Oracle® Identity Management

統合ガイド

10*g*（10.1.4.0.1）

部品番号 : B31462-01

2006 年 11 月

ORACLE®

Oracle Identity Management 統合ガイド , 10*g*（10.1.4.0.1）

部品番号 : B31462-01

原本名 : Oracle Identity Management Integration Guide, 10*g* (10.1.4.0.1)

原本部品番号 : B15995-01

原本著者 : Don Gosselin

制限付権利の説明

このプログラム（ソフトウェアおよびドキュメントを含む）には、オラクル社およびその関連会社に所有権のある情報が含まれています。このプログラムの使用または開示は、オラクル社およびその関連会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と工業所有権に関する法律により保護されています。

独立して作成された他のソフトウェアとの互換性を得るために必要な場合、もしくは法律によって規定される場合を除き、このプログラムのリバース・エンジニアリング、逆アセンブル、逆コンパイル等は禁止されています。

このドキュメントの情報は、予告なしに変更される場合があります。オラクル社およびその関連会社は、このドキュメントに誤りが無いことの保証は致し兼ねます。これらのプログラムのライセンス契約で許諾されている場合を除き、プログラムを形式、手段（電子的または機械的）、目的に関係なく、複製または転用することはできません。

このプログラムが米国政府機関、もしくは米国政府機関に代わってこのプログラムをライセンスまたは使用する者に提供される場合は、次の注意が適用されます。

U.S. GOVERNMENT RIGHTS

Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

このプログラムは、核、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への用途を目的としておりません。このプログラムをかかる目的で使用する際、上述のアプリケーションを安全に使用するために、適切な安全装置、バックアップ、冗長性（redundancy）、その他の対策を講じることは使用者の責任となります。万一かかるプログラムの使用に起因して損害が発生いたしましても、オラクル社およびその関連会社は一切責任を負いかねます。

Oracle、JD Edwards、PeopleSoft、Siebel は米国 Oracle Corporation およびその子会社、関連会社の登録商標です。その他の名称は、他社の商標の可能性があります。

このプログラムは、第三者の Web サイトへリンクし、第三者のコンテンツ、製品、サービスへアクセスすることがあります。オラクル社およびその関連会社は第三者の Web サイトで提供されるコンテンツについては、一切の責任を負いかねます。当該コンテンツの利用は、お客様の責任になります。第三者の製品またはサービスを購入する場合は、第三者と直接の取引となります。オラクル社およびその関連会社は、第三者の製品およびサービスの品質、契約の履行（製品またはサービスの提供、保証義務を含む）に関しては責任を負いかねます。また、第三者との取引により損失や損害が発生いたしましても、オラクル社およびその関連会社は一切の責任を負いかねます。

RSA and RC4 are trademarks of RSA Data Security. Portions of Oracle Internet Directory have been licensed by Oracle Corporation from RSA Data Security.

Oracle Directory Manager requires the Java™ Runtime Environment. The Java™ Runtime Environment, Version JRE 1.1.6. ("The Software") is developed by Sun Microsystems, Inc. 2550 Garcia Avenue, Mountain View, California 94043. Copyright (c) 1997 Sun Microsystems, Inc.

This product contains SSLPlus Integration Suite™ version 1.2, from Consensus Development Corporation.

Sun Java System Directory Server and iPlanet are registered trademarks of Sun Microsystems, Inc.

目次

第 III 部　Oracle Directory Integration Platform との同期

5　Oracle Directory Synchronization Service

6　ディレクトリ同期プロファイルの構成

7　ディレクトリ同期の管理

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

9 リレーショナル・データベースの表との同期

10 Oracle Human Resources との同期化

11 サード・パーティのメタディレクトリ・ソリューションとの同期

第 IV 部　Oracle Directory Integration Platform によるプロビジョニング

12　Oracle Directory Integration Platform Service の概要

13　プロビジョニング統合アプリケーションの配置

14　Oracle Internet Directory プロビジョニング・コンソールによる管理

18 サード・パーティ・ディレクトリとの同期の構成

19 Microsoft Active Directory との統合

20 Oracle Password Filter for Microsoft Active Directory の配置

21 Sun Java System Directory との統合

22 Novell eDirectory または OpenLDAP との統合

23 サード・パーティ・ディレクトリとの統合の管理

第 VI 部　付録

A　Oracle Directory Integration Server 管理ツールの要素

B　事例 : Oracle Directory Integration Platform の配置

C　Oracle Directory Integration Platform のトラブルシューティング

図一覧

表一覧

はじめに

『Oracle Identity Management 統合ガイド』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。

対象読者

『Oracle Identity Management 統合ガイド』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、UNIX/Linux オペレーティング・システムまたは Microsoft Windows のいずれかに精通し、このマニュアルのコマンドや例を理解できる必要があります。

このマニュアルを使用するには、**Lightweight Directory Access Protocol** にある程度精通している必要があります。

ドキュメントのアクセシビリティについて

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

ドキュメント内のサンプル・コードのアクセシビリティについて

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

外部 Web サイトのドキュメントのアクセシビリティについて

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

Oracle サポート・サービスへの TTY アクセス

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

関連ドキュメント

詳細は、次の Oracle ドキュメントを参照してください。

- Oracle Directory Manager、Oracle Delegated Administration Services および Oracle Enterprise Manager 10*g* で使用できるオンライン・ヘルプ。
- Oracle Application Server および Oracle Database のドキュメント・セット。特に次のマニュアルを参照してください。
  - 『Oracle Identity Management インフラストラクチャ管理者ガイド』
  - 『Oracle Internet Directory 管理者ガイド』
  - 『Oracle Identity Management 委任管理ガイド』
  - 『Oracle Identity Management アプリケーション開発者ガイド』
  - 『Oracle Application Server Single Sign-On 管理者ガイド』
  - 『Oracle Application Server Certificate Authority 管理者ガイド』
  - 『Oracle Identity Management ユーザー・リファレンス』
  - 『Oracle Application Server 高可用性ガイド』
  - 『Oracle Application Server 管理者ガイド』
  - 『Oracle Database 管理者ガイド』
  - 『Oracle Database Net Services 管理者ガイド』
  - 『Oracle Database Oracle Clusterware および Oracle Real Application Clusters 管理およびデプロイメント・ガイド』
  - 『Oracle Database アドバンスト・レプリケーション』
  - 『Oracle Advanced Security 管理者ガイド』

詳しい情報は、次のドキュメントを参照してください。

- David Chadwick 著『Understanding X.500 - The Directory』（Thomson Computer Press, 1996）。
- Tim Howes、Mark Smith 著『LDAP: Programming Directory-enabled Applications with Lightweight Directory Access Protocol』（Macmillan Technical Publishing, 1997）。
- Tim Howes、Mark Smith、Gordon Good 著『Understanding and Deploying LDAP Directory Services』（Macmillan Technical Publishing, 1999）。
- オブジェクト識別子については、Internet Assigned Numbers Authority のホームページ（`http://www.iana.org`）を参照してください。
- `http://www.ietf.org` で入手可能な Internet Engineering Task Force（IETF）のドキュメント。特に次のものを参照してください。
  - LDAPEXT の Charter および LDAP の Draft
  - LDUP の Charter および Draft
  - RFC 2254「The String Representation of LDAP Search Filters」
  - RFC 1823「The LDAP Application Program Interface」
- OpenLDAP Community（`http://www.openldap.org`）。

表記規則

このマニュアルでは次の表記規則を使用します。

規則	意味
太字	太字は、操作に関連する Graphical User Interface 要素、または本文中で定義されている用語および用語集に記載されている用語を示します。
イタリック	イタリックは、ユーザーが特定の値を指定するプレースホルダ変数を示します。
固定幅フォント	固定幅フォントは、段落内のコマンド、URL、サンプル内のコード、画面に表示されるテキスト、または入力するテキストを示します。

サポートおよびサービス

次の各項に、各サービスに接続するための URL を記載します。

Oracle サポート・サービス

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

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

製品マニュアル

製品のマニュアルは、次の URL にあります。

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

研修およびトレーニング

研修に関する情報とスケジュールは、次の URL で入手できます。

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

その他の情報

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

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

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

Oracle Identity Management 統合の新機能

ここでは、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、各新機能の詳細が記載された関連項目および関連資料を示します。内容は次のとおりです。

Oracle Application Server 10*g*（10.1.4.0.1）で導入された新機能

この項では、Oracle Application Server 10*g*（10.1.4.0.1）で導入された機能について説明します。

- **Sun Java System Directory コネクタの Express 構成 :** Sun Java System Directory コネクタの Express 構成を実行できるようになりました。Express 構成では、デフォルトのマッピングおよびフィルタ処理を使用して Oracle Internet Directory と Sun Java System Directory サーバー間で変更を同期化します。2 つの同期プロファイルが Express 構成で作成されます。1 つは Sun Java System Directory から Oracle Internet Directory に変更を同期化するプロファイル、もう 1 つは Oracle Internet Directory から Sun Java System Directory に変更を同期化するプロファイルです。詳細は、第 21 章「Sun Java System Directory との統合」を参照してください。
- **Microsoft Active Directory コネクタでの Microsoft Exchange Server のサポート :** Microsoft Active Directory コネクタで Microsoft Exchange Server との統合をサポートするようになりました。詳細は、第 19 章「Microsoft Active Directory との統合」を参照してください。
- **Novell eDirectory および OpenLDAP との統合 :** Oracle Directory Integration Platform で Oracle Internet Directory と、Novell eDirectory または OpenLDAP 間の統合をサポートするようになりました。詳細は、第 22 章「Novell eDirectory または OpenLDAP との統合」を参照してください。
- **Microsoft Active Directory からのパスワードの同期 :** Microsoft Active Directory から Oracle Internet Directory にユーザーを同期化する際に、Oracle Password Filter for Microsoft Active Directory を使用してパスワードも同期化できるようになりました。詳細は、第 20 章「Oracle Password Filter for Microsoft Active Directory の配置」を参照してください。
- **Directory Integration アシスタントでの SSL のサポート :** Directory Integration アシスタント（`dipassistant`）で Secure Sockets Layer（SSL）をサポートするようになりました。
- **Oracle Directory Integration Platform:** Oracle Directory Integration and Provisioning は Oracle Directory Integration Platform と呼ばれるようになりました。

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

この項では、Oracle Application Server 10*g* リリース 2（10.1.2）で導入された新機能について説明します。

- **拡張されたプロビジョニング機能 :** このリリースには、Oracle Directory Integration Platform Provisioning の拡張機能が含まれます。管理者は、Oracle Internet Directory でユーザーをプロビジョニングするためのグラフィカル・インタフェースである新しい Oracle Internet Directory プロビジョニング・コンソールを使用できます。Oracle Internet Directory プロビジョニング・コンソールは、Oracle Delegated Administration Services で作成され、Oracle Internet Directory セルフ・サービス・コンソールとともに動作します。詳細は、第 IV 部「Oracle Directory Integration Platform によるプロビジョニング」を参照してください。
- **Oracle Directory Integration Platform のグラフィカル管理 :** 新しい Oracle Directory Integration Server 管理ツールが使用できるようになりました。これは、Oracle Directory Integration Platform をグラフィカルに管理するための Java ベースのユーティリティです。詳細は、第 3 章「Oracle Directory Integration Platform 管理ツール」を参照してください。
- **Microsoft Active Directory コネクタの Express 構成 :** Microsoft Active Directory コネクタの Express 構成を実行できるようになりました。Express 構成では、デフォルトの設定を使用してすべての必須構成を自動的に実行し、インポート用とエクスポート用の 2 つの同期プロファイルも作成します。

関連項目：

- 第 3 章「Oracle Directory Integration Platform 管理ツール」
- 第 19 章「Microsoft Active Directory との統合」

- **Windows ネイティブ認証の簡易構成 :** このマニュアルでは、Windows ネイティブ認証についての詳細な指示が記載されています。詳細は、第 19 章「Microsoft Active Directory との統合」を参照してください。

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

この項では、Oracle Internet Directory 10*g*（9.0.4）で導入された新機能について説明します。

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

  関連項目： 第 19 章「Microsoft Active Directory との統合」

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

  関連資料 :

  - 『Oracle Internet Directory 管理者ガイド』のカスタマイズされた外部認証パスワードの設定に関する章
  - 17-13 ページの「パスワードの格納場所の選択」

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。

- **新しいディレクトリ統合機能 :** Oracle Internet Directory リリース 9.0.2 では、(Oracle および Oracle 以外で作成された）他のアプリケーションやリポジトリとの新しい種類の接続性が導入されました。新しい Oracle Directory Integration Platform Service および Oracle Directory Synchronization Service は、Oracle Directory Integration Platform（Oracle8*i* の Oracle Internet Directory リリース 2.1.1.1 で導入）上に構築されます。

  - **Oracle Directory Integration Platform 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限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 Integration Platform Service によって、サブスクライバ・アプリケーションやビジネス・エンティティは、ローカル・リポジトリの同期を維持するために、Oracle Internet Directory の更新に常に注意を払うことができます。Oracle Internet Directory をプライマリ・リポジトリ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、ネットワーク・オペレーティング・システム（NOS）のユーザー・リポジトリなど、すでに配置されている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 との間で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 1 章「Oracle Identity Management 統合の概要」

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。

- **Oracle Directory Integration Platform:** この機能によって、多数のディレクトリを Oracle Internet Directory と同期化できます。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。

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 で導入された機能について説明します。

- **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、この機能を使用して、複数ディレクトリを Oracle Internet Directory と同期させることができます。

注意： この機能は、リリース 3.0.1 で Oracle Directory Integration Platform に置き換えられました。詳細は、第 1 章「Oracle Identity Management 統合の概要」を参照してください。

第I部

Oracle Directory Integration Platform スタート・ガイド

第 I 部では、Oracle Directory Integration Platform の概念、コンポーネント、アーキテクチャおよびセキュリティ機能について説明します。次の各章で構成されています。

1

Oracle Identity Management 統合の概要

この章では、Oracle Identity Management 統合とそのコンポーネント、構造および管理ツールの概要について説明します。

この章の内容は次のとおりです。

- Oracle Identity Management 統合を行う理由
- Oracle Identity Management のインストール・オプション
- 同期、プロビジョニングおよび両者の相違点
- Oracle Identity Management 統合に必要なコンポーネント

> **関連項目：** Oracle Identity Management 統合の配置の例は、付録 B「事例 : Oracle Directory Integration Platform の配置」を参照してください。

Oracle Identity Management 統合を行う理由

Oracle Identity Management により、アプリケーションとディレクトリ（サード・パーティの LDAP ディレクトリを含む）を Oracle Internet Directory に統合して、管理作業にかかる時間とコストを削減できます。これには、Oracle Directory Integration Platform を使用します。たとえば、企業には次のようなニーズがあります。

- Oracle Human Resources と Oracle Internet Directory で従業員レコードの整合性を維持すること。Oracle Directory Integration Platform では、Oracle Directory Synchronization Service によりこの同期化を行います。
- 変更が Oracle Internet Directory に適用されるたびに、Oracle Application Server Portal（OracleAS Portal）などの LDAP 対応アプリケーションに通知すること。Oracle Directory Integration Platform では、Oracle Directory Integration Platform Service によりこの通知を行います。

統合処理全体を通して、Oracle Directory Integration Platform は、アプリケーションとその他のディレクトリが確実な方法で必要な情報をやり取りすることを保証します。

Microsoft Active Directory、Sun Java System Directory、Novell eDirectory、OpenLDAP など、様々なディレクトリとの統合が可能です。たとえば、Oracle Application Server 環境では、Oracle コンポーネントへのアクセスは、Oracle Internet Directory に格納されているデータに基づいて行いますが、企業の中央ディレクトリとして Microsoft Active Directory も使用できます。これらのディレクトリのユーザーが Oracle コンポーネントにアクセスできるのは、Oracle Directory Integration Platform により、Microsoft Active Directory 内のデータを、Oracle Internet Directory 内のデータと同期化できるためです。

関連項目：

- 第 10 章「Oracle Human Resources との同期化」
- 第 19 章「Microsoft Active Directory との統合」
- 第 21 章「Sun Java System Directory との統合」

図 1-1 に、Oracle Directory Integration Platform の配置例を示します。

図 1-1 Oracle Directory Integration Platform 環境の例

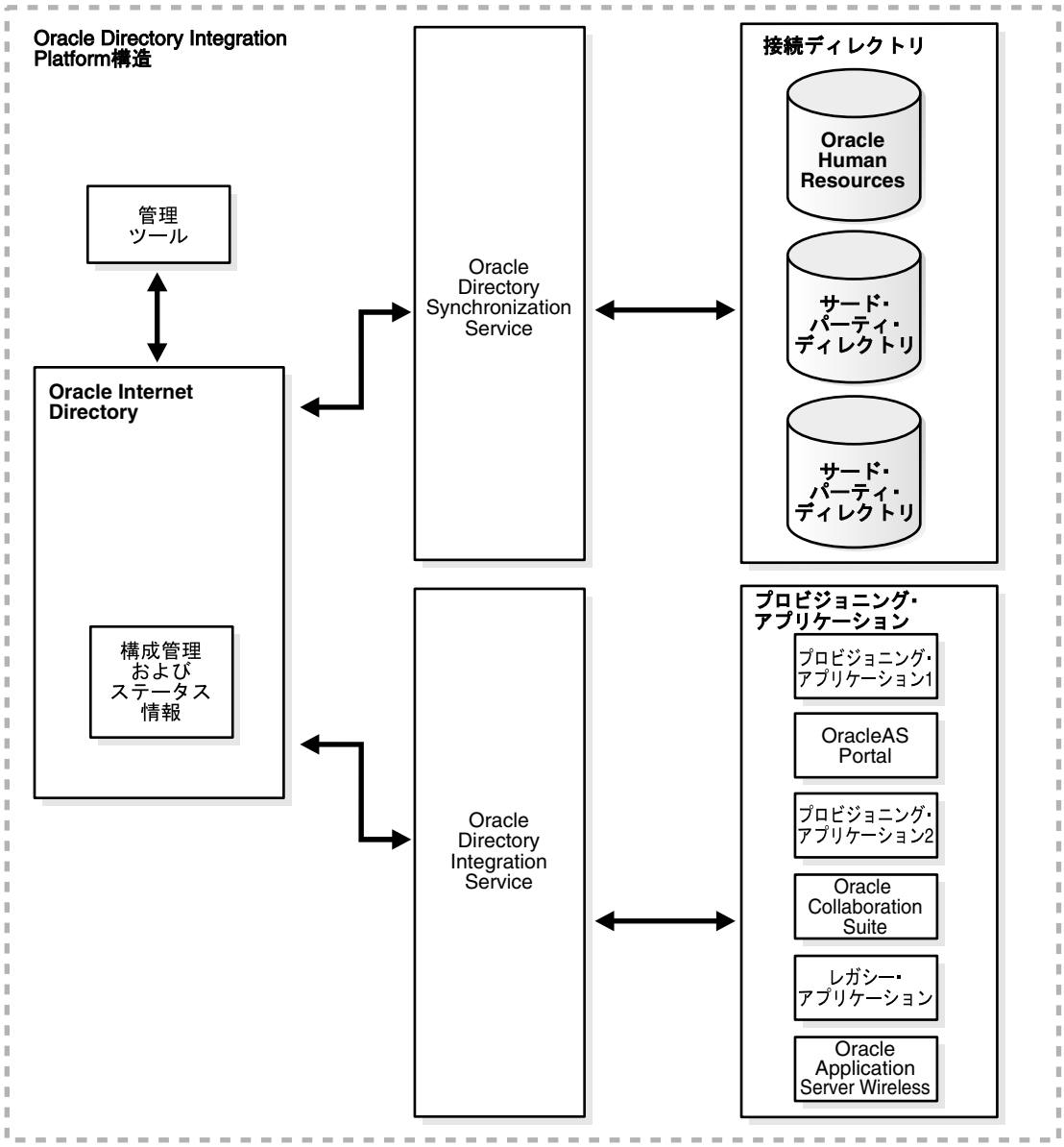


図 1-1 の例では、Oracle Internet Directory は Oracle Directory Synchronization Service によって接続ディレクトリと同期化されます。この例での接続ディレクトリは、Oracle Human Resources およびサード・パーティ・ディレクトリです。同様に Oracle Internet Directory 内の変更は、Oracle Directory Integration Platform Service を使用して各種のアプリケーションに送信されます。この例では、プロビジョニング・アプリケーションとして OracleAS Portal、Oracle Collaboration Suite、Oracle Application Server Wireless、不特定の 2 つのプロビジョニング・アプリケーション、レガシー・アプリケーションがあります。

Oracle Identity Management のインストール・オプション

デフォルトでは、Oracle Directory Integration Platform は、Oracle Internet Directory のコンポーネントとしてインストールされます。ただし、Oracle Directory Integration Platform をスタンドアロンでインストールすることもできます。次のような状況では、Oracle Directory Integration Platform のスタンドアロン・インスタンスをインストールする必要があります。

- パフォーマンス上の理由から、Oracle Internet Directory を別のホストで実行する必要がある場合
- プロビジョニングおよび同期化が必要なアプリケーションに、集中的な処理が必要な場合
- 高可用性のために複数の Oracle Directory Integration Platform インスタンスを実行する必要がある場合

同期、プロビジョニングおよび両者の相違点

同期が扱うのは、アプリケーションではなくディレクトリです。同期では、Oracle Internet Directory と他の接続ディレクトリの両方に存在するエントリと属性の一貫性を確保します。

プロビジョニングが扱うのは、アプリケーションです。プロビジョニングは、アプリケーションで追跡が必要なユーザーやグループのエントリまたは属性への変更を、アプリケーションに通知します。

この項の内容は次のとおりです。

同期

同期によって、Oracle Internet Directory と接続ディレクトリの間で変更を調整できます。すべてのディレクトリが最新のデータのみを使用し、提供するためには、その他の接続ディレクトリでの変更がすべて各ディレクトリに伝達される必要があります。同期は、プロビジョニングによって更新されたデータも含めて、ディレクトリ情報に対する変更の一貫性を確保します。

サード・パーティのディレクトリを Oracle Internet Directory に接続する場合は、特定のディレクトリ用に同期プロファイルを作成します。このプロファイルによって、Oracle Internet Directory と接続ディレクトリとの間で同期化されるデータの書式と内容が指定されます。同期プロファイルを作成するには、Directory Integration アシスタントを使用します。

関連資料：

- 第 III 部「Oracle Directory Integration Platform との同期」
- Directory Integration アシスタントの詳細は、『Oracle Identity Management ユーザー・リファレンス』の Oracle Directory Integration Platform のツールに関する章を参照してください。

プロビジョニング

プロビジョニングによって、たとえば、ユーザーまたはグループに関する情報への変更をアプリケーションに確実に通知できます。このような変更は、アプリケーションでプロセスに対するユーザー・アクセスを許可するかどうかや、使用できるリソースを決定するかどうかに影響を及ぼすことがあります。

プロビジョニングを使用するのは、次の要件を持つアプリケーションを設計またはインストールする場合です。

- ディレクトリを維持しないアプリケーション
- LDAP 対応のアプリケーション
- リソースへのアクセスを認可ユーザーのみに限定するアプリケーション

プロビジョニング対象のアプリケーションをインストールする場合、プロビジョニング・サブスクリプション・ツールを使用して、そのためのプロビジョニング統合プロファイルを作成する必要があります。

関連資料：

- 第 IV 部「Oracle Directory Integration Platform によるプロビジョニング」
- プロビジョニング・サブスクリプション・ツールの詳細は、『Oracle Identity Management ユーザー・リファレンス』の Oracle Directory Integration Platform のツールに関する章を参照してください。

同期とプロビジョニングの相違点

同期とプロビジョニングには、表 1-1 に示すように、操作に重要な相違があります。

表 1-1 ディレクトリ同期とプロビジョニング統合の相違点

比較要素	ディレクトリ同期	プロビジョニング統合
アクションの時期	アプリケーションの配置時。ディレクトリ同期は、Oracle Internet Directory との同期を必要とする接続ディレクトリを対象としています。	アプリケーションの設計時。プロビジョニング統合は、LDAP 対応アプリケーションの開発を担当するアプリケーション設計者を対象としています。
通信方向	一方向または双方向（Oracle Internet Directory から接続ディレクトリへ、またはその逆方向、あるいは両方向）。	双方向（Oracle Internet Directory からプロビジョニング・アプリケーションへ、およびプロビジョニング・アプリケーションから Oracle Internet Directory へ）。
データの種類	ディレクトリ内のあらゆるデータ。	プロビジョニング対象のユーザーとグループに限定。
例	Oracle Human Resources Sun Java System Directory Microsoft Active Directory Novell eDirectory OpenLDAP	OracleAS Portal

Oracle Identity Management 統合に必要なコンポーネント

この項では、Oracle Identity Management 統合に必要なコンポーネントを説明します。内容は次のとおりです。

Oracle Internet Directory

Oracle Internet Directory は、Oracle コンポーネントとサード・パーティのアプリケーションによって、ユーザー ID および資格証明が格納され、アクセスされるリポジトリです。ここでは、Oracle ディレクトリ・サーバーを使用して、ユーザーにより入力された資格証明を Oracle Internet Directory に格納された資格証明と比較することで、ユーザー認証が行われます。資格証明がサード・パーティのディレクトリに格納されていて、Oracle Internet Directory に格納されていない場合でも、ユーザーを認証することはできます。この場合は、Oracle Internet Directory では、サード・パーティのディレクトリ・サーバーに対してユーザー認証を行う外部認証プラグインが使用されます。

Oracle Directory Integration Server

Oracle Directory Integration Server は、Oracle Directory Synchronization Service と Oracle Directory Integration Platform Service の機能を提供する共有サーバー・プロセスです。

Oracle Directory Integration Server の機能

Oracle Directory Integration Server は、次のサービスを実行します。

- Oracle Directory Synchronization Service
  - スケジューリング : 事前定義されたスケジュールに基づいて同期プロファイルを処理
  - マッピング : 接続ディレクトリと Oracle Internet Directory の間のデータ変換ルールを実行
  - データ伝播 : コネクタを使用して接続ディレクトリとデータを交換
  - エラー処理
- Oracle Directory Integration Platform Service
  - スケジューリング : 事前定義されたスケジュールに基づいてプロビジョニング・プロファイルを処理
  - イベント通知 : Oracle Internet Directory に格納されているユーザー・データまたはグループ・データに関連した変更をアプリケーションに通知
  - エラー処理

関連項目 : 第 4 章「Oracle Directory Integration Platform の管理」

Oracle Directory Synchronization Service の概要

Oracle Directory Integration Platform 環境における接続ディレクトリの内容は、Oracle Directory Synchronization Service を介して Oracle Internet Directory と同期化されます。

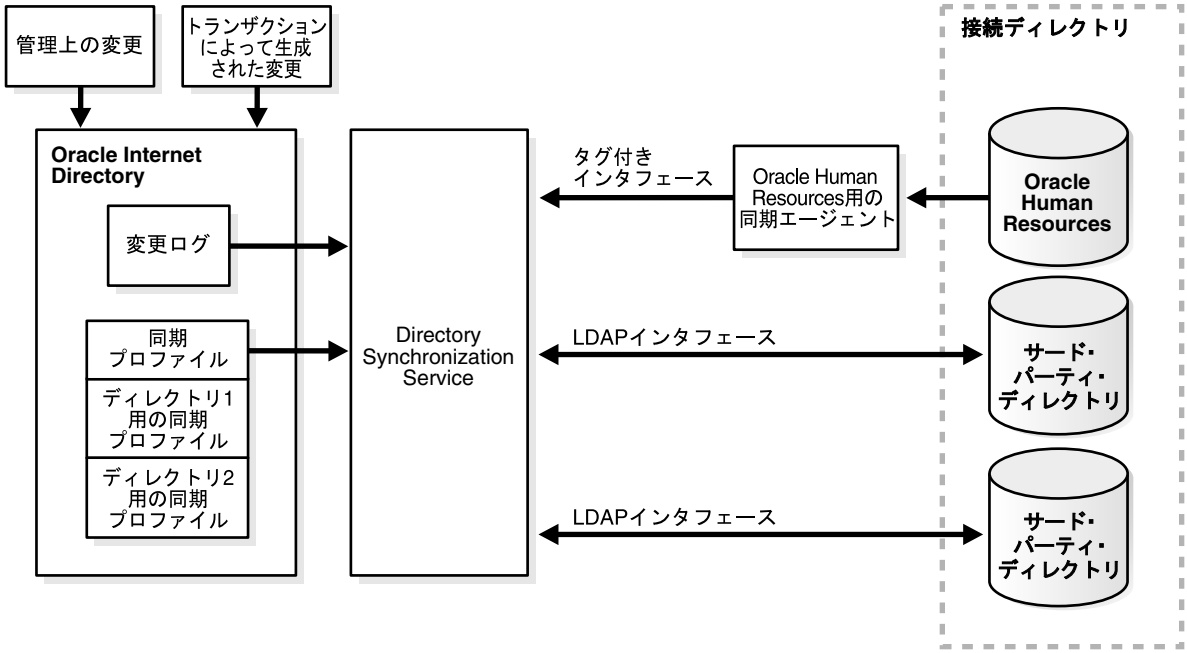
Oracle Application Server コンポーネントの場合、Oracle Internet Directory はすべての情報の中央ディレクトリであり、他のすべてのディレクトリと同期しています。この同期には、次の 2 つの方向があります。

