容量計画、サイズ設定およびチューニング	14-8
容量計画	14-9
サイズ設定に関する考慮事項	14-9
チューニングに関する考慮事項	14-11
1つのホストにおける複数の Oracle Internet Directory インストールの実行	14-12

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

Oracle のコンポーネントとディレクトリ使用の概要	15-2
すぐに使用可能なデフォルト構成	15-2
ルート Oracle コンテキスト	15-3
サブスクライバの Oracle コンテキスト	15-5
デフォルトのサブスクライバ構成	15-9

16 ディレクトリ・ベースのアプリケーション・セキュリティ

委任ディレクトリの管理	16-2
アプリケーション固有のアクセス制御	16-3
ディレクトリのドメインとロール	16-4

17 ユーザー認証資格証明のディレクトリ格納

ユーザー認証資格証明の集中格納の概要	17-2
Oracle Internet Directory への認証用パスワード・ベリファイアの格納	17-2
Oracle Directory Manager を使用したパスワード保護の管理	17-3
ldapmodify を使用したパスワード保護の管理	17-4
Oracle のコンポーネントに対する認証用パスワードの格納	17-4
パスワード・ベリファイアの概要	17-4
パスワード・ベリファイアを格納するための属性	17-6
例：パスワード検証の動作	17-8
Oracle Directory Manager を使用したパスワード・ベリファイア・プロファイルの管理	17-9
Oracle Directory Manager を使用したパスワード・ベリファイア・プロファイルの表示と変更	17-9

コマンドライン・ツールを使用したパスワード・ベリファイア・プロファイルの管理	17-10
コマンドライン・ツールを使用したパスワード・ベリファイア・プロファイルの表示	17-10
コマンドライン・ツールを使用したパスワード・ベリファイア・プロファイルの変更	17-10

18 パスワード・ポリシー

パスワード・ポリシーの概要	18-2
Oracle Directory Manager を使用したパスワード・ポリシーの管理	18-6
Oracle Directory Manager を使用したサブスクライバのパスワード・ポリシーの表示	18-8
Oracle Directory Manager を使用したサブスクライバのパスワード・ポリシーの変更	18-8
コマンドライン・ツールを使用したパスワード・ポリシーの管理	18-9
コマンドライン・ツールを使用したパスワード・ポリシーの設定	18-9
コマンドライン・ツールを使用したサブスクライバのパスワード・ポリシーの管理	18-9
例: コマンドライン・ツールを使用したサブスクライバのパスワード・ポリシーの表示	18-9
例: コマンドライン・ツールを使用したサブスクライバのパスワード・ポリシーの変更	18-9
エラー・メッセージ	18-10

19 容量計画に関する考慮事項

容量計画の説明	19-2
ディレクトリの使用パターンの理解: 事例	19-3
I/O サブシステムの要件	19-6
I/O サブシステムの説明	19-6
ディスク領域要件の概算	19-7
ディスク領域要件の詳細な計算	19-8
メモリー要件	19-12
ネットワーク要件	19-14
CPU 要件	19-15
CPU 構成	19-15
CPU 要件の概算	19-16
CPU 要件の詳細な計算	19-16
Acme Corporation の容量計画のまとめ	19-17

20 チューニングに関する考慮事項

チューニングの概要	20-2
パフォーマンス・チューニング用のツール	20-2
CPU 使用量のチューニング	20-4
Oracle Internet Directory のプロセスに関する CPU のチューニング	20-5
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	20-6
SMP システムにおけるプロセッサ親和性の利用	20-6
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	20-7
メモリーのチューニング	20-7
Oracle9i 用の SGA のチューニング	20-7
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	20-8
ディスクのチューニング	20-8
表領域の均衡化	20-9
RAID	20-9
データベースのチューニング	20-10
必須パラメータ	20-10
Oracle Internet Directory サーバーの構成に依存しているパラメータ	20-11
共有サーバー・プロセスの使用	20-11
ハードウェア・リソースに依存している SGA パラメータ	20-11
エントリ・キャッシング	20-12
パフォーマンスに関するトラブルシューティング	20-12

21 高い可用性とフェイルオーバーに関する考慮事項

Oracle Internet Directory の高い可用性とフェイルオーバーの概要	21-2
Oracle Internet Directory および Oracle9i のテクノロジ・スタック	21-2
クライアントにおけるフェイルオーバー・オプション	21-4
ユーザー入力からの代替サーバー・リスト	21-4
Oracle Internet Directory サーバーからの代替サーバー・リスト	21-4
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	21-5
ハードウェア・ベースの接続リダイレクション	21-7
ソフトウェア・ベースの接続リダイレクション	21-7
Oracle Internet Directory の可用性とフェイルオーバー機能	21-7

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	21-8
IP アドレス・テイクオーバー (IPAT)	21-8
冗長リンク	21-8
高い可用性の配置例	21-9

第 V 部 ディレクトリ・レプリケーション

22 ディレクトリ・レプリケーションの概要

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	22-2
Oracle9i レプリケーション	22-3
レプリケーション・アーキテクチャ	22-3
サブライヤ側のレプリケーション・プロセス	22-4
コンシューマ側のレプリケーション・プロセス	22-5
変更ログの削除	22-6
レプリケーションにおける競合の解消	22-7
レプリケーション競合が発生するレベル	22-7
エントリ・レベルの競合	22-7
属性レベルの競合	22-8
競合の一般的な原因	22-8
競合の自動解消	22-8
レプリケーション・プロセス	22-9
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	22-9
レプリケーション・プロセスがエントリを削除する動作	22-11
レプリケーション・プロセスがエントリを変更する動作	22-12
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	22-13
レプリケーション・プロセスが識別名を変更する動作	22-14

23 Oracle ディレクトリ・レプリケーション・サーバーの管理

レプリケーションのインストールと構成	23-2
タスク 1: DRG の全ノードへの Oracle Internet Directory のインストール	23-3
タスク 2: Oracle9i 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	23-4
タスク 3: ディレクトリ・レプリケーション・グループ用の Oracle9i レプリケーションの設定 ...	23-4
全ノードでのレプリケーション用の Oracle Net Services 環境の準備	23-4
MDS でのディレクトリ・レプリケーション用の Oracle9i レプリケーションの構成	23-8
タスク 4: ディレクトリへのデータのロード	23-10
タスク 5: 全ノードでの Oracle ディレクトリ・サーバー・インスタンスの起動	23-11
タスク 6: DRG の全ノードでのレプリケーション・サーバーの起動	23-11
タスク 7: ディレクトリ・レプリケーションのテスト	23-12
レプリケーションの管理	23-13
ディレクトリ・レプリケーション・サーバーの構成パラメータの変更	23-13
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 ...	23-15
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	23-16
レプリケーション承諾のパラメータの変更	23-18
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 ...	23-18
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	23-20
全ノードでのレプリケーション管理者パスワードの変更	23-22
レプリケーション・ノードの追加	23-22
タスク 1: 全ノードでディレクトリ・レプリケーション・サーバーを停止	23-23
タスク 2: 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	23-24
タスク 3: ldifwrite を使用したスポンサ・ノードのバックアップ	23-24
タスク 4: Oracle9i レプリケーション追加ノードの設定の実行	23-25
タスク 5: スポンサー・ノードの更新可能モードへの切替え	23-26
タスク 6: 新規ノード以外の全ノードでディレクトリ・レプリケーション・サーバーを起動	23-26
タスク 7: bulkload を使用して新規ノードにデータをロード	23-27
タスク 8: 新規ノードで LDAP サーバーを起動	23-27
タスク 9: 新規ノードでディレクトリ・レプリケーション・サーバーを起動	23-27
レプリケーション・ノードの削除	23-28
タスク 1: 全ノードでディレクトリ・レプリケーション・サーバーを停止	23-28

タスク 2: 削除するノード内の全プロセスの停止	23-29
タスク 3: マスター定義サイトからのノードの削除	23-29
タスク 4: すべてのノードでディレクトリ・レプリケーション・サーバーを起動	23-30
手動での競合の解消	23-30
レプリケーション変更の競合のモニター	23-30
競合解消メッセージの例	23-31
例 1: 存在しないエントリを変更しようとした場合	23-31
例 2: 既存のエントリを追加しようとした場合	23-31
例 3: 存在しないエントリを削除しようとした場合	23-31
管理者操作キュー操作ツールの使用	23-32
OID 調停ツールの使用	23-32
ホストから独立したものとしてのノードの識別	23-33
レプリケーション設定のトラブルシューティング	23-34

24 データベース・コピー・プロシージャを使用したノードの追加

前提事項	24-2
スポンサ・ディレクトリ・サイトの環境	24-2
新規ディレクトリ・サイトの環境	24-3
スポンサ・ノードで実行されるタスク	24-3
新規ノードで実行されるタスク	24-9
検証プロセス	24-12

第 VI 部 ディレクトリとクラスタ

25 クラスタ構成でのフェイルオーバー

概要	25-2
クラスタ化された環境でのフェイルオーバーの構成	25-4
ステップ 1: OID モニターの起動	25-4
ステップ 2: OID 制御ユーティリティを使用したディレクトリ・サーバーまたは ディレクトリ・レプリケーション・サーバーの起動	25-5
ステップ 3: ディレクトリ・サーバーと OID モニターの停止と再起動	25-5
クラスタ化された環境でのフェイルオーバーの動作	25-6

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

用語	26-2
Oracle9i Real Application Clusters 環境での Oracle ディレクトリ・サーバー	26-3
基本的な高い可用性の構成の Oracle Internet Directory	26-3
デフォルトの N ノード構成の Oracle Internet Directory	26-7
Oracle9i Real Application Clusters 環境での Oracle ディレクトリ・レプリケーション・サーバー	26-12

第 VII 部 ディレクトリ・プラグイン

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

ディレクトリ・サーバー・プラグインの概要	27-2
操作ベースのプラグイン	27-3
プラグインの登録	27-4
orclPluginConfig オブジェクト・クラス	27-4
コマンドライン・ツールによるプラグイン・エントリの追加	27-5
例 1	27-5
例 2	27-6

第 VIII 部 Oracle Directory Integration Platform

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

Oracle Directory Integration Platform	28-2
Oracle Directory Integration Platform が必要な理由	28-2
Oracle Directory Integration Platform の構造	28-3
プロビジョニングと同期との対比	28-5
プロビジョニング	28-5
同期	28-6
プロビジョニングと同期の相違点	28-6
ディレクトリ同期サービス	28-7
プロビジョニング統合サービス	28-8
Oracle Directory Integration Server	28-10

ディレクトリ統合ツールキット	28-11
管理ツールと監視ツール	28-12
Oracle Directory Manager	28-12
OID 制御と OID モニター	28-12
Oracle Enterprise Manager	28-13
Oracle Directory Integration Platform のサンプル配置	28-13
全体的な配置	28-14
ユーザーの作成とプロビジョニング	28-15
ユーザー・プロパティの変更	28-16
ユーザーの削除	28-17

29 Oracle Directory Synchronization Service

コネクタとディレクトリ統合プロファイルの概要	29-2
コネクタ	29-2
ディレクトリ同期プロファイル	29-3
一意の形式によるディレクトリ	29-3
同期の使用例	29-4
Oracle Internet Directory から接続先ディレクトリへの同期	29-4
接続先ディレクトリから Oracle Internet Directory への同期	29-4
コネクタの Oracle Directory Integration Platform への登録	29-5
追加コネクタ構成情報	29-9
マッピング・ルールとその形式	29-10
マッピング・ルールの更新	29-16
ファイルの位置とネーミング	29-18
同期プロファイルの管理	29-18
Oracle Directory Manager を使用したプロファイルの管理	29-18
Oracle Directory Manager を使用したプロファイルの登録	29-18
Oracle Directory Manager を使用したプロファイルの登録解除	29-23
コマンドラインによるコネクタの管理	29-23
コマンドライン・ツールによる同期プロファイルの作成	29-23
ldapdeleteConn.sh を使用したプロファイルの登録解除	29-25

30 Oracle Directory Integration Server の管理

Oracle Directory Integration Server の概要	30-2
Oracle Directory Integration Server の登録	30-3
Oracle Directory Integration Server の操作情報	30-4
Oracle Directory Integration Server と構成設定エントリ	30-4
Directory Integration Server イベントの標準の順序	30-6
メイン・スレッド・プロセスの順序	30-6
スケジューラ・プロセスの順序	30-6
コネクタ・プロセスの順序	30-7
構成設定エントリの管理	30-7
Oracle Directory Integration Server の管理	30-8
Oracle Directory Integration Server の起動	30-8
OID モニターと制御ユーティリティを使用した Oracle Directory Integration Server の起動	30-9
OID モニターと OID 制御ユーティリティを使用しない	
Oracle Directory Integration Server の起動	30-11
Oracle Directory Integration Server の停止	30-11
OID モニターと OID 制御ユーティリティを使用したサーバーの停止	30-11
OID モニターと OID 制御ユーティリティを使用しない	
Directory Integration Server の停止	30-12
restart コマンドの使用	30-13
デバッグ・レベルの設定	30-13
ログ・ファイルの検索	30-15
同期ステータス属性の変更	30-15
Oracle Directory Integration Server の情報の表示	30-15
Oracle Directory Manager を使用した Oracle Directory Integration Server の	
実行時情報の表示	30-16
ldapsearch を使用した Oracle Directory Integration Server の実行時情報の表示	30-16
レプリケート環境での Oracle Directory Integration Platform の管理	30-17

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

認証	31-2
Secure Sockets Layer (SSL) と Oracle Directory Integration Platform	31-2
Oracle Directory Integration Server の認証	31-2
非 SSL 認証	31-3
SSL モードでの認証	31-3
プロファイルの認証	31-4
アクセス制御と認可	31-4
Oracle Directory Integration Server に対するアクセス制御	31-4
エージェントに対するアクセス制御	31-5
データの整合性	31-6
データ・プライバシー	31-6
ツールのセキュリティ	31-6

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

接続先ディレクトリからの Oracle Internet Directory のブートストラップ	32-2
外部ツールを使用した Oracle Internet Directory へのデータ・インポート	32-2
コネクタの設定による Oracle Internet Directory へのデータ・インポート	32-2
Oracle Internet Directory からの接続先ディレクトリのブートストラップ	32-3
外部ツールを使用した OID からのデータ・エクスポート	32-3
コネクタの設定による OID からのデータ・エクスポート	32-3

33 Oracle Human Resources との同期化

概要	33-2
Oracle Human Resources からインポートできるデータ	33-2
Oracle Human Resources との同期の管理	33-4
Oracle Human Resources コネクタのディレクトリ統合プロファイルの構成	33-4
Oracle Internet Directory と同期化される属性のリストのカスタマイズ	33-8
Oracle Human Resources の同期化される属性の追加	33-10
Oracle Human Resources の同期化される属性の除外	33-11
構成ファイルでの SQL SELECT 文の構成による複雑な選択基準のサポート	33-11
Oracle Human Resources コネクタに関するマッピング・ルールのカスタマイズ	33-12
デフォルトの Oracle Human Resources コネクタのマッピング・ルール	33-13

Oracle Human Resources の属性マッピング・ルールを作成	33-14
Oracle Human Resources の属性マッピング・ルールの変更	33-15
Oracle Human Resources の属性マッピング・ルール削除	33-15
Oracle Human Resources から Oracle Internet Directory への同期の実行	33-16
同期の準備	33-16
同期化プロセス	33-17
Oracle HR からの Oracle Internet Directory のブートストラップ	33-18

34 iPlanet Directory Server との同期化

Oracle Internet Directory サーバーと iPlanet Directory Server 間を同期化する iPlanet コネクタ	34-2
iPlanet Directory Server 用の Oracle Internet Directory 統合ソリューションの構成	34-2
タスク 1: 同期化する双方のディレクトリの準備	34-3
タスク 2: iPlanet Directory Server 用の Oracle Internet Directory 統合ソリューションの統合プロファイルの構成	34-4
タスク 3: マッピング・ルール構成	34-8
タスク 4: アクセス制御の構成	34-8
タスク 5: パスワード保護の構成	34-9
Oracle Internet Directory と iPlanet Directory Server 間の同期	34-10
同期の準備	34-10
同期化プロセス	34-10
トラブルシューティング	34-11
今回のリリースでの制限事項	34-11

35 サード・パーティのメタディレクトリ・ソリューションとの同期

変更ログ	35-2
外部エージェントと Oracle Internet Directory との同期化への対応	35-3
タスク 1: 初期ブートストラップの実行	35-3
タスク 2: 外部エージェント用変更サブスクリプション・オブジェクトの Oracle Internet Directory での作成	35-4
変更サブスクリプション・オブジェクトの概要	35-4
変更サブスクリプション・オブジェクトの作成	35-4

タスク 3: Oracle Internet Directory の変更ログ・オブジェクト・コンテナへの 外部エージェント・アクセス権の付与	35-5
同期化プロセス	35-6
接続先ディレクトリによって、最初に Oracle Internet Directory から変更を取得する方法	35-6
接続先ディレクトリによって、Oracle Internet Directory 内の orclLastAppliedChangeNumber 属性を更新する方法	35-7
変更サブスクリプション・オブジェクトの無効化と削除	35-8
変更サブスクリプション・オブジェクトの無効化	35-8
変更サブスクリプション・オブジェクトの削除	35-8

36 Oracle Directory Provisioning Integration Service

Oracle Directory Provisioning Integration Service の概要	36-2
プロビジョニングの概要	36-2
プロビジョニングの手順	36-2
アプリケーションでのユーザーの登録	36-3
プロビジョニング情報	36-3
Oracle Directory Provisioning Integration Service が、変更を Oracle Internet Directory から取得する方法	36-4
アプリケーションが、Oracle Directory Provisioning Integration Service を使用して、 プロビジョニング情報を取得する方法	36-7
Oracle Directory Provisioning Integration Service 環境の管理	36-9
概要 : Oracle Directory Provisioning Integration Service の配置	36-9
Oracle Directory Provisioning Integration Service の管理	36-9
Oracle Directory Integration Server の管理	36-9
プロビジョニング・プロファイルの管理	36-10
セキュリティと Oracle Directory Provisioning Integration Service	36-11
プロビジョニング・プロファイルへのアクセス制御の必要性	36-11
アクセス権限が必要なエンティティ	36-11
エンティティに付与されるエントリ・レベルの権限	36-12
エンティティに付与される属性レベルの権限	36-13
Oracle Directory Provisioning Integration Service のトラブルシューティング	36-15

第 IX 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 の構文	A-4
ldapaddmt の構文	A-6
ldapbind の構文	A-8
ldapcompare の構文	A-10
ldapdelete の構文	A-11
ldapmoddn の構文	A-13
ldapmodify の構文	A-15
ldapmodifymt の構文	A-20
ldapsearch の構文	A-22
ldapsearch フィルタの例	A-24
ldapUploadAgentFile.sh の構文	A-26
ldapCreateConn.sh の構文	A-27
StopOdiServer.sh の構文	A-29
プロビジョニング・サブスクリプション・ツールの構文	A-30
バルク・ツールの構文	A-33
bulkdelete の構文	A-33
bulkload の構文	A-34
bulkmodify の構文	A-36
ldifwrite の構文	A-38
カタログ管理ツールの構文	A-39
OID モニターの構文	A-41
OID モニターの開始	A-41
OID モニターの停止	A-42
OID 制御ユーティリティの構文	A-42
Oracle ディレクトリ・サーバー・インスタンスの起動と停止	A-43
Oracle ディレクトリ・サーバー・インスタンスの起動	A-43
Oracle ディレクトリ・サーバー・インスタンスの停止	A-44
Oracle ディレクトリ・レプリケーション・サーバー・インスタンスの起動と停止	A-45
Oracle ディレクトリ・レプリケーション・サーバー・インスタンスの起動	A-45
Oracle ディレクトリ・レプリケーション・サーバー・インスタンスの停止	A-46

ディレクトリ・サーバー・インスタンスの再起動	A-46
ディレクトリ・サーバー・インスタンスの起動に関するトラブルシューティング	A-47
OID データベース・パスワード・ユーティリティの構文	A-48
管理者操作キュー操作ツールの構文	A-49
管理者操作キューからリトライ・キューへの変更の移動	A-49
管理者操作キューからページ・キューへの変更の移動	A-50
例: 管理者操作キュー操作ツールの使用	A-51
例: 変更の再試行と廃棄	A-51
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	A-51
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	A-51
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	A-51
OID 調停ツールの構文	A-52
OID 調停ツールを使用した一貫性のないデータの調停	A-52
OID 調停ツールの動作	A-53
OID データベース統計収集ツールの構文	A-55
SchemaSync の構文	A-56

B アクセス制御ディレクティブ書式

orclACI のスキーマ	B-2
orclEntryLevelACI のスキーマ	B-3

C スキーマ要素

Oracle Internet Directory で施行されている IETF Requests for Comments (RFC)	C-2
Oracle Internet Directory で施行されている IETF Draft	C-3
Oracle Internet Directory 独自のスキーマ要素	C-3
LDAP 構文	C-7
Oracle Internet Directory で施行されている LDAP 構文	C-7
Oracle Internet Directory が認識する、一般的に使用されている LDAP 構文	C-8
Oracle Internet Directory が認識する、その他の LDAP 構文	C-9
属性値のサイズ	C-9
一致規則	C-10
ユーザーを表現するスキーマ	C-11

D Oracle Wallet Manager

概要	D-2
Wallet の管理	D-3
Oracle Wallet Manager の起動	D-4
Wallet の新規作成	D-4
既存の Wallet のオープン	D-5
Wallet のクローズ	D-5
変更の保存	D-5
オープンしている Wallet の新しい位置への保存	D-6
システム・デフォルトへの保存	D-6
Wallet の削除	D-7
パスワードの変更	D-7
自動ログインの使用方法	D-8
自動ログインの有効化	D-8
自動ログインの無効化	D-8
Oracle Application Server での Oracle Wallet Manager の使用方法	D-8
証明書の管理	D-9
ユーザー証明書の管理	D-9
証明書要求の作成	D-9
ユーザーの証明書要求のエクスポート	D-11
Wallet へのユーザー証明書のインポート	D-11
Wallet からのユーザー証明書の削除	D-12
信頼できる証明書の管理	D-12
信頼できる証明書のインポート	D-12
信頼できる証明書の削除	D-14
信頼できる証明書のエクスポート	D-14
信頼できるすべての証明書のエクスポート	D-15
Wallet のエクスポート	D-15

E Oracle Internet Directory のアップグレード

単一ノード環境でのアップグレード	E-18
マルチノード環境でのアップグレード	E-18
LDIF ベースのアップグレード	E-18
タスク 1: 旧リリースの Oracle Internet Directory のバックアップ	E-18
タスク 2: Oracle Internet Directory リリース 3.0.1 の新規インストールの実行	E-19
タスク 3: Oracle Internet Directory の以前のバージョンからの、 ユーザー定義のスキーマとデータのリストア	E-19
タスク 4: Oracle Internet Directory プロセスの開始	E-20
スタンドアロンの Oracle Internet Directory ノードのアップグレード	E-21
タスク 1: 以前のバージョンのノード上にある Oracle ディレクトリ・サーバーの停止	E-21
タスク 2: エクスポート・ユーティリティを使用したスポンサ・ノードのバックアップ	E-22
タスク 3: インポート・ユーティリティを使用した新規ノードへのデータのロード	E-22
タスク 4: Oracle Internet Directory スキーマのアップグレードの実行	E-23

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
LDAP 準拠のディレクトリからデータを移行するためのタスク	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 ファイルからの独自のディレクトリ・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 LDAP フィルタ定義

H **トラブルシューティング**

インストール時のエラー	H-10
管理エラー・メッセージとその原因	H-10
スキーマ変更が原因の Oracle データベース・サーバー・エラー	H-10
Oracle ディレクトリ・サーバーから戻される標準エラー・メッセージ	H-10
その他のエラー・メッセージ	H-14
パスワード・ポリシー違反のエラー・メッセージ	H-17

I **ユーザー・データのアプリケーション固有リポジトリからの移行**

アプリケーション固有リポジトリからの移行の概要	I-2
アプリケーション固有のリポジトリからデータを移行するためのタスク	I-3
タスク 1: 中間テンプレート・ファイルの作成	I-3
例: 中間テンプレート・ファイル内のユーザー・エントリ	I-4
ユーザー・エントリの属性	I-5
タスク 2: OID Migration Tool の実行	I-7
OID Migration Tool	I-7
例: OID Migration Tool の使用	I-10
参照モードでの移行ツールの使用	I-10
参照オプションを指定しない場合の OID Migration Tool の使用	I-11
参照モードで取得した置換変数値のオーバーライド	I-11
OID Migration Tool のエラー・メッセージ	I-12

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。

この章では、次の項目について説明します。

- [対象読者](#)
- [このマニュアルの構成](#)
- [関連文書](#)
- [表記規則](#)

対象読者

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

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

このマニュアルの構成

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

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

表 1 各管理タスク領域に関連する項

管理タスク領域	このマニュアルの関連する項
ルーチン管理	第 II 部 : 基本的なディレクトリ管理 第 III 部 : ディレクトリのセキュリティ
企業およびホスティングされた環境でのディレクトリ計画と配置	第 III 部 : ディレクトリのセキュリティ 第 IV 部 : ディレクトリ配置 第 V 部 : ディレクトリ・レプリケーション 第 VI 部 : Oracle Internet Directory およびクラスタ 第 VII 部 : Oracle Internet Directory プラグイン
Oracle Internet Directory とその他のディレクトリとの統合	第 VIII 部 : Oracle Directory Integration Platform

第 I 部：スタート・ガイド

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

第 1 章「概要」

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

第 2 章「概念およびアーキテクチャ」

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

第 3 章「事前に実行するタスクと情報」

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

第 4 章「ディレクトリ管理ツール」

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

第 II 部：基本的なディレクトリ管理

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

第 5 章「Oracle ディレクトリ・サーバーの管理」

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

第 6 章「ディレクトリ・スキーマの管理」

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

第 7 章「ディレクトリ・エントリの管理」

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

第 8 章「ディレクトリにおける グローバリゼーション・サポート」

この章では、Oracle Internet Directory で使用されるグローバリゼーション・サポートについて説明します。

第 9 章「Delegated Administration Service」

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

第 10 章「属性一意性」

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

第 III 部：ディレクトリのセキュリティ

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

第 11 章「ディレクトリ・セキュリティの概要」

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

第 12 章「Secure Sockets Layer (SSL) とディレクトリ」

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

第 13 章「ディレクトリ・アクセス制御」

この章では、アクセス制御ポリシー・ポイントの概要を提供し、ディレクトリ・アクセスの管理方法について説明します。

第 IV 部 : ディレクトリ配置

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

第 14 章「一般的な配置の考慮事項」

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

第 15 章「Oracle のコンポーネントと Oracle Internet Directory」

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

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

第 16 章「ディレクトリ・ベースのアプリケーション・セキュリティ」

この章では、Oracle Internet Directory でのアクセス制御ポリシー・ポイントの格納方法を活用して、大企業やホスティングされた環境でアプリケーションを保護する方法について説明します。

第 17 章「ユーザー認証資格証明のディレクトリ格納」

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

第 18 章「パスワード・ポリシー」

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

第 19 章「容量計画に関する考慮事項」

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

第 20 章「チューニングに関する考慮事項」

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

第 21 章「高い可用性とフェイルオーバーに関する考慮事項」

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

第 V 部：ディレクトリ・レプリケーション

第 V 部では、レプリケーションとその管理方法について詳しく説明します。

第 22 章「ディレクトリ・レプリケーションの概要」

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

第 23 章「Oracle ディレクトリ・レプリケーション・サーバーの管理」

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

第 24 章「データベース・コピー・プロシージャを使用したノードの追加」

この章では、ディレクトリが非常に大きい場合に、レプリケート・ディレクトリ・システムにノードを追加するための代替方法について説明します。

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

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

第 25 章「クラスタ構成でのフェイルオーバー」

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

第 26 章「Oracle9i Real Application Clusters 環境でのディレクトリ・フェイルオーバー」

この章では、Oracle9i Real Application Clusters のシステムで Oracle Internet Directory を実行する方法について説明します。

第 VII 部 : Oracle Internet Directory プラグイン

第 27 章「Oracle Internet Directory のプラグイン・フレームワーク」

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

第 VIII 部 : Oracle Directory Integration Platform

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

第 28 章「Oracle Directory Integration Platform の概要とコンポーネント」

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

第 29 章「Oracle Directory Synchronization Service」

この章では、ディレクトリ統合エージェントと、ディレクトリ統合エージェントが Oracle Directory Integration Platform で実行する操作について説明します。ここでは、Oracle Directory Manager/ コマンドライン・ツールを使用してパートナ・エージェントを管理する方法を示します。

第 30 章「Oracle Directory Integration Server の管理」

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

第 31 章「Oracle Directory Integration Platform におけるセキュリティ」

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

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

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

第 33 章「Oracle Human Resources との同期化」

従業員のデータを Oracle Internet Directory に格納しており、Oracle Human Resources を使用して、このデータを作成、変更および削除する場合は、両者の間でデータが同期していることを確認する必要があります。この章では、この操作を可能にする Oracle Human Resources エージェントについて説明します。

第 34 章「iPlanet Directory Server との同期化」

この章では、iPlanet Directory Server 用の Oracle Internet Directory 統合ソリューションを使用して、Oracle Internet Directory と iPlanet Directory Server を同期化する方法について説明します。

第 35 章「サード・パーティのメタディレクトリ・ソリューションとの同期」

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

第 36 章「Oracle Directory Provisioning Integration Service」

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

第 IX 部：付録

付録 A「LDIF およびコマンドライン・ツールの構文」

この付録では、LDAP 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「アクセス制御ディレクティブ書式」

この付録では、アクセス制御情報アイテム (ACI) の書式 (構文) について説明します。

付録 C「スキーマ要素」

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

付録 D「Oracle Wallet Manager」

この付録では、Wallet と証明書を作成および管理するために Oracle Wallet Manager を使用する方法について説明します。

付録 E「Oracle Internet Directory のアップグレード」

この付録では、Oracle Internet Directory リリース 2.1.1 から Oracle Internet Directory リリース 9.0.2 へアップグレードする方法について説明します。

付録 F「他の LDAP 準拠のディレクトリからのデータの移行」

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について説明します。

付録 G「LDAP フィルタ定義」

この付録（**Internet Engineering Task Force (IETF)** の許可によりコピー）では、読みおよび更新のアクセス権を提供するディレクトリ・アクセス・プロトコルについて説明します。

付録 H「トラブルシューティング」

この付録では、発生する可能性がある障害とエラー・コードおよび考えられる原因について説明します。

付録 I「ユーザー・データのアプリケーション固有リポジトリからの移行」

この付録では、中間テンプレート・ファイルを作成して OID Migration Tool を実行し、アプリケーション固有のリポジトリからデータを移行する方法について説明します。

関連文書

詳細は、次のマニュアルを参照してください。

- Oracle Directory Manager、Delegated Administration Service および Oracle Enterprise Manager から使用できるオンライン・ヘルプ
- Oracle9i Application Server および Oracle9i データベース・サーバーのドキュメント・セット。特に次のマニュアルを参照してください。
 - 『Oracle Internet Directory アプリケーション開発者ガイド』
 - 『Oracle9i データベース管理者ガイド』
 - 『Oracle9i アプリケーション開発者ガイド - 基礎編』
 - 『Oracle9i Application Server 管理者ガイド』
 - 『Oracle9i Net Services 管理者ガイド』
 - 『Oracle9i Real Application Clusters 管理』
 - 『Oracle9i レプリケーション』
 - 『Oracle Advanced Security 管理者ガイド』

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

<http://otn.oracle.co.jp/membership/>

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

<http://otn.oracle.co.jp/document/>

詳しい情報は、次を参照してください。

- 『Chadwick, David, Understanding X.500 - The Directory. Thomson Computer Press, 1996』
- 『Howes, Tim and Mark Smith, LDAP: Programming Directory-enabled Applications with Lightweight Directory Access Protocol. Macmillan Technical Publishing, 1997』
- 『Howes, Tim, Mark Smith and Gordon Good, Understanding and Deploying LDAP Directory Services. Macmillan Technical Publishing, 1999』
- <http://www.iana.org> (Internet Assigned Numbers Authority のホームページ。オブジェクト識別子に関する情報)
- 次を初めとする Internet Engineering Task Force (IETF) のドキュメント。
 - <http://www.ietf.org> (IETF のホームページ)
 - <http://www.ietf.org/html.charters/ldapext-charter.html> (ldapext の Charter と LDAP Draft)
 - <http://www.ietf.org/html.charters/ldup-charter.html> (LDUP の Charter と Draft)
 - <http://www.ietf.org/rfc/rfc2254.txt>、『The String Representation of LDAP Search Filters』
 - <http://www.ietf.org/rfc/rfc1823.txt>、『The LDAP Application Program Interface』
- <http://www.openldap.org> (OpenLDAP Community)

表記規則

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

- [本文中の表記規則](#)
- [コード例の表記規則](#)
- [Windows オペレーティング・システムの表記規則](#)

本文中の表記規則

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

規則	意味	例
太字	太字は、本文中に定義されている用語または用語集に含まれている用語、あるいはその両方を示します。	この句を指定する場合は、 索引構成表 を作成します。
固定幅フォントの大文字	固定幅フォントの大文字は、システムにより指定される要素を示します。この要素には、パラメータ、権限、データ型、Recovery Manager キーワード、SQL キーワード、SQL*Plus またはユーティリティ・コマンド、パッケージとメソッド、システム指定の列名、データベース・オブジェクトと構造体、ユーザー名、およびロールがあります。	この句は、NUMBER 列に対してのみ指定できます。 BACKUP コマンドを使用すると、データベースのバックアップを作成できます。 USER_TABLES データ・ディクショナリ・ビューの TABLE_NAME 列を問い合わせます。 DBMS_STATS.GENERATE_STATS プロシージャを使用します。
固定幅フォントの小文字	固定幅フォントの小文字は、実行可能ファイル、ファイル名、ディレクトリ名およびサンプルのユーザー指定要素を示します。この要素には、コンピュータ名とデータベース名、ネット・サービス名、接続識別子の他、ユーザー指定のデータベース・オブジェクトと構造体、列名、パッケージとクラス、ユーザー名とロール、プログラム・ユニット、およびパラメータ値があります。 注意： 一部のプログラム要素には、大文字と小文字の両方が使用されます。この場合は、記載されているとおりに入力してください。	sqlplus と入力して SQL*Plus をオープンします。 パスワードは orapwd ファイルに指定されています。 データ・ファイルと制御ファイルのバックアップを /disk1/oracle/dbs ディレクトリに作成します。 department_id、department_name および location_id の各列は、hr.departments 表にあります。 初期化パラメータ QUERY_REWRITE_ENABLED を true に設定します。 oe ユーザーで接続します。 これらのメソッドは JRepUtil クラスに実装されます。

規則	意味	例
固定幅フォントの小文字のイタリック	固定幅フォントの小文字のイタリックは、プレースホルダまたは変数を示します。	<code>Uold_release.SQL</code> を実行します。 <code>old_release</code> は、アップグレード前にインストールしたリリースです。

コード例の表記規則

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

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

次の表は、コード例の記載上の表記規則と使用例を示しています。

規則	意味	例
[]	大カッコで囲まれている項目は、1 つ以上のオプション項目を示します。大カッコ自体は入力しないでください。	<code>DECIMAL (digits [, precision])</code>
{ }	中カッコで囲まれている項目は、そのうちの 1 つのみが必要であることを示します。中カッコ自体は入力しないでください。	<code>{ENABLE DISABLE}</code>
	縦線は、大カッコまたは中カッコ内の複数の選択肢を区切るために使用します。オプションのうち 1 つを入力します。縦線自体は入力しないでください。	<code>{ENABLE DISABLE}</code> <code>[COMPRESS NOCOMPRESS]</code>
...	水平の省略記号は、次のどちらかを示します。 <ul style="list-style-type: none">■ 例に直接関係のないコード部分が省略されていること。■ コードの一部が繰り返し可能であること。	<code>CREATE TABLE ... AS subquery;</code> <code>SELECT col1, col2, ... , coln FROM employees;</code>
.	垂直の省略記号は、例に直接関係のない数行のコードが省略されていることを示します。	<code>SQL> SELECT NAME FROM V\$DATAFILE;</code> <code>NAME</code> ----- <code>/fsl/dbs/tbs_01.dbf</code> <code>/fsl/dbs/tbs_02.dbf</code> <code>.</code> <code>.</code> <code>.</code> <code>/fsl/dbs/tbs_09.dbf</code> <code>9 rows selected.</code>

規則	意味	例
その他の表記	大カッコ、中カッコ、縦線および省略記号以外の記号は、示されているとおりに入力してください。	acctbal NUMBER(11,2); acct CONSTANT NUMBER(4) := 3;
イタリック	イタリックの文字は、特定の値を指定する必要があるプレースホルダまたは変数を示します。	CONNECT SYSTEM/system_password DB_NAME = database_name
大文字	大文字は、システムにより指定される要素を示します。これらの用語は、ユーザー定義用語と区別するために大文字で記載されています。大カッコで囲まれている場合を除き、記載されているとおりの順序とスペルで入力してください。ただし、この種の用語は大 / 小文字区別がないため、小文字でも入力できます。	SELECT last_name, employee_id FROM employees; SELECT * FROM USER_TABLES; DROP TABLE hr.employees;
小文字	小文字は、ユーザー指定のプログラム要素を示します。たとえば、表名、列名またはファイル名を示します。 注意： 一部のプログラム要素には、大文字と小文字の両方が使用されます。この場合は、記載されているとおりに入力してください。	SELECT last_name, employee_id FROM employees; sqlplus hr/hr CREATE USER mjjones IDENTIFIED BY ty3MU9;

Windows オペレーティング・システムの表記規則

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

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

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

規則	意味	例
ORACLE_HOME および ORACLE_BASE	<p>Oracle8i リリース 8.0 以前では、Oracle コンポーネントをインストールすると、すべてのサブディレクトリはトップレベルの ORACLE_HOME ディレクトリの下にあります。ORACLE_HOME ディレクトリの名前は、デフォルトでは次のとおりです。</p> <ul style="list-style-type: none">■ C:¥orant (Windows NT の場合)■ C:¥orawin98 (Windows 98 の場合) <p>このリリースは、Optimal Flexible Architecture (OFA) のガイドラインに準拠しています。すべてのサブディレクトリがトップレベルの ORACLE_HOME ディレクトリの下にあるわけではありません。このリリースでは、最上位ディレクトリとして ORACLE_BASE があり、デフォルトでは C:¥oracle になります。他の Oracle ソフトウェアがインストールされていないコンピュータに Oracle9i リリース 1 (9.0.1) をインストールすると、最初の Oracle ホーム・ディレクトリのデフォルト設定は C:¥oracle¥ora90 となります。この Oracle ホーム・ディレクトリは、ORACLE_BASE の直下のディレクトリです。</p> <p>このマニュアルでは、ディレクトリ・パスの例はすべて OFA 規則に従っています。</p>	%ORACLE_HOME%¥rdbms¥admin ディレクトリへ移動します。

Oracle Internet Directory の新機能

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

- [Oracle Internet Directory リリース 9.0.2 で導入された新機能](#)
- [Oracle Internet Directory リリース 3.0.1 で導入された新機能](#)
- [Oracle Internet Directory リリース 2.1.1 で導入された新機能](#)

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

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

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

関連項目： 20-12 ページの「[エントリ・キャッシング](#)」

- **新しいディレクトリ統合機能**— Oracle Internet Directory リリース 9.0.2 では、他のアプリケーションやリポジトリ（Oracle および Oracle 以外で作成された）との新しい種類の接続が導入されました。新しい Oracle Directory Provisioning Integration Service および Oracle Directory Synchronization Service は、Oracle Directory Integration Platform (Oracle8i の Oracle Internet Directory リリース 2.1.1.1 で導入) 上に構築されます。
- **Oracle Directory Provisioning Integration Service** —プロビジョニングとは、ビジネス・ルールに基づいて、アプリケーション・リソースに対するユーザーのアクセス権を付与または取り消すプロセスです。ユーザーとは、人間であるエンド・ユーザーまたはアプリケーションの場合があります。

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

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

関連項目： 第 28 章「[Oracle Directory Integration Platform の概要とコンポーネント](#)」

- **エンタープライズ・パスワード・ポリシー管理の拡張** 一次の機能を使用して、パスワード・ポリシーを構成できるようになりました。
 - 有効期限
 - 猶予期間
 - パスワードの必要最小限の長さ
 - 許可されるパスワード構文および再試行制限
 - ディレクトリ・サービスへの不正なアクセス試行のロックアウト（指定した回数を超えてアクセスに失敗した場合）

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

- **MD4**: 128 ビットのハッシュを生成する一方向ハッシュ関数です。
- **MD5**: MD4 を改善した、より複雑なバージョンです。
- **SHA**: Secure Hash Algorithm。MD5 よりも長い 160 ビットのハッシュを生成します。このアルゴリズムは MD5 よりも若干速度が遅くなりますが、大きなメッセージ・ダイジェストによって、総当たり攻撃や反転攻撃に対処できます。

salted SHA も使用できます。**salt** は、ハッシュ値に追加され、ハッシュ値とともに格納される乱数です。このソルトは、当初のハッシュ値のリカバリに極端にコストがかかるようにすることで、事前に算出されたディクショナリによる攻撃を回避します。

- **UNIX Crypt**: UNIX 暗号化アルゴリズムです。
- ハッシングなし

関連項目：

- 概念の説明は、11-7 ページの「[ディレクトリ認証用ユーザー・パスワードの保護](#)」を参照してください。
 - パスワード・ハッシングの設定方法は、[第 18 章「パスワード・ポリシー」](#)を参照してください。
- **属性一意性** 以前の Oracle Internet Directory アーキテクチャでは、属性一意性を規定する唯一の方法は、属性をユーザーの識別名の一部にすることでした。この方法は、ユーザー識別子（相対識別名として使用されている場合）には有効でしたが、必ずしも適切かつ簡単に構成できるわけではありませんでした。属性は、ツリー分岐の 1 レベル内で一意性を保証されていました。たとえば、識別名が **uid=dlin, ou=people, o=oracle** の場合、この識別名は **ou=people** の直下で一意でした。ただし、別の分岐（たとえば、**uid=dlin, ou=others, o=oracle**）では、同じユーザー識別子を使用できました。つまり、属性一意性は、指定された分岐の 1 レベル内でのみ保証されていました。

Oracle Internet Directory と同期化するアプリケーションでは、識別名以外の属性を一意キーとして使用できます。属性一意性を規定する Oracle Internet Directory のこの機能によって、すべてのアプリケーションは、それぞれ独自のユーザーに関する認識を持ち、ユーザー・ベースを企業の Oracle Internet Directory サーバーに格納されているユーザー・リポジトリと同期化することができます。

- **複数パスワード・ベリファイアのサポート**— Oracle Internet Directory では、複数のアプリケーションやプロトコルに対するパスワードを格納できるようになりました。たとえば、ボイスメールの個人識別番号 (PIN) 4 桁を、同一のユーザーに対するより長い英数字のシングル・サインオン・パスワードと X509 v3 のデジタル証明書とともに保持できます。この新機能によって、アプリケーション開発者には、ディレクトリ対応の製品スタックについて高い柔軟性が与えられます。

関連項目： [第 17 章「ユーザー認証資格証明のディレクトリ格納」](#)

- **拡張されたプロキシ・ユーザー機能**— この新機能によって、開発者は中間層の能力をより有効に活用できます。ユーザーは、独立した、ディレクトリとは無関係なセッションを確立する必要はありません。中間層が Oracle9i Application Server などからプロキシ・ユーザーのバインド方法を、多数のクライアントにかわって連続して起動する場合、実際のバインドを行うエージェントが全体にわたって変わらないときにも、Oracle Internet Directory は、各クライアントの資格証明と権限をそれぞれ考慮します。

関連項目：

- [第 11 章「ディレクトリ・セキュリティの概要」](#)
- [5-18 ページの「スーパー・ユーザー、ゲスト・ユーザーおよびプロキシ・ユーザーの管理」](#)
- **Oracle9i Application Server のコンポーネントとの統合**— Oracle Directory Provisioning Integration Service を介して、Oracle Internet Directory リリース 9.0.2 は Oracle9i Application Server の中央コンポーネントとして機能します。Oracle9i Application Server の各コンポーネントは、有効なユーザー識別子とそのパスワードなど、共通のコンポーネント間メタデータの格納に Oracle Internet Directory を使用できるようになりました。

関連項目： [第 15 章「Oracle のコンポーネントと Oracle Internet Directory」](#)

- **Delegated Administration Service セルフ・サービス・コンソール**—この新機能によって、中央のチームから、または分散化と委任を介して、アプリケーション、サブスクライバおよびエンド・ユーザーを柔軟に管理できます。

Delegated Administration Service セルフ・サービス・コンソールによって、許可されたエンド・ユーザーは、パーソナライズされた作業環境の表示および自身の Oracle9iAS Single Sign-On パスワードの更新を行うことができます。また、個人および他のディレクトリ・ベースのリソース情報を Oracle Internet Directory で検索するための直観的なユーザー・インタフェースを提供します。

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

関連項目： 第9章「[Delegated Administration Service](#)」

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

関連項目： 5-23 ページの「[ディレクトリ・サーバーの監視、デバッグおよび監査](#)」

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

高水準の OEM GUI では使用できなかったディレクトリ固有の構成タスクまたはメンテナンス・タスクが、Oracle Internet Directory が提供するコマンドライン・インタフェースに加えて、Oracle Directory Manager を介して実行できるようになりました。

関連項目： 第4章「[ディレクトリ管理ツール](#)」

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

関連項目： [第 27 章「Oracle Internet Directory のプラグイン・フレームワーク」](#)

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

関連項目： [5-36 ページの「別名エントリの間接参照」](#)

- **Delegated Administration Service の拡張**

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

- 他の領域または部門の管理者の作成
- 特定の領域または部門のユーザーを管理する特定の委任権限の付与

Oracle Internet Directory セルフ・サービス・コンソールは、統一されたリソースをディレクトリ管理者、ディレクトリ・サービス・サブスクライバおよびエンド・ユーザーに提供します。

関連項目： [第 9 章「Delegated Administration Service」](#)

- **アップグレード手順**

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

関連項目： [付録 E「Oracle Internet Directory のアップグレード」](#)

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

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

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

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

関連項目： 14-12 ページの「[1 つのホストにおける複数の Oracle Internet Directory インストールの実行](#)」

- **Delegated Administration Service**

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

関連項目： [第 9 章「Delegated Administration Service」](#)

- **クラスタ構成でのフェイルオーバー**

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

関連項目： [第 25 章「クラスタ構成でのフェイルオーバー」](#)

- **Oracle9i Real Application Clusters 環境でのフェイルオーバー**

Oracle9i Real Application Clusters は、複数の、相互接続されたコンピュータの処理能力を活用するコンピューティング環境です。Oracle9i Real Application Clusters は、クラスタと呼ばれるハードウェアの集合とともに、各コンポーネントの処理能力を単一の、強力なコンピューティング環境にまとめます。クラスタは、ノードとも呼ばれる 2 つ以上のコンピュータで構成されます。

Oracle9i Real Application Clusters システムで Oracle Internet Directory を実行できます。

関連項目： [第 26 章「Oracle9i Real Application Clusters 環境でのディレクトリ・フェイルオーバー」](#)

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

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

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

- **Oracle Directory Integration Platform**

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

関連項目： 第 VIII 部：「[Oracle Directory Integration Platform](#)」

- **パスワード・ポリシーの管理**

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

関連項目：

- 概念の説明は、「[パスワード・ポリシー](#)」を参照してください。
- [第 18 章「パスワード・ポリシー」](#)

- **パフォーマンスと拡張性の強化**
- **アップグレード手順**

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

関連項目： [付録 E「Oracle Internet Directory のアップグレード」](#)

- **UTF8 制限の削除**

Oracle ディレクトリ・サーバーとデータベース・ツールの実行を UTF8 データベース上に限定する制限はなくなりました。

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

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

■ 属性オプション（言語コードを含む）

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

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

関連項目：

- 概念の説明は、2-7 ページの「[属性オプション](#)」を参照してください。
- 7-10 ページの「[Oracle Directory Manager を使用した属性オプション付きエントリの管理](#)」
- 7-14 ページの「[コマンドライン・ツールを使用した属性オプション付きエントリの管理](#)」

■ 変更ログの削除機能拡張

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

関連項目：

- 概念の説明は、22-6 ページの「[変更ログの削除](#)」を参照してください。
- 23-13 ページの「[ディレクトリ・レプリケーション・サーバーの構成パラメータの変更](#)」

■ 次の操作属性の拡張サポート

- `creatorsName`
- `createTimestamp`
- `modifiersName`
- `modifyTimestamp`

この拡張サポートを使用して、これらの属性を1つ以上、検索に使用できます。

関連項目：

- 概念の説明は、2-5 ページの「[属性情報の種類](#)」を参照してください。
- `createTimestamp` 属性を使用した検索操作の例は、A-25 ページの「[例 7: 全ユーザー属性および指定した操作属性の検索](#)」を参照してください。

■ **他の LDAP 準拠のディレクトリからの移行**

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

関連項目： [付録 F「他の LDAP 準拠のディレクトリからのデータの移行」](#)

■ **オブジェクト・クラスの増加**

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

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

■ **OID データベース統計収集ツール**

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

関連項目： 4-16 ページの「[OID データベース統計収集ツールの使用方法](#)」

■ **パスワード保護機能の拡張**

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

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

- ハッシングなし

関連項目：

- 概念の説明は、11-7 ページの「[ディレクトリ認証用ユーザー・パスワードの保護](#)」を参照してください。
- パスワード・ハッシングの設定方法は、第 18 章「[パスワード・ポリシー](#)」を参照してください。

- レプリケーション・ツール

次の新しいレプリケーション・ツールが追加されました。

- **管理者操作キュー操作ツール**

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

- **OID 調停ツール**

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

関連項目：

- このツールの簡単な説明は、4-15 ページの「[レプリケーション・ツールの使用方法](#)」を参照してください。
- 23-32 ページの「[管理者操作キュー操作ツールの使用](#)」
- 23-32 ページの「[OID 調停ツールの使用](#)」

- レプリケーション・ノードの削除

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

関連項目： 23-28 ページの「[レプリケーション・ノードの削除](#)」

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

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

注意： この機能は、リリース 9.0.2 で Oracle Directory Integration Platform に置き換えられました。詳細は、第 28 章「[Oracle Directory Integration Platform の概要とコンポーネント](#)」を参照してください。

- **アップグレード手順（リリース 2.1.1 のみ）**

この新しい手順を使用して、Oracle Internet Directory リリース 2.0.4.x またはリリース 2.0.6 からアップグレードできます。リリース 2.1.1.1 またはリリース 9.0.2 では、この機能はサポートされていません。

関連項目： [付録 E「Oracle Internet Directory のアップグレード」](#)

第 I 部

スタート・ガイド

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

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

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

この章では、次の項目について説明します。

- ディレクトリとは
- LDAP とは
- Oracle Internet Directory とは
- Oracle 製品における Oracle Internet Directory の使用方法

ディレクトリとは

ディレクトリは、複雑な情報を簡単に検索できるように編成します。ディレクトリには、リソース（たとえば、人、図書館の本、百貨店の商品など）をリストし、それぞれに関する詳細情報を設定します。コンピュータ以外の場面（オフライン）で使用しているディレクトリの例としては、電話帳や図書館のカード目録、百貨店のカタログなどがあります。

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

この項では、次の項目について説明します。

- [拡大するオンライン・ディレクトリの役割](#)
- [問題：特別な用途を指定された多数のディレクトリ](#)

拡大するオンライン・ディレクトリの役割

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

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

- 従業員は、メール・クライアントを使用して、会社のインターネットのアドレス帳から電子メール・アドレスを調べます。
- メッセージ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・ディレクトリはデータベース（データの構造化された集合）ですが、[リレーショナル・データベース](#)にはなっていません。次の表はオンライン・ディレクトリをリレーショナル・データベースと対比しています。

オンライン・ディレクトリ

主に読込みを目的としています。一般的な使用例では、データの更新が比較的少なく、検索が多い傾向があります。

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。

ロケーションに依存しないように設計されています。ディレクトリ・アプリケーションは、問合せ中のサーバーに関係なく、配置環境全体にわたって常に同じ情報を参照していると想定しています。問合せ先のサーバーにローカルの情報が格納されていない場合、そのサーバーはその情報を取り出すか、クライアント・アプリケーションにその情報を透過的に示す必要があります。

情報をエントリに格納するように設計されています。これらのエントリは、従業員、E-Commerce パートナ、会議室、プリンタのような共有ネットワーク・リソースなど、管理が必要なリソースを表します。各エントリには、多数の属性が対応付けられます。それぞれの属性には1つ以上の値が割り当てられる場合があります。たとえば、person エントリの一般的な属性は、姓名、電子メール・アドレス、デフォルトのメール・サーバーのアドレス、パスワードまたは他のログイン資格証明、デジタル化された顔写真などです。

リレーショナル・データベース

主に書込みを目的としています。一般的な使用例では、トランザクションが連続的に記録され、検索が比較的少ない傾向があります。

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。

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。

リレーショナル表に行として情報を格納するように設計されています。

問題：特別な用途を指定された多数のディレクトリ

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

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

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

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

LDAP とは

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

この項では、次の項目について説明します。

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

LDAP と単純化されたディレクトリ管理

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

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

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

LDAP バージョン 3

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

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

関連項目：

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

Oracle Internet Directory とは

Oracle Internet Directory は、分散ユーザーやネットワーク・リソースに関する迅速な情報検索および情報の中央管理を可能にする、汎用ディレクトリ・サービスです。[Lightweight Directory Access Protocol \(LDAP\)](#) バージョン 3 と Oracle9i 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。

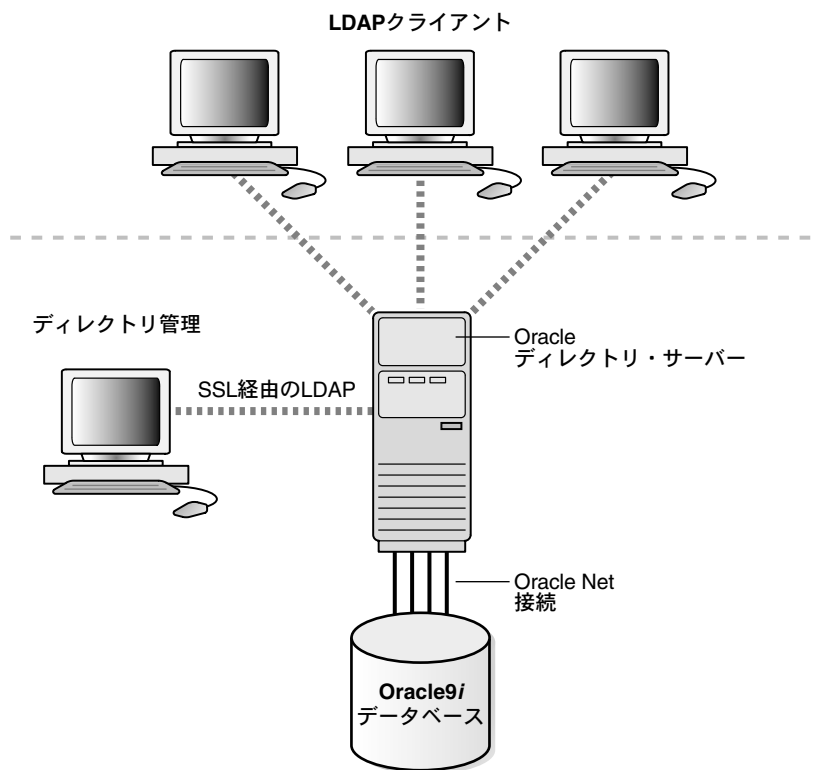
この項では、次の項目について説明します。

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

Oracle Internet Directory のアーキテクチャ

Oracle Internet Directory は Oracle9i 上のアプリケーションとして動作します。オペレーティング・システムに依存しない Oracle のデータベース接続ソリューションである Oracle Net Services を使用して、データベース（オペレーティング・システムが異なってもかまいません）と通信します。[図 1-1](#) はこの関係を示しています。

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



Oracle Internet Directory のコンポーネント

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

- Oracle ディレクトリ・サーバー。人員とリソースの情報に関するクライアントの要求に応答します。また、TCP/IP を介し、複数層アーキテクチャを直接使用して、その情報を更新します。
- Oracle ディレクトリ・レプリケーション・サーバー。Oracle ディレクトリ・サーバー間で、LDAP データをレプリケートします。
- ディレクトリ管理ツールには、次の内容が含まれます。
 - Oracle Directory Manager。Java ベースの Graphical User Interface (GUI) を使用してディレクトリの管理を簡素化します。
 - 各種のコマンドライン管理ツールとデータ管理ツール。これらは LDAP クライアントから呼び出されます。
 - Delegated Administration Service (DAS)。重要で複雑なディレクトリ管理タスクからグローバル・ディレクトリ管理者を解放します。DAS は、次の利点を備えた使いやすい Web インタフェースを提供して、管理者の負担を軽減します。
 - * エンド・ユーザーは、管理者の介入なしに自分のパスワードを変更できます。
 - * 非技術系マネージャなどの委任管理者が、ユーザーとグループの両方を作成および管理できます。
 - * すべてのユーザーが、アクセス権限のあるディレクトリの各部を検索できます。
 - OID サーバー・インスタンスを管理する Oracle Enterprise Manager の Web ベース・インタフェース内のツール。管理者は、これらのツールを使用して標準的なブラウザからリアルタイム・イベントや統計を監視でき、必要な場合は、これらの今後のデータを新しい履歴リポジトリに収集するプロセスを開始できます。
- Oracle Directory Integration Platform (Oracle Directory Integration Server を含む)。これを使用して、接続先ディレクトリやサブスクライブしたアプリケーションを Oracle Internet Directory と同期化できます。Oracle Directory Integration Platform を使用して独自の接続エージェントを開発し、配置することもできます。

関連項目： Oracle Directory Integration Platform の詳細は、第 VIII 部の「[Oracle Directory Integration Platform](#)」を参照してください。

Oracle Internet Directory の利点

Oracle Internet Directory の大きな利点は、拡張性、高い可用性、セキュリティおよび Oracle 環境との緊密な統合です。

拡張性

Oracle Internet Directory は、Oracle9i 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ル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、ディレクトリ・サーバー間における完全なマルチマスター・レプリケーションをサポートします。レプリケーション・コミュニティ内のサーバーの 1 つが使用できなくなった場合、ユーザーは別のサーバーからデータにアクセスできます。サーバー上にあるディレクトリのデータの変更情報は、Oracle9i データベース上の専用の表に格納されます。この表は、堅牢なレプリケーション方式である **Oracle9i レプリケーション** 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、Oracle9i 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、Oracle9i 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、Oracle9i データベースは、大規模なデータストアおよび高負荷で実行されていても、システム障害からすぐにリカバリできます。

セキュリティ

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

Oracle 環境との統合

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

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

Oracle Internet Directory によって、Oracle のコンポーネントは、簡単で対費用効果の高いアプリケーション環境の管理、集中化されたセキュリティ・ポリシー管理による厳重なセキュリティ、および企業の各分散ディレクトリ間での統合ポイントを実現できます。この項では、例を示して説明します。

簡単で対費用効果の高い管理

Oracle Net Services は、データベース・サービスと単純な名前（ネット・サービス名と呼ばれ、サービスを表すために使用できる）の格納と解決に **Oracle Internet Directory** を使用します。ネット・サービス名は、クライアントの接続文字列内で接続識別子として機能します。ディレクトリ・サーバーは、これらの接続識別子を接続記述子に変換し、クライアントに戻します。

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

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

統合されたセルフ・サービスのエンタープライズ・ポータル（**Oracle9iAS Portal** を使用）は、**Oracle Internet Directory** にアクセスして共通のユーザー属性とグループ属性を格納します。**Oracle9iAS Portal** 管理ツールは、特定のタスクに対しては **Delegated Administration Service** も利用します。

集中化されたセキュリティ・ポリシー管理による厳重なセキュリティ

Oracle9i は、**Oracle Internet Directory** を使用して、ユーザー名とパスワードを格納し、ユーザーを **SSL** ではなく **LDAP** メカニズムを使用して認証します。また、**Oracle Internet Directory** を使用して各ユーザーのエントリとともにパスワード・ベリファイアを格納します。

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

- ユーザー認証資格証明の集中管理

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

- ユーザー認可の集中管理

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

- 共有スキーマへのマッピング

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

- シングル・パスワード認証

Oracle9i では、Oracle Advanced Security によって、エンタープライズ・ユーザーは、単一の集中管理されたパスワードを使用して複数のデータベースに対する認証を実行できます。パスワードは、ユーザーのエントリの属性としてディレクトリに格納され、暗号化とアクセス制御リスト（ACL）によって保護されます。この機能によって、クライアントでの Secure Sockets Layer（SSL）の設定に関係するオーバーヘッドを削減し、複数のパスワードを記憶する必要性からユーザーを解放します。

- エンタープライズ・ユーザー・セキュリティ

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

- PKI 資格証明の集中格納

Oracle9i では、ユーザー Wallet をユーザーのエントリの属性としてディレクトリに格納できます。この機能によって、モバイル・ユーザーは、Enterprise Login Assistant を使用して Wallet を取得およびオープンできます。Wallet のオープン中は認証が透過的です。つまり、ユーザーは、スキーマを所有または共有しているデータベースに、再度認証せずにアクセスできます。

Oracle9iAS Single Sign-On は、Oracle Internet Directory を使用してユーザー・エントリを格納します。また、パートナ・アプリケーションのユーザーを Oracle Internet Directory エントリのユーザー・エントリにマップし、LDAP メカニズムを使用して認証します。

分散ディレクトリの統合

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

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

- Oracle のすべてのコンポーネントは、あらかじめ Oracle Internet Directory に統合されているため、ユーザーが各コンポーネントをディレクトリ・サービスに統合する必要はありません。
- サード・パーティの各ディレクトリを Oracle Internet Directory に統合することによって、Oracle 環境全体をサード・パーティ・ディレクトリに簡単に統合できます。各アプリケーションを各ディレクトリに時間をかけて統合する必要はありません。

概念およびアーキテクチャ

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

この章では、次の項目について説明します。

- エントリ
- 属性
- オブジェクト・クラス
- ネーミング・コンテキスト
- ディレクトリ・スキーマ
- セキュリティ
- グローバリゼーション・サポート
- Oracle Internet Directory のアーキテクチャ
- 例 : Oracle Internet Directory の動作
- 分散ディレクトリ
- Delegated Administration Service
- Oracle Directory Integration Platform

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、xxxix ページの「[関連文書](#)」を参照してください。

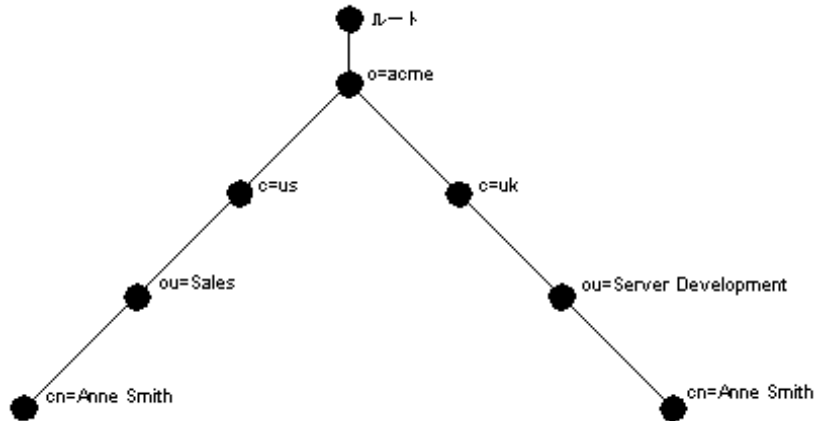
エントリ

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

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

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

図 2-1 ディレクトリ情報ツリー



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

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

この Anne Smith エントリの識別名は次のとおりです。

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

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

識別名内の最下位コンポーネントは**相対識別名**と呼ばれます。たとえば、前述の Anne Smith のエントリの相対識別名は cn=Anne Smith です。同様に、Anne Smith の相対識別名のすぐ上のエントリに対応する相対識別名は、ou=Server Development、ou=Server Development のすぐ上のエントリに対応する相対識別名は、c=uk です。識別名は、このように各相対識別名をカンマで区切って順に並べたものです。

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

エントリに対して迅速で効率的な操作を行うために、Oracle Internet Directory は、各エントリに一意の識別子を割り当て、指定された数の識別子をキャッシュ・メモリーに格納します。ユーザーがエントリに対する操作を行うと、ディレクトリ・サーバーは、キャッシュ内でエントリ識別子を検索し、対応するエントリをディレクトリから取得します。エントリ・キャッシングと呼ばれるこの方法によって、Oracle Internet Directory のパフォーマンスが強化されます。比較的小規模または中規模の企業では特に有用です。

注意： Oracle Internet Directory リリース 9.0.2 では、単一サーバー、単一インスタンスの Oracle Internet Directory ノードの場合にのみ、エントリ・キャッシングを使用できます。

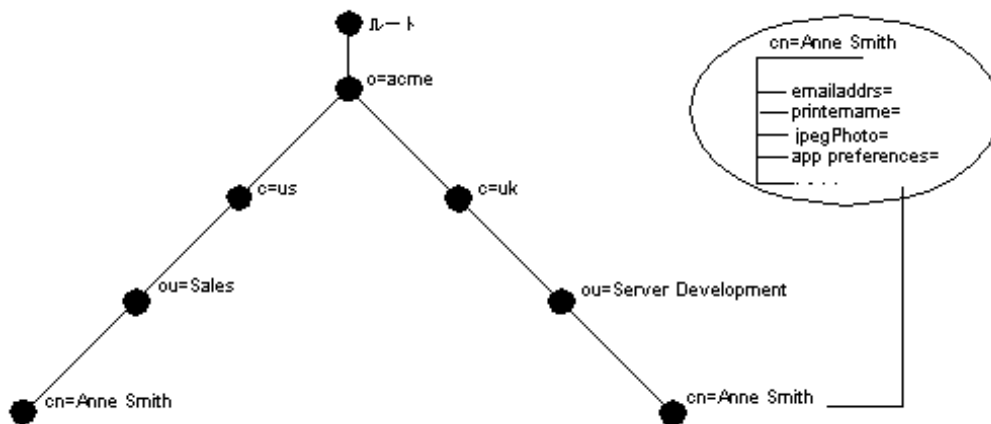
関連項目： [第 7 章「ディレクトリ・エントリの管理」](#)

属性

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

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

図 2-2 Anne Smith のエントリの属性



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

この項では、次の項目について説明します。

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

属性情報の種類

属性には 2 種類の情報があります。

- アプリケーション情報

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

- 操作情報

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

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

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

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

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

関連項目： システム操作属性の構成方法は、5-13 ページの「[システム操作属性の設定](#)」を参照してください。

単一値と複数值の属性

属性には、単一値または複数值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、複数值の属性には複数の値を設定できます。複数值の属性の例には、グループ全員の名前を載せたグループ・メンバーシップ・リストがあります。