- 一方向 : 一部の接続ディレクトリは、Oracle Internet Directory に変更を提供するのみで、変更を受け取ることがありません。たとえば、従業員情報のプライマリ・リポジトリで比較のための基準である Oracle Human Resources がこれに該当します。
- 双方向 : Oracle Internet Directory での変更を接続ディレクトリにエクスポートでき、接続ディレクトリでの変更を Oracle Internet Directory にインポートできます。

同期サービスでは、特定の属性を対象とする（または無視する）ことができます。たとえば、Oracle Human Resources 内の従業員バッジ番号の属性は、Oracle Internet Directory、その接続ディレクトリまたはクライアント・アプリケーションには関係ありません。同期は不要です。その一方で、従業員識別番号はこれらのコンポーネントとも関係があるため、同期が必要です。

図 1-2 に、配置例における Oracle Directory Synchronization Service 内のコンポーネント間の相互作用を示します。

図 1-2 Oracle Directory Synchronization Service のディレクトリ同期の相互作用



このような同期アクティビティのすべてをトリガーする中心的なメカニズムが、Oracle Internet Directory の変更ログです。Oracle Internet Directory など、接続ディレクトリへの変更ごとに、変更ログに 1 つ以上のエントリが追加されます。Oracle Directory Synchronization Service の機能は次のとおりです。

- 変更ログを監視します。
- 変更が 1 つ以上の同期プロファイルに対応している場合は、常にアクションを実行します。
- ログに記録された変更に個々のプロファイルが対応している他の接続ディレクトリすべてに、該当する変更を提供します。接続ディレクトリには、リレーショナル・データベース、Oracle Human Resources、Microsoft Active Directory、Sun Java System Directory、Novell eDirectory、OpenLDAP などがあります。Oracle Directory Synchronization Service は、接続ディレクトリが要求するインタフェースと書式を使用してこれらの変更を提供し

ます。Oracle Directory Integration Platform コネクタを介した同期によって、Oracle Internet Directory クライアントに必要なすべての情報について、Oracle Internet Directory が最新の状態に保持されます。

Oracle Directory Integration Platform Service の概要

Oracle Directory Integration Platform Service は、ユーザーまたはグループ情報などの変更が各プロビジョニング・アプリケーションに通知されることを保証します。これは、プロビジョニング統合プロファイルに含まれている情報に基づいて行われます。各プロビジョニング・プロファイルの役割は、次のとおりです。

- そのプロファイルを適用するアプリケーションと組織を一意に識別します。
- アプリケーションに通知する必要があるユーザー、グループ、操作などを指定します。

プロファイルは、アプリケーションのインストール時に、プロビジョニング・サブスクリプション・ツールを使用して作成する必要があります。

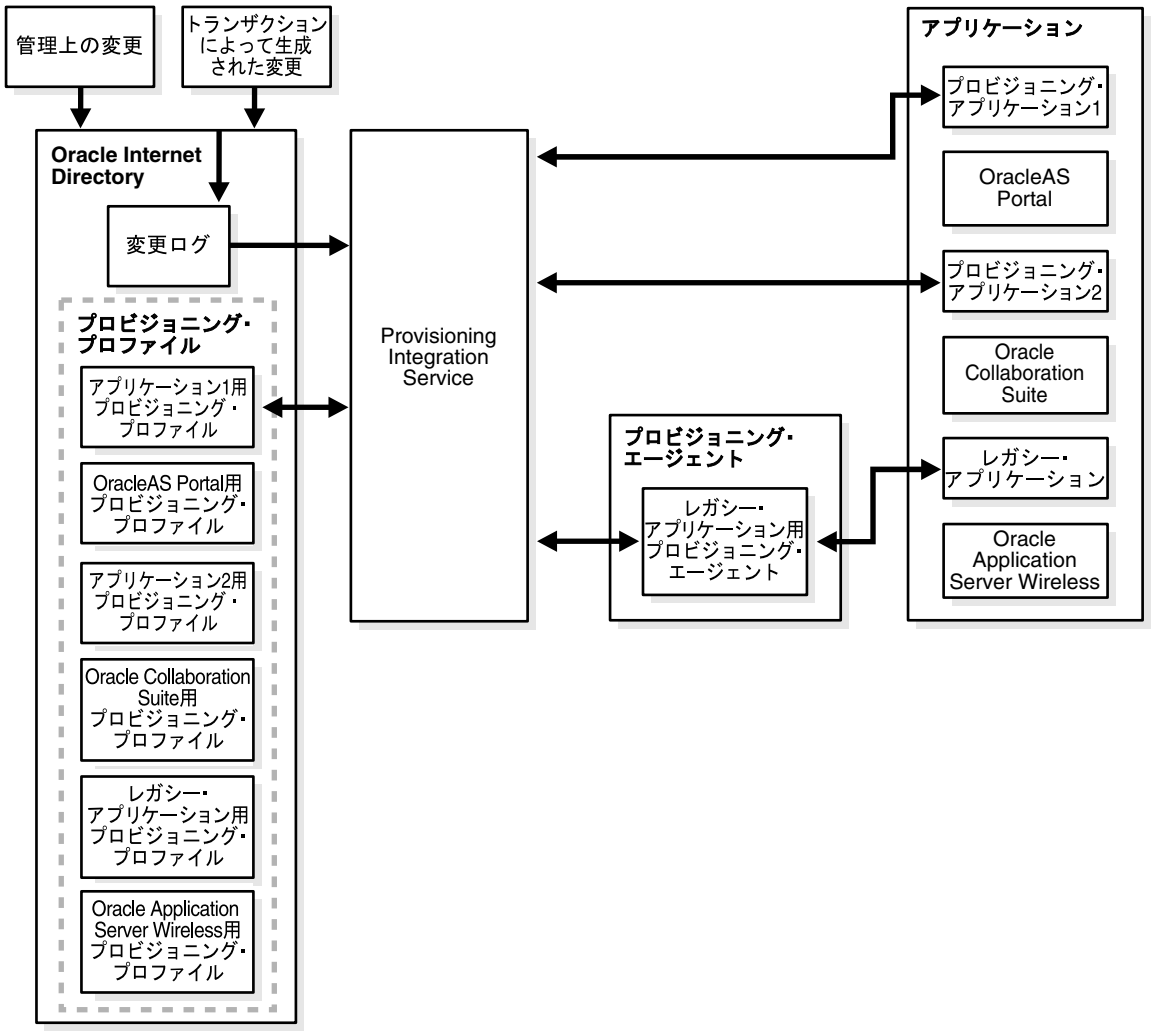
> **関連資料：** プロビジョニング・サブスクリプション・ツールの詳細は、『Oracle Identity Management ユーザー・リファレンス』の Oracle Directory Integration Platform のツールに関する章を参照してください。

Oracle Internet Directory での変更がアプリケーションのプロビジョニング・プロファイルに指定されているものと一致すると、Oracle Directory Integration Platform Service は、そのアプリケーションに関連データを送信します。

注意： レガシー・アプリケーション（Oracle Directory Integration Platform Service のインストール前に稼働状態であったアプリケーション）は、インストール時に通常の方法ではサブスクライブされません。レガシー・アプリケーションを使用してプロビジョニング情報を受信できるようにするには、プロビジョニング・プロファイルに加えて、**プロビジョニング・エージェント**を開発する必要があります。このエージェントは、Oracle Internet Directory からの関連データをレガシー・アプリケーションに必要な正確な書式に変換する必要があります。

図 1-3 に、Oracle Directory Integration Platform Service 環境でのコンポーネント間の相互作用を、レガシー・アプリケーションに使用するプロビジョニング・エージェントの特別なケースも含めて示します。

図 1-3 Oracle Directory Integration Platform Service の相互作用



Oracle Application Server Single Sign-On

Oracle Application Server Single Sign-On（OracleAS Single Sign-On）を使用すると、ユーザーは 1 回のみのログインで、Web ベースの Oracle コンポーネントにアクセスできます。

Oracle コンポーネントは、ログイン機能を OracleAS Single Sign-On Server に委任します。初めて Oracle コンポーネントにログインする場合は、そのコンポーネントによって OracleAS Single Sign-On Server にログインがリダイレクトされます。OracleAS Single Sign-On Server では、Oracle Internet Directory に格納されている資格証明に対して、ユーザーが入力した資格証明を検証することによってユーザーが認証されます。ユーザーを認証すると、残りのセッション中、使用を要求し認可されたすべてのコンポーネントに対するユーザー・アクセス権限を OracleAS Single Sign-On Server によって付与されます。

> **関連資料：** OracleAS Single Sign-On の詳細は、『Oracle Application Server Single Sign-On 管理者ガイド』を参照してください。

2

Oracle Directory Integration Platform のセキュリティ機能

この章では、Oracle Directory Integration Platform のセキュリティにおける最も重要な事項について説明します。内容は次のとおりです。

Oracle Directory Integration Platform での認証

認証は、Oracle ディレクトリ・サーバーが、そのディレクトリに接続しているユーザーの正確な識別情報を取得するプロセスです。認証は、LDAP セッションが `ldapbind` 操作によって確立されたときに発生します。

Oracle Directory Integration Platform の各コンポーネントが、ディレクトリへのアクセスを許可される前に適切に認証されることは重要です。

この項の内容は次のとおりです。

Secure Sockets Layer と Oracle Directory Integration Platform

Oracle Directory Integration Platform は、**Secure Sockets Layer** を使用するかどうかにかかわらず配置できます。SSL の実装は、次のモードをサポートします。

- 認証なし : SSL データ暗号化を提供しますが、認証には SSL を使用しません。
- SSL サーバー認証 : SSL データ暗号化とクライアントに対する SSL 認証の両方が含まれます。Oracle Directory Integration Platform では、サーバーはディレクトリ・サーバーであり、クライアントは Oracle Directory Integration Platform です。

  サーバーは、信頼できる**認証局**が発行する**証明書**を送信することにより、クライアントに対する自己識別を行います。このモードには、公開鍵インフラストラクチャ（PKI）と証明書を保持するための SSL ウォレットが必要です。

Oracle Directory Integration Platform で SSL を使用するには、Oracle ディレクトリ・サーバーと Oracle Directory Integration Platform の両方を SSL モードで起動する必要があります。

> **関連資料 :** Oracle ディレクトリ・サーバーを SSL モードで起動する方法は、『Oracle Internet Directory 管理者ガイド』の予備的なタスクと情報に関する章を参照してください。

Oracle Directory Integration Server 認証

Directory Integration Server の複数のインスタンスは、様々なホストにインストールして実行することができます。ただし、これを行う場合は、Directory Integration Server を装う不正なユーザーまたはその不正コピーを使用する不正なユーザーに注意する必要があります。

このようなセキュリティ問題を回避するには、次の点に注意します。

- 各 Directory Integration Server が正しく識別されていることを確認する。
- Directory Integration Server が Oracle Internet Directory へのアクセス権限を取得する前に正しく認証されていることを、Directory Integration Server の起動時に確認する。

非 SSL 認証

非 SSL 認証を使用するには、odisrvreg と呼ばれる登録ツールを使用して、各 Directory Integration Server を登録します。

この登録ツールでは、次のものを作成できます。

- ディレクトリ内の識別情報エントリ。Directory Integration Server は、ディレクトリにバインドするときにこのエントリを使用します。
- 暗号化されたパスワード。このパスワードは、Directory Integration Server エントリ内に格納されます。
- ローカル・ホストのプライベート・ウォレット。このウォレットには、暗号化されたパスワードを含むセキュリティ資格証明が含まれています。ウォレットの名前は odi.properties ファイルに指定され、$*ORACLE_HOME*/ldap/odi/conf ディレクトリに格納されます。

Directory Integration Server は、ディレクトリにバインドするときにプライベート・ウォレット内の暗号化されたパスワードを使用します。

注意： このウォレットは不正アクセスから保護するようにしてください。

関連項目： 4-13 ページの「Oracle Directory Integration Platform の手動登録」

SSL モードでの認証

ディレクトリ・サーバーの識別情報を設定するには、Oracle Internet Directory と Directory Integration Server の両方を SSL サーバー認証モードで起動します。この場合、ディレクトリ・サーバーは自身の証明書を Directory Integration Server に提供し、Directory Integration Server は Oracle Internet Directory のクライアントとして機能します。

Directory Integration Server は、非 SSL モードと同じメカニズムを使用して認証されます。

サード・パーティのディレクトリに接続するときに SSL を使用するように Oracle Directory Integration Platform を構成することもできます。この場合は、4-7 ページの「Oracle Internet Directory と接続ディレクトリの SSL 証明書の管理」で説明されているように、接続ディレクトリ証明書をウォレットに保存します。

プロファイルの認証

Oracle Internet Directory では、統合プロファイルは、識別名（DN）とパスワードを持つユーザーを表します。プロファイルにアクセスできるユーザーは次のとおりです。

- Oracle Directory Integration Platform の管理者（DIPAdmin）、識別名 Cn=dipadmin,cn=dipadmins,cn=directory integration platform, cn=products,cn=oraclecontext
- Oracle Directory Integration Platform 管理者グループのメンバー（DIPAdminGroup）、識別名 cn=dipadmingrp,cn=dipadmin,cn=directory integration platform, cn=products,cn=oraclecontext

Directory Integration Server が統合プロファイルに基づいて Oracle Internet Directory にデータをインポートする場合、その統合プロファイルとしてディレクトリにプロキシ・バインドします。Oracle Directory Integration Platform は、SSL モードでも非 SSL モードでもバインドできます。

アクセス制御、認可および Oracle Directory Integration Platform

認可は、ユーザーが権限を持つ情報のみの読取りまたは更新を行うことを保証するプロセスです。ディレクトリ・セッション内でディレクトリ操作が行われようとすると、ディレクトリ・サーバーは、その操作の実行に必要な権限がユーザーに与えられていることを確認します(ユーザーの識別は、セッションに対応付けられた認可識別子によって行われます)。ユーザーに権限がない場合、ディレクトリ・サーバーはこれらの操作を許可しません。この方法（アクセス制御）によって、ディレクトリ・サーバーは、ディレクトリ・ユーザーによる不正操作からディレクトリ・データを保護します。

アクセスを Oracle Internet Directory データの必要なサブセットのみに制限するには、Directory Integration Server とコネクタの両方に対する適切なアクセス・ポリシーをディレクトリに設定します。

この項では、このようなポリシーの詳細を説明します。内容は次のとおりです。

Oracle Directory Integration Platform のアクセス制御

Oracle Directory Integration Server は、次のようにディレクトリへのバインドをそれ自身として行う場合と、プロファイルのかわりに行う場合があります。

- それ自身としてバインドする場合、Directory Integration and Provisioning Server は様々な統合プロファイルに情報をキャッシュできます。これによって、Directory Integration Server は、様々なコネクタによって実行される同期アクションをスケジュールできます。
- プロファイルのかわりに操作を行う場合、Directory Integration Server はプロファイルのプロキシとして動作します。つまり、ディレクトリにバインドして様々な操作を実行するためにプロファイル資格証明を使用します。Directory Integration Server は、プロファイルで許可された操作のみをディレクトリ内で実行できます。

Directory Integration Server に付与されるアクセス権限を設定し管理するために、Oracle Directory Integration Platform はインストール時に `odisgroup` と呼ばれるグループ・エントリを作成します。`odisgroup` の識別名は `cn=odisgroup,cn=odi,cn=oracle internet directory` です。Directory Integration Server は、登録時にこのグループのメンバーになります。

Directory Integration Server に付与されるアクセス権限を制御するには、`odisgroup` エントリにアクセス制御ポリシーを設定します。デフォルトのポリシーでは、プロファイルにアクセスするための様々な権限が Directory Integration Server に付与されます。たとえば、デフォルトのポリシーでは、Directory Integration Server は、プロファイルのかわりにプロキシとしてバインドする Oracle Internet Directory と接続ディレクトリとの間でユーザー・パスワードを比較できます。デフォルトのポリシーによって、Directory Integration Server は、最終正常実行時間や同期ステータスなど、プロファイルのステータス情報を変更することもできます。

プロファイルのアクセス制御

統合プロファイルを使用して Oracle Internet Directory データへのアクセスを制御するには、Oracle Internet Directory 内に適切なアクセス制御ポリシーを設定します。このポリシーによって、あるプロファイルが同期化または処理したデータを他のプロファイルの干渉から保護できます。また、ある属性の変更を、その属性の同期を所有する統合プロファイルにのみ許可することもできます。

> **関連資料：** グループ・エントリのアクセス制御ポリシーの設定方法については、『Oracle Internet Directory 管理者ガイド』のアクセス制御の章のセキュリティ・グループに関する項を参照してください。

たとえば、Oracle Internet Directory のインストール時に `odipgroup` と呼ばれるグループ・エントリを作成すると、様々なプロファイルに付与したアクセス権限を制御できます。権限は、適切なアクセス・ポリシーを `odipgroup` エントリに設定することによって制御されます。各プロファイルはこのグループのメンバーです。メンバーシップは、プロファイルがシステムに登録されるときに設定されます。製品とともに自動的にインストールされたデフォルトのアクセス・ポリシーでは、プロファイルに対して、そのプロファイルが所有する統合プロファイルへの標準的なアクセス権限が付与されます。たとえば、統合プロファイル内の `orclodipConDirLastAppliedChgTime` パラメータなどのステータス情報を変更できる権限が付与されます。また、デフォルトのアクセス・ポリシーの場合、プロファイルは Oracle Internet Directory の変更ログにアクセスできます（デフォルトのアクセス・ポリシー以外ではアクセスは制限されます）。

`odisgroup` グループ・エントリとそのデフォルトのポリシーは、Oracle Internet Directory のサーバー・インストール時に作成されます。Oracle Directory Integration Platform のみのインストールの場合は、これらのグループおよびポリシーは作成されません。

データ整合性と Oracle Directory Integration Platform

Oracle Directory Integration Platform は、SSL を使用して、送信時にデータの変更、削除または再現が行われてい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、Message-Digest algorithm 5（MD5）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そのメッセージ・ダイジェストを組み込みます。

データ・プライバシと Oracle Directory Integration Platform

Oracle Directory Integration Platform は、SSL で使用可能な公開鍵暗号を使用して、データが送信中に開示されないことを保証します。公開鍵暗号では、メッセージの送信側が受信側の公開鍵を使用して、メッセージを暗号化します。メッセージが送達されると、受信側は、受信側の秘密鍵を使用して、メッセージを復号化します。

Directory Integration Server と Oracle Internet Directory の間でデータを安全に交換するには、両方のコンポーネントを SSL モードで実行します。

ツール・セキュリティと Oracle Directory Integration Platform

一般的に使用されているツールは、すべて SSL モードで実行することにより Oracle Internet Directory にデータを安全に送信できます。たとえば、次のツールがあります。

- Oracle Directory Manager
- Oracle Directory Integration Server 登録ツール
- Oracle Directory Integration Server 管理ツール
- Directory Integration アシスタント（`dipassistant`）
- プロビジョニング・サブスクリプション・ツール

第II部

Oracle Directory Integration Platform の一般管理

第 II 部では、Oracle Directory Integration Platform の実行に関連する一般的な管理タスクのいくつかを説明します。より具体的な管理情報については、それぞれの項を参照してください。

第 II 部は次の各章で構成されています。

3

Oracle Directory Integration Platform 管理ツール

この章では、Oracle Directory Integration Server 管理ツールと、Oracle Directory Integration Platform の管理に使用されるその他の各種ツールについて説明します。内容は次のとおりです。

Oracle Directory Integration Server 管理ツール

Oracle Directory Integration Server 管理ツールは、Oracle Directory Integration Platform をグラフィカルに管理するための Java ベースのユーティリティです。この項では、その基本機能のいくつかを説明します。

この項の内容は次のとおりです。

Oracle Directory Integration Server 管理ツールの起動

Oracle Directory Integration Server 管理ツールを起動するには、ディレクトリ・サーバー・インスタンスが稼働している必要があります。

> **関連項目：** Oracle Directory Integration Server 管理ツールによる Oracle Directory Integration Platform の管理方法の詳細は、第 7 章「ディレクトリ同期の管理」を参照してください。

Oracle Directory Integration Server 管理ツールを起動するには、表 3-1 に示すように、使用しているオペレーティング・システムの方法に従ってください。

表 3-1 オペレーティング・システム固有の Oracle Directory Integration Server 管理ツールの起動方法

オペレーティング・システム	方法
Windows	「**スタート**」メニューから、「**プログラム**」、「***ORACLE_HOME***」、「**Integrated Management**」、「**Oracle Directory Integration Server Administration**」を選択します。
UNIX/Linux	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。 `dipassistant -gui`

初めて Oracle Directory Integration Server 管理ツールを起動すると、サーバーに接続する必要があることを知らせるアラートが表示されます。「**OK**」をクリックします。「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。

Oracle Directory Integration Server 管理ツールを使用したディレクトリ・サーバーへの接続

> **注意：** このツールを使用するには、cn=dipadmingrp,cn=dipadmin,cn=directory integration platform,cn=products,cn=oraclecontext グループのメンバーであることが必要です。正しい権限を持っていない場合は、ツールへのアクセスが拒否されます。

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。ポート番号は変更できます。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 Directory Integration Server 管理の「接続」ダイアログ・ボックスが表示されます。

   接続対象のディレクトリ・サーバーが最初のログイン・ウィンドウに表示されていない（つまり、デフォルトのディレクトリ・サーバーではない）場合は、「**サーバー**」フィールドの右にあるボタンをクリックすると、別のディレクトリ・サーバーを選択できます。

   このダイアログ・ボックスには、過去に接続したすべてのディレクトリ・サーバーのリストが表示されます。このリストからディレクトリ・サーバーを選択すれば、そのサーバーに対する接続、削除、編集の他、サーバーを別の管理接続用のテンプレートとして使用することもできます。

   リストからサーバーに接続するには、そのサーバーを選択し、ダイアログ・ボックスの下にある「**選択**」をクリックします。Oracle Internet Directory の「接続」ダイアログ・ボックスにサーバーおよびポートが表示され、ここから接続できます。

   既存の定義済接続を削除するには、サーバーを選択し、「**削除**」をクリックします。サーバーのエントリは、定義済管理接続のリストから削除されます。

   新しい管理接続を定義する手順は、次のとおりです。

   - 新しい管理接続を追加する場合は、「**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。このダイアログ・ボックスにサーバー名とポートを入力し、「**OK**」をクリックすると、「ディレクトリ・サーバーの選択」ダイアログ・ボックスに新しい管理接続が表示されます。ここから、この管理接続を選択して Oracle Internet Directory の「接続」ダイアログ・ボックスに表示し、接続できるようにします。
   - 既存の管理接続を新しい接続用のテンプレートとして使用する場合は、テンプレートとして使用するサーバーを選択し、「**類似サーバーの追加**」をクリックします。テンプレート・サーバー情報が記入された「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。新しい管理接続を作成するには、これらのエントリを編集する必要があります。このダイアログ・ボックスにサーバー名とポートを入力し、「**OK**」をクリックすると、「ディレクトリ・サーバーの選択」ダイアログ・ボックスに新しい管理接続が表示されます。ここから、この管理接続を選択して Oracle Internet Directory の「接続」ダイアログ・ボックスに表示し、接続できるようにします。
   - 既存の接続を編集する場合は、その接続を選択して、「**編集**」をクリックします。サーバーおよびポート情報が記入された「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。エントリを編集し、変更を保存します。このダイアログ・ボックスにサーバー名とポートを入力し、「**OK**」をクリックすると、「ディレクトリ・サーバーの選択」ダイアログ・ボックスに新しい管理接続が表示されます。ここから、この管理接続を選択して Oracle Internet Directory の「接続」ダイアログ・ボックスに表示し、接続できるようにします。

2. 「資格証明」タブ・ページの各フィールドに、このサーバー・インスタンスに固有の情報を入力します。

   「資格証明」タブ・ページのフィールドの詳細は、A-2 ページの表 A-1 を参照してください。

   関連資料：

   - SSL の有効化の方法と、セキュリティに対するポート変更の影響については、『Oracle Internet Directory 管理者ガイド』の SSL とディレクトリに関する章を参照してください。
   - 識別名の書式設定の方法については、『Oracle Internet Directory 管理者ガイド』の概念の章のエントリに関する項を参照してください。
   - SSL の使用時に Oracle Wallet Manager を使用してウォレットを作成する方法は、『Oracle Advanced Security 管理者ガイド』を参照してください。

3. 「**資格証明**」タブ・ページの「**SSL 使用可能**」チェック・ボックスを選択した場合は、次に「**SSL**」タブを選択します。
4. 「SSL」タブ・ページで、必要なデータをフィールドに入力します。

   「SSL」タブ・ページのフィールドの詳細は、A-4 ページの表 A-2 を参照してください。
5. 「**ログイン**」を選択します。Oracle Directory Integration Server 管理ツールが表示されます。

Oracle Directory Integration Server 管理ツールのナビゲート

この項では、Oracle Directory Integration Server 管理の概要を紹介し、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 Integration Server 管理の概要

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。最初にツールを開いたときのナビゲータ・ペインには、1 つのツリー項目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、変更がコミットされ、ウィンドウではそのまま変更操作を続けることができます。「OK」をクリックすると、変更がコミットされ、ウィンドウが閉じます。

同様に、一部のウィンドウには「**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 Integration Server 管理のメニュー・バー

表 3-2 に、メニュー・バーからアクセスできるメニューを示します。各メニュー項目は、表示しているペインやタブ・ページによって、使用できる場合と使用できない場合があります。

表 3-2 Oracle Directory Integration Server 管理のメニュー・バー

メニュー	メニュー項目
ファイル	**作成 :** オブジェクトを追加します。
	類似項目の作成 : 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 Integration Server 管理ツールを終了します。
編集	**編集 :** オブジェクトを変更します。
	削除 : オブジェクトを削除します。
	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。
表示	**リフレッシュ :** メモリーに格納されているデータを更新し、データベースに変更を反映します。
	切離し : Oracle Directory Integration Server 管理ツール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。
ヘルプ	**目次 :** ヘルプ・ナビゲータの「目次」タブ・ページを表示します。
	キーワードで検索 : オンライン・ヘルプ・ガイドのワード検索に使用するヘルプ検索ダイアログ・ボックスを表示します。
	Oracle Internet Directory のバージョン情報 Oracle Internet Directory: Oracle Internet Directory のバージョン情報を表示します。

Oracle Directory Integration Server 管理ツールを使用したディレクトリ・サーバーからの切断

Oracle Directory Integration Server 管理ツールを使用してディレクトリ・サーバーから切断するには、「**ファイル**」メニューから「**切断**」を選択します。また、Oracle Directory Integration Server 管理ツールを終了すると、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、`osdadmin.ini` ファイルのユーザーのホーム・ディレクトリに格納されます。

Oracle Directory Integration Server 管理ツールを再起動すると、これまでのサーバー接続がすべて、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 Integration Platform 管理用のグラフィカル・ツール

Oracle Directory Integration Server 管理ツールの他に、次のグラフィカル・ツールを使用して Oracle Directory Integration Platform を管理できます。

- Oracle Directory Manager
- Oracle Internet Directory セルフ・サービス・コンソール
- Oracle Internet Directory プロビジョニング・コンソール

Oracle Directory Manager

Oracle Directory Manager は、Oracle Internet Directory をグラフィカルに管理するための Java ベースのツールです。Oracle Directory Manager を使用すると、次の操作を行うことができます。

- 同期用のディレクトリ統合プロファイルの作成、変更および削除
- 同期プロファイルおよび同期ステータスの監視
- すべての Oracle Directory Integration Server インスタンスのステータスの監視
- 同期の問題のトラブルシューティング

関連資料：

- Oracle Directory Manager の詳細は、『Oracle Internet Directory 管理者ガイド』を参照してください。
- 第 4 章「Oracle Directory Integration Platform の管理」

Oracle Internet Directory セルフ・サービス・コンソール

Oracle Internet Directory セルフ・サービス・コンソールによって、管理者権限を複数の管理者およびユーザーに委任することができます。これは、Oracle Delegated Administration Services を使用して作成されたスタンドアロン・アプリケーションで、委任された管理者やユーザーがディレクトリ内のデータを管理するための唯一のグラフィカル・インタフェースを提供します。Oracle Internet Directory セルフ・サービス・コンソールを使用すると、管理者もユーザーも各自の権限に応じて、各種のディレクトリ操作を実行できます。統合された配置では、Oracle Internet Directory セルフ・サービス・コンソールは、主にレルム・パラメータのカスタマイズに使用されます。

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

Oracle Internet Directory プロビジョニング・コンソール

Oracle Internet Directory プロビジョニング・コンソールは、管理者が Oracle Internet Directory でユーザーをプロビジョニングするための単一のグラフィカル・インタフェースです。プロビジョニング・コンソールは、Oracle Delegated Administration Services で作成され、Oracle Internet Directory セルフ・サービス・コンソールとともに動作します。

関連項目： 第 IV 部「Oracle Directory Integration Platform によるプロビジョニング」

Oracle Directory Integration Platform 管理用のコマンドライン・ツール

次のコマンドライン・ツールは、Oracle Directory Integration Platform の管理に使用できます。

- OID 制御と OID モニター
- Oracle Directory Integration Platform 登録ツール
- Directory Integration アシスタント
- プロビジョニング・サブスクリプション・ツール
- エントリおよび属性の管理コマンドライン・ツール
- スキーマ同期ツール

関連資料： この項で説明している各ツールに必要な構文と、Oracle Internet Directory および Oracle Directory Integration Platform の管理に使用できるその他のコマンドライン・ツールについては、『Oracle Identity Management ユーザー・リファレンス』を参照してください。

OID 制御と OID モニター

OID 制御と OID モニターは、Oracle Directory Integration Platform の起動、停止および監視のために使用します。

Oracle Internet Directory では、OID 制御と OID モニターを使用して、Oracle ディレクトリ・サーバーまたは Oracle Directory Integration Server のいずれかがインストールされている *ORACLE_HOME* で、Directory Integration Server を制御できます。

Oracle Internet Directory をクライアントのみにインストールした場合は、OID 制御ユーティリティと OID モニターはインストールされません。この場合は、手動で Oracle Directory Integration Server を起動します。この構成でも、Oracle Directory Integration Server 管理ツールを使用して Oracle Directory Integration Server のステータスを調べることはできます。

関連項目： 第 4 章「Oracle Directory Integration Platform の管理」

Oracle Directory Integration Platform 登録ツール

Oracle Directory Integration Platform 登録ツール（`odisrvreg`）により、Oracle Directory Integration Platform がディレクトリに登録されます。登録は、ディレクトリにエントリを作成し、Oracle Directory Integration Platform のパスワードを設定することで行われます。登録エントリがすでに存在する場合は、`odisrvreg` ツールを使用して既存のパスワードを再設定できます。`odisrvreg` ツールにより、odisrvwallet_hostname というローカルファイルを $*ORACLE_HOME*/ldap/odi/conf に作成することもできます。このファイルは、Oracle Directory Integration Platform のプライベート・ウォレットとして機能し、起動時にディレクトリにバインドするために使用されます。

Directory Integration アシスタント

Directory Integration アシスタント（dipassistant）は、Oracle Directory Integration Server 管理ツールのコマンドライン版です。Directory Integration アシスタントで実行できるタスクには次のようなものがあります。

- 同期プロファイルの作成、変更および削除
- Oracle Internet Directory でのすべての同期プロファイルの表示
- 特定の同期プロファイルの詳細の表示
- 接続ディレクトリと Oracle Internet Directory 間のデータの移行（ブートストラップ）
- Oracle Directory Integration Platform に対するウォレット・パスワードの設定
- Oracle Directory Integration Platform 管理者のパスワードのリセット
- 別の Oracle Internet Directory ノードへの統合プロファイルの移動

注意： Oracle Identity Management 10*g*（10.1.4.0.1）から、Directory Integration アシスタント（dipassistant）では Secure Sockets Layer（SSL）もサポートします。

プロビジョニング・サブスクリプション・ツール

ディレクトリのプロビジョニング・プロファイル・エントリを管理するには、プロビジョニング・サブスクリプション・ツール（oidprovtool）を使用します。すなわち、プロビジョニング・サブスクリプション・ツールを使用して次のことができます。

- 新しいプロビジョニング・プロファイルの作成
- 既存のプロビジョニング・プロファイルの有効化または無効化
- 既存のプロビジョニング・プロファイルの変更
- 既存のプロビジョニング・プロファイルの削除
- プロビジョニング・プロファイルの現行ステータスの取得
- 既存のプロビジョニング・プロファイル内にあるすべてのエラーの消去

エントリおよび属性の管理コマンドライン・ツール

表 3-3 に、Oracle Directory Integration Platform とともに使用できるエントリおよび属性の管理コマンドライン・ツールを示します。

表 3-3 エントリおよび属性の管理コマンドライン・ツール

ツール	説明
カタログ管理ツール（`catalog.sh`）	索引付き属性。
`ldapadd`	エントリとそれらのオブジェクト・クラス、属性および値をディレクトリに追加します。
`ldapaddmt`	エントリとそれらのオブジェクト・クラス、属性および値を同時にディレクトリに追加するための複数のスレッドをサポートします。
`ldapbind`	クライアントをサーバーに対して認証できるかどうかを決定します。
`ldapcompare`	指定された属性値をエントリの属性値と照合します。
`ldapdelete`	ディレクトリからエントリを削除します。
`ldapmoddn`	エントリの識別名または相対識別名を変更します。
`ldapmodify`	エントリの属性を変更します。
`ldapmodifymt`	エントリを同時に変更するための複数のスレッドをサポートします。
`ldapsearch`	ディレクトリ内のエントリを検索します。

スキーマ同期ツール

スキーマ同期ツール（`schemasync`）を使用すると、Oracle Internet Directory とサード・パーティの LDAP ディレクトリとの間で、スキーマ要素（つまり、属性とオブジェクト・クラス）を同期化できます。

4

Oracle Directory Integration Platform の管理

この章では、Oracle Directory Integration Server について説明し、その構成方法と管理方法を示します。内容は次のとおりです。

- Oracle Directory Integration Platform についての操作情報
- Oracle Directory Integration Platform の情報の表示
- Oracle Directory Integration Platform が使用する構成設定エントリの管理
- Oracle Internet Directory と接続ディレクトリの SSL 証明書の管理
- Oracle Directory Integration Platform の起動、停止および再起動
- 高可用性を目的とした場合の Oracle Directory Integration Platform の起動と停止
- Oracle Directory Integration Platform に対するデバッグ・レベルの設定
- レプリケート環境での Oracle Directory Integration Platform の管理
- ログ・ファイルの検索
- Oracle Directory Integration Platform の手動登録

関連項目： Oracle Directory Integration Platform により実行される機能の概要は、1-6 ページの「Oracle Directory Integration Server」を参照してください。

注意： セキュリティ上の理由により、ディレクトリ・サーバーと同じホスト上で Oracle Directory Integration Server を実行することをお薦めします。別のホスト上で実行する場合は、『Oracle Internet Directory 管理者ガイド』の SSL およびディレクトリに関する章で説明されているように、SSL を使用して実行してください。

Oracle Directory Integration Platform についての操作情報

この項では、Oracle Directory Integration Platform の構造および操作方法について説明します。内容は次のとおりです。

ディレクトリ同期プロファイル

Oracle Directory Integration Platform では、ディレクトリ同期プロファイルとディレクトリ・プロビジョニング・プロファイルという 2 種類のプロファイルを作成できます。**ディレクトリ同期プロファイル**は、Oracle Internet Directory と外部システムとの間で同期が実行される方法を記述します。ディレクトリ同期プロファイルは、インポート・プロファイルとエクスポート・プロファイルの 2 種類を作成できます。インポート・プロファイルは、接続ディレクトリから Oracle Internet Directory に変更をインポートするのに対し、エクスポート・プロファイルは、Oracle Internet Directory から接続ディレクトリに変更をエクスポートします。**ディレクトリ・プロビジョニング・プロファイル**は、Oracle Directory Integration Platform からディレクトリ対応アプリケーションに送信されるプロビジョニング関連の通知の性質を記述します。プロファイルの各タイプは特殊な種類の**ディレクトリ統合プロファイル**で、Oracle Directory Integration Platform と外部システムとの通信方法と通信内容を記述する Oracle Internet Directory 内のエントリです。

Oracle Directory Integration Platform と構成設定エントリ

各 Oracle Directory Integration Server は、次のいずれかの操作を行うためにコネクタ・セットを実行できます。

- Oracle Internet Directory と接続ディレクトリとの同期化。同期用のコネクタ・セットは、Oracle Directory Integration Server の起動時にコマンドラインに入力した構成設定番号で指定されます。
- Oracle コンポーネント用のユーザー、グループおよびレルムのプロビジョニング。プロビジョニング用のプロファイル・セットは、Oracle Directory Integration Server の起動時にコマンドラインに入力した `grpID` 引数で指定されます。

構成設定番号を指定しない場合、Oracle Directory Integration Server はプロビジョニング・プロファイル処理用のモードで起動します。構成設定番号を指定し、その構成設定番号用のディレクトリに統合プロファイルがない場合、Oracle Directory Integration Server は、その構成設定に統合プロファイルが追加されるまで待機します。この待機は、構成設定に指定されている統合プロファイルが使用禁止になっている場合にも発生します。

コマンドラインで指定した構成設定がディレクトリ内に存在しない場合、Oracle Directory Integration Server は、この情報をログ・ファイルに記録して終了します。プロビジョニング・プロファイルの場合、コマンドラインで引数として渡される `grpID` 属性に関して同じ動作になります。

コネクタによる同期またはプロビジョニングがスケジューリングされている場合、常に、Oracle Directory Integration Server は別のスレッドを起動します。このスレッドは、Oracle Internet Directory からのエントリの読取りまたは書込みを実行するため、ディレクトリ・サーバーへの LDAP 接続をオープンし、終了前にこの接続をクローズします。

Oracle Directory Integration Platform は、表 4-1 に示す 3 種類のスレッドをプロセス内で実行します。

表 4-1 Oracle Directory Integration Platform のスレッド

スレッド	説明
メイン・スレッド	Oracle Directory Integration Server のデーモン・スレッド。このスレッドは、起動したスケジューラに更新シグナルを定期的に送信し、変更されたプロファイルを検索してスケジューラのキャッシュを更新します。このスレッドは、OID モニター（oidmon）による停止シグナルも検索します。この停止シグナルによって、スケジューラに停止シグナルを送信した後、スレッド自体が停止します。
スケジューラ・スレッド	指定されたスケジューリング間隔に基づいた同期用のコネクタのスケジューラ。このスレッドは、メイン・スレッドからシグナルを受信すると、同期プロファイルを最新の値に更新します。
コネクタ・スレッド	同期化において、プロファイル内で名前が付けられたコネクタ実行可能ファイルを起動し、属性をマッピングおよびフィルタ処理するスレッド。指定された個々のスケジューリング間隔でスケジューラによって生成されます。ソース・ディレクトリからの変更がすべて宛先ディレクトリに伝播された後、このスレッドは終了します。

Oracle Directory Integration Platform イベントの標準の順序

Oracle Directory Integration Server の各インスタンスによって、プロビジョニングまたは同期がサポートされます。Oracle Directory Integration Server は、同期とプロビジョニングのイベント伝播を処理するときに、共有サーバー・プロセスとして動作します。

表 4-1 で説明した 3 つのスレッドは相互に機能して、次の一般的なプロセス・フローの順序を作成します。

メイン・スレッド・プロセスの順序

起動時に、メイン・スレッドが起動されます。これはサーバーのデーモン・スレッドであり、スケジューラを起動します。ディレクトリ内のインスタンスの登録が検証されます。インスタンスが登録されていない場合、OID モニターからは起動されません。かわりに、構成設定番号とインスタンス番号とともに Oracle Internet Directory に自身を登録します。

メイン・スレッドは更新時期を定期的にチェックし、メイン・スレッドの更新をスケジューラに通知します。また、停止シグナルを定期的にチェックします。停止シグナルを受信すると、スケジューラ・スレッドは停止します。

スケジューラ・スレッドが停止すると、メイン・スレッドは登録を解除し、停止します。

スケジューラ・スレッド・プロセスの順序

スケジューラ・スレッドは、メイン・スレッドによって起動されると、構成設定を読み取り、スケジューリングを行う統合プロファイルを判断します。スケジューリング対象プロファイルのリストを作成し、指定されたスケジューリング間隔に基づいてスケジュールを設定します。プロファイルのリストを作成する間に、スケジューラ・スレッドは属性の妥当性をチェックします。プロファイル属性に無効な値がある場合、そのプロファイルは、同期またはプロビジョニングの対象となりません。

更新シグナルを受信したスケジューラ・スレッドは、統合プロファイルを更新します。スケジューラ・スレッドは停止シグナルを受信すると、すべてのコネクタが同期またはプロビジョニングのイベント伝播を完了するまで待機します。その後、メイン・スレッドに制御を戻します。

同期用のコネクタ・スレッド・プロセスの順序

同期スレッドは次のプロセスに従います。

1. 接続ディレクトリおよび Oracle Internet Directory との接続を確立します。
2. インポート操作では、コネクタに指定されているエージェント実行コマンドを実行します。
3. 必要に応じて、DB/LDAP/LDIF/ タグ付きファイルを開きます。
4. ソースから 1 つずつ変更を読み取ります。
5. 該当する場合、変更をフィルタ処理します。
6. マッピング・ルールの指定に従って変更をマップします。
7. 宛先変更レコードを作成します。
8. 変更を宛先に書き込みます。
9. すべての変更を適用した後、スレッドを閉じます。

プロビジョニング用のコネクタ・スレッド・プロセスの順序

プロビジョニング・スレッドは次のプロセスに従います。

1. 接続ディレクトリとの接続を確立します。
2. ソースから 1 つずつ変更を読み取ります。
3. 該当する場合、変更をフィルタ処理します。
4. 変更を次の特定のイベントとして識別します。
   - USER 追加 / 変更 / 削除
   - GROUP 追加 / 変更 / 削除
5. イベント通知レコードを作成します。
6. イベント通知を消費する所定のパッケージを起動します。

Oracle Internet Directory マルチマスター・レプリケーション環境での Oracle Directory Integration Platform イベント伝播

Oracle Internet Directory マルチマスター・レプリケーション環境では、ある Oracle Internet Directory ノード上のディレクトリ統合プロファイルへの変更は、その他の Oracle Internet Directory ノードでは自動的にレプリケートされません。このため、Oracle Internet Directory マルチマスター・レプリケーション環境で Oracle Directory Integration Platform を実装する場合は、この項で説明されている考慮事項に注意する必要があります。

Oracle Internet Directory マルチマスター・レプリケーション環境でのディレクトリ同期

Oracle Internet Directory プライマリ・ノード上のディレクトリ同期プロファイルは自動的に Oracle Internet Directory のセカンダリ・ノードにレプリケートされないため、プライマリ・ノードのプロファイルをセカンダリ・ノードに対して定期的に手動でコピーする必要があります。これにより、プライマリ・ノード上で問題が発生した場合、ディレクトリ同期プロファイルをセカンダリ・ノードで実行できます。ただし、ディレクトリ同期プロファイルの `lastchangenumber` 属性に指定した値は、プロファイルがある Oracle Internet Directory ノードのローカルな値です。つまり、ディレクトリ同期プロファイルをある Oracle Internet Directory ノードから別のノードにコピーしても、同期またはイベント伝播の正しい状態は維持されません。

注意： ディレクトリ・レプリケーション・サーバー（oidrepld）または Oracle Directory Integration Server（odisrv）（あるいはその両方）を実行するプライマリ・ノードに障害が発生した場合、セカンダリ・ノードの OID モニターが、5 分後にこれらのプロセスをセカンダリ・ノード上で起動します。ただし、プライマリ・ノードが再起動しても、これらのサーバーはプライマリ・ノード上で自動的に再起動されません。

正常な停止はフェイルオーバーとして扱われません。つまり、正常に停止した後、セカンダリ・ノードの OID モニターは、5 分後にこれらのプロセスをセカンダリ・ノード上で起動しません。また、障害が発生した場合と同様に、プライマリ・ノードが再起動しても、これらのサーバーはプライマリ・ノード上で自動的に再起動されません。

あるノードから別のノードにインポート・プロファイルをコピーすると、値が接続ディレクトリから取得されるため、lastchangenumber 属性は不適切なものになります。しかし、エクスポート・プロファイルをターゲット・ノードにコピーした後には、lastchangenumber 属性をターゲット・ノードの値で次のように更新する必要があります。

1. 4-9 ページの「Oracle Directory Integration Platform の停止」で説明されているように、Oracle Directory Integration Server を停止します。
2. 『Oracle Identity Management ユーザー・リファレンス』の Oracle Directory Integration Platform ツールの章の dipassistant showprofile に関する項の説明に従い、ターゲット・ノードで lastchangenumber 属性の値を取得します。
3. 『Oracle Identity Management ユーザー・リファレンス』の Oracle Directory Integration Platform ツールの章の dipassistant reassociate に関する項の説明に従い、ディレクトリ同期プロファイルをプライマリ・ノードからターゲット・ノードにコピーします。
4. Oracle Directory Integration Server 管理ツールまたは Directory Integration アシスタント（dipassistant）を使用して、ターゲット・ノードにコピーしたエクスポート・プロファイルの lastchangenumber 属性を、手順 2 で取得した値で更新します。

   関連資料：

   - 3-2 ページの「Oracle Directory Integration Server 管理ツール」
   - 『Oracle Identity Management ユーザー・リファレンス』

5. 4-8 ページの「Oracle Directory Integration Platform の起動」で説明されているように、Oracle Directory Integration Server を起動します。

Oracle Internet Directory マルチマスター・レプリケーション環境でのディレクトリ・プロビジョニング

デフォルトの Oracle Internet Directory マルチマスター・レプリケーション環境では、Oracle Directory Integration Platform はプライマリ Oracle Internet Directory と同じ場所にインストールされます。プライマリ・ノードに障害が発生した場合、そのノードにあるすべてのプロファイルに対するイベント伝播は停止します。イベントはキューに入れられ、プライマリ・ノードの停止中にも失われませんが、どのアプリケーションにも伝播されません。プライマリ・ノードが停止したときにも、イベントが引き続き伝播されることを保証するには、Oracle Internet Directory マルチマスター環境で、ディレクトリ・プロビジョニング・プロファイルを他のセカンダリ・ノードにコピーする必要があります。しかし、ディレクトリ・プロビジョニング・プロファイルは、アプリケーションがインストールされた直後、Oracle Internet Directory でユーザー変更が行われる前にしか、プライマリ・ノードからセカンダリ・ノードに対してコピーされません。

ディレクトリ・プロビジョニング・プロファイルをプライマリ・ノードからセカンダリ・ノードにコピーするには、『Oracle Identity Management ユーザー・リファレンス』の Oracle Directory Integration Platform ツールの章の dipassistant reassociate コマンドに関する項の説明に従ってください。

Oracle Directory Integration Platform の情報の表示

Oracle Directory Integration Server は、起動時に固有の実行時情報を生成し、ディレクトリ内に格納します。これには次の情報が含まれます。

- Oracle Directory Integration Server のインスタンス番号
- 実行されているホスト
- Oracle Directory Integration Server の起動に使用された構成設定
- 実行中のプロビジョニング・プロファイル・グループのグループ識別子

この情報は、Oracle Directory Integration Server 管理ツールまたは `ldapsearch` ユーティリティを、次の項目で説明されているように使用すると表示できます。

- Oracle Directory Integration Server 管理ツールを使用した Oracle Directory Integration Platform の実行時情報の表示
- ldapsearch ユーティリティを使用した Oracle Directory Integration Platform の実行時情報の表示

Oracle Directory Integration Server 管理ツールを使用した Oracle Directory Integration Platform の実行時情報の表示

Oracle Directory Integration Server 管理ツールを使用して Oracle Directory Integration Server インスタンスの実行時情報を表示するには、次のようにします。

1. ナビゲータ・ペインで、「***directory server instance***」を展開します。
2. 「**統合プロファイルの構成**」を選択します。右側のペインに「アクティブ・プロセス」ボックスが現れ、Oracle Directory Integration Platform の実行時情報が表示されます。

ldapsearch ユーティリティを使用した Oracle Directory Integration Platform の実行時情報の表示

`ldapsearch` ユーティリティを使用して Oracle Directory Integration Server インスタンスの登録情報を表示するには、エントリでベース検索を実行します。たとえば、次のようになります。

```
ldapsearch -p 3060 -h my_host -D "mybinddn" -w mypassword -b
cn=instance1,cn=odisrv,cn=subregistrysubentry -s base -v "objectclass=*"
```

この例の検索では、次の情報が返されます。

```
dn: cn=instance1,cn=odisrv,cn= subregistrysubentry
cn: instance1
orclodipconfigdns: orclodipagentname=HRAgent,cn=subscriber profile,cn=changelog
subscriber,cn=oracle internet directory
orcldiaconfigrefreshflag: 0
orclhostname: my_host
orclconfigsetnumber: 1
objectclass: top
objectclass: orclODISInstance
```

Oracle Directory Integration Platform が使用する構成設定エントリの管理

構成設定エントリを作成、変更および表示するには、Oracle Directory Integration Server 管理ツールまたは Directory Integration アシスタント（`dipassistant`）を使用します。コネクタが登録されると、統合プロファイルが作成され、所定の構成設定に追加されます。この構成設定エントリは、Oracle Directory Integration Server の動作を決定します。

Oracle Directory Integration Server の起動時に異なる構成設定エントリを使用することによって、Oracle Directory Integration Server の実行時動作を制御できます。たとえば、ホスト H1 の Oracle Directory Integration Server のインスタンス 1 を configset1 で起動し、ホスト H1 のインスタンス 2 を configset2 で起動することができます。インスタンス 1 の動作は configset1 に依存し、インスタンス 2 の動作は configset2 に依存します。ホスト H1 上のエージェントを 2 つの構成設定エントリに分割すると、2 つの Oracle Directory Integration Server インスタンスに負荷が分散されます。同様に、異なるホスト上で異なる構成設定とインスタンスを実行すると、サーバー間で負荷のバランスをとることができます。

Oracle Internet Directory と接続ディレクトリの SSL 証明書の管理

Oracle Directory Integration Server では、SSL を使用して、Oracle Internet Directory と接続ディレクトリに接続できます。Oracle Internet Directory への接続に認証なしの SSL を使用する場合、証明書は不要です。ただし、サーバー認証のある SSL を使用して Oracle Internet Directory に接続する場合は、LDAP サーバーに接続するためのトラスト・ポイント証明書が必要です。Oracle Directory Integration Server では、証明書はウォレット内にあるものと想定します。ウォレットとは、個々のエンティティのセキュリティ資格証明を格納および管理するために使用されるデータ構造です。Oracle Wallet Manager は、ウォレット所有者およびセキュリティ管理者が、各自のウォレット内でセキュリティ資格証明を管理および編集するために使用するアプリケーションです。

> **関連資料：**『Oracle Advanced Security 管理者ガイド』の Oracle Wallet Manager に関する章

ウォレットの場所およびウォレットを開くためのパスワードは、Oracle Directory Integration Platform が使用するプロパティ・ファイルに保存されています。このファイルは、$*ORACLE_HOME*/ldap/odi/conf/odi.properties です。

典型的な odi.properties ファイルには、表 4-2 に示すエントリがあります。odi.properties ファイルは、自分の配置に適した値で更新する必要があります。

表 4-2 odi.properties ファイルのエントリ

エントリ	説明
`RegWalletFile: odi/conf/srvWallet`	Oracle Internet Directory を使用して Oracle Directory Integration Platform の登録情報の場所を示します。ファイルの場所は、$*ORACLE_HOME*/ldap ディレクトリに対して示されます。
`CertWalletFile:` *`location_of_certificate_wallet`*	証明書ウォレットの場所を示します。証明書ウォレット・ファイルは、ewallet.p12 ファイルの場所です。

表 4-2 odi.properties ファイルのエントリ（続き）

エントリ	説明
`CertWalletPwdFile:` *`location_of_certificate_wallet_password_file`*	暗号化されたウォレット・パスワードを含むファイルの場所を示します。このパスワードは、Directory Integration アシスタント（`dipassistant`）を使用して更新する必要があります。 **関連資料：** 『Oracle Internet Directory 管理者ガイド』の SSL およびディレクトリに関する章 『Oracle Identity Management ユーザー・リファレンス』

たとえば、odi.properties ファイルの内容は次のようになります。

```
RegWalletFile:  /private/myhost/orahome/ldap/odi/conf
CertWalletFile:  /private/myhost/orahome/ldap/dipwallet
CertWalletPwdFile: /private/myhost/orahome/ldap/
```

この例では、ファイルの場所は絶対パス名です。この例では、ウォレット・ファイル ewallet.p12 は、/private/myhost/orahome/ldap/dipwallet ディレクトリにあります。

Oracle Directory Integration Platform の起動、停止および再起動

この項では、Oracle Directory Integration Platform の起動、停止および再起動について説明します。内容は次のとおりです。

- Oracle Directory Integration Platform の起動
- Oracle Directory Integration Platform の停止
- Oracle Directory Integration Platform の再起動

> **注意：** Oracle Directory Integration Server をデフォルト・モードで起動すると、Oracle Directory Integration Platform Service のみがサポートされ、Oracle Directory Synchronization Service はサポートされません。

Oracle Directory Integration Platform の起動

Oracle Directory Integration Platform は、Oracle Internet Directory のコンポーネントとして、またはスタンドアロンとしてインストールできます。Oracle Directory Integration Server の起動方法は、Oracle Directory Integration Platform を Oracle Internet Directory のコンポーネントとしてインストールするか、またはスタンドアロンとしてインストールするかによって異なります。

Oracle Directory Integration Platform を Oracle Internet Directory のコンポーネントとして起動するには、Oracle Internet Directory モニター（`oidmon`）および Oracle Internet Directory 制御ユーティリティ（`oidctl`）を使用します。これらのユーティリティは、Oracle Process Manager and Notification Server 制御ユーティリティ（`opmnctl`）を使用して 2 つ同時に起動できます。Oracle Directory Integration Platform を Oracle Internet Directory のコンポーネントとしてインストールする場合、Oracle Directory Integration Server のインスタンスは、プロビジョニングのリクエストを処理する場合にのみ起動されます。同期を実行する追加の Oracle Directory Integration Server インスタンスを起動するには、Oracle Internet Directory 制御ユーティリティ（`oidctl`）を使用する必要があります。`oidmon`、`oidctl` および `opmnctl` ユーティリティの詳細は、『Oracle Identity Management ユーザー・リファレンス』の Oracle Identity Management サーバー管理ツールに関する章を参照してください。

Oracle Directory Integration Platform のスタンドアロン・インストールを起動するには、Oracle Directory Integration Server 制御ツール（`odisrv`）を使用します。このツールの詳細

は、『Oracle Identity Management ユーザー・リファレンス』の Oracle Identity Management サーバー管理ツールに関する章を参照してください。Oracle Directory Integration Platform のスタンドアロン・インストールでは、同じ Oracle Application Server Infrastructure 内で稼働する Oracle Directory Integration Server インスタンスが他に存在しない場合、デフォルトで Oracle Directory Integration Server インスタンスが起動します。

注意：30 秒以内にサーバーの停止と起動を手動で行うと、新しいインスタンスの起動前に古いサーバー・インスタンスが停止しない可能性があります。これは、Oracle Directory Integration Server が、`cn=odisrv,cn=subregistrysubentry` に格納された登録エントリを 30 秒ごとにポーリングして停止するかどうかを判断しているためです。このため、サーバーを再起動する前には、必ず 30 秒間待機してください。

Oracle Directory Integration Platform の停止

Oracle Directory Integration Server の停止方法は、起動に使用したユーティリティによって異なります。`oidctl` または `opmnctl` ユーティリティのいずれかを使用してサーバーを起動した場合、`oidctl` ユーティリティを使用して停止する必要があります。`odisrv` ユーティリティを使用してサーバーを起動した場合、`stopodiserver.sh` コマンドで停止する必要があります。`opmnctl` コマンドを使用すると、特定のノード上で稼働している Oracle Internet Directory インスタンス（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、Oracle Directory Integration Server など）をすべて停止することもできます。`oidctl`、`opmnctl`、`odisrv` および `stopodiserver.sh` ユーティリティの詳細は、『Oracle Identity Management ユーザー・リファレンス』の Oracle Identity Management サーバー管理ツールに関する章を参照してください。