一般的な LDAP 属性

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

表 2-1 一般的な LDAP 属性

属性の型	属性の文字列	説明
commonName	cn	エントリの一般的な名前 (Anne Smith など)。
domainComponent	dc	ドメイン・ネーム・システム (DNS) にあるコンポーネントの識別名 (dc=uk、dc=acme、dc=com など)。
jpegPhoto	jpegPhoto	JPEG フォーマットの写真イメージ。エントリの属性として組み込む JPEG イメージのパスとファイル名 (/photo/audrey.jpg など)。
organization	o	組織の名前 (my_company など)。
organizationalUnitName	ou	組織内の単位の名前 (Server Development など)。
owner	owner	エントリの所有者を識別する名前 (cn=Anne Smith, ou=Server Development, o= Acme, c=uk など)。
surname、sn	sn	ユーザーの姓 (Smith など)。
telephoneNumber	telephoneNumber	電話番号 ((650) 123-4567、6501234567 など)。

関連項目： Oracle Internet Directory が用意している専用の属性のリストは、付録 C「スキーマ要素」を参照してください。

属性の構文

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

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

関連項目： C-7 ページの「[LDAP 構文](#)」

属性の一致規則

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

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

関連項目： C-10 ページの「[一致規則](#)」

属性オプション

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

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

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

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

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

関連項目：

- 7-10 ページの「[Oracle Directory Manager を使用した属性オプション付きエントリの管理](#)」
- 7-14 ページの「[コマンドライン・ツールを使用した属性オプション付きエントリの管理](#)」

オブジェクト・クラス

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

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

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

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

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

この項では、次の項目について説明します。

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

サブクラス、スーパークラスおよび継承

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

サブクラスは、そのスーパークラスの属性をすべて**継承**します。たとえば、サブクラス `organizationalPerson` は、そのスーパークラス `person` の属性を継承しています。各エントリは、複数のオブジェクト・クラスによって定義された属性を継承できます。

注意： オブジェクト・クラス自体に値は含まれていません。値を持つのは、オブジェクト・クラスのインスタンス、つまりエントリのみです。サブクラスがスーパークラスから属性を継承するときはスーパークラスの属性フレームワークのみ継承し、属性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、オブジェクト・クラス階層の最上位レベルを指定する際にのみ使用されます。エントリに対する唯一のオブジェクト・クラスにはできません。たとえば、オブジェクト・クラス `top` は抽象型オブジェクト・クラスです。これは、構造型オブジェクト・クラスすべてに対するスーパークラスとして必要ですが、単独では使用できません。

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

- `orclGuid`: エントリが移動しても変わらないグローバル識別子
- `creatorsName`: オブジェクト・クラス作成者の名前
- `createTimestamp`: オブジェクト・クラスが作成された時間

- `modifiersName`: オブジェクト・クラスを最後に変更したユーザーの名前
- `modifyTimestamp`: オブジェクト・クラスが最後に変更された時間
- `orclACI`: この属性が定義されている [アクセス制御ポリシー・ポイント](#) の次のサブツリーにあるすべてのエントリに適用される [アクセス制御リストディレクティブ](#)
- `orclEntryLevelACI`: 特殊なユーザーなどの特定のエンティティのみに関連するアクセス制御ポリシー・ポイント

関連項目： アクセス制御ポリシー・ポイントおよび ACL の詳細は、2-13 ページの「[グローバルゼーション・サポート](#)」を参照してください。

構造型オブジェクト・クラス

これらのオブジェクト・クラスは、構造規則を使用して、指定したオブジェクト・クラスの下に作成可能なオブジェクト・クラスの種類の制限を与えます。たとえば、構造規則では `organization (o)` オブジェクト・クラスの下にあるすべてのオブジェクトは `organizational units (ou)` であることが要求されます。この規則に従うと、`person` オブジェクトを `organization` オブジェクト・クラスの下に直接入力できません。同様に、構造規則では、`person` オブジェクトの下に `organizational unit (ou)` オブジェクトを置くことはできません。

補助型オブジェクト・クラス

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

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

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

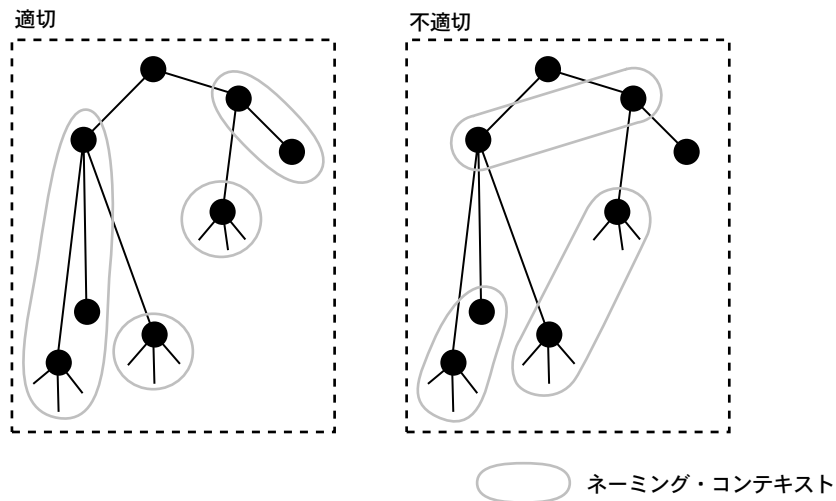
関連項目： [第 6 章「ディレクトリ・スキーマの管理」](#)

ネーミング・コンテキスト

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

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

図 2-3 有効なネーミング・コンテキストと無効なネーミング・コンテキスト



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

関連項目： ネーミング・コンテキストの公開方法は、5-17 ページの「[ネーミング・コンテキストの管理](#)」を参照してください。

ディレクトリ・スキーマ

ディレクトリ・[スキーマ](#)には、ディレクトリ情報ツリー内のデータを組織する方法に関するすべての情報（[オブジェクト・クラス](#)、[属性](#)、[一致規則](#)、構文などのメタデータ）が含まれています。ディレクトリ・スキーマはこの情報を、[サブエントリ](#)と呼ばれる特別なクラスのエントリに格納します。Oracle Internet Directory は、LDAP バージョン 3 の規格に従って、subSchemaSubentry と呼ばれるサブエントリにスキーマ定義を保持します。

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

関連項目：

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

セキュリティ

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

- データ整合性：送信中にデータが変更されないことを保証します。
- データ・プライバシー：送信中にデータが不適切に検出されないことを保証します。
- 認証：ユーザー、ホストおよびクライアントの識別情報が正しく検証されていることを保証します。
- 認可：ユーザーが権限を持つ情報のみを読み込みまたは更新することを保証します。
- パスワード・ポリシー：パスワードの定義方法と使用方法に関する規則を確立し、適用することを保証します。
- パスワード保護：パスワードのセキュリティを保証します。

さらに重要なことは、企業やホスティングされた環境では、これらの機能すべてを使用してアプリケーションのメタデータへのアクセスを制御できるという点です。このメタデータとは、アプリケーションの動作とアクセスできるユーザーを制御するための情報です。このためには、管理業務の委任を行うためのディレクトリを配置します。この配置によって、たとえばグローバル管理者は、部門にあるアプリケーションのメタデータに対するアクセスをその部門の管理者に委任できます。その結果、部門の管理者が自部門のアプリケーションへのアクセスを制御できるようになります。

関連項目： Oracle Internet Directory のセキュリティ機能の詳細は、[第 11 章「ディレクトリ・セキュリティの概要」](#)を参照してください。

グローバル化・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 グローバリゼーション・サポートがサポートするほとんどすべての言語の文字データを格納できます。また、Oracle Internet Directory の実装では異なる **Application Program Interface (API)** がいくつか含まれていますが、Oracle Internet Directory では、各 API に正しい文字エンコーディングが使用されることを保証しています。

グローバル化・サポートでは、シングルスバイト文字とマルチバイト文字の双方を使用します。シングルスバイト文字は、1 バイトのメモリで表されます。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、簡体字中国語はマルチバイト文字を使用します。簡体字中国語のディレクトリ・エントリは次のようになります。

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

属性値は、簡体字中国語キャラクタ・セットの文字列に相当します。

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

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

関連項目：

- Oracle Internet Directory の主なコンポーネントの詳細は、2-15 ページの「[Oracle Internet Directory のアーキテクチャ](#)」を参照してください。
- Oracle Internet Directory のグローバリゼーション・サポートの使用方は、[第 8 章「ディレクトリにおける グローバリゼーション・サポート」](#)を参照してください。
- グローバリゼーション・サポートの詳細は、『[Oracle9i グローバリゼーション・サポート・ガイド](#)』を参照してください。

注意： Oracle ディレクトリ・サーバーとデータベース・ツールの実行を UTF8 データベース上に限定していた、従来の制限はなくなりました。ただし、Oracle Internet Directory サーバーの基礎となるデータベースが UTF8 でない場合は、クライアントとデータベースで同じキャラクタ・セットを使用することをお勧めします。異なるキャラクタ・セットの場合は、クライアント・データをデータベースのキャラクタ・セットにマップできない場合に、LDAP の追加、変更または識別名の変更操作でデータが損失する可能性があります。

Oracle Internet Directory のアーキテクチャ

この項では、次の項目について説明します。

- [Oracle Internet Directory のノード](#)
- [Oracle ディレクトリ・サーバー・インスタンス](#)
- [構成設定エントリ](#)

Oracle Internet Directory のノード

2-16 ページの図 2-4 は、単一ノード上で稼働している様々なディレクトリ・サーバー・コンポーネントと、それらの関連を示しています。

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 Oracle Net Services が使用されます。

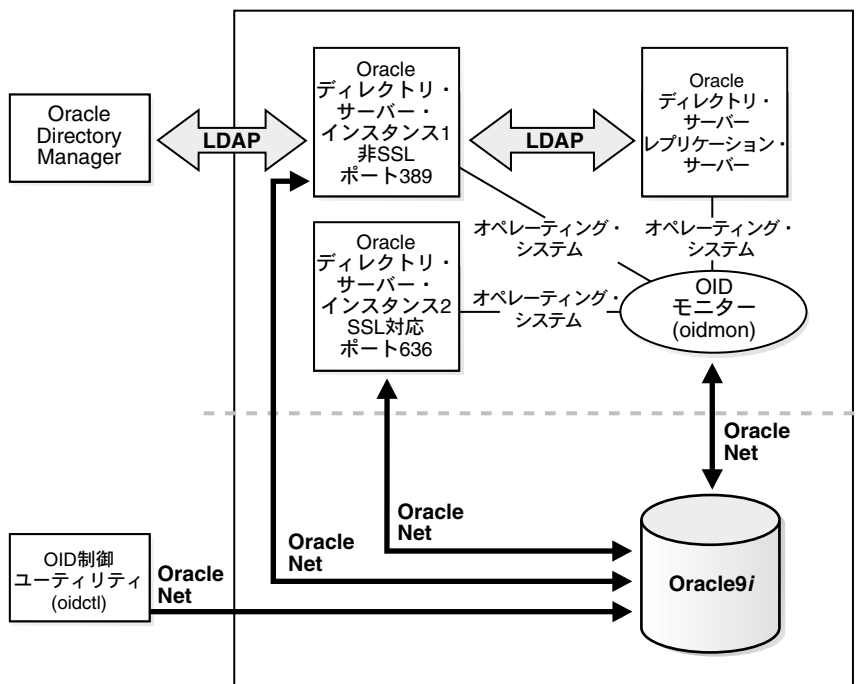
- [OID 制御ユーティリティ](#)
- Oracle ディレクトリ・サーバー・インスタンス 1 非 SSL ポート 389
- Oracle ディレクトリ・サーバー・インスタンス 2 SSL 対応ポート 636
- [OID モニター](#)

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

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

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

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



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

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

コンポーネント	説明
Oracle ディレクトリ・サーバー・インスタンス	<p>LDAP サーバー・インスタンスまたはディレクトリ・サーバー・インスタンスとも呼ばれます。ディレクトリ・サーバー・インスタンスは、特定の TCP/IP ポートでリスニングする単一の Oracle Internet Directory ディスパッチャ・プロセスを介して、ディレクトリの要求に応答します。それぞれが異なるポートでリスニングする複数のディレクトリ・サーバー・インスタンスをノードに持つことができます。</p> <p>1 つのインスタンスは、1 つのディスパッチャ・プロセスと 1 つ以上のサーバー・プロセスで構成されます。デフォルトでは、インスタンスごとに 1 つのサーバー・プロセスがありますが、これは増やすことができます。Oracle Internet Directory ディスパッチャとサーバー・プロセスは、複数のスレッドを使用して、負荷を分散できます。</p>
Oracle ディレクトリ・レプリケーション・サーバー	<p>レプリケーション・サーバーとも呼ばれます。他の Oracle Internet Directory システム内のレプリケーション・サーバーの変更を追跡し、その内容を送信します。1 つのノード上に設定できるレプリケーション・サーバーは 1 つのみです。レプリケーション・サーバーをインストールして使用するかどうかは選択できます。</p>
Oracle9i データベース	<p>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。</p>

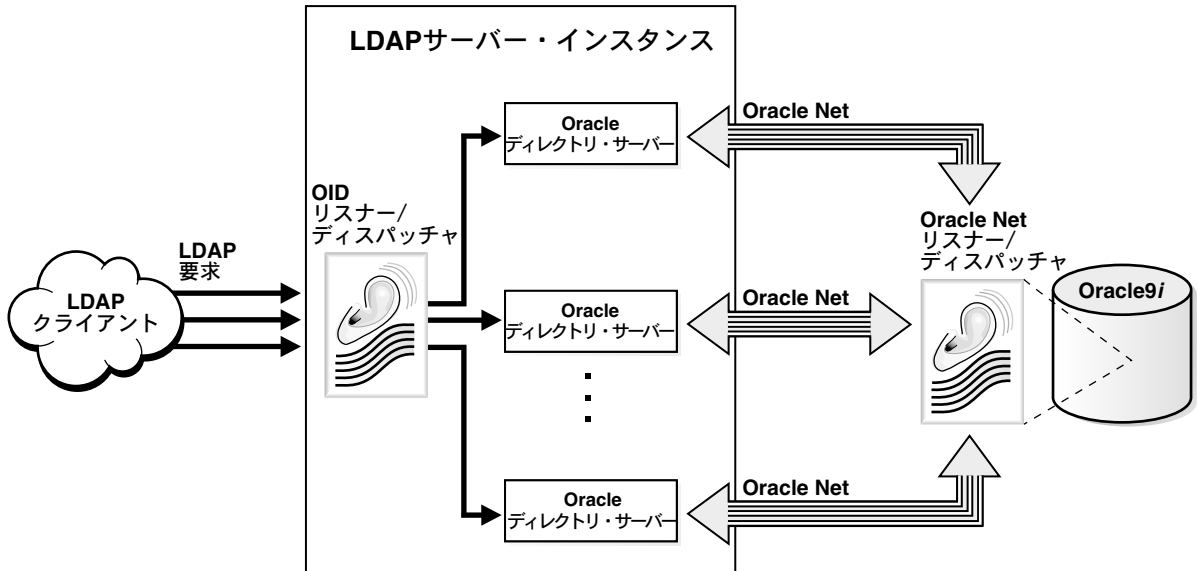
コンポーネント	説明
OID モニター (OIDMON)	<p>LDAP のサーバー・プロセスを開始、モニターおよび終了します。レプリケーション・サーバーをインストールすると、OID モニターがこれを制御します。OID 制御ユーティリティ (OIDCTL) を使用してディレクトリ・サーバー・インスタンスを起動または停止するコマンドを発行すると、そのコマンドはこのプロセスによって解釈されます。</p> <p>OID モニターは、管理者が OID 制御ユーティリティで行う LDAP サーバー・インスタンスの起動と停止の要求を処理します。また、OID モニターはサーバーを監視し、例外的な理由で実行が停止した場合に再起動させます。</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。ディレクトリ・サーバー・インスタンスが停止すると、レジストリ・エントリおよびその特定のサーバー・インスタンスに対応しているデータをプロセス表から削除します。OID モニターが異常終了したサーバーを再起動する場合は、そのサーバーの起動時間でレジストリ・エントリを更新します。</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 のサーバー・ファイル・システム上にあります。</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)	<p>Oracle Internet Directory のサーバー表にメッセージ・データを格納することによって、OID モニターと通信します。このメッセージ・データには、各 Oracle ディレクトリ・サーバー・インスタンスの実行に必要な構成パラメータが含まれています。</p>

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

Oracle ディレクトリ・サーバー・インスタンス

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

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



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

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

構成パラメータ ORCLMAXCC に設定した数値によって、各サーバー・プロセスとデータベースとの間に必要な数の接続が生成されます。このパラメータのデフォルト値は 10 です。サーバー・プロセスは、Oracle Net Services を介してデータ・サーバーと通信します。Oracle Net Services リスナー / ディスパッチャは、Oracle9i 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 ディレクトリ・サーバー・インスタンスの構成パラメータは、構成設定エントリ (configset) と呼ばれるディレクトリ・エントリに格納されます。構成設定エントリは、ディレクトリ・サーバーの特定インスタンスに関する構成パラメータを保持しています。管理者が OID 制御ユーティリティを使用してサーバーのインスタンスを起動すると、その起動コマンドにこの configset の 1 つへの参照が含まれ、その中の情報が使用されます。

Oracle ディレクトリ・サーバーは、デフォルトの構成設定エントリ (configset0) でインストールされているので、ディレクトリ・サーバーはすぐに実行できます。特定のパラメータを変更した新しい構成設定エントリを必要に応じて追加することによって、カスタマイズされた構成設定エントリを作成できます。このエントリを表示、追加および変更するには、[Oracle Directory Manager](#) または該当するコマンドライン・ツールを使用します。

関連項目：

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

例 : Oracle Internet Directory の動作

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

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

4. ディレクトリ・サーバーがユーザーを認証します。このプロセスはバインドと呼ばれます。ディレクトリ・サーバーは、アクセス制御リスト (ACL) もチェックして、そのユーザーが、要求した検索の実行を許可されているかどうかを検証します。
5. ディレクトリ・サーバーは、LDAP からの検索要求を Oracle Call Interface (OCI) および Oracle Net Services に変換し、Oracle9i データベースに送信します。
6. Oracle9i データベースは、情報を取得し、ディレクトリ・サーバー、次に C API、最後にクライアントと連鎖的に戻します。

分散ディレクトリ

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

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

この項では、次の項目について説明します。

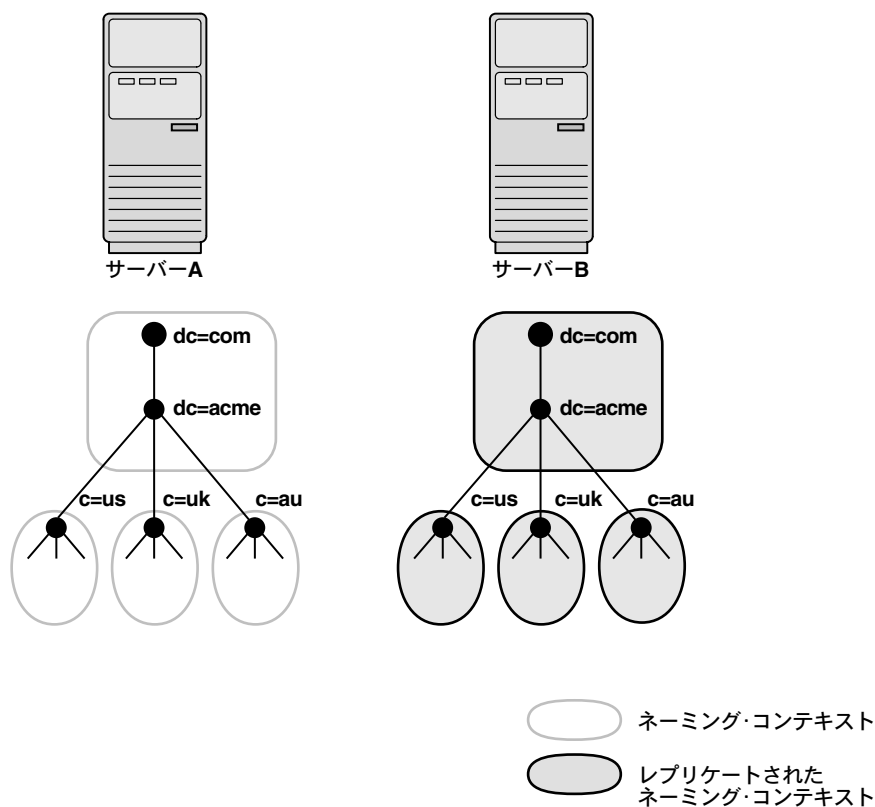
- [レプリケーション](#)
- [パーティション化](#)

レプリケーション

レプリケーションでは、同じネーミング・コンテキストが複数のサーバーに格納され、より多くのサーバーを使用して問合せを処理することによってパフォーマンスが向上します。また、ある箇所で発生した障害から派生するリスクを排除できるため信頼性が向上します。

図 2-6 は、レプリケート・ディレクトリを示しています。

図 2-6 レプリケート・ディレクトリ



サーバー内に格納されているネーミング・コンテキストの各コピーは、レプリカと呼ばれます。ディレクトリ・サーバーには、読取り専用レプリカと更新可能レプリカの両方を保持できます。更新可能レプリカを保持するサーバーは、サプライヤと呼ばれます。このレプリカを変更すると、コンシューマと呼ばれる他のサーバーに伝播されます。

レプリケーション・プロセスで変更が適用できないことがあります。たとえば、サプライヤのノード A がコンシューマに変更を送信し、その直後にサプライヤのノード B が同じエントリに更新を送信したとします。このとき、なんらかの問題が発生して、サプライヤのノード A からのエントリ送信が遅れたが、サプライヤのノード B からの更新送信にはそのような問題が発生しなかったとします。この結果、サプライヤのノード B からの更新が、エントリの変更よりも先にコンシューマに到着することになります。この場合、レプリケーション・サーバーは、指定された回数まで変更の適用を試みます。指定された回数に達しても変更が適用できなかった場合、レプリケーション・サーバーは変更内容を管理者操作キューに移動し、それ以降は指定した間隔よりも少ない頻度で定期的に適用を試みます。

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

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

関連項目： レプリケーションの詳細は、[第 22 章「ディレクトリ・レプリケーションの概要」](#)を参照してください。これには、Oracle9i レプリケーションのアーキテクチャ、変更ログの削除、競合の解決、レプリケーションのプロセスが含まれています。

パーティション化

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

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

図 2-7 パーティション化されたディレクトリ

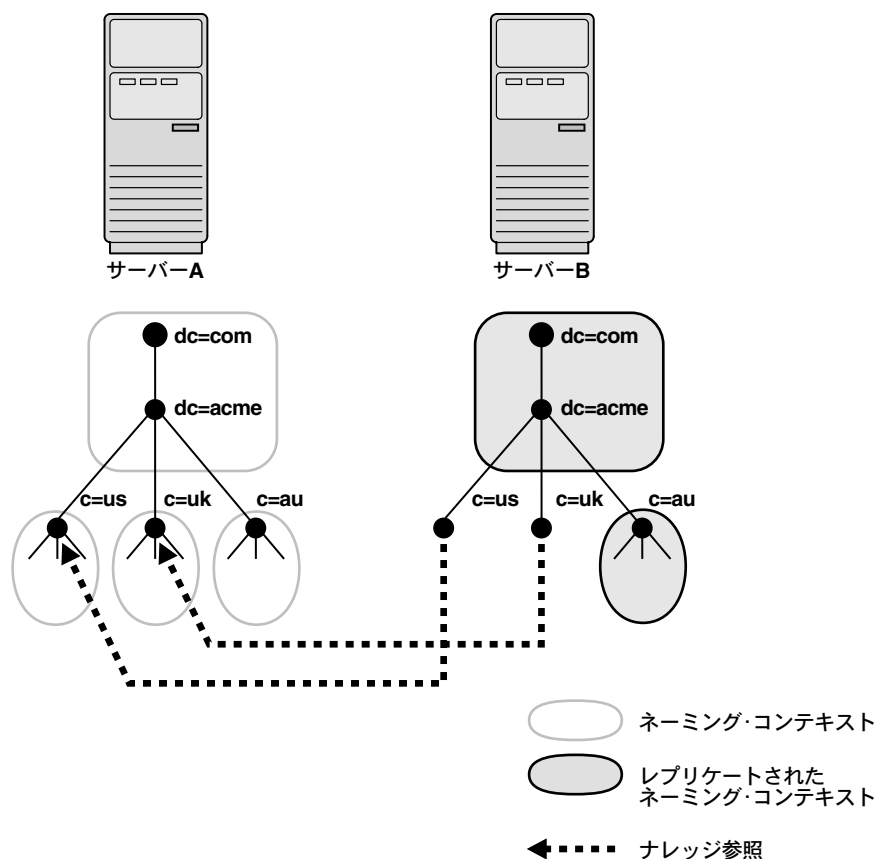


図 2-7 では、サーバー A に次の 4 つのネーミング・コンテキストが常駐しています。

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

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

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

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

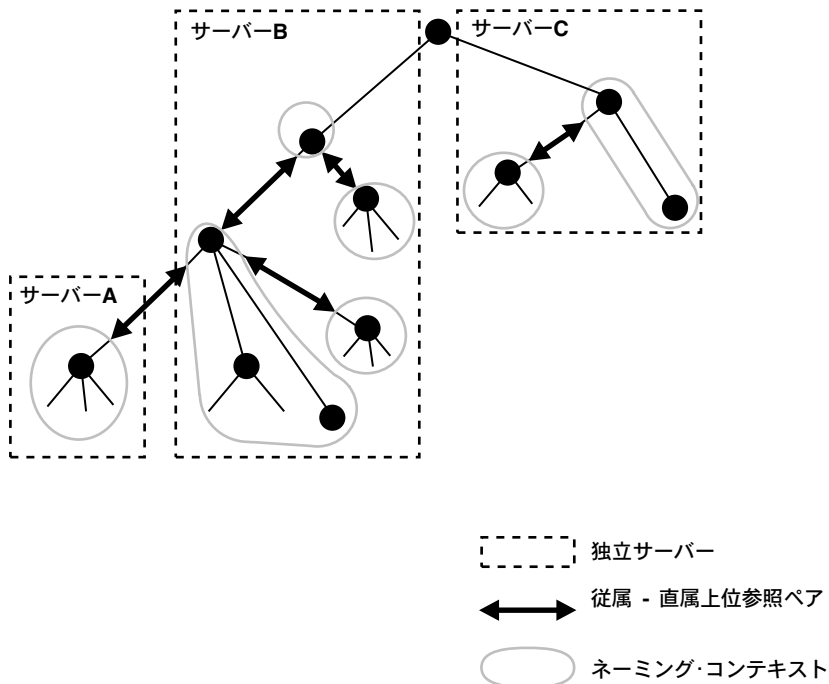
ナレッジ参照と参照

ナレッジ参照は、別のパーティションに保持されている様々なネーミング・コンテキストの名前とアドレスを提供します。図 2-7 のサーバー B は、ナレッジ参照を使用して、サーバー A の c=us と c=uk のネーミング・コンテキストを指し示します。クライアントがサーバー A に常駐している情報をサーバー B に要求すると、サーバー B は、サーバー A への 1 つ以上の参照をクライアントに提供します。その後、クライアントは、これらの参照を使用してサーバー A と通信できます。

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

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

図 2-8 ナレッジ参照を使用したネーミング・コンテキストへの指示



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

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

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

参照の種類

参照には次の2つの種類があります。

- スマート参照

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

たとえば、次のような場合があります。

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

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

- デフォルト参照

ベース・オブジェクトがディレクトリになく、さらに操作が別のサーバーのネーミング・コンテキストで実行されたときに戻されます。デフォルト参照は通常、ディレクトリ・パーティション化対策についてより多くのナレッジを持つサーバーにクライアントを送信します。

たとえば、サーバー A が次のものを保持するとします。

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

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

関連項目： 7-19 ページの「[ナレッジ参照と参照の管理](#)」

Delegated Administration Service

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

Delegated Administration Service はサーブレットと呼ばれる小型の Java プログラムに対応した Apache Web サーバーを利用しており、次の処理を実行します。

1. クライアントからの要求を受信します。
2. Oracle Internet Directory のデータを取得または更新することによって、クライアントの要求を処理し、その結果を生成します。
3. 回答をクライアントに返送します。

Oracle Directory Integration Platform

Oracle Directory Integration Platform を使用すると、多数のディレクトリを Oracle Internet Directory と同期させることができます。また、サード・パーティのメタディレクトリ・ベンダーと開発者は、独自の接続エージェントの開発と配置が容易になります。

この項では、次の項目について説明します。

- [メタディレクトリ](#)
- [Oracle Directory Integration Platform 環境](#)

メタディレクトリ

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

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

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

メタディレクトリ環境では、たとえば各従業員ごとにグローバル・ディレクトリ・エントリを作成できます。このエントリには、人事管理アプリケーション、メッセージ・システムま

たは NOS データベースなど、様々な同期化されたディレクトリからのデータを移入できます。ユーザーは、各 [接続先ディレクトリ](#) と同期化された最新のデータを含むものとして、このグローバル・エントリにアクセスできます。

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

Oracle Directory Integration Platform 環境

Oracle Directory Integration Platform によって、企業はアプリケーションやその他のディレクトリを Oracle Internet Directory に統合できます。このプラットフォームは、Oracle Internet Directory のデータとエンタープライズ・アプリケーションや接続先ディレクトリのデータとの一貫性を維持するために必要な、インタフェースとインフラストラクチャのすべてを提供します。

たとえば、企業では人事管理データベースの従業員レコードと Oracle Internet Directory との同期が必要な場合があります。また、変更が Oracle Internet Directory に適用されるたびに通知が必要な LDAP 対応のアプリケーション（Oracle*i*AS Portal など）が配置されている可能性もあります。このサービスはプロビジョニングと呼ばれ、Oracle Directory Integration Platform は、それらのアプリケーションに必要な通知を提供します。

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

- 同期化統合サービス—接続先ディレクトリと中央の Oracle Internet Directory との一貫性を維持します。
- プロビジョニング統合サービス—ユーザーのステータスまたは情報に対する変更を反映するために、定期的にターゲット・アプリケーションに通知を送信します。

関連項目： 第 VIII 部：「[Oracle Directory Integration Platform](#)」

事前に実行するタスクと情報

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

この項では、次の項目について説明します。

- [タスク 1: OID モニターの開始](#)
- [タスク 2: サーバー・インスタンスの起動](#)
- [タスク 3: デフォルト・セキュリティ構成の再設定](#)
- [タスク 4: データベースのデフォルト・パスワードの再設定](#)
- [タスク 5: OID データベース統計収集ツールの実行](#)
- [ログ・ファイルの位置](#)

タスク 1: OID モニターの開始

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

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

この項では、次の項目について説明します。

- [OID モニターの開始](#)
- [OID モニターの停止](#)

OID モニターの開始

OID モニターを開始する手順は、次のとおりです。

1. 次の環境変数を設定します。
 - `ORACLE_HOME`
 - `ORACLE_SID` または適切な TNS CONNECT 文字列
 - `NLS_LANG` (`APPROPRIATE_LANGUAGE.UTF8`)。インストール時のデフォルトの言語設定は、`AMERICAN_AMERICA` です。
2. コマンド・プロンプトで、次のコマンドを入力します。

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

引数	説明
<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=15 start
```

OID モニターの停止

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

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

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

次のようなコマンドを実行します。

```
oidmon connect=dbsl stop
```

タスク 2: サーバー・インスタンスの起動

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

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

この項では、次の項目について説明します。

- [Oracle ディレクトリ・サーバー・インスタンスの起動](#)
- [Oracle ディレクトリ・サーバー・インスタンスの停止](#)
- [Oracle ディレクトリ・レプリケーション・サーバー・インスタンスの起動](#)
- [Oracle ディレクトリ・レプリケーション・サーバー・インスタンスの停止](#)
- [ディレクトリ・サーバー・インスタンスの再起動](#)
- [ディレクトリ・サーバー・インスタンスの起動に関するトラブルシューティング](#)

Oracle ディレクトリ・サーバー・インスタンスの起動

Oracle ディレクトリ・サーバー・インスタンスを起動する構文は、次のとおりです。

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

引数	説明
connect=net_service_name	すでに tnsnames.ora ファイルを構成している場合は、\$ORACLE_HOME/network/admin にある、そのファイルに指定されているネット・サービス名です。
server=oidldapd	起動するサーバーの種類（有効な値は OIDLDAPD と OIDREPLD です）。大文字と小文字は区別されません。
instance=server_instance_number	起動するサーバーのインスタンス番号。1 ～ 1000 の間の数値を設定してください。
configset=configset_number	サーバーの起動に使用される configset の番号。未設定の場合は、デフォルトで configset0 に設定されます。0 ～ 1000 の間の数値を設定してください。
-p port_number	サーバー・インスタンス起動中のポート番号を指定します。デフォルトのポート番号は 389 です。
-work maximum_number_of_worker_threads_per_server	このサーバーのワーカー・スレッドの最大数を指定します。
-debug debug_level	Oracle ディレクトリ・サーバー・インスタンス起動中のデバッグ・レベルを指定します。
-l change_logging	レプリケーションの変更ログを記録するかどうかを設定します。設定をオフにする場合は、-l false を入力します。設定をオンにするには、次のいずれかを実行します。 <ul style="list-style-type: none">■ -l フラグを省略します。■ -l を入力します。■ -l true を入力します。 -l false で、指定したノードに対する変更ログの記録をオフにすると、2 つの問題が発生します。指定したノードから DRG のその他のノードへの更新のレプリケーションが阻止され、アプリケーション・プロビジョニングおよび接続先ディレクトリの同期が阻止されます。これは、この 2 つのサービスには、アクティブな変更ログが必要なためです。デフォルトは TRUE で、レプリケーション、プロビジョニングおよび同期を許可します。

引数	説明
<code>-server number_of_server_processes</code>	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。
<code>start</code>	<code>server</code> 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ディレクトリ・サーバー・インスタンスを起動するには、コマンド・プロンプトで次のように入力します。

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

Oracle ディレクトリ・サーバー・インスタンスの起動と停止では、コマンド `start` または `stop` 同様に、サーバー名とインスタンス番号が必須です。その他の引数はすべてオプションです。

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

フラグは引用符で囲む必要があります。

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

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

Oracle ディレクトリ・サーバー・インスタンスの停止

ディレクトリ・サーバー・インスタンスを起動または停止するときは、常に OID モニターが実行中であることが必要です。

コマンド・プロンプトで、次のコマンドを入力します。

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

次のようなコマンドを実行します。

```
oidctl connect=dba1 server=oidldapd instance=3 stop
```

Oracle ディレクトリ・レプリケーション・サーバー・インスタンスの起動

Oracle ディレクトリ・レプリケーション・サーバーを起動する構文は、次のとおりです。

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

引数	説明
connect=net_service_name	すでに tnsnames.ora ファイルを構成している場合は、\$ORACLE_HOME/network/admin にある、そのファイルに指定されている名前です。
server=oidrepld	起動するサーバーの種類（有効な値は oidldapd と oidrepld です）。大文字と小文字は区別されません。
instance=server_instance_number	起動するサーバーのインスタンス番号。1 ～ 1000 の間の数値を設定してください。
configset=configset_number	サーバーの起動に使用される configset の番号。デフォルトの設定は、configset0 です。0 ～ 1000 の間の数値を設定してください。
-p directory_server_port_number	TCP ポート directory_server_port_number 上のディレクトリへの接続でレプリケーション・サーバーが使用するポート番号。このオプションを指定しない場合は、デフォルト・ポート（389）に接続されます。
-d debug_level	レプリケーション・サーバー・インスタンス起動中のデバッグ・レベルを指定します。
-h directory_server_host_name	レプリケーション・サーバーを、デフォルトのホスト以外のホスト（つまり、ローカル・コンピュータ）に接続する場合、directory_server_host_name で指定します。directory_server_host_name には、コンピュータ名または IP アドレスを指定します。（レプリケーション・サーバーのみ）
-m [true false]	競合の解消を行うかどうかを設定します。TRUE および FALSE が有効な値です。デフォルトは TRUE です。（レプリケーション・サーバーのみ）
-z transaction_size	各レプリケーション更新サイクルで適用される変更の数を指定します。指定しない場合は、Oracle ディレクトリ・サーバーの sizelimit パラメータの値で決まります。sizelimit パラメータのデフォルト設定は 1024 です。この設定は変更できます。
start	server 引数で指定したサーバーを起動します。

たとえば、インスタンスが 1、ポート 12000、デバッグ・レベル 1024 でレプリケーション・サーバーを起動するには、コマンド・プロンプトで次のように入力します。

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

Oracle ディレクトリ・レプリケーション・サーバーの起動と停止では、`-h` フラグ（ホスト名を指定する引数）が必須です。その他のフラグはすべてオプションです。

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

フラグは引用符で囲む必要があります。

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

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

Oracle ディレクトリ・レプリケーション・サーバー・インスタンスの停止

ディレクトリ・サーバー・インスタンスを起動または停止するときは、常に OID モニターが実行中であることが必要です。

コマンド・プロンプトで、次のコマンドを入力します。

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

次のようなコマンドを実行します。

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

ディレクトリ・サーバー・インスタンスの再起動

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

ディレクトリ・サーバー・インスタンスを再起動するには、コマンド・プロンプトで次のコマンドを入力します。

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

ディレクトリ・サーバー・インスタンスを起動、停止または再起動するときは、常に OID モニターが実行中である必要があります。

ダウンしているサーバーに接続しようとする、SDK からエラー・メッセージ「81:LDAP サーバーと通信できません。」を受け取ります。

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

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

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

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

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

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

重要： 再起動を実行中、クライアントは Oracle ディレクトリ・サーバー・インスタンスにアクセスできません。ただし、再起動にかかる時間は数秒です。

ディレクトリ・サーバー・インスタンスの起動に関するトラブルシューティング

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

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

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

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

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

タスク 3: デフォルト・セキュリティ構成の再設定

Oracle Internet Directory は、この項で後述するデフォルトのセキュリティ構成でインストールされます。最初に、環境のニーズに対応してこのデフォルトの構成を変更し、各ユーザーが適切な認可を確実に受け取るようにする必要があります。

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

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

デフォルトのアクセス・ポリシー

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

ルート DSE でのデフォルトのアクセス・ポリシー

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

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

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

- サブスクリバ DAS ユーザー作成グループ
(`cn=oracledascreateuser,cn=groups,cn=oraclecontext,distinguished_name_of_subscriber`) には、オブジェクト・クラス `orcluser` のエントリを参照および追加する権限があります。
- サブスクリバ DAS ユーザー削除グループ
(`cn=oracledasdeleteuser,cn=groups,cn=oraclecontext,distinguished_name_of_subscriber`) には、オブジェクト・クラス `orcluser` のエントリを参照および削除する権限があります。
- サブスクリバ DAS ユーザー編集グループ
(`cn=oracledasedituser,cn=groups,cn=oraclecontext,distinguished_name_of_subscriber`) には、オブジェクト・クラス `orcluser` のエントリを参照する権限があります。
- サブスクリバ DAS ユーザー編集グループには、オブジェクト・クラス `orcluser` のエントリで、`userpassword` も含めたすべての属性に対する完全なアクセス権限があります。ユーザー（自身）には、各自の属性に対する完全なアクセス権限があります。他のユーザーにあるのは、これらの属性を参照する権限のみです。

- 認証サービス・グループ
(`cn=authenticationServices,cn=groups,cn=oraclecontext,distinguished_name_of_subscriber`) には、`userpassword` に対する比較権限がありますが、他のユーザーには一切権限がありません。
- ベリファイア・サービス・グループには、`authpassword` および `orclpasswordverifier` に対して読み込み、検索および比較を行う権限があります。ユーザー（自身）には、各自のベリファイア属性に対する完全なアクセス権限がありますが、他のユーザーにはありません。

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

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

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

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

Oracle コンテキスト管理者に対するデフォルトのアクセス・ポリシー

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

Oracle9i Application Server 管理者に対するデフォルトのアクセス・ポリシー

Oracle9i Application Server 管理者コンテナは、`cn=IASAdmins,cn=groups,cn=OracleContext,distinguished_name_of_subscriber` です。Oracle9i Application Server 管理者グループのメンバーには、指定された Oracle コンテキストの Oracle9i Application Server 製品ノード全体に対する完全な管理権限があります。さらに、次の権限が付与されます。

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

関連項目：

- Oracle Internet Directory のセキュリティ機能を含めた基本概念の概要は、[第 2 章「概念およびアーキテクチャ」](#)を参照してください。
- セキュリティを構成するために使用する管理ツールについては、[第 4 章「ディレクトリ管理ツール」](#)を参照してください。
- アクセス制御のオプションの説明およびセキュリティの設定方法は、[第 13 章「ディレクトリ・アクセス制御」](#)を参照してください。
- Oracle コンテキスト・スキーマの詳細は、[第 15 章「Oracle のコンポーネントと Oracle Internet Directory」](#)を参照してください。
- コマンドライン・ツールの構文と使用方法は、[付録 C「スキーマ要素」](#)を参照してください。

タスク 4: データベースのデフォルト・パスワードの再設定

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

関連項目： 構文と使用方法は、A-48 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。

タスク 5: OID データベース統計収集ツールの実行

bulkload ツール (bulkload.sh) 以外の手段でデータをディレクトリにロードする場合は、ロード後に OID データベース統計収集ツールを実行する必要があります。統計の収集は、Oracle オプティマイザが LDAP 操作に対応する問合せを実行する際に、最適な計画を選択するために不可欠です。OID データベース統計収集ツールは、OID デーモンを停止せずにいつでも実行できます。

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

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

関連項目：

- 4-16 ページの「OID データベース統計収集ツールの使用方法」
- A-55 ページの「OID データベース統計収集ツールの構文」

ログ・ファイルの位置

Oracle Internet Directory の各コンポーネントは、ログ情報とトレース情報を `ORACLE_HOME` 環境のログ・ファイルに出力します。表 3-1 に各コンポーネントと対応するログ・ファイルの位置をリストします。

表 3-1

コンポーネント	ログ・ファイル名
バルク・ローダー (bulkload.sh)	<code>\$ORACLE_HOME/ldap/log/install.log</code>
カタログ管理ツール (catalog.sh)	<code>\$ORACLE_HOME/ldap/log/catalog.log</code>
ディレクトリ統合エージェント	<code>\$ORACLE_HOME/ldap/odi/log/AgentName.err</code> (<code>AgentName</code> にはエージェント名が入ります)
Directory Integration Server (odisrv)	<code>\$ORACLE_HOME/ldap/log/odisrvXX.log</code> (XX には Oracle Directory Integration Server インスタンス番号が入ります)

表 3-1 (続き)

コンポーネント	ログ・ファイル名
ディレクトリ・レプリケーション・サーバー (oidrepld)	\$ORACLE_HOME/ldap/log/oidrepld00.log
ディレクトリ・サーバー (oidldapd)	\$ORACLE_HOME/ldap/log/oidldapdXXspid.log (<i>pid</i> にはサーバー・プロセス識別子が入ります)
LDAP ディスパッチャ (oidldapd)	\$ORACLE_HOME/ldap/log/oidldapdXX.log (<i>XX</i> にはサーバー・インスタンス番号が入ります)
OID モニター (oidmon)	\$ORACLE_HOME/ldap/log/oidmon.log
レプリケーション設定 (ldaprepl.sh)	\$ORACLE_HOME/ldap/admin/LOGS/ldaprepl.log

ディレクトリ管理ツール

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

この章では、次の項目について説明します。

- [Oracle Directory Manager の使用方法](#)
- [コマンドライン・ツールの使用方法](#)
- [OID データベース・パスワード・ユーティリティの使用法](#)
- [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](#)

ディレクトリ管理では Delegated Administration Service による支援を受け、次の内容を実行することもできます。

- 非技術系マネージャなどの委任管理者が、ユーザーとグループの両方を作成および管理できます。
- エンド・ユーザーは、管理者の介入なしに自分のパスワードを変更できます。

関連項目： [第9章「Delegated Administration Service」](#)

Oracle Directory Manager の使用方法

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

この項では、次の項目について説明します。

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

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

Oracle Directory Manager の起動

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

関連項目：

- サーバー・インスタンスの起動方法は、[第 3 章「事前に実行するタスクと情報」](#)を参照してください。
- ディレクトリ・サーバー・インスタンスの概念の説明は、2-15 ページの「[Oracle Internet Directory のアーキテクチャ](#)」を参照してください。

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

オペレーティング・システム**参照箇所**

Windows NT	「スタート」メニューから、「プログラム」>「ORACLE_HOME」>「Oracle Internet Directory」>「Oracle Internet Directory」をクリックします。
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。「ディレクトリ・サーバーの接続」ダイアログ・ボックスが表示されます。

ディレクトリ・サーバーへの接続

ディレクトリ・サーバーへ接続する手順は、次のとおりです。

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

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

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

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

フィールド	説明
ユーザー	<p>初めてログインするときは、スーパー・ユーザーまたは匿名でログインします。このセッション中に SSL の機能を構成する場合は、スーパー・ユーザーでログインします。</p> <p>スーパー・ユーザーでログインする場合は、「ユーザー」ボックスに <code>cn=orcladmin</code> と入力します。</p> <p>匿名でログインする場合は、「ユーザー」ボックスを空白のままにします。</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">■ 「ユーザー」フィールドの右側のボタンを使用し、そのエントリをブラウズして選択します。■ そのユーザーのエントリに対する識別名を、次の例のように正しい書式で入力します。 <code>cn=Susie Brown,ou=HR,o=acme,c=us</code>
パスワード	<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「パスワード」ボックスに入力します。パスワードを指定していない場合は、デフォルトのパスワード <code>welcome</code> を入力します。Oracle Directory Manager にログインし、ディレクトリ・サーバーに接続した後、ディレクトリを保護するためにこのパスワードを変更してください。</p> <p>匿名でログインする場合は、「パスワード」ボックスを空白のままにします。</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>関連項目：パスワードの変更方法は、5-18 ページの「スーパー・ユーザー、ゲスト・ユーザーおよびプロキシ・ユーザーの管理」を参照してください。</p>

フィールド	説明
サーバー	<p>「サーバー・リスト」から、接続するディレクトリ・サーバーのあるホストを選択します。</p> <p>ディレクトリ・サーバーにすでに接続している場合に、別のホストのディレクトリ・サーバーに接続する手順は、次のとおりです。</p> <ol style="list-style-type: none">1. 「サーバー」フィールドの右側のボタンをクリックします。使用可能なサーバーのリストが、「ディレクトリ・サーバーの選択」ダイアログ・ボックスに表示されます。2. サーバーを選択します。3. 「OK」をクリックします。 <p>ディレクトリ・サーバーをリストに追加する手順は、次のとおりです。</p> <ol style="list-style-type: none">1. 「ディレクトリ・サーバーの選択」ダイアログ・ボックスで「追加」をクリックします。「ディレクトリ・サーバーの接続」ダイアログ・ボックスが表示されます。2. 「サーバー」フィールドに、追加するディレクトリ・サーバーの名前を入力します。3. 「ポート」フィールドに、追加するサーバーのポート番号を入力します。4. 「OK」をクリックします。追加したディレクトリが、「ディレクトリ・サーバーの選択」ダイアログ・ボックスのリストに表示されます。 <p>リストにあるディレクトリ・サーバーを変更する手順は、次のとおりです。</p> <ol style="list-style-type: none">1. 変更するディレクトリ・サーバーを選択します。2. 「編集」をクリックします。「ディレクトリ・サーバーの接続」ダイアログ・ボックスが表示されます。3. 「サーバー」フィールドおよび「ポート」フィールドを変更して、「OK」をクリックします。サーバーに対する変更が、「ディレクトリ・サーバーの選択」ダイアログ・ボックスのリストに表示されます。
ポート	<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ディレクトリ・サーバー・インスタンスが存在している場合、各ディレクトリ・サーバー・インスタンスごとにポートが異なり、ディレクトリ・サーバー・インスタンスを選択すると、そのポート番号がこのフィールドに表示されます。</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">1. 「サーバー」フィールドの右側のボタンをクリックします。2. 「ディレクトリ・サーバーの選択」ダイアログ・ボックスで、ディレクトリ・サーバーを選択します。3. 「編集」をクリックします。「ディレクトリ・サーバーの接続」ダイアログ・ボックスが表示されます。4. 「ディレクトリ・サーバーの接続」ダイアログ・ボックスの「ポート」フィールドにポート番号を入力して、「OK」をクリックします。

フィールド	説明
SSL 使用可能	<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>ディレクトリ・サーバーには、SSL の使用または SSL なしのいずれでも接続できます。SSL を使用して接続すると、Oracle Directory Manager は SSL クライアントになります。</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">■ 接続先のサーバーが SSL を使用していること。接続先のサーバーが SSL を使用していない場合にこのチェックボックスを選択すると、認証に失敗します。■ 証明書と信頼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。

関連項目：

- SSL を使用可能にする方法は、[第 12 章「Secure Sockets Layer \(SSL\) とディレクトリ」](#)を参照してください。
 - Wallet の作成方法は、[付録 D「Oracle Wallet Manager」](#)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、12-3 ページの「[SSL パラメータの構成](#)」を参照してください。
3. 「資格証明」タブの「SSL 使用可能」チェックボックスを選択した場合は、次に「SSL」タブを選択してください。
4. 次の表の説明に従って、各フィールドに必要なデータを入力します。

フィールド	説明
SSL 位置	<p>クライアントとサーバーの認証に使用するクライアントの Wallet を指定します。クライアントの Wallet がローカル・マシン上にある場合は、その Wallet のパスとファイル名を次の構文で入力します。</p> <p><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 パスワード	ユーザーの Wallet をオープンするパスワード。

フィールド	説明
SSL 認証	<p>認証レベルを次の中から選択します。</p> <ul style="list-style-type: none"> ■ SSL 認証なし: クライアントとサーバーのいずれも、相手に対して自己認証を行いません。証明書の送信または交換は行われません。「資格証明」タブの「SSL 使用可能」チェックボックスを選択して、このオプションを選択した場合は、SSL 暗号化 / 復号化のみが使用されます。 ■ SSL クライアントとサーバーの認証: クライアントとサーバーの認証。クライアントとサーバーは、証明書を交換します。 ■ SSL サーバー認証: サーバー認証。ディレクトリ・サーバーがクライアントに証明書を送信することによって、ディレクトリ・サーバーからクライアントに対してサーバー認証を行います。

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

Oracle Directory Manager のナビゲート

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

Oracle Directory Manager の概要

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

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

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

Oracle Directory Manager のメニュー・バー

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

メニュー	メニュー項目
ファイル	作成 : オブジェクトを追加します。 類似項目の作成 : ナビゲータ・ペインで選択したオブジェクトをテンプレートとして使用し、新規オブジェクトを追加します。 接続 : ナビゲータ・ペインで選択したディレクトリ・サーバーに接続します。 切断 : ナビゲータ・ペインで選択したディレクトリ・サーバーから切断します。 終了 : Oracle Directory Manager を終了します。
編集	編集 : オブジェクトを変更します。 取消 : 選択したオブジェクトを削除します。 オブジェクト・クラスの検索 : オブジェクト・クラスを検索します。
ビュー	リフレッシュ : データベース上での変更内容を画面表示に反映するために、メモリーに格納されているデータを更新します。 切離し : Oracle Directory Manager の右側のペインに表示されているフィールドと値を含むセカンダリ・ダイアログを生成します。2 つの情報を比較する場合に便利です。

メニュー	メニュー項目
操作	<p>オブジェクト・クラスの作成: 新規オブジェクト・クラスの追加に使用する「新規オブジェクト・クラス」ウィンドウを表示します。</p> <p>属性の作成: エントリへの新規属性の追加に使用する「新規属性の型」ダイアログ・ボックスを表示します。</p> <p>アクセス制御ポイントの作成: 新規アクセス制御ポリシー・ポイントの追加に使用する「新規アクセス制御ポイント」ダイアログ・ボックスを表示します。</p> <p>エントリの作成: 新規ディレクトリ・エントリの追加に使用する「新規エントリ」ダイアログ・ボックスを表示します。</p> <p>エントリのリフレッシュ: メモリーに格納されているエントリのデータを更新し、データベースに変更内容を反映します。</p> <p>サブツリー・エントリのリフレッシュ: メモリーに格納されているエントリの子を更新し、データベースに変更内容を反映します。</p> <p>索引の削除: 属性から索引を削除します。この項目を選択すると、削除の確認を要求する警告が表示されます。</p> <p>検索: ACP 検索の構成を可能にします。</p> <p>ユーザー設定項目: 次の操作のためのダイアログ・ボックスを表示します。</p> <ul style="list-style-type: none">■ エントリ検索結果の表示の構成■ ACP の表示を Oracle Directory Manager の実行のたびに行うか、検索の結果としてのみ行うかの設定
ヘルプ	<p>目次: ヘルプ・ナビゲータの「目次」タブ・ページを表示します。</p> <p>トピックの検索: オンライン・ヘルプ・ガイドのワード検索に使用する「ヘルプ・ナビゲータ」ダイアログ・ボックスを表示します。</p> <p>バージョン情報: 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 に Oracle Internet Directory のツールバーを示します。このツールバーについて左から順番に表 4-1 で説明します。各ボタンは、Oracle Directory Manager に表示しているペインやタブ・ページによって、使用できる場合と使用できない場合があります。

図 4-1 Oracle Directory Manager のツールバー

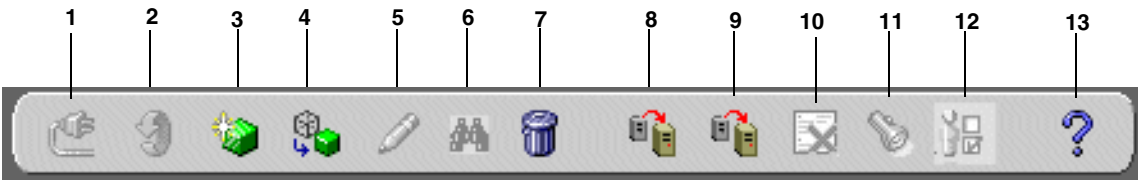


表 4-1 Oracle Directory Manager のツールバー

ボタン	用途
1	「接続」: ナビゲータ・ペインで選択したディレクトリ・サーバーに接続します。または選択したディレクトリ・サーバーから切断します。
2	リフレッシュ: メモリーに格納されているエントリ以外のオブジェクトのデータを更新し、データベースに変更内容を反映します。
3	作成: 新規オブジェクトを追加します。
4	類似項目の作成: 別のオブジェクトをテンプレートとして使用して、新規オブジェクトを追加します。
5	編集: オブジェクトを変更します。
6	オブジェクトの検索: コンテキストに応じて、オブジェクト・クラスまたは属性を検索します。ナビゲータ・ペインで「Oracle Internet Directory サーバー」>「 <i>directory server instance</i> 」>「サーバーの管理」>「オブジェクト・クラス」の順にナビゲートすると、このボタンでオブジェクト・クラスを検索できます。「Oracle Internet Directory サーバー」>「 <i>directory server instance</i> 」>「サーバーの管理」>「属性」の順にナビゲートすると、このボタンで属性を検索できます。
7	削除: オブジェクトを削除します。
8	エントリのリフレッシュ: メモリーに格納されているエントリのデータを更新し、データベースに変更内容を反映します。
9	サブツリー・エントリのリフレッシュ: メモリーに格納されているエントリの子を更新し、データベースに変更内容を反映します。
10	索引の削除: 属性から索引を削除します。このボタンをクリックすると、削除の確認を要求する警告が表示されます。

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

ボタン	用途
11	検索 : ACP 検索の構成を可能にします。
12	ユーザー設定項目 : 検索操作のエントリと同様に、ナビゲータ・ペインの ACP の表示を構成できるようにします。
13	ヘルプ : ヘルプ・システムを表示します。

追加のディレクトリ・サーバーへの接続

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

追加のディレクトリ・サーバーに接続する手順は、次のとおりです。

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

ディレクトリ・サーバーからの切断

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

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

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

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

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

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

タスクの領域	参照箇所
スキーマの管理	6-6 ページの「 Oracle Directory Manager を使用したオブジェクト・クラスの管理 」 6-16 ページの「 Oracle Directory Manager を使用した属性の管理 」
エントリの管理	7-2 ページの「 Oracle Directory Manager を使用したエントリの管理 」
アクセス制御ポリシー・ポイント（ACP）の管理	13-12 ページの「 Oracle Directory Manager を使用したアクセス制御の管理 」 13-40 ページの「 コマンドライン・ツールを使用したアクセス制御の管理 」
パーティション化とレプリケーション	第 23 章「 Oracle ディレクトリ・レプリケーション・サーバーの管理 」

コマンドライン・ツールの使用方法

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

- LDAP ツールー LDAP データ交換フォーマット（LDIF）で記述されたテキスト・ファイル内のオブジェクトを変更します。
- バルク・ツールー他のアプリケーションのデータを使用して大量のディレクトリ・エントリを作成または管理します。
- カタログ管理ツールー既存の属性を索引付きの属性にします。

大部分のコマンドライン・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。

これら 3 種類のコマンドライン・ツールは、後続の各項と付録の中で説明されています。

LDAP エントリに直接影響を与えるツール

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
ldapadd	エントリを一度に 1 つずつ追加します。	A-4 ページの「 ldapadd の構文 」
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 ページの「 ldapaddmt の構文 」
ldapbind	ディレクトリ・サーバーに対して、ユーザーまたはクライアントを認証します。	A-8 ページの「 ldapbind の構文 」
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-10 ページの「 ldapcompare の構文 」
ldapdelete	エントリを削除します。	A-11 ページの「 ldapdelete の構文 」
ldapmoddn	エントリの識別名または相対識別名の変更、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-13 ページの「 ldapmoddn の構文 」
ldapmodify	エントリの属性データを作成、更新および削除します。	A-15 ページの「 ldapmodify の構文 」
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-20 ページの「 ldapmodifymt の構文 」
ldapsearch	ディレクトリ・エントリを検索します。	A-22 ページの「 ldapsearch の構文 」

関連項目： コマンドライン・ツールとグローバリゼーション・サポートの説明は、8-6 ページの「[コマンドライン・ツールでのグローバリゼーション・サポートの使用方法](#)」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：

- 4-15 ページの「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-48 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」

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-34 ページの「bulkload の構文」
ldifwrite	ディレクトリ情報ベースのデータを、LDAP 準拠のディレクトリ・サーバーで読み込み可能な 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-38 ページの「ldifwrite の構文」
bulkmodify	大量の既存エントリを効率的に変更します。	A-15 ページの「ldapmodify の構文」
bulkdelete	サブツリーを効率的に削除します。	A-33 ページの「bulkdelete の構文」

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、エントリ cn=catalogs に、検索で使用する属性がリストされます。等価の一致規則を持つ属性のみが索引付けできます。

その他の属性を検索フィルタで使用する場合は、使用する属性をカタログ・エントリに追加する必要があります。この操作は、Oracle Directory Manager を使用して属性を作成するときに実行できます。ただし、すでに存在している属性への索引付けに使用できるのは、カタログ管理ツールのみです。

関連項目：

- 構文と使用方法は、A-39 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。
- 6-29 ページの「コマンドライン・ツールを使用した属性の索引付け」
- 6-26 ページの「Oracle Directory Manager を使用した属性の索引付け」

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-42 ページの「[OID 制御ユーティリティの構文](#)」
- 概念の説明は、2-15 ページの「[Oracle Internet Directory のアーキテクチャ](#)」を参照してください。

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： 構文と使用方法是、A-48 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 ディレクトリ・レプリケーション・サーバーは変更をリトライ・キューに入れ、指定した回数に応じてそれらの適用を試みます。指定した回数を超えて失敗が続いた場合、レプリケーション・サーバーは変更を管理者操作キューに入れます。そこから、レプリケーション・サーバーはより短い間隔で変更アプリケーション・プロセスを繰り返しながら管理者によるアクションを待ちます。

このとき、必要な手順は次のとおりです。

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

この処理では次の 2 つのツールが役に立ちます。競合している変更を同期させるには OID 調停ツールを使用します。また、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・キューへ移動するには、管理者操作キュー操作ツールを使用します。

関連項目：

- 23-32 ページの「[OID 調停ツールの使用](#)」
- OID 調停ツールの構文と動作の説明は、A-52 ページの「[OID 調停ツールの構文](#)」を参照してください。
- 23-32 ページの「[管理者操作キュー操作ツールの使用](#)」
- A-49 ページの「[管理者操作キュー操作ツールの構文](#)」

OID データベース統計収集ツールの使用方法

OID データベース統計収集ツール (oidstats.sh) は、\$ORACLE_HOME/ldap/admin に格納されています。ディレクトリへのデータの初期ロードも含め、ディレクトリのデータに重要な変更がある場合は常に、このユーティリティを実行する必要があります。

バルク・ロード・ツール (bulkload.sh) 以外の手段でデータをディレクトリにロードする場合は、ロード後に OID データベース統計収集ツールを実行する必要があります。統計の収集は、Oracle オプティマイザが LDAP 操作に対応する問合せを実行する際に、最適な計画を選択するために不可欠です。OID データベース統計収集ツールは、OID デーモンを停止せずにいつでも実行できます。

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

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

関連項目： A-55 ページの「[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。次の表に、一般的なタスクの一部について必要な情報を示します。

タスク	参照箇所
属性の管理	
コマンドライン・ツールを使用した属性の追加、変更または削除	6-27 ページの「 コマンドライン・ツールを使用した属性の管理 」
Oracle Directory Manager を使用した属性の追加、変更または削除	6-16 ページの「 Oracle Directory Manager を使用した属性の管理 」
エントリの管理	
コマンドライン・ツールを使用したディレクトリ・エントリの追加、変更または削除	7-12 ページの「 コマンドライン・ツールを使用したエントリの管理 」
Oracle Directory Manager を使用したディレクトリ・エントリの追加、変更または削除	7-2 ページの「 Oracle Directory Manager を使用したエントリの管理 」
大量のデータ・ファイルのインポート	A-34 ページの「 bulkload の構文 」 A-2 ページの「 LDAP データ交換フォーマット (LDIF) の構文 」
エントリのディレクトリ情報ツリー階層の表示	7-2 ページの「 Oracle Directory Manager を使用したエントリの管理 」
オブジェクト・クラスの管理	
コマンドライン・ツールを使用したオブジェクト・クラスの追加、変更または削除	6-13 ページの「 コマンドライン・ツールを使用したオブジェクト・クラスの管理 」
Oracle Directory Manager を使用したオブジェクト・クラスの追加、変更または削除	6-6 ページの「 Oracle Directory Manager を使用したオブジェクト・クラスの管理 」
レプリケーションの管理	
レプリケーションの設定	第 23 章「 Oracle ディレクトリ・レプリケーション・サーバーの管理 」
レプリケーション変更の競合の解消	23-30 ページの「 手動での競合の解消 」
レプリケーション変更の管理者操作キューからリトライ・キューかページ・キューへの移動	23-32 ページの「 管理者操作キュー操作ツールの使用 」
セキュリティの管理	
アクセス制御ポリシー・ポイント (ACP) の設定	第 13 章「 ディレクトリ・アクセス制御 」
SSL の設定	第 12 章「 Secure Sockets Layer (SSL) とディレクトリ 」

タスク	参照箇所
サーバーの管理	
コマンドライン・ツールを使用したサーバー・インスタンス・パラメータの構成	5-11 ページの「 コマンドライン・ツールを使用したサーバー構成設定エントリの管理 」
Oracle Directory Manager を使用したサーバー・インスタンス・パラメータの構成	5-4 ページの「 Oracle Directory Manager を使用したサーバーの構成設定エントリの管理 」
Oracle Directory Manager を使用したディレクトリへの接続	4-3 ページの「 ディレクトリ・サーバーへの接続 」 4-11 ページの「 追加のディレクトリ・サーバーへの接続 」
ディレクトリ・サーバー・プロセスの起動	第 3 章「事前に実行するタスクと情報」
ディレクトリ・サーバー・プロセスの停止	第 3 章「事前に実行するタスクと情報」
システム操作属性の表示	5-13 ページの「 Oracle Directory Manager を使用したシステム操作属性の設定 」 5-16 ページの「 ldapmodify を使用したシステム操作属性の設定 」

第 II 部

基本的なディレクトリ管理

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

- 第 5 章「Oracle ディレクトリ・サーバーの管理」
- 第 6 章「ディレクトリ・スキーマの管理」
- 第 7 章「ディレクトリ・エントリの管理」
- 第 8 章「ディレクトリにおける グローバリゼーション・サポート」
- 第 9 章「Delegated Administration Service」
- 第 10 章「属性一意性」

Oracle ディレクトリ・サーバーの管理

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

この章では、次の項目について説明します。

- [サーバーの構成設定エントリの管理](#)
- [システム操作属性の設定](#)
- [ネーミング・コンテキストの管理](#)
- [スーパー・ユーザー、ゲスト・ユーザーおよびプロキシ・ユーザーの管理](#)
- [検索の構成](#)
- [ディレクトリ・サーバーの監視、デバッグおよび監査](#)
- [アクティブ・サーバー・インスタンスの情報の表示](#)
- [Oracle データベース・サーバー接続時のパスワードの変更](#)
- [別名エントリの間接参照](#)

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

サーバーの構成設定エントリの管理

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

関連項目：

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

この項では、次の項目について説明します。

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

構成設定エントリ管理のための事前の考慮事項

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

実行しているサーバーのインスタンスすべてに対しては有効ではない値を変更するときは、構成設定エントリを新規に作成することをお勧めします。この方法は、Oracle ディレクトリ・サーバー・インスタンスにのみ適用されます。Oracle ディレクトリ・レプリケーション・サーバーがサポートする構成設定は 1 つのみです。

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

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

図 5-1 複数の構成設定エントリを示すディレクトリ・エントリ階層

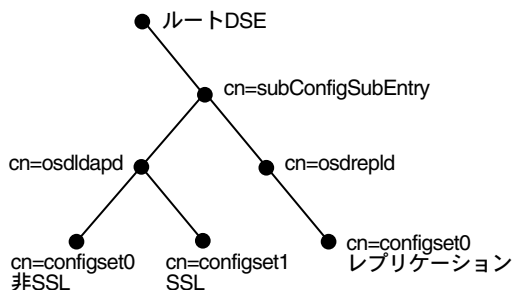


図 5-1 は、次のものを表しています。

- 次のインスタンスを含む Oracle ディレクトリ・サーバー (cn=osldlapd)
 - デフォルト・ポートでリスニングし、SSL がオフ状態の configset0 を使用している 1 つのインスタンス
 - SSL ポートでリスニングし、SSL がオン状態の configset1 を使用している 2 番目のインスタンス
- configset0 を使用しているレプリケーション・サーバー・インスタンス (cn=osdrepld)

関連項目：

- SSL の構成パラメータの詳細は、[第 12 章「Secure Sockets Layer \(SSL\) とディレクトリ」](#)を参照してください。
- レプリケーションの構成パラメータの詳細は、[第 23 章「Oracle ディレクトリ・レプリケーション・サーバーの管理」](#)を参照してください。
- ディレクトリ・サーバー・インスタンスの構成に使用する、属性の全セットのリストとその説明は、C-5 ページの「[構成設定エントリの属性](#)」を参照してください。

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

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

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

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

ディレクトリ・サーバー・インスタンスを再起動する方法は、3-9 ページの「[タスク 3: デフォルト・セキュリティ構成の再設定](#)」を参照してください。

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

構成設定エントリを表示する手順は、次のとおりです。

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

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

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

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

初めて構成設定エントリを追加するときには、次の操作が可能です。

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

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

1. ナビゲータ・ペインで、「Oracle Internet Directory サーバー」 > 「*directory server instance*」 > 「サーバーの管理」 > 「ディレクトリ・サーバー」の順に展開し、「デフォルト構成設定」を選択します。
2. ツールバーの「類似項目の作成」ボタンをクリックします。「構成設定」ダイアログ・ボックスに「一般」タブが表示されます。
3. 次の表の説明に従って、各フィールドに情報を入力します。

フィールド	説明
DB の最大接続数	1 つのディレクトリ・サーバー・プロセスで処理可能なデータベースの同時接続数を入力します。デフォルトは 10 です。
子プロセスの数	単一のインスタンスが起動できるサーバー・プロセスの数を入力します。デフォルトは 1 です。
設定	構成設定エントリの番号を入力します。デフォルトの構成設定は 0（ゼロ）です。異なる構成設定を必要な数だけ設定できます。複数のインスタンスで同じパラメータを必要とする場合は、同一の構成設定を使用できます。設定番号は変更可能です。

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

フィールド	説明
SSL 使用可能	非保護操作のみの場合は 0（ゼロ）を設定します。デフォルト・ポートは 839 で、この値未満で変更可能です。 SSL 認証のみの場合は 1 を設定します。デフォルト・ポートは 636 で、この値未満で変更可能です。 非保護操作と SSL 認証の両方の場合は 2 を設定します。

フィールド	説明
SSL 認証	次の中から 1 つ選択します。 <ul style="list-style-type: none">■ SSL 認証なし: クライアントとサーバーのいずれも、相手に対して自己認証を行いません。証明書の送信または交換は行われません。この場合は、SSL 暗号化 / 復号化のみ使用されます。■ SSL クライアントとサーバーの認証: クライアントとサーバーは相互に自己認証を行い、相互に証明書を送信します。■ SSL サーバー認証: ディレクトリ・サーバーのみ、クライアントに対して自己認証を行います。ディレクトリ・サーバーは、そのサーバーが認証されていることを証明する証明書をクライアントに送信します。
SSL Wallet URL	サーバー側の SSL Wallet の位置を入力します。Wallet の位置を変更する場合は、このパラメータを変更する必要があります。クライアントとサーバーの両方で Wallet の位置を設定する必要があります。たとえば Solaris では、このパラメータは次のように設定します。 file:/home/my_dir/my_wallet Windows NT では、このパラメータは次のように設定します。 file:C:¥my_dir¥my_wallet
SSL Wallet パスワード	サーバー側 Wallet のパスワードを入力します。このパスワードは、Wallet の作成時に設定されています。パスワードを変更する場合は、このパラメータを変更する必要があります。
SSL Wallet パスワードの確認	パスワードを変更するときは、このフィールドに新規パスワードを再度入力します。
SSL ポート	デフォルトの SSL ポートは 636 です。SSL ポートは変更できます。
非 SSL ポート	デフォルトの非 SSL ポートは 839 です。この非 SSL ポートは変更できません。

5. 「適用」をクリックします。

注意： アクティブ・ディレクトリ・サーバー・インスタンスには、再起動するまで変更内容が適用されません。3-7 ページの「[ディレクトリ・サーバー・インスタンスの再起動](#)」を参照してください。

関連項目：

- Oracle Wallet の位置と Oracle Wallet のパスワードの設定は、[付録 D「Oracle Wallet Manager」](#) を参照してください。
- 5-27 ページの「[OID 制御ユーティリティを使用したデバッグ・ログイン・レベルの設定](#)」

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

1. ナビゲータ・ペインで、「Oracle Internet Directory サーバー」 > 「*directory server instance*」 > 「サーバーの管理」 > 「ディレクトリ・サーバー」の順に展開し、「デフォルト構成設定」を選択します。
2. ツールバーの「作成」ボタンをクリックします。「構成設定」ダイアログ・ボックスに「一般」タブ・ページが表示されます。次の表の説明に従って、フィールドに値を入力します。

フィールド	説明
DB の最大接続数	1 つのディレクトリ・サーバー・プロセスで処理可能なデータベースの同時接続数を入力します。デフォルトは 10 です。
子プロセスの数	単一のインスタンスが起動できるサーバー・プロセスの数を入力します。デフォルトは 1 です。
設定	構成設定エントリの番号を入力します。デフォルトの構成設定は 0（ゼロ）です。異なる構成設定を必要な数だけ設定できます。複数のインスタンスで同じパラメータを必要とする場合は、同一の構成設定を使用できます。設定番号は変更可能です。

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

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

フィールド	説明
SSL 認証	次の中から 1 つ選択します。 <ul style="list-style-type: none">■ SSL 認証なし: クライアントとサーバーのいずれも、相手に対して自己認証を行いません。証明書の送信または交換は行われません。この場合は、SSL 暗号化 / 復号化のみ使用されます。■ SSL クライアントとサーバーの認証: クライアントとサーバーは相互に自己認証を行い、相互に証明書を送信します。■ SSL サーバー認証: ディレクトリ・サーバーのみ、クライアントに対して自己認証を行います。ディレクトリ・サーバーは、そのサーバーが認証されていることを証明する証明書をクライアントに送信します。
SSL Wallet URL	サーバー側の SSL Wallet の位置を入力します。Wallet の位置を変更する場合は、このパラメータを変更する必要があります。クライアントとサーバーの両方で Wallet の位置を設定する必要があります。たとえば Solaris では、このパラメータは次のように設定します。 file:/home/my_dir/my_wallet Windows NT では、このパラメータは次のように設定します。 file:C:¥my_dir¥my_wallet
SSL Wallet パスワード	サーバー側 Wallet のパスワードを入力します。このパスワードは、Wallet の作成時に設定されています。パスワードを変更する場合は、このパラメータを変更する必要があります。
SSL Wallet パスワードの確認	パスワードを変更するときは、このフィールドに新規パスワードを再度入力します。
SSL ポート	デフォルトの SSL ポートは 636 です。SSL ポートは変更できます。

4. 「OK」をクリックします。

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

構成設定エントリを変更する手順は、次のとおりです。

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

次の表の説明に従って、「一般」タブのフィールドの値を変更します。

フィールド	説明
DB の最大接続数	1 つのディレクトリ・サーバー・プロセスで処理可能なデータベースの同時接続数を入力します。デフォルトは 10 です。
子プロセスの数	単一のインスタンスが起動できるサーバー・プロセスの数を入力します。デフォルトは 1 です。
設定	構成設定エントリの番号を入力します。デフォルトの構成設定は 0（ゼロ）です。異なる構成設定を必要な数だけ設定できます。複数のインスタンスで同じパラメータを必要とする場合は、同一の構成設定を使用できます。設定番号は変更可能です。

どの値も変更できます。「適用」をクリックして変更値を保存してください。

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

フィールド	説明
SSL 使用可能	SSL 認証を使用可能にするときに選択します。このチェックボックスを選択しない場合、SSL は使用されないため、このページの他のパラメータを設定する必要はありません。
SSL 認証	次の中から 1 つ選択します。 <ul style="list-style-type: none"> ■ SSL 認証なし: クライアントとサーバーのいずれも、相手に対して自己認証を行いません。証明書の送信または交換は行われません。この場合は、SSL 暗号化 / 復号化のみ使用されます。 ■ SSL クライアントとサーバーの認証: クライアントとサーバーは相互に自己認証を行い、相互に証明書を送信します。 ■ SSL サーバー認証: ディレクトリ・サーバーのみ、クライアントに対して自己認証を行います。ディレクトリ・サーバーは、そのサーバーが認証されていることを証明する証明書をクライアントに送信します。
SSL Wallet URL	<p>サーバー側の SSL Wallet の位置を入力します。Wallet の位置を変更する場合は、このパラメータを変更する必要があります。クライアントとサーバーの両方で Wallet の位置を設定する必要があります。たとえば Solaris では、このパラメータは次のように設定します。</p> <pre>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 パスワード	サーバー側 Wallet のパスワードを入力します。このパスワードは、Wallet の作成時に設定されています。パスワードを変更する場合は、このパラメータを変更する必要があります。
SSL Wallet パスワードの確認	パスワードを変更するときは、このフィールドに新規パスワードを再度入力します。
SSL ポート	デフォルトの SSL ポートは 636 です。SSL ポートは変更できます。

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

注意： アクティブ・ディレクトリ・サーバー・インスタンスには、再起動するまで変更内容が適用されません。3-7 ページの「[ディレクトリ・サーバー・インスタンスの再起動](#)」を参照してください。

関連項目： Oracle Wallet の位置と Oracle Wallet のパスワードの設定は、[付録 D「Oracle Wallet Manager」](#)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。

- ナビゲータ・ペインで、「サーバーの管理」>「ディレクトリ・サーバー」の順に展開します。
- 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。
- ツールバーの「削除」ボタンをクリックします。

注意： アクティブ・ディレクトリ・サーバー・インスタンスには、再起動するまで変更内容が適用されません。3-7 ページの「[ディレクトリ・サーバー・インスタンスの再起動](#)」を参照してください。

コマンドライン・ツールを使用したサーバー構成設定エントリの管理

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

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

関連項目： LDIF の詳細は、A-2 ページの「**LDAP 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 ディレクトリ・サーバー・インスタンスを追加する場合は、既存の構成設定エントリを使用するか、新しいインスタンス用に新規の構成設定エントリを追加します。

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

1. テキスト・エディタで入力ファイルを作成します。

入力ファイルは LDIF 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 は新規エントリの相対識別名（ローカル名）、Wallet の位置は /HOME/test/wallet、Wallet パスワードは welcome です。

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

2. 入力ファイルを使用して `ldapadd` を実行します。

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

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

関連項目：

- A-2 ページの「[LDAP データ交換フォーマット \(LDIF\) の構文](#)」
- このコマンドで利用できるオプションの詳細は、A-4 ページの「[ldapadd の構文](#)」を参照してください。
- 構成設定エントリの属性の説明は、C-5 ページの「[構成設定エントリの属性](#)」を参照してください。

ldapmodify を使用した構成設定エントリの変更と削除

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

1. 入力ファイルを作成します。

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

入力ファイルは LDIF 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=osldapd,cn=subconfigsubentry` が、既存の構成設定エントリの識別名（ローカル名）です。この例は、`orclsslport` パラメータを 7000 に変更する方法を示しています。