Oracle Directory Integration Platform の再起動

Oracle Directory Integration Server を再起動するには、まず 4-9 ページの「Oracle Directory Integration Platform の停止」の手順に従ってサーバーを停止し、30 秒間待機してから、4-8 ページの「Oracle Directory Integration Platform の起動」の手順に従ってサーバーを再起動します。30 秒間待機する理由は、Oracle Directory Integration Server が、`cn=odisrv,cn=subregistrysubentry` に格納された登録エントリを 30 秒間隔でポーリングして停止するかどうかを判断しているためです。次のポーリング間隔の前にサーバーを起動すると、サーバーの最初のインスタンスが停止されず、2 つのインスタンスが稼働することになります。

高可用性を目的とした場合の Oracle Directory Integration Platform の起動と停止

Oracle Directory Integration Platform は、一定の制限付きで、高可用性を目的とした様々な場合に実行できます。この項では、Oracle Real Application Clusters 環境および Oracle Application Server Cold Failover Cluster（Infrastructure）で運用する Oracle Directory Integration Server について説明します。内容は次のとおりです。

- Oracle Real Application Clusters 環境での Oracle Directory Integration Platform
- Oracle Application Server Cold Failover Cluster（Infrastructure）での Oracle Directory Integration Platform

どちらのタイプの高可用性環境でも、Oracle Directory Integration Platform を構成するための共通の使用例が 2 つあります。これには、次のようなものがあります。

- 同じ場所 : Oracle Directory Integration Server は、Oracle Internet Directory と同じノード上のクラスタ内に配置されます。
- クラスタ外 : Oracle Directory Integration Server は、クラスタ外の独立したノードにインストールされます。

Oracle Real Application Clusters 環境での Oracle Directory Integration Platform

Oracle Internet Directory インフラストラクチャは、Oracle Real Application Clusters（Oracle RAC）モードで動作するように構成されます。Oracle RAC では、Oracle Directory Integration Server は、すべてのディレクトリ・ノードに対して実行できます。

個々の構成設定は、Oracle Directory Integration Server の 1 つのインスタンスのみによって実行されます。このため、デフォルトのインストール中は、1 つのサーバー・インスタンス（つまりインスタンス 1）のみが、Oracle RAC のマスター・ノードで起動されます。このサーバー・インスタンスは、構成設定 0 を実行します。そのサーバー・インスタンスはマスター・ノード上でのみ起動されますが、そのサーバーはすべてのノード上に登録されます。

マスター・ノードで障害が発生した場合は、セカンダリ・ノードの OID モニターによって、Oracle Directory Integration Server インスタンスが起動されます。複数のセカンダリ・ノードが存在する場合は、1 番目の OID モニターによってサーバーが起動され、マスター・ノードに障害が発生したことが認識されます。

サーバーの起動時、OID モニターは、マスター・ノードで使用されていたものと同じインスタンス番号および構成設定を使用します。これは、エンド・ユーザーに対して透過的に行われ、マスター・ノードと同じインスタンス番号および構成設定が使用されると、セカンダリ・ノードの Oracle Directory Integration Server がプライマリ・サーバーとして動作します。サーバーは、セカンダリ・ノードが使用可能であるかぎり、セカンダリ・ノード上での実行を継続します。

2 つのノードで実行されている別々の Oracle Directory Integration Server インスタンスは、同じ構成設定を同時に実行することはできません。OID モニターはこれをチェックしませんが、Oracle Directory Integration Server 自体が起動に失敗します。

OID 制御ユーティリティを使用すると、いつでも Oracle Directory Integration Server を停止できます。ただし、停止すると、他のノードでそのサーバーを自動的に起動することはできません。別のノードでサーバーを起動するには、OID 制御ユーティリティを使用して手動で起動してください。

`opmnctl stopall` コマンドを実行した後、`opmnctl startall` コマンドを実行すると、Oracle Directory Integration Server が起動します。

つまり、OID 制御コマンドによって Oracle Directory Integration Server を停止しないかぎり、OID モニターによって必ずサーバーが実行されていることになります。

同じ場所に配置する構成

同じ場所に配置する構成では、クラスタ内の任意のノードから Oracle Directory Integration Platform を起動できます。あるノードで Oracle Directory Integration Server を起動したら、別のノードで起動する必要はありません。Oracle Directory Integration Server ノードに障害が発生すると、OracleAS クラスタ（Identity Management）の別のノードによって障害が検出され、Oracle Directory Integration Server が起動されます。Oracle Directory Integration Platform を登録するために別の OID 制御コマンドを使用する必要はありません。

ほとんどの場合、Oracle Directory Integration Platform server は、Oracle ディレクトリ・サーバーの単一のデフォルト・インスタンスとのみ通信します。ただし、手動で Oracle Directory Integration Server を構成し、Oracle ディレクトリ・サーバーの 2 番目のインスタンスと通信することも可能です。Oracle ディレクトリ・サーバーの 2 番目のインスタンスが他のノードに構成されていない場合、フェイルオーバー時には、残りの稼働ノードが Oracle Directory Integration Platform と Oracle ディレクトリ・サーバーの 2 番目のインスタンスの両方を起動します。

同じ場所に配置する構成では、ノード障害は次のように処理されます。残りの稼働ノード上にある OID モニターは、10 秒ごとに他のすべてのノードをポーリングし続けます。あるノードによって別のノードからの応答がないことが検出されると、稼働ノードの OID モニターは、Oracle Directory Integration Server と（デフォルト・ノードに存在しない場合、必要に応じて）LDAP サーバーを起動します。

クラスタ外構成

クラスタ外構成では、Oracle Directory Integration Server ノードには、フェイルオーバー機能がありません。この構成の場合、複数の Oracle Internet Directory ノードの前面にあるロード・バランサまたは仮想サーバーを使用して、Oracle Internet Directory LDAP サーバーに接続するよう Oracle Directory Integration Platform を構成できます。

Oracle Application Server Cold Failover Cluster（Infrastructure）での Oracle Directory Integration Platform

この構成では、仮想ホスト名で Oracle Directory Integration Server を起動します。これは、インストール時のデフォルト構成です。

アクティブ・ノードに障害が発生した場合は、スタンバイ・ノードの OID モニターが、スタンバイ・ノードの Oracle Directory Integration Server インスタンスを起動します。この場合、以前アクティブ・ノードで使用されていたものと同じインスタンス番号および構成設定がスタンバイ・ノードで使用されます。これは、エンド・ユーザーに対して透過的です。アクティブ・ノードが使用可能であるかぎり、アクティブ・ノード上で実行を継続します。Oracle Application Server Cold Failover Cluster（Infrastructure）では、仮想ホスト名がアクティブ・ノードとスタンバイ・ノードの両方で同一であるため、サーバーは一度に両方に登録されます。

OID 制御ユーティリティを使用すると、いつでも Oracle Directory Integration Server を停止できます。ただし、停止すると、このノードでそのサーバーを再度起動することはできません。さらに、このノードがフェイルオーバーされると、スタンバイ・ノードの OID モニターは、Oracle Directory Integration Server を起動しません。サーバーを起動するには、OID 制御ユーティリティを使用する必要があります。

`opmnctl stopall` コマンドを実行した後、`opmnctl startall` を実行すると、Oracle Directory Integration Server が起動します。

つまり、OID 制御コマンドによって Oracle Directory Integration Server を停止しないかぎり、OID モニターによって必ずサーバーが実行されていることになります。

> **関連資料：**『Oracle Application Server 高可用性ガイド』の Oracle Application Server Cold Failover Cluster（Infrastructure）に関する章

同じ場所に配置する構成

同じ場所に配置する構成では、次のコマンドを使用して Oracle Directory Integration Platform server を起動します。

```
oidctl connect=connStr host=virtualHost server=odisrv instance=1 \
      flags="host=virtualHost port=OIDPORT" start
```

クラスタ外構成

クラスタ外構成では、次のコマンドを使用して Oracle Directory Integration Platform server を起動します。

```
oidctl connect=connStr server=odisrv instance=1 \
      flags="host=OIDvirtualHost port=OIDPORT" start
```

注意： 同じ場所に配置する構成とクラスタ外構成のコマンドラインの例には、2 つの `host` パラメータがあります。

- flags 以外の `host` パラメータでは、OID 制御ユーティリティが稼働しており、OID モニターにリクエストを送信するノードを指定します。
- flags 内の `host` パラメータでは、Oracle Directory Integration Platform およびレプリケーション・サーバーの接続先となる LDAP サーバーを指定します。このパラメータは、これらのサーバーに対してのみ有効です。

Oracle Directory Integration Platform に対するデバッグ・レベルの設定

デバッグ・レベルを設定するには、プロファイルの orclodipdebuglevel 属性の値を指定します。orclodipdebuglevel 属性に指定する値により、Oracle Directory Integration Server と各コネクタのトレース・ロギング・レベルを個別に制御できます。

サーバーの実行に関しては、トレースは $*ORACLE_HOME*/ldap/log/odisrv_*nn*.log ファイルに保存されます（nn は、起動されたインスタンスの番号です）。コネクタに関しては、トレースは *$ORACLE_HOME*/ldap/odi/log/*profile_name*.trc に保存されます。

> **関連項目：** ファイルのトレースと記録の方法の詳細は、付録 C「Oracle Directory Integration Platform のトラブルシューティング」を参照してください。

表 4-3 に、orclodipdebuglevel 属性に指定できるサーバー・デバッグ・レベルを示します。0（ゼロ）以外のデバッグ・レベルを指定すると、サーバー・ログ・ファイル内の各トレース文に次の種類のトレース文が含まれます。

- Main: コントローラ・スレッドからのメッセージ
- Scheduler: スケジューラ・スレッドからのメッセージ

表 4-3 サーバー・デバッグ・レベル

デバッグ・イベント・タイプ	数値
スレッドの起動と停止	1
プロファイルの更新	2
コネクタの初期化、実行および終了の詳細	4
コネクタ実行時の詳細	8
コネクタの変更レコード	16
コネクタのマッピングの詳細	32
コネクタの実行時間の詳細	64

> **関連項目：** スレッドを選択的にデバッグする方法は、第 7 章「ディレクトリ同期の管理」を参照してください。

デバッグ・フラグに値が設定されていない場合のデフォルト・レベルは 0（ゼロ）で、4-12 ページの表 4-3 のいずれのデバッグ・イベントも記録されません。ただし、エラーと例外は常に記録されます。

各コネクタのデバッグ・レベルは、プロファイル自体に設定できます。表 4-4 に、orclodipdebuglevel 属性に指定できるコネクタ・デバッグ・レベルを示します。

表 4-4 コネクタ・デバッグ・レベル

デバッグ・イベント・タイプ	数値
初期化と終了	1
接続内での検索	2
検索後のエントリの処理	4
変更レコードの作成	8
変更レコードの詳細の処理	16
詳細のマッピング	32

関連資料： 同期プロファイルのデバッグ属性の詳細は、『Oracle Identity Management ユーザー・リファレンス』の Oracle Directory Integration Platform ツールの章の `oidprovtool` に関する項を参照してください。

レプリケート環境での Oracle Directory Integration Platform の管理

プロビジョニングおよび同期化では、レプリケート・ディレクトリはマスター・ディレクトリと異なります。元のディレクトリで作成されたプロファイルを新しいディレクトリで再作成し、すべての構成を元のディレクトリと同様に実行する必要があります。

ログ・ファイルの検索

実行の詳細とデバッグ情報は、$*ORACLE_HOME*/ldap/log/odisrv*Instance_number*.log ディレクトリのログ・ファイルにあります。

たとえば、サーバーがサーバー・インスタンス番号 3 として起動された場合、ログ・ファイルのパス名は $*ORACLE_HOME*/ldap/log/odisrv03.log になります。

サーバー内のその他の例外は odisrv_jvm_*nnnn*.log ファイルにあります。*nnnn* は、その表で Oracle Directory Integration Server を実行中のプロセスの識別子です。

プロファイル固有のデバッグ・イベントはすべて、$*ORACLE_HOME*/ldap/odi/log/*profile_name*.trc にあるプロファイル固有のトレース・ファイルに格納されます。

Oracle Directory Integration Platform の手動登録

Oracle Directory Integration Platform のインストール時に、Oracle Directory Integration Server は Oracle Internet Directory に登録されます。この登録により、指定されたホストが Oracle Directory Integration Platform の実行権限を持つことを示すフットプリントが、ディレクトリ内に作成されます。

クライアント側でこれを手動で登録する必要がある場合があります。たとえば、インストール中に障害が発生した場合などです。これは、Oracle Directory Integration Server 登録ツール（`odisrvreg`）または Oracle Enterprise Manager 10*g* Application Server Control コンソールのいずれかを使用して実行できます。

各ホストにインストールされている各 Oracle Directory Integration Server は、そのホストで `odisrvreg` を実行して個別に登録する必要があります。このツールを実行するには、ディレクトリ・サーバーを管理する権限が必要になります。

関連資料：

- `oidsrvreg` の使用方法の詳細は、『Oracle Identity Management ユーザー・リファレンス』の Oracle Directory Integration Platform ツールの章の `oidsrvreg` に関する項を参照してください。
- C-24 ページの「同期に関するトラブルシューティング」

Oracle Enterprise Manager 10*g* Application Server Control コンソールの使用による Oracle Directory Integration Server の手動登録

Oracle Enterprise Manager 10*g* Application Server Control コンソールを使用して、Oracle Identity Management インフラストラクチャで Oracle Directory Integration Platform を構成できます。この場合、Application Server Control コンソールによって Oracle Directory Integration Server がこのインフラストラクチャに登録されます。

1. Application Server Control コンソールのメイン・ページの「**スタンドアロン・インスタンス**」セクションで、管理する Oracle Application Server インスタンスの名前を選択します。選択したインスタンスについて、Oracle Application Server ホームページが開きます。
2. 「システム・コンポーネント」表のすぐ上にある「**コンポーネントの構成**」をクリックします。「コンポーネントの選択」ページが表示されます。

   注意 :「**コンポーネントの構成**」ボタンは、Oracle Application Server コンポーネントをインストールし、まだ構成していない場合にのみ使用可能です。

3. 「**Oracle Directory Integration Platform**」を選択し、「**続行**」を選択します。「ログイン」画面が表示されます。
4. ディレクトリのスーパー・ユーザーのユーザー名とパスワードを入力します。デフォルトのユーザー名は `cn=orcladmin` です。
5. 「**終了**」をクリックし、登録を完了します。

第 III 部

Oracle Directory Integration Platform との同期

第 III 部では、Oracle Directory Integration Platform とその他の ID 管理システム間の同期に関する概念とコンポーネントについて説明します。また、同期の配置方法を決定する際に考慮する必要のある事項についても説明します。

5

Oracle Directory Synchronization Service

この章では、Oracle Internet Directory と接続ディレクトリをリンクする同期プロファイルとコネクタについて説明します。内容は次のとおりです。

- Oracle ディレクトリの同期に必要なコンポーネント
- 同期の機能

> **関連項目：** Oracle Directory Integration Platform の概念の説明は、第 1 章「Oracle Identity Management 統合の概要」を参照してください。

Oracle ディレクトリの同期に必要なコンポーネント

この項では、Oracle ディレクトリの同期に必要なコンポーネントについて説明します。内容は次のとおりです。

ディレクトリ同期用のコネクタ

Oracle Internet Directory と接続ディレクトリを同期化するため、Oracle Directory Integration Platform はコネクタと呼ばれるあらかじめパッケージされた接続ソリューションを使用します。このコネクタは最小でも、同期に必要な全設定情報を含む 1 つの**ディレクトリ統合プロファイル**で構成されます。

コネクタとサポート対象インタフェースの使用

Oracle Internet Directory と接続ディレクトリを同期化するとき、Oracle Directory Integration Platform は、DB、LDAP、タグ付きまたは LDIF のいずれかのインタフェースを使用します。接続ディレクトリがこれらのインタフェースの 1 つを使用するときにコネクタに必要なものは、同期させるためのディレクトリ統合プロファイルのみです。たとえば、Oracle Internet Directory とともに提供される Sun Java System Directory コネクタは、LDAP インタフェースを使用して、Sun Java System Directory から変更を読み取ります。変更は Sun Java System Directory に固有な形式をとるため、Sun Java System Directory 内で `ldapsearch` を実行することで判別できます。

サポート対象インタフェースなしのコネクタの使用

接続ディレクトリで Oracle Directory Integration Platform によってサポートされているインタフェースの 1 つを使用できない場合は、ディレクトリ統合プロファイルに加えてエージェントが必要です。エージェントは、Oracle Directory Integration Platform がサポートする書式の 1 つから、接続ディレクトリがサポートする書式に、データを変換します。一例が、Oracle Human Resources コネクタです。このコネクタには、あらかじめパッケージされた統合プロファイルと Oracle Human Resources エージェントの両方があります。エージェントは、Oracle Internet Directory との通信に、Oracle Directory Integration Platform がサポートしているタグ付きファイル形式を使用します。Oracle Human Resources システムとの通信には、（OCI インタフェース経由で）SQL を使用します。

ディレクトリ同期プロファイル

ディレクトリ同期プロファイルと呼ばれる同期用のディレクトリ統合プロファイルには、次のような同期化に必要な設定情報がすべて含まれます。

- 同期の方向

  一部の接続ディレクトリは、Oracle Internet Directory からのデータの受信のみを行います。つまり、エクスポート操作のみに関与します。その他の接続ディレクトリは、Oracle Internet Directory にデータを供給するのみです。つまり、インポート操作のみに関与します。インポート操作とエクスポート操作の両方に関与する接続ディレクトリもあります。

  プロファイルは、方向ごとに（つまり、接続ディレクトリから Oracle Internet Directory への情報用に 1 つ、Oracle Internet Directory から接続ディレクトリへの情報用に 1 つ）個別に使用されます。

- インタフェースのタイプ

  一部の接続ディレクトリは、Oracle Directory Integration Platform に組み込まれているインタフェースのいずれかでデータを受け取ることができます。LDAP、タグ付き、DB（読取り専用）、LDIF などのインタフェースがあります。これらの接続ディレクトリについては、プロファイルに格納されている情報を使用して Oracle Directory Synchronization Service が同期そのものを直接実行します。

- マッピング・ルールとその形式

  ディレクトリ同期環境では、あるドメインの典型的なエントリ・セットを別のドメインに移動できます。同様に、ある属性のセットを別の属性のセットにマップすることができます。

  マッピング・ルールは、接続ディレクトリと Oracle Internet Directory 間の属性の変換を制御します。各コネクタでは、その同期プロファイルの `orclodipAttributeMappingRules` 属性に一連のマッピング・ルールが格納されています。Oracle Directory Integration Server はこれらのルールを使用し、ディレクトリからエクスポートする場合、および接続ディレクトリまたはファイルからインポートしたデータを変換する場合に、必要に応じて属性をマップします。Oracle Directory Integration Server では、変更を Oracle Internet Directory にインポートする場合、マッピング・ルールに従って接続ディレクトリの変更レコードを LDAP 変更レコードに変換します。同様に、エクスポート時は、コネクタが Oracle Internet Directory での変更内容を接続ディレクトリが理解できる形式に変換します。

- 接続ディレクトリの接続詳細

  この詳細には、ホスト、ポート、接続モード（SSL または非 SSL）など、接続ディレクトリについての情報および接続情報が含まれます。

- その他の情報

  コネクタによる Oracle Internet Directory と接続ディレクトリの同期に必要なほとんどの情報は、同期プロファイルに格納されますが、コネクタによっては、さらに多くの情報が必要な場合があります。これは、操作によっては実行時に追加構成情報が必要となるためです。

  追加のコネクタ構成情報は、どこにでも、またどのような方法でも格納できます。ただし、Oracle Directory Integration Platform では、追加のコネクタ構成情報を同期プロファイルに `orclODIPAgentConfigInfo` と呼ばれる属性として格納できます。使用するかどうかは任意です。コネクタがこのような情報を必要としない場合は、この属性を空白のまま残しておきます。

  この構成情報は、コネクタまたは接続ディレクトリ（あるいはその両方）に関連付けることができます。Oracle Internet Directory および Oracle Directory Integration Server は、この情報を変更しません。コネクタの起動時に、Oracle Directory Integration Server は、この属性の情報を一時ファイルとしてコネクタに提供します。

  > **関連資料：** ディレクトリ統合プロファイル内の属性のリストおよび説明は、『Oracle Identity Management ユーザー・リファレンス』の属性リファレンスに関する章を参照してください。

同期の機能

変更が行われたかどうかによって、次の方向で同期がとられます。

- 接続ディレクトリから Oracle Internet Directory へ
- Oracle Internet Directory から接続ディレクトリへ
- 両方向

データが流れる方向に関係なく、次のことを前提としています。

- 同期時に、一方のディレクトリに対する増分変更が他方のディレクトリに伝播されます。
- 同期の完了後、両方のディレクトリには同じ情報が維持されています。

この項の内容は次のとおりです。

- Oracle Internet Directory から接続ディレクトリへの同期
- 接続ディレクトリから Oracle Internet Directory への同期
- Oracle Internet Directory がサポートしていないインタフェースを持つディレクトリとの同期化

Oracle Internet Directory から接続ディレクトリへの同期

Oracle Internet Directory は、ディレクトリ・オブジェクトへの増分変更が保存される変更ログを保持します。変更ログ番号に基づいて、これらの変更が順に保存されます。

Oracle Internet Directory から接続ディレクトリへの同期は、この変更ログを活用します。したがって、Oracle Directory Integration Server の実行時は、変更ロギングが有効であるデフォルト設定で Oracle Internet Directory を起動する必要があります。変更ロギングが無効のときは、OID 制御ユーティリティ（`oidctl`）の `-l` フラグを使用して有効にできます。詳細は、『Oracle Identity Management ユーザー・リファレンス』を参照してください。

Oracle Directory Synchronization Service は、同期プロファイルを処理するたびに、次のように動作します。

1. すべての変更が適用済である、最新の変更ログ番号を検索します。
2. その番号より新しい各変更ログ・エントリをチェックします。
3. プロファイル内のフィルタリング・ルールを使用して、接続ディレクトリと同期化する変更を選択します。
4. エントリに対してマッピング・ルールを適用し、接続ディレクトリ内で必要な変更を行います。

次に、その接続ディレクトリ内の適切なエントリまたは属性が更新されます。接続ディレクトリで、DB、LDAP、タグ付きまたは LDIF の各形式が直接使用されていない場合は、プロファイルに指定されているエージェントが起動されます。正常に使用された最終ログ番号がプロファイルに保存されます。

Oracle Internet Directory は、すべてのプロファイルが必要な変更ログを使用した後、その変更ログを定期的にパージして、後続の同期の開始位置を示します。

接続ディレクトリから Oracle Internet Directory への同期

接続ディレクトリで、DB、LDAP、タグ付きまたは LDIF の各形式が直接使用されている場合、そのエントリまたは属性への変更は、Oracle Directory Synchronization Service によって自動的に同期化されます。それ以外の場合、コネクタは同期プロファイル内にエージェントを持ち、エージェントが LDIF またはタグ付き形式でファイルへの変更を書き込みます。次に、Oracle Directory Synchronization Service は、この接続ディレクトリ・データのファイルを使用して、Oracle Internet Directory を更新します。

Oracle Internet Directory がサポートしていないインタフェースを持つディレクトリとの同期化

一部の接続ディレクトリは、Oracle Internet Directory でサポートされているどのインタフェースを使用してもデータを受信できません。このタイプのディレクトリに対するプロファイルには、同期用の個別のプログラムを識別する属性が含まれています。これはエージェントと呼ばれます。エージェントは接続ディレクトリの固有な形式と同期データが入っている DB、LDAP、タグ付きまたは LDIF ファイルとの間の変換を行います。プロファイル内で識別されているとおり、エージェントは Oracle Directory Synchronization Service によって起動されます。

Oracle Internet Directory からこのタイプの接続ディレクトリへデータをエクスポートする場合、Oracle Directory Synchronization Service は、必要なファイルをタグ付き形式または LDIF 形式で作成します。次にエージェントは、そのファイルを読み込んで、データを受信する接続ディレクトリに適した形式に変換し、そのディレクトリにデータを格納します。

このタイプの接続ディレクトリから Oracle Internet Directory へデータをインポートする場合、エージェントは必要なファイルをタグ付きまたは LDIF 形式で作成します。次に、Oracle Directory Synchronization Service は、このファイルのデータを使用して、Oracle Internet Directory を更新します。

6

ディレクトリ同期プロファイルの構成

この章では、Oracle Directory Integration Platform へのコネクタの登録方法と、マッピング・ルール属性の書式設定方法について説明します。内容は次のとおりです。

> **関連資料：** 同期プロファイル内の属性のリストおよび説明は、『Oracle Identity Management ユーザー・リファレンス』の属性リファレンスに関する章を参照してください。

Oracle Directory Integration Platform でのコネクタの登録

コネクタは、Oracle Internet Directory に登録してから配置します。この登録には、ディレクトリにエントリとして格納されるディレクトリ同期プロファイルの作成作業が含まれます。

ディレクトリ統合プロファイルを作成するには、次のいずれかのツールを使用します。

- Oracle Directory Integration Server 管理ツール
- Directory Integration アシスタント（`dipassistant`）

関連項目：

- 第 3 章「Oracle Directory Integration Platform 管理ツール」
- 5-2 ページの「ディレクトリ同期プロファイル」

同期プロファイル・エントリの属性は、オブジェクト・クラス `orclodiProfile` に属します。ただし、`orclodiplastappliedchangenumber` 属性のみは `orclchangesubscriber` オブジェクト・クラスに属します。

プラットフォーム関連のクラスと属性には、オブジェクト識別子の接頭辞 `2.16.840.1.113894.7` が割り当てられます。

ディレクトリ内の様々な同期プロファイル・エントリが、コンテナ `cn=subscriber profile,cn=changelog subscriber,cn=oracle internet directory` の下に作成されます。たとえば、`OracleHRAgent` というコネクタは、`orclodipagentname=OracleHRAgent,cn=subscriber profile,cn=changelog subscriber,cn=oracle internet directory` として、ディレクトリに格納されます。

同期プロファイルのサンプル

Oracle Directory Integration Platform をインストールすると、次のものに対するインポートおよびエクスポートの同期プロファイルのサンプルが、自動的に作成されます。

- Microsoft Active Directory 2000/2003
- Microsoft Exchange 2000/2003
- Sun Java System Directory 5.2
  Sun Java System Directory は、以前の Sun ONE Directory Server、iPlanet Directory Server および Netscape Directory Server です。Oracle Internet Directory 10*g*（10.1.4.0.1）は、Netscape Directory Server 4.13 以上のすべてのバージョンとの統合が保証されています。
- Novell eDirectory 8.6.2 および 8.7
- OpenLDAP 2.2
- LDIF ファイル
- タグ付きファイル

サンプル・プロファイルの作成に使用されるプロパティ・ファイルとマッピング・ファイルは、$*ORACLE_HOME*/ldap/odi/samples ディレクトリおよび $*ORACLE_HOME*/ldap/odi/conf ディレクトリにあります。

接続詳細の構成

サード・パーティ・ディレクトリは、Directory Integration アシスタント（dipassistant）で Express 構成オプションを使用して構成できます。この方法を使用すると、接続詳細を入力として指定できます。構成方法として、この方法をお薦めします。

インストール時に用意されたテンプレート・プロパティ・ファイルに基づいて、プロファイルを作成することもできます。これを行う場合、プロファイルの odip.profile.condirurl、odip.profile.condiraccount および odip.profile.condirpassword の各プロパティに接続詳細を指定する必要があります。接続詳細の指定に加えて、サード・パーティ・ディレクトリのユーザー・アカウントに、ユーザーおよびグループ情報の読取りに必要な権限があることを確認する必要もあります。

Microsoft Active Directory では、ユーザー・アカウントに、変更の監視対象となっているフォレストのすべてのドメインに対して、ディレクトリ変更をレプリケートする権限があることを確認する必要もあります。これは、次のいずれかの方法により実行できます。

- このアカウントにドメイン管理許可を付与する。
- このアカウントを Domain Administrators グループのメンバーにする。
- このアカウントに、変更の監視対象であるフォレストのすべてのドメインに対する「ディレクトリの変更の複製」権限を付与する。

この権限を管理者以外のユーザーに付与するには、Microsoft Help and Support（http://support.microsoft.com/）の記事「How to Grant the 'Replicating Directory Changes' Permission for the Microsoft Metadirectory Services ADMA Service Account」の「More Information」の項の指示に従います。