```
dn:cn=configset2,cn=osldapd,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 ページの「[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-15 ページの「[ldapmodify の構文](#)」を参照してください。
- 構成設定エントリの属性の説明は、C-5 ページの「[構成設定エントリの属性](#)」を参照してください。

システム操作属性の設定

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

この項では、次の項目について説明します。

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

関連項目： 2-5 ページの「[属性情報の種類](#)」

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

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

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

フィールド	説明	デフォルト値	変更可能？
構成設定の位置	このサーバーに最上位のネーミング・コンテキストを保持しているエントリの識別名。	cn=subconfigsubentry	いいえ
索引付き属性の位置	すべての索引付き属性を含むエントリの識別名。	cn=catalogs	いいえ
命名コンテキスト	このサーバーに格納されているネーミング・コンテキストの識別名。新しい値をフィールドに入力します。値に自信がない場合は、「参照」をクリックして検索ウィンドウを表示してください。	なし	はい
ディレクトリ・バージョン	使用している Oracle Internet Directory のバージョン（リリース）。	OID9.0.2.1.0	いいえ
暗号化パスワード	パスワードを暗号化するハッシュ・アルゴリズム。オプションは次のとおりです。 <ul style="list-style-type: none">■ MD4■ MD5■ 暗号化なし■ SHA■ UNIX Crypt	MD4	はい
プロセス・インスタンスの位置	このサーバーにインスタンス・レジストリを保持しているエントリの識別名。	cn=subregistrysubentry	いいえ
問合せエントリの返送制限	検索で戻されるエントリの最大数。	1000	はい
レプリケーション承諾	レプリケーション承諾を保持しているエントリの識別名。	cn=orclareplagreements	いいえ
レプリケーション・ログの位置	このサーバーに変更ログを保持しているエントリの識別名。	cn=changelog	いいえ
レプリケーション状態の位置	このサーバーに変更ステータスを保持しているエントリの識別名。	cn=changestatus	いいえ
スキーマ定義の位置	スキーマの識別名。	cn=subschemasubentry	いいえ

フィールド	説明	デフォルト値	変更可能？
サーバー・モード	サーバーにデータを書き込むことができるかどうかを指定します。この値は、「読み込み / 書き込み」か「読み込み専用」のいずれかに変更できます。レプリケーション時はデフォルトを「読み込み専用」に変更してください。	読み込み / 書き込み	選択肢は「読み込み / 書き込み」および「読み込み専用」です。
サーバー処理の制限時間	検索の最大実行時間（秒）。	3600	はい
「サポートされた制御リスト」	任意の LDAP 操作の拡張情報。Oracle Internet Directory がサポートしている制御の種類は、supportedcontrol 属性の値としてルート DSE にリストされています。制御の各種類には、LDAP 規格で定義されているオブジェクト識別子が関連付けられています。サポートされている制御属性の値は、制御の種類に割り当てられた標準のオブジェクト識別子です。	manageDSACtrl	いいえ
エントリ・キャッシュを使用可能にする	エントリ・キャッシングを使用可能にするかどうかを指定します。使用可能にする場合は 1、使用禁止にする場合は 0（ゼロ）です。	1	はい
エントリ・キャッシュ・サイズ（バイト）	エントリ・キャッシュが使用できる RAM の最大バイト数を指定します。	100M	はい
エントリ・キャッシュ内の最大エントリ	エントリ・キャッシュ内に存在可能な最大エントリ数を指定します。	25,000	はい

ldapmodify を使用したシステム操作属性の設定

変更可能なシステム操作属性は、次のとおりです。

属性	説明	デフォルト
namingContexts	このサーバーに格納されているネーミング・コンテキストの最上位識別名。ネーミング・コンテキストとして識別名を公開するには、スーパー・ユーザー権限を持っている必要があります。	なし
orclCryptoScheme	パスワードを暗号化するハッシュ・アルゴリズム。オプションは次のとおりです。 <ul style="list-style-type: none">■ MD4■ MD5■ 暗号化なし■ SHA■ UNIX Crypt	MD4
orclSizeLimit	検索で戻されるエントリの最大数。	1000
orclServerMode	サーバーにデータを書き込むことができるかどうかを指定します。レプリケーション時はデフォルトを「読み専用」に変更してください。	読み / 書き
orclTimeLimit	検索の最大実行時間（秒）。	3600
orclcacheenabled	エントリ・キャッシングを使用可能にするかどうかを指定します。使用可能にする場合は 1、使用禁止にする場合は 0（ゼロ）です。	1
orclcachemaxsize	エントリ・キャッシュが使用できる RAM の最大バイト数。	100M
orclcachemaxentries	エントリ・キャッシュ内に存在可能な最大エントリ数。	25,000

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

関連項目： ldapmodify の詳細とそのオプションのリストは、A-15 ページの「[ldapmodify の構文](#)」を参照してください。

ネーミング・コンテキストの管理

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

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

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

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

ネーミング・コンテキストを公開する前に、次のことを確認してください。

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

この項では、次の項目について説明します。

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

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

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

ldapmodify を使用したネーミング・コンテキストの公開

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

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

スーパー・ユーザー、ゲスト・ユーザーおよびプロキシ・ユーザーの管理

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

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

11-5 ページの「[間接認証](#)」で説明されているように、通常**プロキシ・ユーザー**はファイアウォールまたは RADIUS サーバーなど、中間層のある環境で使用されます。プロキシ・ユーザーのデフォルトのユーザー名は `proxy`、デフォルトのパスワードは `proxy` です。

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

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

関連項目： アクセス権限の設定方法は、[第 13 章「ディレクトリ・アクセス制御」](#)を参照してください。

この項では、次の項目について説明します。

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

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

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

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

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

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

フィールド	説明
スーパー・ユーザー名	スーパー・ユーザーの名前を入力します。デフォルトは <code>orcladmin</code> です。
スーパー・ユーザー・パスワード	スーパー・ユーザーのパスワードを入力します。デフォルトは <code>welcome</code> です。このパスワードはすぐに変更してください。
ゲストのログイン名	ゲスト・ログイン名を入力します。ゲストには、そのディレクトリ内の アクセス制御ポリシー・ポイント で指定されている権限が与えられます。デフォルトは <code>guest</code> です。
ゲストのログイン・パスワード	ゲスト・ログイン・パスワードを入力します。デフォルトは <code>guest</code> です。
プロキシ・ログイン名	プロキシ・ログイン名を入力します。プロキシ・ユーザーには、そのディレクトリ内の <code>ACP</code> で指定されている権限が与えられます。デフォルトは <code>proxy</code> です。
プロキシ・ログイン・パスワード	プロキシ・ログイン・パスワードを入力します。デフォルトは <code>proxy</code> です。このパスワードはすぐに変更してください。

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

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

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

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

たとえば、スーパー・ユーザーのパスワードを *superuserpassword* に変更するには、ldapmodify で、次のように記述した LDIF ファイルを使用して [ディレクトリ固有のエントリ](#) 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-15 ページの [「ldapmodify の構文」](#) を参照してください。

検索の構成

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

この項では、次の項目について説明します。

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

Oracle Directory Manager を使用した検索の構成

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

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

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

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

1. ナビゲータ・ペインで、「Oracle Internet Directory サーバー」を展開して、ディレクトリ・サーバー・インスタンスを選択します。そのサーバーに対応するタブ・ページが右側のペインに表示されます。
2. 「システム操作属性」タブ・ページの「サーバー処理の制限時間」フィールドに、検索の完了までの最大秒数を入力します。デフォルトは 3600 です。
3. 「適用」をクリックします。

ldapmodify を使用した検索の構成

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は 500 に変更されます。

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

ldapmodify を使用した、検索の最大時間の設定

次の例では、検索の最大時間は 2400 に変更します。

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

関連項目： A-15 ページの「[ldapmodify の構文](#)」

ディレクトリ・サーバーの監視、デバッグおよび監査

この項では、次の項目について説明します。

- [Oracle Internet Directory サーバー管理機能フレームワークによる Oracle Internet Directory サーバーの監視](#)
- [デバッグ・ロギング・レベルの設定](#)
- [監査ログの使用方法](#)

Oracle Internet Directory サーバー管理機能フレームワークによる Oracle Internet Directory サーバーの監視

Oracle Internet Directory サーバー管理機能フレームワークを使用すると、ディレクトリ・サーバーに関する次の統計を監視できます。

- LDAP 要求キュー、メモリー、LDAP セッションおよびデータベース・セッションに関するサーバーの健全性統計
- サーバーの操作とキューに関する一般統計
- セキュリティに関係する重要なイベント
- システム・リソースに関係する重要イベント
- レプリケーション・サーバーのステータス情報
- Oracle Directory Integration Server のステータス情報と統合プロファイル

関連項目： [第 28 章「Oracle Directory Integration Platform の概要とコンポーネント」](#)

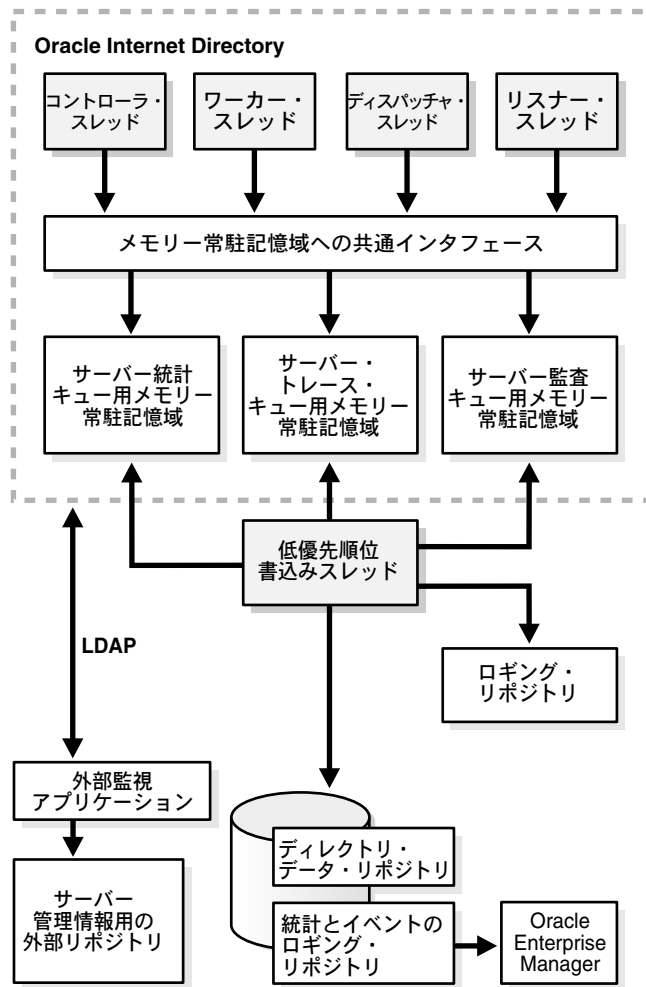
これらの統計とイベントには、LDAP 問合せインタフェースが提供されないことに注意してください。

一部の監視情報は、Oracle Enterprise Manager の Web ベース Graphical User Interface (GUI) ツールによって使用可能です。OID のサーバー管理機能については、Oracle Enterprise Manager の Web ベース GUI ツールのオンライン・ヘルプを参照してください。

Oracle Internet Directory サーバー管理機能のアーキテクチャとコンポーネント

[図 5-2](#) と後続の説明は、ディレクトリ・サーバー管理機能の様々なコンポーネント間の関係を示しています。

図 5-2 Oracle Internet Directory サーバー管理機能のアーキテクチャ



ディレクトリ・サーバー ディレクトリ・サーバーは、クライアントからのディレクトリ要求に応答します。ディレクトリ・サーバーには、4種類の機能スレッド（ディスパッチャ、リスナー、コントローラおよびワーカー）があります。ディレクトリ・サーバーは、クライアントからの LDAP 要求を受け入れて処理し、LDAP 応答をクライアントに戻します。

Oracle Internet Directory サーバー管理機能フレームワークを使用して実行時監視を設定すると、サーバーの4つの機能スレッドによって指定の情報が記録され、ローカル・メモリーに格納されます。

関連項目： ディレクトリ・サーバーの説明は、2-19 ページの「[Oracle ディレクトリ・サーバー・インスタンス](#)」を参照してください。

メモリー常駐記憶域 この記憶域は、ローカル・プロセス・メモリーです。Oracle Internet Directory サーバー管理機能フレームワークは、統計、トレースおよび監査用にそれぞれローカル・プロセス・メモリーを割り当てます。各メモリーは、ローカル・メモリー記憶域でそれぞれ個別のデータ構造を維持します。

低優先順位書込みスレッド この専用書込みスレッドはサーバー機能スレッドとは異なり、サーバー統計、監査ログおよびトレース情報をリポジトリに書き込みます。システム・オーバーヘッドに影響を与えないように、優先順位は低く抑えられています。

外部監視アプリケーション Oracle Internet Directory サーバー管理機能フレームワークに対しては専用モジュールまたは外部モジュールであるこのモジュールは、ディレクトリ・サーバーとの標準 LDAP インタフェースを介して統計を収集し、このモジュール自体のリポジトリに格納します。

サーバー管理情報用の外部リポジトリ 監視エージェントが、収集されたディレクトリ・サーバー統計の格納に使用するリポジトリです。監視エージェントによって、このリポジトリの実装方法が決定します。

Oracle Enterprise Manager (OEM) Oracle Enterprise Manager は、統計とイベントのリポジトリから監視データを抽出し、Web ベースの GUI で表します。ユーザーは、標準的なブラウザでそのデータを参照できます。リポジトリには、一般的な問合せやカスタム問合せで収集されたデータを格納できます。

ロギング・リポジトリ (ファイル・システム) このリポジトリはファイル・システムを使用して、ディレクトリ・サーバーの様々なモジュールでトレースした情報を格納します。この格納にファイル・システムを使用することによって、Oracle Internet Directory サーバー管理機能フレームワークは、オペレーティング・システムの機能とセキュリティを利用します。

ディレクトリ・データ・リポジトリ このリポジトリには、ユーザー・エントリやグループ・エントリなど、ユーザーが登録した全データが格納されます。

統計とイベントのリポジトリ このリポジトリは、情報をファイル・システムではなく、ディレクトリ・データ・リポジトリと同じデータベースに格納する点を除いて、トレース・リポジトリと類似しています。Oracle Internet Directory サーバー管理機能フレームワークは、次の場合にこのリポジトリを使用します。

- 標準 LDAP 操作を使用して、情報を格納および取得する場合
- 既存のアクセス制御ポリシー・ポイントを使用して、収集した情報のセキュリティを管理する場合

ディレクトリ管理機能フレームワークは、この 2 つの情報を個別に格納することによって、ディレクトリ・データと収集された情報を区別します。

Oracle Internet Directory サーバー管理機能の構成情報の位置

Oracle Internet Directory サーバー管理機能フレームワークは、サーバー統計、サーバー・トレースおよびサーバー監査の 3 モジュールすべての構成パラメータをディレクトリの DSE ルートに格納します。収集する情報の周期性、量およびレベルを指定するには、これらのパラメータに適切な値を設定する必要があります。

Oracle Internet Directory サーバー管理機能の構成

Oracle Internet Directory サーバー管理機能フレームワークを構成するには、ldapmodify を使用して DSE ルート・エントリのこれらの属性に正の整数値を設定します。

属性	説明
orclStatsFlag	Oracle Internet Directory サーバー管理機能フレームワークを使用可能にするかどうかを示します。使用可能にするには、1 に設定します。使用禁止にするには、0（ゼロ）に設定します。
orclStatsPeriodicity	サンプル統計を収集する頻度、つまり間隔（分単位）を指定します。1（分単位）以上を設定します。

関連項目： Oracle Internet Directory サーバー管理機能を使用した Oracle Internet Directory サーバーの監視と管理の詳細は、Oracle Enterprise Manager オンライン・ヘルプ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

デバッグ・ロギング・レベルを設定する手順は、次のとおりです。

1. ナビゲータ・ペインで、「Oracle Internet Directory サーバー」を展開して、サーバーのインスタンスを選択します。そのサーバーに対応するタブ・ページが右側のペインに表示されます。
2. 「デバッグ・フラグ」タブを選択します。

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

OID 制御ユーティリティを使用したデバッグ・ロギング・レベルの設定

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

デバッグ・レベルは加算方式であるため、アクティブ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、**ディレクトリ固有のエントリ** 属性 `orcldebugflag` を必要なレベルに変更します。デバッグ・レベルは、次のレベルのいずれかに構成できます。

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

表 5-1 は、デバッグ・ロギング・レベルの全リストです。

表 5-1 デバッグ・ロギング・レベル

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

表 5-1 デバッグ・ロギング・レベル（続き）

ロギング・レベルの値	提供される情報
32768	レプリケーション固有の操作
65535	潜在的なすべてのデバッグ操作 / データ

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

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

この例では、デバッグ・フラグを付けて、Oracle ディレクトリ・サーバーと Oracle ディレクトリ・レプリケーション・サーバーを再起動しています。

監査ログの使用方法

監査ログには、Oracle ディレクトリ・サーバーに関するセキュリティ上および操作上重要なイベントが記録されています。ログはディレクトリ・サーバーのイベントによって生成されるため、開発者による監査ログ・エントリの作成はできません。監査ログ・エントリを作成できるのはディレクトリ・サーバー自体のみです。

監査ログは、通常のディレクトリ・エントリで構成されています。イベントごとに 1 つのエントリがあります。監査ログは `ldapsearch` を使用して問い合わせることができ、監査ログ・エントリは `Oracle Directory Manager` を使用して表示できます。

デフォルトでは、監査ログは使用禁止です。監査ログを使用可能にするには、[ディレクトリ固有のエントリ](#) 属性の `orclauditlevel` を必要なレベルに変更します。監査レベルは、選択したイベントのみを監査するように構成できます。

関連項目：

- 監査レベルのリストは、5-30 ページの「[監査可能なイベント](#)」を参照してください。
- 監査レベルの指定は、5-31 ページの「[監査レベルの設定](#)」を参照してください。
- 5-33 ページの「[Oracle Directory Manager を使用した監査ログ・エントリの検索](#)」
- 5-34 ページの「[ldapsearch を使用した監査ログ・エントリの検索](#)」
- A-11 ページの「[ldapdelete の構文](#)」

監査ログ・エントリの構造

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

属性	説明
<code>orclsequence</code>	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。
<code>orcleventtype</code>	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。
<code>orcleventtime</code>	イベントを発生させる時刻を指定します。時刻は、 UTC (Coordinated Universal Time) 形式です。UTC 形式であることは、値の最後の <code>z</code> によって示されます。たとえば、次のようになります。 <code>orcleventtime: 199811281010z</code>
<code>orcluserdn</code>	操作を実行するために Oracle ディレクトリ・サーバーにログインしたユーザーの識別子を指定します。これはカタログ化属性です。
<code>orclopresult</code>	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。
<code>orclauditmessage</code>	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。
<code>objectclass</code>	値は <code>top</code> と <code>orclauditoc</code> 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・エントリは含まれません。たとえば、検索条件が `objectclass=top` の場合、監査ログ・エントリは結果として戻されません。検索のベースとして `cn=auditlog` を指定した場合のみ、監査ログ・エントリが検索できます。

注意： デフォルトでは、属性 `orcleventtype` と `orcluserdn` は、Oracle Internet Directory のインストール時に索引付けされています。これらの属性から索引を削除すると、この 2 つの属性の検索はできなくなります。索引を再作成するには、カタログ管理ツールを使用します。6-29 ページの「[コマンドライン・ツールを使用した属性の索引付け](#)」を参照してください。

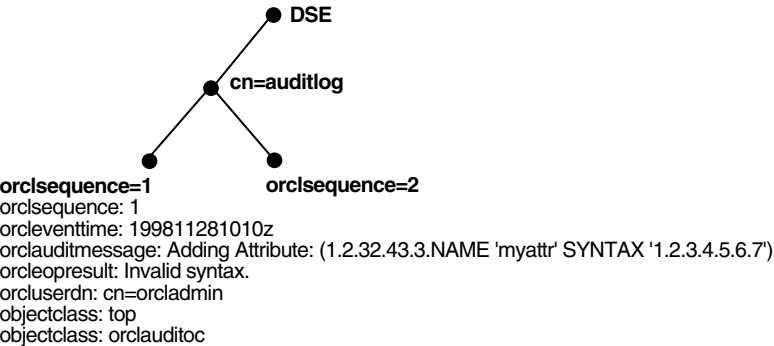
関連項目：

- カタログ化属性の詳細は、A-39 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、2-9 ページの「[オブジェクト・クラスの型](#)」を参照してください。

ディレクトリ情報ツリーにおける監査ログ・エントリの位置

監査ログのコンテナは DSE の一部です。そのエントリは DSE の子として保持され、orclsequence 属性に従って構成されています。[図 5-3](#) を参照してください。

図 5-3 DSE 下のサンプル監査ログ



監査可能なイベント

[表 5-2](#) は、監査可能なイベントとその監査レベルを示しています。3 列目の「監査レベル」は 16 進の値です。複数のイベントを監査するには、この列のそれぞれのイベントに対応する値を加算します。

表 5-2 監査可能なイベント

イベント	説明	監査レベル
スーパー・ユーザー・ログイン	スーパー・ユーザーのサーバーへのバインド (成功または失敗)	0x0001
スキーマ要素の追加 / 置換	新規スキーマ要素の追加 (成功または失敗)	0x0002
スキーマ要素の削除	スキーマの削除 (成功または失敗)	0x0004
バインド	バインドに失敗した例	0x0008

表 5-2 監査可能なイベント（続き）

イベント	説明	監査レベル
アクセス違反	アクセス制御ポリシー・ポイントで否認されたアクセス	0x0010
ディレクトリ固有のエントリ (DSE) の変更	DSE に対する変更（成功または失敗）	0x0020
レプリケーション・ログイン	レプリケーション・サーバーの認証（成功または失敗）	0x0040
ACL の変更	アクセス制御リストの変更	0x0080
ユーザー・パスワードの変更	ユーザー・パスワード属性の変更	0x0100
追加	ldapadd 操作（成功または失敗）	0x0200
削除	ldapdelete 操作（成功または失敗）	0x0400
変更	ldapmodify 操作（成功または失敗）	0x0800
識別名の変更	ldapModifyDN 操作（成功または失敗）	0x1000

監査レベルの設定

DSE 属性 `orclauditlevel` の設定は、現行の監査レベルを示します。前述の項で説明したイベントを使用可能または使用禁止にできます。属性の値が 0（ゼロ）の場合（これがデフォルトです）、監査は使用禁止です。

監査レベルの設定には、Oracle Directory Manager または `ldapmodify` のいずれかを使用します。この項では、両方の方法について説明します。

Oracle Directory Manager を使用した監査レベルの設定 Oracle Directory Manager を使用して監査レベルを設定する手順は、次のとおりです。

1. ナビゲータ・ペインで、「Oracle Internet Directory サーバー」を展開して、ディレクトリ・サーバー・インスタンスを選択します。
2. 右側のペインで、「監査マスク・レベル」タブ・ページを選択します。
3. 使用する監査レベルのチェックボックスを選択します。
4. 「適用」をクリックします。

成功したイベントと失敗したイベントが選択されている場合は、次を除き、双方とも監査ログに入力されます。

- バインド：バインドに失敗した例のみをログに記録します。
- アクセス違反：ACP によってアクセスが拒否されたイベントのみをログに記録します。

orclauditlevel に変更を加えた場合は、変更内容を有効にするためにディレクトリ・サーバー・インスタンスを再起動してください。

関連項目： ディレクトリ・サーバーを再起動する方法は、3-7 ページの「[ディレクトリ・サーバー・インスタンスの再起動](#)」を参照してください。

関連項目： 各監査レベルの説明は、5-30 ページの「[監査可能なイベント](#)」を参照してください。

ldapmodify を使用した監査レベルの設定 複数のイベントを監査するには、その監査マスクの値を加算します。たとえば、次の 3 つのイベントを監査するとします。

イベント	監査レベル	値
スキーマ要素の削除	0x0004	4
DSE の変更	0x0020	32
追加	0x0200	512
合計		548

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

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

orclauditlevel に変更を加えた場合は、変更内容を有効にするためにディレクトリ・サーバー・インスタンスを再起動してください。

関連項目： ディレクトリ・サーバーを再起動する方法は、3-7 ページの「[ディレクトリ・サーバー・インスタンスの再起動](#)」を参照してください。

監査ログ・エントリの検索

Oracle Directory Manager または ldapsearch を使用して、監査ログ・エントリを検索できます。

Oracle Directory Manager を使用した監査ログ・エントリの検索

Oracle Directory Manager を使用して監査ログ・エントリを表示する手順は次のとおりです。

1. ナビゲータ・ペインで、「Oracle Internet Directory サーバー」 > 「*directory server instance*」の順に展開し、「監査ログの管理」を選択します。対応する右側のペインが表示されます。
2. 「最大結果件数」フィールドに、検索で取り出すエントリの最大数を入力します。デフォルトは 200 です。ここで指定できるディレクトリ・サーバーのエントリ数は、最大 1000 です。
3. 「最长検索時間」ボックスに、検索の最大時間を秒数で入力します。ここで入力する値は、少なくともデフォルト値の 25 以上にする必要があります。ここで指定できるディレクトリ・サーバーの最大検索時間は、1 時間です。
4. 「検索基準」ボックスで、検索基準バーのリストとテキスト・フィールドを使用して、検索基準をさらに詳細に指定します。
 - a. 検索基準バーの一番左のリストから、検索するエントリの属性を選択します。各エントリですべての属性が使用されているわけではないため、指定した属性が、検索しているエントリの属性に実際に一致していることを確認する必要があります。一致する属性がない場合は、検索に失敗します。
 - b. 検索基準バーの中央のリストから、フィルタを選択します。オプションは次のとおりです。

フィルタ	説明
開始	属性の値の始めの数文字のみを使用して検索します。
終了	指定した属性の値の終わりの数文字のみを使用してエントリを検索します。
含む	値の位置を限定せずに、ユーザーの入力値が指定した属性に含まれているエントリを検索します。
完全一致	指定した属性がユーザーの入力値に一致するエントリを検索します。
以上	指定した属性が、数値順またはアルファベット順で入力値より大か等しいエントリを検索します。
以下	指定した属性が、数値順またはアルファベット順で入力値より小か等しいエントリを検索します。
存在	指定した属性を持つエントリが、ツリーのそのレベルに存在するかどうかを判断します。この関連の使用に値の入力は不要です。

- c. 検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。
たとえば、選択した属性が cn の場合は、検索する個々の一般名を入力します。
- 5. 検索をさらに詳細に指定するには、「検索基準」ボックスのボタンを使用して検索基準バーを拡張します。

ボタン	説明
新規作成	「検索基準」フィールドに、新しい検索基準バーを作成します。このボタンは、「検索基準」フィールドに何も表示されていないときのみ使用可能です。
AND	「検索基準」フィールドに、別の検索基準バーを作成します。指定した両方の属性を持つエントリをすべて検索します。たとえば、cn=Baldwins And title=Laborer と指定すると、cn が Baldwins で、かつ title が laborer のエントリがすべて取り出されます。
OR	「検索基準」フィールドに、別の検索基準バーを作成します。指定した属性のいずれかを持つエントリをすべて検索します。たとえば、title=Laborer Or title=Foreman と指定すると、title が laborer または foreman の従業員がすべて取り出されます。
NOT	選択した検索基準バーの基準を除外し、指定した基準を満たさないエントリをすべて取り出します。たとえば、cn=Frank Not title=Laborer と指定すると、cn が Frank で、title が laborer ではない個人がすべて取り出されます。
削除	選択した検索基準バーを削除します。

- 6. 「検索」をクリックします。検索結果は「識別名」ボックスに表示されます。
- 7. 特定の監査ログ・エントリのプロパティを表示するには、そのプロパティを「識別名」ボックスで選択し、「プロパティの表示」をクリックします。「監査ログ・エントリ」ダイアログ・ボックスに、選択した監査ログのプロパティが表示されます。

関連項目： 検索で表示するエントリ数と検索の制限時間の設定方法は、5-21 ページの「[検索の構成](#)」を参照してください。

ldapsearch を使用した監査ログ・エントリの検索 監査ログのコンテナの **DN** は、cn=auditlog です。監査ログ・エントリを検索するには、検索のベースとしてコンテナ・オブジェクト cn=auditlog を指定し、サブツリー検索または 1 レベルの検索を実行します。

関連項目： A-22 ページの「[ldapsearch の構文](#)」

監査ログの削除

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

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

アクティブ・サーバー・インスタンスの情報の表示

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

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

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

Oracle データベース・サーバー接続時のパスワードの変更

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

関連項目： [A-48 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」](#)

別名エントリの間接参照

この項では、別名エントリ間接参照の概要について説明し、使用モデルおよびメッセージのリストを示します。

この項では、次の項目について説明します。

- [別名エントリ間接参照の概要](#)
- [別名エントリ間接参照の使用方法](#)
- [成功メッセージとエラー・メッセージ](#)

別名エントリ間接参照の概要

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

[図 5-4](#) の `ou=uk sales,ou=global sales,o=oracle,c=us` エントリは、`ou=sales,o=oracle,c=uk` エントリを指し示す別名エントリです。（すべての情報と同様に）ポインタは、属性（別名エントリの別名化されたオブジェクト名の属性）として保持されます。別名エントリとディレクトリのオブジェクト・エントリとを区別するために、別名エントリには特別なオブジェクト・クラス別名があります。

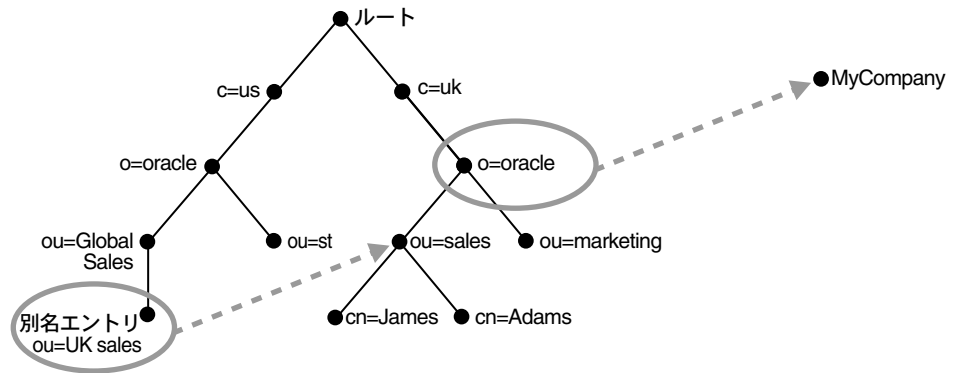
別名オブジェクト・クラスの定義

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

別名化されたオブジェクト名の定義

(2.4.5.1 NAME 'aliasedObjectName' EQUALITY distinguishedNnameMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE)

図 5-4 別名エントリの例



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

別名エントリ間接参照の使用方法

この項では、次の項目について説明します。

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

別名エントリの追加

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

1. 次のエントリで `sample.ldif` ファイルを作成します。

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

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

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

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

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

2. 次のコマンドを使用して、エントリをディレクトリに追加します。

```
ldapadd -p <port> -h <host> -f sample.ldif
```

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

関連項目： エラー・メッセージは、5-41 ページの表 5-3 「エントリ別名間接参照メッセージ」を参照してください。

図 5-5 sample.ldif ファイルの作成結果を示すツリー

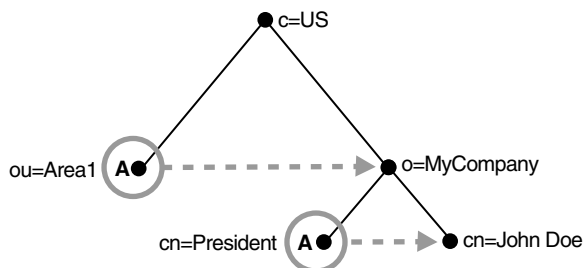


図 5-5 の文字 A は、別名エントリを表します。

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

ベース検索

ベース検索は、指定した別名エントリの最上位レベルを検索します。

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

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

```

ディレクトリ・サーバーは、ベース検索時に検索要求に指定されたベースを調査し、位置が特定された場合はその位置をユーザーに戻します。例のように、ベースが別名エントリで、検索要求に -a find が指定されている場合、LDAP サーバーは別名エントリを自動的に間接参照し、間接参照エントリを戻します。したがって、検索では ou=Areal,c=us (別名エントリ) が間接参照され、o=oracle,c=us が戻されます。

1 レベルの検索

1 レベル検索では、指定したベース・レベルに対する子のみを検索します。

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

フラグは、次のとおりです。

フラグ	内容
LDAP_DEREF_NEVER	-a never
LDAP_DEREF_FINDING	-a find

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

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

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

```

LDAP サーバーは、検索操作を 2 つのステップで実行します。

- 1. LDAP サーバーは、検索要求に指定されたベースを検索します。
- 2. ベースの位置を特定した LDAP サーバーは、ベース以下のすべての 1 レベル・エントリを検索してフィルタ基準と一致するエントリを戻します。

この例では検索要求に -a find が指定されているため、LDAP サーバーは、ベースの検索中 (最初のステップ) に自動的に間接参照しますが、ベースの 1 レベル下の別名エントリは間接参照しません。したがって、検索では ou=Areal,c=us (別名エントリ) が間接参照さ

れ、o=oracle,c=us 以下の 1 レベル・エントリが検索されます。1 レベル・エントリの 1 つは、間接参照されずにそのまま戻される cn=President,o=oracle,c=us です。

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

サブツリーの検索

サブツリー検索は、ベース、子、孫（ファミリー・ツリー）を検索します。

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

フラグは、次のとおりです。

フラグ	内容
LDAP_DEREF_NEVER	-a never
LDAP_DEREF_FINDING	-a find

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

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

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

LDAP サーバーは、検索操作を 2 つのステップで実行します。

- LDAP サーバーは、検索要求に指定されたベースを検索します。
- ベースの位置を特定した LDAP サーバーは、ベース以下のすべてのエントリを検索してフィルタ基準と一致するエントリを戻します。

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

この検索では、次の情報が戻されます。

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

別名エントリの変更

別名エントリは変更することができます。

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

```
dn: cn=President, o=oracle, c=us
changetype : modify
replace: aliasObjectName
aliasObjectName: cn=XYZ, o=oracle, c=us
```

次のコマンドを使用して、別名エントリを変更します。

```
ldapmodify -p <port> -h <host> -f sample.ldif
```

成功メッセージとエラー・メッセージ

説明列に示した別名の問題が見つかったと、次のメッセージが戻ります。

表 5-3 エントリ別名間接参照メッセージ

メッセージ	説明
別名に問題があります。	次のいずれかの問題が発生した場合に、このエラー・メッセージがクライアントに戻ります。 別名は間接参照されたが、ディレクトリ情報ツリー内のエントリを指し示していない場合。 親が別名である別名エントリを追加しようとした場合。
別名の参照解除に問題があります。	アクセス制御上の問題のため、ユーザーによる別名の間接参照が許可されていない場合は、このエラー・メッセージがクライアントに戻ります。
該当するオブジェクトがありません。	検索要求に指定されたベース識別名がサーバーで見つからない場合は、このエラー・メッセージがクライアントに戻ります。
識別名の構文に誤りがあります。	別名エントリを追加または変更する際、 <code>aliasedObjectName</code> に指定した値に無効な識別名の構文が含まれている場合は、LDAP サーバーがクライアントに <code>invalidDNsyntax</code> エラー・メッセージを戻します。
成功しました	クライアント操作が正常に完了した場合は、LDAP サーバーが成功メッセージを戻します。 間接参照ターゲットが見つかり、検索要求に指定したフィルタと一致しない場合、サーバーは一致エントリなしで成功メッセージを戻します。
不十分なアクセス権限	間接参照エントリに対するアクセス権限がユーザーにない場合は、このエラー・メッセージが戻ります。

ディレクトリ・スキーマの管理

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

この章では、次の項目について説明します。

- [ディレクトリ・スキーマの概要](#)
- [オブジェクト・クラス管理](#)
- [Oracle Directory Manager を使用したオブジェクト・クラスの管理](#)
- [コマンドライン・ツールを使用したオブジェクト・クラスの管理](#)
- [属性管理の概要](#)
- [Oracle Directory Manager を使用した属性の管理](#)
- [コマンドライン・ツールを使用した属性の管理](#)
- [一致規則の表示](#)
- [構文の表示](#)

ディレクトリ・スキーマの概要

ディレクトリ・スキーマには、次の特徴があります。

- ディレクトリに格納できるオブジェクトの種類に関する規則を含んでいます。
- 検索などの処理時にディレクトリ・サーバーとクライアントが情報を扱う方法の規則を含んでいます。
- ディレクトリに格納されているデータの整合性と品質をメンテナンスするのに役立ちます。
- データの重複を削減します。
- ディレクトリに対応したアプリケーションがディレクトリ・オブジェクトにアクセスしたり変更したりするための、予測可能な方法を提供します。

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

この章では、これらの各要素について説明します。

関連項目： 2-12 ページの「[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、2-8 ページの「[オブジェクト・クラス](#)」を参照してください。
- Oracle Internet Directory とともにインストールされるスキーマ・コンポーネントのリストは、[付録 C「スキーマ要素」](#)を参照してください。

この項では、次の項目について説明します。

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

オブジェクト・クラスの追加のガイドライン

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

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

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

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

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

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

関連項目： 6-15 ページの「[属性管理の概要](#)」

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

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

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

オブジェクト・クラスを追加するときは、次のガイドラインに注意してください。

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

関連項目： これらの用語の概念の説明は、2-9 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 ページの「[Oracle Directory Manager を使用したオブジェクト・クラスの管理](#)」
- 6-13 ページの「[コマンドライン・ツールを使用したオブジェクト・クラスの管理](#)」

オブジェクト・クラスの削除のガイドライン

オブジェクト・クラスの削除に関しても、いくつかの制限事項があります。

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

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

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

この項では、次の項目について説明します。

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

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

次の方法でオブジェクト・クラスを検索できます。

- オブジェクト・クラスのプロパティを選択する方法。たとえば、名前やオブジェクト識別子を選択します。
- 選択したプロパティの値を入力する方法。
- 選択したオブジェクト・クラスのプロパティと入力値との関連を指定する検索フィルタを選択する方法。「次の文字で始まる」または「完全に一致する」などのフィルタがあります。

この項では、オブジェクト・クラスの検索の入力方法を説明します。

オブジェクト・クラスを検索する手順は、次のとおりです。

1. ナビゲータ・ペインで「スキーマの管理」を選択します。「スキーマの管理」タブ・ページが、右側のペインに表示されます。
2. 右側のペインの右下の「オブジェクト・クラスの検索」ボタンをクリックするか、メニュー・バーから「編集」>「オブジェクト・クラスの検索」をクリックします。「検索: オブジェクト・クラス」ダイアログ・ボックスが表示されます。
3. 検索基準バーの一番左のメニューから、検索するオブジェクト・クラスのプロパティを選択します。オプションは次のとおりです。

オプション	説明
名前	検索するオブジェクト・クラスの名前。たとえば、「名前」「完全一致」「subAc1」と指定すると、subAc1 オブジェクト・クラスを検索できます。
オブジェクト ID	検索するオブジェクト・クラスのオブジェクト識別子。たとえば、「オブジェクト ID」「次の文字で始まる」「2.5.2」と指定すると、オブジェクト ID が 2.5.2 で始まるオブジェクト・クラスのリストが表示されます。

オプション	説明
説明	「説明」フィールドに含まれている語。たとえば、「説明」「含む」「Shoe」と指定すると、説明列に <i>shoe</i> を含むオブジェクト・クラスのリストが表示されます。
型	検索するオブジェクト・クラスの型。「抽象型」、「構造型」または「補助型」のいずれかを指定します。
スーパー・クラス	検索するオブジェクト・クラスのスーパークラス。
必須属性	検索するオブジェクト・クラスの必須属性。たとえば、「必須属性」「含む」「cn」と指定すると、cn 属性が必須の、すべてのオブジェクト・クラスのリストが表示されます。
オプション属性	検索するオブジェクト・クラスのオプション属性。

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

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

フィルタ	説明
開始	検索するオブジェクト・クラスのプロパティの、始めの数文字のみ使用して検索します。たとえば、「型」「次の文字で始まる」「aux」と指定すると、補助型オブジェクト・クラスの全リストが表示されます。
終了	検索するオブジェクト・クラスのプロパティの、終わりの数文字のみ使用して検索します。たとえば、「型」「終了」「ral」と指定すると、構造型オブジェクト・クラスの全リストが表示されます。
含む	値の位置を限定せずに、ユーザーの入力値が選択したプロパティに含まれているオブジェクト・クラスを検索します。たとえば、「オプション属性」「含む」「cn」と指定すると、cn がオプション属性であるすべてのオブジェクト・クラスのリストが表示されます。
完全一致	選択したプロパティが入力値に完全に一致するオブジェクト・クラスを検索します。たとえば、「スーパー・クラス」「完全一致」「person」と指定すると、スーパークラスとして person を持つすべてのオブジェクト・クラスのリストが表示されます。

フィルタ	説明
以上	選択したプロパティが数値順またはアルファベット順でユーザーの入力値より大か等しいオブジェクト・クラスを検索します。たとえば、「名前」「以上」「orcl」と指定すると、orcl で始まるオブジェクト・クラスから、アルファベットの最後の文字で始まるオブジェクト・クラスまでのリストが表示されます。
以下	選択したプロパティが数値順またはアルファベット順で入力値より小か等しいオブジェクト・クラスを検索します。たとえば、「名前」「以下」「orcl」と指定すると、orcl で始まるオブジェクト・クラスから、アルファベットの最初の文字で始まるオブジェクト・クラスまでのリストが表示されます。
「存在」	選択したプロパティが存在するすべてのオブジェクト・クラスを検索します。たとえば、「必須属性」「存在」と指定すると、必須属性を含むすべてのオブジェクト・クラスのリストが表示されます。

5. 検索基準バーの一番右のテキスト・ボックスに、検索するオブジェクト・クラスのプロパティの値を入力します。たとえば、名前が orcl で始まるすべてのオブジェクト・クラスを検索するには、検索基準バーの一番右のテキスト・ボックスに orcl と入力します。
6. 「検索基準」フィールドの下に、次の表で説明する 5 つのボタンがあります。これらのボタンを使用すると、検索基準をさらに詳細に指定できます。

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

7. 「検索」をクリックします。検索結果が、「検索 : オブジェクト・クラス」ダイアログ・ボックスの下部のウィンドウに表示されます。

Oracle Directory Manager を使用したオブジェクト・クラスのプロパティの表示

スキーマ内のすべてのオブジェクト・クラスを表示する手順は、次のとおりです。

1. ナビゲータ・ペインで「スキーマの管理」を展開します。「スキーマの管理」ペインにある各タブに、スキーマの次のコンポーネントが表示されます。
 - オブジェクト・クラス
 - 属性
 - 構文
 - 一致規則
2. 右側のペインで、「オブジェクト・クラス」タブ・ページを選択します。

個々のオブジェクト・クラスとその属性を調べるには、「オブジェクト・クラス」タブ・ページのオブジェクト・クラスをクリックします。選択したオブジェクト・クラスのプロパティが、「オブジェクト・クラス」ダイアログ・ボックスに表示されます。
3. 「オブジェクト・クラス」ダイアログ・ボックスは、次のとおりです。
 - 属性の継承元のオブジェクト・クラスが「スーパー・クラス」ボックスにリストされます。
 - 必須属性が「必須属性」ボックスにリストされます。
 - オプション属性が「オプション属性」ボックスにリストされます。

各属性が検索式で使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 サーバー」 > 「ディレクトリ・サーバー」の順に展開し、「スキーマの管理」を選択します。
2. 次のいずれかの方法を選択します。
 - 右側のペインで「オブジェクト・クラス」タブを選択し、ツールバーの「作成」ボタンをクリックします。
 - 右側のペインの下「作成」ボタンをクリックします。
 - 「操作」メニューから、「オブジェクト・クラスの作成」を選択します。

「新規オブジェクト・クラス」ダイアログ・ボックスが表示されます。

作成するオブジェクト・クラスに類似しているオブジェクト・クラスを選択して、「類似項目の作成」をクリックする方法もあります。ダイアログ・ボックスが表示され、選択したオブジェクト・クラスの属性が表示されます。選択したオブジェクト・クラスをテンプレートとして使用して、新規のオブジェクト・クラスを作成できます。

3. 次の表に説明されている各フィールドに、情報を入力します。

フィールド	説明
名前	作成するオブジェクト・クラスの名前を入力します。
オブジェクト ID	オブジェクト識別子を入力します。これは、IETF 規格に基づいた、標準化された数値順序です。一意、かつ組織内に設定されたシステムに準拠したものである必要があります。通常この値は、ANSI または ISO など、登録機関によって割り当てられた ID から導出されます。
説明	このオプションのフィールドは、説明の記述のみに使用します。
型	オブジェクト・クラスの型を指定します。「抽象型」、「構造型」、「補助型」、「なし」のいずれかを指定します。
スーパー・クラス	このオブジェクト・クラスを導出するクラスを指定します。このオブジェクト・クラスは、選択したスーパークラスの属性をすべて継承します。構造型オブジェクト・クラスの場合は、そのスーパークラスの 1 つとして必ず top を設定する必要があります。「追加」をクリックすると「スーパー・クラス・セクタ」ダイアログ・ボックスが表示され、追加するスーパークラスを選択できます。
必須属性	値の入力が必要な属性を指定します。「追加」をクリックすると「必須属性セクタ」ダイアログ・ボックスが表示され、追加する必須属性を選択できます。

フィールド	説明
オプション属性	値が必須ではない属性を指定します。「追加」をクリックすると「オプション属性セレクト」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。

- 「OK」をクリックします。

関連項目：

- 2-9 ページの「オブジェクト・クラスの型」
- 2-9 ページの「サブクラス、スーパークラスおよび継承」
- オブジェクト・クラスを追加する方法の詳細は、Oracle Directory Manager のオンライン・ヘルプを参照してください。

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

オブジェクト・クラスを変更する手順は、次のとおりです。

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

フィールド	説明
名前	作成するオブジェクト・クラスの名前を入力します。
オブジェクト ID	オブジェクト識別子を入力します。これは、IETF 規格に基づいた、標準化された数値順序です。一意、かつ組織内に設定されたシステムに準拠したものである必要があります。通常この値は、ANSI または ISO など、登録機関によって割り当てられた ID から導出されます。
説明	このオプションのフィールドは、説明の記述のみに使用します。
型	オブジェクト・クラスの型を指定します。「抽象型」、「構造型」、「補助型」、「なし」のいずれかを指定します。
スーパー・クラス	このオブジェクト・クラスを導出するクラスを指定します。このオブジェクト・クラスは、選択したスーパークラスの属性をすべて継承します。構造型オブジェクト・クラスの場合は、そのスーパークラスの 1 つとして必ず top を設定する必要があります。「追加」をクリックすると「スーパー・クラス・セレクト」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。

フィールド	説明
必須属性	値の入力が必要な属性を指定します。「追加」をクリックすると「必須属性セクタ」ダイアログ・ボックスが表示され、追加する必須属性を選択できます。
オプション属性	値が必須ではない属性を指定します。「追加」をクリックすると「オプション属性セクタ」ダイアログ・ボックスが表示され、追加するオプション属性を選択できます。

4. 「OK」をクリックします。

関連項目：

- 2-9 ページの「[オブジェクト・クラスの型](#)」
- 2-9 ページの「[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例は、6-14 ページの「[例：補助型またはユーザー定義のオブジェクト・クラスへの新規属性の追加](#)」を参照してください。

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

1. ナビゲータ・ペインで「スキーマの管理」を選択します。
2. 右側のペインで「オブジェクト・クラス」タブを選択し、削除するオブジェクト・クラスを選択します。
3. 「削除」をクリックします。

コマンドライン・ツールを使用したオブジェクト・クラスの管理

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

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

関連項目： A-15 ページの「[ldapmodify の構文](#)」

この項では、次の例について説明します。

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

例：新規オブジェクト・クラスの追加

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

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

左右のカッコとオブジェクト識別子の間には、必ず空白を入れてください。

このファイルをロードするには、次のコマンドを入力します。

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

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

抽象型オブジェクト・クラスを作成する場合は、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 ディレクトリ・サーバーによって 1 回のトランザクションでコミットされます。既存のデータは影響されません。入力ファイルには次のように指定します。

```
dn: cn=subschemasubentry
changetype: modify
delete: objectclasses
objectclasses: old value
-
add: objectclasses
objectclasses: new value
```

たとえば、既存のオブジェクト・クラス `country` に属性 `changes` を追加する場合、入力ファイルは次のようになります。

```
dn: cn=subschemasubentry
changetype: modify
delete: objectclasses
objectclasses: ( 2.5.6.2 NAME 'country' SUP top STRUCTURAL MUST c MAY
( searchGuide $ description ) )
-
add: objectclasses
objectclasses: ( 2.5.6.2 NAME 'country' SUP top STRUCTURAL MUST c MAY
( searchGuide $ description $ changes ) )
```

属性管理の概要

この項では、次の項目について説明します。

- [属性の追加に関する規則](#)
- [属性の変更に関する規則](#)
- [属性の削除に関する規則](#)

属性を扱う操作を実行する前に、概念的な観点から属性を理解する必要があります。

多くの場合、ベース・スキーマにある属性で、ユーザーの組織のニーズを満たすことができます。ベース・スキーマにない属性を使用する場合は、新規属性の追加または既存属性の変更が可能です。

デフォルトでは、属性は複数値です。Oracle Directory Manager またはコマンドライン・ツールを使用して、属性を単一値に指定できます。

関連項目： 属性の概念の説明は、2-4 ページの「[属性](#)」を参照してください。

属性の追加に関する規則

属性の追加に関しては、次の規則があります。

- 属性の名前とオブジェクト識別子は、すべてのスキーマ・コンポーネントを通して一意である必要があります。
- 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識別子は、すべてのスキーマ・コンポーネントを通して一意である必要があります。
- 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。

- 削除できるのはユーザー定義属性のみです。ベース・スキーマの属性は削除しないでください。
- 他のスキーマ・コンポーネントから直接または間接的に参照されていない属性は、削除することができます。

エントリの参照先である属性を削除すると、そのエントリはディレクトリ操作に使用できなくなります。

Oracle Directory Manager を使用した属性の管理

この項では、次の項目について説明します。

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

関連項目：

- 属性オプションの詳細は、2-7 ページの「[属性オプション](#)」を参照してください。
- 属性オプションを追加する方法と削除する方法および属性オプションを含むエントリの検索方法は、7-10 ページの「[Oracle Directory Manager](#) を使用した属性オプション付きエントリの管理」および 7-14 ページの「[コマンドライン・ツールを使用した属性オプション付きエントリの管理](#)」を参照してください。

Oracle Directory Manager を使用したすべてのディレクトリ属性の表示

Oracle Directory Manager を使用して属性を表示する手順は、次のとおりです。

1. ナビゲータ・ペインで、「Oracle Internet Directory サーバー」 > 「*directory server instance*」の順に展開し、「スキーマの管理」を選択します。
2. 右側のペインで「属性」タブを選択します。このタブ・ページには、属性プロパティを含む表が表示されます。次に、「属性」タブ・ページに表示される表の各列の説明を示します。

列	説明
名前	属性の標準化タイプ名。
索引付け	属性が索引付けされているかどうかを示すチェックボックス。
オブジェクト ID	各属性の標準化オブジェクト識別子。
説明	様々な属性を説明する語。
構文	データ・エントリに関して各属性の型に適用される標準化規則。
サイズ	各オブジェクトの最大サイズ。
使用方法	属性の使用方法を指定する規格。userApplications、directoryOperation、distributedOperationおよび dSAOperation という 4 つのオプションがあります。
順序	値に対して設定される優先順位を指定する規格。
等価	比較と検索操作における等価の判断方法を指定する規格。
サブストリング	正規表現の一致に使用されます。
単一値	この属性の型の値が最大 1 つであることを示します。
スーパー	各属性のスーパー属性。

関連項目： 特定のエントリの属性を表示する方法は、7-5 ページの「[Oracle Directory Manager を使用した特定エントリの属性の表示](#)」を参照してください。

Oracle Directory Manager を使用した属性の検索

Oracle Directory Manager を使用して属性を検索する手順は、次のとおりです。

1. ナビゲータ・ペインで「スキーマの管理」を選択します。「スキーマの管理」タブ・ページが、右側のペインに表示されます。
2. 「属性」タブ・ページを選択します。
3. 右下隅の「属性の検索」ボタンをクリックします。「検索：属性」ダイアログ・ボックスが表示されます。
4. 検索基準バーの一番左のメニューから、検索する属性のプロパティを選択します。オプションは次のとおりです。

フィールド	説明
名前	検索する属性の名前。
索引付け	索引付き属性のリスト。
オブジェクト ID	検索する属性のオブジェクト識別子。たとえば、「オブジェクト ID」「次の文字で始まる」「2.5.2」と指定すると、オブジェクト ID が 2.5.2 で始まる属性のリストが表示されます。
説明	属性の説明列に記述されている語。
構文	データ・エントリに関してこの属性の型に適用される標準化規則。この規則を使用して、特定の構文を使用している属性の検索範囲を絞り込むことができます。
サイズ	このオブジェクトの最大サイズ。
使用方法	属性の使用方法を指定する規格。userApplications、directoryOperation、distributedOperation および dSAOperation のいずれか 1 つを入力して、検索範囲を絞り込みます。
順序	値に対して設定される優先順位を指定する規格。
等価	比較と検索操作における等価の判断方法を指定する規格。
サブストリング	正規表現の一致に使用されます。
単一値	この属性の型の値が最大 1 つであることを示します。
スーパー	検索する属性のスーパー属性。

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

オプション	説明
開始	プロパティの値の始めの数文字のみを使用して検索します。たとえば、「構文」「次の文字で始まる」「1.3」と指定すると、構文識別子が 1.3 で始まるすべての属性のリストが表示されます。
終了	プロパティの値の終わりの数文字のみを使用して検索します。たとえば、「名前」「終了」「License」と指定すると、carLicense など、License で終わるすべての属性のリストが表示されます。
含む	入力した値を含んだプロパティを持つ属性を検索します。たとえば、「順序」「含む」「time」と指定すると、「順序」列に time という語を含むすべての属性のリストが表示されます。
完全一致	指定した属性プロパティ内の値に完全に一致する値を検索します。たとえば、「等価」「完全一致」「caseIgnoreMatch」と指定すると、caseIgnoreMatch 一致規則を持つすべての属性のリストが表示されます。
以上	数値順またはアルファベット順でユーザーの入力値より大か等しいプロパティを持つ属性を検索します。たとえば、「名前」「以上」「orcl」と指定すると、orcl で始まる属性からアルファベットの最後の文字で始まる属性までのリストが表示されます。
以下	数値順またはアルファベット順でユーザーの入力値以下のプロパティを持つ属性を検索します。たとえば、「名前」「以下」「orcl」と指定すると、orcl で始まる属性からアルファベットの最初の文字で始まる属性までのリストが表示されます。
「存在」	選択した属性プロパティが存在しているすべての属性を検索します。たとえば、「説明」「存在」と指定すると、「説明」フィールドにテキストがあるすべての属性のリストが表示されます。

6. 検索基準バーの一番右のテキスト・ボックスに、検索する属性の値または値の一部を入力します。たとえば、名前が orcl で始まる属性をすべて検索するには、検索基準バーの一番右のテキスト・ボックスにこの文字を入力して、「名前」「次の文字で始まる」「orcl」という句を作成します。

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

ボタン	説明
新規作成	「検索基準」フィールドに、新しい検索基準バーを作成します。このボタンは、「検索基準」フィールドに何も表示されていないときのみ使用可能です。
AND	「検索基準」フィールドに、別の検索基準バーを作成します。指定した 2 つのプロパティが両方ある属性をすべて検索します。
OR	「検索基準」フィールドに、別の検索基準バーを作成します。指定した 2 つのプロパティのいずれかを持つ属性をすべて検索します。
NOT	選択した検索基準バーの基準を除外し、指定したプロパティがない属性をすべて検索します。
削除	選択した検索基準バーを削除します。

8. 「検索」をクリックします。検索結果が、「検索 : 属性」ダイアログ・ボックスの下部のウィンドウに表示されます。

Oracle Directory Manager を使用した属性の追加

新しい属性の作成や既存の属性からのコピーが可能です。

ヒント： 等価、構文および一致規則は数が多く複雑であるため、これらの特性は、類似の既存属性からコピーすると作業が簡単になります。

Oracle Directory Manager を使用した新規属性の追加

新規属性を追加する手順は、次のとおりです。

- ナビゲータ・ペインで、「Oracle Internet Directory サーバー」 > 「ディレクトリ・サーバー」の順に展開し、「スキーマの管理」を選択します。
- 次のいずれか 1 つを行います。
 - 右側のペインで「属性」タブを選択し、ツールバーの「作成」ボタンをクリック。
 - 右側のペインで「属性」タブを選択し、「属性」タブ・ページの下の「作成」ボタンをクリック。
 - 「操作」メニューから、「属性の作成」を選択。「新規属性の型」ダイアログ・ボックスが表示されます。そこには、「一般」と「拡張」の 2 つのタブ・ページがあります。これらの各フィールドでは、値を入力するかまたはメニューから選択します。