ディレクトリ同期プロファイルの最も重要な部分のいくつかには、表 6-1 に示すプロパティに指定する接続詳細が含まれます。

表 6-1 接続詳細のプロパティ

プロパティ	説明
odip.profile.condirurl	接続ディレクトリの URL ■ LDAP ディレクトリに接続するには、*host*:*port* の形式を使用します。 ■ SSL モードで接続するには、*host*:*port*:1 の形式を使用します。 ■ データベースに接続するには、*host*:*port*:*sid* の形式を使用します。
odip.profile.condiraccount	サード・パーティ・ディレクトリへの接続に使用される識別名またはアカウント名
odip.profile.condirpassword	サード・パーティ・ディレクトリへの接続に使用されるパスワード

注意：

- 指定するアカウント情報には、接続するディレクトリでの十分な権限が必要です。
- LDIF またはタグ付きデータ形式を使用している場合には、アカウント名とパスワードのプロパティは不要です。

追加構成情報

同期プロファイルの「追加構成情報」（orclodipAgentConfigInfo）属性には、コネクタで Oracle Internet Directory と接続ディレクトリの同期化を行うために必要な追加の構成情報が格納されます。必須ではありませんが、次のパラメータを「追加構成情報」属性とともに使用すると、同期の効率を大幅に向上させることができます。

- SearchDeltaSize パラメータ
- SkipErrorToSyncNextChange パラメータ
- UpdateSearchCount

「追加構成情報」属性の変更には、Oracle Directory Integration Server 管理ツールまたは Oracle Directory Manager を使用できません。かわりに、Directory Integration アシスタント（dipassistant）を使用します。

関連資料：

- 『Oracle Identity Management ユーザー・リファレンス』
- Novell eDirectory および OpenLDAP とともに使用できる追加構成情報パラメータについては、22-6 ページの「手順 7: 追加構成情報の属性用の同期パラメータの指定」を参照してください。

SearchDeltaSize パラメータ

SearchDeltaSize パラメータにより、同期サイクルの各反復中に処理される増分変更数が決まります。デフォルトでは、SearchDeltaSize パラメータに 500 の値が割り当てられています。各同期サイクル中に実行される反復の回数は、保留中の変更数によって異なります。たとえば、SearchDeltaSize パラメータに 500 の値が割り当てられていて保留中の変更が 498 ある場合、同期に必要な反復は 1 回です。しかし、保留中の変更が 501 ある場合は、同期に必要な反復は 2 回となります。場合によっては、このパラメータにより大きな値を指定すると、同期の効率が向上します。ただし、指定する値が接続ディレクトリ・サーバーの LDAP 検索制限を超えないようにしてください。制限を超えると、同期中にエラーが発生し、一部の変更が処理されない可能性があります。

注意：SearchDeltaSize パラメータを変更する際、特に 2,000 を超える値を指定する場合は、必ず配置を十分に分析し、テストしてください。

SkipErrorToSyncNextChange パラメータ

SkipErrorToSyncNextChange パラメータにより、同期中に変更を処理するときに Oracle Directory Integration Server でエラーを処理する方法が決まります。デフォルトでは、SkipErrorToSyncNextChange パラメータに false の値が割り当てられ、Oracle Directory Integration Server はエラーが解決されるまで変更の処理を続行します。
SkipErrorToSyncNextChange パラメータに true の値を指定すると、Oracle Directory Integration Server はエラーの原因となる変更をスキップします。失敗はすべて $*ORACLE_HOME*/ldap/odi/log/*profile_name*.aud 監査ログ・ファイルに記録されます。
SkipErrorToSyncNextChange パラメータに true の値を指定しない場合は、失敗がないか監査ログを必ず定期的に調べてください。

関連項目： C-24 ページの「同期に関するトラブルシューティング」

UpdateSearchCount

UpdateSearchCount パラメータは、同期プロセス中に接続ディレクトリで実行する反復の最大回数を指定します。同期プロセスは、指定された回数の検索が実行されると停止し、次にスケジュールされた間隔に再開します。

マッピング・ルールの構成

この項では、マッピング・ルールの構成方法について説明します。内容は次のとおりです。

- 識別名マッピング
- 属性レベル・マッピング
- 新規マッピング・ファイルの作成方法
- サポートされている属性マッピング・ルールと例
- 例 : タグ付きファイル・インタフェース用のマッピング・ファイル
- 例 : LDIF インタフェース用のマッピング・ファイル
- マッピング・ルールの更新

マッピング・ルール属性を使用して、ソースから宛先へエントリを変換する方法を指定します。Oracle Internet Directory は、ソースまたは宛先のいずれかである必要があります。エントリを変換する際のマッピング・ルールには、ドメイン・ルール、属性ルールおよびリコンシリエーション・ルールの 3 種類があります。これらのマッピング・ルールにより、識別名マッピング、属性レベル・マッピングおよびリコンシリエーション・ルールを指定できます。リコンシリエーション・ルールは、Novell eDirectory と OpenLDAP でのみ使用されます。リコンシリエーション・ルールの使用方法の詳細は、第 22 章「Novell eDirectory または OpenLDAP との統合」を参照してください。

マッピング・ルールは固定表形式で編成されます。この形式には慎重に従う必要があります。DomainRules という語のみが指定されている行と、3 つの番号記号（###）のみが指定されている行の間に、マッピング・ルールの各セットが記述されます。各ルール内のフィールドは、コロン（:）で区切られます。

```
DomainRules
srcDomainName1: [dstDomainName1]: [DomainMappingRule1]
srcDomainName2: [dstDomainName2]: [DomainMappingRule2]
AttributeRules
srcAttrName1:[ReqAttrSeq]:[SrcAttrType]:[SrcObjectClass]:[dstAttrName1]:
[DstAttrType]:[DstObjectClass]:[AttrMappingRule1]
srcAttrName1,srcAttrName2:[ReqAttrSeq]:[SrcAttrType]:[SrcObjectClass]:
[dstAttrName2]:[DstAttrType]:[DstObjectClass]:[AttrMappingRule2]
###
```

この例の *srcAttrName1* と *srcAttrName2* を拡張するには、それぞれ改行なしで 1 行に記述する必要があります。

識別名マッピング

この項では、Oracle Internet Directory と接続ディレクトリ間でエントリをマップする方法を指定します。Oracle Internet Directory と別の LDAP ディレクトリ間のマッピングの場合は、6-5 ページの「マッピング・ルールの構成」で説明されているように、複数のマッピング・ルールを作成できます。ドメイン・ルールは、キーワード DomainRules のみが指定されている行の後に指定されます。各ドメイン・ルールは、コロンで区切られたコンポーネントで表現されます。これらのコンポーネントの詳細は表 6-2 を参照してください。

表 6-2 ドメイン・ルールのコンポーネント

コンポーネント名	説明
SrcDomainName	関係のあるドメインまたはコンテナの名前。LDAP および LDIF 以外のソースには、NONLDAP を指定します。
DstDomainName	宛先に関係のあるドメイン名。このコンポーネントは、宛先ディレクトリ内のエントリのコンテナが、ソース・ディレクトリでのコンテナと異なる場合に指定します。 SrcDomainName に割り当てられた値が LDAP または LDIF ドメインの場合、このフィールドも同じ値を継承します。ただし、SrcDomainName に割り当てられた値が LDAP または LDIF ドメイン以外の場合、エントリの作成場所となるコンテナを指定する必要があります。 未指定の場合、このフィールドは有効な状態にある SrcDomainName の値を継承します。LDAP および LDIF 以外の宛先には、NONLDAP を指定します。インポートとエクスポートは、常に Oracle Internet Directory を参照するため、NONLDAP:NONLDAP の組合せは許可されません。
DomainMappingRule	このルールは、ソース・ドメイン名または AttributeRules に指定されている属性（あるいはその両方）から、宛先識別名を構成するために使用されます。このフィールドの形式は、通常、cn=%,l=%,o=oracle,dc=com です。これらの指定は、エントリをディレクトリ内の異なるドメインまたはコンテナに配置するために使用されます。LDAP 以外のソースの場合、このルールにより、ディレクトリにエントリを追加できるようターゲット識別名を構成する方法を指定します。 このフィールドは、Oracle Internet Directory へのインポート、または LDIF ファイルまたは他の外部 LDAP 準拠ディレクトリへのエクスポートの場合にのみ有効です。このコンポーネントは、宛先ディレクトリ内のエントリのいずれかの識別名が、ソース・ディレクトリのエントリの識別名と異なる場合に指定します。 このコンポーネントは、LDAP から LDIF、LDAP から LDAP、または LDIF から LDAP への同期の場合はオプションです。未指定の場合、ソース・ドメイン名と宛先ドメイン名は同じと考えられます。

例 6-1 識別名マッピングの例

```
Distinguished Name Rules
%USERBASE INSOURCE%:%USERBASE ATDEST%:
```

USERBASE は、サード・パーティ・ディレクトリのユーザーおよびグループのマップ元のコンテナを指します。通常、これは、サード・パーティ・ディレクトリ・ドメインのルートの下にある users コンテナです。

例 6-2 1 対 1 識別名マッピングの例

1 対 1 マッピングを行うには、サード・パーティ・ディレクトリの識別名が Oracle Internet Directory の識別名と一致する必要があります。この例では、サード・パーティ・ディレクトリの識別名が Oracle Internet Directory の識別名に一致します。具体的には、次の条件を満たしている必要があります。

- サード・パーティ・ディレクトリのホストは us.mycompany.com ドメインにあり、したがって、サード・パーティ・ディレクトリ・ドメインのルートは us.mycompany.com です。ドメインの下にある user コンテナの DN 値は、cn=users,dc=us,dc=mycompany,dc=com になります。
- Oracle Internet Directory のデフォルトのレルム値は、dc=us,dc=mycompany,dc=com です。このデフォルトのレルムには、DN 値が cn=users,dc=us,dc=mycompany,dc=com の users コンテナが自動的に含まれます。

サード・パーティ・ディレクトリの識別名が Oracle Internet Directory の識別名と一致するため、ディレクトリ間の 1 対 1 識別名マッピングが行われます。

dc=us,dc=mycompany,dc=com の下の cn=users コンテナのみを同期化する場合、ドメイン・マッピング・ルールは次のとおりです。

```
Distinguished Name Rules
cn=users,dc=us,dc=mycompany,dc=com:cn=users,dc=us,dc=mycompany,dc=com
```

このルールでは、cn=users,dc=us,dc=mycompany,dc=com の下のすべてのエントリが同期化されます。ただし、このコンテナの下で同期化されるオブジェクトのタイプは、識別名マッピング・ルールに従う属性レベルのマッピング・ルールによって決まります。

cn=users,dc=us,dc=mycompany,dc=com の下のエントリ cn=groups,dc=us,dc=mycompany,dc=com を同期化する場合、ドメイン・マッピング・ルールは次のとおりです。

```
cn=groups,dc=us,dc=mycompany,dc=com: cn=users,dc=us,dc=mycompany,dc=com
```

関連項目： この章の終わりにあるマッピング・ファイルの例

属性レベル・マッピング

属性ルールは、キーワード AttributeRules のみが指定されている行の後に指定されます。属性ルールにより、エントリのプロパティ値が 2 つの LDAP ディレクトリ間で、どのように関係付けられるかを指定します。たとえば、あるディレクトリのユーザー・オブジェクトの cn 属性は、別のディレクトリの givenname オブジェクトにマップできます。同様に、あるディレクトリのグループ・オブジェクトの cn 属性は、別のディレクトリの displayname 属性にマップできます。各属性ルールは、コロンで区切られたコンポーネントで表現されます。これらのコンポーネントの詳細は表 6-3 を参照してください。属性ルールの指定は、3 つの番号記号（###）のみが指定されている行で終わります。

表 6-3 属性ルールのコンポーネント

コンポーネント名	説明
SrcAttrName	LDAP 準拠ディレクトリのリポジトリの場合、このパラメータは変換する属性の名前を意味します。 Oracle Database のリポジトリの場合、このパラメータは、SrcClassName で指定された表の ColumnName を意味します。 他のリポジトリの場合、このパラメータは適切に解釈されます。
ReqAttrSeq	ソース属性を宛先に渡す必要があるかどうかを示します。エントリを Oracle Internet Directory と接続ディレクトリ間で同期化する場合は、一部の属性を同期キーとして使用する必要があります。このフィールドは、指定した属性がキーとして使用されているかどうかを示します。使用されている場合は、属性の変化には関係なく、その属性の値がソースから抽出されます。 属性を相手側に常に渡す必要がある場合は、このフィールドに 0（ゼロ）以外の整数値を指定します。
SrcAttrType	このパラメータは、整数、文字列、バイナリなど、属性の型を意味し、マッピング・ルールの妥当性をチェックします。

表 6-3 属性ルールのコンポーネント（続き）

コンポーネント名	説明
SrcObjectClass	共有している属性のソースが LDAP 準拠ディレクトリの場合は、このパラメータによって、その属性が所属しているオブジェクト・クラスの名前が指定されます。 共有属性のソースが Oracle Database のリポジトリの場合、このパラメータは表名を意味し、指定は必須です。他のリポジトリの場合、このパラメータは無視されます。
DstAttrName	オプションの属性。未指定の場合は、SrcAttrName が使用されます。 LDAP 準拠ディレクトリの場合、このパラメータは宛先の属性の名前を意味します。 Oracle Database のリポジトリの場合、このパラメータは、SrcClassName で指定された表の ColumnName を意味します。 他のリポジトリの場合、このパラメータは適切に解釈されます。
DstAttrType	このパラメータは、整数、文字列、バイナリなど、属性の型を意味します。ソースおよび宛先の属性型の互換性を保証する責任は管理者にあります。Oracle Directory Integration Platform はこの互換性を保証しません。
DstObjectClass	LDAP 準拠ディレクトリの場合、このパラメータは、属性が所属するオブジェクト・クラスを意味します。このパラメータはオプションです。 Oracle Database のリポジトリの場合、このパラメータは表名を意味し、指定は必須です。 他のリポジトリの場合、このパラメータは無視されます。
AttrMapping Rule	演算子 +、| と、ファンクション toUpper(string)、toLower(String)、trunc(string,char) を使用するオプションの算術式。未指定の場合は、ソース属性値が宛先属性の値としてコピーされます。リテラルは一重引用符（'）または二重引用符（""）で指定できます。

新規に作成した同期プロファイルのマッピング・ルールは空になります。マッピング・ルールを入力するには、適切な形式に厳密に従ったファイルを編集します。

注意： マッピング・ファイルに属性およびオブジェクト・クラスが定義される際、スキーマに定義されているそれぞれの属性およびオブジェクト・クラスはソース・ディレクトリに入っているとみなされます。

同期用に親コンテナが選択されると、マッピング・ルールに一致するすべての子も同様に同期化されます。子コンテナを選択して同期から排除することはできません。

新規マッピング・ファイルの作成方法

新規マッピング・ファイルを作成するには、次のようにします。

1. ソース・ディレクトリ内で同期に関係のあるコンテナを指定します。
2. ソース・コンテナ内のオブジェクトのマッピング先である宛先コンテナを指定します。指定されたコンテナがディレクトリ内に存在することを確認します。
3. 宛先ディレクトリ内に作成されるエントリの識別名作成ルールを決定します。LDAP から LDAP への場合、マッピングは通常 1 対 1 です。LDAP 以外から LDAP への場合は、ドメインの識別名構成ルールが必要です。たとえば、タグ付きファイルまたは Human Resources エージェントからの同期の場合、マッピング・ルールの形式は `uid=%,dc=mycompany,dc=com` になります。その場合、Oracle Human Resources から適用されるすべての変更に `uid` 属性が存在する必要があります。手順 6 で指定するとおり、必須属性として `uid` 属性を指定する必要があります。
4. ディレクトリ間で同期化するオブジェクト（ソースおよび宛先ディレクトリ内の関連オブジェクト・クラス）を指定します。通常、ディレクトリ間で同期化されるオブジェクトには、ユーザー、グループ、組織単位、組織およびその他のリソースがあります。これらのオブジェクトを識別するには、ディレクトリで使用されている実際のオブジェクト・クラスを識別します。
5. ディレクトリ間で同期化する各種オブジェクトのプロパティ（LDAP コンテキストの属性）を指定します。オブジェクトの属性すべてを同期化する必要はありません。同期化対象のユーザー・プロパティは、`cn`、`sn`、`uid` および `mail` です。
6. マッピング・ルールを定義します。各マッピング・ルールの形式は次のとおりです。

   ```
   <srcAttrName>:<ReqdFlag>:<srcAttrType>:<SrcObjectClass>:
   <dstAttrName>:<dstAttrType>:<dstObjectClass>: <Mapping Rule>
   ```

   マッピング・ルールを定義するときは、必ず次のことを確認してください。

   - 必須属性にはそれぞれ順序番号が付いていること。たとえば、手順 3 で `uid` 属性が必須として指定された場合は、`<ReqdFlag>` のかわりに `1` の値を割り当てます。
   - 関連オブジェクト・クラスは、それぞれ宛先ディレクトリ上にスキーマ定義を持つこと。
   - 宛先オブジェクト・クラス内の必須属性は、すべてソースから割り当てられた値を持つこと。様々な LDAP 実装は標準に完全に準拠していないこともありますが、これは標準オブジェクト・クラスにも当てはまります。

   ソース・オブジェクト・クラスに属する属性のすべてを 1 つの宛先オブジェクト・クラスに割り当てる必要はありません。ソース・オブジェクト・クラスの各種の属性は、異なる宛先オブジェクト・クラスに属する様々な属性に割り当てることができます。

   属性がバイナリ値をとる場合は、`<attrtype>` フィールドで `binary` として指定します。

マッピング・ルールには柔軟性があり、1 対多と多対 1 の両方のマッピングを組み込むことができます。

- 1 対多

  接続ディレクトリの 1 つの属性を、Oracle Internet Directory の多数の属性にマップできます。たとえば、接続ディレクトリのある属性が `Address:123 Main Street/MyTown, MyState 12345` であるとします。Oracle Internet Directory のこの属性は、LDAP 属性 `homeAddress` と LDAP 属性 `postalAddress` の両方にマップできます。

- 多対 1

  接続ディレクトリの複数の属性を、Oracle Internet Directory の 1 つの属性にマップできます。たとえば、Oracle Human Resources ディレクトリでは、`firstname=Anne` と `lastname=Smith` の 2 つの属性を使用して Anne Smith を表すとします。これらの 2 つの属性は、Oracle Internet Directory の 1 つの属性 `cn=Anne Smith` にマップできます。ただし、双方向同期では、逆方向のマッピングはできません。たとえば、`cn=Anne Smith` を複数の属性にマップすることはできません。

関連項目： この章の終わりにあるマッピング・ファイルの例

サポートされている属性マッピング・ルールと例

サポートされている属性マッピング・ルールは、次のとおりです。

- 連結演算子（+）: 2 つの文字列属性を連結します。

  次のようなマッピング・ルールについて考えてみます。

  ```
  Firstname,lastname: : : givenname: : inetorgperson: firstname+lastname
  ```

  たとえば、ソースの Firstname が John、LastName が Doe の場合、このルールによって、宛先の givenname 属性は、JohnDoe という値になります。

- OR 演算子（|）: 2 つの文字列属性の値の 1 つを宛先に割り当てます。

  次のようなマッピング・ルールについて考えてみます。

  ```
  Fistname,lastname : : : :givenname: :inetorgperson: firstname | lastname
  ```

  この例では、firstname の値が存在する場合は、それが givenname に割り当てられます。firstname 属性が存在しない場合、lastname の値が givenname に割り当てられます。両方の値が空である場合、値は割り当てられません。

- bin2b64 ( ): ソース・ディレクトリのバイナリ値を Base64 のエンコード値として宛先ディレクトリに保存します。通常、次のように使用します。

  ```
  objectguid: : : :binary: :orclobjectguid: orcladuser:bin2b64(objectguid)
  ```

  (objectguid) の値を検索する必要がある場合、これは必須です。

- tolower(): 文字列属性値を小文字に変換します。

  ```
  firstname: : : :givenname: :inetorgperson: tolower(firstname)
  ```

- toupper(): 文字列属性値を大文字に変換します。

  ```
  firstname: : : :givenname: :inetorgperson: toupper(firstname)
  ```

- trunc(str,char): 指定した char が最初に出現する箇所以降の文字列を切り捨てます。

  ```
  mail : : : : uid : : inetorgperson : trunc(mail,'@')
  ```

  たとえば、ソースの mail が John.Doe@acme.com の場合、このルールによって、宛先の uid 属性は、John.Doe という値になります。

- truncl(str, char): 指定した char が最初に出現する箇所まで、文字列を切り捨てます。

  ```
  mail : : : : uid : : inetorgperson : truncl(mail,'@')
  ```

  たとえば、ソースの mail が John.Doe@acme.com の場合、このルールによって、宛先の uid 属性は、acme.com という値になります。

- trunc(str1, str2): 指定した文字列が最初に出現する箇所以降の文字列を切り捨てます。

  ```
  mail : : : : uid : : inetorgperson : truncl(mail, "@")
  ```

- dnconvert(str): ドメイン・マッピングが使用される場合に、DN タイプ属性を変換します。

  この例は、次のドメイン・マッピング・ルールを前提としています。

  ```
  DomainRules
  cn=srcdomain:cn=dstdomain:
  ```

  たとえば、次のようになります。

  ```
  uniquemember : : : groupofuniquenames : uniquemember : :groupofuniquenames :
  dnconvert(uniquemember)
  ```

この場合、ソースの uniquemember が cn=testuser1,cn=srcdomain の場合、宛先の uniquemember は、cn=test user1,cn=dstdomain になります。

- リテラル:

```
Userpassword: : :person: userpassword: :person: 'welcome1'
```

例 : タグ付きファイル・インタフェース用のマッピング・ファイル

前述の説明に基づいて、ここではタグ付きファイル・インタフェースを使用して、Oracle Human Resources データベース表からユーザー・エントリをインポートするためのマッピング・ファイルの例を示します。ソースは LDAP 以外のディレクトリです。このサンプル・ファイルはインストール時に提供され、$*ORACLE_HOME*/ldap/odi/conf/oraclehragent.map.master にあります。

```
DomainRules
NONLDAP:dc=myCompany,dc=com:uid=%dc=myCompany,dc=com
AttributeRules
firstname: : : :cn: :person
email : : : :cn: :person: trunc(email,'@')
email : 1 : :uid: :person:trunc(email,'@')
firstname,lastname: : : :cn: :person: firstname+","+lastname
lastname,firstname: : : :cn: :person: lastname+","+firstname
firstname,lastname: : : :sn: :person: lastname | firstname
EmployeeNumber: : : :employeenumber: :inetOrgperson
EMail: : : :mail: :inetOrgperson
TelephoneNumber1: : : :telephonenumber: :person
TelephoneNumber2: : : :telephonenumber: :person
TelephoneNumber3: : : :telephonenumber: :person
Address1: : : :postaladdress: :person
state: : : :st: :locality
street1: : : :street: :locality
zip: : : :postalcode: :locality
town_or_city: : : :l: :locality
Title: : : :title: :organizationalperson
#Sex: : : :sex: :person
###
```

前述のように、マッピング・ファイルは、キーワードおよびドメインと属性の一連のマッピング・ルール・エントリで構成されています。この例のマッピング・ファイルには、ドメイン・ルール NONLDAP:dc=myCompany,dc=com:cn=%,dc=myCompany,dc=com が含まれています。

- このルールは、ソース・ドメインが NONLDAP で、ソース・ドメインがないことを示しています。
- 宛先ドメイン（:dc=myCompany,dc=com）は、このプロファイルが処理するすべてのディレクトリ・エントリが、ドメイン dc=myCompany,dc=com にあることを示しています。同期化を開始する前に、ドメインが存在することを確認してください。
- ドメイン・マッピング・ルール（:uid=%,dc=myCompany,dc=com）は、ソースからのデータが、このドメイン・マッピング・ルールで構成した識別名を持つディレクトリ内のエントリを参照することを示しています。この場合の uid は、常に NULL 以外の値を持つ宛先属性の 1 つである必要があります。同期化するエントリに対応するデータが NULL 値の場合、マッピング・エンジンは、そのエントリを無効と判断し、次のエントリに進みます。ディレクトリでエントリを正確に識別するには、uid が単一値であることも必要です。
- タグ付きファイルの場合、ソース・エントリは同期化対象のオブジェクトのタイプを示すオブジェクト・クラスを持ちません。SrcObjectClass フィールドは空白です。
- 宛先が Oracle Internet Directory であるオブジェクトは、それぞれオブジェクト・クラスを持つ必要があります。

- email は、マッピング・ファイル例では必須属性として指定されています。それは、uid 属性が email 属性から導出されているためです。同期化を成功させるには、タグ付きファイルに指定されているすべての変更に、次のとおり email 属性を指定する必要があります。

  ```
  Email : 1 : : :uid : : person : trunc(email,'@')
  ```

- 場合によっては、複数値属性の名前を使用して識別名の RDN を構成する必要があります。たとえば、cn=%,l=%,dc=myCompany,dc=com（cn は複数値属性）の識別名でエントリを構成する場合、DomainMappingRule は、rdn,l=%,dc=myCompany,dc=com（rdn は、NULL 値以外の宛先属性の 1 つ）のような形式になります。これをサポートする典型的なマッピング・ファイルは、次のような形式です。

  ```
  DomainRules
  NONLDAP:dc=us,dc=myCompany,dc=com:rdn,l=%,dc=us,dc=myCompany,dc=com
  AttributeRules
  firstname: : :cn: :person
  email : : : :cn: :person: trunc(email,'@')
  email : 1: : :rdn: :person: 'cn='+trunc(email,'@')
  firstname,lastname: : : :cn: :person: firstname+","+lastname
  lastname,firstname: : : :cn: :person: lastname+","+firstname
  firstname,lastname: : : :sn: :person: lastname | firstname
  EmployeeNumber: : : :employeenumber: :inetOrgperson
  EMail: : : :mail: :inetOrgperson
  TelephoneNumber1: : : :telephonenumber: :person
  TelephoneNumber2: : : :telephonenumber: :person
  TelephoneNumber3: : : :telephonenumber: :person
  Address1: : : :postaladdress: :person
  Address1: : : :postaladdress: :person
  Address1: : : :postaladdress: :person
  state: : : :st: :locality
  street1: : : :street: :locality
  zip: : : :postalcode: :locality
  town_or_city: 2 : : :1: :locality
  Title: : : :title: :organizationalperson
  #Sex: : : :sex: :person
  ###
  ```

例 : LDIF インタフェース用のマッピング・ファイル

Directory Integration アシスタント（dipassistant）を使用したインストールの一部として、一連の統合プロファイルのサンプルが作成されます。プロファイルの作成に使用されるプロパティ・ファイルは、$*ORACLE_HOME*/ldap/odi/samples ディレクトリにあります。

インポート・マッピング・ファイル例

```
DomainRules
dc=mycompany.oid,dc=com:dc=mycompany.iplanet,dc=com
AttributeRules
# Mapping rules to map the domains and containers
o: : :organization: o: :organization
ou: : :organizationalUnit: ou: : organizationalUnit
dc: : :domain:dc: :domain
# Mapping Rules to map users
uid : : :person: uid: :inetOrgperson
sn: : :person:sn: :person
cn: : :person:cn: :person
mail: :inetorgperson: mail: :inetorgperson
employeenumber: :organizationalPerson: employeenumber: :organizationalperson
c: : :country:c: :country
l: : :locality: l: :locality
telephonenumber: :organizationalPerson: telephonenumber: :organizationalperson
userpassword: : :person: userpassword: :person
uid: : :person: orcldefaultProfileGroup: :orclUserV2
```

```
# Mapping Rules to map groups
cn: : :groupofuniquenames:cn: :groupofuniquenames
member: : :groupofuniquenames:member: :orclgroup
uniquemember: : :groupofuniquenames:uniquemember: :orclgroup
owner: : :groupofuniquenames:owner: :orclgroup
# userpassword: :base64:userpassword: :binary:
```

この例では、ソース・ドメインと宛先ドメインの両方が、ドメイン・マッピング・ルール・セクションで指定されています。この例では、ソース・ドメインと宛先ドメインは同じです。ただし、コンテナが宛先ディレクトリにある場合は、異なる宛先ドメインを指定できます。

また、この例では、属性ルールがユーザー属性マッピング・ルールとグループ属性マッピング・ルールの 2 つのセクションに分かれています。マッピング・ルールにオブジェクト・クラスを指定すると、あるオブジェクトの特定の属性を一意にマップできます。

マッピング・ルールの更新

マッピング・ルールは、新規ルールの追加、既存ルールの変更または `orclodipAttributeMappingRules` 属性に指定されているマッピング・ルール・セットからの一部のルールの削除によって、カスタマイズできます。通常、これらの操作を実行するには、マッピング・ルールが指定されているファイルを指定するか、または『Oracle Internet Directory 管理者ガイド』で説明されているように `ldapsearch` コマンドを使用してファイルの属性値を格納します。