3. 次の表の説明に従って、「一般」タブの各フィールドに値を入力します。

フィールド	説明
名前	この属性の名前を入力します。
オブジェクト ID	この属性のオブジェクト ID を入力します。オブジェクト ID は、IETF 規格に基づいた、標準化された数値順序です。値は一意であることが必要です。通常この値は、ANSI または ISO など、登録機関によって割り当てられた ID から導出されます。 標準識別子の説明は、現行の LDAP 規格を参照してください。LDAP 規格は IETF の Web サイトで参照できます。
説明	説明を記述するオプションのフィールドです。
構文	データ・エントリに関してこの属性の型に適用される標準化規則を入力します。
サイズ	このオブジェクトの最大サイズを入力します。
単一値	このチェックボックスを選択すると、この属性の型の値が最大 1 つであることを指定できます。

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

フィールド	説明
索引付け	このフィールドを選択するとこの属性が索引に追加され、検索で使用できるようになります。等価の一致規則を持つ属性のみが索引付けできます。
使用方法	属性の使用方法を指定する規格を指定します。オプションは次のとおりです。 <ul style="list-style-type: none"> ■ <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>） ■ <code>directoryOperation</code> ディレクトリ・サーバーによって値が入力される属性（例: <code>creatorName</code> または <code>timeStamp</code>） ■ <code>distributedOperation</code> ■ <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>）
順序	値に対して設定される優先順位を指定する規格を指定します。
等価	比較と検索操作における等価の判断方法を指定する規格を指定します。
サブストリング	一致する正規表現を指定します。

フィールド	説明
スーパー	この属性のスーパー属性を追加します。この手順は、次のとおりです。 <ol style="list-style-type: none">このフィールドの横の「追加」ボタンをクリックします。「スーパー属性セクタ」が表示されます。追加するスーパー属性を選択して、「選択」をクリックします。必要に応じてこの処理を繰り返します。 「スーパー」フィールドからスーパー属性を削除するには、削除する属性を選択して、「削除」をクリックします。

5. 「OK」をクリックします。

注意： この属性を使用するには、オブジェクト・クラスに対する属性セットの一部であることを必ず宣言してください。宣言は、ナビゲータ・ペインで「スキーマの管理」を選択した後、右側のペインで「オブジェクト・クラス」タブ・ページを選択して行います。詳細は、6-4 ページの「[オブジェクト・クラスの変更のガイドライン](#)」を参照してください。

Oracle Directory Manager を使用した既存の属性からの新規属性の作成

既存属性を利用して属性を追加する手順は、次のとおりです。

- ナビゲータ・ペインで「スキーマの管理」を選択します。
- 右側のペインで「属性」タブを選択します。
- 「属性」タブ・ページで、コピーする属性を選択します。
- 右側のペインの下「類似項目の作成」ボタンをクリックします。その属性の「新規属性の型」ダイアログ・ボックスが表示されます。このダイアログ・ボックスには、「一般」と「拡張」の2つのタブ・ページがあります。これらの各フィールドには値を直接入力するか、メニューから値を選択します。
- 「一般」タブを選択し、次の表の説明に従って各フィールドに値を入力します。識別名は、新規属性の識別名に必ず変更する必要があります。

フィールド	説明
名前	この属性の名前を入力します。
オブジェクト ID	この属性のオブジェクト ID を入力します。オブジェクト ID は、IETF 規格に基づいた、標準化された数値順序です。値は一意であることが必要です。通常この値は、ANSI または ISO など、登録機関によって割り当てられた ID から導出されます。 標準識別子の説明は、現行の LDAP 規格を参照してください。LDAP 規格は IETF の Web サイトで参照できます。
説明	説明を記述するオプションのフィールドです。
構文	データ・エントリに関してこの属性の型に適用される標準化規則を入力します。
サイズ	このオブジェクトの最大サイズを入力します。
単一値	このチェックボックスを選択すると、この属性の型の値が最大 1 つであることを指定できます。

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

フィールド	説明
索引付け	このフィールドを選択するとこの属性が索引に追加され、検索でできるようになります。等価の一致規則を持つ属性のみが索引付けできます。
使用方法	属性の使用方法を指定する規格を指定します。オプションは次のとおりです。 <ul style="list-style-type: none"> ■ <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>） ■ <code>directoryOperation</code> ディレクトリ・サーバーによって値が入力される属性（例：<code>creatorName</code> または <code>timeStamp</code>） ■ <code>distributedOperation</code> ■ <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>）
順序	値に対して設定される優先順位を指定する規格を指定します。
等価	比較と検索操作における等価の判断方法を指定する規格を指定します。
サブストリング	一致する正規表現を指定します。

フィールド	説明
スーパー	この属性のスーパー属性を追加します。この手順は、次のとおりです。 <ol style="list-style-type: none">このフィールドの横の「追加」ボタンをクリックします。「スーパー属性セレクト」が表示されます。追加するスーパー属性を選択して、「選択」をクリックします。必要に応じてこの処理を繰り返します。 「スーパー」フィールドからスーパー属性を削除するには、削除する属性を選択して、「削除」をクリックします。

7. 「OK」をクリックします。

Oracle Directory Manager を使用した属性の変更

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

- ナビゲータ・ペインで「スキーマの管理」を選択します。
- 右側のペインで「属性」タブを選択して、リストの中から編集可能な属性を選択します。
- 「編集」をクリックします。「属性」ダイアログ・ボックスには、「一般」と「拡張」の2つのタブ・ページが表示されます。これらの各フィールドには値を直接入力するか、メニューから値を選択します。
- 「一般」タブを選択し、次の表の説明に従って各フィールドに値を入力します。

フィールド	説明
名前	この属性の名前を入力します。
オブジェクト ID	この属性のオブジェクト ID を入力します。オブジェクト ID は、IETF 規格に基づいた、標準化された数値順序です。値は一意であることが必要です。通常この値は、ANSI または ISO など、登録機関によって割り当てられた ID から導出されます。 標準識別子の説明は、現行の LDAP 規格を参照してください。LDAP 規格は IETF の Web サイトで参照できます。
説明	説明を記述するオプションのフィールドです。
構文	データ・エントリに関してこの属性の型に適用される標準化規則を入力します。
サイズ	このオブジェクトの最大サイズを入力します。
単一値	このチェックボックスを選択すると、この属性の型の値が最大 1 つであることを指定できます。

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

フィールド	説明
索引付け	このフィールドを選択するとこの属性が索引に追加され、検索で使用できるようになります。等価の一致規則を持つ属性のみが索引付けできます。
使用方法	属性の使用方法を指定する規格を指定します。オプションは次のとおりです。 <ul style="list-style-type: none"> ■ <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>） ■ <code>directoryOperation</code> ディレクトリ・サーバーによって値が入力される属性（例：<code>creatorName</code> または <code>timeStamp</code>） ■ <code>distributedOperation</code> ■ <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>）
順序	値に対して設定される優先順位を指定する規格を指定します。
等価	比較と検索操作における等価の判断方法を指定する規格を指定します。
サブストリング	一致する正規表現を指定します。
スーパー	この属性のスーパー属性を追加します。この手順は、次のとおりです。 <ol style="list-style-type: none"> 1. このフィールドの横の「追加」ボタンをクリックします。「スーパー属性セレクタ」が表示されます。 2. 追加するスーパー属性を選択して、「選択」をクリックします。 3. 必要に応じてこの処理を繰り返します。 「スーパー」フィールドからスーパー属性を削除するには、削除する属性を選択して、「削除」をクリックします。

6. 「OK」をクリックします。

Oracle Directory Manager を使用した属性の削除

注意： 削除できるのはユーザー定義属性のみです。ベース・スキーマの属性は削除しないでください。

属性を削除する方法は次のとおりです。

1. ナビゲータ・ペインで「スキーマの管理」を選択します。
2. 右側のペインで「属性」タブを選択して、リストの中から編集可能な属性を選択します。
3. 「削除」をクリックします。

Oracle Directory Manager を使用した属性の索引付け

Oracle Internet Directory は、索引を使用して属性を検索できるようにしています。Oracle Internet Directory のインストール時に、特定の属性はすでに索引付けされています。その他の属性を検索フィルタで使用する場合は、使用する属性に索引を付ける必要があります。

注意： Oracle Directory Manager では、属性の作成時にのみ索引を付けることができます。Oracle Directory Manager を使用して、既存の属性に索引を付けることはできません。既存の属性に索引を付けるには、6-29 ページの「[コマンドライン・ツールを使用した属性の索引付け](#)」で説明されているカタログ管理ツールを使用します。

次の条件を満たす属性のみ索引を付けることができます。

- 等価の一致規則を持つ
 - C-10 ページの「[一致規則](#)」にリストされているように、Oracle Internet Directory でサポートされる一致規則を持つ
 - 属性の名前が 28 文字以下
-

Oracle Directory Manager を使用した索引付き属性の表示

索引付き属性を表示する手順は、次のとおりです。

1. ナビゲータ・ペインで「スキーマの管理」を選択します。
2. 右側のペインで「属性」タブを選択します。「属性」タブに、スキーマ内のすべての属性が表示されます。「索引付け」列のチェックボックスが選択されている場合は、索引付き属性であることを示しています。

Oracle Directory Manager を使用した属性への索引の追加

6-20 ページの「[Oracle Directory Manager を使用した属性の追加](#)」の説明にあるように属性を作成する場合は、「新規属性の型」ダイアログ・ボックスを使用します。そのダイアログ・ボックスの「拡張」タブ・ページで、「索引付け」チェックボックスを選択してください。

Oracle Directory Manager を使用した属性からの索引の削除

属性から索引を削除する手順は、次のとおりです。

1. ナビゲータ・ペインで「スキーマの管理」を選択します。
2. 右側のペインで「属性」タブを選択します。
3. 索引付き属性を選択します。選択する属性は編集可能である必要があります。編集可能かどうかは、属性名の左にアイコンで示されています。
4. 「索引の削除」をクリックします。

コマンドライン・ツールを使用した属性の管理

この項では、コマンドライン・ツールを使用した属性の追加、変更および索引付けについて説明します。この項では、次の項目について説明します。

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

ldapmodify を使用した属性の追加と変更

ldapmodify コマンドを使用して新規属性をスキーマに追加するには、コマンド・プロンプトで次のようなコマンドを入力します。

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

LDIF ファイルには、次のようなデータが含まれています。

```
dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: ( 1.2.3.4.5 NAME 'myattr' SYNTAX
                  '1.3.6.1.4.1.1466.115.121.1.38' )
```

Oracle Directory Manager または ldapsearch コマンドライン・ツールを使用して、指定した構文のオブジェクト ID を検索できます。

関連項目：

- `ldapmodify` とそのオプションの詳細は、A-15 ページの「[ldapmodify の構文](#)」を参照してください。
- Oracle Directory Manager または `ldapsearch` を使用した構文の表示方法は、6-31 ページの「[構文の表示](#)」を参照してください。

ldapmodify を使用した属性の削除

注意： 削除できるのはユーザー定義属性のみです。ベース・スキーマの属性は削除しないでください。

`ldapmodify` を使用して属性を削除するには、システム・プロンプトで次のようなコマンドを入力します。

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

LDIF ファイルには、次のようなデータが含まれています。

```
dn: cn=subschemasubentry
changetype: modify
delete: attributetypes
attributetypes: ( 1.2.3.4.5 NAME 'myattr' SYNTAX
                  '1.3.6.1.4.1.1466.115.121.1.38' )
```

Oracle Directory Manager または `ldapsearch` コマンドライン・ツールを使用して、指定した構文のオブジェクト ID を検索できます。

関連項目：

- `ldapmodify` とそのオプションの詳細は、A-15 ページの「[ldapmodify の構文](#)」を参照してください。
- Oracle Directory Manager または `ldapsearch` を使用した構文の表示方法は、6-31 ページの「[構文の表示](#)」を参照してください。

コマンドライン・ツールを使用した属性の索引付け

Oracle Internet Directory は、索引を使用して属性を検索できるようにしています。Oracle Internet Directory のインストール時に、エントリ cn=catalogs に、検索で使用できる属性がリストされます。

その他の属性を検索フィルタで使用する場合は、使用する属性をカタログ・エントリに追加する必要があります。次の条件を満たす属性のみ索引を付けることができます。

- 等価の一致規則を持つ
- C-10 ページの「[一致規則](#)」にリストされているように、Oracle Internet Directory でサポートされる一致規則を持つ
- 属性の名前が 28 文字以下

新しい属性（ディレクトリにデータが存在していない属性）に、ldapmodify を使用して索引を付けることができます。ディレクトリにデータがすでに存在している属性に索引を付けるには、カタログ管理ツールを使用します。属性から索引を削除するには、ldapmodify を使用することもできますが、オラクル社ではカタログ管理ツールを使用することをお勧めします。

ldapmodify を使用した、データが存在していない属性の索引付け

スキーマに新規属性を定義した後、ldapmodify を使用してその属性をカタログ・エントリに追加できます。

ディレクトリ・データが存在していない属性に ldapmodify を使用して索引を付けるには、ldapmodify で LDIF ファイルをインポートします。たとえば、すでにスキーマに定義されている属性 foo に索引を付けるには、ldapmodify で次の LDIF ファイルをインポートします。

```
dn: cn=catalogs
changetype: modify
add: orclindexedattribute
orclindexedattribute: foo
```

この方法は、ディレクトリにデータが存在している属性に索引を付ける場合には使用しないでください。データが存在している属性に索引を付けるには、カタログ管理ツールを使用します。

ldapmodify を使用した属性からの索引の削除

ldapmodify を使用して属性から索引を削除するには、LDIF ファイルで delete を指定します。たとえば、次のようにします。

```
dn: cn=catalogs
changetype: modify
delete: orclindexedattribute
orclindexedattribute: foo
```

関連項目： A-15 ページの「[ldapmodify の構文](#)」

カタログ管理ツールを使用した、データが存在している属性の索引付け
データがすでに存在している属性に対する索引付けおよび属性からの索引の削除には、カタログ管理ツールを使用します。

関連項目： A-39 ページの「[カタログ管理ツールの構文](#)」

注意： Oracle Internet Directory でインストールされたベース・スキーマによって作成された索引ではないことが確信できない場合は、`catalog.sh -delete` オプションを使用して属性の索引を削除しないでください。ベース・スキーマ属性から索引を削除すると、Oracle Internet Directory の操作に悪影響を及ぼす場合があります。

一致規則の表示

この項では、次の項目について説明します。

- [Oracle Directory Manager を使用した一致規則の表示](#)
- [ldapsearch を使用した一致規則の表示](#)

注意： 一致規則は変更できません。

Oracle Directory Manager を使用した一致規則の表示

1. ナビゲータ・ペインで、「Oracle Internet Directory サーバー」 > 「*directory server instance*」の順に展開し、「スキーマの管理」を選択します。
2. 右側のペインで「一致規則」タブを選択します。このタブ・ページのフィールドは列見出しとして表示されます。これには次のようなものがあります。

列見出し	意味
名前	属性一致規則の名前
オブジェクト ID	この一致規則の一意な識別子
説明	一致規則を説明する語（オプション）
構文	この一致規則に使用される構文

ldapsearch を使用した一致規則の表示

サブエントリ cn=subSchemaSubentry で ldapsearch を使用します。

関連項目： A-22 ページの「[ldapsearch の構文](#)」

構文の表示

この項では、次の項目について説明します。

- [Oracle Directory Manager を使用した構文の表示](#)
- [ldapsearch を使用した構文の表示](#)

注意： 構文は変更できません。

Oracle Directory Manager を使用した構文の表示

Oracle Directory Manager を使用して構文を表示する手順は、次のとおりです。

1. ナビゲータ・ペインで「スキーマの管理」を選択します。
2. 右側のペインで「構文」タブを選択します。このタブ・ページのフィールドは列見出しとして表示されます。これには次のようなものがあります。
 - 説明：属性構文の名前
 - オブジェクト ID: この構文の一意な識別子

ldapsearch を使用した構文の表示

サブエントリ cn=subSchemaSubentry で ldapsearch を使用します。

関連項目： A-22 ページの「[ldapsearch の構文](#)」

ディレクトリ・エントリの管理

この章では、エントリを表示、追加、変更および削除する方法について説明します。

この章では、次の項目について説明します。

- [Oracle Directory Manager](#) を使用したエントリの管理
- コマンドライン・ツールを使用したエントリの管理
- バルク・ツールを使用したエントリの管理
- ナレッジ参照と参照の管理

関連項目： ディレクトリ・エントリ、ディレクトリ情報ツリー、識別名および相対識別名の概要は、[第2章「概念およびアーキテクチャ」](#)を参照してください。

Oracle Directory Manager を使用したエントリの管理

この項では、次の項目について説明します。

- [Oracle Directory Manager を使用したエントリの検索](#)
- [Oracle Directory Manager を使用した特定エントリの属性の表示](#)
- [Oracle Directory Manager を使用したエントリの追加](#)
- [Oracle Directory Manager を使用したエントリの変更](#)
- [Oracle Directory Manager を使用した属性オプション付きエントリの管理](#)

Oracle Directory Manager を使用したエントリの検索

すべてのエントリの表示にはナビゲータ・ペインを、1 つ以上の特定のエントリの検索には Oracle Directory Manager の検索機能を使用できます。

ナビゲータ・ペインにエントリを表示するには、「Oracle Internet Directory サーバー」>「*directory server instance*」>「エントリ管理」の順に展開して、そのサブツリーを表示します。

ツリーのルートが最初にリストされ、次に第 2 レベル、第 3 レベルというように、左から右へ移動してリストされます。サブツリーには、各エントリの **RDN** が階層順にリストされます。サブツリー内の下位レベルのエントリを表示するには、親エントリの横のプラス記号 (+) をクリックします。

ディレクトリ・エントリを検索する手順は、次のとおりです。

1. ナビゲータ・ペインで、「Oracle Internet Directory サーバー」>「*directory server instance*」の順に展開します。右側のペインに「検索」フィールドが表示されます。
2. 「検索のルート」フィールドに、検索のルートの **DN** を入力します。

たとえば、Americas にある IMC 組織の Manufacturing 部門に勤務する従業員を検索するとします。検索のルートの識別名は、次のようになります。

```
ou=Manufacturing,ou=Americas,o=IMC,c=US
```

この識別名を「検索のルート」テキスト・ボックスに入力します。

[ディレクトリ情報ツリー](#)を参照して検索のルートを選択することもできます。この手順は、次のとおりです。

- a. 「検索のルート」フィールドの右側の「参照」をクリックします。「識別名 (DN) パスの選択 : ツリー・ビュー」ダイアログ・ボックスが表示されます。
- b. 「ツリー・ビュー」の横のプラス記号 (+) をクリックして、そのエントリを表示します。
- c. 検索のルートのレベルを表すエントリまで、ナビゲートします。

- d. そのエントリを選択して、「OK」をクリックします。検索のルートの識別名が、右側のペインの「検索のルート」テキスト・ボックスに表示されます。
3. 「最大結果件数」ボックスに、検索で取り出すエントリの最大数を入力します。デフォルトは 200 です。ここで設定できるディレクトリ・サーバーのエントリ数は、最大 1000 です。
4. 「最長検索時間」ボックスに、検索の最大時間を秒数で入力します。ここで入力する値は、少なくともデフォルト値の 25 以上にする必要があります。ここで指定できるディレクトリ・サーバーの最大検索時間は、1 時間です。
5. 「検索の深さ」のリストで、検索するディレクトリ情報ツリーのレベルを選択します。オプションは次のとおりです。
 - ベース: 特定のディレクトリ・エントリを取り出します。この検索レベルの場合は、検索基準バーを使用して、属性 `objectClass` とフィルタ「存在」を選択します。
 - 1 レベル: 検索のルートの 1 レベル下のすべてのエントリに検索を制限します。
 - サブツリー: 検索のルートを含め、サブツリー全体のエントリを検索します。
6. 「検索基準」ボックスで、検索基準バーのリストとテキスト・フィールドを使用して、検索基準をさらに詳細に指定します。
 - a. 検索基準バーの一番左のリストから、検索するエントリの属性を選択します。各エントリですべての属性が使用されているわけではないため、指定した属性が、検索しているエントリの属性に実際に一致していることを確認する必要があります。一致する属性がない場合は、検索に失敗します。
 - b. 検索基準バーの中央のリストから、フィルタを選択します。オプションは次のとおりです。

フィルタ	説明
開始	属性の値の始めの数文字のみを使用して検索します。たとえば、「cn」「次の文字で始まる」「Fran」と指定すると、cn 属性が Fran で始まるすべてのエントリが取り出されます。この場合は、Frank、Fran、Frances、Franklin などが取り出されます。
終了	指定した属性の値の終わりの数文字のみを使用してエントリを検索します。たとえば、「cn」「終了」「son」と指定すると、Baldisson、Jacobson、Johnson などが取り出されます。
含む	値の位置を限定せずに、ユーザーの入力値が指定した属性に含まれているエントリを検索します。たとえば、「cn」「含む」「Wins」と指定すると、cn 属性に wins を含むエントリがすべて取り出されます。この場合は、Winslow、Czerwinski、Winship などが取り出されます。

フィルタ	説明
完全一致	指定した属性がユーザーの入力値に一致するエントリを検索します。たとえば、「cn」「完全に一致する」「Franklin Baldwins」と指定すると、cn 属性の値が Franklin Baldwins のエントリがすべて取り出されます。
以上	指定した属性が、数値順またはアルファベット順で入力値より大か等しいエントリを検索します。たとえば、「cn」「以上」「Frank」と指定すると、cn 属性の範囲が、Frank からアルファベットの最後の文字までのエントリがすべて取り出されます。
以下	指定した属性が、数値順またはアルファベット順で入力値より小か等しいエントリを検索します。たとえば、「cn」「以下」「Frank」と指定すると、Frank からアルファベットの最初の文字までの cn 属性がすべて取り出されます。
存在	指定した属性を持つエントリが、ツリーのそのレベルに存在するかどうかを判断します。この関連の使用に値の入力は不要です。「cn」「存在」と指定すると、ツリーのそのレベルで、cn 属性を持つエントリがすべて取り出されます。

- c.

検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。たとえば、選択した属性が cn の場合は、検索する個々の一般名を入力します。
7.

検索をさらに詳細に指定するには、「検索基準」ボックスのボタンを使用して検索基準バーを拡張します。

ボタン	説明
新規作成	「検索基準」フィールドに、新しい検索基準バーを作成します。このボタンは、「検索基準」フィールドに何も表示されていないときのみ使用可能です。
AND	「検索基準」フィールドに、別の検索基準バーを作成します。指定した両方の属性を持つエントリをすべて検索します。たとえば、cn=Baldwins And title=Laborer と指定すると、cn が Baldwins で、かつ title が laborer のエントリがすべて取り出されます。
OR	「検索基準」フィールドに、別の検索基準バーを作成します。指定した属性のいずれかを持つエントリをすべて検索します。たとえば、title=Laborer Or title=Foreman と指定すると、title が laborer または foreman の従業員がすべて取り出されます。
NOT	選択した検索基準バーの基準を除外し、指定した基準を満たさないエントリをすべて取り出します。たとえば、cn=Frank Not title=Laborer と指定すると、cn が Frank で、title が laborer ではない個人がすべて取り出されます。
削除	選択した検索基準バーを削除します。

ボタン	説明
拡張	<p>検索に属性オプションを含ませる場合に、検索基準バーを追加します。この場合は次の構文を使用します。attribute;attribute_option filter attribute_option_value</p> <p>たとえば、cn;lang_sp=J* と指定すると、文字 J で始まる cn;lang_sp= の属性オプション値をすべて取り出します。</p> <p>注意：属性オプション値を検索に使用するには、その属性オプションの親属性が索引付けされている必要があります。たとえば、属性オプション carLicense;lang_sp を検索に使用するには、carLicense 属性が索引付けされている必要があります。</p> <p>関連項目：</p> <ul style="list-style-type: none">■ 6-26 ページの「Oracle Directory Manager を使用した属性の索引付け」■ 6-29 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」

8. 「検索」をクリックします。検索結果は「識別名」ボックスに表示されます。

関連項目： 検索で表示するエントリ数と検索の制限時間の設定方法は、5-21 ページの「[検索の構成](#)」を参照してください。

Oracle Directory Manager を使用した特定エントリの属性の表示

検索結果の表示後、属性を参照するエントリをクリックします。「エントリ」ダイアログ・ボックスに、そのエントリの属性が表示されます。

一部の属性は、識別名である可能性もあります。たとえば、指定した従業員の 1 つの属性がその従業員のマネージャで、そのマネージャに識別名がある場合があります。この場合、従業員の「エントリ」ダイアログ・ボックスを表示すると、「マネージャ」テキスト・ボックスの横に「参照」ボタンが表示されます。そのマネージャの情報を検索するには、「参照」をクリックして「ディレクトリ:エントリ管理」ダイアログ・ボックスを表示し、7-2 ページの「[Oracle Directory Manager を使用したエントリの検索](#)」の手順に従って検索してください。

関連項目： ディレクトリの属性をすべて表示する方法は、6-17 ページの「[Oracle Directory Manager を使用したすべてのディレクトリ属性の表示](#)」を参照してください。

Oracle Directory Manager を使用したエントリの追加

この項では、個々のエントリおよびグループ・エントリを追加する方法を説明します。

注意： エントリを追加または削除する場合、Oracle ディレクトリ・サーバーではエントリ属性値の構文検証は行われません。

Oracle Directory Manager を使用した新規エントリの追加

Oracle Directory Manager でエントリを追加または削除するには、親エントリに対する書込みアクセス権限があり、新規エントリの識別名を認識している必要があります。

新規エントリを追加する手順は、次のとおりです。

1. 「Oracle Internet Directory サーバー」 > 「*directory server instance*」の順に展開し、「エントリ管理」を選択します。
2. ツールバーの「作成」ボタンをクリックします。「新規エントリ」ダイアログ・ボックスが表示されます。
3. 「識別名」フィールドに、完全な識別名を入力します。「参照」をクリックして、追加するエントリの親の識別名の位置を識別して選択することもできます。選択したエントリが「識別名」フィールドに表示されます。その親の識別名の左に新規エントリの相対識別名を入力し、その後にカンマを付けます。
4. 新規エントリの**オブジェクト・クラス**を指定するには、「オブジェクト・クラス」ボックスの横の「追加」をクリックします。「スーパー・クラス・セレクトア」ダイアログ・ボックスが表示されます。
5. 「スーパー・クラス・セレクトア」ダイアログ・ボックスでオブジェクト・クラスを選択して、「選択」をクリックします。オブジェクト・クラス・リストからオブジェクト・クラスを選択すると、「新規エントリ」ダイアログ・ボックスの下半分のタブ・ページにあるウィンドウに、必須属性とオプション属性が表示されます。必須属性のフィールドには、値を入力する必要があります。オプション属性のフィールドには、値を必ずしも入力する必要はありません。
6. オブジェクト・クラスを選択して、対応する属性に値を入力した後、「OK」をクリックします。

Oracle Directory Manager の既存エントリを利用したエントリの追加

Oracle Directory Manager では、既存エントリをコピーしてその識別名を変更する方法で、新規エントリを作成できます。この操作を行う場合は、名前やアドレスなどの属性も、新規識別名に対応するように変更してください。エントリを追加するには、その親に対する書込みアクセス権限が必要です。

ヒント： 検索ペインで他の類似エントリを参照して、新規識別名用のテンプレートを検索できます。

既存エントリを利用してエントリを追加する手順は、次のとおりです。

1. ナビゲータ・ペインで、「Oracle Internet Directory サーバー」 > 「*directory server instance*」の順に展開し、「エントリ管理」を選択します。右側のペインに「検索」インタフェースが表示されます。このペインで、テンプレートとして使用するエントリを検索します。
2. 取り出したエントリから、テンプレートとして使用するエントリをダブルクリックします。そのエントリに対応する「エントリ」ダイアログ・ボックスが表示されます。
3. 「エントリ」ダイアログ・ボックスで、「類似項目の作成」をクリックします。「新規エントリ : 類似項目の作成」ダイアログ・ボックスが表示されます。
4. このエントリを作成するエントリに調整するために、重要なフィールドを変更します。この操作で、識別名と一般名は必ず変更する必要があります。変更しないと、新規エントリのデータは保存されません。たとえば、Henri Latour のエントリをテンプレートとして使用して Henri Latrobe のエントリを作成する場合は、識別名の `cn=Henri Latour` を `cn=Henri Latrobe` に変更する必要があります。また、この他にも従業員番号や電話番号など、一意であることが必要な属性をすべて変更する必要があります。
5. 「OK」をクリックして、変更内容を保存します。

関連項目： フィールドに情報を追加する方法は、このダイアログ・ボックスのオンライン・ヘルプを参照してください。

例 : Oracle Directory Manager を使用したユーザー・エントリの追加

この例では、Anne Smith というユーザーを作成し、パスワードを割り当てます。

1. administrator でログインします。
2. 「Oracle Internet Directory サーバー」 > 「*directory server instance*」の順に展開し、「エントリ管理」を選択します。
3. ツールバーの「作成」ボタンをクリックします。「新規エントリ」ダイアログ・ボックスが表示されます。
4. 「識別名」フィールドに、完全な識別名を入力します。「参照」ボタンをクリックして、このエントリの親の識別名を探し、親の識別名の左に相対識別名、つまり `cn=Anne Smith` を入力して、その後にカンマを付けることもできます。
5. 「オブジェクト・クラス」ボックスの右側の「追加」をクリックします。「スーパー・クラス・セレクト」ダイアログ・ボックスが表示されます。
6. 「スーパー・クラス・セレクト」ダイアログ・ボックスで `person` オブジェクト・クラスを選択して、「選択」をクリックします。「新規エントリ」ダイアログ・ボックスに戻ります。

7. 「新規エントリ」ダイアログ・ボックスで「オプション・プロパティ」タブをクリックし、「userPassword」ウィンドウまでスクロールします。
8. Anne Smith 用のパスワードを入力します。

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

グループ・エントリは、エントリのリスト（例：電子メール・リスト）を含むエントリです。グループ・エントリは、オブジェクト・クラス `orclPrivilegeGroup` をサブクラスとして持つ、`groupOfNames` または `groupOfUniqueNames` オブジェクト・クラスのいずれかと関連付けられます。

エントリが `groupOfNames` オブジェクト・クラスに属している場合は複数値の属性 `member` に、`groupOfUniqueNames` オブジェクト・クラスに属している場合は属性 `uniqueMember` に識別名を追加して、グループのメンバーシップを決定します。

グループ・エントリを追加する手順は、次のとおりです。

1. 「Oracle Internet Directory サーバー」>「*directory server instance*」の順に展開し、「エントリ管理」を選択します。
2. ツールバーの「作成」ボタンをクリックします。「新規エントリ」ダイアログ・ボックスが表示されます。
3. 「識別名」フィールドに、完全な識別名を入力します。「参照」ボタンを使用して、追加するエントリの親の識別名を探し、親の識別名の左に新規エントリの相対識別名を入力して、その後にカンマを付けることもできます。
4. 新規エントリに使用するオブジェクト・クラスを指定するには、「オブジェクト・クラス」ボックスの右の「追加」をクリックします。「スーパー・クラス・セレクト」ダイアログ・ボックスが表示されます。
5. 「スーパー・クラス・セレクト」ダイアログ・ボックスで、`top` オブジェクト・クラスを選択し、「選択」ボタンをクリックします。「新規エントリ」ダイアログ・ボックスの「オブジェクト・クラス」ボックスに、`top` オブジェクト・クラスが表示されます。
6. 同様に、次の手順を実行します。
 - a. 「オブジェクト・クラス」ボックスの右の「追加」をクリックします。
 - b. 「スーパー・クラス・セレクト」ダイアログ・ボックスから、「`groupOfNames`」または「`groupOfUniqueNames`」オブジェクト・クラスを選択します。
 - c. 「選択」をクリックします。「新規エントリ」ダイアログ・ボックスの「オブジェクト・クラス」ウィンドウに、選択したオブジェクト・クラスが表示されます。

7. グループ・エントリの必須属性とオプション属性を入力します。

「groupOfNames」オブジェクト・クラスを選択した場合は、いくつかのフィールド、たとえば「必須プロパティ」タブ・ページの「メンバー」フィールドの横に、「参照」ボタンが表示されます。ブラウズによって必須プロパティを入力する手順は、次のとおりです。

- a. 「参照」をクリックします。「ディレクトリ:エントリ管理」ダイアログ・ボックスが表示されます。
- b. このダイアログ・ボックスを使用して、リストに追加する特定のエントリを検索します。
- c. 「ディレクトリ:エントリ管理」ダイアログ・ボックスの「識別名」ウィンドウで、エントリを選択して「OK」をクリックします。「新規エントリ」ダイアログ・ボックスに戻ります。選択したエントリが、「メンバー」ウィンドウのリストに追加されています。

8. 「OK」をクリックします。

関連項目：

- 検索ペインの使用法は、7-2 ページの「[Oracle Directory Manager を使用したエントリの検索](#)」を参照してください。
- グループ・エントリのアクセス制御ポリシー・ポイントの設定方法は、13-3 ページの「[アクセス制御グループ](#)」を参照してください。
- アクセス権限の詳細は、2-13 ページの「[グローバル化・サポート](#)」および第 13 章「[ディレクトリ・アクセス制御](#)」を参照してください。

Oracle Directory Manager を使用したエントリの変更

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

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

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

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

注意： エントリを追加または削除する場合、Oracle ディレクトリ・サーバーではエントリ属性値の構文検証は行われません。

エントリを変更する手順は、次のとおりです。

1. 7-2 ページの「[Oracle Directory Manager を使用したエントリの検索](#)」の説明に従って、変更するエントリの検索を実行します。
2. 右側のペインの「識別名」ボックスで、変更するエントリを選択します。
3. 「編集」をクリックします。「エントリ」ダイアログ・ボックスが表示されます。
4. 「OK」をクリックします。

例：Oracle Directory Manager を使用したユーザー・エントリの変更

この例では、7-7 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「識別名」ボックスで、Anne Smith のエントリを選択します。
3. 「編集」をクリックします。
4. 「エントリ」ダイアログ・ボックスで、「userPassword」ウィンドウまでスクロールしてその値を変更します。
5. 「OK」をクリックします。

Oracle Directory Manager を使用した属性オプション付きエントリの管理

この項では、属性オプションを追加、変更および削除する方法を説明します。

関連項目： 属性オプション付きエントリの検索方法は、7-2 ページの「[Oracle Directory Manager を使用したエントリの検索](#)」を参照してください。

Oracle Directory Manager を使用した、既存エントリへの属性オプションの追加

注意： Oracle Internet Directory リリース 9.0.2 の Oracle Directory Manager では、エントリを作成した時点で、そのエントリに属性オプションを追加することはできません。すでに存在しているエントリに対してのみ、Oracle Directory Manager を使用して属性オプションを追加できます。

既存のエントリに属性オプションを追加する手順は、次のとおりです。

1. 「Oracle Internet Directory サーバー」 > 「*directory server instance*」 > 「エントリ管理」の順に展開して、属性オプションを追加するエントリを選択します。対応するタブ・ページが、右側のペインに表示されます。
2. 右側のペインにある「プロパティ」タブ・ページの「プロパティの表示」フィールドで、「拡張」を選択します。この操作に伴って、「プロパティ」タブ・ページが変わります。
3. 「属性」フィールドで、オプションを追加する属性（たとえば、ou）を選択します。
4. 「属性オプション」フィールドで、属性オプション（たとえば、lang-en）を入力します。
5. 「属性値」フィールドで、指定する属性オプションの値（たとえば、Server Technologies）を入力します。指定した属性オプションに複数の値を追加するには、各値をセミコロンで区切ります。
6. 「適用」をクリックします。

Oracle Directory Manager を使用した属性オプションの変更

属性オプションを変更する手順は次のとおりです。

1. 「Oracle Internet Directory サーバー」 > 「*directory server instance*」 > 「エントリ管理」の順に展開して、属性オプションを削除するエントリを選択します。対応するタブ・ページが、右側のペインに表示されます。
2. 「プロパティ」タブ・ページの「プロパティの表示」フィールドで、「NULL 以外の値のみ」または「すべて」を選択します。
3. 変更する属性オプションを含むフィールドまでスクロールします。
4. フィールドの値を変更します。
5. 「適用」をクリックします。

Oracle Directory Manager を使用した属性オプションの削除

属性オプションを削除する手順は次のとおりです。

1. 「Oracle Internet Directory サーバー」 > 「*directory server instance*」 > 「エントリ管理」の順に展開して、属性オプションを削除するエントリを選択します。対応するタブ・ページが、右側のペインに表示されます。
2. 「プロパティ」タブ・ページの「プロパティの表示」フィールドで、「NULL 以外の値のみ」または「すべて」を選択します。
3. 削除する属性オプションを含むフィールドまでスクロールします。

- 4. フィールドの値を削除します。
- 5. 「適用」をクリックします。

コマンドライン・ツールを使用したエントリの管理

この項では、エントリの管理に使用できるコマンドライン・ツールについて説明します。また、コマンドライン・ツールを使用したエントリ管理の例もいくつか紹介します。次の項目について説明します。

- エントリ管理のためのコマンドライン・ツール
- 例: `ldapadd` を使用したユーザー・エントリの追加
- 例: `ldapmodify` を使用した属性オプションの追加
- 例: `ldapmodify` を使用したユーザー・エントリの変更
- コマンドライン・ツールを使用した属性オプション付きエントリの管理

エントリ管理のためのコマンドライン・ツール

次の表に、各コマンドライン・ツールと、それぞれのツールの構文と使用方法の参照箇所を示します。

ツール	タスク	構文と使用方法
<code>ldapsearch</code>	ディレクトリ・エントリを検索します。	A-22 ページの「 ldapsearch の構文 」
<code>ldapbind</code>	ディレクトリ・サーバーに対して、ユーザーまたはクライアントを認証します。 クライアントをサーバーに接続できるかどうかを検証します。	A-8 ページの「 ldapbind の構文 」
<code>ldapadd</code>	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 ページの「 ldapadd の構文 」
<code>ldapaddmt</code>	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 ページの「 ldapaddmt の構文 」
<code>ldapmodify</code>	エントリの属性データを作成、更新および削除します。 構成設定エントリを変更します。 エントリの識別名または相対識別名を変更します。	A-15 ページの「 ldapmodify の構文 」
<code>ldapmodifymt</code>	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-20 ページの「 ldapmodifymt の構文 」

ツール	タスク	構文と使用方法
ldapdelete	エントリを削除します。	A-11 ページの「 ldapdelete の構文 」
ldapcompare	ユーザーが指定した属性値とディレクトリ・エントリ内の属性値を比較します。	A-10 ページの「 ldapcompare の構文 」
ldapmoddn	エントリの識別名または相対識別名を変更します。 エントリまたはサブツリーを改名します。 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-13 ページの「 ldapmoddn の構文 」

例 : ldapadd を使用したユーザー・エントリの追加

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

```
dn: cn=john, c=us
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
cn: john
cn;lang-fr:Jean
cn;lang-en-us:John
sn: Doe
jpegPhoto: /photo/john.jpg
userpassword: welcome
```

このファイルには、cn、sn、jpegPhoto および userpassword の各属性が含まれています。

cn 属性では、cn;lang-fr および cn;lang-en-us という 2 つのオプションを指定しています。これらのオプションは、French（フランス語）または American English（米語）での一般名を戻します。

jpegPhoto 属性では、エントリの属性として組み込む、対応する JPEG イメージのパスとファイル名を指定しています。

注意： エントリを追加または削除する場合、Oracle ディレクトリ・サーバーではエントリ属性値の構文検証は行われません。

例 : ldapmodify を使用したユーザー・エントリの変更

次の例では、Audrey というユーザーのパスワードを、welcome から audreyspassword に変更します。前述の例と同様に、このユーザー・エントリ用のデータは entry.ldif ファイルに記述されています。このファイルの内容は次のとおりです。

```
dn: cn=audrey,c=us
changetype: modify
replace: userpassword
userpassword: audreyspassword
```

ファイルを変更するには、次のコマンドを発行します。

```
ldapmodify -p 389 -v -f entry.ldif
```

-v は冗長モードを指定します。

注意： エントリを追加または削除する場合、Oracle ディレクトリ・サーバーではエントリ属性値の構文検証は行われません。

コマンドライン・ツールを使用した属性オプション付きエントリの管理

この項では、属性オプションを追加する例と削除する例、および属性オプション付きエントリを検索する例を紹介します。

例 : ldapmodify を使用した属性オプションの追加

John のエントリのスペイン語属性を追加するとします。また、このユーザー・エントリ用のデータは entry.ldif ファイルに記述されているとします。このファイルの内容は次のとおりです。

```
dn: cn=john,c=us
changetype: modify
add: cn;lang-sp
cn;lang-sp: Juan
```

ファイルを変更するには、次のコマンドを発行します。

```
ldapmodify -h myhost -p 389 -b -f entry.ldif
```

例 : ldapmodify を使用した属性オプションの削除

次の例では、John のエントリから cn;lang-fr 属性オプションを削除します。前述の例と同様に、このユーザー・エントリ用のデータは entry.ldif ファイルに記述されているとします。このファイルの内容は次のとおりです。

```
dn: cn=john, c=us
changetype: modify
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 -h myhost -p 389 -b -f entry.ldif
```

例：ldapsearch を使用した属性オプション付きエントリの検索

次の例では、言語コード属性オプションを指定するオプションのある一般名（cn）属性を持つエントリを取り出します。この例の場合には、一般名がフランス語で、R で始まるエントリを取り出します。

```
ldapsearch -p 389 -h myhost -b "c=US" -s sub "cn;lang-fr=R*"
```

John のエントリで、cn;lang-it 言語コード属性オプションに値が設定されていないと想定します。この場合、次の例は失敗します。

```
ldapsearch -p 389 -h myhost -b "c=us" -s sub "cn;lang-it=Giovanni"
```

関連項目： 2-7 ページの「[属性オプション](#)」

バルク・ツールを使用したエントリの管理

この項では、バルク・ツールで実行する一般的なタスクの一部を説明します。

この項では、次の項目について説明します。

- [bulkload](#) を使用した LDIF ファイルのインポート
- [ディレクトリ・データの LDIF への変換](#)
- [多数のエントリの変更](#)
- [多数のエントリの削除](#)

注意： ディレクトリへの移入に `bulkload` ユーティリティを使用しない場合は、`oidstats.sh` ツールを実行して、検索パフォーマンスの深刻な低下を回避する必要があります。

関連項目：

- [oidstats.sh](#) ツールの説明と構文は、A-55 ページの「[OID データベース統計収集ツールの構文](#)」を参照してください。
- これらのツールの概要は、4-13 ページの「[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： **bulkload** ユーティリティは、空のディレクトリを想定しています。ディレクトリに既存のエントリがあると、**bulkload** ユーティリティは失敗するか、既存のエントリを上書きします。

バルク・ロードを実行する前に、**Oracle Internet Directory** プロセスを停止してください。ディレクトリ・サーバー・インスタンスの停止方法は、[第3章「事前に実行するタスクと情報」](#)を参照してください。

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

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

この項では、次の項目について説明します。

- [タスク 1: Oracle サーバーのバックアップ](#)
- [タスク 2: Oracle Internet Directory のパスワードの準備](#)
- [タスク 3: スキーマ違反とデータ整合性違反に関する入力チェック](#)
- [タスク 4: SQL*Loader 用の入力ファイルの生成](#)
- [タスク 5: 入力ファイルのロード](#)
- [バルク・ロードに失敗した場合](#)

タスク 1: Oracle サーバーのバックアップ

ファイルをインポートする前に、安全対策として Oracle データベース・サーバーをバックアップします。

関連項目：『Oracle9i ユーザー管理バックアップおよびリカバリ・ガイド』を参照してください。

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： 4-15 ページの「[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 ファイルは通常は次の場所にあります。

```
$ORACLE_HOME/ldap/bin
```

Windows NT では、このファイルは通常は次の場所にあります。

```
%ORACLE_HOME%\ldap\bin
```

入力ファイルをチェックするには、次のように入力します。

```
bulkload.sh -connect net_service_name -check path_to_ldif-filename
```

すべてのスキーマ違反が

`$ORACLE_HOME/ldap/log/schemacheck.log` に記録されます。

入力ファイルに違反が検出された場合は、ASCII テキスト・ファイル・エディタを使用してその違反を修正または削除してください。エントリが重複している場合、その識別名は `$ORACLE_HOME/ldap/log/duplicate.log` に記録されます。

タスク 4: SQL*Loader 用の入力ファイルの生成

入力ファイルのエラー修正後、次の例のように `-generate` オプションを指定して bulkload を再実行します。このステップで、LDIF データは SQL*Loader 固有の形式に変換されます。

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

ロード時のエラーはすべて

`$ORACLE_HOME/ldap/log` に記録されます。

このコマンドが正常に完了すると、SQL*Loader が -load モードで使用する *.dat ファイルが、\$ORACLE_HOME/ldap/load ディレクトリに生成されます。このファイルは変更できません。

タスク 5: 入力ファイルのロード

入力ファイルの生成後、-load オプションを指定して bulkload を再実行します。このステップで、Oracle SQL*Loader 固有の形式の *.dat ファイルがデータベースにロードされ、属性の索引が作成されます。構文は次のとおりです。

```
bulkload.sh -connect net_service_name -load
```

バルク・ロードに失敗した場合

ロード時のエラーはすべて、\$ORACLE_HOME/ldap/log/directory にファイル拡張子 .bad で記録されます。

バルク・ロードに失敗した場合は、データベースが一貫性のない状態のままになっている可能性があります。バルク・ロードを操作する前の状態にデータベースをリストアする必要があります。

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-38 ページの「[ldifwrite の構文](#)」

多数のエントリの変更

bulkmodify ユーティリティを使用すると、多数の既存エントリを効率的に変更できます。

関連項目： A-36 ページの「[bulkmodify の構文](#)」

多数のエントリの削除

bulkdelete ユーティリティを使用すると、サブツリー全体を効率的に削除できます。

関連項目： A-33 ページの「[bulkdelete の構文](#)」

ナレッジ参照と参照の管理

ナレッジ参照は**参照**とも呼ばれ、特定のタイプの**エン트리**としてディレクトリ内で表されます。ナレッジ参照エントリを作成するときには、**referral オブジェクト・クラス**および **extensibleObject** オブジェクト・クラスにそのエントリを対応付けます。通常、ナレッジ参照エントリは、パーティションを確立する **DIT** 内の場所に作成されます。

ナレッジ参照は、LDAP URL を含む参照をユーザーに提供します。この URL を、**ref** 属性の値として入力してください。任意のナレッジ参照エントリに複数の **ref** 属性が指定されている場合があります。同様に、ディレクトリ情報ツリーに複数のナレッジ参照エントリがある場合もあります。

関連項目： ナレッジ参照の概要、**スマート・ナレッジ参照**および**デフォルト・ナレッジ参照**の説明は、2-24 ページの「パーティション化」を参照してください。

この項では、次の項目について説明します。

- **スマート参照の構成**
- **デフォルト参照の構成**

スマート参照の構成

検索結果には、ナレッジ参照とともに通常のエントリも含まれる場合があります。ユーザーが検索操作を実行すると、**Oracle Internet Directory** は指定された検索の適用範囲内でナレッジ参照エントリを探します。ナレッジ参照が見つかった場合、**Oracle Internet Directory** は参照をクライアントに戻します。

ユーザーがナレッジ参照エントリの下に置かれたエントリに対して追加、削除または変更操作を実行すると、**Oracle Internet Directory** は参照を戻します。

たとえば、ディレクトリ・サーバーの地理的な場所に基づいたディレクトリ情報ツリーを分割するとします。この例では、次のように仮定します。

- **c=us** ネーミング・コンテキストは、米国のサーバー **A** とサーバー **B** にローカルに保持されています。
- **c=uk** ネーミング・コンテキストは、英国のサーバー **C** とサーバー **D** にローカルに保持されています。

ここで、この 2 つのネーミング・コンテキスト間のナレッジ参照を、次のように構成するとします。

1. 米国のサーバー **A** で、サーバー **C** とサーバー **D** の **c=uk** オブジェクトのナレッジ参照を構成します。

```
dn: c=uk
c: uk
```

```
ref: ldap://host C:389/c=uk
ref: ldap://host D:686/c=uk
objectclass: top
objectclass: referral
objectClass: extensibleObject
```

2. 同様に英国のサーバー C で、サーバー A とサーバー B の c=us オブジェクトのナレッジ参照を構成します。

```
dn: c=us
c: us
ref: ldap://host A:4000/c=us
ref: ldap://host B:5000/c=us
objectclass: top
objectclass: referral
objectClass: extensibleObject
```

結果は、次のようになります。

- サーバー A にベース o=foo,c=uk で問い合わせるクライアントは、参照を受信します。
- サーバー C にベース o=foo,c=us で問い合わせるクライアントは、参照を受信します。
- サーバー A またはサーバー B での o=foo,c=uk の追加操作は失敗します。かわりに、Oracle Internet Directory は参照を戻します。

デフォルト参照の構成

Oracle Internet Directory は、サーバーによってローカルに保持されているすべての**ネーミング・コンテキスト**を DSE の namingcontext 属性を使用して判断します。namingcontext 属性には、ネーミング・コンテキスト情報を正しく反映させてください。

DSE エントリの ref 属性の値を入力して、デフォルト参照を指定します。ref 属性が DSE エントリにない場合は、デフォルト参照は戻されません。

デフォルト参照を構成するときは、LDAP URL の識別名を指定しないでください。

たとえば、サーバー A の DSE エントリに、次の namingcontext 値が含まれているとします。

```
namingcontext: c=us
```

さらに、デフォルト参照が次のとおりと仮定します。

```
Ref: ldap://host PQR:389
```

ユーザーが、サーバー A でネーミング・コンテキスト c=canada にベース識別名を持つ操作を入力したとします。たとえば次のとおりです。

```
ou=marketing,o=foo,c=canada
```


このユーザーはホスト PQR への参照を受信することになります。これは、サーバー A が c=canada ベース識別名を保持しておらず、その DSE の namingContext 属性が値 c=canada を保持していないためです。

関連項目： ナレッジ参照の概念の説明は、2-25 ページの「[ナレッジ参照と参照](#)」を参照してください。

ディレクトリにおける グローバリゼーション・サポート

Oracle Internet Directory ではグローバリゼーション・サポートを使用して、システム固有の言語でデータの格納、処理および取得を行います。グローバリゼーション・サポートは、Oracle Internet Directory のユーティリティとエラー・メッセージを、システム固有の言語とロケールに自動的に調整します。

この章では、Oracle Internet Directory で使用されるグローバリゼーション・サポートと、Oracle Internet Directory 環境における様々なコンポーネントとツールに必要な環境変数 NLS_LANG について説明します。

関連項目： グローバリゼーション・サポートを構成する前に、2-13 ページの「[グローバリゼーション・サポート](#)」を参照してください。

この章では、次の項目について説明します。

- [環境変数 NLS_LANG](#)
- [非 UTF-8 データベースの使用方法](#)
- [LDIF ファイルでのグローバリゼーション・サポートの使用方法](#)
- [コマンドライン・ツールでのグローバリゼーション・サポートの使用方法](#)
- [クライアント環境における NLS_LANG の設定](#)
- [バルク・ツールでのグローバリゼーション・サポートの使用方法](#)

環境変数 NLS_LANG

NLS_LANG パラメータには、language、territory および charset の 3 つのコンポーネントがあります。形式は次のとおりです。

```
NLS_LANG = language_territory.charset
```

各コンポーネントは、グローバリゼーション・サポート機能のサブセットの作用を制御します。

コンポーネント	説明
language	<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>関連項目：言語の完全なリストは、『Oracle9i グローバリゼーション・サポート・ガイド』を参照してください。</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>関連項目：地域の完全なリストは、『Oracle9i グローバリゼーション・サポート・ガイド』を参照してください。</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>関連項目：キャラクタ・セットの完全なリストは、『Oracle9i グローバリゼーション・サポート・ガイド』を参照してください。</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

非 UTF-8 データベースの使用法

非 UTF-8 データベースで Oracle ディレクトリ・サーバーおよびデータベース・ツールを実行できますが、クライアントとデータベースのキャラクタ・セットが同一であることを確認する必要があります。キャラクタ・セットが異なると、ldapadd、ldapdelete、ldapmodify または ldapmodifydn 操作中にデータが損失する可能性があります。たとえば、シングルバイト文字のみを使用する基礎となるデータベース上で、マルチバイト・キャラクタ・セットを使用して ldapadd 操作を実行すると仮定します。入力するバイトのすべてがデータベースで受け入れられるわけではないため、データが消失します。

LDIF ファイルでのグローバリゼーション・サポートの使用法

関連項目： A-2 ページの「[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、簡体字中国語（.ZHS16GBK）のキャラクタ・セットのマルチバイト文字を使用できます。

属性の値は、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。次に例を 2 つあげます。

- [ASCII 文字列のみを含む LDIF ファイル](#)
- [UTF-8 エンコーディング文字列を含む LDIF ファイル](#)

ASCII 文字列のみを含む LDIF ファイル

この例では、属性値の文字列も ASCII 文字列です。

すべてのツールがデフォルトで UTF-8 キャラクタ・セットを使用しており、ASCII は UTF-8 の正しいサブセットであるため、いずれのツールもこのファイルを解釈できます。キーボードで ASCII 文字列の値をそのまま入力する場合も同様です。UTF-8 エンコーディング文字列を含む LDIF ファイル

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](#)

ディレクトリ・サーバーは UTF-8 エンコーディング文字列のみを理解し、UTF-8 エンコーディング文字列を受信することを想定しているため、ケース 1、3 および 4 は、LDAP サーバーに送信する前に、UTF-8 文字列に変換しておく必要があります。

ケース 1: ネイティブ文字列（非 UTF-8）

コマンドライン・ツール、ldifwrite および bulkmodify で、-E 引数を使用します。bulkload および bulkdelete ツールでは、-encode 引数を使用します。

この例では、簡体字中国語のネイティブ文字列を UTF-8 に変換しています。ベース識別名は、簡体字中国語で記述できます。

```
ldapsearch -h my_host -p 389 -E ".ZHS16GBK" -b base_DN -s base "objectclass=**"
```

ケース 2: UTF-8 文字列

変換は不要です。

ケース 3: BASE64 でエンコーディングされた 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使用できる言語セットは 1 つのみです。

コマンドライン・ツールでのグローバル化・サポートの使用法

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かぎり、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、簡体字中国語から UTF-8 に変換されます。

`-E` 引数を指定すると、`-E` 引数で指定したキャラクタ・セット（`-E ".character_set"`）が UTF-8 キャラクタ・セットに正しく変換されます。

コマンドライン・ツールは、`-E` 引数を使用して、`-E` 引数に指定されたキャラクタ・セットで入力を処理します。出力は、環境変数 `NLS_LANG` で指定されたキャラクタ・セットで表示します。

たとえば、簡体字中国語のキャラクタ・セット（`.ZHS16GBK`）でエンコーディングされた 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"`（簡体字中国語のキャラクタ・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" で指定されている簡体字中国語から UTF-8 にデータを変換します。たとえば、各コマンドの -D オプションと -w オプションの値が簡体字中国語で記述されます。-E 引数を指定すると、これらの値が UTF-8 に変換されます。

次の表の例には、.ZHS16GBK キャラクタ・セットに属している実際のキャラクタは含まれていないことに注意してください。したがって、これらの例は -E 引数の指定なしで動作します。ただし、引数の値に .ZHS16GBK キャラクタ・セット内の実際のキャラクタが含まれる場合は、-E 引数を使用する必要があります。

関連項目： 各コマンドライン・ツールの構文と使用方法は、[付録 A「LDIF およびコマンドライン・ツールの構文」](#)を参照してください。

ツール	例
ldapbind	ldapbind -h my_host -p 389 -E ".ZHS16GBK" -D "o=acme,c=us" -w my_password
ldapsearch	ldapsearch -h my_host -p 389 -E ".ZHS16GBK" -D "o=acme,c=us" -w my_password
ldapadd	ldapadd -h my_host -p 389 -E ".ZHS16GBK" -D "o=acme,c=us" -w my_password
ldapaddmt	ldapaddmt -h my_host -p 389 -E ".ZHS16GBK" -D "o=acme,c=us" -w my_password
ldapmodify	ldapmodify -h my_host -p 389 -E ".ZHS16GBK" -D "o=acme,c=us" -w my_password
ldapmodifymt	ldapmodifymt -h my_host -p 389 -E ".ZHS16GBK" -D "o=acme,c=us" -w my_password
ldapdelete	ldapdelete -h my_host -p 389 -E ".ZHS16GBK" -D "o=acme,c=us" -w my_password
ldapcompare	ldapcompare -h my_host -p 389 -E ".ZHS16GBK" -D "o=acme,c=us" -w my_password -b "ou=Construction,ou=Manufacturing,o=acme,c=us" -a title -v manager
ldapmoddn	ldapmoddn -h my_host -p 389 -E ".ZHS16GBK" -D "o=acme,c=us" -w my_password -b "cn=Franklin Badlwins,ou=Construction,ou=Manufacturing,c=us,o=acme" -N "ou=Contracting,ou=Manufacturing,o=acme,c=us" -r

クライアント環境における NLS_LANG の設定

クライアントに必要な出力が 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。

クライアントに必要な出力が UTF-8 以外の場合は、環境変数 NLS_LANG を設定する必要があります。この設定によって、UTF-8 キャラクタ・セットからクライアントが要求したキャラクタ・セットに正しく変換されます。

たとえば、環境変数 NLS_LANG が簡体字中国語のキャラクタ・セットに設定されている場合、コマンドライン・ツールは、そのキャラクタ・セットで出力を表示します。環境変数が設定されていない場合、出力にはデフォルトで UTF-8 キャラクタ・セットが使用されます。

注意： Windows を使用している場合、サーバーの起動後にコマンドライン・ツールを使用するには、MS-DOS ウィンドウで NLS_LANG を再設定する必要があります。MS-DOS セッションのコード・ページに一致するキャラクタ・セットを設定してください。UTF-8 は使用できません。MS-DOS セッションでコマンドライン・ツールに使用するキャラクタ・セットの詳細は、『Oracle9i Database for Windows インストレーション・ガイド』を参照してください。

Oracle Internet Directory とともに、事前にインストールされた Oracle9i リリース 1 (9.0.1) の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。詳細は、『Oracle9i グローバリゼーション・サポート・ガイド』および『Oracle9i Database for Windows インストレーション・ガイド』を参照してください。

レジストリの NLS_LANG パラメータの値を変更しないように注意してください。

バルク・ツールでのグローバル化・サポートの使用法

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](#) でのグローバル化・サポートの使用法
- [ldifwrite](#) でのグローバル化・サポートの使用法
- [bulkdelete](#) でのグローバル化・サポートの使用法
- [bulkmodify](#) でのグローバル化・サポートの使用法

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 でのグローバル化・サポートの使用法

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
```

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

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

ldifwrite でのグローバル化・サポートの使用法

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、ディレクトリ・サーバーに格納されている UTF-8 文字列または ldifwrite の実行時に環境変数 NLS_LANG の設定で指定されたネイティブ文字列にも使用できます。

次のようなコマンドを実行します。

```
ldifwrite -c net_service_name -b baseDN -f output_file
```

環境変数 NLS_LANG が未設定の場合または `language_territory.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 my_host -p port_number -f output_file
```

この場合、デコードされた BASE64 文字列はすでに UTF-8 でエンコー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、簡体字中国語（`.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 文字列は簡体字中国語であり、サーバーに送信する前に UTF-8 文字列に変換する必要があるため、`-E` 引数が必要です。

bulkdelete でのグローバリゼーション・サポートの使用方法

引数 `-encode ".character_set"` をコマンドに追加します。

次のようなコマンドを実行します。

```
bulkdelete.sh -connect net_service_name -encode ".ZHS16GBK" -base  
"ou=manufacturing,o=acme,c=us"
```

この例では、`-base` オプションの値に、ZHS16GBK ネイティブ・キャラクタ・セット（簡体字中国語）を使用できます。

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

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

bulkmodify でのグローバリゼーション・サポートの使用方法

引数 `-E ".character_set"` をコマンドに追加します。

次のようなコマンドを実行します。

```
bulkmodify.sh -c my_service_name -E ".ZHS16GBK" -b "ou=manufacturing,o=acme,c=us" -r  
title -v Foreman -f "objectclass=*
```

この例では、`-b`、`-v` および `-f` の各引数の値を簡体字中国語キャラクタ・セットを使用して指定できます。

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

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

Delegated Administration Service

Delegated Administration Service (DAS) によって、グローバル・ディレクトリ管理者は、重要で複雑なディレクトリ管理タスクから解放されます。このサービスを使用すると、次の処理を実行できます。

- エンド・ユーザーは、管理者の介入なしで自分のパスワードを変更できます。
- 非技術系マネージャなどの委任管理者が、ユーザーとグループの両方を作成および管理できます。
- すべてのユーザーが、アクセス権限のあるディレクトリの各部を検索できます。

この章では、次の項目について説明します。

- [Delegated Administration Service の概要](#)
- [Delegated Administration Service の概念とアーキテクチャ](#)
- [Delegated Administration Service の起動と停止](#)
- [Delegated Administration Service のインストールと構成](#)
- [Delegated Administration Service を使用したユーザー・エントリとグループ・エントリの検索](#)
- [Delegated Administration Service を使用したユーザー、グループおよびサブスクライバの管理](#)

Delegated Administration Service の概要

この項では、次の項目について説明します。

- [Delegated Administration Service ユニット](#)
- [Oracle Internet Directory セルフ・サービス・コンソール](#)
- [Delegated Administration Service と Oracle Internet Directory セルフ・サービス・コンソールの利点](#)

Delegated Administration Service ユニット

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

Delegated Administration Service ユニットは、ユーザーの作成、グループの作成、エントリの検索およびユーザー・パスワードの変更などの操作を実行します。また、アプリケーションのかわりに操作を実行し、その操作結果を表示するユーザー・インタフェースを提供します。

Delegated Administration Service ユニットは、ディレクトリに公開される URL を介して起動されます。DAS ユニットを起動するために、アプリケーションはディレクトリ内で対応する URL を検索します。

ユーザーは、独自の専門サービスを定義して、既存の Delegated Administration Service フレームワークにプラグインできます。

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

Oracle Internet Directory には、Oracle Internet Directory セルフ・サービス・コンソールと呼ばれる事前に構築された Delegated Administration Service ベースの Web アプリケーションも組み込まれています。このアプリケーションによって、ディレクトリで管理されるアプリケーション・データに対する管理アクセスが可能になります。このアプリケーションを使用すると、次の処理を実行できます。

- エンド・ユーザーは、管理を許可されているデータに対してセルフ・サービスを実行できます。たとえば、Oracle Internet Directory セルフ・サービス・コンソールを使用して、パスワード、個人データ（電話番号や事務所の場所など）またはアプリケーション作業環境を変更できます。
- サブスクライバ管理者は、次のことができます。
 - サブスクライバ・レベルの情報管理（サブスクライバ構成の変更など）
 - 新規ユーザーおよびグループの準備

- サブスクライバ内のユーザー・レベルおよびグループ・レベルの情報管理（ユーザー・エントリおよびグループ・エントリの作成や編集など）

また、サブスクライバ管理者は、セルフ・サービス・コンソールを使用して次のようなディレクトリ操作を実行できます。

- ホワイト・ページ・アプリケーションへのアクセス制御
- 特定のアプリケーションに関連付けられていないディレクトリ属性（電話番号や事務所の場所など）の管理
- サイト管理者は、次のことができます。
 - サイト・レベルの情報管理（サイト構成など）
 - サブスクライバ・レベルの情報管理（新規サブスクライバの作成、サブスクライバのアクセス権限や管理権限の変更など）

Delegated Administration Service と Oracle Internet Directory セルフ・サービス・コンソールの利点

Delegated Administration Service と Oracle Internet Directory セルフ・サービス・コンソールを使用すると、次のような利点があります。

- ディレクトリ対応アプリケーションの迅速な開発と配置

Delegated Administration Service ユニットを使用して、アプリケーションでディレクトリを管理するために必要なツールをより簡単に開発できます。これらのユニットは、アプリケーションに必要なほとんどの機能を提供します。

- ディレクトリに対する保護アクセス

Delegated Administration Service では、Oracle Internet Directory の**プロキシ・ユーザー**機能を使用して、ユーザーのかわりに様々な操作を実行します。Delegated Administration Service ユニットを使用して管理アプリケーションを作成した場合は、この機能を活用できます。この機能によって、プロキシ・アクセス権限が1箇所で集中管理されるため、ディレクトリ・セキュリティが向上します。アプリケーションに必要な様々なディレクトリ管理ツールに対して、ディレクトリ管理者がスーパー・ユーザーのアクセス権限を提供する必要はなくなります。

- アプリケーション・ユーザーにとっての使い勝手のよさ

ディレクトリ対応の複数のアプリケーションのユーザーは、アプリケーションに関連するディレクトリ・データを管理する単一セットのサービスとインタフェースをとりまします。

- ディレクトリ・データの管理を委任するためのサイトの機能

Delegated Administration Service によって、ディレクトリ管理者が定義したディレクトリ・データの管理をサブスクライバ管理者およびアプリケーションのエンド・ユーザー

に委任できます。委任によって、サイトでのディレクトリ・データの管理がより簡単になります。

Delegated Administration Service の概念とアーキテクチャ

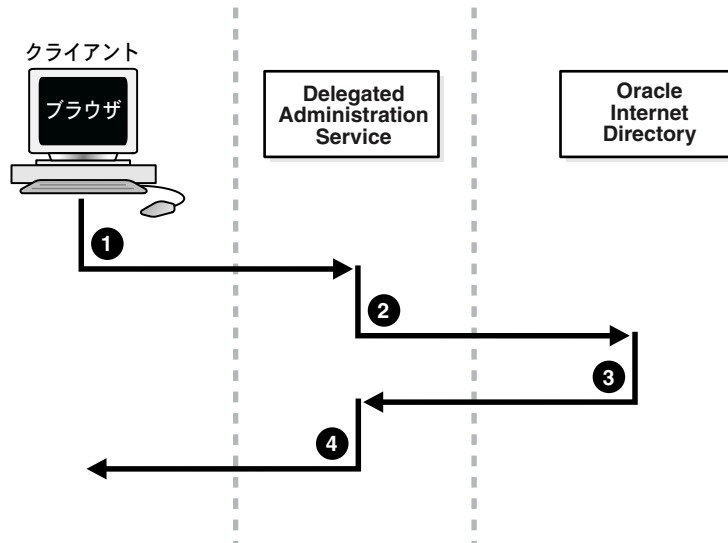
Delegated Administration Service は、サーブレットと呼ばれる小型の Java プログラムが使用可能な Oracle9iAS Containers for J2EE (OC4J) を使用します。Oracle9iAS Containers for J2EE (OC4J) とサーブレットを組み合わせて使用することにより、次の処理を実行できます。