マッピング・ルールは、Oracle Directory Integration Server 管理ツールでは編集できません。かわりに、マッピング・ルールをファイルに格納し、そのファイルを属性の値としてディレクトリにアップロードします。マッピング・ファイルをアップロードするには、Directory Integration アシスタント（`dipassistant`）を使用します。作成およびアップロードされたマッピング・ファイルのコピーは、$*ORACLE_HOME*/ldap/odi/conf ディレクトリに保持でき、将来更新した後に再度アップロードできます。

> **関連資料：** Directory Integration アシスタント（`dipassistant`）の使用方法の詳細は、『Oracle Identity Management ユーザー・リファレンス』を参照してください。

エントリのマッピング・ルール・ファイルへの追加

新規エントリをマッピング・ルール・ファイルに追加するには、そのファイルを編集して、レコードをファイルに追加します。これには、次のようにします。

1. Oracle Internet Directory にマップする必要がある接続ディレクトリの属性名とオブジェクト・クラスを識別します。
2. Oracle Internet Directory 内の対応する属性名およびマップ先のオブジェクト・クラスを識別します。
3. 属性値に対して実行する必要がある変換を示すマッピング・ルール要素を生成します。
4. 属性マッピング・ルール・ファイルを同期プロファイルにロードします。

   たとえば、ソース・ディレクトリ内のあるエントリの電子メール属性を宛先の固有識別子にマップする必要がある場合は、次のようになります。

   ```
   Email:  :  : inetorgperson: uid: : person:
   ```

マッピング・ルール・ファイル内のエントリの変更

マッピング・ルール・ファイル内の変更するエントリを特定した後、属性値の変換に必要なマッピング・ルール要素を生成します。

エントリのマッピング・ルール・ファイルからの削除

マッピング・ルール・ファイル内の削除するエントリを特定した後、エントリをファイルから削除するか、エントリの前に番号記号（#）を付けてそのエントリをコメント化することができます。

関連資料：

- Directory Integration アシスタント（dipassistant）の使用方法の詳細は、『Oracle Identity Management ユーザー・リファレンス』の Oracle Directory Integration Platform ツールに関する章を参照してください。
- マッピング・ルール・ファイルの名前については、6-15 ページの「ファイルの場所とネーミング」を参照してください。
- Oracle*MetaLink* Note: 261342.1「Understanding DIP Mapping Files」（Oracle*MetaLink*（http://metalink.oracle.com/）で参照可能）。

一致フィルタの構成

デフォルトで、コネクタにより、同期用に構成されたコンテナ内のすべてのオブジェクトに対する変更が取得されます。しかし、ユーザーおよびグループに対する変更のみなど、特定のタイプの変更のみを同期化する場合があります。マッピング・ルールにより、エントリをあるディレクトリから別のディレクトリに変換する方法を指定できますが、ディレクトリ間で同期化されるオブジェクトをフィルタ処理することもできます。接続ディレクトリからの変更を Oracle Internet Directory にインポートする前に、同期プロファイルで変更を「接続されたディレクトリ一致フィルタ」（orclODIPConDirMatchingFilter）属性を使用してフィルタ処理できます。同様に、Oracle Internet Directory から接続ディレクトリにエクスポートする前に、変更を「OID 一致フィルタ」（orclODIPOIDMatchingFilter）属性を使用してフィルタ処理できます。どちらの属性の場合も、次の項で説明されているように、接続ディレクトリに対して、LDAP 検索により増分変更を取得するか、または変更ログに変更を格納するかのいずれかのフィルタを指定できます。

- LDAP 検索による変更のフィルタ処理
- 変更ログからの変更のフィルタ処理

一致フィルタを更新するには、Oracle Directory Integration Server 管理ツールまたは Directory Integration アシスタント（dipassistant）を使用します。

関連項目： 第 3 章「Oracle Directory Integration Platform 管理ツール」

LDAP 検索による変更のフィルタ処理

変更ログをサポートしていない接続ディレクトリの場合、LDAP 検索の実行によりエントリの最新のフットプリントが取得されます。objectclass=* を指定して実行される LDAP 検索では、所定のツリーまたはサブツリー内のエントリがすべて返されるため、同期に関係のあるオブジェクトのみを取得するには、LDAP フィルタ構文を使用してフィルタを指定する必要があります。たとえば、検索フィルタを orclOdipConDirMatchingFilter 属性に割り当てることができます。フィルタは、searchfilter=LDAP_SEARCH_FILTER と指定します。

次の例では、組織単位、グループおよびユーザーを取得し、コンピュータは取得しない LDAP 検索フィルタを作成します。

```
searchfilter=(|(objectclass=group)(objectclass=organizationalUnit)
(&(objectclass=user)(!(objectclass=computer))))
```

変更ログからの変更のフィルタ処理

変更ログに変更を格納する接続ディレクトリの場合、Oracle Directory Integration Platform に用意されている次の単純な演算子を使用すれば、「接続されたディレクトリ一致フィルタ」（orclODIPConDirMatchingFilter）または「OID 一致フィルタ」（orclODIPOIDMatchingFilter）に一致フィルタを指定できます。

- =（等しい演算子）
- !=（等しくない演算子）

> **注意：** LDAP 検索を使用して増分変更を取得する接続ディレクトリでは、searchfilter 属性なしで、前述の演算子を使用することもできます。ただし、指定できる式は 1 つのみで、複数の式を指定すると、検索は失敗します。

LDAP または LDAP 以外のディレクトリで、変更ログから増分変更が取得される場合は、前述の演算子を使用できます。searchfilter 属性を使用しない場合は、前述の演算子ではワイルドカードやパターン一致はサポートされません。ただし、フィルタに複数の演算子のペアが含まれている場合、式は AND 論理演算子として評価されます。たとえば、次の式には 4 つの演算子のペアが含まれています。

```
(objectclass=group)(objectclass=organizationalUnit)
(objectclass=user)(objectclass!=computer)
```

この式は次のように評価されます。

```
objectclass is equal to group
AND objectclass is equal to organizationalUnit
AND objectclass is equal to user
AND objectclass is NOT equal to computer
```

変更を変更ログに格納する接続ディレクトリの場合、一致フィルタで同期化できるのは、変更ログに現れる属性についてのみです。変更ログにない属性を一致フィルタに含めると、検索操作は失敗します。このため、一致フィルタの使用は、変更ログに増分変更を格納する接続ディレクトリに限られます。

ファイルの場所とネーミング

表 6-4 に、ディレクトリ統合プロファイル内および同期時に使用される各種のファイルの場所を示します。

表 6-4 ファイルの場所と名前

ファイル	ファイル名
インポート・データ・ファイル	$*ORACLE_HOME*/ldap/odi/data/import/*Profile_Name*.dat
エクスポート・データ・ファイル	$*ORACLE_HOME*/ldap/odi/data/export/*Profile_Name*.dat
追加構成情報ファイル	$*ORACLE_HOME*/ldap/odi/conf/*Profile_Name*.cfg
マッピング・ルール・ファイル	$*ORACLE_HOME*/ldap/odi/conf/*Profile_Name*.map

たとえば、Oracle Human Resources コネクタのデータ・ファイル名は oraclehrprofile.dat です。

7

ディレクトリ同期の管理

この章では、同期プロファイルの管理方法について説明します。内容は次のとおりです。

- 同期プロファイルの管理
- コマンドライン・ツールを使用した同期プロファイルの管理

関連項目： C-24 ページの「同期に関するトラブルシューティング」

同期プロファイルの管理

この項では、Oracle Directory Integration Server 管理ツールまたは Oracle Directory Manager を使用したプロファイルの登録と登録解除の方法について説明します。内容は次のとおりです。

プロファイルの作成

プロファイルは、次の 2 つの方法のいずれかで作成します。

- 新規構成設定エントリを作成し、次にこのエントリにプロファイルを追加する方法
- 既存の構成設定エントリを選択し、次にこのエントリにプロファイルを追加する方法

プロファイルを作成するには、次のようにします。

1. 次の手順に従って、Oracle Directory Integration Server 管理ツールを起動します。
   a. 次のコマンドを実行して、Oracle Directory Integration Server 管理ツールを起動します。

      ```
      dipassistant -gui
      ```

   b. ナビゲータ・ペインで「**統合プロファイルの構成**」を選択します。

   または

   次の手順に従って、Oracle Directory Manager を起動します。

   a. 次のコマンドを実行して、Oracle Directory Manager を起動します。

      ```
      oidadmin
      ```

   b. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「***directory server instance***」、「**サーバー管理**」、「**統合サーバー**」の順に展開します。
2. プロファイルを作成する構成設定を選択します。「統合コネクタ」タブ・ページが右側のペインに表示されます。
3. 「統合コネクタ」タブで、「**作成**」を選択します。「統合コネクタ」ダイアログ・ボックスが表示されます。次の 2 つのオプションがあります。
   - 既存のものをコピーして統合プロファイルを作成

     この場合は、コピーする Oracle Directory Integration Platform プロファイルを選択し、「**類似項目の作成**」を選択します。「統合プロファイル」ダイアログ・ボックスに「一般」タブ・ページが表示されます。
   - 既存のものをコピーせずに統合プロファイルを作成

     この場合は、「**新規作成**」を選択します。「統合プロファイル」ダイアログ・ボックスに「一般」タブ・ページが表示されます。

     関連項目：「統合プロファイル」ダイアログ・ボックスの詳細は、A-6 ページの「統合コネクタ」を参照してください。
4. 「一般」タブ・ページの各フィールドに情報を入力します。

   「一般」タブ・ページのフィールドの詳細は、A-6 ページの表 A-3 を参照してください。
5. 「実行」タブをクリックし、各フィールドに情報を入力します。

   「実行」タブ・ページのフィールドの詳細は、A-7 ページの表 A-4 を参照してください。

6. 「マッピング」タブをクリックし、各フィールドに情報を入力します。

   「マッピング」タブ・ページのフィールドの詳細は、A-8 ページの表 A-5 を参照してください。

7. 「ステータス」タブをクリックし、各フィールドに情報を入力します。このページにはコネクタの実行ステータスが表示されるため、ほとんどのフィールドは編集できません。

   「ステータス」タブ・ページのフィールドの詳細は、A-9 ページの表 A-6 を参照してください。

8. 情報を入力した後、「**OK**」をクリックします。「構成設定」ダイアログ・ボックスに戻ります。このダイアログ・ボックスには、作成した統合プロファイルがリストされています。これで作成したプロファイルが Oracle Internet Directory に登録されます。

プロファイルの変更

プロファイルを変更するには、次のようにします。

1. 次の手順に従って、Oracle Directory Integration Server 管理ツールを起動します。

   a. 次のコマンドを実行して、Oracle Directory Integration Server 管理ツールを起動します。

      ```
      dipassistant -gui
      ```

   b. ナビゲータ・ペインで「**統合プロファイルの構成**」を選択します。

   または

   次の手順に従って、Oracle Directory Manager を起動します。

   a. 次のコマンドを実行して、Oracle Directory Manager を起動します。

      ```
      oidadmin
      ```

   b. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「***directory server instance***」、「**サーバー管理**」、「**統合サーバー**」の順に展開します。

2. プロファイルを変更する構成設定を選択します。「統合コネクタ」タブ・ページが右側のペインに表示されます。
3. 「統合コネクタ」タブ・ページで、変更するプロファイルを選択します。
4. 「**編集**」をクリックします。「一般」タブ・ページが表示されます。
5. 「一般」タブ・ページの各フィールドを必要に応じて変更します。

   「一般」タブ・ページのフィールドの詳細は、A-6 ページの表 A-3 を参照してください。

6. 「実行」タブをクリックし、各フィールドを必要に応じて変更します。

   「実行」タブ・ページのフィールドの詳細は、A-7 ページの表 A-4 を参照してください。

7. 「マッピング」タブをクリックし、各フィールドを必要に応じて変更します。

   「マッピング」タブ・ページのフィールドの詳細は、A-8 ページの表 A-5 を参照してください。

8. 「ステータス」タブをクリックし、各フィールドを必要に応じて変更します。このページにはコネクタの実行ステータスが表示されるため、ほとんどのフィールドは編集できません。このタブの編集可能なフィールド（「前回適用された変更番号」フィールドなど）を変更する必要がある場合は、7-4 ページの「同期ステータス属性の変更」の手順に従う必要があります。

   「ステータス」タブ・ページのフィールドの詳細は、A-9 ページの表 A-6 を参照してください。

9. 情報の変更が完了したら、「**OK**」をクリックします。

プロファイルの削除

プロファイルを削除するには、次のようにします。

1. 次の手順に従って、Oracle Directory Integration Server 管理ツールを起動します。
   a. 次のコマンドを実行して、Oracle Directory Integration Server 管理ツールを起動します。

      ```
      dipassistant -gui
      ```

   b. ナビゲータ・ペインで「**統合プロファイルの構成**」を選択します。

   または

   次の手順に従って、Oracle Directory Manager を起動します。

   a. 次のコマンドを実行して、Oracle Directory Manager を起動します。

      ```
      oidadmin
      ```

   b. ナビゲータ・ペインで、「**Oracle Internet Directory サーバー**」、「***directory server instance***」、「**サーバー管理**」、「**統合サーバー**」の順に展開します。
2. 削除するプロファイルが含まれる構成設定を選択します。「統合コネクタ」タブが右側のペインに表示されます。
3. 「統合コネクタ」タブ・ページで、削除するプロファイルを選択します。
4. 「**削除**」をクリックします。

同期ステータス属性の変更

同期プロセス中、サーバーは `orcllastappliedchangenumber` 同期ステータス属性を常に更新します。Oracle Directory Integration Server 管理ツールでは、このフィールドは「**OID 前回適用された変更番号**」と呼ばれます。同期ステータス属性の変更はお薦めしません。しかし、`lastappliedchangenumber` 属性を更新する必要がある場合もあります。たとえば、なんらかの変更を再適用したり、特定のエントリの同期をスキップする必要がある場合などです。

同期ステータス属性を Oracle Directory Integration Server 管理ツールを使用して変更するには、次のようにします。

1. Oracle Directory Integration Platform がプロファイルに対する使用禁止フラグを認識することを確認します。

   デフォルト・モードでは、Oracle Directory Integration Server がこのフラグを認識するために、2 分ほどかかる場合があります。このフラグを迅速に認識させるには、更新間隔に低い値を設定します。詳細は、『Oracle Identity Management ユーザー・リファレンス』の Oracle Internet Directory サーバー管理ツールの章の `odisrv` に関する項を参照してください。
2. Oracle Directory Integration Server 管理ツールを使用して、エージェントを使用禁止にします。
3. 7-3 ページの「プロファイルの変更」の手順に従って、同期ステータス属性を変更します。
4. 変更後、エージェントを再度使用可能にします。

コマンドライン・ツールを使用した同期プロファイルの管理

Directory Integration アシスタント（dipassistant）を使用して、同期プロファイルの作成、変更および削除ができます。詳細は、『Oracle Identity Management ユーザー・リファレンス』の Oracle Directory Integration Platform ツールの章の dipassistant に関する項を参照してください。

8

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、ディレクトリのブートストラップ（接続ディレクトリと Oracle Internet Directory 間の初期のデータ移行）について説明します。同期プロセスでは接続ディレクトリと Oracle Internet Directory 間のデータの移行も処理されるため、ディレクトリのブートストラップを実行する必要はありません。ただし、初期のデータ移行を同期プロセスに依存すると、特にデータの量が多い場合など、時間がかかる可能性があります。このため、初めて Oracle Directory Integration Platform を配置する場合には、ディレクトリのブートストラップを実行します。

この章の内容は次のとおりです。

> **関連資料：**『Oracle Internet Directory 管理者ガイド』の他のディレクトリおよびデータ・リポジトリからのデータの移行に関する章

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

Oracle Directory Integration Platform では、ブートストラップは、`bootstrap` オプションを指定した Directory Integration アシスタント（`dipassistant`）を使用して処理されます。コマンドは次のとおりです。

```
dipassistant bootstrap
```

Directory Integration アシスタントの使用方法を参照するには、次のように入力します。

```
dipassistant bootstrap -help
```

Directory Integration アシスタントによって、パラメータ・ファイルまたは完全に構成された統合プロファイルのいずれかを使用して、ブートストラップができるようになります。この章では、両方の方法について説明します。

> **関連資料：**『Oracle Identity Management ユーザー・リファレンス』の Oracle Directory Integration Platform ツールの章の `dipassistant` に関する項

パラメータ・ファイルを使用したブートストラップ

このファイルのパラメータは、次のものを指定します。

- ソースおよび宛先のインタフェース・タイプ（LDIF および LDAP）
- 接続詳細および資格証明（LDAP の場合のみ有効）
- マッピング・ルール

各種パラメータと、Directory Integration アシスタントがファイルの読取り時にそれらに対して想定するデフォルト値の詳細は、『Oracle Identity Management ユーザー・リファレンス』の Oracle Directory Integration Platform ツールの章の `dipassistant` に関する項を参照してください。

次のいずれかの方法で、LDIF ファイルを使用してブートストラップすることができます。

- Directory Integration アシスタントを使用したソース・ディレクトリの読取り
- ディレクトリ依存ツールを使用したソース・ディレクトリの読取り
- Directory Integration アシスタントを使用した Oracle Internet Directory へのデータのロード

インストール時に、次のサンプル・パラメータ・ファイルが $*ORACLE_HOME*/ldap/odi/samples/ ディレクトリにコピーされます。

- Ldp2ldp.properties
- Ldp2ldf.properties
- Ldf2ldp.properties
- Ldf2ldf.properties

これらのファイルには、ブートストラップにおける各パラメータの機能が記述されています。

ブートストラップ用にツールを実行する場合は、*`ORACLE_HOME`* と `NLS_LANG` が正しく設定されていることを確認してください。

ブートストラップは、中間ファイルの有無にかかわらず、サービス間で実行できます。ただし、大きいディレクトリの場合は、中間 LDIF ファイルが必要です。

この項の内容は次のとおりです。

LDIF ファイルを使用しないブートストラップ

この方法は、エントリが次の状態の小さいディレクトリに使用することをお薦めします。

- 比較的少数
- フラット構造
- 非相互依存（グループ・エントリの作成はユーザー・メンバー・エントリの存在に依存する場合などとは異なり、この場合、エントリの作成は別のエントリの存在には依存しない）

この方法を使用する手順は、次のとおりです。

1. 適切なマッピング・ルールを持つマッピング・ファイルを作成します。マッピング・ファイルは、ブートストラップ・ファイル内のプロパティの 1 つです。同期用に定義されたマッピング・ルールと一致していることを確認してください。
2. ソースを LDAP、宛先タイプを LDIF と指定した必須の詳細情報を持つパラメータ・ファイルを作成します。サンプル・パラメータ・ファイル ldp2ldf.properties は、$*ORACLE_HOME*/ldap/odi/samples にあります。バイナリ属性が、`SrcAttrType` フィールドでバイナリとして指定されていることを確認します。
3. 次のように指定されている構成ファイルを使用して、Directory Integration アシスタントの `bootstrap` コマンドを実行します。
   - ソースが LDAP ディレクトリと指定されている。
   - 宛先タイプが LDIF と指定されている。

   次のように入力して、Directory Integration アシスタントを実行します。

   ```
   dipassistant bootstrap -cfg parameter_file
   ```
4. エラーがないかどうか、$*ORACLE_HOME*/ldap/odi/log/bootstrap.log ファイルと $*ORACLE_HOME*/ldap/odi/log/bootstrap.trc ファイルをチェックします。
5. `bulkload` ユーティリティを使用して、Oracle Internet Directory にデータをアップロードします。
6. 同期を継続するには、最後の変更番号を更新します。

   ```
   dipassistant mp -profile profile_name -updcln
   ```

LDIF ファイルを使用したブートストラップ

この項では、LDIF ファイルを使用してディレクトリをブートストラップする 2 つの方法について説明します。

ディレクトリ依存ツールを使用してソース・ディレクトリを読み取ることによって LDIF ファイルからブートストラップする方法

大きいディレクトリに対してはこの方法を使用することをお薦めします。この方法を使用する手順は、次のとおりです。

1. ディレクトリから LDIF ファイルにデータをダウンロードします。使用するツールは、データのロード元のディレクトリによって異なります。Microsoft Active Directory からブートストラップしている場合は、`ldifde` コマンドを使用してデータをロードします。各エントリに必要なすべての属性をロードしてください。
2. 適切なマッピング・ルールを持つマッピング・ファイルを作成します。さらに同期を行う場合は、マッピング・ファイルが同期に使用されるものと同じであることを確認してください。
3. LDIF としてのソースと宛先、およびその他の詳細情報を持つ宛先パラメータ・ファイルを作成します。サンプル・パラメータ・ファイルは $*ORACLE_HOME*/ldap/odi/samples/ldf2ldf.properties にあります。

4. ソースを LDIF、宛先タイプを LDIF と指定したパラメータ・ファイルとともに、Directory Integration アシスタントの `bootstrap` コマンドを使用します。これによって、ソース・データが変換され、Oracle Internet Directory で必要な新しい LDIF が作成されます。次のように入力して、Directory Integration アシスタントを実行します。

   ```
   dipassistant bootstrap -cfg parameter_file
   ```

5. エラーがないかどうか、`bootstrap.log` ファイルと `bootstrap.trc` ファイルをチェックします。

6. Oracle Internet Directory のバルク・ロード・ツール（`bulkload.sh`）を使用して、データを Oracle Internet Directory にアップロードします。

7. さらに同期を行うために対応する同期プロファイルを作成する場合は、最後の変更番号を更新します。

   ```
   dipassistant mp -profile profile_name -updcln
   ```

Directory Integration アシスタントを使用してデータを Oracle Internet Directory にロードすることによって LDIF ファイルからブートストラップする方法

この方法を使用する手順は、次のとおりです。

1. ディレクトリから LDIF ファイルにデータをダウンロードします。使用するツールは、データのロード元のディレクトリによって異なります。Microsoft Active Directory からブートストラップしている場合は、`ldifde` コマンドを使用してデータをロードします。各エントリに必要なすべての属性をロードしてください。

2. 適切なマッピング・ルールを持つマッピング・ファイルを準備します。さらに同期を行う場合は、マッピング・ファイルが同期に使用されるものと同じであることを確認してください。

3. ソースを LDIF、宛先を LDAP と指定して、プロパティ・ファイルを作成します。

4. ソースを LDIF ファイル、宛先タイプを LDAP、宛先を Oracle Internet Directory と指定したパラメータ・ファイルとともに、Directory Integration アシスタントの `bootstrap` コマンドを使用します。これによってソース・データが変換され、Oracle Internet Directory 内に必要なエントリが作成されます。サンプル・プロパティ・ファイル ldf2ldp.properties は、$*ORACLE_HOME*/ldap/odi/samples にあります。

5. エラーがないかどうか、bootstrap.log ファイルと bootstrap.trc ファイルをチェックします。

6. さらに同期を行うために対応する同期プロファイルを作成する場合は、最後の変更番号を更新します。

   ```
   dipassistant mp -profile profile_name -updcln
   ```

デフォルト統合プロファイルを使用した直接ブートストラップ

ブートストラップは、同期用に構成された既存の統合プロファイルに依存します。サード・パーティ・ディレクトリへの接続に使用される構成情報

この方法を使用する場合は、ソース・ディレクトリを読取り専用モードに設定します。

プロファイルがインポート・プロファイルの場合は、接続ディレクトリ内の必須オブジェクトのフットプリントが Oracle Internet Directory に作成されます。プロファイルがエクスポート・プロファイルの場合は、Oracle Internet Directory からの必須オブジェクトのフットプリントが接続ディレクトリ内に作成されます。

これらのエントリの作成中、統合プロファイルに指定されているとおり、識別名およびオブジェクト・レベルのマッピングが使用されます。エントリのアップロードに失敗した場合は、$*ORACLE_HOME*/ldap/odi/log/bootstrap.log に情報が記録されます。トレース情報は、$*ORACLE_HOME*/ldap/odi/log/bootstrap.trc ファイルに書き込まれます。

たとえば、Sun Java System Directory から Oracle Internet Directory にブートストラップする場合は、次の手順を実行します。

1. デフォルトの統合プロファイル `iPlanetImport` をカスタマイズします。このプロファイルは、21-2 ページの「Sun Java System Directory との拡張統合の構成」の方法に従ってインストールの一部として作成されます。
2. 次のコマンドを入力します。

   ```
   dipassistant bootstrap -profile iPlanetImport -D  'cn=orcladmin' -w 'welcome'
   ```

3. bootstrap.log ファイルと bootstrap.trc ファイルをチェックし、ブートストラップが正常に終了したことを確認してください。

Directory Integration アシスタント（`dipassistant`）を使用してブートストラップしている場合は、ブートストラップ処理の最後に Directory Integration アシスタントによって、以降の同期化のために `lastchangenumber` 属性が初期化されます。

SSL モードでのブートストラップ

パラメータ・ファイルまたは統合プロファイルを使用すると、SSL モードでブートストラップできます。SSL モードでブートストラップすると、Oracle Internet Directory または接続ディレクトリ、あるいはその両方を SSL モードで実行できます。

パラメータ・ファイルから SSL モードでブートストラップするには、パラメータ・ファイルで `odip.bootstrap.srcsslmode` 引数と `odip.bootstrap.destsslmode` 引数に `true` または `false` の値を割り当てる必要があります。

統合プロファイルから SSL モードでブートストラップするには、Directory Integration アシスタントの `-bootstrap` コマンドで `-U` 引数を使用します。`-U` 引数には、次の値のいずれかを指定できます。

- **1**: 認証なしの SSL モード
- **2**: サーバー認証ありの SSL モード
- **3**: サーバーおよびクライアント認証ありの SSL モード

デフォルトの統合プロファイルからブートストラップすると、デフォルトの統合プロファイルの `odip.profile.condirurl` に割り当てられた値を使用して、接続ディレクトリへの SSL 接続が確立されます。

> **関連資料：** `dipassistant` コマンドを SSL モードで実行する方法の詳細は、『Oracle Identity Management ユーザー・リファレンス』を参照してください。

ブートストラップの推奨方法

データのロード元であるソース・ディレクトリに大量のエントリがある場合、ターゲット・ディレクトリをブートストラップする最も迅速で簡単な方法は LDIF ファイルを使用する方法です。この場合、ソース・ディレクトリとターゲット・ディレクトリ間での読取りおよび書込みで接続エラーが発生する可能性があるため、統合プロファイルを使用したブートストラップはお薦めしません。LDIF ファイルの使用は、識別名に特殊文字が含まれる場合にもお薦めします。特殊文字は、統合プロファイルを使用したブートストラップでは適切にエスケープされないことがあるためです。

9

リレーショナル・データベースの表との同期

この章では、リレーショナル・データベース内の表のデータを Oracle Internet Directory と同期させる方法について説明します。同期は、増分（たとえば、データベース表の行単位）またはすべてのデータベース表を一括で実行できます。データベースとの同期プロセスでは、ディレクトリ統合プロファイルを実行する必要があります。このプロセスには 2 つの手順があります。

1. データベースからのデータの取得。これには、指定したデータ・レコードをデータベースから取得する SQL の `SELECT` 文を実行する必要があります。
2. ディレクトリへのデータの書込み。これには、取得したデータ・レコードを LDAP 属性値に変換し、ディレクトリに対して LDAP 操作を実行する必要があります。

注意： この章を読む前に、Oracle Directory Integration Platform の概要についての次の章をよく理解しておく必要があります。

- 第 1 章「Oracle Identity Management 統合の概要」
- 第 5 章「Oracle Directory Synchronization Service」

Oracle Internet Directory 10*g*（10.1.4.0.1）では、Oracle Internet Directory からリレーショナル・データベースへのデータのエクスポートはサポートされていません。

この章の内容は次のとおりです。

追加構成情報ファイルの準備

リレーショナル・データベースから Oracle Internet Directory への同期中、データベースからのデータの取得は、追加構成情報ファイルによって制御されます。追加構成情報ファイルは、Oracle Directory Integration Server に次の情報を提供します。

- 実行する SELECT 文
- 増分同期に使用される属性またはデータベース列のいずれか。通常、タイムスタンプを含む属性、または次の SQL 文で増分データの取得に使用する必要がある変更順序番号のいずれかです。

このファイルを構成するには、$*ORACLE_HOME*/ldap/odi/conf ディレクトリにあるサンプル・ファイル DBReader.cfg.master をユーザーの仕様に従って編集してください。

追加構成情報ファイルの形式

このファイルの構成では、正しい形式に従うことが非常に重要です。TAG 名を使用して、各種セクションに分割します。各 TAG セクションには、パラメータのリストとそれぞれの値を示します。通常のレイアウトは次のとおりです。

```
[TAG]
PARAMETER1: value
PARAMETER2: value

[TAG]
PARAMETER1: value
PARAMETER2: value\
VALUE continuation\
value continuation\
end of value continuation

[TAG]
PARAMETER1: value
PARAMETER2: value\
end of value continuation
```