1. クライアントからのリクエストを受信します。
2. Oracle Internet Directory のデータを取得または更新することによってクライアントのリクエストを処理し、LDAP 結果を HTML ページに編成します。
3. HTML ページをクライアントの Web ブラウザに戻します。

Delegated Administration Service の動作

図 9-1 は、Delegated Administration Service 環境のコンポーネント間の関係を示しています。

図 9-1 Delegated Administration Service のコンポーネント



1. ユーザーはブラウザから HTTP を使用して、Oracle Internet Directory への問合せが含まれているリクエストを Delegated Administration Service に送信します。

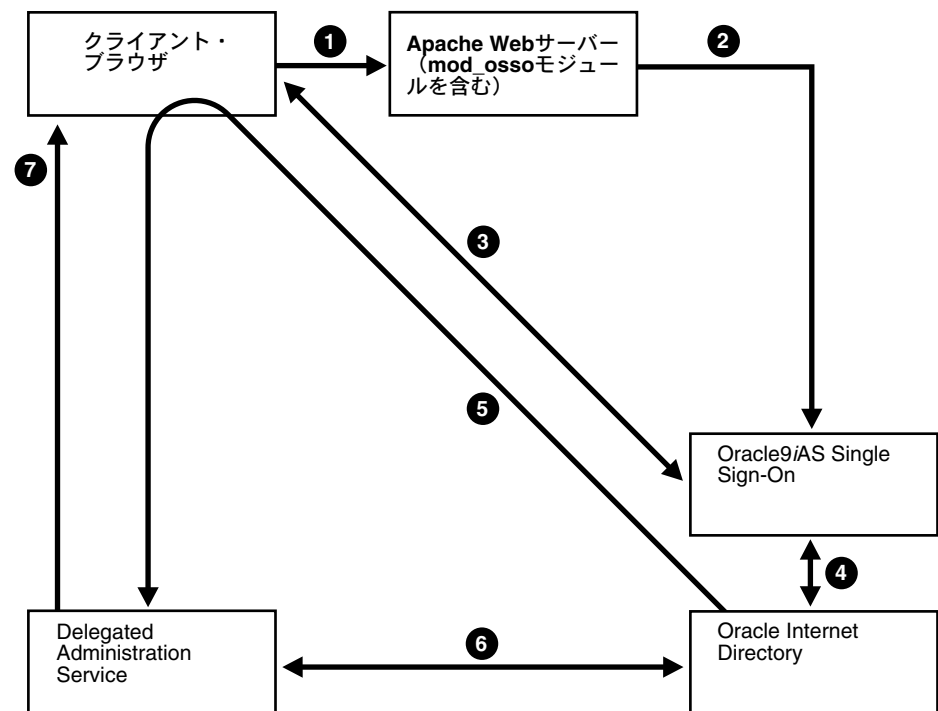
2. Delegated Administration Service はリクエストを受信し、適切なサーブレットを起動します。このサーブレットはリクエストを解析し、LDAP を使用してそのリクエストを Oracle Internet Directory に送信します。
3. Oracle Internet Directory は、LDAP 結果を Delegated Administration Service に送信します。
4. Delegated Administration Service は、LDAP 結果を HTML ページに編成し、クライアントの Web ブラウザに送信します。

Delegated Administration Service と Oracle9iAS Single Sign-On

Delegated Administration Service は、Oracle9iAS Single Sign-On と組み合わせて使用できます。

図 9-2 は、Oracle9iAS Single Sign-On 環境での検索操作における Delegated Administration Service コンポーネント間の関係を示しています。

図 9-2 Delegated Administration Service と Oracle9iAS Single Sign-On



1. ユーザーは、Oracle HTTP Server および mod_osso モジュールを介して Delegated Administration Service へのアクセスを要求します。
2. 1 つのセッションの中でユーザーが初めて Delegated Administration Service にアクセスしようとした場合、Oracle HTTP Server は、認証のためにユーザーを Oracle9iAS Single Sign-On に透過的にリダイレクトします。
3. Oracle9iAS Single Sign-On は、Oracle HTTP Server を介して、ユーザー名とパスワードを要求するプロンプトを表示します。ユーザーは、ユーザー名とパスワードを入力します。
4. Oracle9iAS Single Sign-On は、ユーザーが入力した値を Oracle Internet Directory に格納されている対応する値と比較して、ユーザーの資格証明を検証します。
5. ユーザー名とパスワードの有効性が正しく検証された場合は、Oracle9iAS Single Sign-On がユーザーを Delegated Administration Service にリダイレクトします。また、ユーザー識別子を含む暗号化パラメータを Delegated Administration Service に送信します。
6. Delegated Administration Service は、Oracle9iAS Single Sign-On によるユーザー認証を受け入れます。

ユーザーがディレクトリにアクセスできるようにするため、Delegated Administration Service は次の処理を実行します。

- エンド・ユーザーのかわりに、識別情報を切り替える権限を持つ**プロキシ・ユーザー**で Oracle Internet Directory にログインします。
- 次に、エンド・ユーザーの識別名を使用して、ディレクトリへの 2 回目のバインドを実行します。

Delegated Administration Service がエンド・ユーザーの識別名を使用してディレクトリ・サーバーにログインすると、ディレクトリ・サーバーでは次の判断が行われます。

- この 2 回目のバインドは、プロキシ・ユーザーがエンド・ユーザーの ID に切り替えようとしているものと認識します。
- Delegated Administration Service によってエンド・ユーザーに付与された認証を受け入れます。
- エンド・ユーザーのパスワードを要求せずに、2 回目のバインドの実行を許可します。

関連項目： プロキシ・ユーザーおよび間接認証の詳細は、11-4 ページの「**認証**」を参照してください。

7. Delegated Administration Service は、Oracle Internet Directory から LDAP 結果を取得します。
8. Delegated Administration Service は、LDAP 結果を HTML ページに編成し、クライアントの Web ブラウザに送信します。

Delegated Administration Service の起動と停止

サービスを起動するには、次のコマンドを入力します。

```
$ORACLE_HOME/opmn/bin/opmnctl startall
```

サービスを停止するには、次のコマンドを入力します。

```
$ORACLE_HOME/opmn/bin/opmnctl stopall
```

Delegated Administration Service のインストールと構成

この項では、次の項目について説明します。

- [Delegated Administration Service 環境でのコンポーネントのログ・ファイル](#)
- [タスク 1: Delegated Administration Service のインストール](#)
- [タスク 2: Delegated Administration Service が稼働していることの検証](#)
- [タスク 3: デフォルト・サブスクリバ・コンテキストの構成](#)
- [タスク 4: ユーザー・エントリの構成](#)

Delegated Administration Service 環境でのコンポーネントのログ・ファイル

表 9-1 は、Delegated Administration Service 環境で、各コンポーネントのログ・ファイルが格納される位置を示しています。

表 9-1 Delegated Administration Service 環境でのコンポーネントのログ・ファイル

アプリケーション	ログ・ファイルの位置
Oracle HTTP Server	\$ORACLE_HOME/Apache/Apache/logs
Oracle9i Containers for J2EE (OC4J)	\$ORACLE_HOME/opmn/logs
Delegated Administration Service	\$ORACLE_HOME/ldap/log/das.log

Delegated Administration Service をインストールおよび構成するには、次のタスクを実行します。

- [タスク 1: Delegated Administration Service のインストール](#)
- [タスク 2: Delegated Administration Service が稼働していることの検証](#)
- [タスク 3: デフォルト・サブスクリバ・コンテキストの構成](#)
- [タスク 4: ユーザー・エントリの構成](#)

タスク 1: Delegated Administration Service のインストール

Delegated Administration Service は、Oracle Internet Directory リリース 9.0.2 とともにインストールされます。Oracle9iAS Single Sign-On を使用可能にするには、Oracle9iAS Single Sign-On Server をインストールして構成する必要があります。

関連項目：

- 使用しているオペレーティング・システム用の Oracle Internet Directory リリース 9.0.2 のインストール・ガイドを参照してください。
- 『Oracle9iAS Single Sign-On 管理者ガイド』を参照してください。

タスク 2: Delegated Administration Service が稼働していることの検証

次の手順に従って、Delegated Administration Service が稼働していることを検証します。

手順 1: Oracle HTTP Server が稼働していることの検証

検証するには、次のコマンドを入力します。

```
ps -ef | grep http
```

関連項目：

- Delegated Administration Service 環境で、各コンポーネントのログ・ファイルが格納される位置については、9-7 ページの表 9-1 を参照してください。
- 9-7 ページの「[Delegated Administration Service の起動と停止](#)」

手順 2: Java (OC4J JVM) が稼働していることの検証

検証するには、次のコマンドを入力します。

```
ps -ef | grep java
```

Java プロセスが稼働していることを確認します。稼働していない場合は、ログ・ファイルを参照してください。

関連項目： ログ・ファイルの位置については、9-7 ページの表 9-1 を参照してください。

手順 3: Delegated Administration Service が稼働していることの検証

任意のブラウザを使用して、次のコマンドを入力します。

```
http://host_name:port_number/oiddas/
```

`host_name` は Oracle HTTP Server が稼働しているコンピュータの名前です。Delegated Administration Service ホームページが表示されます。

タスク 3: デフォルト・サブスクライバ・コンテキストの構成

Delegated Administration Service のインストール後、デフォルト・サブスクライバ・コンテキスト（つまり、デフォルト・サブスクライバのエントリがすべて含まれているネーミング・コンテキストのルート・エントリ）を構成できます。

デフォルト・サブスクライバを構成する手順は、次のとおりです。

1. **administrator** でログインします。デフォルト管理ユーザー名は **orcladmin**、デフォルト・パスワードはインストール時に指定したものです。
2. 「構成」タブを選択します。
3. 「ディレクトリ構成」セクションで、次の操作を実行します。
 - a. 「ログイン名の属性」フィールドに、ログイン時にユーザー自身を識別するために使用する属性（たとえば、**cn**、**UID**、**EmployeeNumber**、**SSN**）を入力します。
 - b. 「ユーザー検索ベース・コンテキスト」フィールドに、このサブスクライバのユーザー・エントリが置かれたエントリの識別名を入力します。
 - c. 「グループ検索ベース・コンテキスト」フィールドに、このサブスクライバのグループ・エントリが置かれたエントリの識別名を入力します。
 - d. 「検索結果制限」フィールドに、検索結果として表示するエントリの数を入力します。
4. 「ロゴ・マネージメント」セクションで、次の操作を実行します。
 - a. Delegated Administration Service ユーザー・インタフェースの左上端にサブスクライバのロゴを表示する場合は、「サブスクライバ・ロゴを使用可能にする」チェックボックスを選択します。それ以外の場合は未選択のままにします。
 - b. Delegated Administration Service ユーザー・インタフェースの左上端に製品名 **Internet Directory** を表示する場合は、「製品ロゴを使用可能にする」チェックボックスを選択します。それ以外の場合は未選択のままにします。
 - c. 「サブスクライバ・ロゴの更新」フィールドに、サブスクライバ・ロゴのパスとファイル名を入力するか、または「参照」を選択してロゴ・ファイルが格納されている位置にナビゲートします。
5. 企業イメージ・ロゴ・ファイルの位置を入力し、「送信」を選択して変更を保存します。

タスク 4: ユーザー・エントリの構成

ユーザーがユーザー・エントリを作成または編集する場合、様々なカテゴリ（基本情報、パスワードおよび写真など）とその一連の属性が表示されます。管理者は、**Delegated Administration Service** によるこれらのカテゴリと対応する属性の表示方法をカスタマイズできます。

具体的には、**Delegated Administration Service** では次のことができます。

- ユーザー・エントリへのオブジェクト・クラスの追加、およびその属性の追加と変更
- ユーザーによる追加または変更を可能にする属性カテゴリの指定
- **Delegated Administration Service** でのカテゴリと属性の表示方法のカスタマイズ

ユーザー・エントリを構成する手順は、次のとおりです。

1. 「構成」タブを選択し、次に「ユーザー・エントリ」を選択します。「ユーザー・オブジェクト・クラスの構成」ウィンドウに、ユーザー・エントリの既存のオブジェクト・クラスのリストが表示されます。
2. ユーザー・エントリにオブジェクト・クラスを追加するには、次の手順を実行します。
 - a. 「オブジェクト・クラスの追加」を選択します。「すべてのオブジェクト・クラス」ウィンドウが表示されます。
 - b. 追加するオブジェクト・クラスを選択し、次に「追加」を選択します。「オブジェクト・クラスの指定」ウィンドウが表示されます。選択したオブジェクト・クラスが既存のオブジェクト・クラスとしてリストされます。
 - c. オブジェクト・クラスをさらに追加する場合は、これらの手順を繰り返します。オブジェクト・クラスの追加作業を完了した場合は、「次」を選択して「属性の構成」ウィンドウを表示します。
3. 属性を追加、または **Delegated Administration Service** での属性の表示方法を変更するには、次の手順を実行します。
 - a. 「新規属性の追加」を選択し、「新規属性の追加」ウィンドウを表示します。
 - b. 「ディレクトリ属性名」コンボ・ボックスから、追加する属性を選択します。
 - c. [表 9-2](#) の説明に従って、各フィールドに値を入力します。

表 9-2 「属性の構成」ウィンドウのフィールド

フィールド	説明
「UI ラベル」	ユーザー・インタフェースの属性にわかりやすい名前を指定します。たとえば、sn 属性を「姓」と表示できます。
必須	属性が必須かどうかを指定します。必須属性には、フィールドの左側にアスタリスク (*) が表示されます。このチェックボックスを選択しない場合、属性はオプションになります。
表示可能	このチェックボックスを選択して、検索結果に属性を表示するかどうかを指定します。
UI タイプ	このフィールドのインタフェースの種類を指定します。オプションは次のとおりです。 <ul style="list-style-type: none"> ■ 「単一行テキスト」: 値を入力する 1 行のテキスト・フィールド。 ■ 「複数行テキスト」: 複数行のテキストを入力できるテキスト領域。 ■ 「事前定義テキスト」: ドロップダウン・リストから値を選択するコンボ・ボックス。ドロップダウン・リストの値を指定するには、「編集」を選択して「属性の編集」ウィンドウを表示します。「LOV 値」テキスト領域にそれぞれの値を入力し、[ENTER] キーを押します。 ■ 日付: 日付（従業員の誕生日など）を入力するテキスト・フィールド。 ■ 「参照と選択」: マネージャの入力や、属性値に識別名が必要な場合の入力を参照できるボタン。 ■ 「数値」: 数値のみ（郵便番号など）を入力できるテキスト・フィールド。

- d. 「完了」を選択して「ユーザー属性の構成」ウィンドウに戻ります。選択した属性が属性リストに表示されます。

ユーザー属性の追加作業を完了した場合は、「次」を選択して「属性カテゴリの作成」ウィンドウを表示します。

4. 「属性カテゴリの作成」ウィンドウを使用して、属性のカテゴリ表示方法をカスタマイズします。

新規カテゴリを追加するには、次の手順を実行します。

- 「新規カテゴリの追加」を選択します。
- 「UI ラベル」フィールドに、わかりやすいカテゴリの名前（電話番号、組織の詳細など）を入力します。
- 「完了」を選択して「属性カテゴリの作成」ウィンドウに戻ります。

カテゴリを変更するには、次の手順を実行します。

- a. 「選択」列で、適切なカテゴリを選択します。
- b. 「UI ラベル」列と「順序の表示」列で、適切なフィールドを編集します。表示順序は、ウィンドウで最上位に表示するカテゴリには 0（ゼロ）、その次に表示するカテゴリには 1、その次は 2（以下同様）と指定します。

カテゴリを削除するには、「削除」を選択します。

属性のカテゴリの作業を完了した場合は、「次」を選択して「属性カテゴリの構成」ウィンドウを表示します。

5. 属性の各カテゴリを構成するには、「属性カテゴリの構成」ウィンドウを使用します。各カテゴリに対して、2つのリストが表示されます。

- 「All Attributes」：このカテゴリに使用可能なすべての属性
- 「Selected Attributes」：このカテゴリでユーザーによる変更が可能な属性

各属性カテゴリを構成するには、次の手順を実行します。

- a. 2つのリスト間で移動させる項目を一度に1つ以上選択して、適切な矢印を選択します。
- b. 各カテゴリの「Selected Attributes」リストで、リスト右側の上下矢印ボタンを使用して属性の表示順序を設定します。

属性カテゴリの構成を終了した後、「次」を選択して「Public グループの構成」ウィンドウを表示します。

6. Delegated Administration Service ユーザー・インタフェースに表示される Public グループ・リストを構成するには、次の手順を実行します。

ユーザーを Public グループに割当て可能にするには、「Public グループを使用可能にする」チェックボックスを選択します。それ以外の場合は未選択のままにします。

Public グループを追加するには、「グループの追加」ボタンを選択して「Search and Select: Public グループ」を表示します。「次の文字で始まるグループ名」フィールドに、追加するグループ名の始めの数文字を入力して、検索結果の表から該当するグループ名を指定し、「選択」をクリックします。

Public グループを削除するには、削除するグループを表から選択し、「削除」をクリックします。

Delegated Administration Service を使用したユーザー・エントリとグループ・エントリの検索

この項では、次の項目について説明します。

- [Delegated Administration Service を使用したユーザー・エントリの検索](#)
- [Delegated Administration Service を使用したグループ・エントリの検索](#)

Delegated Administration Service を使用したユーザー・エントリの検索

ユーザーを検索する手順は、次のとおりです。

1. 「ディレクトリ」タブを選択し、次に「ユーザー」を選択します。
2. 「ユーザーの検索」フィールドに、ユーザー名の始めの数文字を入力します。たとえば、Anne Smith を検索する場合は、Ann のように入力します。
3. 「進む」を選択して検索結果を表示します。

Delegated Administration Service を使用したグループ・エントリの検索

グループを検索する手順は、次のとおりです。

1. 「ディレクトリ」タブを選択し、次に「グループ」を選択します。
2. 「グループ名の検索」テキスト・ボックスに、検索するグループ名の始めの数文字を入力します。
3. 「進む」を選択して、入力した基準に一致するエントリを表示します。

Delegated Administration Service を使用したユーザー、グループおよびサブスクライバの管理

この項では、次の項目について説明します。

- [Delegated Administration Service を使用したユーザー・エントリの作成](#)
- [Delegated Administration Service を使用したユーザー・エントリの変更](#)
- [Delegated Administration Service を使用したユーザー・エントリの削除](#)
- [Delegated Administration Service を使用したユーザー権限の割当て](#)
- [Delegated Administration Service を使用したグループ・エントリの作成](#)
- [Delegated Administration Service を使用したグループ・エントリの変更](#)
- [Delegated Administration Service を使用したグループ・エントリの削除](#)
- [Delegated Administration Service を使用したグループ権限の割当て](#)
- [Delegated Administration Service を使用したパスワードの変更](#)

Delegated Administration Service を使用したユーザー・エントリの作成

ユーザー・エントリを作成する手順は、次のとおりです。

1. 「ディレクトリ」タブを選択し、次に「ユーザー」を選択します。
2. 「作成」を選択して「ユーザーの作成」ウィンドウを表示します。
3. 必須フィールドおよびその他の適切なフィールドに値を入力します。
4. 入力したすべての情報が正しいことを確認し、「送信」を選択します。

Delegated Administration Service を使用したユーザー・エントリの変更

ユーザー・エントリを変更する手順は、次のとおりです。

1. 「ディレクトリ」タブを選択し、エントリを変更するユーザーを検索します。
2. エントリを変更するユーザーを選択し、次に「編集」を選択して「ユーザーの編集」ウィンドウを表示します。
3. 必須フィールドおよびその他の適切なフィールドの値を変更し、「終了」を選択します。

関連項目：[「Delegated Administration Service を使用したユーザー・エントリの検索」](#)

Delegated Administration Service を使用したユーザー・エントリの削除

ユーザー・エントリを削除する手順は、次のとおりです。

1. 「ディレクトリ」タブを選択し、エントリを削除するユーザーを検索します。
2. エントリを削除するユーザーを選択し、次に「削除」を選択します。

Delegated Administration Service を使用したユーザー権限の割当て

次の 1 つまたはすべてを実行する権限をユーザーに付与できます。

- ユーザーおよびグループの作成と編集
- 他のユーザーおよびグループへの権限の割当て

ユーザーから権限を取り消すこともできます。

権限をユーザーに割り当てる手順は、次のとおりです。

1. 「ディレクトリ」タブを選択し、権限を割り当てるユーザー・エントリを検索します。
2. 権限を割り当てるユーザーを選択し、次に「権限の割当て」を選択して権限のリストを表示します。
3. このユーザーに割り当てる権限を選択します。オプションは次のとおりです。

権限	付与されるアクセス権限の説明
ユーザー作成を許可します。	ユーザー・エントリを作成できます。
ユーザー編集を許可します。	ユーザー・エントリを変更できます。
ユーザー削除を許可します。	ユーザー・エントリを削除できます。
グループ作成を許可します。	グループ・エントリを作成できます。
グループ編集を許可します。	グループ・エントリを変更できます。
グループ削除を許可します。	グループ・エントリを削除できます。
ユーザーへの権限の割当てを許可します。	アクセス権限をユーザーに付与できます。

権限	付与されるアクセス権限の説明
グループへの権限の割当てを許可します。	アクセス権限をグループに付与できます。
「Delegated Administration Service 構成を許可します。」	Delegated Administration Service ユーザー・インタフェースを構成できます。

4. 「送信」を選択するか、または権限を別のユーザーに割り当てるために「他のグループを指定してください。」を選択して処理を繰り返します。

Delegated Administration Service を使用したグループ・エントリの作成

グループ・エントリを作成する手順は、次のとおりです。

- 「ディレクトリ」タブを選択し、次に「グループ」、「作成」を順に選択します。「グループの作成」ウィンドウが表示されます。
- 「基本情報」セクションで、このグループの名前を「Name」フィールドに入力します。
- 「Display Name」フィールドに、わかりやすい名前を入力します。たとえば、**RDN** が OracleDBCreators の場合は、表示名に「Oracle データベース作成者」のように入力できます。
- 「Description」フィールドに、このグループの簡潔な説明を入力します。
- このグループ・エントリを所有者以外のすべてのユーザーに対して非表示にする場合は、「Group Visibility」フィールドで PRIVATE を選択します。また、それ以外は、PUBLIC を選択します。
- グループの作成者は、自動的にグループ所有者になります。別の所有者をこのグループに追加指定するには、次の手順を実行します。
 - 「オーナー」セクションで、「オーナーの追加」を選択して「検索および選択 : ユーザー」ウィンドウを表示します。
 - このグループの所有者に指定するユーザーのエントリを検索し、「選択」をクリックします。「グループの作成」ウィンドウが表示されます。指定したユーザーが「オーナー」セクションにリストされます。所有者を削除するには、「オーナー」セクションで、所有者の名前を選択して「削除」を選択します。
- ユーザーをこのグループのメンバーに追加するには、次の手順を実行します。
 - 「メンバー」セクションで、「ユーザー・メンバーの追加」を選択して「Search and Select」ウィンドウを表示します。

- b. このグループのメンバーに指定するユーザーのエントリを検索し、「選択」をクリックします。「グループの作成」ウィンドウが表示されます。指定したユーザーが「メンバー」セクションにリストされます。

このグループからユーザーを削除するには、「ユーザー・メンバーの追加」セクションで、ユーザーの名前を選択して「削除」を選択します。

8. グループをこのグループのメンバーに追加するには、次の手順を実行します。
 - a. 「メンバー」セクションで、「グループ・メンバーの追加」を選択して「Search and Select」ウィンドウを表示します。
 - b. このグループのメンバーに指定するグループのエントリを検索し、「選択」をクリックします。「グループの作成」ウィンドウが表示されます。指定したグループが「メンバー」セクションにリストされます。

Delegated Administration Service を使用したグループ・エントリの変更

グループ・エントリを変更する手順は、次のとおりです。

1. 「ディレクトリ」タブを選択し、エントリを変更するグループを検索します。
2. 変更するグループ・エントリを選択し、次に「編集」を選択して「グループの編集」ウィンドウを表示します。
3. 9-16 ページの「[Delegated Administration Service を使用したグループ・エントリの作成](#)」の説明に従ってフィールドを変更し、「終了」を選択します。

Delegated Administration Service を使用したグループ・エントリの削除

グループ・エントリを削除する手順は、次のとおりです。

1. 「ディレクトリ」タブを選択し、エントリを削除するグループを検索します。
2. エントリを削除するグループを選択し、次に「削除」を選択します。

Delegated Administration Service を使用したグループ権限の割当て

次の 1 つ以上を実行する権限をグループに付与できます。

- ユーザーおよびグループの新規作成と編集
- ユーザーおよび他のグループへの権限の割当て

権限をグループに割り当てる手順は、次のとおりです。

1. 「ディレクトリ」タブを選択し、次に「グループ」を選択して権限を割り当てるグループ・エントリを検索します。
2. 権限を割り当てるグループを選択し、「権限の割当て」を選択して権限のリストを表示します。
3. このグループに割り当てる権限を選択します。オプションは次のとおりです。

権限	付与されるアクセス権限の説明
ユーザー作成を許可します。	ユーザー・エントリを作成できます。
ユーザー編集を許可します。	ユーザー・エントリを変更できます。
ユーザー削除を許可します。	ユーザー・エントリを削除できます。
グループ作成を許可します。	グループ・エントリを作成できます。
グループ編集を許可します。	グループ・エントリを変更できます。
グループ削除を許可します。	グループ・エントリを削除できます。
ユーザーへの権限の割当てを許可します。	アクセス権限をユーザーに付与できます。
グループへの権限の割当てを許可します。	アクセス権限をグループに付与できます。
「Delegated Administration Service 構成を許可します。」	Delegated Administration Service インタフェースを構成できます。

4. 「送信」を選択するか、または権限を別のグループに割り当てるために「他のグループを指定してください」を選択して処理を繰り返します。

Delegated Administration Service を使用したパスワードの変更

ユーザーは自身のパスワードを変更できます。また、ユーザーまたはグループ・エントリの変更権限がある場合は、別のユーザーまたはグループのパスワードを変更できます。

ユーザー自身のパスワード変更

ユーザーは、Oracle9iAS Single Sign-On、Delegated Administration Service、Enterprise Security Manager および Oracle9iAS Portal に対する認証に使用するパスワードを変更できます。その他の Oracle のコンポーネントに対するパスワードも変更できます。

パスワードを変更する手順は、次のとおりです。

1. Delegated Administration Service にログインし、「プロファイル」タブを選択します。
2. 「パスワードの変更」を選択します。

Oracle9iAS Single Sign-On、Delegated Administration Service、Enterprise Security Manager および Oracle9iAS Portal のパスワードを変更するには、次の手順を実行します。

- a. 「シングル・サインオンのパスワード」セクションで、現在のパスワードを「旧パスワード」フィールドに入力します。
- b. 新しいパスワードを「新規パスワード」フィールドに入力し、次に「新規パスワードの確認」フィールドで新しいパスワードを再入力します。
- c. 「送信」を選択します。

その他の Oracle のコンポーネントに対するパスワードを変更するには、次の手順を実行します。

- a. 「アプリケーション・パスワード」セクションで、新しいパスワードを指定する Oracle のコンポーネントを選択します。
- b. 「パスワードの更新」を選択して、「アプリケーション・パスワードの変更」ウィンドウを表示します。
- c. 新しいパスワードを「新規パスワード」フィールドに入力し、次に「新規パスワードの確認」フィールドで新しいパスワードを再入力します。
- d. 「送信」を選択します。

別のユーザーのパスワード変更

必要なアクセス権限がある場合は、別のユーザーのパスワードを変更できます。別のユーザーのパスワードを変更する手順は、次のとおりです。

1. 「ディレクトリ」タブを選択し、パスワードを変更するユーザーのエントリを検索します。
2. ユーザー・エントリを選択し、「編集」を選択して「ユーザーの編集」ウィンドウを表示します。
3. 「基本情報」セクションで、ユーザーに割り当てるパスワードを入力し、次に再入力します。
4. 「送信」を選択します。

10

属性一意性

この章では、Oracle Internet Directory の属性一意性について説明します。

この章では、次の項目について説明します。

- [概要](#)
- [概念](#)
- [要件](#)
- [既知の制限事項](#)

概要

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

Oracle Internet Directory と同期化するアプリケーションでは、識別名以外の属性を一意キーとして使用できます。属性一意性を規定する Oracle Internet Directory のこの機能によって、すべてのアプリケーションは、それぞれ独自のユーザーに関する認識を持ち、ユーザー・ベースを企業の Oracle Internet Directory サーバーに格納されているユーザー・リポジトリと同期化することができます。属性一意性は、エントリが変更されるたびに、指定された属性の値が一意であることを保証するチェックを実施します。

ユーザーは次の各範囲内で属性一意性を定義できます。

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

概念

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

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

ディレクトリ・サーバーは、次の範囲で属性一意性チェックを実行します。

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

注意： 属性一意性は、カタログ化属性でのみ機能します。

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

属性一意性制約を構成するには、次の異なる方法があります。

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

たとえば、Oracle が Company1 と Company2 のディレクトリをホスティングしているとします。uid=dlin,ou=people,o=Company1,dc=oracle,dc=com のエントリを追加する場合は、o=Company1,dc=oracle,dc=com サブツリー内のみ、一意性を適用する必要があります。これを行うには、属性一意性制約の構成で、サブツリーの識別名を明示的に列挙します

- 1 つのオブジェクト・クラス内での属性一意性を定義できます。

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

要件

この項では、属性一意性に関する要件について説明します。

次の項目について説明します。

- [属性一意性の作成](#)
- [ディレクトリ全体での属性一意性の作成](#)
- [1 つのサブツリー内での属性一意性の作成](#)
- [1 つのオブジェクト・クラス内での属性一意性の作成](#)
- [属性一意性の有効化と無効化](#)
- [サブツリーの指定](#)
- [属性一意性ポリシーの削除](#)
- [構成インタフェース](#)
- [定義されたポリシーの位置およびモデル](#)
- [ポリシー有効範囲決定規則](#)
- [属性一意性機能の適用](#)

属性一意性の作成

ディレクトリ内の特定の属性が常に一意の値になるようにするには、チェックする属性に対して属性一意性のインスタンスを作成する必要があります。たとえば、メール属性を持つディレクトリ内のすべてのエントリが、その属性に対して一意の値を保持するためには、メールに関連付けられた属性一意性のインスタンスを作成する必要があります。

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

ディレクトリ全体での属性一意性の作成

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

1つのサブツリー内での属性一意性の作成

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

- 値の一意性を適用する属性名
- 一意性制約を適用するサブツリーの位置

1つのオブジェクト・クラス内での属性一意性の作成

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

- 値の一意性を適用する属性名
- オブジェクト・クラス名

属性一意性の有効化と無効化

属性一意性を有効または無効にできます。

属性一意性の有効化

ldapmodify コマンドライン・ツールを使用して、属性一意性ポリシーの状態をオンに変更できます。属性一意性制約を変更した場合は、ディレクトリ・サーバーを再起動する必要があります。

属性一意性の無効化

ldapmodify コマンドライン・ツールを使用して、属性一意性ポリシーの状態をオフに変更できます。属性一意性制約を削除した場合は、ディレクトリ・サーバーを再起動する必要があります。

サブツリーの指定

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

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

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

属性一意性ポリシーの削除

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

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

構成インタフェース

表 10-2「属性一意性制約エントリ」に示すように、各属性一意性制約エントリには、次の属性があります。

表 10-1 属性一意性制約エントリの属性

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

定義されたポリシーの位置およびモデル

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

表 10-2 に示すように、属性一意性制約エントリで orcluniquescopesubtree または orcluniqueobjectclass が未指定の場合は、デフォルト値がそれぞれ適用されます。デフォルトでは、orcluniquescopesubtree はサブツリー、orcluniquesubtree はディレクトリ全体、orcluniqueobjectclass はすべてのオブジェクト・クラスです。

ポリシー有効範囲決定規則

複数の属性一意性制約で、orcluniqueattrname の値が異なる場合、その有効性は互いに独立しています。

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

複数の属性一意性制約で、orcluniqueattrname および orcluniquesubtree の値が同一で、orcluniquescope の値が異なる場合は、最大の検索有効範囲を持つ属性一意性制約が有効となります。

複数の属性一意性制約で、orcluniqueattrname、orcluniquesubtree および orcluniquescope の値が同一で、orcluniqueobjectclass の値が異なる場合は、それらのオブジェクト・クラスに属する属性を結合したものがチェックされます。

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

複数の属性一意性制約で、orcluniqueattrname、orcluniquesubtree および orcluniqueobjectclass の値がそれぞれ同一の場合は、最大の検索有効範囲を持つ属性一意性制約が有効となります。

表 10-2 属性一意性制約エントリ

属性名	必須	有効値	デフォルト値	デフォルト有効範囲
orcluniqueattrname	はい	文字列	該当なし	該当なし
orcluniquescope	いいえ	次のいずれかの値	sub	
		base		ベースのみを検索
		onelevel		1 レベルを検索
		sub		サブツリーを検索
orcluniquesubtree	いいえ	文字列	" "	ディレクトリ全体
orcluniqueobjectclass	いいえ	文字列	" "	すべてのオブジェクト・クラス

属性一意性機能の適用

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

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

解決策：次の手順に従って、属性一意性制約を作成して適用します。

1. 次のように、属性一意性制約エントリを（LDIF フォーマットで）作成します。

```
dn: cn=constraint1, cn=unique, cn=common, cn=products, cn=oraclecontext
objectclass: orclUniqueConfig
orcluniqueattrname: employeenumber
orcluniquesubtree: o=Oracle Corporation, c=US
orcleuniqueobjectclass: person
```

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

```
ldapadd -h <host> -p <port> -D <dn> -w <password> -f constraint1.dat
```

3. ディレクトリ・サーバーを再起動します。

米国オラクル社の全従業員の従業員 ID に属性一意性が適用されます。

この制約を削除するには、次の手順を実行します。

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

既知の制限事項

レプリケーションと属性一意性に関して、属性一意性制約が Oracle Internet Directory レプリケーション環境にある場合は、各サーバーでの属性一意性制約の構成は慎重に行ってください。

単純なレプリケーション使用例

クライアント・アプリケーションによる変更はすべてサプライヤ・サーバーで実行されます。したがって、サプライヤ・サーバーの属性一意性制約を使用可能に設定してください。コンシューマ・サーバーで属性一意性制約を使用可能にする必要はありません。

コンシューマ・サーバーの属性一意性制約を使用可能にしても、Oracle Internet Directory サーバーの正しい動作を妨害することはありませんが、パフォーマンスが低下する可能性があります。

マルチマスター・レプリケーション使用例

マルチマスター・レプリケーション使用例では、2 台のマスターが、同じレプリカのサプライヤとコンシューマの両方として動作します。マルチマスター・レプリケーションでは、ゆるやかな一貫性をもつレプリケーション・モデルを使用します。1 台のサーバーの属性一意性制約を使用可能にしても、指定された時間に両方のマスターで属性値が一意であることは保証されません。1 台のサーバーのみで属性一意性制約を使用可能にすると、各レプリカに保持されているデータに不整合が生じる可能性があります。

属性一意性制約は、両方のマスターで使用可能にする必要があります。

ただし、それでも不整合な状態になる可能性があります。たとえば、両方のマスターで、それぞれのエントリを同じ属性値に変更することができます。後で、変更が別のノードにレプリケートされる際、競合が明白になります。この種の競合解消も考慮する必要があります。つまり、競合解消方法（競合の解消はレプリケーション・サーバーの責任であるかどうか）について判断を行う必要があります。

第 III 部

ディレクトリのセキュリティ

第 III 部では、ディレクトリ内のデータを保護する機能について説明します。また、企業およびホスティングされた環境にあるアプリケーションを管理するアクセス制御を確立する方法についても説明します。第 III 部は、次の章で構成されています。

- 第 11 章「ディレクトリ・セキュリティの概要」
- 第 12 章「Secure Sockets Layer (SSL) とディレクトリ」
- 第 13 章「ディレクトリ・アクセス制御」

ディレクトリ・セキュリティの概要

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

- データ整合性
- データ・プライバシー
- 認可
- 認証
- ディレクトリ認証用ユーザー・パスワードの保護
- パスワード・ポリシー

データ整合性

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

関連項目： SSL の詳細は、[第 12 章「Secure Sockets Layer \(SSL\) とディレクトリ」](#)を参照してください。

データ・プライバシー

Oracle Internet Directory は、SSL とともに使用可能な**公開鍵暗号**を使用して、送信時にデータが開示されないことを保証します。公開鍵暗号では、メッセージの送信側が受信側の公開鍵を使用して、メッセージを暗号化します。メッセージが送達されると、受信側は、受信側の秘密鍵を使用して、メッセージを復号化します。Oracle Internet Directory では特に、SSL によって使用可能な次の 2 つのレベルの暗号化をサポートします。

- DES40

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

- RC4_40

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

関連項目： SSL の詳細は、[第 12 章「Secure Sockets Layer \(SSL\) とディレクトリ」](#)を参照してください。

認可

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

アクセス制御情報アイテム (ACI) は、アクセス制御に関連する管理ポリシーを記録したディレクトリ・メタデータです。この情報は、ユーザーによる変更が可能な操作属性として、Oracle Internet Directory に格納されています。各属性は、[アクセス制御情報アイテム \(ACI\)](#) と呼ばれます。

通常、[アクセス制御リスト \(ACL\)](#) と呼ばれるこの ACI 属性値のリストは、ディレクトリ・オブジェクトと関連付けられています。このリストにある属性値によって、そのディレクトリ・オブジェクトに対するアクセス・ポリシーが管理されます。

ディレクトリ・オブジェクトに関連付けられているアクセス制御情報アイテム (ACI) は、様々なディレクトリ・ユーザー・エンティティ (対象) が、指定したオブジェクトに対して所有している権限を表しています。したがって、ACI は次のコンポーネントで構成されています。

- アクセス権限を付与するオブジェクト
- アクセス権限を付与するエンティティ (対象)
- 付与するアクセス権限の種類

アクセス制御ポリシー・ポイントは規定的です。つまり、そのセキュリティ・ディレクティブは、[ディレクトリ情報ツリー](#)内の下位エントリすべてに適用されるように設定できます。アクセス制御ポリシー・ポイントが適用される開始地点は、[アクセス制御ポリシー・ポイント \(ACP\)](#) と呼ばれます。

ACI は、ディレクトリ内にテキスト文字列として記述され、格納されています。この文字列は、ACI ディレクティブ書式と呼ばれる、明確に定義された書式に従う必要があります。ACI 属性の各有効値は、個別のアクセス制御ポリシー・ポイントを表します。

ホスティングされた環境で実行されているアプリケーションでは、ディレクトリ・アクセス制御の次の機能が使用できます。

- 規定のアクセス制御

サービス・プロバイダは、ディレクトリ・オブジェクトの集合に対してアクセス制御リスト (ACL) を指定できます。個々のオブジェクトごとにポリシーを設定する必要はありません。この機能によって、アクセス制御の管理が簡素化されます。特に同じポリシーまたは同等のポリシーで管理されるオブジェクトが多数含まれる大きなディレクトリで有効です。

- 階層的なアクセス制御管理のモデル

サービス・プロバイダは、サブスクライバにディレクトリ管理を委任できます。必要であれば、サブスクライバから委任することもできます。

- 委任ドメインに対する管理制御のオーバーライド

サービス・プロバイダは、アカウントの意図しないロックアウトやセキュリティの不慮の露見に対する診断とリカバリを実行できます。

- アクセス制御エンティティの動的評価

サブツリーの管理者は、対象とオブジェクトの双方を、その名前空間およびディレクトリのその他のオブジェクトとの関連の点で、識別できます。たとえば、サブスクライバ・サブツリーの管理者は、ユーザーの上司のみに、そのユーザーの給与属性の更新を認めることができます。他のサブスクライバ・サブツリーの管理者は、給与属性に関してこれとは異なるポリシーを確立して、適用できます。

認証

認証は、ディレクトリ・サーバーが、そのディレクトリに接続しているユーザーの正確な識別情報を設定するプロセスです。認証は、LDAPセッションが `ldapbind` 操作によって確立されたときに発生します。このようにして、すべてのセッションにユーザー ID が関連付けられます。

ユーザー、ホストおよびクライアントの ID を検証するために、Oracle Internet Directory では、直接認証と間接認証の 2 種類の一般的な認証を使用できます。

直接認証

3 種類の直接認証オプションがあります。

- 匿名認証

匿名で認証する場合、ユーザーは、ユーザー名とパスワードのフィールドを空白のままにしてログインします。各匿名ユーザーは、匿名ユーザーに付与されている権限すべてを使用できます。

- 簡易認証

簡易認証を使用する場合、クライアントは、ネットワーク上を暗号化されずに送信される識別名とパスワードによって、サーバーに対して自己認証を行います。

- Secure Sockets Layer (SSL) 認証

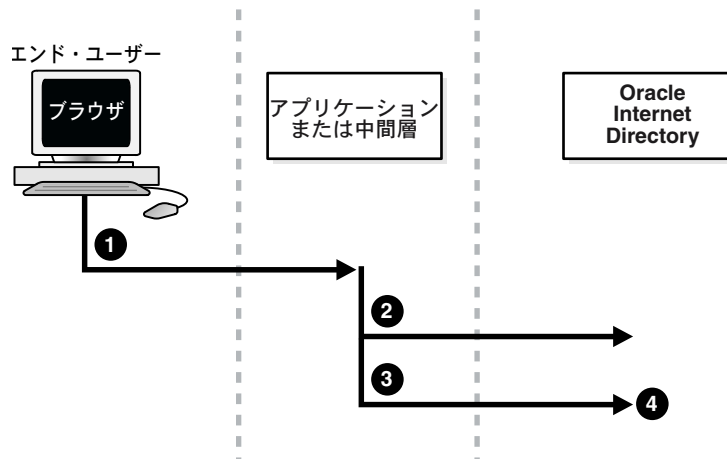
信用のある認証局が発行する証明書の交換が含まれます。

間接認証

間接認証は、ディレクトリに資格証明を保持するエンティティ（たとえば、Delegated Administration Service などのアプリケーション、またはファイアウォールや RADIUS サーバーなどの中間層）を介して発生します。アプリケーションまたは中間層は、エンド・ユーザーの代理である**プロキシ・ユーザー**となり、エンド・ユーザーのかわりにディレクトリ操作を実行します。

次の図 11-1 および図に続く説明は、間接認証がどのように実行されるかを示しています。

図 11-1 間接認証



間接認証は、次の手順で行われます。

1. エンド・ユーザーが、Oracle Internet Directory への問合せが含まれているリクエストをアプリケーションまたは中間層に送信します。アプリケーションまたは中間層がエンド・ユーザーを認証します。
2. アプリケーションまたは中間層がディレクトリにバインドします。
3. アプリケーションまたは中間層は、エンド・ユーザーの識別名を使用して、2 回目のバインドを実行します。この場合、エンド・ユーザーのパスワードは入力しません。
4. この 2 回目のバインドは、ディレクトリ・サーバーによって、アプリケーションまたは中間層がエンド・ユーザーの ID に切り替えようとしているものと認識されます。ディレクトリ・サーバーは、アプリケーションまたは中間層によってエンド・ユーザーに付与された認証を受け入れます。ただし、アプリケーションまたは中間層に、このユーザーのプロキシとなる権限があるかどうかを検証する必要があります。ディレクトリ・サーバーは、エンド・ユーザーのエントリを管理する ACP によって、このエンド・

ユーザーに対するプロキシ権限がこのアプリケーションまたは中間層に付与されているかどうかをチェックします。

- * アプリケーションまたは中間層が必要なプロキシ権限を持っている場合、ディレクトリ・サーバーは、認証 ID をエンド・ユーザーの認証 ID に変更します。後続するすべての操作は、そのエンド・ユーザーがサーバーに直接接続して直接認証された場合と同様に行われます。
- * アプリケーションまたは中間層が必要なプロキシ権限を持っていない場合、ディレクトリ・サーバーは、「アクセス権限が不十分です」というエラー・メッセージを戻します。

関連項目： 13-10 ページの「操作: 付与するアクセス権の種類」

ディレクトリ・サーバーは同一セッションで、その他のエンド・ユーザーを認証および許可できます。また、エンド・ユーザーのセッションから、そのセッションをオープンしたアプリケーションまたは中間層のセッションに切り替えることもできます。

セッションをクローズするには、アプリケーションまたは中間層がバインド解除要求をディレクトリ・サーバーに送信します。

たとえば、次の場合を想定します。

- `cn=User1` でディレクトリにバインドする中間層には、ディレクトリ全体に対するプロキシ・アクセス権限があります。
- `cn=User2` でディレクトリにバインドできるエンド・ユーザーがいます。

このエンド・ユーザーが、Oracle Internet Directory に対する問合せが含まれているリクエストをアプリケーションまたは中間層に送信すると、アプリケーションまたは中間層がエンド・ユーザーを認証します。その後、中間層サービスは、そのサービスの ID である `cn=User1` を使用してディレクトリにバインドし、次に、エンド・ユーザーの識別名 `cn=User2` のみを使用して 2 回目のバインドを実行します。この 2 回目のバインドは、Oracle ディレクトリ・サーバーでは、プロキシ・ユーザーがエンド・ユーザーの代理になろうとしているものと認識されます。Oracle ディレクトリ・サーバーは、`cn=user1` にプロキシ・アクセス権限があることを確認した後、この 2 回目のバインドの実行を許可します。パスワードなど、エンド・ユーザー識別名の妥当性をさらに要求することはありません。このセッションでは、これ以降すべての LDAP 操作は、`cn=User2` が実行しているかのようにアクセス制御されます。

先行ユーザーがサービスを受けている間に、このアプリケーションの別のユーザーがそのサービスをリクエストした場合、アプリケーションは、先行ユーザーのセッションを中断せずに、新規接続を確立して前述のとおり処理を進めることができます。ただし、先行ユーザーがサービスを受けていない場合は、新規接続を確立せずに既存の確立済み接続を何度も使用できます。

ディレクトリ認証用ユーザー・パスワードの保護

Oracle Internet Directory では、ユーザーのディレクトリ・パスワードを一方方向ハッシュ値として `userPassword` 属性に格納することで、そのパスワードを保護します。管理者は、使用するハッシング・アルゴリズムを選択します。パスワードを暗号値ではなく一方方向ハッシュ値として格納することによって、パスワードのセキュリティが向上します。これは、悪意のあるユーザーにはこれらの値を読むことも復号化することもできないためです。

関連項目： [「Oracle Internet Directory への認証用パスワード・ベリファイアの格納」](#)

パスワード・ポリシー

パスワード・ポリシーとは、パスワードの使用方法を定めた一連の規則のことです。ユーザーがディレクトリへのバインドを試みると、ディレクトリ・サーバーは、ユーザーのパスワードがパスワード・ポリシーの様々な要件に適合するかを確認します。

パスワード・ポリシーを確立する際は、次のような規則を設定します。なお、この規則はほんの一部です。

- 指定したパスワードの有効期限
- パスワードの最小必須文字数
- パスワードに必要な数字の文字数

関連項目： パスワード・ポリシーの確立で設定する規則の詳細は、[第 18 章「パスワード・ポリシー」](#)を参照してください。

Secure Sockets Layer (SSL) とディレクトリ

この章では、Oracle Internet Directory で使用するために Secure Sockets Layer (SSL) を構成する方法について説明します。SSL を使用すると、厳密認証、データ整合性およびデータ・プライバシーも構成できます。

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、2-12 ページの「[セキュリティ](#)」を参照してください。

サポートされている Cipher Suite

Cipher Suite は、ネットワーク・ノード間でのメッセージ交換に使用される認証、暗号化およびデータ整合性アルゴリズムのセットです。SSL ハンドシェイク時に、2 つのノード間で折衝し、メッセージを送受信するときに使用する Cipher Suite を確認します。

Oracle Internet Directory では、次の SSL Cipher Suite がサポートされています。

表 12-1 Oracle Internet Directory でサポートされている SSL Cipher Suite

Cipher Suite	認証	暗号化	データ整合性
SSL_RSA_WITH_3DES_EDE_CBC_SHA	RSA	DES40	SHA
SSL_RSA_WITH_RC4_128_SHA	RSA	RC4_40	SHA
SSL_RSA_WITH_RC4_128_MD5	RSA	なし	MD5
SSL_RSA_WITH_DES_CBC_SHA	RSA	なし	SHA
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA		3DES_EDE_CBC	SHA
SSL_DH_anon_WITH_RC4_128_MD5		RC4_40	MD5
SSL_DH_anon_WITH_DES_CBC_SHA		DES_CBC	SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5		RC4_40	MD5
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA		DES40	SHA
SSL_DH_anon_EXPORT_WITH_RC4_40_MD5		RC4_40	MD5
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA		DES40	SHA

SSL クライアントの使用例

Oracle Internet Directory のクライアントは、SSL 2.0 または SSL 3.0 を使用できます。SSL を使用するクライアントは、匿名または簡易認証あるいは厳密認証を使用してサーバーに接続できます。

クライアントとサーバーの双方が相互に自己認証を行うと、SSL は 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

ディレクトリ・サーバー・インスタンスの起動時に、SSL プロファイルのパラメータを含む 1 セットの構成パラメータがディレクトリに読み込まれます。SSL が使用可能な状態でこのディレクトリを実行する場合は、**構成設定エントリ**の SSL パラメータを確認する必要があります（多くの場合、再構成が必要です）。

サーバー・インスタンスを保護モードで実行するには、構成設定の「SSL 使用可能」パラメータを 1（デフォルトの保護ポートは 636）に設定します。同一のインスタンスを同時に非保護接続で実行できるようにするには、「SSL 使用可能」を 2（デフォルトの非保護ポートは 839）に設定します。

管理者は、異なる値を持つ複数の構成パラメータのセットを作成および変更し、Oracle Internet Directory のインスタンスごとに異なる構成設定エントリを使用できます。これは、セキュリティ・ニーズの異なるクライアントを制御する便利な方法です。

SSL の値を変更するときは、デフォルトの構成設定にある SSL の値を変更するのではなく、別の構成設定を作成して、その SSL の値を変更する方法をお勧めします。デフォルトの構成設定は、技術的な問題を診断するときにオラクル社カスタマ・サポート・センターで必要となる場合があります。

関連項目：

- これらのパラメータの設定方法は、5-2 ページの「**サーバーの構成設定エントリの管理**」を参照してください。
- これらのパラメータの説明は、C-5 ページの「**構成設定エントリの属性**」を参照してください。

Oracle Directory Manager を使用した SSL パラメータの構成

作成した各構成設定エントリおよび現在実行中の各サーバー・インスタンスの SSL 構成パラメータの値を、確認および変更できます。

注意： アクティブ・インスタンスのパラメータを直接変更することはできません。アクティブ・インスタンスのパラメータを変更する場合は、構成設定エントリ内のパラメータを変更して、それを保存してください。保存後は、現行のインスタンスを停止して、サーバーの起動メッセージ内にある新たに変更された構成設定を参照できます。

SSL 構成パラメータを表示および変更する手順は、次のとおりです。

1. Oracle Directory Manager のナビゲータ・ペインで、「Oracle Internet Directory サーバー」>「ディレクトリ・サーバー」>「サーバーの管理」の順に展開します。
2. 「ディレクトリ・サーバー」または「レプリケーション・サーバー」の適切な項目を展開します。選択した項目の下に、番号付きの構成設定が表示されます。
3. 検証する構成設定を選択します。その構成設定エントリに対応するタブ・ページが右側のペインに表示されます。
4. 「SSL 設定」タブ・ページを選択します。

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

フィールド	説明
SSL/non-SSL Enable	非保護操作のみの場合は 0（ゼロ）を設定します。デフォルト・ポートは 839 で、この値未満に変更可能です。 SSL 認証のみの場合は 1 を設定します。デフォルト・ポートは 636 で、この値未満に変更可能です。 非保護操作と SSL 認証の両方の場合は 2 を設定します。
SSL 認証	次の中から 1 つ選択します。 <ul style="list-style-type: none">■ SSL 認証なし: クライアントとサーバーのいずれも、相手に対して自己認証を行いません。証明書の送信または交換は行われません。この場合は、SSL 暗号化 / 復号化のみ使用されます。■ SSL クライアントとサーバーの認証: クライアントとサーバーは相互に自己認証を行い、相互に証明書を送信します。■ SSL サーバー認証: ディレクトリ・サーバーのみ、クライアントに対して自己認証を行います。ディレクトリ・サーバーは、そのサーバーが認証されていることを証明する証明書をクライアントに送信します。

フィールド	説明
SSL Wallet URL	<p>サーバー側の SSL Wallet の位置を入力します。Wallet の位置を変更する場合は、このパラメータを変更する必要があります。クライアントとサーバーの両方で Wallet の位置を設定する必要があります。たとえば Solaris では、このパラメータは次のように設定します。</p> <pre>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 パスワード	<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 ポート	<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>
Non-SSL Port	<p>デフォルトの非 SSL ポートは 839 です。非 SSL ポートは変更できます。</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： 5-11 ページの「[コマンドライン・ツールを使用したサーバー構成設定エントリの管理](#)」

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

同じホストで、SSL クライアントと非 SSL クライアントの両方をサポートする場合は、2 つの別々のサーバー・インスタンスを構成する必要があります。

Oracle Internet Directory リリース 9.0.2 では、Oracle ディレクトリ・レプリケーション・サーバーは、SSL 対応の Oracle ディレクトリ・サーバー・インスタンスとは直接通信できません。

関連項目： サーバー・インスタンスの構成方法は、[第 5 章「Oracle ディレクトリ・サーバーの管理」](#)を参照してください。

ディレクトリ・アクセス制御

この章では、アクセス制御ポリシー・ポイントの概要および Oracle Directory Manager またはコマンドライン・ツール `ldapmodify` を使用して、ディレクトリのアクセス制御を管理する方法について説明します。

この章では、次の項目について説明します。

- [アクセス制御ポリシー・ポイントの管理の概要](#)
- [Oracle Directory Manager を使用したアクセス制御の管理](#)
- [コマンドライン・ツールを使用したアクセス制御の管理](#)
- [ACL 評価の動作](#)

関連項目：

- アクセス制御ポリシー・ポイントの実装と管理を始める前の概要は、2-13 ページの「[グローバルゼーション・サポート](#)」を参照してください。
- アクセス制御情報アイテム (ACI) の書式 (構文) の詳細は、[付録 B 「アクセス制御ディレクティブ書式」](#) を参照してください。

アクセス制御ポリシー・ポイントの管理の概要

アクセス制御ポリシー・ポイントは、対応するエントリ内の **ACI** 属性の値を構成して管理します。そのためには、Oracle Directory Manager または ldapmodify のいずれかを使用します。

この項では、次の項目について説明します。

- [アクセス制御管理の構造体](#)
- [アクセス制御情報アイテム \(ACI\) のコンポーネント](#)

アクセス制御管理の構造体

この項では、Oracle Internet Directory でアクセス制御に使用される構造について説明します。たとえば次のようなものです。

- アクセス制御ポリシー・ポイント (ACP)
- 規定のアクセス制御のための orclACI 属性
- エントリ・レベルのアクセス制御のための orclEntryLevelACI 属性
- 権限グループ

アクセス制御ポリシー・ポイント (ACP)

ACP は、orclACI 属性が指定されたエントリです。orclACI 属性の値は、エントリのサブツリーによって継承されるアクセス・ポリシーを示します。エントリのサブツリーは、そのサブツリーのルートとなる ACP から始まります。

ディレクトリ・サブツリー内に複数の ACP の階層が存在する場合、そのサブツリー内の従属エントリは、すべての上位 ACP からアクセス・ポリシーを継承します。継承結果のポリシーは、そのエントリより上位の ACP 階層内のポリシーを集約したものです。

たとえば、HR 部門のエントリに ACP が設定されており、HR 部門内に、Benefits、Payroll および Insurance グループのエントリがある場合、この 3 つのグループ内のエントリはいずれも、HR 部門のエントリに指定されたアクセス権を継承します。

ACP の階層内に競合するポリシーがある場合、ディレクトリは、集約したポリシーの評価には明確に定義された優先順位規則を適用します。

関連項目： 13-44 ページの「[ACL 評価の動作](#)」

規定のアクセス制御のための orclACI 属性

orclACI 属性には、規定の[アクセス制御リスト](#)ディレクティブが含まれています。つまりこのディレクティブは、この属性が定義されている ACP より下位のサブツリー内にあるすべてのエントリに適用されます。ディレクトリ内のあらゆるエントリに、この属性の値を含

めることができます。この属性自体へのアクセスは、他の属性に対するアクセスと同様に制御されます。

注意： 単一のエントリ固有の ACL ディレクティブを `orclACI` 属性で示すことができます。ただし、その場合には管理の容易さとパフォーマンス上の利点から、13-3 ページの「[エントリ・レベルのアクセス制御のための `orclEntryLevelACI` 属性](#)」で説明する `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。

エントリ・レベルのアクセス制御のための `orclEntryLevelACI` 属性

あるポリシーが特定のエンティティ（例：特別のユーザー）のみに関係するとき、単一のエントリ内で、そのエントリに固有の ACL ディレクティブをメンテナンスできます。Oracle Internet Directory では、`orclEntryLevelACI` と呼ばれるユーザーが変更可能な操作属性を使用して前述のディレクティブを管理できます。`orclEntryLevelACI` 属性には、関連付けられたエントリにのみ適用される ACL ディレクティブが含まれます。

いずれのディレクトリ・エントリにも、この属性の値をオプションで設定できます。それは、Oracle Internet Directory が抽象型クラス `top` を拡張し、オプション属性として `orclEntryLevelACI` を組み込むからです。

`orclEntryLevelACI` 属性は複数値の属性で、構造は `orclACI` と類似しています。構造の定義については、この章で後述します。

アクセス制御グループ

Oracle Internet Directory 内のグループ・エントリは、`groupOfNames` オブジェクト・クラスまたは `groupOfUniqueNames` オブジェクト・クラスのいずれかと関連付けられます。グループ内のメンバーシップは、それぞれ `member` 属性または `uniqueMember` 属性の値として指定されます。

個人またはエンティティのグループにアクセス権を指定するには、アクセス制御グループでそのグループを識別します。アクセス制御グループには、ACP グループと権限グループの 2 つのタイプがあります。

ACP グループ 個人が ACP グループのメンバーである場合、ディレクトリ・サーバーは、その ACP グループに関連付けられている権限をその個人に単純に付与します。

ACP グループを使用して、ACP のレベルでアクセス権を解決します。たとえば、エントリを参照できるアクセス権を数百ものユーザーに付与すると仮定します。参照権限を各エントリに個別に付与することもできますが、この作業には相当な管理オーバーヘッドが必要となります。さらに、後日その権限の変更が決定した場合は、各エントリを個々に修正する必要があります。より効率的な解決策は、権限を集散的に割り当てることです。そのためには、

グループ・エントリを作成して ACP グループとして指定し、必要な権限をそのグループに割り当てた後、ユーザーをそのグループのメンバーに割り当てます。その後、アクセス権を変更する場合は、個々のユーザーに対してではなく、グループに対して 1 箇所で変更を行います。同様に、権限を削除する場合は、多数の各エントリにアクセスするのではなく、グループから権限を削除することによって、複数のユーザーから権限を削除できます。

ACP グループは、`orclacpgroup` オブジェクト・クラスに関連付けられています。

権限グループ 権限グループは、上位レベルのアクセス・グループです。同様の権限を持つユーザーを管理する点では、ACP グループと類似しています。ただし、権限グループは、単一の ACP 以外に追加チェックを提供します。たとえば、ある ACP によってアクセスが制限される場合、ディレクトリ・サーバーは、アクセスを制限されるユーザーがいずれかの権限グループに属しているかどうかをユーザー・エントリの属性によって判断します。権限グループに属している場合、このユーザーには上位管理レベルで別途の権限があるため、ディレクトリ情報ツリーで上位管理レベルすべてがチェックされます。要求したオブジェクトへのアクセス権を権限グループに付与することを示す上位 ACP が見つかった場合、ディレクトリ・サーバーは、下位 ACP による制限を無視してアクセス権をユーザーに付与します。

通常は、ACP グループのみを実装します。権限グループが提供する追加チェックは、パフォーマンスを低下させる可能性があります。下位レベルの標準的な制御よりも上位レベルのアクセス制御を優先させる権限が必要な場合にのみ、権限グループを使用します。

権限グループを使用して、ディレクトリ情報ツリーの下位 ACP では認識されない管理者に対して、アクセス権を付与します。たとえば、ホスティングされた環境のグローバル管理者が、サブスクライバのサブツリーで操作を行う必要があると仮定します。グローバル管理者の ID はサブスクライバのサブツリーでは認識されないため、そのサブツリーの ACP のみに依存している場合、ディレクトリ・サーバーによって必要なアクセスが制限されます。ただし、グローバル管理者が権限グループのメンバーである場合、ディレクトリ・サーバーは、ディレクトリ情報ツリーで上位で、そのサブツリーへのアクセス権をこの権限グループに付与している ACP を検索します。アクセス権を付与している ACP が見つかった場合、ディレクトリ・サーバーは、サブスクライバのサブツリーにある ACP による制限を無視します。

権限グループは、`orclPrivilegeGroup` オブジェクト・クラスに関連付けられています。

両方のタイプのグループに属するユーザー ユーザーが ACP グループと権限グループの両方のメンバーの場合、ディレクトリ・サーバーは、各タイプのグループについて評価を行います。ディレクトリ・サーバーは、ディレクトリ情報ツリーで上位の ACP に注目して、権限グループのアクセス権を解決します。

概要：グループへのアクセス権の付与 アクセス権をユーザーのグループに付与する手順は、次のとおりです。

1. 通常の方法でグループ・エントリを作成します。
2. グループ・エントリを `orclPrivilegeGroup` オブジェクト・クラスまたは `orclACPgroup` オブジェクト・クラスに関連付けます。
3. そのグループのアクセス・ポリシーを指定します。

4. メンバーをグループに割り当てます。

ディレクトリ・サーバーによるアクセス制御グループ・メンバーシップの検出方法 エントリは、グループの直接のメンバーとなるか、またはグループをネストして権限グループの一群を形成し、他の ACP または権限グループの間接のメンバーとなることができます。与えられたレベルで指定されているアクセス・ポリシーは、そのレベル以下のすべてのメンバーに直接的または間接的に適用されます。

Oracle Internet Directory は、アクセス制御グループのみをアクセス制御目的で評価するため、その他のタイプのグループに対してアクセス・ポリシーを設定できません。ユーザーが特定の識別名とバインドされると、Oracle Internet Directory は、アクセス制御グループ内でそのユーザーの直接のメンバーシップを検出します。指定した識別名の第 1 レベルのグループを認識すると、Oracle Internet Directory は、この第 1 レベルのグループすべての、他のアクセス制御グループに対するネストを検出します。この処理は、評価対象のネストされたグループがなくなるまで行われます。

各アクセス制御グループ（ネストされているかどうかに関係なく）は、アクセス制御グループのオブジェクト・クラス（`orclACPgroup` または `orclPrivilegeGroup`）に関連付けられている必要があります。グループがアクセス制御グループのメンバーの場合でも、アクセス制御グループのオブジェクト・クラスに関連付けられていないかぎり、ディレクトリ・サーバーではアクセス制御目的のグループとはみなされません。アクセス制御グループ内でユーザーのメンバーシップが判断された場合、ディレクトリ・サーバーでは、セッションの存続期間にわたってその情報を使用します。

例：アクセス制御グループ・メンバーシップの検出 たとえば、次のエントリのグループを仮定します。group4 以外は、それぞれ権限グループ（`objectclass:orclprivilegeGroup`）として指定されています。管理者は、group1、group2 および group3 のメンバーに適用されるアクセス制御ポリシー・ポイントを設定できます。

group 1

```
dn:cn=group1, c=us
cn:group1
objectclass:top
objectclass:groupofUniquenames
objectclass:orclprivilegeegroup
uniquemember:cn=mary smith, c=us
uniquemember:cn=joe smith, c=us
uniquemember:cn=bill smith, c=us
```

group 2

```
dn:cn=group2, c=us
cn:group2
objectclass:top
objectclass:groupofUniquenames
objectclass:orclprivilegeegroup
uniquemember:cn=mary jones, c=us
uniquemember:cn=joe jones, c=us
uniquemember:cn=bill jones, c=us
```

group 3

```
dn:cn=group3, c=us
cn:group3
objectclass:top
objectclass:groupofUniquenames
objectclass:orclprivilegeegroup
uniquemember:cn=group2, c=us
uniquemember:cn=group1, c=us
uniquemember:cn=group4, c=us
```

group 4

```
dn:cn=group4, c=us
cn:group4
objectclass:top
objectclass:groupofUniquenames
uniquemember:cn=john doe, c=uk
uniquemember:cn=jane doe, c=uk
uniquemember:cn=anne smith, c=us
```

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・ポイントは、`group3`、`group1` および `group2` のメンバーに適用されます。これは、各グループが権限グループとして指定されているためです。この同じアクセス制御ポリシー・ポイントは、`group4` のメンバーには適用されません。これは、`group4` は権限グループとして指定されていないためです。

たとえば、ユーザーが識別名 `cn=john smith, c=uk` で `group 4` のメンバーとして Oracle Internet Directory にバインドされている場合を考えてみます。`group3` のメンバーに適用されるアクセス・ポリシーがこのユーザーに適用されることはありません。これは、このユー

ザーの唯一の直接メンバーシップが非権限グループに対するものであるためです。これに対して、ユーザーが `cn=john smith,c=us`、つまり、`group1` と `group2` のメンバーとしてバインドされている場合、そのアクセス権は `group1`、`group2` および `group3` (`group1` と `group2` がネストされているため) のメンバーに対して設定されているアクセス・ポリシーで管理されます。これは、この 3 つのグループすべてがオブジェクト・クラス `orclPrivilegeGroup` と関連付けられているためです。

アクセス制御情報アイテム (ACI) のコンポーネント

ACI とは、様々なエンティティまたは対象がディレクトリ内の指定されたオブジェクトに対して操作を行う必要がある権限を表します。したがって、ACI は次の 3 つのコンポーネントで構成されています。

- アクセス権を付与するオブジェクト
- アクセス権を付与するエンティティ (対象)
- 付与するアクセス権の種類

オブジェクト: アクセス権を付与するオブジェクト

アクセス制御ディレクティブのオブジェクト部分は、そのアクセス制御が適用されるエントリと属性を決定します。エントリまたは属性のいずれかに適用できます。

ACI に関連付けられているエントリ・オブジェクトは、ACI 自体が定義されているエントリまたはサブツリーによって暗黙的に識別されます。属性のレベルにおけるその他の条件は、ACL 式で明示的に指定されます。

`orclACI` 属性においては、ACI のオブジェクトのエントリ識別名コンポーネントは、暗黙的に、最上位のエントリの ACP から始まるサブツリー内のエントリすべての識別名コンポーネントです。たとえば、`dc=com` が ACP の場合、その ACI で管理されるディレクトリ領域は次のようになります。

`.*, dc=com.`

ただし、ディレクトリ領域は暗黙的であるため、この識別名コンポーネントは不要で、構文的にも許可されません。

`orclEntryLevelACI` 属性においては、ACL のオブジェクトのエントリ識別名コンポーネントは、暗黙的にエントリ自体の識別名コンポーネントです。たとえば、`dc=acme,dc=com` にエントリ・レベルの ACI が関連付けられている場合、その ACI が管理しているエントリは `dc=acme,dc=com` そのものです。ただし、これは暗黙的であるため、この識別名コンポーネントは不要で、構文的にも許可されません。

ACL のオブジェクト部分は、次のようにエントリ内の属性と一致させるフィルタによって、エントリをオプションで限定できます。

```
filter=(ldapFilter)
```

`ldapFilter` は、LDAP 検索フィルタの文字列を表しています。特別なエントリ・セクタ * 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は、特別なオブジェクト・キーワード `ENTRY` を使用して、付与または否認する必要があります。属性に対してアクセス権を付与するのみでは不十分で、`ENTRY` キーワードを指定してエントリ自体にアクセス権を付与する必要があることに注意してください。

関連項目： ACI の書式（構文）の詳細は、[付録 B「アクセス制御ディレクティブ書式」](#) を参照してください。

対象：アクセス権を付与する対象

この項では、次の項目について説明します。

- アクセス権が付与されるエンティティ
- バインド・モード（つまり、そのエンティティ識別情報の検証に使用される認証モード）
- オブジェクト追加制約（アクセス権を付与されたユーザーが、親の下に追加できるオブジェクトの種類の制限）

エンティティ アクセス権は、エントリではなくエンティティに対して付与されます。エンティティ・コンポーネントは、アクセス権が付与されているエンティティを指定します。

直接または間接的にエンティティを指定できます。

エンティティの直接指定： この方法は、実際のエンティティ値の入力（たとえば、`group=managers`）を必要とします。次の要素を使用して値を入力します。

- 任意のエントリと一致するワイルド・カード文字（*）
- アクセス権によって保護されているエントリと一致するキーワード `SELF`
- エントリの識別名と一致する正規表現（たとえば、`dn=regex`）

- 権限グループ・オブジェクトのメンバー (group=dn)

エンティティの間接指定：これはエンティティを動的に指定する方法です。アクセス権を付与しているエントリの一部である識別名値属性を指定する必要があります。識別名値属性には次の3つのタイプがあります。

- **dnattr**: この属性を使用して、このエントリに対してアクセス権を付与または制限しているエンティティの識別名を指定します。
- **groupattr**: この属性を使用して、このエントリに対してアクセス権を付与または制限している管理グループの識別名を指定します。
- **guidattr**: この属性を使用して、このエントリに対してアクセス権を付与または制限するエントリのグローバル・ユーザー識別子 (orclGUID) を指定します。

たとえば、Anne Smith のマネージャが彼女のエントリで給与属性を変更できるように指定する場合を想定します。マネージャの識別名を直接指定するかわりに、識別名値属性を指定します (dnattr=<manager>)。次に、John Doe が Anne の給与属性を変更しようとする、ディレクトリ・サーバーでは次の処理が実行されます。

- Anne のマネージャ属性の値を参照し、John Doe であることを確認します。
- バインド識別名とマネージャ属性が一致することを確認します。
- 適切なアクセス権を John Doe に付与します。

バインド・モード バインド・モードは、対象が使用する認証方法を指定します。次の4つのモードがあります。

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

バインド・モードの指定はオプションです。ディレクトリ・サーバーは、ユーザーのバインド・モードが、ユーザーが通信しようとするノードのバインド・モードと互換性があるかどうかを検証します。あるノードで指定されているバインド・モードは、通信先のノードで指定されているバインド・モードと一致している必要があります。たとえば、一方のノードで SSLTwoWay 認証を指定する場合は、もう一方のノードもこのタイプの認証を行うように構成する必要があります。

オブジェクト追加制約 親エントリに追加アクセス権がある場合、階層内の下位エントリとしてオブジェクトを追加できます。オブジェクト追加制約は、*ldapfilter* を指定することによって、追加アクセス権を制限するために使用できます (付録 B「アクセス制御ディレクトリ書式」および付録 G「LDAP フィルタ定義」を参照してください)。

操作 : 付与するアクセス権の種類

付与するアクセス権の種類は次のいずれかです。

- なし
- Compare/nocompare
- Search/nosearch
- Browse/nobrowse
- Proxy/noproxy
- Read/noread
- Selfwrite/noselfwrite
- Write/nowrite
- Add/noadd
- Delete/nodelete

各アクセス・レベルを個々に付与または否認できることに注意してください。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。

エントリに関連付けられているアクセス権と、属性に関連付けられているアクセス権があることに注意してください。

アクセス・レベル	説明	オブジェクトのタイプ
比較	属性値で比較操作を実行する権限。	属性
読み込み	属性の値を読み込む権限。属性に対して読取り権限が与えられている場合でも、エントリ自体にブラウズ権限がないかぎり値は戻されません。	属性
検索	検索フィルタで属性を使用する権限。	属性
自己書き込み	識別名のグループ・エントリ属性のリスト内で、ユーザー自身の追加 / 削除あるいは自身のエントリを変更を行う権限。このレベルを使用すると、メンバーがリスト上の自分自身をメンテナンスできます。たとえば次のコマンドを実行すると、グループ内のユーザーが member 属性上で、自分自身の識別名のみを追加または削除できます。 access to attr=(member) by dnattr=(member) (selfwrite) dnattr セレクタは、member 属性にリストされているエンティティにアクセス権が適用されるように指定します。selfwrite アクセス権セレクタは、そのメンバーが、属性上で自分自身の識別名のみを追加または削除できるように指定します。	属性
書き込み	エントリの属性を変更 / 追加 / 削除する権限。	属性

アクセス・レベル	説明	オブジェクトのタイプ
なし	アクセス権なし。対象とオブジェクトの組合せにアクセス権を付与しない場合、対象にとってオブジェクトがそのディレクトリに存在しないかのように見えるという効果があります。	エン트리および属性
追加	ターゲットのディレクトリ・エントリの下にエントリを追加する権限。	エントリ
プロキシ	別のユーザーの代理となる許可。	エントリ
参照	検索結果に識別名を戻すための権限。X.500 のリスト権限と同等です。この権限は、クライアントがエントリの識別名を <code>ldapsearch</code> 操作でベース識別名として使用するときにも必要です。	エントリ
削除	ターゲットのエントリを削除する権限。	エントリ

エントリ・レベルのアクセス・ディレクティブは、オブジェクト・コンポーネント内のキーワード `ENTRY` で識別されます。

注意： デフォルトのアクセス制御ポリシー・ポイントでは、エントリおよび属性の両方を対象に、すべての人に、エントリ内の全属性の「読み込み」、「検索」、「書き込み」および「比較」の各アクセス権が付与されており、「自己書き込み」権限は未指定です。エントリが未指定の場合、アクセス権は、そのアクセス権が指定されている直近の上位レベルで判断されます。

Oracle Directory Manager を使用したアクセス制御の管理

ACP 内のアクセス制御情報アイテム (ACI) は、Oracle Directory Manager またはコマンドライン・ツールを使用して表示および変更できます。この項では、Oracle Directory Manager でこれらのタスクを実行する方法について説明します。

注意： Oracle Internet Directory のインストール直後に、3-9 ページの「[タスク 3: デフォルト・セキュリティ構成の再設定](#)」の説明に従ってデフォルトのセキュリティ構成を必ずリセットしてください。

この項では、次の項目について説明します。

- [アクセス制御管理のための Oracle Directory Manager の構成](#)
- [Oracle Directory Manager を使用した ACP の表示](#)
- [Oracle Directory Manager を使用した ACP の追加](#)
- [Oracle Directory Manager の ACP 作成ウィザードを使用した ACP の追加](#)
- [Oracle Directory Manager を使用した ACP の変更](#)
- [Oracle Directory Manager を使用したエントリ・レベルのアクセス権の付与](#)
- [例: Oracle Directory Manager を使用した ACP の管理](#)

関連項目： コマンドライン・ツールの説明は、[付録 A 「LDIF およびコマンドライン・ツールの構文」](#) を参照してください。

アクセス制御管理のための Oracle Directory Manager の構成

Oracle Directory Manager での ACP の表示方法および ACP 検索の実行方法を構成できます。

Oracle Directory Manager の ACP の表示の構成

Oracle Directory Manager では、ナビゲータ・ペインですべての ACP を自動的に表示するか、検索の結果としてのみ表示するかを決められます。ACP の数が多い場合は、検索の結果としてのみ表示できます。

ACP の表示を構成する手順は、次のとおりです。

1. ナビゲータ・ペインで「Oracle Internet Directory サーバー」を展開して、構成するサーバーを選択します。
2. ツールバーの「ユーザー設定項目」をクリックします。「ユーザー設定項目」ダイアログ・ボックスが表示されます。
3. 「アクセス制御ポリシー管理の構成」タブ・ページを選択します。

4. 次のいずれかを選択します。
 - 「常にすべての ACP を表示」
 - 「検索要求に基づく ACP のみ表示」
5. 「OK」をクリックします。

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

Oracle Directory Manager を使用する場合の ACP の検索の構成

Oracle Directory Manager では、ACP の検索に次の項目が指定できます。

- 検索のルート
- 取り出されるエントリの最大数
- 検索の制限時間
- 検索の深さ

ACP エントリの検索を構成する手順は、次のとおりです。

1. ナビゲータ・ペインで「Oracle Internet Directory サーバー」を展開し、「*directory server instance*」を選択します。
2. ツールバーの「ユーザー設定項目」を選択します。「ユーザー設定項目」ダイアログ・ボックスが表示されます。
3. 「エントリ管理の構成」タブを選択します。
4. 「1 レベルのサブツリー・エントリの最大数」のラベルが付いているフィールドに、ACP 検索で取得するエントリ数を入力します。
5. 「最大の検索時間」フィールドに、検索の最大時間を秒単位で入力します。
6. 「OK」をクリックします。

Oracle Directory Manager を使用した ACP の表示

13-12 ページの「[Oracle Directory Manager の ACP の表示の構成](#)」の説明に従って常に ACP を表示するように Oracle Directory Manager を構成した場合、ACP の位置を特定および表示する手順は、次のとおりです。

1. ナビゲータ・ペインで「Oracle Internet Directory サーバー」>「*directory server instance*」>「アクセス制御管理」の順に展開します。定義したすべての ACP は、いずれもナビゲータ・ペインの「アクセス制御管理」の下に表示されます。

2. ナビゲータ・ペインで「アクセス制御管理」の下 の ACP を選択すると、その情報が右側のペインに表示されます。

「アクセス制御管理」ペインには次の 3 つのフィールドがあります。

フィールド	説明
サブツリー制御ポイントへのパス	ACP で定義されているパスが表示されます。このポイントまでツリーを下位方向へナビゲートすると、このポイントへのパスがこのフィールドに表示されます。新しい ACP を作成する場合は、このフィールドに新規 ACP へのパスを入力する必要があります。
構造型アクセス項目 (エントリ・レベル操作)	<p>エントリへのアクセス権のリストです。「構造型アクセス項目」ボックスにリストされている項目は、次のカテゴリによってエントリを識別します。</p> <ul style="list-style-type: none">■ 責任者: アクセス権を付与する人またはエンティティ (対象)■ バインド・モード: バインド・モード (認証) が使用されているかどうか■ アクセス権限: 「参照」、「追加」、「プロキシ」 および 「削除」 <p>関連項目: 構造的なアクセス項目の変更方法は、13-29 ページの「タスク 2: 構造型アクセス項目の変更」を参照してください。</p>
コンテンツ・アクセス項目 (属性レベル操作)	<p>「エントリ・フィルタ」列に定義されているエントリまたはエンティティ内の属性に対するアクセス権のリストです。このウィンドウには次の列があります。</p> <ul style="list-style-type: none">■ 責任者: アクセス権を付与する人またはエンティティ (対象)■ バインド・モード: バインド・モード (認証) が使用されているかどうか■ Op: 属性に対して実行される一致操作。選択肢は「EQ」(=) と「NEQ」(!=) です。■ 属性: アクセス権が付与または否認される特定の属性 (オブジェクト)。■ アクセス権限: 「読み込み」、「検索」、「書き込み」、「自己書き込み」または「比較」。 <p>関連項目: コンテンツ・アクセス項目の変更方法は、13-33 ページの「タスク 3: コンテンツ・アクセス項目の変更」を参照してください。</p>

13-12 ページの「[Oracle Directory Manager の ACP の表示の構成](#)」の説明に従って検索の結果としてのみ ACP を表示するように Oracle Directory Manager を構成した場合に、ACP の位置を特定して表示する手順は、次のとおりです。

1. 「Oracle Internet Directory サーバー」 > 「*directory server instance*」の順に展開し、「エン트리管理」を選択します。ACP として指定したエントリの検索を実行します。検索結果が右側ペインの下半分の「識別名」ボックスに表示されます。
2. 「識別名」ボックスで、エントリをダブルクリックします。対応する「エン트리」ダイアログ・ボックスが表示されます。
3. この ACP のサブツリーのアクセス制御を表示するには、「サブツリー・アクセス」タブを選択します。

この ACP のエントリ・レベルのアクセス制御を表示するには、「ローカル・アクセス」タブを選択します。

Oracle Directory Manager を使用した ACP の追加

ACP は、規定の、すなわち継承可能なアクセス制御情報アイテム (ACI) を含んだエントリです。この情報は、エントリ自体とその下位エントリすべてに影響を与えます。一般的に、サブツリー全体にわたる規模の大きいアクセス制御をブロードキャストする ACP を作成します。

Oracle Directory Manager を使用して ACP を追加するには、次の 3 つのタスクが必要です。

- タスク 1: ACP にするエントリを指定します。
- タスク 2: 構造型アクセス項目（つまり、エントリに関係する ACI）を構成します。
- タスク 3: コンテンツ・アクセス項目（つまり、属性に関係する ACI）を構成します。

タスク 1: ACP にするエントリの指定

1. 13-12 ページの「[Oracle Directory Manager の ACP の表示の構成](#)」の説明に従って常に ACP を表示するように Oracle Directory Manager を構成した場合は、次のように開始します。

- a. ナビゲータ・ペインで「Oracle Internet Directory サーバー」 > 「*directory server instance*」の順に展開します。
- b. 「アクセス制御管理」を選択し、ステップ 2 に進みます。

13-12 ページの「[Oracle Directory Manager の ACP の表示の構成](#)」の説明に従って検索の結果としてのみ ACP を表示するように Oracle Directory Manager を構成した場合は、次のように開始します。

- a. ナビゲータ・ペインで「Oracle Internet Directory サーバー」 > 「*directory server instance*」 > 「アクセス制御管理」の順に展開します。
- b. ACP を常駐させるノードを選択します。構成された ACP が存在しない場合は、「DSE ルート」の下に ACP を選択できます。

2. ツールバーの「作成」ボタンをクリックします。「新規アクセス制御ポイント」ダイアログ・ボックスが表示されます。

- 3. 「エントリーへのパス」フィールドで、ACP に指定するエントリーの識別名を入力します。次のいずれかの方法で、識別名を検索できます。
 - 「エントリーへのパス」フィールド右側の「参照」をクリックします。
 - 「エントリー管理」の下ナビゲータ・ペインを検索します。

タスク 2: 構造型アクセス項目の構成

- 1. 構造型アクセス項目（つまり、エントリーに関する ACI）を定義するには、「構造型アクセス項目」ウィンドウの下「作成」をクリックします。「構造型アクセス項目」ダイアログ・ボックスが表示されます。このダイアログ・ボックスには、「エントリー・フィルタ」、「追加されたオブジェクト・フィルタ」、「責任者」および「アクセス権限」の 4 つのタブがあります。
- 2. ACP の下位エントリーすべてを ACP で管理する場合は、「エントリー・フィルタ」タブ・ページには何も入力せず、次のステップに進みます。

ACP では、定義されたアクセス権は、他のフィルタによりアクセスがそれ以上制限されないかぎり、このエントリーおよびそのエントリーのすべてのサブエントリーに適用されます。適切な場合、「エントリー・フィルタ」タブ・ページを使用して、アクセスを指定するエントリーを識別します。

エントリーへのアクセスを、このエントリーの 1 つ以上の属性に基づいて制限できます。たとえば、役職名がマネージャで組織単位がアメリカであるすべてのエントリーへのアクセスを制限できます。

アクセスを指定するエントリーを識別する手順は、次のとおりです。

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

フィルタ	説明
開始	属性値の始めの数文字のみを使用して検索します。
終了	指定した属性値の終わりの数文字のみを使用してエントリーを検索します。
含む	値の位置を限定せずに、ユーザーの入力値が指定した属性に含まれているエントリーを検索します。
完全一致	指定した属性がユーザーの入力値に一致するエントリーを検索します。
以上	指定した属性が、数値順またはアルファベット順で入力値より大か等しいエントリーを検索します。アルファベットの先頭により近いエントリーが、アルファベット順で上位とされます。
以下	指定した属性が、数値順またはアルファベット順で入力値より小か等しいエントリーを検索します。アルファベットの先頭により近いエントリーが、アルファベット順で下位とされます。

フィルタ	説明
存在	指定した属性を持つエントリが、ツリーのそのレベルに存在するかどうかを判断します。この関連の使用に値の入力は不要です。たとえば、「cn」「存在」と指定すると、ツリーのそのレベルで、cn 属性値を持つすべてのエントリが取り出されます。

- c. 検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。

3. 「追加されたオブジェクト・フィルタ」タブ・ページを選択します。

ACI を指定して、ユーザーが追加できるエントリの種類を制限できます。たとえば、ユーザーが `objectclass=country` を持つエントリのみを追加できるように、DSE ルート・エントリで ACI を指定できます。その後、ディレクトリ・サーバーによって、新規エントリがこのフィルタの制限に適合するかどうかを検証されます。

ユーザーが追加できるエントリの種類を制限するには、次の手順を実行します。

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

フィルタ	説明
開始	属性値の始めの数文字のみを使用して検索します。
終了	指定した属性値の終わりの数文字のみを使用してエントリを検索します。
含む	値の位置を限定せずに、ユーザーの入力値が指定した属性に含まれているエントリを検索します。
完全一致	指定した属性がユーザーの入力値に一致するエントリを検索します。
以上	指定した属性が、数値順またはアルファベット順で入力値より大か等しいエントリを検索します。アルファベットの先頭により近いエントリが、アルファベット順で上位とされます。
以下	指定した属性が、数値順またはアルファベット順で入力値より小か等しいエントリを検索します。アルファベットの先頭により近いエントリが、アルファベット順で下位とされます。
存在	指定した属性を持つエントリが、ツリーのそのレベルに存在するかどうかを判断します。この関連の使用に値の入力は不要です。たとえば、「cn」「存在」と指定すると、ツリーのそのレベルで、cn 属性値を持つすべてのエントリが取り出されます。

- c. 検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。

4. 「責任者」タブ・ページを選択します。
- a. 「バインド・モード」リストから、対象（つまり、アクセス権を要求しているエンティティ）が使用する認証のタイプを選択します。次の 5 つのバインド・モードの中から選択します。

バインド・モード	説明
なし	認証なし
SSL 認証なし	クライアントとサーバーのいずれも、他方に対して自己認証を行いません。証明書の送信または交換は行われません。この場合は、SSL 暗号化 / 復号化のみ使用されます。
SSL 一方向	ディレクトリ・サーバーのみ、クライアントに対して自己認証を行います。ディレクトリ・サーバーは、そのサーバーが認証されていることを証明する証明書をクライアントに送信します。
SSL 双方向	クライアントとサーバーは、相互に自己認証を行います。これは、相互に証明書を送信する方法で行われます。
簡易	クライアントは、ネットワーク上を平文で送信される識別名とパスワードによって、サーバーに対して自己認証を行います。サーバーは、クライアントが送信した識別名とパスワードが、ディレクトリに保存されている識別名とパスワードに一致しているかどうかを検証します。

バインド・モードは、対象の指定においてはオプションです。認証方式を設定しない場合は、どの種類の認証も受け入れられます。あるノードで指定されているバインド・モードは、通信先のノードで指定されているバインド・モードと一致している必要があります。

- b. アクセス権を付与するエンティティを指定します。

エンティティ	説明
すべての人 (*)	エントリにアクセスする人すべて。
特定のグループ	事前に定義したグループ名。
特定のエントリ	事前に定義したディレクトリ・エントリ。
サブツリー	ディレクトリ内の選択したサブツリー全体。
セッション・ユーザーの識別名 (DN) が属性により識別された場合	識別名がエントリ内の属性である人すべて。たとえば、グループ・エントリに対する読み込みアクセス権をグループのメンバーに付与する場合があります。

エンティティ	説明
セッション・ユーザーの一意 ID (orclGUID) が属性により識別された場合	このエントリに対してアクセス権を付与または制限するエントリのグローバル・ユーザー識別子 (orclGUID)。
セッション・ユーザーの識別名 (DN) がアクセス・エントリと一致する場合	指定したエントリで正常にログインしている人すべて。

5. 「アクセス権限」タブ・ページを選択します。

a. 付与する権限の種類を指定します。

- * 「参照」－対象にエントリの表示を許可します。
- * 「追加」－対象に、このエントリの下への他のエントリの追加を許可します。
- * 「削除」－対象にエントリの削除を許可します。
- * 「プロキシ」－対象に、別のユーザーの代理となることを許可します。

b. 「OK」をクリックします。

タスク 3: コンテンツ・アクセス項目の構成

1. コンテンツ・アクセス項目（つまり、属性に関する ACI）を定義するには、「コンテンツ・アクセス項目」ウィンドウの下への「作成」をクリックします。「コンテンツ・アクセス項目」ダイアログ・ボックスが表示されます。各タブ・ページには、変更可能な項目が含まれています。
2. ACP の下位エントリすべてを ACP で管理する場合は、「エントリ・フィルタ」タブ・ページには何も入力せず、次のステップに進みます。

ACP では、定義されたアクセス権は、他のフィルタによりアクセスがそれ以上制限されないかぎり、このエントリおよびそのエントリのすべてのサブエントリに適用されます。適切な場合は、「エントリ・フィルタ」タブ・ページを使用して、アクセスを指定するエントリを識別します。

エントリへのアクセスを、このエントリの 1 つ以上の属性に基づいて制限できます。たとえば、役職名がマネージャで組織単位がアメリカであるすべてのエントリへのアクセスを制限できます。

アクセスを指定するエントリを識別する手順は、次のとおりです。

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

フィルタ	説明
開始	属性値の始めの数文字のみを使用して検索します。
終了	指定した属性値の終わりの数文字のみを使用してエントリを検索します。
含む	値の位置を限定せずに、ユーザーの入力値が指定した属性に含まれているエントリを検索します。
完全一致	指定した属性がユーザーの入力値に一致するエントリを検索します。
以上	指定した属性が、数値順またはアルファベット順で入力値より大か等しいエントリを検索します。アルファベットの先頭により近いエントリが、アルファベット順で上位とされます。
以下	指定した属性が、数値順またはアルファベット順で入力値より小か等しいエントリを検索します。アルファベットの先頭により近いエントリが、アルファベット順で下位とされます。
存在	指定した属性を持つエントリが、ツリーのそのレベルに存在するかどうかを判断します。この関連の使用に値の入力は不要です。たとえば、「cn」「存在」と指定すると、ツリーのそのレベルで、cn 属性値を持つすべてのエントリが取り出されます。

- c. 検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。
3. 「責任者」タブ・ページを選択します。
- a. 「バインド・モード」リストから、対象（つまり、アクセス権を要求しているエンティティ）が使用する認証のタイプを選択します。次の 5 つのバインド・モードの中から選択します。

バインド・モード	説明
なし	認証なし
SSL 認証なし	クライアントとサーバーのいずれも、他方に対して自己認証を行いません。証明書の送信または交換は行われません。この場合は、SSL 暗号化 / 復号化のみ使用されます。
SSL 一方向	ディレクトリ・サーバーのみ、クライアントに対して自己認証を行います。ディレクトリ・サーバーは、そのサーバーが認証されていることを証明する証明書をクライアントに送信します。
SSL 双方向	クライアントとサーバーは、相互に自己認証を行います。これは、相互に証明書を送信する方法で行われます。
簡易	クライアントは、ネットワーク上を平文で送信される識別名とパスワードによって、サーバーに対して自己認証を行います。サーバーは、クライアントが送信した識別名とパスワードが、ディレクトリに保存されている識別名とパスワードに一致しているかどうかを検証します。

バインド・モードは、対象の指定においてはオプションです。認証方式を設定しない場合は、どの種類の認証も受け入れられます。あるノードで指定されているバインド・モードは、通信先のノードで指定されているバインド・モードと一致している必要があります。

- b. アクセス権を付与するエンティティを指定します。

エンティティ	説明
すべての人 (*)	エントリにアクセスする人すべて。
特定のグループ	事前に定義したグループ名。
特定のエントリ	事前に定義したディレクトリ・エントリ。
サブツリー	ディレクトリ内の選択したサブツリー全体。
セッション・ユーザーの識別名 (DN) が属性により識別された場合	識別名がエントリ内の属性である人すべて。たとえば、グループ・エントリに対する読み込みアクセス権をグループのメンバーに付与する場合があります。
セッション・ユーザーの一意 ID (orclGUID) が属性により識別された場合	このエントリに対してアクセス権を付与または制限するエントリのグローバル・ユーザー識別子 (orclGUID)。
セッション・ユーザーの識別名 (DN) がアクセス・エントリと一致する場合	指定したエントリで正常にログインしている人すべて。

4. 「属性」タブ・ページを選択します。
- a. 右のメニューから、アクセス権を付与または否認する属性を選択します。
 - b. 左のメニューから、属性に対して実行する一致操作を選択します。選択肢は「EQ」(=) と「NEQ」(!=) です。
- たとえば、「EQ」と「cn」を選択した場合は、付与したアクセス権が cn 属性に適用されます。「NEQ」と「cn」を選択した場合は、付与したアクセス権が cn 属性に適用されません。

5. 「アクセス権限」タブ・ページを選択して、表 13-1 の説明に従って各項目を指定します。

表 13-1 属性に関するアクセス権

アクセス権	説明
読み込み	属性の値を読み込む権限。属性に対して読み取り権限が与えられている場合でも、エントリ自体にブラウズ権限がないかぎり値は戻されません。
検索	検索フィルタで属性を使用する権限。
書き込み	エントリの属性を変更 / 追加 / 削除する権限。

表 13-1 属性に関するアクセス権（続き）

アクセス権	説明
自己書込み	識別名のグループ・エントリ属性のリスト内で、ユーザー自身の追加 / 削除あるいは自身のエントリを変更を行う権限。このレベルを使用すると、メンバーがリスト上の自分自身をメンテナンスできます。たとえば次のコマンドを実行すると、グループ内のユーザーが member 属性上で、自分自身の識別名のみを追加または削除できます。 access to attr=(member) by dnattr=(member) (selfwrite) dnattr セレクタは、 member 属性にリストされているエンティティにアクセス権が適用されるように指定します。selfwrite アクセス権セレクタは、そのメンバーが、属性上で自分自身の識別名のみを追加または削除できるように指定します。
比較	属性値で比較操作を実行する権限。

6. 「OK」をクリックしてこのダイアログ・ボックスを閉じ、Oracle Directory Manager のメイン・ダイアログ・ボックスに戻ります。

Oracle Directory Manager の ACP 作成ウィザードを使用した ACP の追加

ACP 作成ウィザードを使用すると、ACP を追加するために必要なタスクを順に実行できます。次のタスクがあります。

- タスク 1: ACP にするエントリを指定します。
- タスク 2: 構造型アクセス項目（つまり、エントリに関係する ACI）を構成します。
- タスク 3: コンテンツ・アクセス項目（つまり、属性に関係する ACI）を構成します。

タスク 1: ACP にするエントリの指定

- 13-12 ページの「[Oracle Directory Manager の ACP の表示の構成](#)」の説明に従って常に ACP を表示するように Oracle Directory Manager を構成した場合は、次のように開始します。
 - ナビゲータ・ペインで「Oracle Internet Directory サーバー」 > 「*directory server instance*」の順に展開します。
 - ナビゲータ・ペインで「アクセス制御管理」を選択し、ステップ 2 に進みます。13-12 ページの「[Oracle Directory Manager の ACP の表示の構成](#)」の説明に従って検索の結果としてのみ ACP を表示するように Oracle Directory Manager を構成した場合は、次のように開始します。
 - ナビゲータ・ペインで「Oracle Internet Directory サーバー」 > 「*directory server instance*」 > 「アクセス制御管理」の順に展開します。

- b. ナビゲータ・ペインで ACP を常駐させるノードを選択します。構成された ACP が存在しない場合は、「DSE ルート」の下で ACP を選択できます。
2. ツールバーの「作成」ボタンをクリックします。「新規アクセス制御ポイント」ダイアログ・ボックスが表示されます。
3. 「エントリへのパス」フィールドで、ACP に指定するエントリの識別名を入力します。「エントリ管理」の下でナビゲータ・ペインを探すか、または「参照」をクリックして、識別名を検索することもできます。

タスク 2: ACP 作成ウィザードを使用した構造型アクセス項目の構成

1. ウィザードを使用して構造型アクセス項目（つまり、エントリに関係する ACI）を定義するには、「構造型アクセス項目」ウィンドウの下で「作成」をクリックします。最初の「構造型アクセス項目」ダイアログ・ボックスが表示されます。

ACP では、定義されたアクセス権は、このエントリおよびそのエントリのすべてのサブエントリに適用されるか、または特定のエントリだけに適用されます。次に、両オプションでの ACP の構成方法を説明します。

規範的な構造型アクセス項目を指定した場合は、ACP の下位エントリすべてをこの ACP が管理します。規範的な構造型アクセス項目を希望する場合は、この最初の「構造型アクセス項目」ダイアログ・ボックスには何も入力する必要がありません。

1. アクセスを指定するエントリを識別する手順は、次のとおりです。
 - a. 「基準」バーの一番左のメニューから、属性タイプを選択します。
 - b. バーの中央のメニューから、次のフィルタ・オプションのいずれかを選択します。

フィルタ	説明
開始	属性値の始めの数文字のみを使用して検索します。
終了	指定した属性値の終わりの数文字のみを使用してエントリを検索します。
含む	値の位置を限定せずに、ユーザーの入力値が指定した属性に含まれているエントリを検索します。
完全一致	指定した属性がユーザーの入力値に一致するエントリを検索します。
以上	指定した属性が、数値順またはアルファベット順で入力値より大か等しいエントリを検索します。アルファベットの先頭により近いエントリが、アルファベット順で上位とされます。
以下	指定した属性が、数値順またはアルファベット順で入力値より小か等しいエントリを検索します。アルファベットの先頭により近いエントリが、アルファベット順で下位とされます。

フィルタ	説明
存在	指定した属性を持つエントリが、ツリーのそのレベルに存在するかどうかを判断します。この関連の使用に値の入力は不要です。たとえば、「cn」「存在」と指定すると、ツリーのそのレベルで、cn 属性値を持つすべてのエントリが取り出されます。

- c.

検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。
- d.

「次」をクリックします。ユーザーが追加できるエントリの種類を制限するための ACI の指定を要求する、2 番目の「構造型アクセス項目」ダイアログ・ボックスが表示されます。
2.

ACI を指定して、ユーザーが追加できるエントリの種類を制限できます。たとえば、ユーザーが `objectclass=country` を持つエントリのみを追加できるように、DSE ルート・エントリで ACI を指定できます。その後、ディレクトリ・サーバーによって、新規エントリがこのフィルタの制限に適合するかどうかを検証されます。
- ユーザーが追加できるエントリの種類を制限するには、次の手順を実行します。
- a.

「基準」バーの一番左のメニューから、属性タイプを選択します。
- b.

バーの中央のメニューから、次のフィルタ・オプションのいずれかを選択します。

フィルタ	説明
開始	属性値の始めの数文字のみを使用して検索します。
終了	指定した属性値の終わりの数文字のみを使用してエントリを検索します。
含む	値の位置を限定せずに、ユーザーの入力値が指定した属性に含まれているエントリを検索します。
完全一致	指定した属性がユーザーの入力値に一致するエントリを検索します。
以上	指定した属性が、数値順またはアルファベット順で入力値より大か等しいエントリを検索します。アルファベットの先頭により近いエントリが、アルファベット順で上位とされます。
以下	指定した属性が、数値順またはアルファベット順で入力値より小か等しいエントリを検索します。アルファベットの先頭により近いエントリが、アルファベット順で下位とされます。
存在	指定した属性を持つエントリが、ツリーのそのレベルに存在するかどうかを判断します。この関連の使用に値の入力は不要です。たとえば、「cn」「存在」と指定すると、ツリーのそのレベルで、cn 属性値を持つすべてのエントリが取り出されます。

- c.

検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。

- d. 「次」を選択します。ウィザードによって、認証タイプ（バインド・モードと呼ばれます）およびアクセス権を付与する対象の指定が要求されます。
3. バインド・モードは、対象の指定においてはオプションです。認証方式を設定しない場合、または「なし」を選択する場合は、どの種類の認証も受け入れられます。あるノードで指定されているバインド・モードは、通信先のノードで指定されているバインド・モードと一致している必要があります。
 - a. 認証のタイプ（バインド・モード）を指定するには、「バインド・モード」リストから、対象（つまり、アクセス権を要求しているエンティティ）が使用する認証のタイプを選択します。次の 5 つのバインド・モードの中から選択します。
 - b. アクセス権を付与するエンティティを指定するには、次のいずれか 1 つを選択します。

エンティティ	説明
すべての人 (*)	エントリにアクセスする人すべて。
特定のグループ	事前に定義したグループ名。
特定のエントリ	事前に定義したディレクトリ・エントリ。
サブツリー	ディレクトリ内の選択したサブツリー全体。
セッション・ユーザーの識別名 (DN) が属性により識別された場合	識別名がエントリ内の属性である人すべて。たとえば、グループ・エントリに対する読み込みアクセス権をグループのメンバーに付与する場合があります。
セッション・ユーザーの一意 ID (orclGUID) が属性により識別された場合	このエントリに対してアクセス権を付与または制限するエントリのグローバル・ユーザー識別子 (orclGUID)。
セッション・ユーザーの識別名 (DN) がアクセス・エントリと一致する場合	指定したエントリで正常にログインしている人すべて。

4. 「次」をクリックします。アクセス権情報の入力を要求する「構造型アクセス項目」ダイアログ・ボックスが表示されます。付与する権限の種類を指定します。
 - 「参照」：対象にエントリの表示を許可します。
 - 「追加」：対象に、このエントリの下への他のエントリの追加を許可します。
 - 「削除」：対象にエントリの削除を許可します。
 - 「プロキシ」：パスワードを指定せずに、エンティティの代理となることを許可します。
5. 「終了」をクリックします。

タスク 3: ACP 作成ウィザードを使用したコンテンツ・アクセス項目の構成

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

規範的なコンテンツ・アクセス項目を指定した場合は、ACP の下位エントリすべてをこの ACP が管理します。規範的なコンテンツ・アクセス項目を希望する場合は、この最初の「コンテンツ・アクセス項目」ダイアログ・ボックスには何も入力する必要がありません。

- 1. アクセスを指定する属性を識別する手順は、次のとおりです。
 - a. 「基準」バーの一番左のメニューから、属性タイプを選択します。
 - b. バーの中央のメニューから、次のフィルタ・オプションのいずれかを選択します。

フィルタ	説明
開始	属性値の始めの数文字のみを使用して検索します。
終了	指定した属性値の終わりの数文字のみを使用してエントリを検索します。
含む	値の位置を限定せずに、ユーザーの入力値が指定した属性に含まれているエントリを検索します。
完全一致	指定した属性がユーザーの入力値に一致するエントリを検索します。
以上	指定した属性が、数値順またはアルファベット順で入力値より大か等しいエントリを検索します。アルファベットの先頭により近いエントリが、アルファベット順で上位とされます。
以下	指定した属性が、数値順またはアルファベット順で入力値より小か等しいエントリを検索します。アルファベットの先頭により近いエントリが、アルファベット順で下位とされます。
存在	指定した属性を持つエントリが、ツリーのそのレベルに存在するかどうかを判断します。この関連の使用に値の入力は不要です。たとえば、「cn」「存在」と指定すると、ツリーのそのレベルで、cn 属性値を持つすべてのエントリが取り出されます。

- c. 検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。
 - d. 「次」をクリックします。アクセス権を付与する人の指定を要求する、2 番目の「コンテンツ・アクセス項目」ダイアログ・ボックスが表示されます。
- 2. 対象（アクセス権を要求しているエンティティ）が使用する認証のタイプ（バインド・モードとも呼びます）を指定します。

バインド・モードは、対象の指定においてはオプションです。認証方式を設定しない場合、または「なし」を選択する場合は、どの種類の認証も受け入れられます。あるノー

ドで指定されているバインド・モードは、通信先のノードで指定されているバインド・モードと一致する必要があります。

次の 5 つのバインド・モードの中から選択します。

バインド・モード	説明
なし	認証なし
SSL 認証なし	クライアントとサーバーのいずれも、他方に対して自己認証を行いません。証明書の送信または交換は行われません。この場合は、SSL 暗号化 / 復号化のみ使用されます。
SSL 一方向	ディレクトリ・サーバーのみ、クライアントに対して自己認証を行います。ディレクトリ・サーバーは、そのサーバーが認証されていることを証明する証明書をクライアントに送信します。
SSL 双方向	クライアントとサーバーは、相互に自己認証を行います。これは、相互に証明書を送信する方法で行われます。
簡易	クライアントは、ネットワーク上を平文で送信される識別名とパスワードによって、サーバーに対して自己認証を行います。サーバーは、クライアントが送信した識別名とパスワードが、ディレクトリに保存されている識別名とパスワードに一致しているかどうかを検証します。

3. アクセス権を付与するエンティティを指定します。

エンティティ	説明
すべての人 (*)	エントリにアクセスする人すべて。
特定のグループ	事前に定義したグループ名。
特定のエントリ	事前に定義したディレクトリ・エントリ。
サブツリー	ディレクトリ内の選択したサブツリー全体。
セッション・ユーザーの識別名 (DN) が属性により識別された場合	識別名がエントリ内の属性である人すべて。たとえば、グループ・エントリに対する読み込みアクセス権をグループのメンバーに付与する場合があります。
セッション・ユーザーの一意 ID (orclGUID) が属性により識別された場合	このエントリに対してアクセス権を付与または制限するエントリのグローバル・ユーザー識別子 (orclGUID)。
セッション・ユーザーの識別名 (DN) がアクセス・エントリと一致する場合	指定したエントリで正常にログインしている人すべて。

- 4. 「次」をクリックします。属性およびこの属性に対して実行する一致操作の選択を要求する、「コンテンツ・アクセス項目」ダイアログ・ボックスが表示されます。
- 5. 属性およびこの属性に対して実行する一致操作を選択するには、次の手順を実行します。
 - a. 「コンテンツ・アクセス項目」ダイアログ・ボックスの「属性」フィールドで、アクセス権を付与または制限する属性を右のリストから選択します。
 - b. 左のリストから、属性に対して実行する一致操作を選択します。選択肢は「EQ」(=) と「NEQ」(!=) です。
 - c. 「次」をクリックします。アクセス権の指定を要求する「コンテンツ・アクセス項目」ダイアログ・ボックスが表示されます。
- 6. 表 13-2 の説明に従って、付与する権限の種類を指定します。

表 13-2 属性に関するアクセス権

アクセス権	説明
読み込み	属性の値を読み込む権限。属性に対して読取り権限が与えられている場合でも、エントリ自体にブラウズ権限がないかぎり値は戻されません。
検索	検索フィルタで属性を使用する権限。
書き込み	エントリの属性を変更 / 追加 / 削除する権限。
自己書き込み	識別名のグループ・エントリ属性のリスト内で、ユーザー自身の追加 / 削除あるいは自身のエントリを変更を行う権限。このレベルを使用すると、メンバーがリスト上の自分自身をメンテナンスできます。たとえば次のコマンドを実行すると、グループ内のユーザーが member 属性上で、自分自身の識別名のみを追加または削除できます。 <div>access to attr=(member) by dnattr=(member) (selfwrite)</div> dnattr セレクタは、member 属性にリストされているエンティティにアクセス権が適用されるように指定します。selfwrite アクセス権セレクタは、そのメンバーが、属性上で自分自身の識別名のみを追加または削除できるように指定します。
比較	属性値で比較操作を実行する権限。

- 7. 「終了」をクリックします。

Oracle Directory Manager を使用した ACP の変更

Oracle Directory Manager を使用して ACP を変更するには、次の 3 つのタスクが必要です。

- タスク 1: 変更するエントリを指定します。
- タスク 2: 構造型アクセス項目（つまり、エントリに関する ACI）を変更します。
- タスク 3: コンテント・アクセス項目（つまり、属性に関する ACI）を変更します。

タスク 1: 変更するエントリの指定

1. 13-12 ページの「[Oracle Directory Manager の ACP の表示の構成](#)」の説明に従って常に ACP を表示するように Oracle Directory Manager を構成した場合は、次のように開始します。

- a. ナビゲータ・ペインで「Oracle Internet Directory サーバー」>「*directory server instance*」>「アクセス制御管理」の順に展開します。「アクセス制御管理」を選択します。ナビゲータ・ペインの「アクセス制御管理」の下にリストに、定義済みのすべての ACP が表示されます。同じ内容のリストが、右側のペインにも表示されます。
- b. 「アクセス制御管理」の下で、変更する ACP を選択します。その ACP の情報が右側のペインに表示されます。または、右側のペインの ACP をダブルクリックすると、独立したダイアログ・ボックスにデータが表示されます。

13-12 ページの「[Oracle Directory Manager の ACP の表示の構成](#)」の説明に従って検索の結果としてのみ ACP を表示するように Oracle Directory Manager を構成した場合は、次のように開始します。

- a. ナビゲータ・ペインで「Oracle Internet Directory サーバー」>「*directory server instance*」>「アクセス制御管理」の順に展開し、変更する ACP を選択します。その ACP の情報が右側のペインに表示されます。
- b. 「編集」をクリックします。「サブツリーのアクセス制御ポイント」ダイアログ・ボックスが表示されます。

タスク 2: 構造型アクセス項目の変更

新規構造型アクセス項目を追加、または既存の構造型アクセス項目を変更できます。

関連項目： 構造型アクセス項目の追加の詳細は、13-16 ページの「[タスク 2: 構造型アクセス項目の構成](#)」を参照してください。

構造型アクセス項目を変更する手順は、次のとおりです。

1. 「構造型アクセス項目」ウィンドウで変更する項目を選択し、「構造型アクセス項目」ウィンドウの下に「編集」をクリックします。「構造型アクセス項目」ダイアログ・ボックスが表示されます。

2. 「エントリ・フィルタ」タブ・ページを使用して、アクセス権を付与するエントリのセットを絞り込みます。ACP の下位エントリすべてを ACP で管理する場合は、次のステップに進んでください。

1 つ以上の属性に基づいてエントリを選択する場合があります。たとえば、`title` が `secretary` の個人をすべて検索したり、`title` が `manager` で `organization unit` が `Americas` の個人をすべて検索することができます。

「エントリ・フィルタ」タブ・ページの「基準」ウィンドウで、検索基準バーを使用して属性を選択し、その属性の値を入力し、さらに指定した属性と入力値との一致条件を示すフィルタを指定します。この手順は、次のとおりです。

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

フィルタ	説明
開始	属性値の始めの数文字のみを使用して検索します。
終了	指定した属性値の終わりの数文字のみを使用してエントリを検索します。
含む	値の位置を限定せずに、ユーザーの入力値が指定した属性に含まれているエントリを検索します。
完全一致	指定した属性がユーザーの入力値に一致するエントリを検索します。
以上	指定した属性が、数値順またはアルファベット順で入力値より大か等しいエントリを検索します。アルファベットの先頭により近いエントリが、アルファベット順で上位とされます。
以下	指定した属性が、数値順またはアルファベット順で入力値より小か等しいエントリを検索します。アルファベットの先頭により近いエントリが、アルファベット順で下位とされます。
存在	指定した属性を持つエントリが、ツリーのそのレベルに存在するかどうかを判断します。この関連の使用に値の入力は不要です。たとえば、「 <code>cn</code> 」 「存在」と指定すると、ツリーのそのレベルで、 <code>cn</code> 属性値を持つすべてのエントリが取り出されます。

- c. 検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。
3. 「追加されたオブジェクト・フィルタ」タブ・ページを使用して、ユーザーが追加できるエントリの種類を制限するために ACI を指定できます。たとえば、ユーザーが `objectclass=country` を持つエントリのみを追加できるように、DSE ルート・エントリで ACI を指定できます。その後、ディレクトリ・サーバーによって、新規エントリがこのフィルタの制限に適合するかどうかを検証されます。
- ユーザーが追加できるエントリの種類を制限するには、次の手順を実行します。
- a. 「基準」バーの一番左のメニューから、属性タイプを選択します。

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

フィルタ	説明
開始	属性値の始めの数文字のみを使用して検索します。
終了	指定した属性値の終わりの数文字のみを使用してエントリを検索します。
含む	値の位置を限定せずに、ユーザーの入力値が指定した属性に含まれているエントリを検索します。
完全一致	指定した属性がユーザーの入力値に一致するエントリを検索します。
以上	指定した属性が、数値順またはアルファベット順で入力値より大か等しいエントリを検索します。アルファベットの先頭により近いエントリが、アルファベット順で上位とされます。
以下	指定した属性が、数値順またはアルファベット順で入力値より小か等しいエントリを検索します。アルファベットの先頭により近いエントリが、アルファベット順で下位とされます。
存在	指定した属性を持つエントリが、ツリーのそのレベルに存在するかどうかを判断します。この関連の使用に値の入力は不要です。たとえば、「cn」「存在」と指定すると、ツリーのそのレベルで、cn 属性値を持つすべてのエントリが取り出されます。

- c. 検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。

4. 「責任者」タブ・ページを使用して、ACI の対象（つまり、アクセス権を要求しているエンティティ）を指定します。

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

バインド・モード	説明
なし	認証なし
SSL 認証なし	クライアントとサーバーのいずれも、他方に対して自己認証を行いません。証明書の送信または交換は行われません。この場合は、SSL 暗号化 / 復号化のみ使用されます。
SSL 一方向	ディレクトリ・サーバーのみ、クライアントに対して自己認証を行います。ディレクトリ・サーバーは、そのサーバーが認証されていることを証明する証明書をクライアントに送信します。
SSL 双方向	クライアントとサーバーは、相互に自己認証を行います。これは、相互に証明書を送信する方法で行われます。

バインド・モード	説明
簡易	クライアントは、ネットワーク上を平文で送信される識別名とパスワードによって、サーバーに対して自己認証を行います。サーバーは、クライアントが送信した識別名とパスワードが、ディレクトリに保存されている識別名とパスワードに一致しているかどうかを検証します。

バインド・モードは、対象の指定においてはオプションです。ディレクティブを適用する場合、あるノードで指定されているバインド・モードは、通信先のノードで指定されているバインド・モードと一致している必要があります。

- b. アクセス権を付与するエンティティを指定します。

エンティティ	説明
すべての人 (*)	エントリにアクセスする人すべて。
特定のグループ	事前に定義したグループ名。
特定のエントリ	事前に定義したディレクトリ・エントリ。
サブツリー	ディレクトリ内の選択したサブツリー全体。
セッション・ユーザーの識別名 (DN) が属性により識別された場合	識別名がエントリ内の属性である人すべて。たとえば、グループ・エントリに対する読み込みアクセス権をグループのメンバーに付与する場合があります。
セッション・ユーザーの一意 ID (orclGUID) が属性により識別された場合	このエントリに対してアクセス権を付与または制限するエントリのグローバル・ユーザー識別子 (orclGUID)。
セッション・ユーザーの識別名 (DN) がアクセス・エントリと一致する場合	指定したエントリで正常にログインしている人すべて。

- 5. 「アクセス権限」タブ・ページを選択します。
 - a. 付与する権限の種類（「参照」、「追加」、「削除」または「プロキシ」）を決定します。エントリが未指定の場合、アクセス権は、そのアクセス権が指定されている直近の上位レベルで判断されます。
 - b. 「OK」をクリックします。

タスク 3: コンテンツ・アクセス項目の変更

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

関連項目： コンテンツ・アクセス項目の追加の詳細は、13-19 ページの「タスク 3: コンテンツ・アクセス項目の構成」を参照してください。

コンテンツ・アクセス項目を変更する手順は、次のとおりです。

1. 「コンテンツ・アクセス項目」ボックスで変更するコンテンツ・アクセス項目を選択し、「コンテンツ・アクセス項目」ウィンドウの下「編集」をクリックします。「コンテンツ・アクセス項目」ダイアログ・ボックスが表示されます。各タブ・ページには、変更可能な項目が含まれています。
2. ACP の下位エントリすべてを ACP で管理する場合は、「エントリ・フィルタ」タブ・ページには何も入力せず、次のステップに進みます。

ACP では、定義されたアクセス権は、他のフィルタによりアクセスがそれ以上制限されないかぎり、このエントリおよびそのエントリのすべてのサブエントリに適用されます。適切な場合は、「エントリ・フィルタ」タブ・ページを使用して、アクセスを指定するエントリを識別します。

エントリへのアクセスを、このエントリの 1 つ以上の属性に基づいて制限できます。たとえば、役職名がマネージャで組織単位がアメリカであるすべてのエントリへのアクセスを制限できます。

アクセスを指定するエントリを識別する手順は、次のとおりです。

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

フィルタ	説明
開始	属性値の始めの数文字のみを使用して検索します。
終了	指定した属性値の終わりの数文字のみを使用してエントリを検索します。
含む	値の位置を限定せずに、ユーザーの入力値が指定した属性に含まれているエントリを検索します。
完全一致	指定した属性がユーザーの入力値に一致するエントリを検索します。
以上	指定した属性が、数値順またはアルファベット順で入力値より大か等しいエントリを検索します。アルファベットの先頭により近いエントリが、アルファベット順で上位とされます。
以下	指定した属性が、数値順またはアルファベット順で入力値より小か等しいエントリを検索します。アルファベットの先頭により近いエントリが、アルファベット順で下位とされます。

フィルタ	説明
存在	指定した属性を持つエントリが、ツリーのそのレベルに存在するかどうかを判断します。この関連の使用に値の入力は不要です。たとえば、「cn」「存在」と指定すると、ツリーのそのレベルで、cn 属性値を持つすべてのエントリが取り出されます。

- c. 検索基準バーの一番右のテキスト・ボックスに、選択した属性の値を入力します。
3. 「責任者」タブ・ページを選択します。
- a. 「バインド・モード」リストから、対象（つまり、アクセス権を要求しているエンティティ）が使用する認証のタイプを選択します。次の 5 つのバインド・モードの中から選択します。

バインド・モード	説明
なし	認証なし
SSL 認証なし	クライアントとサーバーのいずれも、他方に対して自己認証を行いません。証明書の送信または交換は行われません。この場合は、SSL 暗号化 / 復号化のみ使用されます。
SSL 一方向	ディレクトリ・サーバーのみ、クライアントに対して自己認証を行います。ディレクトリ・サーバーは、そのサーバーが認証されていることを証明する証明書をクライアントに送信します。
SSL 双方向	クライアントとサーバーは、相互に自己認証を行います。これは、相互に証明書を送信する方法で行われます。
簡易	クライアントは、ネットワーク上を平文で送信される識別名とパスワードによって、サーバーに対して自己認証を行います。サーバーは、クライアントが送信した識別名とパスワードが、ディレクトリに保存されている識別名とパスワードに一致しているかどうかを検証します。

- バインド・モードは、対象の指定においてはオプションです。認証方式を設定しない場合は、どの種類の認証も受け入れられます。あるノードで指定されているバインド・モードは、通信先のノードで指定されているバインド・モードと一致している必要があります。
- b. アクセス権を付与するエンティティを指定します。

エンティティ	説明
すべての人 (*)	エントリにアクセスする人すべて。
特定のグループ	事前に定義したグループ名。

エンティティ	説明
特定のエントリ	事前に定義したディレクトリ・エントリ。
サブツリー	ディレクトリ内の選択したサブツリー全体。
セッション・ユーザーの識別名 (DN) が属性により識別された場合	識別名がエントリ内の属性である人すべて。たとえば、グループ・エントリに対する読込みアクセス権をグループのメンバーに付与する場合があります。
セッション・ユーザーの一意 ID (orclGUID) が属性により識別された場合	このエントリに対してアクセス権を付与または制限するエントリのグローバル・ユーザー識別子 (orclGUID)。
セッション・ユーザーの識別名 (DN) がアクセス・エントリと一致する場合	指定したエントリで正常にログインしている人すべて。

4. 「属性」タブ・ページを選択します。

- a. 右のメニューから、アクセス権を付与または否認する属性を選択します。
- b. 左のメニューから、属性に対して実行する一致操作を選択します。選択肢は「EQ」(=) と「NEQ」(!=) です。

たとえば、「EQ」と「cn」を選択した場合は、付与したアクセス権が cn 属性に適用されます。「NEQ」と「cn」を選択した場合は、付与したアクセス権が cn 属性に適用されません。

5. 「アクセス権限」タブ・ページを選択して、表 13-1 の説明に従って各項目を指定します。

表 13-3 属性に関するアクセス権

アクセス権	説明
読込み	属性の値を読み込む権限。属性に対して読取り権限が与えられている場合でも、エントリ自体にブラウズ権限がないかぎり値は戻されません。
検索	検索フィルタで属性を使用する権限。
書込み	エントリの属性を変更 / 追加 / 削除する権限。

表 13-3 属性に関するアクセス権（続き）

アクセス権	説明
自己書込み	識別名のグループ・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を変更を行う権限。このレベルを使用すると、メンバーがリスト上の自分自身をメンテナンスできます。たとえば次のコマンドを実行すると、グループ内のユーザーが member 属性上で、自分自身の識別名のみを追加または削除できます。 access to attr=(member) by dnattr=(member) (selfwrite) dnattr セレクタは、 member 属性にリストされているエンティティにアクセス権が適用されるように指定します。selfwrite アクセス権セレクタは、そのメンバーが、属性上で自分自身の識別名のみを追加または削除できるように指定します。
比較	属性値で比較操作を実行する権限。

6. 「OK」をクリックします。

Oracle Directory Manager を使用したエントリ・レベルのアクセス権の付与

Oracle Directory Manager を使用してエントリ・レベルのアクセス権を付与する手順は、次のとおりです。

- 1. ナビゲータ・ペインで「Oracle Internet Directory サーバー」>「*directory server instance*」>「エントリ管理」の順に展開します。次のいずれかの方法で起動できます。
 - エントリを選択して、右側のペインにそのプロパティを表示します。
 - 検索パネルを使用してエントリを検索し、エントリをダブルクリックして「エントリ」ダイアログ・ボックスを開きます。
- 2. 「ローカル・アクセス」タブ・ページを選択して、「構造型アクセス項目」ボックスと「コンテンツ・アクセス項目」ボックスで、ローカル ACI を作成および編集します。
- 3. 変更後、「適用」をクリックします。

注意： 入力した情報をディレクトリ・サーバーに送信するには、「適用」をクリックする必要があります。「適用」をクリックしないと、入力した情報は、単に Oracle Directory Manager のキャッシュに入れられます。

例 : Oracle Directory Manager を使用した ACP の管理

この例では、Oracle Directory Manager を使用して、ACI を含めた新規 ACP を作成する方法を紹介します。大企業の管理者が、ユーザー・パスワードに対するアクセス権を制限して、比較はすべての人が可能に、読み取りと変更は各パスワードの所有者（つまり、ユーザー）のみ可能に設定する場合の例です。

この例では、新しい ACP を作成し、その ACP に次の各権限を設定する 4 つの ACI を移入します。

- すべての人による userpassword 属性に対する制限付きアクセス権
- ユーザー本人による同一 userpassword 属性への開かれたアクセス権
- すべての属性に対する開かれたアクセス権（すべての人による userpassword に対するアクセス権を除く）
- すべての人へのすべての属性に対する開かれたアクセス権

新規 ACP の作成

1. ナビゲータ・ペインで「Oracle Internet Directory サーバー」>「*directory server instance*」の順に展開し、「アクセス制御管理」を選択します。ACP のリストが右側のペインに表示されます。
2. 右側のペインの下に「作成」ボタンをクリックします。「新規アクセス制御ポイント」ダイアログ・ボックスが表示されます。
3. 「エントリへのパス」フィールドで、ACP に指定する識別名を入力します。ACP 内の ACI は、すべての下位エントリ（その識別名も含めて）に適用されます。

構造型アクセス項目の構成 エントリに対するアクセス権を設定する手順は次のとおりです。

1. 「構造型アクセス項目」ボックスの下に「作成」をクリックします。「構造型アクセス項目」ダイアログ・ボックスが表示されます。このダイアログ・ボックスには、「エントリ・フィルタ」、「責任者」および「アクセス権限」の 3 つのタブがあります。

ACP の下位エントリすべてに ACI を適用するため、「エントリ・フィルタ」タブ・ページは使用しません。

2. 「責任者」タブ・ページを選択して、ACI の対象を定義します。「バインド・モード」リストから、使用中の環境に適した認証モードを選択します。すべての人に対するアクセス権を作成するには、「すべての人」を選択します。
3. 「アクセス権限」タブ・ページを選択します。デフォルトでは、すべての権限（「参照」、「追加」および「削除」）が付与されています。「プロキシ」は指定されません。
 - a. すべての人が全エントリをブラウズでき、追加や削除はできないようにアクセス権を変更します。
 - b. 「OK」をクリックします。

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

コンテンツ・アクセス項目を定義する手順は、次のとおりです。

1. 「コンテンツ・アクセス項目」ボックスの下に「作成」をクリックします。「コンテンツ・アクセス項目」ダイアログ・ボックスが表示されます。

ACP のすべての下位エントリにこの ACI を適用するため、「エントリ・フィルタ」タブ・ページは使用しません。
2. 「責任者」タブ・ページで、「すべての人」を選択します。
3. 「属性」タブ・ページを選択します。このページには 2 つのフィールドがあります。最初のフィールドの選択肢は、「EQ」（等価）と「NEQ」（非等価）です。2 番目には、属性を設定します。

「EQ」を選択して、「userPassword」を選択します。
4. 「アクセス権限」タブ・ページを選択します。デフォルトでは、すべての権限が付与されています。読込み、検索、書込みおよび比較を否認するように権限を変更します。
5. 「OK」をクリックします。

これで 1 番目の ACI の設定は完了です。

2 番目の ACI の作成 ユーザーに、本人のパスワードの読込み、書込み、検索および比較を許可する 2 番目の ACI を作成します。

1. 「コンテンツ・アクセス項目」ボックスの下に「作成」をクリックします。「コンテンツ・アクセス項目」ダイアログ・ボックスが表示されます。
2. 「責任者」タブ・ページを選択します。「セッション・ユーザーの識別名 (DN) がアクセス・エントリと一致する場合です。」をクリックします。
3. 「属性」タブ・ページを選択します。このタブ・ページには、2 つのリストがあります。最初のリストの選択肢は、「EQ」（等価）と「NEQ」（非等価）です。2 番目には、属性を設定します。

「EQ」と「userPassword」を選択します。
4. 「アクセス権限」タブ・ページを選択します。

読込み、検索、書込みおよび比較の各アクセス権を付与します。「自己書込み」は未指定のままにします。
5. 「OK」をクリックします。

これで 2 つの ACI が作成されました。1 番目の ACP は、userPassword 属性の読込み、検索、書込みおよび比較の各アクセス権をすべての人に対して否認しています。2 番目の ACP は、パスワードの所有者に対して、その属性の読込み、検索、書込みおよび比較を許可しています。

3 番目の ACI の作成

次の ACI は、`userPassword` を除くすべての属性の読み込み、検索および比較の各アクセス権を、すべての人に付与します。書き込みアクセス権は否認します。

1. 「コンテンツ・アクセス項目」フィールドの下で「作成」をクリックして、「コンテンツ・アクセス項目」を表示します。
2. 「責任者」タブ・ページを選択します。「すべての人」を選択します。
3. 「属性」タブ・ページを選択します。

「NEQ」と「`userPassword`」を選択します。

この組合せは、`userpassword` と等しくないあらゆる属性が、この ACI の権限の対象であることを示しています。

4. 「アクセス権限」タブ・ページを選択します。

読み込み、検索および比較の各アクセス権を付与します。「書き込み」アクセス権は否認します。「自己書き込み」は未指定のままにします。

5. 「OK」をクリックしてこれらの権限を適用し、ダイアログ・ボックスを閉じます。

4 番目の ACI の作成

次の ACI は、`userpassword` を除くすべての属性の読み込み、ブラウズおよび書き込みの各アクセス権を、その属性の所有者に付与します。この ACI を組み込むことによって、`userPassword` 以外の属性に対するアクセス権がその属性の所有者と他の人とで同じになるというあいまいさを排除できます。

1. 「コンテンツ・アクセス項目」フィールドの下で「作成」をクリックして、「コンテンツ・アクセス項目」ダイアログ・ボックスを表示します。
2. 「責任者」タブ・ページを選択します。

「セッション・ユーザーの識別名 (DN) がアクセス・エントリと一致する場合です。」をクリックします。

3. 「属性」タブ・ページを選択します。

リストから、「NEQ」と「`userPassword`」を選択します。この組合せは、`userPassword` 以外のすべての属性が、この ACI の権限の対象であることを示しています。

4. 「アクセス権限」タブ・ページをクリックします。

読み込み、検索および書き込みの各アクセス権を付与します。「自己書き込み」は未指定のままにします。

5. 「OK」をクリックしてこれらの権限を適用し、ダイアログ・ボックスを閉じます。

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

コマンドライン・ツールを使用したアクセス制御の管理

13-2 ページの「[アクセス制御ポリシー・ポイントの管理の概要](#)」で説明したように、ディレクトリのアクセス制御ポリシー・ポイントの情報は、ユーザーが変更可能な操作属性で表されます。したがって、`ldapmodify` を使用してこれらの属性の値を設定および変更して、ディレクトリのアクセス制御を管理できます。`ldapmodify` や `ldapmodifymt` などのツールがこのために使用できます。

付録 B「[アクセス制御ディレクティブ書式](#)」の説明に従って ACI を直接編集するには、ACI のディレクトリ表現の書式および構文を理解する必要があります。

関連項目：

- コマンドライン・モードのコマンドに必須の入力フォーマットである、[LDAP データ交換フォーマット](#)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-15 ページの「[ldapmodify の構文](#)」を参照してください。
- ACI の書式（構文）の詳細は、[付録 B「アクセス制御ディレクティブ書式」](#)を参照してください。

例：ユーザーが追加できるエントリの種類の制限

ACI を指定して、ユーザーが追加できるエントリの種類を制限できます。たとえば、ユーザーが `objectclass=country` を持つエントリのみを追加できるように、DSE ルート・エントリで ACI を指定できます。追加できるエントリの種類を制限するには、`added_object_constraint` フィルタを使用します。その後、ディレクトリ・サーバーによって、新規エントリがこのフィルタの制限に適合するかどうかを検証されます。

次の制限を指定する例を示します。

- 対象 `cn=admin,c=us` は、`organization` エントリの下を参照、追加および削除できます。
- 対象 `cn=admin,c=us` は、`organization` エントリの下の `organizationalUnit` オブジェクトを追加できます。

- その他のすべては、organization エントリの下を参照できます。

```
access to entry filter=(objectclass=organization)
by group="cn=admin,c=us"
    constraintonaddedobject=(objectclass=organisationalunit)
    (browse,add,delete)
by * (browse)
```

例 : ldapmodify を使用した継承可能な ACP の設定

この例では、my_ldif_file という名前の LDIF ファイルを使用して、**ルート DSE** で orclACI にサブツリーのアクセス権を設定します。この例は orclACI 属性を参照しているため、このアクセス・ディレクティブはディレクトリ情報ツリーのエントリすべてを制御します。

```
ldapmodify -v -h $1 -D "cn=Directory Manager, o=IMC, c=US" -w "controller" -f my_
ldif_file
```

LDIF ファイル my_ldif_file は次のようになります。

```
dn:
changetype: modify
replace: orclaci
orclaci: access to entry
    by dn="cn=directory manager, o=IMC, c=us" (browse, add, delete)
    by * (browse, noadd, nodelete)
orclaci: access to attr=(*)
    by dn="cn=directory manager, o=IMC, c=us" (search, read, write, compare)
    by self (search, read, write, compare)
    by * (search, read, nowrite, nocompare)
```

例 : ldapmodify を使用したエントリ・レベルの ACI の設定

この例では、my_ldif_file という名前の LDIF ファイルを使用して、orclEntryLevelACI 属性にエントリ・レベルのアクセス権を設定します。この例は orclentrylevelACI 属性を参照しているため、このアクセス・ディレクティブは、それが常駐しているエントリのみを制御します。

```
ldapmodify -v -h myhost -D "cn=Directory Manager, o=IMC, c=US" -w "controller"
-f my_ldif_file
```

LDIF ファイル my_ldif_file は次のようになります。

```
dn:
changetype: modify
replace: orclentrylevelaci
orclentrylevelaci: access to entry
    by dn="cn=directory manager, o=IMC, c=us" (browse, add, delete)
```

```
by * (browse, noadd, nodelete)
orclentrylevelaci: access to attr=(*)
by dn="cn=directory manager, o=IMC, c=us" (search, read, write, compare)
by * (search, read, nowrite, nocompare)
```

注意： この例では、識別名の値が指定されていません。このことは、この ACI がルート DSE とその属性のみに関係していることを意味します。

例：ワイルド・カードの使用方法

この例では、オブジェクトと対象指定子にワイルド・カード (*) を使用しています。acme.com ドメイン内のエントリすべてについて、誰もがすべての属性を読み込み、検索し、かつすべてのエントリをブラウズする権限をもつことになります。

dc=com の ACP 内の orclACI 属性

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

属性の読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：識別名によるエントリの選択

この例では、2 つのアクセス・ディレクティブで識別名を使用してエントリを選択する際の正規表現の使用法を示します。この例では、dc=acme、dc=com アクセス権より下位の address book 属性の読取り専用アクセス権を、すべての人に付与します。

dc=acme、dc=com の orclACI 属性

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

dc=us、dc=acme、dc=com の orclACI 属性

```
access to entry by * (browse)
access to attr=(*) by dn=".*,dc=us,dc=acme,dc=com" (search, read)
```

例：属性セクタと対象セクタの使用方法

この例では、特定の属性に対するアクセス権を付与する属性セクタ、および様々な対象セクタの使用方法を示します。この例は、`dc=us`、`dc=acme`、`dc=com` サブツリー内のエントリに適用されます。この ACI によって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。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の付与

この例では、`dc=acme`、`dc=com` より下位の `address book` 属性の読取り専用アクセス権を、すべての人に付与します。さらに、`dc=us`、`dc=acme`、`dc=com` サブツリー内のみのすべての属性に対する読込みアクセス権をすべての人に付与します。

`dc=acme`、`dc=com` の `orclACI` 属性

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

`dc=us`、`dc=acme`、`dc=com` の `orclACI` 属性

```
access to entry by * (browse)
access to attr=(*) by dn=".*,dc=us,dc=acme,dc=com" (search, read)
```