この形式に従うと、たとえば、DBReader.cfg.master ファイルは次のようになります。

```
[DBQUERY]
SELECT: SELECT\
EMPNO EmpNum,\
ENAME,\
REPLACE(EMAIL),'@ACME.COM','') UID,\
EMAIL,\
TELEPHONE,\
TO_CHAR(LAST_UPDATE_DATE,'YYYYMMDDHH24MISS') Modified_Date\
FROM\
EMPLOYEE\
WHERE\
LAST_UPDATE_DATE>TO_DATE (:Modified_Date,'YYYYMMDDHH24MISS')\
ORDER BY\
LAST_UPDATE_DATE

[SYNC-PARAMS]
CHANGEKEYATTRS: Modified_Date
```

SELECT 文全体が SELECT パラメータの値として、タグ DBQUERY で表されているセクションに入力されています。値が冗長なため、SELECT 文の終わりまですべての行で値継続文字が最後の文字として入力されています。

CHANGEKEYATTRS パラメータ値は、増分同期の実行中に使用される列の名前です。これらの列の値は、常にプロファイルの orclOdipLastAppliedChgNum 属性に格納されます。SELECT 文が実行されるたびに、それに応じてこの属性の現在の値が SQL 文に入力されます。これによって、データは常に増分取得されます。

たとえば、column1:column2 のように複数の列名が CHANGEKEYATTRS にある場合は、プロファイルの orclOdipLastAppliedChgNum 属性の値が value1~value2 などとして格納されます。ここで value1 は column1 に、value2 は column2 に対応しています。

列名は、属性値ペアとして Oracle Directory Integration Platform に取得された後、設定されたマッピング・ルールに従って LDAP 属性値にマッピングされます。このため、SELECT 文で取得されたすべての列名は、式ではなく単純名である必要があります。たとえば、式 REPLACE(EMAIL),'@ACME.COM',''）を使用することはできますが、この式の値は、UID として取得されます。

この例では、Modified_Date が増分同期のキーです。これは日付であるため、文字列書式で指定する必要があります。

プロファイルを作成する場合は、orclOdipLastAppliedChgNum 属性に値を設定する必要があります。この日付より後のすべての変更（この値より大きい LAST_UPDATE_DATE を持つ表内の行）が取得されます。たとえば、orclOdipLastAppliedChgNum 属性を 20000101000000 に設定すると、2000 年 1 月 1 日以降のすべての従業員の変更が取得されます。

ORDER BY 句を使用しているため、返されるすべてのデータベース行は LAST_UPDATE_DATE の順序です。変更は、行われた順に取得されディレクトリに適用されます。最後の変更が取得されて適用された後、次の処理が行われます。

1. orclOdipLastAppliedChgNum 属性値が、取得された最後の行から Modified_Date に設定されます。
2. プロファイルが更新されます。

Oracle Directory Integration Platform は、プロファイルを再実行する場合、常に、すでに格納された値を使用します。

マッピング・ファイルの準備

マッピング・ルールを構成するには、5-3 ページの「マッピング・ルールとその形式」の指示に従います。

ディレクトリ統合プロファイルの準備

ディレクトリ統合プロファイルは、Oracle Directory Integration Server 管理ツールまたは Directory Integration アシスタント（dipassistant）を使用して作成できます。Oracle Directory Integration Server 管理ツールを使用する場合は、Directory Integration アシスタントを使用して、追加構成情報ファイルとマッピング・ファイルをアップロードする必要があります。

ディレクトリ統合プロファイルを構成するには、6-2 ページの「Oracle Directory Integration Platform でのコネクタの登録」の指示に従います。ただし、次の注意事項があります。

- 「エージェントの実行コマンド」（orclodipAgentExeCommand）属性に値を設定しないでください。
- 「インタフェース・タイプ」（orclodipDataInterfaceType）属性を DB に設定します。

例 : リレーショナル・データベース表と Oracle Internet Directory の同期化

この項では、リレーショナル・データベース表と Oracle Internet Directory を同期化する方法について説明します。内容は次のとおりです。

- 追加構成情報ファイルの構成
- マッピング・ファイルの構成
- ディレクトリ統合プロファイルの構成
- 追加構成情報ファイルのアップロード
- マッピング・ファイルのアップロード
- 同期プロセス
- 例に関する注意事項

この例では、従業員データを含む次のリレーショナル・データベース表が Oracle Internet Directory と同期化されます。

EMPNO	ENAME	LAST_UPDATE_DATE	EMAIL	TELEPHONE
98357	JOHN DOE	2-JAN-2000	JOHN.DOE@ACME.COM	435-324-3455
98360	ROGER BECK	3-JUL-2001	ROGER.BECK@ACME.COM	435-324-3600
98365	JIMMY WONG	4-MAR-2001	JIMMY.WONG@ACME.COM	435-324-2390
98370	GEORGE MICHAEL	6-FEB-2002	GEORGE.MICHAEL@ACME.COM	435-324-9232

この例のサンプル・プロファイルは、サンプルの構成ファイルとマッピング・ファイルとともに $*ORACLE_HOME*/ldap/odi/samples ディレクトリにあります。この例では、次のように仮定します。

- 表の名前は、`Employee` です。
- プロファイル名は、`TESTDBIMPORT` です。
- データベース・レコードをディレクトリ・エントリと結合するには、従業員番号（`EMPNO`）が使用されます。この番号は、「OID 一致フィルタ」（`orclOdipOIDMatchingFilter`）属性に指定されています。この属性の詳細は、『Oracle Identity Management ユーザー・リファレンス』の属性リファレンスに関する章を参照してください。
- この表は、データベース内の `testsync/testsyncpwd` スキーマにあります。データベースはホスト `machine.acme.com` に存在し、データベース・リスナー・ポートは `1526`、SID は `iasdb` です。データベース URL は、`machine.acme.com:1526:iasdb` です。
- 適切な読取り / 書込み権限がこのプロファイル、つまり `orclodipagentname=testdbimport,cn=subscriber profile,cn=changelog subscriber,cn=oracle internet directory` に明示的に付与されています。
- プロファイルは、構成設定 1 内に作成されます。

追加構成情報ファイルの構成

この例では、9-2 ページの「追加構成情報ファイルの準備」で説明した追加構成情報ファイルと同じファイルを使用します。

マッピング・ファイルの構成

この例のマッピング・ファイルの内容は次のとおりです。

```
DomainRules
NONLDAP:dc=testdbsync,dc=com:uid=%,dc=testdbsync,dc=com
AttributeRules
ename: : : :cn: :person
ename : : : :sn: :person
uid : : : :uid: :inetOrgperson:
EMail: : : :mail: :inetOrgperson
Telephone: : : :telephonenumber: :inetOrgperson
empnum: : : :employeenumber: :inetOrgperson
```

このマッピング・ファイルは次のことを指定しています。

- ディレクトリ・エントリは `uid=%,dc=testdbsync,dc=com` として作成されます。パーセント記号（`%`）は、`uid` の実際の値のプレースホルダです。マッピング後 `uid` に値が入るようにするには、`uid` がマッピング・ファイル内に存在している必要があります。存在しない場合、識別名の構成は失敗します。
- `cn` と `sn` の両方の属性は、`ename` と同じ値である必要があります。
- `uid` 要素の値は、`EMail` 接頭辞の値（電子メール・アドレス内のアット・マーク（@）文字より前の部分）になります。
- `empnum` 属性は、ディレクトリ・エントリ内の `employeenumber` になります。
- `telephone` 属性は、ディレクトリ・エントリ内の `telephone number` になります。

ディレクトリ統合プロファイルの構成

この例のディレクトリ統合プロファイルには、9-6 ページの表 9-1 に示す属性値が含まれます。これらの値が入ったサンプル統合プロファイルとそれに対応するマッピング・ファイルおよび構成ファイルが $*ORACLE_HOME*/ldap/odi/samples ディレクトリにあります。`createprofile` モードで Directory Integration アシスタント（`dipassistant`）を実行し、引数としてファイルを指定してプロファイルを作成できます。また、Oracle Directory Integration Server 管理ツールを使用してプロファイルを作成することもできます。

関連資料 :

- Directory Integration アシスタント（`dipassistant`）の詳細は、『Oracle Identity Management ユーザー・リファレンス』の Oracle Directory Integration Platform ツールの章の `dipassistant` に関する項を参照してください。
- Oracle Directory Integration Server 管理ツールを使用してプロファイルを作成する方法は、7-2 ページの「プロファイルの作成」を参照してください。

表 9-1 TESTDBIMPORT 用のディレクトリ統合プロファイル

属性	値
プロファイル名（orclOdipAgentName）	TESTDBIMPORT
同期モード（orclOdipSynchronizationMode）	IMPORT
Professoriats（orclOdipAgentControl）	ENABLE
エージェントの実行コマンド（orclodipAgentExeCommad）	NULL
追加構成情報（orclOdipAgentConfigInfo）	前述のファイルに示したとおり。アップロードの必要あり。
接続されたディレクトリ・アカウント（orclOdipConDirAccessAccount）	testdbsync
接続されたディレクトリ・アカウントのパスワード（orclOdipConDirAccessPassword）	testdbsyncpwd
接続されたディレクトリ URL（orclOdipConDirURL）	machine.acme.com:1526:iasdb
インタフェース・タイプ（orclodipDataInterfaceType）	DB
マッピング・ファイル :	ファイルからアップロード。
OID 一致フィルタ（orclOdipOIDMatchingFilter）	employeenumber これは、一致を検索中、ディレクトリの検索に employeenumber が使用されることを意味します。一致が検証されると、ディレクトリ・エントリが修正されます。それ以外の場合は、新しいエントリが作成されます。これは、orclOdipOIDMatchingFilter 属性がデータベース内で一意なことを保証するためにも必要です。 データベース行が取得されると、Oracle Directory Integration Platform では、ドメイン・ルールに従って、dc=testdbsync,dc=com ドメインのディレクトリで employeenumber を検索します。一致が検出された場合は、検索された行内の列の最新の値でそのエントリが更新されます。一致が検出されなかった場合は、列値のすべての属性を持つ新しいエントリがディレクトリ内に作成されます。
前回適用された変更番号（orclodipConDirLastAppliedChgNum）	20000101000000 これは、プロファイルの最初の実行時に、4 つすべての行を取得し同期することを意味します。その後は、表内の LAST_UPDATE_DATE 列が最終更新時刻に更新した場合にのみ、行が取得されます。

追加構成情報ファイルのアップロード

Directory Integration アシスタントを使用して、追加構成情報ファイルを次のようにアップロードします。

```
$ORACLE_HOME/bin/dipassistant modifyprofile [-h hostName] [-p port]
[-D bindDn] [-w password] -profile profName
odip.profile.mapfile=absolute path name of configuration file
```

マッピング・ファイルのアップロード

Directory Integration アシスタントを使用して、マッピング・ファイルを次のようにアップロードします。

```
$ORACLE_HOME/bin/dipassistant modifyprofile [-h hostName] [-p port]
[-D bindDn] [-w password] -profile profName
odip.profile.mapfile=absolute path name of mapping file
```

同期プロセス

この例では、同期プロセスの手順は、次のとおりです。

1. 「スケジューリングの間隔」（orclOdipSchedulingInterval）属性に指定された値が期限切れになるたびに、Oracle Directory Integration Server は、TESTDBIMPORT プロファイル用に新しいプロファイル・スレッドを起動します。
2. プロファイル・スレッドは、追加構成情報を読み取って SQL を準備し、実行します。
3. データベースから取得された行ごとに、マッピング・ルールがレコードに適用され、LDAP 属性が作成されます。
4. 「OID 一致フィルタ」（orclOdipOIDMatchingFilter）属性によって、Oracle Internet Directory 内に一致するエントリがあるかどうかを Oracle Directory Integration Server が判断します。一致するエントリがある場合は更新されます。ない場合は新しいエントリが作成されます。ディレクトリ操作の後、最後に適用された変更番号（orclodipConDirLastAppliedChgNum）属性が更新されます。

例に関する注意事項

行は、次の形式でデータベースから取得されます。

```
EmpNum: 98357
EName: JOHN DOE
UID: JOHN.DOE
EMAIL: JOHN.DOE@ACME.COM
TELEPHONE: 435-324-3455
Modified_Date: 20000102000000
```

このレコード上でマッピングが行われると、次の形式で出力されます。

```
dn: uid=john.doe,dc=testdbsync,dc=com
uid: JOHN.DOE
cn: JOHN DOE
sn: JOHN DOE
mail: JOHN.DOE@ACME.COM
employeenumber: 98357
telephonenumber: 435-324-3455
objectclass: person
objectclass: inetorgperson
```

dc=testdbsync,dc=com ドメイン下の employeenumber=98357 フィルタを使用して、ディレクトリ内でサブツリー検索が行われます。検索結果が既存のエントリの場合は、そのエントリが更新されます。それ以外の場合は、新しいエントリが作成されます。「OID 一致フィルタ」（orclOdipOIDMatchingFilter）属性が employeenumber に設定されているため、取

得されるすべてのデータベース・レコードにはその列があります。この場合は、employeenumber にマップされる EmpNum です。

マッピング・ファイル内のその他の属性で、SQL によって取得されるデータに含まれないもの（birthday 属性など）は無視されます。

プロファイル・スレッドは、SQL からのすべての変更レコードを処理した後、次の属性の正しい値でディレクトリを更新します。

- 前回適用された変更番号（orclodipConDirLastAppliedChgNum）
- 最終実行時間（orclOdipLastExecutionTime）
- 最終正常実行時間（orclOdipLastSuccessfulExecutionTime）

10

Oracle Human Resources との同期化

企業内の従業員データ用のプライマリ・リポジトリとして Oracle Human Resources を使用している場合は、Oracle Human Resources と Oracle Internet Directory を同期化する必要があります。同期化には、Oracle Human Resources コネクタを使用します。

この章では、Oracle Human Resources コネクタを紹介し、その配置方法を説明します。内容は次のとおりです。

> **関連資料：** このリリースの Oracle Internet Directory と同期化できる Oracle Human Resources のリリースを確認する場合は、Oracle Internet Directory のリリース・ノートを参照してください。

Oracle Human Resources との同期化の概要

Oracle Human Resources コネクタによって、従業員データのサブセットを、Oracle Human Resources から Oracle Internet Directory にインポートできます。このコネクタには、あらかじめパッケージされた統合プロファイルと、Oracle Internet Directory との通信を処理する Oracle Human Resources エージェントの両方が含まれます。パッケージ済の統合プロファイルは、Oracle Directory Integration Server 管理ツールまたは Directory Integration アシスタント（dipassistant）を使用して、配置要件に応じてカスタマイズできます。

Oracle Human Resources コネクタは、Oracle Human Resources システムから増分変更を抽出するように構成することによって、いつでも実行できるようにスケジュールできます。また、Oracle Human Resources の列名と Oracle Internet Directory の属性の間のマッピングを設定および変更できます。

Oracle Human Resources からインポートできるデータ

表 10-1 は、Oracle Human Resources スキーマの表を示しています。選択した場合は、これらの属性のほとんどを Oracle Internet Directory にインポートできます。

表 10-1 Oracle Human Resources スキーマの表

表名	コネクタ構成情報フィールドで使用される別名
PER_PEOPLE_F	PER
PER_ADDRESSES	PA
PER_PERIODS_OF_SERVICE	PPS
PER_PERSON_TYPES	PPT

Oracle Human Resources データベースに apps アカウントでログインした場合は、これらの表はすべて参照できます。

属性は実行時に構成ファイルから追加または削除できるので、Oracle Human Resources コネクタは、必要な属性のみを選択して取得する SQL 文を動的に作成します。

表 10-2 は、Oracle Human Resources のユーザー・インタフェースのフィールドの一部を示しています。これらのフィールドは、従業員データを追加または変更するときに表示されます。

表 10-2 Oracle Human Resources のユーザー・インタフェースのフィールド

属性名	説明	フォーム / キャンバス / フィールド名
LAST_NAME	個人の姓	個人情報 / 氏名 / 姓
FIRST_NAME	個人の名	個人情報 / 氏名 / 名
TITLE	個人の役職	個人情報 / 氏名 / タイトル
SUFFIX	サフィックス（Jr、Sr、Ph.D など）	個人情報 / 氏名 / サフィックス
MIDDLE_NAME	ミドルネーム	個人情報 / 氏名 / ミドルネーム
SEX	性別	性別リスト・ボックス
START_DATE	入社日	個人情報 / 入社日
DATE_OF_BIRTH	生年月日	個人情報 / 個人情報 / 生年月日
MARITAL_STATUS	婚姻区分	個人情報 / 個人情報 / ステータス
NATIONAL_INDENTIFIER	米国居住者用社会保障番号	個人情報 /ID/ 社会保障
EMPLOYEE_NUMBER	従業員番号	個人情報 /ID/ 従業員
REGISTERD_DISABLED_FLAG	障害の有無のインジケータ	個人情報 / 個人情報 / 障害の有無

表 10-2 Oracle Human Resources のユーザー・インタフェースのフィールド（続き）

属性名	説明	フォーム / キャンバス / フィールド名
EMAIL_ADDRESS	電子メール・アドレス	個人情報 / 個人情報 /E メール
OFFICE_NUMBER	オフィス所在地	個人情報 / オフィス所在地情報 / オフィス
MAILSTOP	郵便物配達先	個人情報 / オフィス所在地情報 / 郵便宛先
INTERNAL_LOCATION	事務所	個人情報 / オフィス所在地情報 / 事業所
ADDRESS_LINE1	住所 1	個人住所情報 / 住所 1
ADDRESS_LINE2	住所 2	個人住所情報 / 住所 2
ADDRESS_LINE3	住所 3	個人住所情報 / 住所 3
TOWN_OR_CITY	市区町村	個人住所情報 / 市区
REGION_1	地域 1	個人住所情報 / 郡
REGION_2	地域 2	個人住所情報 / 都道府県
POSTAL_CODE	郵便番号	個人住所情報 / 郵便番号
COUNTRY	国	個人住所情報 / 国
TELEPHONE_NUMBER_1	電話番号 1	個人住所情報 / 電話番号
TELEPHONE_NUMBER_2	電話番号 2	個人住所情報 / 電話番号 2

Oracle Human Resources と Oracle Internet Directory 間の同期の管理

この項の内容は次のとおりです。

タスク 1: Oracle Human Resources コネクタのディレクトリ統合プロファイルの構成

Oracle Human Resources コネクタとともにインストールされるパッケージ済の統合プロファイルを構成するには、Oracle Directory Integration Server 管理ツールまたは Directory Integration アシスタントを使用します。Oracle Directory Integration Server 管理ツールの詳細は、第 7 章「ディレクトリ同期の管理」を参照してください。Directory Integration アシスタントの詳細は、『Oracle Identity Management ユーザー・リファレンス』の Oracle Directory Integration Platform ツールの章の `dipassistant` に関する項を参照してください。

パッケージ済統合プロファイルの一部のパラメータでは、Human Resources コネクタとの統合に固有の値を指定する必要があります。Human Resources コネクタに固有のパラメータは、10-4 ページの表 10-3 を参照してください。

表 10-3 Oracle Human Resources コネクタ統合プロファイルに固有の属性

属性	説明
プロファイル名（`orclODIPAgentName`）	システム内でコネクタを識別するための一意名。統合プロファイルを識別する識別名の相対識別名コンポーネントとして使用されます。この名前には英数字のみを使用できます。この属性は必須で、変更不可です。デフォルトの名前は `OracleHRAgent` です。
同期モード（`ModeorclODIPSynchronizationMode`）	Oracle Internet Directory と接続ディレクトリ間での同期の方向。 ■ `IMPORT` は接続ディレクトリから Oracle Internet Directory への変更のインポートを示します。 ■ `EXPORT` は Oracle Internet Directory から接続ディレクトリへの変更のエクスポートを示します。 デフォルトは `IMPORT` です。 この属性は必須で、変更可能です。 **注意：** Oracle Internet Directory 10*g*（10.1.4.0.1）では、Oracle Human Resources のインポート操作のみがサポートされます。
実行情報	

エージェントの実行コマンド（`orclODIPAgentExeCommand`）	Directory Integration Server がコネクタの実行に使用する、コネクタ実行可能ファイルの名前と引数のリスト。
	この属性は必須で、変更可能です。
	デフォルトは次の値です。
	`odihragent OracleHRAgent connect=hrdb \`
	`login=%orclodipConDirAccessAccount \`
	`pass=%orclodipConDirAccessPassword \`
	`date=%orclODIPLastSuccessfulExecutionTime \`
	引数 `connect=hrdb` の値は、Oracle Human Resources システム・データベースの接続文字列に設定する必要があります。

接続されたディレクトリ・アカウント（`orclodipConDirAccessAccount`）	コネクタが同期で使用する、接続ディレクトリ内の有効なユーザー・アカウント。Human Resources Agent の場合のユーザー・アカウントは、Oracle Human Resources データベース内の有効なユーザー識別子です。 **関連項目：** コマンドラインで引数を渡す一般的な使用方法は、第 10 章「Oracle Human Resources との同期化」を参照してください。

表 10-3 Oracle Human Resources コネクタ統合プロファイルに固有の属性（続き）

属性	説明
追加構成情報 (orclODIPAgentConfigInfo)	コネクタが Oracle Internet Directory に格納する構成情報。この構成情報は、コネクタの起動時に、Directory Integration Server によってコネクタに渡されます。この情報は属性として格納され、Directory Integration Server はその内容を認識しません。 この属性に格納される値は、Oracle Human Resources からの同期が必要な（Oracle Human Resources コネクタについて）すべての属性を表します。 **関連項目：**10-6 ページの「タスク 2: Oracle Internet Directory と同期化される属性のリストの構成」 Oracle Human Resources コネクタの場合、この属性は必須です。構成ファイルを編集してからプロファイルに再度アップロードすることによって変更できます。この属性は、Oracle Directory Integration Server 管理ツールでは修正できません。
接続されたディレクトリ URL (orclOdipConDirURL)	接続ディレクトリのホストとポートの詳細情報です。*host:port:sid* の書式で入力する必要があります。
インタフェース・タイプ (orclODIPInterfaceType)	データ転送に使用するインタフェース。このインタフェースはタグ付きファイルの形式であるため、TAGGED に設定されます。 **注意：**Oracle Human Resources プロファイルの場合、この属性は変更しないでください。
マッピング情報	
マッピング・ルール (orclODIPAttributeMappingRules)	マッピング・ルールを格納するための属性。Directory Integration アシスタント（dipassistant）を使用してファイルにマッピング・ルールを格納します。 Oracle Human Resources の場合、この属性は必須で、変更可能です。 **関連項目：** ■ 5-3 ページの「マッピング・ルールとその形式」 ■ 6-5 ページの「マッピング・ルールの構成」
接続されたディレクトリ一致フィルタ (orclODIPConDirMatchingFilter)	Oracle Human Resources 接続には使用されません。
OID 一致フィルタ (orclODIPOIDMatchingFilter)	この属性は、Oracle Internet Directory でのターゲット・エントリの検索に使用される LDAP フィルタを指定します。Oracle Directory Integration Server はこのフィルタを使用して、同期に必要な LDAP 操作の種類を検出します。 employeenumber=% の形式で指定します。 この属性はオプションで、変更可能です。
ステータス情報	
OID 前回適用された変更番号 (orcllastappliedChangenumber)	この属性は、すべてのエキスポート・プロファイルの基準で、Oracle Human Resources の同期には適用されません。
前回適用された変更番号 (orclODIPConDirLastAppliedChgNum)	この属性は、すべてのプロファイルの基準で、Oracle Human Resources の同期には適用されません。

タスク 2: Oracle Internet Directory と同期化される属性のリストの構成

デフォルトの Oracle Human Resources プロファイルは、Oracle Human Resources から Oracle Internet Directory に同期化される属性のデフォルト・リストを提供します。このリストはカスタマイズ可能で、属性を追加または削除できます。

デフォルトの属性リストは、統合プロファイルの一部として `orclodipAgentConfigInfo` 属性に格納されます。構成情報も、$*ORACLE_HOME*/ldap/odi/conf ディレクトリにある oraclehragent.cfg.master ファイルに用意されています。

注意： oraclehragent.cfg.master ファイルはバックアップとして機能するため、変更できません。

表 10-4 に、Oracle Human Resources の属性のデフォルトのリストの列を示します。

表 10-4 デフォルトで Oracle Internet Directory と同期化する Oracle Human Resources の属性

列	説明
ATTRNAME	出力データ・ファイルに生成される出力タグ。
COLUMN_NAME	この値の取得元になるデータベース列名。
TABLE_NAME	この値の取得元になるデータベース表名。
FORMAT	この属性の列データ型（ASCII、NUMBER、DATE）。
MAP	この属性を Oracle Human Resources から抽出するかどうかのインジケータ。値 `Y` は抽出されることを示し、値 `N` は抽出されないことを示します。

oraclehragent.cfg.master ファイルの内容は、次のとおりです。

```
ATTRNAME:COLUMN_NAME:TABLE_NAME:FORMAT:MAP
PersonId:person_id:PER:NUMBER:Y
PersonType:person_type_id:PER:NUMBER:Y
PersonTypeName:system_person_type:PPT:ASCII:Y
LastName:last_name:PER:ASCII:Y
StartDate:start_date:PER:DATE:Y
BirthDate:date_of_birth:PER:DATE:Y
EMail:email_address:PER:ASCII:Y
EmployeeNumber:employee_number:PER:NUMBER:Y
FirstName:first_name:PER:ASCII:Y
FullName:full_name:PER:ASCII:Y
knownas:known_as:PER:ASCII:Y
MaritalStatus:marital_status:PER:ASCII:Y
middleName:middle_names:PER:ASCII:Y
country:country:PA:ASCII:Y
socialsecurity:national_identifier:PER:ASCII:Y
Sex:sex:PER:ASCII:Y
Title:title:PER:ASCII:Y
suffix:suffix:PER:ASCII:Y
street1:address_line1:PA:ASCII:Y
zip:postal_code:PA:ASCII:Y
Address1:address_line1:PA:ASCII:Y
Address2:address_line2:PA:ASCII:Y
Address3:address_line3:PA:ASCII:Y
TelephoneNumber1:telephone_number_1:PA:ASCII:Y
TelephoneNumber2:telephone_number_2:PA:ASCII:Y
TelephoneNumber3:telephone_number_3:PA:ASCII:Y
town_or_city:town_or_city:PA:ASCII:Y
state:region_2:PA:ASCII:Y
Start_date:effective_start_date:PER:DATE:Y
End_date:effective_end_date:PER:DATE:Y
```

```
per_updateTime:last_update_date:PER:DATE:Y
pa_updateTime:last_update_date:PA:DATE:Y
```

同期化される Oracle Human Resources の追加属性の変更

同期化される Oracle Human Resources の属性を追加する手順は、次のとおりです。

1. oraclehragent.cfg.master ファイルをコピーし、*Agent_Name.cfg* 以外の名前を付けます。これは、Oracle Directory Integration Server がこの名前の構成ファイルを生成し、実行時に構成情報を Oracle Human Resources エージェントに渡すのに使用するためです。
2. このファイルにレコードを追加することにより、Oracle Human Resources の同期化される属性を追加します。これには、次の情報が必要です。
   - 属性値の抽出元になるデータベース内の表名。これらの表は、10-2 ページの表 10-1 にリストされています。このファイルでは、同期に使用される 4 つの表に、省略された名前が使用されます。
   - 表の列名。
   - 列のデータ型。有効な値は、`ASCII`、`NUMBER` および `DATE` です。

   また、列名に属性名を割り当てる必要もあります。これは、出力ファイル内でこの属性を識別するための出力タグとして動作します。このタグは、マッピング・ルール内で Oracle Human Resources の属性と Oracle Internet Directory の属性の間のルールを確立するために使用されます。

   `map` 列（レコード内の最後の列）が値 `Y` に設定されていることを確認する必要もあります。

> **注意：** 属性リストに新規属性を追加する場合は、`orclodipAttributeMappingRules` 属性内に対応するルールを定義する必要があります。定義しない場合、Oracle Human Resources の属性は、Oracle Human Resources コネクタに抽出されても Oracle Internet Directory と同期化されません。

Oracle Human Resources の同期化される属性の除外

現在 Oracle Internet Directory と同期化されている Oracle Human Resources の属性を除外する手順は、次のとおりです。