例：グループ・エントリへの自己書込みアクセス権の付与

この例では、US ドメイン内のユーザーに、特定のグループ・エントリ（例：`mailing list`）の `member` 属性に対して自分自身の名前（識別名）の追加または削除のみを行うアクセス権を許可します。

当該のグループ・エントリの `orclEntryLevelACI` 属性

```
access to attr=(member)
by dn=".*, dc=us,dc=acme,dc=com" (selfwrite)
```

ACL 評価の動作

ユーザーが指定されたオブジェクトで操作を実行しようとする、ディレクトリ・サーバーは、そのオブジェクト上で操作を実行するための適切なアクセス権がユーザーにあるかどうかを判断します。オブジェクトがエントリの場合、ディレクトリ・サーバーは、エントリおよびその各属性に対するアクセス権を系統的に評価します。

オブジェクト（エントリの属性も含む）へのアクセス権の評価は、そのオブジェクトの `ACI` ディレクティブすべての検証を必要とする場合があります。これは、`ACP` に階層的な特性があり、上位 `ACP` から従属 `ACP` にポリシーが継承されるためです。

ディレクトリ・サーバーは、最初にエントリ・レベル `ACI` (`orclEntryLevelACI`) の `ACI` ディレクティブを検証します。検証は最も近い `ACP` に進み、評価が完了するまで各上位 `ACP` を次々と考慮します。

ACL の評価時には、属性は次のいずれかの状態になります。

状態	説明
Resolved with permission	属性に対して要求されたアクセスは、ACI で付与されています。
否認による解決	属性に対して要求されたアクセスは、ACI で明示的に否認されています。
Unresolved	対象の属性に対して、適用可能な ACI がまだ見つかりません。

検索を除き、次の場合にはすべての操作の評価が停止します。

- エントリ自体に対するアクセス権が否認される
- 属性のいずれかが「否認による解決」の状態になる

この場合、操作は失敗し、ディレクトリ・サーバーはエラーをクライアントに戻します。

検索操作の場合は、すべての属性が「Resolved」の状態になるまで評価が続けられます。「否認による解決」の属性は戻されません。

ACL の評価の優先順位規則

LDAP の操作では、LDAP セッションの BindDN（つまりサブジェクト）に、そのオブジェクト（エントリ自体およびエントリの個々の属性を含む）で操作を実行するための特定の権限が必要です。

通常は、アクセス制御の管理認可レベルの階層があります。ネーミング・コンテキストのルートから、継承する管理ポイント（または ACP）までが 1 つの階層です。ACP は、orclACI 属性の定義済みの値を持つあらゆるエントリです。また、単一のエントリ固有のアクセス情報をそのエントリ（orclEntryLevelACI）内で示すこともできます。

ACL の評価には、LDAP 操作の実行に必要な権限が対象にあるかどうかを判別する処理が含まれています。通常、orclentryLevelACI または orclACI には、ACL の評価に必要な情報がすべて含まれているわけではありません。したがって、評価が完全に解決されるまで、使用可能なすべての ACL 情報が、一定の順序で処理されます。

処理の順序は次の規則に従います。

- エントリ・レベルの ACI が最初に検証されます。orclACI の ACI は、そのターゲット・エントリに一番近い ACP から順に上位方向に検証されます。
- 必要な権限が判別された時点で、評価は停止します。それ以外は評価が継続されます。

- 単一の ACI 内では、セッションの識別名と関連付けられているエンティティが、by 句で識別される複数の項目と一致している場合、有効なアクセス権が次のように評価されます。
 - 一致する by 句の項目内で付与された全権限の UNION
次の場合の AND 検索
 - 一致する by 句の項目内で否認された全権限の UNION

エントリ・レベルにおける優先順位 エントリ・レベルにおける ACI は、次の順序で評価されます。

1. フィルタを使用している場合。例：

```
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。例：

```
access to entry  
by group1 (browse, add, delete)
```

属性レベルにおける優先順位 属性レベルにおいては、属性が指定されている ACI が未指定の ACI よりも優先されます。

1. 属性が指定されている ACI は、次の順序で評価されます。

- a. フィルタを使用しているもの。例：

```
access to attr=(salary) filter=(salary > 10000)  
by group1 (read)
```

- b. フィルタを使用していないもの。例：

```
access to attr=(salary)  
by group1 (search, read)
```

2. 属性が未指定の ACI は、次の順序で評価されます。

- a. フィルタを使用している場合。例：

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

- b. フィルタを使用していない場合。例：

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

同一オブジェクトに対する複数 ACI

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

- ACI #1:

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

- ACI #2:

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

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

解決策は、同じ ACP において、このエントリに対して作成する ACI を 1 つのみにすることです。たとえば、次のようにします。

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

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

- ACI #1:

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

- ACI #2:

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

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

エントリに対する ACI と同様に、解決策は、同じ ACP においてこの属性に対して作成する ACI を 1 つのみにすることです。たとえば、次のようにします。

```
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の付与

指定したオブジェクトに ACL が存在している場合は、そのオブジェクト以外のすべてのオブジェクトに対してアクセス権を指定できます。そのためには、アクセス権をすべてのオブジェクトに付与するか、または 1 つのオブジェクトに対するアクセス権を否認します。

次の例は、アクセス権をすべての属性に付与します。

```
access to attr=(*)
by group2 (read)
```

次の例は、userpassword 属性に対するアクセス権を否認します。

```
access to attr!=(userpassword)
by group2 (read)
```

グループの場合の ACL 評価

属性またはエントリ自体の操作が、ディレクトリ情報ツリー内の下位の ACP で明示的に否認されている場合、通常、ACL によるその属性（またはエントリ）の評価は、否認による解決とみなされます。しかし、そのセッションのユーザー（bindDN）がグループ・オブジェクトのメンバーの場合、評価はまだ解決されていないかのように継続されます。グループの対象セクタを介して、ツリー内の上位の ACP でセッションのユーザーに権限が付与されている場合、この権限付与はツリー内の下位での否認よりも優先されます。

この例は、上位レベルの ACP の ACL ポリシーが、ディレクトリ情報ツリー内の下位の ACP ポリシーよりも優先される唯一のケースです。

LDAP 操作のアクセス・レベル要件

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

操作	必要なアクセス権
オブジェクトの作成	親エントリに対する「追加」アクセス権
変更	変更対象の属性に対する「書込み」アクセス権
識別名の変更	現行の親に対する「削除」アクセス権と新しい親に対する「追加」アクセス権
相対識別名の変更	ネーミング属性すなわち相対識別名属性に対する「書込み」アクセス権
オブジェクトの削除	削除対象のオブジェクトに対する「削除」アクセス権
比較	属性に対する「比較」アクセス権

操作	必要なアクセス権
検索	<ul style="list-style-type: none">■ フィルタ属性での「検索」アクセス権およびエントリでの「参照」アクセス権（エントリ識別名が結果として戻される必要がある場合）■ フィルタ属性での「検索」アクセス権、エントリでの「参照」アクセス権および属性での読取り権（その値が結果として戻される必要があるすべての属性について）

用語集

ACI

「[アクセス制御情報アイテム](#)」を参照。

ACL

「[アクセス制御リスト](#)」を参照。

ACP

「[アクセス制御ポリシー・ポイント \(Access Control Policy Point: ACP\)](#)」を参照。

API

「[Application Program Interface \(API\)](#)」を参照。

Application Program Interface (API)

指定したアプリケーションのサービスにアクセスするための一連のプログラム。たとえば、LDAP 対応のクライアントは、LDAP API で使用可能なプログラム・コールを通して、ディレクトリ情報にアクセスする。

Cipher Suite

SSL において、ネットワークのノード間でメッセージ交換に使用される認証、暗号化およびデータ整合性アルゴリズムのセット。SSL ハンドシェイク時に、2 つのノード間で折衝し、メッセージを送受信するときに使用する Cipher Suite を確認する。

configset

「[構成設定エントリ \(configuration set entry\)](#)」を参照。

DES

データ暗号化規格。1970 年代に IBM と米国政府によって公式規格として開発されたブロック暗号。

DIB

「[ディレクトリ情報ベース \(directory information base: DIB\)](#)」を参照。

Directory Integration Server

Oracle Directory Integration Platform 環境で、Oracle Internet Directory と [接続先ディレクトリ \(connected directory\)](#) との間でデータの同期化を実行するサーバー。

DIS

「[Directory Integration Server](#)」を参照。

DIT

「[ディレクトリ情報ツリー \(directory information tree: DIT\)](#)」を参照。

DN

「[識別名 \(distinguished name: DN\)](#)」を参照。

DRG

「[ディレクトリ・レプリケーション・グループ \(directory replication group: DRG\)](#)」を参照。

DSA

「[ディレクトリ・システム・エージェント \(directory system agent: DSA\)](#)」を参照。

DSE

「[ディレクトリ固有のエントリ \(directory-specific entry: DSE\)](#)」を参照。

DSA 固有のエントリ。異なる DSA に同じディレクトリ情報ツリー名を保持できるが、内容は異なる必要がある。つまり、DSE を保持している DSA に固有の内容を保持できる。DSE は、それを保持している DSA に固有の内容を含むエントリである。

Global Unique Identifier (GUID)

マルチマスター・レプリケーション環境では、複数のノードでレプリケートされるエントリは、各ノードで同じ識別名を持つ。ただし、識別名が同じでも、各ノードで異なる GUID が割り当てられる。たとえば、同じ識別名を **node1** と **node2** の両方でレプリケートできるが、**node1** に常駐しているときのその識別名に対する GUID は、**node2** におけるその識別名に対する GUID とは異なる。

GUID

「[Global Unique Identifier \(GUID\)](#)」を参照。

Internet Engineering Task Force (IETF)

新しいインターネット標準仕様の開発に従事する主要機関。インターネット・アーキテクチャおよびインターネットの円滑な操作の発展に関わるネットワーク設計者、運営者、ベンダーおよび研究者による国際的な団体である。

Internet Message Access Protocol (IMAP)

プロトコルの 1 種。クライアントは、このプロトコルを使用して、サーバー上の電子メール・メッセージに対するアクセスおよび操作を行う。リモートのメッセージ・フォルダ（メールボックスとも呼ばれる）を、ローカルのメールボックスと機能的に同じ方法で操作できる。

LDAP

「[Lightweight Directory Access Protocol \(LDAP\)](#)」を参照。

LDAP データ交換フォーマット (LDAP Data Interchange Format: LDIF)

LDAP コマンドライン・ユーティリティに使用する入力ファイルをフォーマットするための一連の規格。

LDIF

「[LDAP データ交換フォーマット \(LDAP Data Interchange Format: LDIF\)](#)」を参照。

Lightweight Directory Access Protocol (LDAP)

標準的で拡張可能なディレクトリ・アクセス・プロトコル。LDAP クライアントとサーバーが通信で使用する共通言語。業界標準のディレクトリ製品（Oracle Internet Directory など）をサポートする設計規則のフレームワーク。

MD4

128 ビットのハッシュまたはメッセージ・ダイジェスト値を生成する一方向ハッシュ関数。1 ビットでもファイルの値が変更された場合、そのファイルの MD4 チェックサムは変更される。元のファイルと同じ結果を MD4 で生成するようにファイルを偽造することはほぼ不可能である。

MD5

MD4 の改善されたバージョン。

MDS

「[マスター定義サイト \(master definition site: MDS\)](#)」を参照。

MTS

「[共有サーバー \(shared server\)](#)」を参照。

OEM

「[Oracle Enterprise Manager](#)」を参照。

OID 制御ユーティリティ (OID Control Utility)

サーバーの起動と停止のコマンドを発行するコマンドライン・ツール。コマンドは、[OID モニター \(OID Monitor\)](#) のプロセスによって解析され、実行される。

OID データベース・パスワード・ユーティリティ (OID Database Password Utility)

Oracle Internet Directory が Oracle データベースに接続するときのパスワードの変更に使用されるユーティリティ。

OID モニター (OID Monitor)

Oracle ディレクトリ・サーバー・プロセスの開始、監視および終了を実行する Oracle Internet Directory のコンポーネント。レプリケーション・サーバー（インストールされている場合）および Oracle Directory Integration Server の制御も行う。

Oracle Call Interface (OCI)

Application Program Interface (API) の 1 つ。これにより、第三代言語のネイティブ・プロシージャやファンクション・コールを使用して、Oracle データベース・サーバーにアクセスし、SQL 文の実行のすべての段階を制御するアプリケーションを作成できる。

Oracle Directory Integration Platform

[Oracle Internet Directory](#) のコンポーネントの 1 つ。Oracle Internet Directory のような中央 LDAP ディレクトリの周囲のアプリケーションを統合するために開発されたフレームワーク。

Oracle Directory Integration Server (DIS)

Oracle Directory Integration Platform 環境で、Oracle Internet Directory の変更イベントを監視し、[ディレクトリ統合プロファイル \(directory integration profile\)](#) の情報に基づいてアクションを行うデーモン・プロセス。

Oracle Directory Manager

Oracle Internet Directory を管理するための、Graphical User Interface (GUI) を備えた Java ベースのツール。

Oracle Enterprise Manager

Oracle 製品の 1 つ。グラフィカルなコンソール、エージェント、共通のサービスおよびツールを組み合わせ、Oracle 製品を管理するための統合された包括的なシステム管理プラットフォームを提供する。

Oracle Internet Directory

分散ユーザーやネットワーク・リソースに関する情報の検索を可能にする、一般的な用途のディレクトリ・サービス。LDAP バージョン 3 と Oracle9i の高度のパフォーマンス、拡張性、耐久性および可用性を組み合わせたもの。

Oracle Net Services

Oracle のネットワーク製品ファミリの基礎。Oracle Net Services を使用すると、サービスやアプリケーションを異なるコンピュータに配置して通信できる。Oracle Net Services の主な機能には、ネットワーク・セッションの確立およびクライアント・アプリケーションとサーバー間のデータ転送がある。Oracle Net Services は、ネットワーク上の各コンピュータに配置される。ネットワーク・セッションの確立後は、Oracle Net Services はクライアントとサーバーのためのデータ伝達手段として機能する。

Oracle PKI 証明書使用 (Oracle PKI certificate usages)

[証明書 \(certificate\)](#) でサポートされる Oracle アプリケーション・タイプを定義する。

Oracle Wallet Manager

セキュリティ管理者が、クライアントとサーバーにおける公開鍵のセキュリティ資格証明の管理に使用する Java ベースのアプリケーション。

Oracle9i レプリケーション (Oracle 9i Replication)

2 つの Oracle データベース間で、データベースの表を継続的に同期化できる Oracle9i の機能。

PKCS #12

[公開鍵暗号 \(public-key encryption\)](#) 規格 (PKCS)。RSA Data Security, Inc. の PKCS #12 は、個人的な認証資格証明を、通常 [Wallet](#) と呼ばれる形式で保管および転送するための業界標準である。

RDN

「[相対識別名 \(relative distinguished name: RDN\)](#)」を参照。

SASL

「[Simple Authentication and Security Layer \(SASL\)](#)」を参照。

Secure Hash Algorithm (SHA)

長さが 264 ビット未満のメッセージを取得して、160 ビットのメッセージ・ダイジェスト値を生成するアルゴリズム。このアルゴリズムは MD5 よりも若干遅いが、メッセージ・ダイジェスト値が大きくなることで、総当たり攻撃や反転攻撃に対してより強力に保護できる。

Secure Sockets Layer (SSL)

ネットワーク接続を保護するために Netscape Communications Corporation が開発した業界標準プロトコル。SSL では公開鍵インフラストラクチャ (PKI) を使用して、認証、暗号化およびデータの整合性を実現している。

SGA

「[システム・グローバル領域 \(System Global Area: SGA\)](#)」を参照。

SHA

「[Secure Hash Algorithm \(SHA\)](#)」を参照。

Simple Authentication and Security Layer (SASL)

接続ベースのプロトコルに認証サポートを追加する方法。この仕様を使用するために、プロトコルには、ユーザーを識別してサーバーに対して認証を行い、オプションで、後続のプロトコル対話に使用するセキュリティ・レイヤーを取り決めるコマンドが含まれる。このコマンドには、SASL 方式を識別する必須引数がある。

SLAPD

スタンドアロンの LDAP デーモン。

SSL

「[Secure Sockets Layer \(SSL\)](#)」を参照。

subACLSubentry

ACL 情報が含まれた特定のタイプのサブエントリ。

subSchemaSubentry

スキーマ情報が含まれた特定のタイプの[サブエントリ \(subentry\)](#)。

TLS

「[Transport Layer Security \(TLS\)](#)」を参照。

Transport Layer Security (TLS)

インターネット上の通信プライバシーを提供するプロトコル。このプロトコルによって、クライアント / サーバー・アプリケーションは、通信時の盗聴、改ざんまたはメッセージの偽造を防止できる。

UCS-2

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 ビット拡張とみなすことができる。

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記述法を含む。Unicode は Unicode Inc. によって所有および定義される。Unicode は標準的なエンコーディングであり、異なるロケールで値を伝達できることを意味する。しかし、Unicode とすべての Oracle キャラクタ・セットとの間で、情報の損失なしにラウンドトリップ変換が行われることは保証されない。

UNIX Crypt

UNIX 暗号化アルゴリズム。

UTC (Coordinated Universal Time)

世界中のあらゆる場所で共通の標準時間。以前から現在に至るまで広くグリニッジ時 (GMT) または世界時と呼ばれており、UTC は名目上は地球の本初子午線に関する平均太陽時を表す。UTC 形式である場合、値の最後に z が示される (例: 200011281010z)。

UTF-8

文字ごとに連続した 1、2 または 3 バイトを使用する **UCS-2** の可変幅エンコーディング。0 ~ 127 の文字 (7 ビット ASCII 文字) は 1 バイトでコード化され、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する。Wallet Resource Locator (WRL) は、Wallet の位置を特定するために必要な情報をすべて提供する。

X.509

公開鍵の署名に使用される ISO の一般的な形式。

アクセス制御情報アイテム (Access Control Information Item: ACI)

どのディレクトリ・データに対して、誰がどのタイプのアクセス権限を持っているかを判断する属性。この属性には、エントリに関係する構造型アクセス項目と、属性に関係するコンテンツ・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。

アクセス制御ポリシー・ポイント (Access Control Policy Point: ACP)

セキュリティ・ディレクティブを含むエントリ。このディレクティブは、**ディレクトリ情報ツリー (directory information tree: DIT)** 内の下位エントリすべてに適用される。

アクセス制御リスト (Access Control List: ACL)

アクセス・ディレクティブのグループ。管理者が定義する。ディレクティブは、特定のクライアントまたはクライアントのグループ、あるいはその両方に対して、特定データへのアクセスのレベルを付与する。

アドバンスド・レプリケーション (Advanced Replication: AR)

「[Oracle9i レプリケーション \(Oracle 9i Replication\)](#)」を参照。

アドバンスド・レプリケーション (ASR)

「[Oracle9i レプリケーション \(Oracle 9i Replication\)](#)」を参照。

暗号化 (cryptography)

データのエンコーディングとデコーディングを行い、保護メッセージを生成する作業。

暗号化 (encryption)

メッセージの内容を、宛先の受信者以外の第三者が読むことのできない形式（暗号文）に変換するプロセス。

一方向関数 (one-way function)

一方向への計算は容易だが、逆の計算、すなわち反対方向への計算は非常に難しい関数。

一方向ハッシュ関数 (one-way hash function)

可変サイズの入力を取得して、固定サイズの出力を作成する[一方向関数 \(one-way function\)](#)。

一致規則 (matching rule)

検索または比較操作における、検索対象の属性値と格納されている属性値との間の等価性の判断。たとえば、telephoneNumber 属性に関連付けられた一致規則では、(650) 123-4567 を (650) 123-4567 または 6501234567 のいずれかと一致させるか、あるいはその両方と一致させることができる。属性の作成時に、その属性を一致規則と対応付けることができる。

インスタンス (instance)

「[ディレクトリ・サーバー・インスタンス \(directory server instance\)](#)」を参照。

インポート・エージェント (import agent)

Oracle Directory Integration Platform 環境で、Oracle Internet Directory にデータをインポートするエージェント。

インポート・データ・ファイル (import data file)

Oracle Directory Integration Platform 環境で、[インポート・エージェント \(import agent\)](#)によってインポートされたデータを格納するファイル。

エージェント (agent)

「[ディレクトリ統合エージェント \(directory integration agent\)](#)」を参照。

エージェント・プロファイル (agent profile)

Oracle Directory Integration Platform 環境で、次の内容を指定する Oracle Internet Directory のエントリ。

- 統合エージェントの構成パラメータ
- 接続先ディレクトリと Oracle Internet Directory との間の同期化に適用するマッピング規則

エクスポート・エージェント (export agent)

Oracle Directory Integration Platform 環境で、Oracle Internet Directory からデータをエクスポートするエージェント。

エクスポート・データ・ファイル (export data file)

Oracle Directory Integration Platform 環境で、[エクスポート・エージェント \(export agent\)](#) によってエクスポートされたデータを格納するファイル。

エクスポート・ファイル (export file)

「[エクスポート・データ・ファイル \(export data file\)](#)」を参照。

エントリ (entry)

ディレクトリの基本単位で、ディレクトリ・ユーザーに関係のあるオブジェクトに関する情報が含まれている。

応答時間 (response time)

要求の発行から応答の完了までの時間。

オブジェクト・クラス (object class)

名前を持った属性のグループ。属性をエントリに割り当てるときは、その属性を保持しているオブジェクト・クラスをそのエントリに割り当てる。

同じオブジェクト・クラスに関連するオブジェクトはすべて、同じ属性を共有する。

介在者 (man-in-the-middle)

第三者によるメッセージの不正傍受などのセキュリティ攻撃。第三者、つまり介在者は、メッセージを復号化して再暗号化し（元のメッセージを変更する場合と変更しない場合がある）、元のメッセージの宛先である受信者に転送する。これらの処理はすべて、正当な送受信者が気付かないうちに行われる。この種のセキュリティ攻撃は、[認証 \(authentication\)](#) が行われていない場合にのみ発生する。

外部エージェント (external agent)

Oracle Directory Integration Server に依存しないディレクトリ統合エージェント。Oracle Directory Integration Server は外部エージェントに対して、スケジューリング、マッピングまたはエラー処理の各サービスを提供しない。外部エージェントは、通常、サード・パーティのメタディレクトリ・ソリューションを Oracle Directory Integration Platform に統合するときに使用する。

鍵 (key)

暗号化において広く使用されているビット列。データの暗号化と復号化を可能にする。鍵は別の数学的な操作にも使用される。暗号が与えられると、鍵によって、平文から暗号文へのマッピングが判断される。

鍵のペア (key pair)

公開鍵 (public key) とそれに対応する **秘密鍵 (private key)** のペア。

「**公開鍵と秘密鍵のペア (public/private key pair)**」を参照。

鍵ペア Wallet (single key-pair wallet)

単一のユーザー**証明書 (certificate)** とその関連する **秘密鍵 (private key)** が含まれる **PKCS #12** 形式の **Wallet**。**公開鍵 (public key)** は証明書に埋め込まれている。

拡張性 (scalability)

限定された使用可能なハードウェア・リソースに比例したスループットを提供するシステム機能。

簡易認証 (simple authentication)

ネットワークでの送信時に暗号化されない識別名とパスワードを使用して、クライアントがサーバーに対して自己認証を行うプロセス。簡易認証オプションでは、クライアントが送信した識別名とパスワードと、ディレクトリに格納されている識別名とパスワードが一致していることをサーバーが検証する。

管理領域 (administrative area)

ディレクトリ・サーバー上の 1 つのサブツリー。そのエントリは、1 つの管理認可レベル（スキーマ、ACL および共通属性）で制御される。

競合 (contention)

リソースの競合。

兄弟関係 (sibling)

1 つ以上の他のエントリと同じ親を持ったエントリ。

共有サーバー (shared server)

多数のユーザー・プロセスが、非常に少数のサーバー・プロセスを共有できるように構成されたサーバー。これにより、サポートされるユーザー数が増える。共有サーバー構成では、多数のユーザー・プロセスがディスパッチャに接続する。ディスパッチャは、複数の着信ネットワーク・セッション要求を共通キューに送る。複数のサーバー・プロセスの共有プールの中で、あるアイドル状態の共有サーバー・プロセスが共通キューから要求を取り出す。これは、サーバー・プロセスの小規模プールで大量のクライアントを処理できることを意味する。専用サーバーと対比。

継承 (inherit)

オブジェクト・クラスが別のクラスから導出されたときに、導出元のオブジェクト・クラスの多数の特性も導出（継承）されること。同様に、属性のサブタイプも、そのスーパータイプの特性を継承する。

ゲスト・ユーザー (guest user)

匿名ユーザーではなく、特定のユーザー・エントリも持っていないユーザー。

コールド・バックアップ (cold backup)

データベース・コピー・プロシージャを使用して、新規 **DSA** ノードを既存のレプリケート・システムに追加する手順。

公開鍵 (public key)

公開鍵暗号における一般に公開される鍵。主に暗号化に使用されるが、署名の検証にも使用される。

公開鍵暗号 (public-key cryptography)

公開鍵と秘密鍵を使用する方法に基づいた暗号化。

公開鍵暗号 (public-key encryption)

メッセージの送信側が、受信側の公開鍵でメッセージを暗号化するプロセス。配信されたメッセージは、受信側の秘密鍵で復号化される。

公開鍵と秘密鍵のペア (public/private key pair)

数学的に関連付けられた 2 つの数字のセット。1 つは秘密鍵、もう 1 つは公開鍵と呼ばれる。公開鍵は通常広く使用可能であるのに対して、秘密鍵はその所有者のみ使用可能である。公開鍵で暗号化されたデータは、それに関連付けられた秘密鍵でのみ復号化でき、秘密鍵で暗号化されたデータは、それに関連付けられた公開鍵でのみ復号化できる。公開鍵で暗号化されたデータを、同じ公開鍵で復号化することはできない。

構成設定エントリ (configuration set entry)

ディレクトリ・サーバーの特定インスタンスに関する構成パラメータを保持しているディレクトリ・エントリ。複数の構成設定エントリを格納でき、実行時に参照できる。構成設定エントリは、DSE の subConfigsubEntry 属性で指定されているサブツリー内でメンテナンスされる。DSE 自体は、サーバーの起動対象である関連の[ディレクトリ情報ベース \(directory information base: DIB\)](#) に常駐している。

コンシューマ (consumer)

レプリケーション更新の宛先となるディレクトリ・サーバー。スレーブと呼ばれることもある。

コンテキスト接頭辞 (context prefix)

[ネーミング・コンテキスト \(naming context\)](#) のルートの [DN](#)。

サービス時間 (service time)

要求の開始から、その要求に対する応答の完了までの時間。

サブエントリ (subentry)

サブツリー内のエントリ・グループに適用可能な情報が含まれているエントリのタイプ。情報には次の 3 つのタイプがある。

- アクセス制御ポリシー・ポイント
- スキーマ規則
- 共通属性

サブエントリは、管理領域のルートのすぐ下に位置している。

サブクラス (subclass)

別のオブジェクト・クラスから導出されたオブジェクト・クラス。導出元のオブジェクト・クラスは、その[スーパークラス \(superclass\)](#) と呼ばれる。

サブスキーマ識別名 (subschem DN)

独立したスキーマ定義を持つディレクトリ情報ツリー領域のリスト。

サブタイプ (subtype)

オプションを持たない同じ属性に対して、1 つ以上のオプションを持つ属性。たとえば、American English をオプションとして持つ commonName (cn) 属性は、そのオプションを持たない commonName (cn) 属性のサブタイプである。逆に、オプションを持たない commonName (cn) 属性は、オプションを持つ同じ属性の[スーパータイプ \(supertype\)](#) である。

サプライヤ (supplier)

レプリケーションにおいて、ネーミング・コンテキストのマスター・コピーを保持しているサーバー。マスター・コピーから **コンシューマ (consumer)**・サーバーに更新を供給する。

参照 (referral)

ディレクトリ・サーバーがクライアントに提供する情報で、要求する情報を見つけるためにクライアントが接続する必要がある他のサーバーを示す情報。

「**ナレッジ参照 (knowledge reference)**」も参照。

識別名 (distinguished name: DN)

ディレクトリ・エントリの一意名。親エントリの個々の名前がすべて、下からルート方向へ順に結合されて構成されている。

思考時間 (think time)

ユーザーが実際にプロセッサを使用していない時間。

システム・グローバル領域 (System Global Area: SGA)

共有メモリ構造の 1 グループ。1 つの Oracle データベース・インスタンスに関するデータと制御情報が含まれている。複数のユーザーが同じインスタンスに同時に接続した場合、そのインスタンスの SGA 内のデータはユーザー間で共有される。したがって、SGA は共有グローバル領域と呼ばれることもある。バックグラウンド・プロセスとメモリ・バッファの組合せは、Oracle インスタンスと呼ばれる。

システム固有のエージェント (native agent)

Oracle Directory Integration Platform 環境において、**Directory Integration Server** の制御下で実行される **エージェント (agent)**。

システム操作属性 (system operational attribute)

ディレクトリ自体の操作に関する情報を保持する属性。一部の操作情報は、サーバーを制御するためにディレクトリによって指定される (例: エントリのタイム・スタンプ)。アクセス情報などのその他の操作情報は、管理者が定義し、ディレクトリ・プログラムの処理時に、そのプログラムによって使用される。

従属参照 (subordinate reference)

エントリのすぐ下から始まるネーミング・コンテキストの参照位置を、ディレクトリ情報ツリー内で下位方向に指し示すナレッジ参照。

上位参照 (superior reference)

ディレクトリ情報ツリー内で、参照先の DSA が保持しているすべてのネーミング・コンテキストより上位のネーミング・コンテキストを保持している DSA を上位方向に指し示すナレッジ参照。

証明書 (certificate)

公開鍵に対して識別情報を安全にバインドする ITU x.509 v3 の標準データ構造。証明書は、エンティティの公開鍵が、信頼されている機関（**認証局 (certificate authority: CA)**）によって署名されたときに有効となる。この証明書は、そのエンティティの情報が正しいこと、および公開鍵がそのエンティティに実際に属していることを保証する。

証明連鎖 (certificate chain)

エンド・ユーザーまたはサブスクライバの証明書とその認証局の証明書を含む、順序付けられた証明書のリスト。

信頼できる証明書 (trusted certificate)

一定の信頼度を有すると認定された第三者の識別情報。信頼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る。一般的に、信頼されている認証局によってユーザーの証明書が発行される。

スーパークラス (superclass)

別のオブジェクト・クラスの導出元のオブジェクト・クラス。たとえば、オブジェクト・クラス `person` は、オブジェクト・クラス `organizationalPerson` のスーパークラスである。後者の `organizationalPerson` は、`person` の**サブクラス (subclass)** であり、`person` に含まれている属性を継承する。

スーパータイプ (supertype)

1 つ以上のオプションを持つ同じ属性に対して、オプションを持たない属性。たとえば、オプションを持たない `commonName (cn)` 属性は、オプションを持つ同じ属性のスーパータイプである。逆に、`American English` をオプションとして持つ `commonName (cn)` 属性は、そのオプションを持たない `commonName (cn)` 属性の**サブタイプ (subtype)** である。

スーパー・ユーザー (super user)

一般的にはディレクトリ情報へのあらゆるアクセスが可能な、特別なディレクトリ管理者。

スキーマ (schema)

属性、オブジェクト・クラスおよびそれらに対応する一致規則の集合体。

スポンサ・ノード (sponsor node)

レプリケーションにおいて、新規ノードに初期データを供給するために使用されるノード。

スマート・ナレッジ参照 (smart knowledge reference)

ナレッジ参照エントリが検索の有効範囲内にあるときに戻される**ナレッジ参照 (knowledge reference)**。要求された情報を格納しているサーバーを示す。

スループット (throughput)

Oracle Internet Directory が単位時間ごとに処理する要求の数。通常、「操作 / 秒」(1 秒当りの操作件数) で表される。

スレーブ (slave)

「[コンシューマ \(consumer\)](#)」を参照。

整合性 (integrity)

受信メッセージの内容が、送信時の元のメッセージの内容から変更されていないことを保証すること。

セッション鍵 (session key)

1 つのメッセージまたは 1 つの通信セッションの継続時間に使用される、対称鍵暗号方式の鍵。

接続記述子 (connect descriptor)

特別にフォーマットされた、ネットワーク接続の接続先の説明。接続記述子には、宛先サービスとネットワーク・ルート情報が含まれる。

宛先サービスを示すには、その Oracle9i リリース 1 (9.0.1) データベースに対応するサービス名、あるいは Oracle リリース 8.0 またはバージョン 7 のデータベースに対応する Oracle システム識別子 (SID) を使用する。ネットワーク・ルートは、少なくとも、ネットワーク・アドレスによってリスナーの位置を提供する。

接続先ディレクトリ (connected directory)

Oracle Directory Integration Platform 環境で、それ自体 (たとえば、Oracle Human Resource データベース) と Oracle Internet Directory との間で完全なデータの同期が必要な情報リポジトリ。

相対識別名 (relative distinguished name: RDN)

ローカルの最下位レベルのエントリ名。エントリのアドレスを一意に識別するために使用される他の修飾エントリ名は含まれない。たとえば、cn=Smith,o=acme,c=US では、cn=Smith が相対識別名である。

属性 (attribute)

エントリの性質を説明する断片的な情報項目。1 つのエントリは 1 組の属性から構成され、それぞれが [オブジェクト・クラス \(object class\)](#) に所属する。さらに、各属性にはタイプと値があり、タイプは属性の情報の種類を説明するものであり、値には実際のデータが格納されている。

属性構成ファイル (attribute configuration file)

Oracle Directory Integration Platform 環境で、接続先ディレクトリに関係のある属性を指定するファイル。

属性値 (attribute value)

エントリで表出される情報の特定の値。たとえば、jobTitle 属性に対する値には manager がある。

属性の型 (attribute type)

属性に含まれている情報の種類 (例: jobTitle)。

その他の情報リポジトリ (other information repository)

Oracle Internet Directory 以外のすべての情報リポジトリ。Oracle Directory Integration Platform 環境では、Oracle Internet Directory が **中央ディレクトリ (central directory)** として機能する。

待機時間 (latency)

指定したディレクトリ操作が完了するまでのクライアントの待機時間。待機時間は、空費時間として定義される場合がある。ネットワーク通信では、待機時間は、ソースから宛先へパケットが移動する時間として定義される。

待機時間 (wait time)

要求の発行から応答の開始までの時間。

中央ディレクトリ (central directory)

Oracle Directory Integration Platform 環境で、中央リポジトリとして機能するディレクトリ。Oracle Directory Integration Platform 環境では、Oracle Internet Directory が中央ディレクトリになる。

データ整合性 (data integrity)

受信メッセージの内容が、送信時の元のメッセージの内容から変更されていないことを保証すること。

ディレクトリ固有のエントリ (directory-specific entry: DSE)

ディレクトリ・サーバー固有のエントリ。異なるディレクトリ・サーバーに同じディレクトリ情報ツリー名を保持できるが、内容は異なる必要がある。つまり、DSE を保持しているディレクトリに固有の内容を保持できる。DSE は、それを保持しているディレクトリ・サーバーに固有の内容を含むエントリである。

ディレクトリ・サーバー・インスタンス (directory server instance)

ディレクトリ・サーバーの個々の起動のこと。異なるディレクトリ・サーバーの起動（それぞれ、同じまたは異なる構成設定エントリと起動フラグで起動）は、異なるディレクトリ・サーバー・インスタンスと呼ばれる。

ディレクトリ・システム・エージェント (directory system agent: DSA)

ディレクトリ・サーバーを表す X.500 の用語。

ディレクトリ情報ツリー (directory information tree: DIT)

エントリの識別名で構成されるツリー形式の階層構造。

ディレクトリ情報ベース (directory information base: DIB)

ディレクトリに保持されているすべての情報の完全なセット。DIB は、[ディレクトリ情報ツリー \(directory information tree: DIT\)](#) 内で、階層的に相互に関連するエントリで構成されている。

ディレクトリ同期プロファイル (directory synchronization profile)

Oracle Internet Directory と外部システム間の同期の実現方法を記述した特殊な[ディレクトリ統合プロファイル \(directory integration profile\)](#)。

ディレクトリ統合エージェント (directory integration agent)

Oracle Directory Integration Platform 環境で、接続先ディレクトリと Oracle Internet Directory との間の変更を同期化するために、接続先ディレクトリとの対話を行うプログラム。

ディレクトリ統合プロファイル (directory integration profile)

Oracle Directory Integration Platform 環境で、Oracle Directory Integration Platform が外部システムとどのように通信し、何を通信するかを示す Oracle Internet Directory のエントリ。

ディレクトリ・ネーミング・コンテキスト (directory naming context)

「[ネーミング・コンテキスト \(naming context\)](#)」を参照。

ディレクトリ・プロビジョニング・プロファイル (Directory Provisioning Profile)

Oracle Directory Integration Platform がディレクトリ対応アプリケーションに送信するプロビジョニング関連通知の性質を記述した特殊な[ディレクトリ統合プロファイル \(directory integration profile\)](#)。

ディレクトリ・レプリケーション・グループ (directory replication group: DRG)

レプリケーション承諾のメンバーであるディレクトリ・サーバーの集まり。

デフォルト・ナレッジ参照 (default knowledge reference)

ベース・オブジェクトがディレクトリになく、操作がサーバーによってローカルに保持されていないネーミング・コンテキストで実行されたときに戻される[ナレッジ参照 \(knowledge reference\)](#)。デフォルト・ナレッジ参照は、一般的にディレクトリ・パーティション化対策についてより多くのナレッジを持つサーバーに送信する。

統合エージェント (integration agent)

「[エージェント \(agent\)](#)」を参照。

同時クライアント (concurrent clients)

Oracle Internet Directory とのセッションを確立しているクライアントの総数。

同時操作 (concurrent operations)

すべての同時クライアントの要求に基づいてディレクトリで実行されている操作の数。一部のクライアントではセッションがアイドル状態の可能性があるため、この数は同時クライアントの数と必ずしも同じではない。

特定管理領域 (specific administrative area)

次の 3 つの側面を制御する管理領域。

- サブスキーマ管理
- アクセス制御管理
- 共通属性管理

特定管理領域では、この 3 つの管理面の 1 つが制御される。特定管理領域は、自律型管理領域の一部である。

匿名認証 (anonymous authentication)

ディレクトリがユーザー名とパスワードの組合せを要求せずにユーザーを認証するプロセス。各匿名ユーザーは、匿名ユーザー用に指定された権限を行使する。

ナレッジ参照 (knowledge reference)

リモート **DSA** に関するアクセス情報（名前とアドレス）およびそのリモート **DSA** が保持している **DIT** のサブツリーの名前。ナレッジ参照は、参照とも呼ばれる。

認可 (authorization)

オブジェクトまたはオブジェクトのセットへのアクセスのためにユーザー、プログラムまたはプロセスに与えられる許可。

認証 (authentication)

コンピュータ・システム内のユーザー、デバイスまたはその他のエンティティの識別情報を検証するプロセス。多くの場合、システム内のリソースへのアクセスを許可する前提条件として使用される。

認証局 (certificate authority: CA)

他のエンティティ（ユーザー、データベース、管理者、クライアント、サーバーなど）が本物であることを証明する信頼性のあるサード・パーティ。認証局は、ユーザーの識別情報を検証し、認証局の秘密鍵を使用して署名した証明書を発行する。

ネーミング・コンテキスト (naming context)

完全に 1 つのサーバーに常駐しているサブツリー。サブツリーは連続している必要がある。つまり、サブツリーの最上位の役割を果たすエントリから始まり、下位方向にリーフ・エントリまたは従属ネーミング・コンテキストへの[ナレッジ参照 \(knowledge reference\)](#) (参照とも呼ばれる) のいずれかまでを範囲とすることがある。単一のエントリからディレクトリ情報ツリー全体までを範囲とすることができる。

ネーミング属性 (naming attribute)

異なるタイプの [RDN](#) の値を保持する特別な属性。ネーミング属性は、そのニーモニック・ラベル (通常 cn、sn、ou、o、c など) で識別できる。たとえば、ネーミング属性 c は、ネーミング属性 country (国) のニーモニックで、特定の国の値に対応する相対識別名が保持されている。

ネット・サービス名 (net service name)

接続記述子に変換されるサービスの単純な名前。ユーザーは、接続するサービスに対する接続文字列内のネット・サービス名に従ってユーザー名とパスワードを渡すことによって、接続要求を開始する。次に例を示す。

```
CONNECT username/password@net_service_name
```

必要に応じて、ネット・サービス名は次のような様々な場所に格納できる。

- 各クライアントのローカル構成ファイル (tnsnames.ora)
- ディレクトリ・サーバー
- Oracle Names サーバー
- NDS、NIS または CDS などの外部ネーミング・サービス

パーティション (partition)

一意の重複していないディレクトリ・ネーミング・コンテキスト。1 つのディレクトリ・サーバーに格納されている。

パートナ・エージェント (partner agent)

Oracle Directory Integration Server がマッピング、スケジューリングおよびエラー処理を実行するためのディレクトリ統合エージェント。

バインド (binding)

ディレクトリに対して認証を行うプロセス。

ハッシュ (hash)

アルゴリズムを使用してテキスト文字列から生成される数値。ハッシュ値は、テキスト文字列より大幅に短くなる。ハッシュの数値は、セキュリティの目的とデータに対する高速アクセスの目的で使用する。

ハンドシェイク (handshake)

2 台のコンピュータが通信セッションを開始するために使用するプロトコル。

秘密鍵 (private key)

公開鍵暗号における秘密鍵。主に復号化に使用されるが、デジタル署名とともに暗号化にも使用される。

フィルタ (filter)

データ（通常、検索対象のデータ）を限定する方法。フィルタは、常に識別名で表される。

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（平文）に変換する処理。

プロキシ・ユーザー (proxy user)

通常、ファイアウォールなどの中間層を備えた環境で利用されるユーザー。このような環境では、エンド・ユーザーは中間層に対して認証を行う。この結果、中間層はエンド・ユーザーにかわってディレクトリにログインする。プロキシ・ユーザーには ID を切り替える権限があり、一度ディレクトリにログインすると、エンド・ユーザーの ID に切り替える。次に、その特定のエンド・ユーザーに付与されている認可を使用して、エンド・ユーザーのかわりに操作を実行する。

プロビジョニング・アプリケーション (provisioned applications)

ユーザーおよびグループの情報が Oracle Internet Directory に一元化される環境にあるアプリケーション。これらのアプリケーションは、一般的に Oracle Internet Directory 内の該当する情報に対する変更に関心がある。

プロビジョニング・エージェント (provisioning agent)

Oracle 固有のプロビジョニング・イベントを外部またはサード・パーティのアプリケーション固有のイベントに変換するアプリケーションまたはプロセス。

プロファイル (profile)

「[ディレクトリ統合プロファイル \(directory integration profile\)](#)」を参照。

並行性 (concurrency)

複数の要求を同時に処理できる機能。並行性メカニズムの例には、スレッドおよびプロセスなどがある。

平文 (plaintext)

暗号化されていないメッセージ・テキスト。

変更ログ (change logs)

ディレクトリ・サーバーに加えられた変更を記録するデータベース。

マスター・サイト (master site)

レプリケーションにおいて、マスター定義サイト以外のサイトで、LDAP レプリケーションのメンバーであるサイト。

マスター定義サイト (master definition site: MDS)

レプリケーションにおいて、管理者が構成スクリプトを実行する Oracle Internet Directory のデータベース。

マッピング規則ファイル (mapping rules file)

Oracle Directory Integration Platform 環境で、Oracle Internet Directory 属性と[接続先ディレクトリ \(connected directory\)](#) の属性との間のマッピングを指定するファイル。

メタディレクトリ (metadirectory)

企業のすべてのディレクトリ間で情報を共有するディレクトリ・ソリューション。すべてのディレクトリを1つの仮想ディレクトリに統合する。集中的に管理できるため、管理コストを削減できる。ディレクトリ間でデータが同期化されるため、企業内のデータに一貫性があり最新であることが保証される。

猶予期間ログイン (grace login)

パスワード期限切れ前の指定された期間内に行われるログイン。

リモート・マスター・サイト (remote master site: RMS)

レプリケート環境における[マスター定義サイト \(master definition site: MDS\)](#) 以外のサイトで、Oracle9i レプリケーションのメンバーであるサイト。

リレーショナル・データベース (relational database)

構造化されたデータの集合。同一の列のセットを持つ1つ以上の行で構成される表にデータが格納される。Oracle では、複数の表のデータを容易にリンクできる。このため、Oracle はリレーショナル・データベース管理システム、すなわち RDBMS と呼ばれる。Oracle はデータを複数の表に格納し、さらに表間の関係を定義できる。このリンクは両方の表に共通の、1つ以上のフィールドに基づいて行われる。

ルート DSE (root DSE)

「[ルート・ディレクトリ固有のエントリ \(root directory specific entry\)](#)」を参照。

ルート・ディレクトリ固有のエントリ (root directory specific entry)

ディレクトリに関する操作情報を格納するエントリ。情報は複数の属性に格納されている。

レジストリ・エントリ (registry entry)

Oracle ディレクトリ・サーバーの起動 (**ディレクトリ・サーバー・インスタンス (directory server instance)**) と呼ばれる) に関連する実行時情報が含まれているエントリ。レジストリ・エントリはディレクトリ自体に格納され、対応するディレクトリ・サーバー・インスタンスが停止するまで保持される。

レプリカ (replica)

ネーミング・コンテキストの個々のコピー。1 つのサーバー内に格納されている。

レプリケーション承諾 (replication agreement)

ディレクトリ・レプリケーション・グループ (directory replication group: DRG) 内のディレクトリ・サーバー間におけるレプリケーションの関係を記述する特別なディレクトリ・エントリ。

数字

1 レベルの検索, 7-3

389 ポート, 3-5, 3-7, A-44, A-46, C-6

636 ポート, 3-5, 3-7, A-44, A-46, C-6

A

accessDirectiveMatch 一致規則, C-10

ACI, 「アクセス制御情報アイテム (ACI)」を参照

ACP, 「アクセス制御ポリシー・ポイント (ACP)」を参照

ACP の検索

ボタン, 4-11

メニュー項目, 4-9

added_object_constraint フィルタ, 13-40

add.log, A-6

AlternateServers 属性、フェイルオーバー, 21-4

Apache Web サーバー

Delegated Administration Service が使用, 2-28

ログ・ファイルの位置, 9-7

稼働していることの検証, 9-8

B

backup_oid.sh, E-18

bitStringMatch 一致規則, C-10

BSTAT/ESTAT スクリプト, 20-8

bulkdelete, 4-14, 7-18, A-33

グローバルゼーション・サポート, 8-11

構文, A-33

bulkload, 4-14, 7-17, 7-18, A-34

.dat ファイル, 7-18

-load オプション, 7-18

グローバルゼーション・サポート, 8-9

構文, A-34

索引の作成, 7-18

チェック・モード、LDIF ファイルで実行, F-4

入力ファイルの生成, 7-18

ログ・ファイルの位置, 3-13

bulkmodify, 4-14

LDIF ファイルベースの変更, A-36

グローバルゼーション・サポート, 8-11

構文, A-36

C

C API, 2-20

caseExactIA5Match 一致規則, C-10

caseExactMatch 一致規則, C-10

caseIgnoreIA5Match 一致規則, C-10

caseIgnoreListMatch 一致規則, C-10

caseIgnoreMatch 一致規則, C-10

caseIgnoreOrderingMatch 一致規則, C-10

catalog.sh

ログ・ファイルの位置, 3-13

catalog.sh, 「カタログ管理ツール」を参照

changeLogEntry 属性, C-4

changeLog 属性, C-4

changeNumber 属性, C-4

changeStatusEntry 属性, C-4

changeStatus 属性, C-4

changetype 属性, C-4

add, A-17

delete, A-19

modify, A-17

modrdn, A-19

Cipher Suite

SSL, 12-2

SSL_RSA_WITH_3DES_EDE_CBC_SHA, 12-2

- SSL_RSA_WITH_NULL_MD5, 12-2
- SSL_RSA_WITH_NULL_SHA, 12-2
- SSL_RSA_WITH_RC4_128_SHA, 12-2
- SSL、サポート, 12-2
- Cluster Manager, 26-2
- cn 属性, 2-6
- commonName 属性, 2-6
- configNLDAP.ora, 24-9
- CPU
 - Oracle のフォアグラウンド・プロセスに関するチューニング, 20-6
 - 構成, 19-15
 - 様々な配置の使用例に必要なとなる能力, 14-9
 - 使用量, 14-11
 - 使用量のチューニング, 20-4
 - 処理能力, 19-15
 - チューニング, 20-4
 - チューニングが必要な場合, 20-4
 - 要件, 19-15
 - 詳細な計算, 19-16
 - 容量計画, 19-15
 - 容量計画, 19-2
- CPU の数
 - 要件, 19-16
- CPU の処理能力, 19-15
- createTimestamp 属性, 2-5, F-3
 - top 内のオプション, 2-9
- creatorsName 属性, 2-5, F-3
 - top 内のオプション属性, 2-9

D

- .dat ファイル、bulkload により生成, 7-18
- DB_BLOCK_BUFFERS, 20-8
- DBMS_STATS パッケージ, 20-2
- DBMS_STATS パッケージの ANALYZE ファンクション, 20-2
- Delegated Administration Service, 2-28
 - Apache Web サーバー
 - ログ・ファイルの位置, 9-7
 - HTTP サーバー, 9-4
 - Java サブレット, 9-4
 - ログ・ファイルの位置, 9-7
 - Single Sign-On, 9-8
 - アーキテクチャ, 9-4, 9-5
 - インストールと構成, 9-7
 - エンド・ユーザーの間接認証, 11-5

- 稼働していることの検証, 9-9
- コンポーネント, 9-4, 9-5
- ログ・ファイルの位置, 9-7
- DES40 暗号化, 11-2
- Directory Integration Server
 - LDAP 接続, 30-4
 - 起動, 30-8
 - 構成設定エントリ, 30-5
 - 再起動, 30-13
 - 実行時情報, 30-15
 - 情報の表示, 30-15
 - 停止, 30-11
 - 登録, 30-3
 - 登録ツール, 30-3
 - ログ・ファイルの位置, 3-13
- DirectoryReplicationGroupDSAs, 23-18
- distinguishedNameMatch 一致規則, C-10
- DIT, 「ディレクトリ情報ツリー」を参照
- DNS (ドメイン・ネーム・システム), 14-3
- DN, 「識別名」を参照
- DSA、環境の設定, 24-3
- 「DSE の変更」イベント, 5-31

E

- extensibleObject オブジェクト・クラス, 7-19

G

- generalizedTimeMatch 一致規則, C-10
- generalizedTimeOrderingMatch 一致規則, C-10
- groupOfNames オブジェクト・クラス, 7-8
- groupOfUniqueNames オブジェクト・クラス, 7-8

H

- HTTP サーバー
 - Delegated Administration Service が使用, 9-4

I

- IETF
 - Draft、Oracle Internet Directory で施行, C-3
 - LDAP 承認
 - Oracle Internet Directory で施行されている RFC, C-2
 - 規格の変更ログ・インタフェース, 28-11

initNLDAP.ora, 24-9
IntegerMatch 一致規則, C-10
Internet Engineering Task Force (IETF), 「IETF」を参照
iostat ユーティリティ, 20-2
I/O サブシステム, 19-6
 サイズ設定, 19-6
 要件, 19-6
 容量計画, 19-2, 19-6
I/O スループット、最大, 19-6
IP アドレス・テイクオーバー (IPAT), 21-8

J

Java クライアント、グローバル化バージョン・サポート, 2-13
Java サブプレット、Delegated Administration Service が使用, 9-4
 ログ・ファイルの位置, 9-7
Java ネイティブ・インタフェース, 2-20
jpegPhoto 属性, 2-6, 7-13
JPEG イメージ、ldapadd を使用した追加, A-6

K

Kerberos 認証, A-5, A-7, A-12

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
 検索のパフォーマンス, 20-12
 検索フィルタ、IETF 準拠, A-22
 構文, C-7
 Oracle Internet Directory で施行, C-7
 Oracle Internet Directory で認識, C-8, C-9
国際化対応, 2-13
サーバー
 管理, 5-1
 マルチスレッド, 1-9
サーバー・インスタンス, 2-17, 2-18, 2-19
 起動, 3-4, A-43
セキュリティ, 1-5
属性、一般的, 2-6

単純化されたディレクトリ管理, 1-5
追加または変更のパフォーマンス, 20-12
バージョン 3, 1-5
ldapadd, 4-13, 7-12, A-4
 JPEG イメージの追加, A-6
 LDIF ファイル, A-4
 エントリの追加, A-4
 グローバル化バージョン・サポート, 8-7
 構文, A-4
ldapaddmt, 4-13, 7-12, A-6
 LDIF ファイル, A-6
 グローバル化バージョン・サポート, 8-7
 構文, A-6
 複数エントリを同時に追加, A-6
 ログ, A-6
ldapbind, A-8
 グローバル化バージョン・サポート, 8-7
 構文, A-8
ldapbind 操作, 11-4
ldapcompare, 4-13, 7-13, A-10
 グローバル化バージョン・サポート, 8-7
 構文, A-10
ldapcreateConn.sh
 構文, A-27
ldapdelete, 4-13, 7-13, A-11
 エントリの削除, A-11
 グローバル化バージョン・サポート, 8-7
 構文, A-11
ldapmoddn, 4-13, 7-13, A-13
 グローバル化バージョン・サポート, 8-7
 構文, A-13
ldapmodify, 4-13, 7-12, A-15
 ACP の追加, 13-41
 LDIF ファイル, A-15
 エントリの削除, A-19
 エントリ・レベルの ACI の追加, 13-41
 オブジェクト・クラス追加, 6-13
 オブジェクト・クラスの変更, 6-13
 監査レベルの変更, 5-32
 グループ・エントリの作成, A-18
 グローバル化バージョン・サポート, 8-7
 構文, A-15
 属性値の置換, A-18
 属性追加, 6-27, 6-28
 属性の変更, 6-27, 6-28
 複数値の属性への値追加, A-18
 変更の種類, A-17

ldapmodifymt, 4-13, 7-12, A-20
LDIF ファイル, A-20
グローバリゼーション・サポート, 8-7
構文, A-20
使用, A-20
マルチスレッド処理, A-21
ldaprepl.sh, 23-8
ldapsearch, A-22, A-26, A-27
監査ログの問合せ, 5-28
グローバリゼーション・サポート, 8-7
構文, A-22
フィルタ, A-24
ldapUploadAgentFile.sh
構文, A-26, A-27
LDAP ディスパッチャ
ログ・ファイルの位置, 3-14
LDAP データ交換フォーマット (LDIF), 4-12, A-2
bulkload 使用時, A-34
構文, A-2
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, 4-12, A-2
ディレクトリ・データの変換, 7-18
ファイル
ldapaddmt コマンド, A-6
ldapadd コマンド, A-4
ldapmodifymt コマンド, A-20
ldapmodify コマンド, A-15
移行での独自データの削除, F-3
インポート、bulkload を使用, 7-16
構成設定エントリの追加, 5-11
コマンドでの参照, 5-12
作成, 5-11
ファイルベースの変更、bulkmodify では
未サポート, A-36
ldifwrite, 4-14, A-38
グローバリゼーション・サポート, 8-10
構文, A-38
listener.ora, 23-7, 24-7
LOAD_BALANCE パラメータ、Oracle Net Services,
26-7
-load オプション、bulkload, 7-18
LSNRCTL ユーティリティ, 23-7

M

maxextents, 23-6
MD4, 5-14, 5-16, 17-3, F-4
MD5, 5-14, 5-16, 17-3, F-4
パスワード暗号化, 17-2, 17-4
member 属性, 7-8
Microsoft Active Directory, 14-2
modifiersName 属性, 2-5, F-3
top 内のオプション, 2-10
modifyTimestamp 属性, 2-5, F-3
top 内のオプション, 2-10
mpstat ユーティリティ, 20-2

N

namingContexts 属性, 5-16, 5-17
複数値, 5-17
newdb.sql, 24-10
NOS ディレクトリ, 14-2, 14-3
Novell の eDirectory ソリューション, 14-2
NULL 値、属性, 6-3
numericStringMatch 一致規則, C-10

O

objectclass 属性, 5-29
objectIdentifierFirstComponentMatch 一致規則, C-10
ObjectIdentifierMatch 一致規則, C-10
OCI, 「Oracle Call Interface」を参照
OctetStringMatch 一致規則, C-10
odisrvreg, 30-3
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-44
oidldapd
ログ・ファイルの位置, 3-14
oidmon, 「OID モニター」を参照
oidprovtool
位置, 36-8
OIDREPLD, 3-7, A-46
oidstats.sh ユーティリティ, A-55
OID 制御ユーティリティ, 3-2, 4-15
restart コマンド, 5-4
構文, A-42
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, 4-15
- サーバーの停止コマンド, 4-15
- OID 調停ツール, 4-15, 23-32, A-52, A-53
 - 構文, A-52
- OID データベース統計収集ツール, 4-16
 - 構文, A-55
- OID データベース統計収集ツールの構文, A-55
- OID データベース・パスワード・ユーティリティ, 4-15, 5-36
- OID パスワード・ユーティリティ, 3-12, 4-15
- OID モニター, 2-18, 4-15, 28-12
 - 開始, 3-2, 3-3, A-41
 - 構文, A-41
 - スリープ・タイム, 3-2, A-41
 - 停止, 3-3, A-42
 - ログ・ファイルの位置, 3-14
- OLTS_ATTRSTORE 表領域, 19-11, 20-9
- OLTS_CT_CN 表領域, 19-11
- OLTS_CT_DN 表領域, 19-11, 20-9
- OLTS_CT_OBJCL 表領域, 19-12
- OLTS_CT_STORE 表領域, 19-12
- OLTS_DEFAULT 表領域, 19-12
- OLTS_IND_ATTRSTORE, 20-9
- OLTS_IND_ATTRSTORE 表領域, 19-11
- OLTS_IND_CT_DN, 20-9
- OLTS_IND_CT_DN 表領域, 19-11
- OLTS_IND_CT_STORE 表領域, 19-12
- OPEN_CURSORS, 20-10
- OpenLDAP Community, xl
- Optimal Flexible Architecture (OFA), 24-2
- Oracle Call Interface, 2-21
- Oracle Directory Integration Platform
 - 概要, 2-28, 2-29, 28-2
 - データ所有権に関するポリシーの遵守, 2-29
 - ログ・ファイル, 30-15
- Oracle Directory Manager, 7-2
 - Oracle Directory Integration Platform, 28-12
 - UNIX、起動, 4-3
 - Windows 95、起動, 4-3
 - Windows NT、起動, 4-3
 - アクセス権の付与, 13-12
 - 「アクセス制御ポリシー・ポイントを作成します」メニュー, 4-9
 - 「以下」フィルタ, 5-33, 6-8, 7-4
 - 「以上」フィルタ, 5-33, 6-8, 7-4
 - エントリの管理, 4-12
 - 「エントリの作成」メニュー項目, 4-9
 - 「エントリのリフレッシュ」ボタン, 4-10
 - オブジェクト・クラスの作成, 4-9
 - 「オブジェクトの検索」ボタン, 4-10, 6-6
 - オブジェクトの削除, 4-8
 - 「回復」ボタン, 4-7
 - 概要, 4-2, 4-8
 - 「完全一致」フィルタ, 5-33, 6-7, 7-4
 - 管理
 - ACP, 4-12
 - エントリ, 4-12
 - 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
 - Sun Solaris, 4-3
 - 「切離し」メニュー項目, 4-8
 - 検索
 - エントリ, 7-2
 - オブジェクト, 4-10
 - 属性, 6-18
 - 検索基準バー, 5-33, 7-3
 - 検索のルート, 7-2
 - 検索フィルタ, 6-7
 - 更新, 4-8
 - サブツリー・エントリ・データ, 4-10
 - 削除
 - オブジェクト, 4-10
 - 構成設定エントリ, 5-4
 - 「削除」ボタン, 4-10
 - 「作成」ボタン, 4-10
 - 「サブツリー・エントリのリフレッシュ」ボタン, 4-10
 - 実行方法, 4-3
 - 「終了」フィルタ, 6-7
 - 「終了」メニュー項目, 4-8
 - スキーマの管理, 4-12
 - 「操作」メニュー, 4-9
 - 属性構文の型の選択, 6-31
 - 属性の型のリスト, A-3
 - 「属性の検索」ボタン, 6-18
 - 属性の作成, 4-9
 - 属性の表示, 7-5
 - 属性、検索, 6-18
 - 「存在」フィルタ, 5-33, 6-8, 7-4
 - 追加
 - ACP, 13-15
 - エントリ, 7-6
 - オブジェクト, 4-8

- オブジェクト・クラス, 6-10
- グループ・エントリ, 7-8
- 構成設定エントリ, 5-4
- 属性, 6-20
- ツールバー, 4-10
- 定義, 1-8
- ディレクトリ・サーバーからの切断, 4-8
- ディレクトリ・サーバーへの接続, 4-8, 4-10
- ディレクトリ統合エージェントの登録, 28-11
- 「適用」ボタンと「OK」ボタンの比較, 4-7
- 「取消」ボタン, 4-7
- ナビゲート, 4-7
- ページ・スケジュール、設定, 23-15
- 「ビュー」メニュー, 4-8
- 「ファイル」メニュー, 4-8
- ヘルプ・ナビゲータの表示, 4-9
- 「ヘルプ」ボタン, 4-11
- 「ヘルプ」メニュー項目, 4-9
- 変更
 - エントリ, 7-9
 - オブジェクト, 4-8, 4-10
 - オブジェクト・クラス, 6-11
 - 構成設定エントリ, 2-20, 5-4
 - レプリケーション承諾, 23-18
- 「編集」ボタン, 4-10
- 「編集」メニュー, 4-8
- メニュー・バー, 4-8
- 「リフレッシュ」ボタン, 4-10
- 「類似項目の作成」の操作, 4-8
- 「類似項目の作成」ボタン, 4-10, 7-7
- Oracle Directory Manager の「接続」ボタン, 4-10
- Oracle Directory Provisioning Integration Service
 - アンインストール, 36-8
 - 管理, 36-9
 - サブスクリプション, 36-8
 - トラブルシューティング, 36-15
 - 配置, 36-9
- Oracle HR
 - インポート, 33-2
 - 属性マッピング・ルール
 - 削除, 33-15
 - 作成, 33-14
 - 変更, 33-15
 - 同期化, 33-1
 - 同期化される属性, 33-8
 - 同期の実行, 33-16
- Oracle HR エージェント, 33-1
 - 統合プロファイルの構成, 33-4
 - マッピング・ルール, 33-12
 - デフォルト, 33-13
- Oracle Internet Directory
 - 同一ホストへの複数インストール, 14-12
 - 利点, 1-9
- Oracle Internet Directory で施行されている RFC, C-2
- Oracle Net Services, 2-18, 2-21
 - LOAD_BALANCE パラメータ, 26-7
 - レプリケーションの準備, 23-4
- Oracle Provisioning Integration Service
 - セキュリティ, 36-11
- Oracle SQL*Loader、bulkload で使用, A-34
- Oracle Wallet
 - 位置の変更
 - ldapaddmt を使用, A-8
 - ldapadd を使用, A-6
 - ldapbind を使用, A-9
 - ldapcompare を使用, A-11
 - ldapdelete を使用, A-13
 - ldapmoddn を使用, A-15
 - ldapmodifymt を使用, A-22
 - ldapmodify を使用, A-16
 - ldapsearch を使用, A-24
- Oracle Wallet Manager, D-1
- Oracle9i, 2-21
 - データベース, 2-17
- Oracle9i
 - Replication Manager、構成, 23-4
- Oracle9i Real Application Clusters, liii
- Oracle9i Real Application Clusters, 26-1
- Oracle9i レプリケーション, 22-3, 23-8
 - Oracle9i とともにインストール, 23-3
 - インストール, 23-4
 - 構成, 23-4, 23-8
 - Oracle9i Replication Manager を使用, 23-4
 - ディレクトリ・レプリケーション用, 23-8
 - 設定, 23-4
- Oracle インスタンス, 用語集 -13
- Oracle グローバリゼーション・サポート, 2-13
- Oracle ディレクトリ・サーバー・インスタンス, 1-8, 2-17, 2-18, 2-19
 - 管理, 5-1
 - 起動, 3-4, 23-11, A-43
 - 停止, 3-5, A-43, A-44

Oracle ディレクトリ・レプリケーション・サーバー・
インスタンス, 1-8, 2-17, 2-18
起動, 3-6, 3-7, 23-11, A-45, A-46
構成パラメータ、位置, 23-13
停止, 3-7, A-45, A-46
Oracle データ・サーバー
エラー・メッセージ, H-10
パスワードの変更, 4-15, 5-36
Oracle のフォアグラウンド・プロセス
CPU のチューニング, 20-6
Oracle バックグラウンド・プロセス, 20-11
orclACI, 13-2, 13-3, C-3
top 内のオプション属性, 2-10
アクセス, 13-3
orclAgreementID, 23-18, 23-20
orclAgreementId, C-4
orclauditattribute, C-5
orclAuditLevel, C-5
orclauditlevel 操作属性, 5-28
orclauditlevel 属性, 5-31
orclauditmessage, C-5
orclauditmessage 属性, 5-29
orclauditoc オブジェクト・クラス, 5-29
orclauditoc 属性, 5-29
orclCatalogEntryDN, C-4
orclChangeLogLife, 23-14
orclChangeRetryCount, 23-14, 23-17, C-4
orclChangeSubscriber, 29-5
orclConfigSet, C-4
orclconfigsetnumber, C-4
orclConsumerReference, C-4
orclcontainerOC, C-4
orclCryptoScheme 属性, 5-16
orclDBType, C-4
orcldebugflag, 5-27
orclDebugLevel, C-4
orcldebuglevel 構成設定エントリ, C-5
orclDirReplGroupAgreement, 23-13, 23-14, C-4
orclDirReplGroupDSAs, 23-20, 23-21, C-4
orclDITRoot, C-4
orclEntryLevelACI, 13-3, C-3
top 内のオプション属性, 2-10
orcleventLog, C-4
orclEvents, C-4
orcleventtime, C-5
orcleventtime 属性, 5-29
orcleventtype, C-5

orcleventtype 属性, 5-29
orclExcludedNamingcontexts, 23-20, C-4
orclGuid, C-4
top 内のオプション属性, 2-9
orclGuName, C-4
orclguname 属性, 5-20
orclGuPassword, C-4
orclgupassword 属性, 5-20
orclhostname, C-4
orclIndexedAttribute, C-4
orclIndexOC, C-4
orclLastAppliedChangeNumber 属性, 35-7
orcllastChangeLogNumber, 29-5
orclLDAPInstance, C-4
orclLDAPSubConfig, C-4
ORCLMAXCC, 20-5
orclMaxCC, C-4
orclmaxcc, 2-19
orclmaxcc 構成設定エントリ, C-5
orclOdipAgentConfigInfo, 29-5
orclodiProfile, 29-5
orclOpResult, C-5
orclopresult 属性, 5-29
orclParentGUID, C-4
orclPrivilegeGroup, 7-8
orclPrName, C-4
orclprname 属性, 5-20
orclPrPassword, C-4
orclprpassword 属性, 5-20
orclPurgeSchedule, 23-14, 23-16, C-4
orclpwdAlphaNumeric 属性, 18-5
orclpwdIllegalValues 属性, 18-5
orclpwdToggle 属性, 18-5
orclReplAgreementEntry, C-4
orclReplBindDN, C-4
orclReplBindPassword, C-4
orclReplicationProtocol, 23-20, C-4
orclREPLInstance, C-4
orclREPLSubConfig, C-4
orclSequence, C-5
orclsequence 属性, 5-29, 5-30
orclServerEvent, C-5
orclServerMode, C-4
orclServerMode 属性, 5-16
ORCLSERVERPROCS, 20-5
orclServerProcs, C-4
orclserverprocs 構成設定エントリ, C-5

orclSizeLimit, C-4
orclSizeLimit 属性, 5-16
orclssl authentication 構成設定エントリ, C-6
orclsslAuthentication, C-5
orclsslEnable, C-5
orclsslenable, C-6
orclsslenable 構成設定エントリ, C-6
orclsslPort, C-5
orclsslport 構成設定エントリ, C-6
orclsslVersion, C-5
orclsslWalletPasswd, C-5
orclsslwalletpasswd 構成設定エントリ, C-7
orclsslWalletURL, C-5
orclsslwalleturl 構成設定エントリ, C-6
orclSuffix, C-4
orclSuName, C-4
orclsuname 属性, 5-20
orclSuPassword, C-4
orclsupassword 属性, 5-20
orclSupplierReference, C-4
orclThreadsPerSupplier, 23-14
orclTimeLimit, C-4
orclTimeLimit 属性, 5-16
orclUpdateSchedule, 23-20, C-4
orclUseEncrypt, C-4
orcluserdn, C-5
orcluserdn 属性, 5-29
organizationalUnitName, 2-6
organization 属性, 2-6
o 属性, 2-6

P

PKI 認証, 11-2
presentationAddressMatch 一致規則, C-10
protocolInformationMatch 一致規則, C-10
pwdCheckSyntax 属性, 18-5
pwdExpireWarning, 18-3
pwdExpireWarning 属性, 18-5
pwdFailureCountInterval, 18-3
pwdFailureCountInterval 属性, 18-5
pwdGraceLoginLimit 属性, 18-5
pwdLockout, 18-3
pwdLockoutDuration, 18-4
pwdLockoutDuration 属性, 18-5
pwdLockout 属性, 18-5
pwdMaxAge, 18-3

pwdMaxAge 属性, 18-5
pwdMaxFailure, 18-3
pwdMaxFailure 属性, 18-5
pwdMinLength 属性, 18-5
pwdPolicy オブジェクト・クラスの属性, 18-5

R

RAID, 20-9
RC4_40 暗号化, 11-2
RDN, 「相対識別名」を参照
Real Application Clusters, 26-7
 ディレクトリ・フェイルオーバー, 26-1
REDO ログ・バッファ・パラメータ, 20-11
referral オブジェクト・クラス, 7-19
ref 属性, 7-19
restart コマンド, 30-13

S

SASL, 「Simple Authentication and Security Layer (SASL)」を参照
Secure Hash Algorithm (SHA), 5-14, 5-16, 17-3
Secure Sockets Layer (SSL), 31-2
 Oracle Directory Manager で使用可能にする方法, 4-6
 管理, 12-1
 構成, 4-4
server mode, 5-15
SESSIONS パラメータ, 20-10
SGA, 「システム・グローバル領域 (SGA)」を参照
SHA, 5-14, 5-16, 17-3, F-4
 パスワード暗号化, 17-3, 17-4
Simple Authentication and Security Layer (SASL), LDAP バージョン 3, 1-5
Single Sign-On、Delegated Administration Service と統合, 9-8
SMP システムにおけるプロセッサ親和性, 20-6
sn 属性, 2-6
SPECint_rate95 ベースライン, 19-15
sqlnet.ora、レプリケーション用の構成, 23-5
SSL, 4-6, 12-3, 12-4, 12-5
 Cipher Suite, 12-2
 Oracle Internet Directory でサポート, 12-2
 SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA, 12-2

SSL_DH_anon_EXPORT_WITH_RC4_40_MD5, 12-2
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA, 12-2
SSL_DH_anon_WITH_DES_CBC_SHA, 12-2
SSL_DH_anon_WITH_RC4_128_MD5, 12-2
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA, 12-2
SSL_RSA_EXPORT_WITH_RC4_40_MD5, 12-2
SSL_RSA_WITH_DES_CBC_SHA, 12-2
SSL_RSA_WITH_NULL_SHA, 12-2
SSL_RSA_WITH_RC4_128_MD5, 12-2
Wallet, C-6
オン・オフの切替え, C-6
クライアントとサーバーの認証, C-6
クライアントの使用例, 12-3
厳密認証, 11-2
構成, 4-4, 12-3
構成パラメータ, 12-3
 変更, 12-4
使用可能, 12-3
 ldapaddmt を使用, A-8
 ldapadd を使用, A-6
 ldapbind を使用, A-9
 ldapmodifymt を使用, A-21
 ldapmodify を使用, A-16
 ディレクトリ・サーバー, C-6
使用禁止, C-6
属性値, C-5
データ・プライバシー, 1-9
デフォルト・ポート, C-6
認証, 13-9
 Oracle Directory Manager, 4-7
 サーバー, 4-7
 サーバーのみ, 4-7
認証アクセス, 1-9
認証なし, 4-7, C-6
バージョン 2, 12-3
バージョン 3, 12-3
パラメータ, 12-3
 Oracle Directory Manager を使用した構成, 12-4
 構成, 12-3
 コマンドライン・ツールを使用して構成, 12-5
ハンドシェイク, 12-2
ポート 636, 12-3
ユーザーの Wallet へのパスワード, 4-6

SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA, 12-2
「SSL 認証なし」オプション, 4-7
subconfig, C-4
subregistry, C-4
subSchemaSubentry
 オブジェクト・クラスの追加, 2-12
 スキーマ定義の保持, 2-12
 変更, 2-12
Sun Solaris、Oracle Directory Manager の起動, 4-3
surname 属性, 2-6
SYSTEM 表領域, 19-12

T

targetDN, C-4
TCP/IP 接続, 21-5, 21-8, C-6
telephoneNumberMatch 一致規則, C-10
tnsnames.ora
 コールド・バックアップ, 24-8
 レプリケーション用の構成, 23-5
top オブジェクト・クラス, 2-9
 オプション属性, 2-9
top ユーティリティ, 20-2
Transport Layer Security (TLS)、LDAP バージョン 3, 1-5

U

Unicode Transformation Format 8-bit (UTF-8), 2-13
uniqueMemberMatch 一致規則, C-10
UNIX Crypt、パスワード暗号化, 5-14, 5-16, 17-3, 17-4, F-4
UNIX Crypt、パスワード・ハッシング, 17-3
UNIX、Oracle Directory Manager の起動, 4-3
userPassword 属性、ハッシュ値, F-4
UTF-8、「Unicode Transformation Format 8-bit」を参照
UTLBSTAT.SQL, 20-2
UTLESTAT.SQL, 20-2

V

vmstat ユーティリティ, 20-2

W

Wallet

- 位置, C-6
- オープン, D-5
- 管理, D-3
- クローズ, D-5
- 削除, D-7
- 作成, 5-6, 5-8, 5-10, 12-5, C-7, D-4
- 自動ログイン, D-8
- 証明書の管理, D-9
- 信頼できる証明書の管理, D-12
- パスワード, 4-6
- パスワードの変更, D-7
- 保存, D-5

Windows NT

- Oracle Directory Manager の起動, 4-3
- Performance Monitor, 20-2
- タスク・マネージャ, 20-2

あ

アーキテクチャ

- Oracle Internet Directory, 2-1

アクセス

- LDAP 操作のレベル要件, 13-48
- 違反イベント, 5-31
- オブジェクト, 13-7
- 権限、Oracle Directory Manager を使用して設定, 13-19, 13-32
- 項目
 - 構造型, 13-14
 - コンテンツ, 13-14
- 種類, 13-10
- 選択、識別名による, 13-42
- 操作, 13-10
- 対象, 13-8
- 付与
 - Oracle Directory Manager を使用, 13-12
 - エントリ・レベル、Oracle Directory Manager を使用, 13-36
 - エントリ・レベル、コマンドライン・ツールを使用, 13-41
 - コマンドライン・ツールを使用, 13-40
- 未指定, 13-11, 13-32

アクセス制御

- Directory Integration Server, 31-4
- Oracle Directory Integration Platform, 31-4
- エージェント, 31-5
- 概念の説明, 11-3
- 概要, 1-9
- 管理, 13-1
 - Oracle Directory Manager を使用, 13-12
 - コマンドライン・ツールを使用, 13-40
- 管理の構造体, 13-2
- 規定, 13-3
- 設定、ワイルド・カードを使用, 13-42
- 定義, 2-12
- ディレクティブ書式、「ACI ディレクティブ書式」を参照
- 認可, 2-12
- ポリシー
 - 競合, 13-2
 - 継承, 13-2
 - ポリシー管理、概要, 13-2
- アクセス制御情報アイテム (ACI)
 - 項目
 - 構文, B-1
 - 書式, B-1
 - コンポーネント, 13-7
 - 属性, 11-3
 - ディレクティブ
 - 書式, 11-3
 - ディレクティブのオブジェクト, 13-7
 - ディレクティブの対象, 13-8
- アクセス制御ポリシー・ポイントの競合, 13-2
- 優先順位
 - 解消するための規則, 13-2
- アクセス制御ポリシー・ポイント (ACP), 13-2, 13-15
 - ACP 作成ウィザードを使用した作成, 13-22
 - 管理、Oracle Directory Manager を使用, 4-12
 - 構造型アクセス項目, 13-14
 - コンテンツ・アクセス項目, 13-14
 - 作成ウィザード, 13-22
 - 追加
 - ldapmodify を使用, 13-41
 - Oracle Directory Manager の ACP 作成ウィザードを使用, 13-22
 - Oracle Directory Manager を使用, 4-9, 13-15
- 表示, 13-13
 - Oracle Directory Manager を使用, 13-13, 13-14

- 表示の構成、Oracle Directory Manager, 13-12
- 表示、Oracle Directory Manager を使用, 13-13, 13-14
- 複数, 13-2
- アクセス制御リスト (ACL), 2-21, 11-3
 - グループ, 13-48
 - サブツリー, 13-2
- 処理, 5-27
- ディレクティブ、エントリ内, 13-3
- 動作, 13-44
- 評価
 - グループ, 13-48
 - 優先順位規則, 13-45
- 変更, 5-31
- 優先順位
 - 規則, 13-45
- 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, 5-35
- 値、属性の削除, A-18
- アドバンスト・レプリケーション, 「Oracle9i レプリケーション」を参照
- アプリケーション
 - 登録、プロビジョニング, 36-3
 - 自動, 36-3
 - 手動, 36-3
- アプリケーション固有リポジトリ、データの移行, I-1
- 暗号化
 - DES40, 11-2
 - Oracle Internet Directory で使用可能なレベル, 11-2
 - RC4_40, 11-2
 - パスワード, 11-7
 - UNIX Crypt, 17-3, 17-4

い

- 「以下」フィルタ, 5-33, 6-8, 7-4
- 移行
 - アプリケーション固有のリポジトリから
 - 中間テンプレート・ファイル, I-2
- 「以上」フィルタ、Oracle Directory Manager, 5-33, 6-8, 7-4
- 以前のリリースからのアップグレード, E-17
 - LDIF ベース, E-18
 - 単一ノード環境, E-18
 - マルチノード環境, E-18

- 一致規則, C-10
 - accessDirectiveMatch, C-10
 - bitStringMatch, C-10
 - caseExactIA5Match, C-10
 - caseExactMatch, C-10
 - caseIgnoreIA5Match, C-10
 - caseIgnoreListMatch, C-10
 - caseIgnoreMatch, C-10
 - caseIgnoreOrderingMatch, C-10
 - distinguishedNameMatch, C-10
 - generalizedTimeMatch, C-10
 - generalizedTimeOrderingMatch, C-10
 - IntegerMatch, C-10
 - numericStringMatch, C-10
 - objectIdentifierFirstComponentMatch, C-10
 - ObjectIdentifierMatch, C-10
 - OctetStringMatch, C-10
 - Oracle Directory Manager のタブ, 6-9
 - Oracle Internet Directory で認識, C-10
 - presentationAddressMatch, C-10
 - protocolInformationMatch, C-10
 - subSchemaSubentry への追加不可, 2-12
 - telephoneNumberMatch, C-10
 - uniqueMemberMatch, C-10
 - スキーマ内のメタデータとして, 2-12
 - スキーマに格納, 2-12
- 属性, 2-7
- イベント、監査可能, 5-30
- インストール時のエラー, H-10
- インテリジェント・クライアントのフェイルオーバー, 14-7
- 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, 14-7

え

- エージェント
 - エージェント・ファイルのアップロード, A-26
 - パートナ
 - 登録解除, 29-23, 29-25
 - ログ・ファイルの位置, 3-13
- エージェント・ツール
 - ldapUploadAgentFile.sh, A-26
- エラー・メッセージ, H-14
 - Oracle ディレクトリ・サーバーから戻される, H-10
 - インストール, H-10

- 管理, H-10
- その他, H-14
- ディレクトリ・サーバー、スキーマ変更が原因,
H-10
- データベース・サーバー, H-10
- 標準, H-10
- プロビジョニング, 36-15
- エンティティ・コンポーネント、アクセス制御, 13-8
- エントリ
 - ACIに関連付けられているオブジェクト, 13-7
 - Oracle Directory Manager を使用して作成, 4-9
 - 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, 5-28
 - 検索, 5-29
 - 管理, 7-1
 - Oracle Directory Manager を使用, 4-12, 7-2
 - コマンドライン・ツールを使用, 7-12
 - バルク・ツールを使用, 7-15
 - グループ, 2-6
 - 検索
 - 1 レベル, 7-3
 - ldapsearch を使用, A-22, A-26, A-27
 - 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
 - 検索のルート, 7-2
 - 削除
 - ldapdelete を使用, 4-13, 7-13, A-11
 - ldapmodify を使用, A-19
 - 多数, 7-18
 - 識別名, 2-2
 - 識別名による選択, 13-42
 - 識別名を使用して位置を識別, 2-3
 - スーパークラスの選択, 7-6
 - スーパークラス、選択, 7-6
 - 属性オプション付き
 - ldapmodify を使用した追加, 7-14
 - ldapsearch を使用した検索, 7-15
 - Oracle Directory Manager を使用した削除,
7-11, 7-14
 - Oracle Directory Manager を使用した変更, 7-11
 - Oracle Directory Manager を使用して管理, 7-10
 - コマンドライン・ツールを使用して管理, 7-14
 - 追加、Oracle Directory Manager を使用, 7-10
 - 属性の継承, 6-3
 - 属性、表示, 7-5
 - 多数、変更, 7-18
 - 追加
 - bulkload を使用, A-34
 - ldapaddmt を使用, 4-13, 7-12, A-6
 - ldapadd を使用, 4-13, 7-12, A-4
 - Oracle Directory Manager を使用, 7-6
 - オプション属性, 7-6
 - 親に対する書込みアクセス権限が必要, 7-6
 - 既存エントリをコピー, 7-6
 - 同時, 4-13, 7-12
 - 必須属性, 7-6
 - 他のアプリケーション, A-34
 - 特定、アクセス権の付与, 13-18, 13-21, 13-25,
13-27, 13-32, 13-35
 - ネーミング, 2-2, 14-2
 - 比較、ldapcompare を使用, 4-13, 7-13
 - 表示, 7-2
 - 変更
 - ldapmodify を使用, A-15
 - LDAP 規則, 7-9
 - Oracle Directory Manager を使用, 7-9
 - 規則, 7-9
 - 多数, A-36
 - 同時、ldapmodifymt を使用, A-20
 - 変更規則, 7-9
 - ユーザー
 - 追加、ldapadd を使用, 7-13
 - 追加、Oracle Directory Manager を使用, 7-7
 - 変更、ldapmodify を使用, 7-14
 - 変更、Oracle Directory Manager を使用, 7-10
 - ユーザーが追加できる種類の制限, 13-17, 13-24,
13-30, 13-40
 - ロード, 6-3
 - エントリ・キャッシング
 - キャッシュ、エントリ, 20-12
 - 使用可能, 5-15, 5-16
 - 「エントリの作成」メニュー項目、Oracle Directory
Manager, 4-9
 - 「エントリのリフレッシュ」ボタン、Oracle Directory
Manager, 4-10
 - 「エントリのリフレッシュ」メニュー項目, 4-9
 - エントリ・レベル・アクセス、Oracle Directory
Manager を使用した付与, 13-36
 - エントリ・レベルの競合、レプリケーション, 22-7

お

オープン・カーソル・パラメータ, 20-10

オブジェクト

ACI ディレクティブ, 13-7

検索

Oracle Directory Manager を使用, 4-10

検索、Oracle Directory Manager を使用, 4-10

コマンドライン・ツールを使用した削除, A-15

削除

Oracle Directory Manager を使用, 4-8, 4-10

コマンドライン・ツールを使用, A-11

追加、Oracle Directory Manager を使用, 4-8, 4-10

追加、テンプレートを使用, 4-10

比較, 4-8

変更

ldapmodify を使用, 7-12

Oracle Directory Manager を使用, 4-8, 4-10

オブジェクト・クラス, 2-8

extensibleObject, 7-19

groupOfNames, 7-8

LDIF ファイル, A-2

Oracle Directory Manager のタブ, 6-9

orclauditoc, 5-29

top, 2-9

一意のオブジェクト識別子, 6-4

一意名, 6-4

エントリへの割当て, 6-2, 6-3

ガイドライン

削除, 6-5

追加, 6-3

変更, 6-4

型, 2-9

管理

Oracle Directory Manager を使用, 6-6

コマンドライン・ツールを使用, 6-13

規則, 2-10

検索, 6-6

検索、Oracle Directory Manager を使用, 6-6

構造型, 2-10

構造型、変換, 6-5

削除

Oracle Directory Manager を使用, 6-12

ベース・スキーマ, 6-5

ベース・スキーマ内以外, 6-5

作成、Oracle Directory Manager を使用, 4-9

サブクラス, 2-9

定義, 2-8

参照, 7-19

スーパークラス, 2-9, 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, 2-12

増加, 6-4

属性の削除, 6-5

タイプ, 2-9

追加, 6-2

Oracle Directory Manager を使用, 6-10

コマンドライン・ツールを使用, 6-13

同時、ldapaddmt を使用, A-6

定義, 2-8

必須属性の再定義, 6-4

表示, 6-9

プロパティの表示, 6-9

ベース・スキーマ、変更, 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, 6-13

補助型, 2-10

補助型の変換, 6-4

オブジェクト・クラス型

構造型, 2-9, 2-10

抽象型, 2-9

補助型, 2-10

オブジェクト・クラスの説明, 6-7

オブジェクト識別子、オブジェクト・クラス, 6-6

オブジェクト追加制約、アクセス制御, 13-9

オブジェクトに対する排他的アクセス権、付与, 13-48

「オブジェクトの検索」ボタン、Oracle Directory

Manager, 4-10, 6-6

オプション属性, 2-8, 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, 2-8

オプション、属性, 2-7

オンライン管理ツール、「Oracle Internet Directory」

を参照

か

「開始」フィルタ、Oracle Directory Manager, 6-7
ガイドライン

- 属性の削除, 6-16
- 属性の追加, 6-15
- 属性の変更, 6-15

「回復」ボタン、Oracle Directory Manager, 4-7

拡張性、LDAP バージョン 3, 1-5

拡張性、Oracle Internet Directory, 1-9

仮想メモリー, 19-12

型

- オブジェクト・クラス, 6-7
- 属性, 2-4

カタログ化属性

- orcleventtype, 5-29
- orcluserdn, 5-29

カタログ管理ツール, 4-14, 6-26, 6-30

- 構文, A-39
- ログ・ファイルの位置, 3-13

ガベージ・コレクション

- 間隔、変更, 23-16
- レプリケーション, 22-6, 23-14

可用性、高い, 21-7

簡易認証, 1-9, 11-4

環境変数 NLS_LANG, 8-2

- 設定, 8-2, 8-3
- クライアント環境, 8-8

環境変数、NLS_LANG, 8-2

監査可能なイベント, 5-30

監査レベル, 5-30

- 設定, 5-31
- ldapmodify を使用, 5-32
- Oracle Directory Manager を使用, 5-31

変更, 5-32

監査ログ, 5-28

イベント

- ACL の変更, 5-31
- DSE の変更, 5-31
- アクセス違反, 5-31
- 削除, 5-31
- 識別名の変更, 5-31
- スーパー・ユーザー・ログイン, 5-30
- スキーマ要素、削除, 5-30
- スキーマ要素、追加 / 置換, 5-30
- 選択, 5-31
- 追加, 5-31

バインド, 5-30

変更, 5-31

ユーザー・パスワードの変更, 5-31

レプリケーション・ログイン, 5-31

エントリ

ldapsearch を使用した検索, 5-34

Oracle Directory Manager を使用した検索, 5-33

検索, 5-29, 5-33

構造, 5-29

ディレクトリ情報ツリーにおける位置, 5-30

ディレクトリ情報ツリー、位置, 5-30

表示, 5-28

エントリの構造, 5-29

コンテナ・オブジェクト, 5-34

削除, 5-35

サンプル, 5-30

使用方法, 5-28

スキーマ要素, C-5

デフォルトの構成, 5-28

間合せ, 5-28

「完全一致」フィルタ、Oracle Directory Manager,
5-33, 6-7, 7-4

管理

ディレクトリ・スキーマ, 6-1

管理者操作キュー操作ツール, 4-15, 23-32

構文, A-49

管理ツール, 4-13, 7-12

bulkdelete, A-33

bulkload, A-34

bulkmodify, A-36

ldapadd, 4-13, 7-12, A-4

ldapaddmt, A-6

ldapbind, A-8

ldapcompare, A-10

ldapdelete, 4-13, 7-13, A-11

ldapmoddn, 4-13, 7-13, A-13

ldapmodify, 4-13, 7-12, A-15

ldapmodifymt, 4-13, 7-12, A-20

ldapsearch, A-22

ldifwrite, A-38

OID データベース・パスワード・ユーティリティ,
4-15

Oracle Directory Manager, 4-2

カタログ管理, 4-14

コマンドライン, 1-8, 4-12

バルク・ツール, 4-13

き

- 規則、LDIF, A-3
- 既存 ACP とそのアクセス制御情報アイテム (ACI)
 - ディレクティブ、変更, 13-29
- 規定のアクセス制御, 13-3
- 競合の解消、レプリケーション, 22-7
- 競合の自動解消, 22-8
- 競合の手動解消, 23-30
- 競合、レプリケーション
 - 一般的な原因, 22-8
 - エントリ・レベル, 22-7
 - 解消, 13-45, 22-7
 - 自動解消, 22-8
 - 手動解消, 23-30
 - 手動での解消, 23-30
 - 属性レベル, 22-8
- 共有サーバー, 20-11
- 共有プール・サイズ, 20-7
 - パラメータ, 20-10
- 切離し、Oracle Directory Manager, 4-8

く

- クライアントとサーバーの認証、SSL, C-6
- クライアントのフェイルオーバー・オプション, 21-4
- クラスタ
 - 定義, 26-2
 - ディレクトリ, 1
 - ハードウェア, 25-2
 - フェイルオーバーの構成, 25-4
- グループ
 - 権限, 13-3
- グループ・エントリ, 2-6
 - 作成
 - ldapmodify を使用, A-18
 - Oracle Directory Manager を使用, 7-8
 - 追加, 7-8
- グローバリゼーション・サポート, 2-13
 - bulkdelete, 8-11
 - bulkload, 8-9
 - bulkmodify, 8-11
 - Java クライアント, 2-13
 - ldapadd, 8-7
 - ldapaddmt, 8-7
 - ldapbind, 8-7
 - ldapcompare, 8-7

- ldapdelete, 8-7
- ldapmoddn, 8-7
- ldapmodify, 8-7
- ldapmodifymt, 8-7
- ldapsearch, 8-7
- ldifwrite, 8-10
- LDIF ファイル, 8-4
- Oracle Internet Directory の設定, 8-2
 - 管理, 8-1
 - コマンドライン・ツール, 8-6
 - バルク・ツールでの使用方法, 8-9
- グローバリゼーション・サポートの -E 引数, 8-6

け

- 継承, 2-9
 - アクセス制御ポリシー・ポイント, 13-2
 - スーパークラス, 6-3, 6-9
 - 属性, 6-9
- ゲスト・ユーザー
 - 管理, 5-18
 - ldapmodify を使用, 5-20
 - Oracle Directory Manager を使用, 5-19
 - ユーザー名とパスワード, 5-18
 - 定義, 5-18
- 権限, 2-12, 11-3
 - 付与
 - Oracle Directory Manager を使用, 13-12
 - コマンドライン・ツールを使用, 13-40
- 権限グループ, 13-3
- 言語コード、属性オプション, 2-7
- 検索
 - 返されるエントリの最大数の指定, 5-33, 7-3
 - 基準パー、Oracle Directory Manager, 5-33, 7-3
 - 検索結果、返されるエントリの最大数の指定, 5-33, 7-3
 - 構成, 5-21
 - ACP、Oracle Directory Manager を使用, 13-13
 - ldapmodify を使用, 5-22
 - Oracle Directory Manager を使用, 5-21
 - 最大時間, 5-33
 - 最大時間の設定
 - ldapmodify を使用, 5-22
 - Oracle Directory Manager を使用, 5-21
 - 比較操作, 2-7

- フィルタ
 - IETF 準拠, A-22
 - ldapsearch, A-24
- フィルタ処理, 5-27
- フィルタを使用, 6-7
- 深さ、指定, 7-3
- 戻されるエントリの最大数の設定
 - ldapmodify を使用, 5-22
 - Oracle Directory Manager を使用, 5-21
- 検索で戻されるエントリの最大数、設定, 5-21
- 検索の最大時間、指定, 5-33, 7-3
- 検索の最大時間、設定, 5-21
- 検索のルート
 - 選択, 7-2
 - 入力, 7-2
- 厳密認証, 11-4

リ

- 公開鍵インフラストラクチャ, 11-2
- 構成設定, 「構成設定エントリ」を参照
- 構成設定エントリ, 2-20
 - LDIF ファイル, 5-11
 - orcldebuglevel, C-5
 - orclmaxcc, C-5
 - orclserverprocs, C-5
 - orclssl authentication, C-6
 - orclsslenable, C-6
 - orclsslport, C-6
 - orclsslwalletpasswd, C-7
 - orclsslwalleturl, C-6
 - SSL 使用禁止, C-6
 - SSL パラメータ, 12-3
- 管理, 4-18, 5-2
 - Oracle Directory Integration Platform, 30-7
 - Oracle Directory Manager を使用, 5-4
 - コマンドライン・ツールを使用, 5-11
 - 事前の考慮事項, 5-2
- 異なるものを使用, 5-2
- 削除, 5-2
 - ldapmodify を使用, 5-12
 - Oracle Directory Manager を使用, 5-4, 5-10
- 使用せずにディレクトリ・サーバーを起動, 3-9
- 追加, 2-20, 5-2, 5-11
 - Oracle Directory Manager を使用, 5-4
 - コマンドライン・ツールを使用, 2-20, 7-12
- ディレクトリ・サーバー・プロセス, C-5

- データベース接続, C-5
- デバッグ・レベル, C-5
- 表示, 5-4
- 複数, 12-3
- 変更, 2-20, 3-8, 5-2, 5-12, A-47
 - ldapmodify を使用, 5-12
 - 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, 7-12
 - ユーザー指定のオーバーライド, 3-9, A-47
 - レプリケーション・サーバー, 23-13
- 構成設定の位置, 5-14
- 構成パラメータ
 - Oracle ディレクトリ・レプリケーション・サーバー位置, 23-13
 - 変更, 2-20
- 構造型アクセス項目, 13-14, 13-37
 - アクセス制御ポイント, 13-14
- 構造型オブジェクト・クラス, 2-10
 - 変換, 6-5
- 構造型オブジェクト・クラス型, 2-9, 2-10
- 構造、監査ログ・エントリ, 5-29
- 構文
 - bulkdelete, A-33
 - bulkload, A-34
 - bulkmodify, A-36
 - LDAP, C-7
 - ldapadd, A-4
 - ldapaddmt, A-6
 - ldapbind, A-8
 - ldapcompare, A-10
 - ldapdelete, A-11
 - ldapmoddn, A-13
 - ldapmodify, A-15
 - ldapmodifymt, A-20
 - ldapsearch, A-22
 - ldapUploadAgentFile.sh, A-26, A-27
 - LDIF, A-2
 - ldifwrite, A-38
 - LDIF およびコマンドライン・ツール, A-1
 - oidctl, A-42
 - OID 制御ユーティリティ, A-42
 - OID データベース統計収集ツール, A-55
 - OID モニター, A-41
 - Oracle Directory Manager のタブ, 6-9
 - subSchemaSubentry への追加不可, 2-12
 - カタログ管理ツール, A-39

- コマンドライン・ツール, A-4
- 新規、追加, 2-7
- スキーマに格納, 2-12
- 属性, 2-6
- バルク・ツール, A-33
- 表示
 - ldapsearch の使用, 6-31
 - Oracle Directory Manager を使用, 6-31
- プロビジョニング・ツール, A-30
- コールド・バックアップ, 24-1
- 国際化対応、LDAP, 8-1
- 異なるノードの複数のインスタンス, 26-7
- コネクタ, 29-1
 - 構成情報, 29-9
 - 登録, 29-5
- コマンドライン・ツール, 1-8
 - ldapadd, 4-13, 7-12, A-4
 - ldapaddmt, 4-13, 7-12, A-6
 - ldapbind, A-8
 - ldapcompare, A-10
 - ldapcreateConn.sh, A-27
 - ldapdelete, 4-13, 7-13, A-11
 - ldapmoddn, 4-13, 7-13, A-13
 - ldapmodify, 4-13, 7-12, A-15
 - ldapmodifymt, 4-13, 7-12, A-20
 - ldapsearch, A-22
 - ldapUploadAgentFile.sh, A-26
- エントリ管理のための, 7-12
- 概要, 4-12
- カタログ管理ツール, 6-26
- 管理
 - エントリ, 7-12
 - 属性, 6-27
 - グローバリゼーション・サポートの設定, 8-6
 - 構成設定エントリの追加, 2-20, 7-12
 - 構成設定エントリの変更, 7-12
 - 構文, A-4
 - 索引付け, 6-26, 6-30
 - 属性値の比較, 7-13
- コマンドライン・モードのコマンドのバッチ処理, 6-13
- コンシューマ・サーバー, 2-22
- コンテンツ・アクセス項目, 13-38
 - アクセス制御ポイント, 13-14
 - 既存 ACP, 13-33
 - 特定のエントリのための指定, 13-28

- コンポーネント
 - ディレクトリ・サーバー, 2-15

さ

- サーバー
 - 構成
 - 入力ファイルを使用, 7-12
 - サーバー, 「ディレクトリ・サーバー」、「ディレクトリ・レプリケーション・サーバー」、「Directory Integration Server」を参照
 - サーバー・インスタンス
 - 実行方法, 4-2
 - 保護モードで実行, 12-3
 - サーバー処理の制限時間, 5-15
 - サーバー認証、SSL, 4-7, C-6
 - サーバーの起動コマンド, 5-2
 - サーバーの起動コマンド、OID 制御ユーティリティを使用, 4-15
 - サーバーの停止コマンド, 4-15
 - サーバー・プロセス
 - 数, C-5
 - サブレット
 - Delegated Administration Service が使用, 2-28
 - 再試行の回数、変更, 23-17
- サイズ
 - 属性値, C-9
 - サイズ, C-9
 - データベース・キャッシュ, 14-10
- サイズ設定, 14-8, 14-9
 - I/O サブシステム, 19-6
 - 配置での考慮事項, 14-9
 - 表領域, 19-8
- 索引
 - bulkload により作成, 7-18
 - 属性からの削除, 5-29, 6-27
 - Oracle Directory Manager を使用, 6-27
- 索引付き属性
 - Oracle Directory Manager で表示, 6-9
- orclevnttype, 5-29
- orcluserdn, 5-29
- 場所, 5-14
- 表示, 6-26
- 「索引の削除」
 - ボタン, 4-10
 - メニュー項目, 4-9
- 「削除」ボタン、Oracle Directory Manager, 4-10

- 「作成」ボタン、Oracle Directory Manager, 4-10
- サブエントリ、定義, 2-12
- サブクラス, 2-9
- サブツリー
 - 表示, 7-2
- サブツリー・エントリ・データ、Oracle Directory Manager を使用して更新, 4-10
- 「サブツリー・エントリのリフレッシュ」ボタン、Oracle Directory Manager, 4-10
- サブツリー・レベルの検索, 7-3
- 「サブツリー・エントリのリフレッシュ」メニュー項目, 4-9
- サブライヤ, 2-22
- 参照, 2-25
 - 種類, 2-27

し

- 時間ベースの変更ログの削除, 22-6
- 識別名, 2-2
 - LDIF ファイル, A-2
 - コンポーネント, 2-3
 - 書式, 2-3
 - 属性, 7-5
 - 変更, 4-13, 7-13
 - ldapmoddn を使用, 4-13, 7-13
 - コマンドライン・ツールを使用, 7-12
- 識別名の変更、監査ログのイベント, 5-31
- システム・グローバル領域 (SGA), 20-7, 23-6
 - Oracle9i 用のチューニング, 20-7
 - サイズ設定, 20-7
 - チューニング・パラメータ, 20-11
 - パラメータ, 20-11
- システム操作属性, 5-13
 - 設定, 5-13
 - ldapmodify を使用, 5-16
 - Oracle Directory Manager を使用, 5-13
 - 表示, 5-13
- 従属ネーミング・コンテキスト, 2-25
- 「終了」フィルタ、Oracle Directory Manager, 6-7
- 「終了」メニュー項目、Oracle Directory Manager, 4-8
- 上位ナレッジ参照 (参照), 2-25
- 障害許容度、レプリケーション, 14-6
- 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, 5-27
 - 接続, 5-27

- 操作, 5-27
- 送信エントリ, 5-27
- 承諾、レプリケーション, 22-2
- 冗長構成, 21-2
 - フェイルオーバー, 14-4
- 冗長リンク, 21-8
- 証明書, 11-4, C-6
 - 管理, D-9
 - ユーザー, D-9
- 証明書ベースの認証, 11-4
- 書式、識別名, 2-3
- 新規構文、追加, 2-7
- 新機能
 - Oracle Internet Directory リリース 2.1.1, lv
 - Oracle Internet Directory リリース 3.0.1, liii
- 信頼性、レプリケーション, 2-22

す

- スーパークラス, 2-9
 - 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
 - 管理, 5-18
 - ldapmodify を使用, 5-20
 - Oracle Directory Manager を使用, 5-19
 - ユーザー名とパスワード, 5-18
 - 定義, 5-18
 - ログイン, 4-4
 - ログイン・イベント, 5-30
- スキーマ
 - orclACI, B-2
 - orclEntryLevelACI, B-3
 - subSchemaSubentry 内の定義, 2-12
 - オブジェクト・クラスの追加と変更 (オンライン), 6-2
 - オブジェクト、Oracle Directory Manager を使用して管理, 4-12
 - 管理, 6-1
 - Oracle Directory Manager を使用, 4-12
 - 定義の位置, 5-14
 - 複数の表領域に分散, 20-9
 - ユーザー, C-11

要素, C-1

Oracle 独自, C-3

削除イベント, 5-30

追加 / 置換イベント, 5-30

特定の Oracle 製品, C-3

スキーマ関連のデバッグ, 5-27

「スキーマの管理」ペイン、Oracle Directory Manager,
6-9

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, 6-13

スタック、テクノロジー, 21-2

スタンドアロンの OID ノードのアップグレード, E-21

ストライブ化, 20-8, 20-9

スポンサ・ノード, 23-24

コールド・バックアップ・プロシージャ, 24-3

スマート・ナレッジ参照 (参照)

構成, 7-19

スリープ・タイム、OID モニター, 3-2, A-41

スループット, 19-6

包括的, 20-2

せ

制御、アクセス, 1-9, 13-1

制約、オブジェクト・クラス, 2-10

セキュリティ, 1-9, 2-12

LDAP バージョン 3, 1-5

Oracle Directory Integration Platform, 31-1

Oracle Internet Directory 環境, 2-12

異なるクライアント, 12-3

異なるクライアントごとの SSL パラメータ, 12-3

接続

管理, 5-27

追加のディレクトリ・サーバー, 4-11

ディレクトリ・サーバー, 4-3, 4-18

一般的なディレクトリ操作, 2-20

プーリング, 1-9

複数のディレクトリ・サーバー, 4-11

リダイレクション, 21-9

ソフトウェア・ベース, 21-7

ネットワーク・レベル, 21-6

ハードウェア・ベース, 21-7

接続時フェイルオーバー, 26-2

「切断」

ボタン、Oracle Directory Manager, 4-8

メニュー項目、Oracle Directory Manager, 4-8

設定プロセス (ldaprepl.sh)

ログ・ファイルの位置, 3-14

選択したイベントの監査, 5-31

選択した監査ログのイベント, 5-31

そ

操作属性, 5-13

ACI, 11-3

「操作」メニュー項目、Oracle Directory Manager, 4-9

送受信パケットの印刷, 5-27

相対識別名, 2-3

各エン트리ごとの表示, 7-2

変更

ldapmodify を使用, A-19

コマンドライン・ツールを使用, 7-12

変更、ldapmoddn を使用, 4-13, 7-13

ソート領域パラメータ, 20-11

属性

ACI に関連付けられているオブジェクト, 13-7

AlternateServers、フェイルオーバー, 21-4

commonName, 2-6

jpegPhoto, 2-6, 7-13

LDIF ファイル, A-2

NULL 値, 6-3

objectclass, 5-29

Oracle Directory Manager のタブ・ページ, 6-9

Oracle Directory Manager を使用して作成, 4-9

orclauditlevel, 5-31

orclauditmessage, 5-29

orclauditoc, 5-29

orcleventtime, 5-29

orcleventtype, 5-29

orclpresult, 5-29

orclsequence, 5-29, 5-30

orcluserdn, 5-29

organization, 2-6

organizationalUnitName, 2-6

ref, 7-19

sn, 2-6

surname, 2-6

top 内, 2-9

値, 2-4

サイズ, C-9

削除, A-18

変更, 7-9

変更規則, 7-9

- 値のサイズ, C-9
- 一致規則, 2-7
- オブジェクト・クラスからの削除, 6-5
- オブジェクト・クラスにより判別, 6-3
- オプション, 2-7, 2-8, 6-3
 - 言語コード, 2-7
- 型, 2-4
- 管理, 6-15
 - Oracle Directory Manager を使用, 6-16
 - 概要, 6-15
 - コマンドライン・ツールを使用, 6-27
- 規則
 - 削除, 6-16
 - 追加, 6-15
 - 変更, 6-15
- 継承, 6-3, 6-9
- 検索で使用可能にする方法, 6-26
- 検索, Oracle Directory Manager を使用, 6-18
- 構文, 2-6
 - 選択, 6-31
 - 変更, 6-15
 - 変更不可, 6-15
- 構文タイプ
 - 選択, 6-31
- コマンドライン・ツールを使用して管理, 6-27
- 索引付け, 6-9
 - 表示, 6-26
- 索引付け, 6-26, 6-30
 - Oracle Directory Manager を使用, 6-26
 - カタログ管理ツールを使用, 6-26
 - コマンドライン・ツールを使用, 6-29
 - 作成時, 6-26
- 索引の削除, 6-27
- 索引、bulkload により作成, 7-18
- 削除, 6-16
 - ldapmodify を使用, A-18
 - ガイドライン, 6-16
- 識別名, 7-5
- システム操作, 5-13
- 情報の種類, 2-5
- スキーマ内のメタデータとして, 2-12
- 操作, 5-13
- 属性オプション, 7-15
 - ldapmodify を使用した追加, 7-14
 - ldapsearch を使用した検索, A-25
 - Oracle Directory Manager を使用した削除, 7-11, 7-14

- Oracle Directory Manager を使用した変更, 7-11
- Oracle Directory Manager を使用して管理, 7-10
- 概念の説明, 2-7
- コマンドライン・ツールを使用して管理, 7-14
- 追加, Oracle Directory Manager を使用, 7-10
- 単一値, 2-6
 - 複数値への変換, 6-15
- 追加, 6-15
 - ldapadd を使用, A-4
 - ldapmodify を使用, 6-27, 6-28
 - Oracle Directory Manager を使用, 6-20, 6-22
 - ガイドライン, 6-15
 - 既存のエントリ, A-4
 - 同時、ldapaddmt を使用, A-6
- ディレクトリ・データが存在しない
 - 索引付け, 6-29
- データが存在する
 - 索引付け, 6-30
- 必須, 2-8, 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, 2-6, 13-3
 - 単一値への変換, 6-15
- ベース・スキーマ, 6-15
 - 削除, 6-16
 - 変更, 6-15
- 変更
 - ldapmodifymt を使用, 7-12
 - ldapmodify を使用, 6-27, 6-28, 7-12
 - Oracle Directory Manager を使用, 6-24, 7-11
 - ガイドライン, 6-15
 - 規則, 6-15
 - 同時, 4-13, 7-12
- 属性オプション, 2-7
 - ldapsearch を使用した検索, 7-15, A-25
 - Oracle Directory Manager を使用した削除, 7-11, 7-14
 - Oracle Directory Manager を使用した変更, 7-11
 - 概念の説明, 2-7
 - 管理
 - Oracle Directory Manager を使用, 7-10
 - コマンドライン・ツールを使用, 7-14
 - 言語コード, 2-7
 - 追加
 - ldapmodify を使用, 7-14
 - Oracle Directory Manager を使用, 7-10

属性情報、種類、2-5
属性値、置換、A-18
「属性の検索」ボタン、Oracle Directory Manager,
6-18
属性レベルの競合、22-8
その他のディレクトリとの同期、35-1, 35-3
ソフトウェア・ベースの接続リダイレクション、21-7
「存在」フィルタ、Oracle Directory Manager, 5-33,
6-8, 7-4

た

待機時間、平均、20-2
構造規則、Oracle Internet Directory では非強制、2-10
対称型マルチプロセッサ (SMP) システム、20-6
代替サーバー・リスト
 Oracle ディレクトリ・サーバー、21-4
 ユーザー入力、21-4
大容量トレースのデバッグ、5-27
高い可用性、1-9, 14-7, 21-2
 Oracle Internet Directory, 21-1
 Oracle Internet Directory の機能、21-7
 配置、例、21-9
 マルチマスター・レプリケーション、21-7
単一値の属性、2-6
 複数値への変換、6-15

ち

蓄積転送、Oracle9i, 22-3
中間層
 プロキシ・ユーザーを使用、5-18, 11-5
中間テンプレート・ファイル
 アプリケーション固有のリポジトリからの移行、I-2
抽象型オブジェクト・クラス、2-9
 top, 2-9
 スーパークラス、6-4
チューニング、14-8, 20-1
 CPU 使用量、20-4
 Oracle Internet Directory のプロセスに関する CPU,
 20-5
 Oracle9i 用のシステム・グローバル領域 (SGA),
 20-7
 Oracle のフォアグラウンド・プロセスに関する
 CPU, 20-6
 SGA パラメータ、20-11
 概要、20-2

考慮事項、14-11
ツール、20-2
ディスク、20-8
配置に関する考慮事項、14-11
メモリー、20-7
チューニング可能、データベース、20-10

つ

通常モード、ディレクトリ・サーバーの実行、C-6
ツール
 チューニング、20-2
「ツリー・ビュー」
 検索のルートの選択、7-2
 ブラウズ、7-2

て

ディスク使用量、14-12
ディスクのチューニング、20-8
ディスク領域要件、19-7
 詳細な計算、19-8
 見積り、19-7
ディレクトリ
 NOS, 14-2, 14-3
 アクセス制御、1-9, 13-1
 アプリケーション固有、2-28
 エントリのネーミング、14-2
 拡大する役割、1-2, 14-2
 情報ツリー
 ブラウズ、7-2
 スキーマ、2-12
 概要、6-2
 管理、6-1
 データベースのリスナー、23-7
 登録、35-4
 特別な用途、1-4
 パーティション化、2-24
 パスワード、変更、5-18
 分散、2-21
 読み込み目的、1-3
 リレーショナル・データベースとの対比、1-2
 レプリケーション・グループ (DRG), 22-2, 23-2
 インストール、23-2
 構成、23-2
 設定、23-2
 レプリケーション承諾、22-2

- ロケーション非依存, 1-3
- ディレクトリ・サーバー, 1-8, 2-19
 - アクティブ・インスタンスのパラメータの変更, 5-4
- 起動
 - 構成設定なし, 3-9
 - 構文, 3-4, A-43
 - デフォルトの構成を使用, 3-9, A-47
 - 必須の引数, 3-5, A-44
- 起動失敗, 3-9
- 構成設定エントリ, 5-2
- 構成設定エントリの変更, 5-12
- 異なる構成設定エントリを使用, 5-2
- 再起動, 3-7, 3-8, 5-4, A-46
- サプライヤとコンシューマ両方の役割, 22-6
- 実行方法, 3-3
- 接続, 4-3, 4-5, 4-11, 4-18
 - Oracle Directory Manager を使用, 4-10
 - 一般的なディレクトリ操作, 2-20
- 接続、Oracle Directory Manager を使用, 4-8
- 切断、Oracle Directory Manager を使用, 4-8, 4-11
- 追加, 4-5
- 追加に接続, 4-11
- 通常モード, C-6
- 停止, 3-5, 4-18, A-44
- デバッグ・レベル, C-5
- パラメータ
 - 構成, 4-18
 - コマンドライン・ツールを使用して構成, 4-18
- プロセス, 2-19, C-5
 - 複数, 2-19
- 別のホストへのホストの接続, 4-5
- 変更, 4-5
- 保護モード, C-6
- ホストの指定, 4-5
- マルチスレッド, 1-9
- マルチマスター・レプリケーション, 1-9, 22-6
- レプリケート環境, 22-6
- ログ・ファイルの位置, 3-14
- ディレクトリ・サーバーからの切断, 4-11
- ディレクトリ使用パターン、習得, 19-3
- ディレクトリ情報ツリー, 2-2
 - 階層と構造, 14-3
 - 監査ログ・エントリ, 5-30
 - データ所有権の境界を反映するように編成, 14-3
 - 編成, 14-3

- ディレクトリ・スキーマ, 2-12
 - 管理, 6-1
- ディレクトリ統合ツールキット, 28-11
- ディレクトリ統合プロファイル, 29-5
- ディレクトリと対比したリレーショナル・データベース, 1-2
- ディレクトリの登録, 35-4
- ディレクトリの登録解除, 35-8
- 「ディレクトリ・バージョン」フィールド、Oracle Directory Manager, 5-14
- ディレクトリ・レプリケーション・グループ (DRG), 22-2
- ディレクトリ・レプリケーション・サーバー, 1-8, 2-17, 2-18
 - Real Application Clusters 環境, 26-12
 - 起動, 3-7, A-45, A-46
 - 構成設定エントリ, 23-13
 - 停止, 3-7, A-46
 - ログ・ファイルの位置, 3-14
- データ移行プロセス, F-2
- データ整合性, 11-2
- データの移行, F-2
 - 他の LDAP 準拠のディレクトリから, F-1, F-2
 - 他の LDAP ディレクトリから, F-2
- データの整合性, 2-12, 2-13, 31-6
- データ・ブライバシ, 2-12, 11-2, 31-6
 - SSL を使用, 1-9
- データベース
 - キャッシュ・サイズ, 14-10
 - サーバー, 1-6
 - サーバー・エラー, H-10
 - 接続, 2-19
 - 同時, 20-11, C-5
 - プーリング, 1-9
 - チューニング, 20-10
 - ディレクトリ専用, 2-17
 - パスワード、変更, 5-36
 - ブロック・サイズ・パラメータ, 20-10
 - ブロック・バッファ・パラメータ, 20-10
- データ、Oracle Directory Manager を使用して更新, 4-10
- デーモン, 3-2
- 「適用」ボタン、Oracle Directory Manager, 4-7
- テクノロジ・スタック, 21-2
- デバッグ
 - すべてを使用可能, 5-28
 - パケット・ハンドリング, 5-27

デバッグ・ロギング・レベル, 5-27, C-5
Directory Integration Server 用の設定, 30-13
設定, 5-26, 5-27
OID 制御ユーティリティを使用, 5-27
Oracle Directory Manager を使用, 5-26
デフォルト・ナレッジ参照 (参照)
構成, 7-20
デフォルト・ポート, 4-3
番号, 3-5, 3-7, A-44, A-46
デフォルト・ポート以外、実行方法, 4-3
テンプレート、エントリの作成, 7-6

と

問合せ
監査ログ, 5-28
重要なイベント, 5-28
問合せエントリの返送制限, 5-14
透過的アプリケーション・フェイルオーバー (TAF),
26-2
同期
Oracle Internet Directory から接続先ディレクト
リへ, 29-4
使用例, 29-4
ステータス属性, 30-15
接続先ディレクトリから Oracle Internet
Directory へ, 29-4
同期化プロセス, 35-6
同期プロファイル, 29-1
統合プロファイル, 29-1
作成, A-27
統合プロファイルの作成, A-27
同時データベース接続, 20-11, C-5
登録、ディレクトリ, 35-4
特別な用途向けディレクトリ, 1-4
匿名認証, 4-4, 11-4
匿名ログイン, 4-4
トラブルシューティング, H-9
ディレクトリ・サーバー, 3-9
ディレクトリ・サーバー・インスタンスの起動,
3-9, A-47
パフォーマンス, 20-12
「取消」ボタン、Oracle Directory Manager, 4-7
トレース、ファンクション・コール, 5-28

な

ナビゲータ・ペイン、Oracle Directory Manager, 4-7
名前、オブジェクト・クラス, 6-6
ナレッジ参照, 2-25, 14-4, 14-5
概要, 2-25
管理権限の制限, 2-26
上位, 2-25
ナレッジ参照 (参照)
管理, 7-19
構成, 7-19
スマート
構成, 7-19
デフォルト
構成, 7-20

に

入力ファイル、作成, 5-11
認可, 2-12, 11-3, 31-4
認証, 11-4
3 つのレベル, 1-9
Kerberos, A-5, A-7, A-12
Oracle Directory Integration Server, 31-2
PKI, 11-2
SSL
ldapaddmt を使用, A-8
ldapadd を使用, A-6
ldapbind を使用, A-9
ldapmodifymt を使用, A-21
ldapmodify を使用, A-16
Oracle Directory Manager, 4-7
サーバー, C-6
サーバーのみ, 4-7
定義, 11-4
なし, 4-7, C-6
モード, 31-3
SSL クライアントとサーバー, C-6
SSL サーバー, C-6
SSL なし, C-6
一般的なディレクトリ操作, 2-21
エージェント, 31-4
概念の説明, 11-4
簡易, 1-9, 4-4, 11-4
間接, 11-5
RADIUS サーバーを介して, 11-5
厳密, 11-4

- 証明書ベース, 11-4
- 中間層を介して, 11-5
- 直接
 - オプション, 11-4
- 定義, 2-12
- 匿名, 4-4, 11-4
- パスワード・ベース, 4-4, 11-4
- パラメータ, C-6
- 非 SSL, 31-3

認証アクセス、SSL を使用, 1-9

認証局, 11-4

ね

ネーミング・コンテキスト, 2-11

- 管理, 5-17
- 検索, 2-11
- 公開, 2-11, 5-17
 - ldapmodify を使用, 5-18
 - Oracle Directory Manager を使用, 5-14, 5-17
- 公開を検索, 5-17
- 従属, 2-25
- 定義, 2-11
- パーティション化されたディレクトリ, 2-24
- レプリケーション, 2-23, 23-2

ネット・サービス名, 3-2, 3-3, A-41, A-42

ネットワーク

- 接続性、容量計画, 19-2
- 帯域幅, 19-14
- 要件, 19-14
- 容量計画, 19-14

ネットワーク・インタフェース・カード (NIC)、

- 障害, 21-8

ネットワーク・レベル

- 接続リダイレクション, 21-6
- フェイルオーバー, 21-5

の

ノード、Oracle Internet Directory, 2-15

は

ページ・スケジュール、Oracle Directory Manager を

- 使用した設定, 23-15

パーティション化, 2-21, 2-24

- 配置に関する考慮事項, 14-5

ハードウェア・ベースの接続リダイレクション, 21-7

パートナ・エージェント

- 登録解除, 29-23, 29-25

配置

- 考慮事項, 14-1
 - CPU の能力, 14-9
 - チューニング, 14-11
 - フェイルオーバー, 14-7
 - レプリケーション, 14-6
 - パーティション化, 14-5
- 例, 21-9

バインド, 2-21

バインド・イベント, 5-30

バインド・モード, 13-9

パスワード

- Oracle データ・サーバー、変更, 4-15, 5-36
- SSL Wallet 用, 4-6
 - 設定, C-7

アカウント・ロックアウト継続時間, 18-4

期限切れ警告, 18-3

シェル・ツール, 4-13, 7-17

失敗のカウント間隔, 18-3

失敗の最大数, 18-3

整合性

- MD4, 17-2

ディレクトリ、変更, 5-18

データベース, 5-36

バルク・ツールを使用, 4-13

保護, 2-12, 11-7

- ldapmodify を使用した変更, 17-4

- ldapmodify を使用して管理, 17-4

- MD5, 17-2, 17-4

- Oracle Directory Manager を使用した変更, 17-3

- Oracle Directory Manager を使用して管理, 17-3

- Oracle Directory Manager を使用して設定, 5-14

- SHA, 17-3, 17-4

- UNIX Crypt, 17-3, 17-4

- スキームを変更, 17-2

ポリシー, 11-7

- Oracle Directory Manager を使用して設定, 18-6

- 概念の説明, 11-7

- 管理, 2-12

- コマンドライン・ツールを使用して設定, 18-9

有効期限, 18-3

ロックアウト, 18-3

パスワード・ベースの認証, 4-4, 11-4

バックアップおよびリカバリの計画, 14-7

バックエンドでの通信の出力, 5-27
ハッシング
 ディレクトリに対するパスワード, 17-2
 保護
 MD4, 17-2
バッチ処理
 コマンドライン・モードのコマンド, 6-13
バッファ・キャッシュ、サイズ, 20-7
パフォーマンス
 orclEntryLevelACI を使用, 13-3
 検索, 20-12
 測定, 20-2
 チューニング、ツール, 20-2
 追加または変更, 20-12
 トラブルシューティング, 20-12
 複数のスレッドの使用, A-7
 レプリケーション, 14-6
パラメータ
 OID データベース統計収集ツール, A-55
 Oracle ディレクトリ・サーバーの構成に依存,
 20-11
 SGA, 20-11
 アクティブ・インスタンス、変更, 12-4
 アクティブ・サーバー・インスタンス
 変更, 5-4
 構成、Oracle ディレクトリ・レプリケーション・
 サーバー, 23-13
 チューニングに必須, 20-10
 レプリケーション承諾, 23-18
バルク・ツール, 4-13
 構文, A-33
バルク・ロードの失敗, 7-18

ひ

非 SSL 認証, 31-3
比較
 2 つのオブジェクト, 4-8
 エントリ, 4-13, 7-13
 属性値, 7-13
必須属性, 2-8, 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

「ビュー」メニュー、Oracle Directory Manager, 4-8
表示

 サブツリー, 7-2
 ディレクトリ・エントリ, 7-2
表領域, 19-8
 OLTS_ATTRSTORE, 19-11
 OLTS_CT_CN, 19-11
 OLTS_CT_DN, 19-11
 OLTS_CT_OBJCL, 19-12
 OLTS_CT_STORE, 19-12
 OLTS_DEFAULT, 19-12
 OLTS_IND_ATTRSTORE, 19-11
 OLTS_IND_CT_DN, 19-11
 OLTS_IND_CT_STORE, 19-12
 SYSTEM, 19-12
 均衡化, 20-9
 サイズ設定, 19-8
 作成, 23-6, 23-7
 レプリケーション, 23-6
表領域の均衡化, 20-9

ふ

ファイル
 位置, 29-18
ファイルのネーミング規則, 29-18
「ファイル」メニュー、Oracle Directory Manager, 4-8
ファンクション・コールのトレース, 5-27, 5-28
フィルタ
 IETF 準拠, A-22
 ldapsearch, A-24
 以下, 6-8, 7-4
 以上, 6-8, 7-4
 開始, 6-7
 完全一致, 6-7, 7-4
 検索, 2-20, 6-7
 Oracle Directory Manager, 6-7
 終了, 6-7
 属性の検索, 6-19
 存在, 6-8
 存在、Oracle Directory Manager, 5-33, 7-4
ブートストラップ, 32-1
 Oracle HR から Oracle Internet Directory の, 33-18
 Oracle Internet Directory から接続先ディレクト
 リの, 32-3
 接続先ディレクトリから Oracle Internet
 Directory の, 32-2

- ブーリング、接続, 1-9
- フェイルオーバー, 1-9, 21-1, 21-2
 - AlternateServers 属性, 21-4
 - Oracle Internet Directory の機能, 21-7
 - Real Application Clusters 環境, 26-1
 - 基本的な高い可用性の構成, 26-3
 - クライアントにおけるオプション, 21-4
 - クラスタ化された環境、動作, 25-6
 - クラスタ構成, 25-1
 - 接続時, 26-2
 - デフォルトの N ノード構成, 26-7
 - ネットワーク・レベル, 21-5
 - 配置での考慮事項, 14-7
 - 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, 21-5
 - 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, 21-8
- フォルト・トレランス機能, 21-3
- 複数値の属性, 2-6
 - member, 7-8
 - orclEntryLevelACI, 13-3
 - 値の追加、ldapmodify を使用, A-18
 - 単一値への変換, 6-15
- 複数の構成設定エントリ, 12-3
- 複数のスレッド, A-21
 - ldapaddmt, A-6
 - 数の増加, A-7
- 物理的な分散、パーティションとレプリカ, 14-4
- 物理メモリー, 19-12
- プライバシー、データ, 2-12, 11-2
 - SSL を使用, 1-9
- プロキシ・ユーザー, 11-5
 - 管理, 5-18
 - ldapmodify を使用, 5-20
 - Oracle Directory Manager を使用, 5-19
 - ユーザー名とパスワード, 5-18
 - 定義, 5-18
- プロセス, 2-18
 - Oracle バックグラウンド, 20-11
- プロセス・インスタンスの位置, 5-14
- プロビジョニング
 - アプリケーションが情報を取得する方法, 36-7
 - アプリケーションでの登録, 36-3
 - 自動, 36-3
 - 手動, 36-3
 - エラー・メッセージ, 36-15
 - コンポーネント間の関係, 36-4

- 定義, 36-2
- 手順, 36-2
- 典型的な配置, 36-5
- 同期との比較, 36-2
- 必要な情報の種類, 36-3
- プロフィール
 - 監視, 36-10
 - 管理, 36-10
- プロビジョニング・サブスクリプション・ツール
 - アプリケーションによるサブスクリプション, 36-8
 - 位置, 36-8
- プロビジョニング・ツール
 - 構文, A-30
- プロフィール
 - 管理, 29-18
 - 登録, 29-18
- プロフィール・ツール
 - ldapUploadAgentFile.sh, A-26
- プロフィール、ディレクトリ統合, 29-5
- 分散ディレクトリ, 2-21, 2-24
 - パーティション化, 2-21
 - パーティションとレプリカ, 14-4
 - レプリケート, 2-21



- 平均待機時間, 20-2
- ページング, 19-12
- ベース検索, 7-3
- ベース・スキーマ
 - オブジェクト・クラス
 - 変更, 6-5
 - 属性, 6-15
 - 削除, 6-16
 - 変更, 6-15
- ヘルプ
 - ボタン、Oracle Directory Manager, 4-11
 - メニュー項目、Oracle Directory Manager, 4-9
- 変換
 - 構造型オブジェクト・クラス, 6-5
 - ディレクトリ・データを LDIF へ, 7-18
 - 補助型オブジェクト・クラス, 6-4
- 変更
 - 管理者操作キューからページ・キューへの移動, A-50
 - 管理者操作キューからリトライ・キューへの移動, A-49

変更適用の失敗, 2-23
変更の種類、ldapmodify 入力ファイル, A-17
変更番号ベースの削除, 22-6
変更リトライ回数、設定, 23-15
変更ログ, 2-23, 22-2
 Oracle Directory Provisioning Integration Service で
 使用, 36-4
 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, 35-2
 削除, 22-6
 時間ベース, 22-6, 23-14, 23-15
 変更番号ベース, 22-6, 23-14
 方法, 22-6
 時間ベースの削除, 22-6
 フラグ, 3-4
 切替え, 3-4
 変更番号ベースの削除, 22-6
 レプリケーション, 1-9, 22-6
変更ログ・インタフェース
 IETF, 28-11
 Oracle 独自, 28-11
変更ログ記録, 3-5, A-44
変更ログの削除, 22-6
 時間ベース, 22-6
 変更番号ベース, 22-6
変更ログの処理に使用されるワーカー・スレッドの数、
 変更, 23-17
変更ログの存続時間パラメータ、変更, 23-16
編集
 ボタン、Oracle Directory Manager, 4-10
 メニュー項目、Oracle Directory Manager, 4-8

ほ

包括的なスループット, 20-2
ポート, 4-5
 デフォルト, 3-5, 3-7, 4-3, A-44, A-46
ポート 389, 3-5, 3-7, A-44, A-46, C-6
ポート 636, 3-5, 3-7, A-44, A-46, C-6
保護
 ポート 636, 12-2, 12-3
保護モード
 サーバー・インスタンスの実行, 12-3
 ディレクトリ・サーバーの実行, C-6
補助型オブジェクト・クラス, 2-10, 6-4
ポリシー、ネーミング、既存のものを活用, 14-2

ま

マスター定義サイト (MDS), 23-4
 指定, 23-4
マッピング・ルール, 29-10
マッピング・ルールの形式, 29-10
マルチ・サーバー・プロセス, 2-19
マルチスレッド LDAP サーバー, 1-9
マルチスレッド・コマンドライン・ツール
 ldapaddmt, 4-13, 7-12, A-6
 ldapmodifymt, 4-13, 7-12, A-21
マルチマスター・フラグ
 切替え, 23-12
マルチマスター・レプリケーション, 1-9, 14-4, 14-6,
 22-2
 高い可用性, 21-7

み

未指定のアクセス権, 13-11, 13-32

め

メタディレクトリ, 2-28
メタデータ、スキーマに格納, 2-12
メニュー・バー、Oracle Directory Manager, 4-8
メモリー
 仮想, 19-12
 使用量, 14-11
 チューニング, 20-7
 必須, 14-10
 不足, 20-8
 物理, 19-12
 容量計画, 19-2
 容量計画の要件, 19-12
メモリー不足, 20-8

ゆ

ユーザー・エントリ
 追加
 ldapadd を使用, 7-13
 Oracle Directory Manager を使用, 7-7
 変更
 ldapmodify を使用, 7-14
 Oracle Directory Manager を使用, 7-10
ユーザー・スキーマ, C-11

「ユーザー設定項目」
ボタン, 4-11
メニュー項目, 4-9
「ユーザー・パスワードの変更」イベント, 5-31
「ユーザー」フィールド、Oracle Directory Manager,
4-4
ユーザー名とパスワード、管理
ldapmodify を使用, 5-20
Oracle Directory Manager を使用, 5-19
ユーザー・ログイン, 4-4
ユーザー、プロキシ, 11-5
優先順位
エントリ・レベル, 13-46
規則
ACL の評価, 13-45
アクセス・ポリシーの競合, 13-2
属性レベル, 13-46

よ

容量計画, 14-8, 14-9, 19-1
I/O サブシステム, 19-6
概要, 19-2
ネットワーク要件, 19-14

り

リカバリ機能、Oracle9i, 1-9
リスナー、ディレクトリ・データベース, 2-17, 2-19
再起動, 23-7
停止, 23-7
「リフレッシュ」ボタン、Oracle Directory Manager,
4-10

る

「類似項目の作成」
操作、Oracle Directory Manager を使用, 4-8
テンプレートをを使用したエントリの追加, 7-6
ボタン、Oracle Directory Manager, 4-10, 7-7

れ

レプリカ, 2-22
配置, 14-4
レプリケーション, 2-22, 2-23, 3-14
Oracle Net Services 環境の準備, 23-4
Oracle9i, 22-3
アーキテクチャ, 22-3
移送方法, 22-3
インストールと構成, 23-2
概要, 22-1
ガベージ・コレクション, 23-14
管理, 23-1
競合
一般的な原因, 22-8
手動での解消, 23-30
発生のレベル, 22-7
構成, 23-13
Oracle9i レプリケーション, 23-8
sqlnet.ora, 23-5
tnsnames.ora, 23-5
構成パラメータ
表示と変更, 23-15
変更, 23-16
考慮事項, 14-6
コールド・バックアップ, 24-1
サーバー
停止, A-46
再試行
回数の変更, 23-17
変更の適用, 2-23
実装する理由, 14-6
障害許容度, 14-6
状態の位置, 5-14
承諾, 5-14, 22-2, 23-18
構成, 23-13, 23-18
ノードの追加, 23-20
承諾のパラメータ, 23-18
表示と変更, 23-18
変更, 23-18, 23-20
新規ノードの追加, 23-22, 23-27
信頼性, 2-22
スボンサ・ノード, 24-3
データベース・コピー・プロシージャ, 24-1
ネーミング・コンテキスト, 23-2

ノード

削除, 23-28

追加, 23-22

ノードを削除, 23-28

配置, 14-6

プロセス, 22-9, 22-11, 22-12, 22-13, 22-14

コンシューマ側, 22-5

サプライヤ側, 22-4

変更の競合

監視, 23-30

変更ログ, 1-9, 22-6

マルチマスター, 1-9, 14-4, 22-2

ゆるやかな一貫性モデル, 14-6

ロード・バランシング, 14-6

ログイン・イベント, 5-31

ログの位置, 5-14

ワーカー・スレッドの数を指定, 23-15

レプリケーション固有のデバッグ, 5-28

レプリケーション・サーバー

ログ・ファイルの位置, 3-14

レプリケーション・サーバー, 「ディレクトリ・レプリケーション・サーバー」を参照

レプリケーションのゆるやかな一貫性モデル, 14-6

レプリケート・ディレクトリ、概念の説明, 2-21

ろ

ロード・バランシング

ネットワーク・レベル, 21-5

レプリケーション, 14-6

ロールバック・セグメント, 23-6

作成, 23-6, 23-7

ログイン

スーパー・ユーザー, 4-4

匿名, 4-4

ユーザー, 4-4

ログ・ファイルの位置, 3-13

ログ・ファイル、Delegated Administration Service, 9-7

ロケーション非依存、ディレクトリ, 1-3

論理ディスク, 20-9

論理ホスト、クラスタ化された環境, 25-2

わ

ワーカー・スレッド, 2-19, 20-11

レプリケーションで指定, 23-15

ワイルド・カード、アクセス制御ポリシー・ポイントの設定, 13-42