1. oraclehragent.cfg.master ファイルをコピーし、*Agent_Name.cfg* 以外の名前を付けます。これは、Directory Integration Server がこの名前の構成ファイルを生成し、実行時に構成情報を Oracle Human Resources コネクタに渡すのに使用するためです。
2. 次のいずれか 1 つを行います。
   - 属性リスト内の対応するレコードの前に番号記号（#）を付けてコメント化する。
   - 列 `map` の値を `N` に設定する。

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

前述のサポートされている属性の構成が、Oracle Human Resources データベースからデータを抽出するには不十分な場合、Oracle Human Resources エージェントは、構成ファイル内にある事前構成済の SQL SELECT 文を実行することもできます。構成ファイルには、このサポートを示すタグ（構成ファイル内の [SELECT]）があります。

次の例は、Oracle Human Resources データベースから情報の一部を取得するサンプルの SELECT 文を示しています。SQL 文を配置できるのは、[SELECT] タグの下のみです。BINDVAR バインド変数は、増分変更を取得するために必要です。代入値によって、この変数の値（タイムスタンプ）が Oracle Human Resources コネクタに渡されます。

SELECT 文で取得される列の式にはすべて列名を指定する必要があります。たとえば、REPLACE(ppx.email_address),'@ORACLE.COM','') は、EMAILADDRESS として取得されます。Oracle Human Resources コネクタは、REPLACE(ppx.email_address),'@ORACLE.COM''' 式の結果の属性値とともに、EMAILADDRESS を属性名として出力ファイルに書き出します。

次に構成ファイル内の SELECT 文の例を示します。

```
[SELECT]

SELECT
     REPLACE(ppx.email_address,'@ORACLE.COM','') EMAILADDRESS ,
     UPPER(ppx.attribute26) GUID,
     UPPER(ppx.last_name) LASTNAME,
     UPPER(ppx.first_name) FIRSTNAME,
     UPPER(ppx.middle_names) MIDDLENAME,
     UPPER(ppx.known_as) NICKNAME,
     UPPER(SUBSTR(ppx.date_of_birth,1,6)) BIRTHDAY,
     UPPER(ppx.employee_number) EMPLOYEEID,
     UPPER(ppos.date_start)  HIREDATE
FROM
   hr_organization_units hou,
   per_people_x ppx,
   per_people_x mppx,
   per_periods_of_service ppos
  WHERE
      pax.supervisor_id  = mppx.person_id(+)
  AND pax.organization_id = hou.organization_id(+)
  AND ppx.person_id = ppos.person_id
  AND ppx.person_id = pax.person_id
  AND ppos.actual_termination_date IS NULL
  AND UPPER(ppx.current_employee_flag) = 'Y'
  AND ppx.last_update_date >= (:BINDVAR,'YYYYMMDDHH24MISS')
```

タスク 3: Oracle Human Resources コネクタに関するマッピング・ルールの設定

属性マッピング・ルールは、Oracle Directory Integration Server が Oracle Human Resources と Oracle Internet Directory の間で属性を変換する方法を制御します。Oracle Directory Integration Server が使用するマッピング・ルールはカスタマイズできます。

Oracle Human Resources エージェント・プロファイルには、デフォルトのマッピング・ファイルがあります。一連のマッピング・ルールはこのマッピング・ファイルの orclodipAttributeMappingRules 属性に格納されています。この情報は、oraclehragent.map.master というファイルにも格納されています。このファイルは、$*ORACLE_HOME*/ldap/odi/conf ディレクトリの下にあります。

注意： oraclehragent.map.master ファイルは変更しないでください。バックアップとして機能しているためです。

関連項目： oraclehragent.map.master ファイルの内容およびマッピング・ルール・レコードの形式の説明は、5-3 ページの「マッピング・ルールとその形式」を参照してください。

タスク 4: Oracle Human Resources から Oracle Internet Directory への同期の準備

この項では、Oracle Human Resources から Oracle Internet Directory への同期の設定方法を説明します。

同期の準備

Oracle Human Resources と Oracle Internet Directory 間の同期を準備するには、次の手順に従います。

1. Oracle Human Resources コネクタと Directory Integration Server が、Oracle Human Resources コネクタの実行元であるホストにインストールされていることを確認します。
2. Oracle Human Resources システムにアクセスするための情報を持っていることを確認します。これには次の情報があります。
   - Oracle Human Resources システムのデータベースへの接続文字列
   - アクセス・アカウント
   - パスワード
3. 10-4 ページの「タスク 1: Oracle Human Resources コネクタのディレクトリ統合プロファイルの構成」の説明に従って、Oracle Human Resources コネクタの統合プロファイルを構成します。統合プロファイルのすべての値が適切に設定されていることを確認します。これには次の値があります。
   - Oracle Human Resources の属性リスト
   - Oracle Human Resources の属性マッピング・ルール
   - スケジューリング間隔
4. すべてを適切に設定した後、「プロファイルのステータス」（`orclodipagentcontrol`）属性を `ENABLE` に設定します。この設定によって、Oracle Human Resources コネクタを実行する準備が完了していることを示します。
5. それぞれのホストで Oracle ディレクトリ・サーバーと Oracle Human Resources が実行されていない場合、これらを起動します。
6. 準備が完了した後、まだこのホストで Directory Integration Server が実行されていない場合は、これを起動します。

   関連項目： Directory Integration Server を起動および停止する方法は、4-8 ページの「Oracle Directory Integration Platform の起動、停止および再起動」を参照してください。

同期プロセス

Oracle Human Resources システム、Oracle Internet Directory および Oracle Directory Integration Server が実行され、Oracle Human Resources コネクタが使用可能になると、Oracle Directory Integration Server は Oracle Human Resources システムから Oracle Internet Directory への変更の同期を自動的に開始します。そのプロセスは、次のとおりです。

1. 「最終実行時間」（orclodipLastExecutionTime）と「スケジューリングの間隔」（orclodipschedulinginterval）に指定されている値に従って、Oracle Directory Integration Server は、Oracle Human Resources コネクタを起動します。
2. Human Resources エージェントは次のものを抽出します。
   - 統合プロファイル内の orclodipLastSuccessfulExecutionTime 属性に指定されている時間に基づいた Oracle Human Resources システムからのすべての変更
   - プロファイル内の orclodipAgentConfigInfo 属性に指定されている属性のみ

   変更は、Oracle Human Resources のインポート・ファイルである $*ORACLE_HOME*/ldap/odi/import/HR_Agent_Name.dat に書き込まれます。
3. エージェントは、実行を完了した後、次のようなデータ・ファイルを作成します。

```
FirstName: John
LastName: Liu
EmployeeNumber: 12345
Title: Mr.
Sex: M
MaritalStatus: Married
TelephoneNumber: 123-456-7891
Mail: Jliu@my_company.com
Address: 100 Jones Parkway
City: MyTown
```

4. Oracle Directory Integration Server は、次の動作により変更を Oracle Internet Directory へインポートします。
   - インポート・ファイルからの各変更レコードの読取り。
   - 統合プロファイルの「マッピング・ルール」（orclodipAttributeMappingRules）に指定されているルールに基づいた、各変更レコードの LDAP 変更エントリへの変換。
5. すべての変更内容が Oracle Internet Directory に正常にインポートされると、Oracle Human Resources コネクタは、インポート・ファイルをアーカイブ・ディレクトリ（$*ORACLE_HOME*/ldap/odi/import/archive）に移動します。ステータスの属性である「最終実行時間」（orclodipLastExecutionTime）と「最終正常実行時間」（orclodipLastSuccessfulExecutionTime）を現在の時間に更新します。

   インポート操作が失敗した場合は、「最終実行時間」（orclodipLastExecutionTime）属性のみが更新され、コネクタは「最終正常実行時間」（orclodipLastSuccessfulExecutionTime）属性に基づいて Human Resources システムからの変更の抽出を試行します。失敗の理由は、$*ORACLE_HOME*/ldap/odi/HR_Agent_Name.trc のトレース・ファイルに記録されます。

Oracle Human Resources からの Oracle Internet Directory のブートストラップ

Oracle Human Resources から Oracle Internet Directory をブートストラップする方法は 2 つあります。

- Oracle Human Resources コネクタを使用する。統合プロファイルで、`orclodipLastSuccessfulExecutionTime` 属性を Oracle Human Resources がインストールされた時間よりも前に設定する。
- 外部ツールを使用して、Oracle Human Resources から Oracle Internet Directory にデータを移行する。

11

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、サポート対象のサード・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。Oracle Directory Integration Server には、サード・パーティのメタディレクトリ・ソリューション用のマッピング・サービスやスケジューリング・サービスは用意されていません。

この章では、変更ログ情報の生成方法と、サポートするソリューションでの変更ログ情報の使用方法について説明します。また、Oracle Internet Directory と同期できるように、サード・パーティのメタディレクトリ・ソリューションを使用可能にする方法を示します。

この章の内容は次のとおりです。

変更ログの概要

Oracle Internet Directory は、各変更をエントリとして変更ログ・コンテナに記録します。サード・パーティのメタディレクトリ・ソリューションは、変更ログ・コンテナから変更を取得し、サード・パーティ・ディレクトリに適用します。これらの変更を取得するために、サード・パーティのメタディレクトリ・ソリューションは Oracle Internet Directory の変更ログをサブスクライブする必要があります。

変更ログの各エントリには変更番号があります。サード・パーティのメタディレクトリ・ソリューションは、最後に適用した変更番号を記録しておき、その番号よりも大きい変更番号の変更のみを Oracle Internet Directory から取得します。たとえば、サード・パーティのメタディレクトリ・ソリューションが取得した最後の変更の番号が 250 だった場合、それ以降の変更の番号は 251 以上になります。

注意： サード・パーティのメタディレクトリ・ソリューションが Oracle Internet Directory の変更ログでサブスクライブされず、ソリューションが最初に取得した変更番号が最後に適用した変更番号よりも 2 以上大きい場合、Oracle Internet Directory 変更ログ内の変更の一部が、すでにパージされています。この場合、サード・パーティのメタディレクトリ・ソリューションは、Oracle Internet Directory 全体を読み取り、そのコピーと Oracle Internet Directory の情報とを同期化する必要があります。

関連項目： ディレクトリ統合プロファイルの概念は、5-2 ページの「Oracle ディレクトリの同期に必要なコンポーネント」を参照してください。

Oracle Internet Directory と同期化するためのサード・パーティのメタディレクトリ・ソリューションの有効化

サード・パーティのメタディレクトリ・ソリューションが Oracle Internet Directory から変更を取得するには、この項で説明する次のタスクを実行します。

- タスク 1: 初期ブートストラップの実行
- タスク 2: Oracle Internet Directory でのサード・パーティのメタディレクトリ・ソリューション用変更サブスクリプション・オブジェクトの作成

タスク 1: 初期ブートストラップの実行

ローカル・ディレクトリと Oracle Internet Directory 間のデータを同期化するためにディレクトリをブートストラップする手順は、次のとおりです。

1. Oracle Internet Directory に記録されている最後の変更番号を検索します。この番号は、DSE ルート属性の `lastChangeNumber` にあります。

   Oracle Internet Directory に記録されている最後の変更番号を検索するには、`ldapsearch` コマンドを使用します。次のコマンドを入力します。

   ```
   ldapsearch -h host_name -p port_number -s base -b "" 'objectclass=*'
   lastchangenumber
   ```

   変更ログがすでにパージされているために変更エントリがない場合、取得される変更番号は `0`（ゼロ）になります。

2. `ldifwrite` コマンドを使用して、データを Oracle Internet Directory から LDIF ファイルにエクスポートします。

3. この LDIF ファイルをクライアント・ディレクトリに適した形式に変換し、クライアント・ディレクトリにロードします。

注意： Oracle Internet Directory の新規インストールでは、初期ブートストラップは不要です。この場合、新規にインストールした Oracle Internet Directory の現行の変更番号は 0（ゼロ）です。

関連資料：『Oracle Identity Management ユーザー・リファレンス』の Oracle Internet Directory データ管理ツールの章の ldifwrite に関する項

タスク 2: Oracle Internet Directory でのサード・パーティのメタディレクトリ・ソリューション用変更サブスクリプション・オブジェクトの作成

サード・パーティのメタディレクトリ・ソリューションが Oracle Internet Directory と同期するには、Oracle Internet Directory にそのソリューション用の変更サブスクリプション・オブジェクトを作成する必要があります。この変更サブスクリプション・オブジェクトによって、Oracle Internet Directory に格納されている変更ログ・オブジェクトへのアクセス権限がサード・パーティのメタディレクトリ・ソリューションに付与されます。

変更サブスクリプション・オブジェクトの概要

変更サブスクリプション・オブジェクトは、Oracle Internet Directory の次のコンテナの下にあるエントリです。

```
cn=Subscriber Profile,cn=ChangeLog Subscriber,cn=Oracle Internet Directory
```

この変更サブスクリプション・オブジェクトは、サード・パーティのメタディレクトリ・ソリューションが Oracle Internet Directory とバインドして変更を取得するための一意の資格証明を提供します。管理者は、この変更サブスクリプション・オブジェクトを補助型オブジェクト・クラスの orclChangeSubscriber に関連付けます。このオブジェクト・クラスにはいくつかの属性があります。次の属性は必須です。

- userPassword

  Oracle Internet Directory の変更ログ・オブジェクトにアクセスするときに、ディレクトリが使用するパスワード。

- orclLastAppliedChangeNumber

  前回の同期で適用された変更番号。この属性によって、ディレクトリは、Oracle Internet Directory での変更から未適用の変更のみを取得できます。

変更サブスクリプション・オブジェクトの作成

変更サブスクリプション・オブジェクトの作成には、ldapadd コマンドを使用します。次の例では、入力ファイル add.ldif を使用して、cn=Subscriber Profile,cn=ChangeLog Subscriber,cn=Oracle Internet Directory コンテナの下に変更サブスクリプション・オブジェクト my_change_subscription_object を作成し、このオブジェクトを使用可能にします。orclLastAppliedChangeNumber 属性は、初期ブートストラップ前のディレクトリにある現行の変更番号で、この例では 250 です。

- add.ldif ファイルの編集：

```
dn: cn=my_change_subscription_object,cn=Subscriber Profile,
  cn=ChangeLog Subscriber,cn=Oracle Internet Directory
userpassword: my_password
orclLastAppliedChangeNumber: 250
orclSubscriberDisable: 0
objectclass: orclChangeSubscriber
objectclass: top
```

- エントリの追加：

```
ldapadd -h my_host -p 389 -f add.ldif
```

関連項目： 変更サブスクリプション・オブジェクトを一時的に使用禁止にする方法、または削除する方法については、11-5 ページの「変更サブスクリプション・オブジェクトの無効化と削除」を参照してください。

同期プロセス

この項の内容は次のとおりです。

- 接続ディレクトリで初めて Oracle Internet Directory から変更を取得する方法
- 接続ディレクトリで Oracle Internet Directory 内の orclLastAppliedChangeNumber 属性を更新する方法

接続ディレクトリで初めて Oracle Internet Directory から変更を取得する方法

次の例では、my_change_subscription_object という名前の変更サブスクリプション・オブジェクトを持つ接続ディレクトリが Oracle Internet Directory から変更を取得します。

```
ldapsearch -h my_host -p 389 -b "cn=changeLog" -s one
(&(objectclass=changeLogEntry)
(changeNumber >= orclLastAppliedChangeNumber )
( ! (modifiersname =cn=my_change_subscription_object,cn=Subscriber Profile,
     cn=ChangeLog Subscriber,cn=Oracle Internet Directory ) ) )
```

ディレクトリで初めて変更を取得する場合、orclLastAppliedChangeNumber の値は、11-3 ページの「タスク 2: Oracle Internet Directory でのサード・パーティのメタディレクトリ・ソリューション用変更サブスクリプション・オブジェクトの作成」で設定した数値です。

フィルタ内の（!(modifiersname=*client_bind_dn*)）引数によって、Oracle Internet Directory からは、接続ディレクトリ自体で行われた変更は返されません。

接続ディレクトリで Oracle Internet Directory 内の orclLastAppliedChangeNumber 属性を更新する方法

Oracle Internet Directory から変更を取得した後、接続ディレクトリでは、Oracle Internet Directory 内の対応する変更サブスクリプション・オブジェクトの orclLastAppliedChangeNumber 属性を更新します。この更新によって、Oracle Internet Directory は、接続ディレクトリで適用済の変更をパージできます。また、この更新によって、接続ディレクトリは、適用済の変更を無視して最新の変更のみを取得できます。

次の例では、接続ディレクトリに my_change_subscription_object という名前の変更サブスクリプション・オブジェクトがあり、前回適用した変更番号が 121 の入力ファイル mod.ldif を使用します。この接続ディレクトリでは、Oracle Internet Directory 内の対応する変更サブスクリプション・オブジェクトの orclLastAppliedChangeNumber を次のように更新します。

1. mod.ldif ファイルの編集：

   ```
   dn: cn=my_change_subscription_object,cn=Subscriber Profile,
       cn=ChangeLog Subscriber,cn=Oracle Internet Directory
   changetype:modify
   replace: orclLastAppliedChangeNumber
   orclLastAppliedChangeNumber: 121
   ```

2. ldapmodify コマンドを使用した編集済 mod.ldif ファイルのロード：

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

   関連資料： 変更番号に応じた変更のパージについては、『Oracle Internet Directory 管理者ガイド』のガベージ・コレクションに関する章を参照してください。

変更サブスクリプション・オブジェクトの無効化と削除

既存の変更サブスクリプション・オブジェクトは、一時的に使用禁止にすることも、削除することもできます。この項の内容は次のとおりです。

変更サブスクリプション・オブジェクトの無効化

サード・パーティのメタディレクトリ・ソリューションにある既存の変更サブスクリプション・オブジェクトを一時的に使用禁止にする場合は、`orclSubscriberDisable` 属性を 1 に設定します。次の例では、入力ファイル mod.ldif を使用して、変更サブスクリプション・オブジェクトを使用禁止にします。

- mod.ldif ファイルの編集 :

```
dn: cn=my_change_subscription_object,cn=Subscriber Profile,
    cn=ChangeLog Subscriber,cn=Oracle Internet Directory
changetype: modify
replace: orclSubscriberDisable
orclSubscriberDisable: 1
```

- エントリの変更 :

```
ldapmodify -h my_ldap_host -p 389 -v -f mod.ldif
```

変更サブスクリプション・オブジェクトの削除

変更サブスクリプション・オブジェクトの削除には、`ldapdelete` コマンドを使用します。次のコマンドを入力します。

```
ldapdelete -h ldap_host -p ldap_port
           "cn=my_change_subscription_object,cn=Subscriber Profile,
            cn=ChangeLog Subscriber,cn=Oracle Internet Directory"
```

第 IV 部

Oracle Directory Integration Platform によるプロビジョニング

第 IV 部では、プロビジョニングと、アプリケーションがユーザー・エントリまたはグループ・エントリ、あるいは追跡の必要な属性に対する変更を受信するために使用するプロセスに関する概念やコンポーネントについて説明します。次の各章で構成されています。

12

Oracle Directory Integration Platform Service の概要

10*g*（10.1.4.0.1）の時点で、異なる使用例について最適化された 2 つの補完的プロビジョニング製品が提供されています。

- Oracle Identity Manager（以前の Oracle Xellerate Identity Provisioning）: ディレクトリ、データベース、メインフレーム、独自のテクノロジ、フラット・ファイルなどを含む高度な異種テクノロジによる複合環境の管理を目的として設計されたエンタープライズ・プロビジョニング・プラットフォームです。Oracle Identity Manager では、豊富な一連の監査およびコンプライアンス機能とともに、フル装備のワークフローおよびポリシー機能を提供します。
- Oracle Directory Integration Platform（Identity Management インフラストラクチャのコンポーネント）: ディレクトリ中心の環境でディレクトリ同期だけでなくプロビジョニング・タスクも実行するように設計されたメタディレクトリ・テクノロジです。Oracle Directory Integration Platform は、ディレクトリや互換性のある Oracle 製品で構成される、より同質的な環境を管理できるように設計されています。Oracle Directory Integration Platform では、データ同期を使用してプロビジョニング・タスクを実行し、ワークフローやフル機能のポリシー・エンジンが不要な場合には小規模な配置フットプリントを提供します。

この章では、Oracle Directory Integration Platform について説明します。内容は次のとおりです。

関連資料：

- 『Oracle Identity Management アプリケーション開発者ガイド』のプロビジョニング統合アプリケーションの開発に関する章
- C-19 ページの「プロビジョニングに関するトラブルシューティング」

プロビジョニングの概要

プロビジョニングとは、ユーザー、グループ、およびその他のオブジェクトに対し、エンタープライズ環境で使用する可能性のあるアプリケーションや他のリソースへのアクセスを提供するプロセスです。プロビジョニング統合アプリケーションとは、プロビジョニング・イベントに対応できるよう、Oracle Internet Directory にプロビジョニング統合プロファイルが登録されているアプリケーションです。アプリケーション固有のディレクトリにあるすべてのユーザー・エントリを Oracle Internet Directory のエントリと同期化するだけでなく、特定のアプリケーションをプロビジョニングしてエントリの一部のみに関する通知を受信することが可能です。たとえば、Oracle Human Resources 用のディレクトリには、通常、企業のすべての従業員に関するデータが含まれており、一般的にはそのデータすべてを Oracle Internet Directory と同期します。ただし、他のアプリケーション（Oracle Email など）をプロビジョニングして、メンバーが特定グループに加入するか、そのグループから脱退した場合にのみ通知を受けることも可能です。

Oracle Identity Management の配置でアプリケーションにユーザー・アカウントをプロビジョニングするには、まずそのアカウントを Oracle Internet Directory に作成しておく必要があります。ユーザー・アカウントは、次のツールまたは方法のいずれかを使用して Oracle Internet Directory に作成します。

- Oracle Internet Directory プロビジョニング・コンソール
- Directory Integration アシスタントの `bulkprov` 操作
- サード・パーティ・ディレクトリとの同期
- LDAP コマンドライン・ツール

Oracle Directory Integration Platform Service は、Oracle Internet Directory でのユーザー・エントリの作成方法にかかわらず、任意のエントリに対して起動できます。ただし、Oracle Internet Directory にユーザー・エントリを作成すれば、Oracle Identity Management 環境のすべてのアプリケーションにアクセスできるわけではありません。ユーザー・アカウントは、管理者が手動でプロビジョニングするか、アプリケーションのプロビジョニング・ポリシーに従って自動でプロビジョニングする必要があります。アプリケーションのデフォルト・プロビジョニング・ポリシーは、次のいずれかです。

- すべてのユーザーをプロビジョニングします。
- ユーザーをプロビジョニングしません。
- プロビジョニング・ポリシーの評価後にユーザーをプロビジョニングします。

プロビジョニング・ポリシーは、エンタープライズ環境ごとの要件に全面的に依存します。たとえば、ある組織では、すべてのユーザーを電子メール・アプリケーションにアクセスできるようプロビジョニングする一方で、人事管理アプリケーションにアクセス可能なプロビジョニング・ユーザーを制限することが可能です。

Oracle Directory Integration Platform Service の構成要素

Oracle Directory Integration Platform Service の構成要素は、次のとおりです。

- Oracle Directory Integration Server

  関連項目： 第 4 章「Oracle Directory Integration Platform の管理」

- Oracle Internet Directory プロビジョニング・コンソール。これは、Oracle Delegated Administration Services を使用して作成された、すぐに使用できるスタンドアロン・アプリケーションです。プロビジョニング・コンソールは、Oracle Directory Integration Platform 管理ツールと密接に連携して動作します。

  関連資料：

  - 第 14 章「Oracle Internet Directory プロビジョニング・コンソールによる管理」
  - 『Oracle Identity Management 委任管理ガイド』

- プロビジョニング統合プロファイル。これは、ユーザーのプロビジョニング対象となるプロビジョニング統合アプリケーションごとに存在します。プロビジョニング統合プロファイルは、プロビジョニング・サブスクリプション・ツールを使用して作成します。

  関連資料： プロビジョニング・サブスクリプション・ツールの詳細は、『Oracle Identity Management ユーザー・リファレンス』の Oracle Directory Integration Platform ツールの章の `oidprovtool` に関する項を参照してください。

プロビジョニング概念の概要

この項では、Oracle Directory Integration Platform でアプリケーションがどのようにプロビジョニングされるかについて説明します。内容は次のとおりです。

- 同期プロビジョニング
- 非同期プロビジョニング
- プロビジョニングのデータ・フロー

同期プロビジョニング

プロビジョニング統合アプリケーションでは、Oracle Internet Directory またはサード・パーティ・リポジトリでユーザー情報を管理できます。Oracle Internet Directory でユーザー情報を管理するアプリケーションでは、データ・アクセス Java プラグインを使用して、Oracle Internet Directory に変更が発生するたびにユーザー・エントリを作成、変更および削除できます。

関連資料： データ・アクセス Java プラグインの詳細は、『Oracle Identity Management アプリケーション開発者ガイド』を参照してください。

データ・アクセス Java プラグインは、Oracle Identity Management（プロビジョニング・コンソールなど）、Directory Integration アシスタント（`dipassistant`）によるバルク・プロビジョニング、および LDAP コマンドライン・ツールから直接起動できます。このため、データ・アクセス Java プラグインでプロビジョニング可能なアプリケーションは、同期的にプロビジョニングされます。したがって、個別のプロビジョニング・イベントを Oracle Directory Integration Server からアプリケーションに送信する必要はありません。データ・アクセス Java プラグインは、Oracle Directory Integration Server に対して `SUCCESS` または `FAILURE` のいずれかを返します。データ・アクセス Java プラグインで `SUCCESS` の実行ステータスが返される場合、プロビジョニング・ステータスも返されます。このステータスは、特定のプロビジョニング統合アプリケーション用として、Oracle Internet Directory にあるユーザーのプロビジョニング・ステータス属性に記録されます。新規のユーザー・プロビジョニング・リクエストに対

して FAILURE のステータスが返された場合、ユーザーのプロビジョニング・ステータスには、PROVISIONING_FAILURE という値が割り当てられます。プロビジョニング・ステータスのリストは、12-10 ページの「Oracle Internet Directory のプロビジョニング・ステータス」を参照してください。

図 12-1 に、プロビジョニング・コンソール、Directory Integration アシスタント（dipassistant）によるバルク・プロビジョニング、およびサード・パーティ・ディレクトリを使用してアプリケーションが同期的にプロビジョニングされる場合のプロセスを示します。

図 12-1 同期プロビジョニング・プロセス

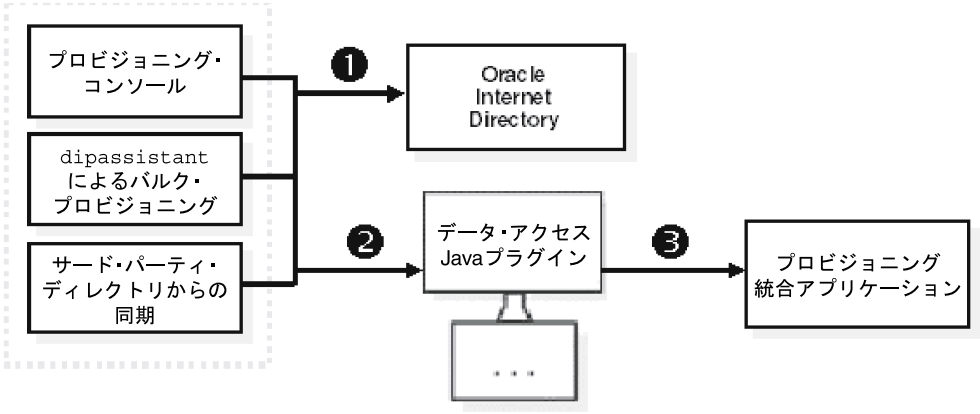


図 12-1 に示されているとおり、プロビジョニング・コンソール、Directory Integration アシスタント（dipassistant）によるバルク・プロビジョニング、およびサード・パーティ・ディレクトリを使用した Oracle Directory Integration Platform Service の同期プロビジョニングは、次のプロセスに従います。

1. 次のソースのいずれかに基づいて、Oracle Internet Directory に新規ユーザー・エントリが作成されます。
   - Oracle Internet Directory プロビジョニング・コンソール
   - Directory Integration アシスタントによるバルク・プロビジョニング
   - サード・パーティ・ディレクトリとの同期
2. 新規ユーザー・エントリを作成した Oracle Identity Management コンポーネントは、データ・アクセス Java プラグインを起動します。
3. データ・アクセス Java プラグインは、アプリケーションに新規ユーザー・アカウントをプロビジョニングします。

図 12-2 に、LDAP コマンドライン・ツールを使用してアプリケーションが同期的にプロビジョニングされる場合のプロセスを示します。

図 12-2 LDAP コマンドライン・ツールによる同期プロビジョニング

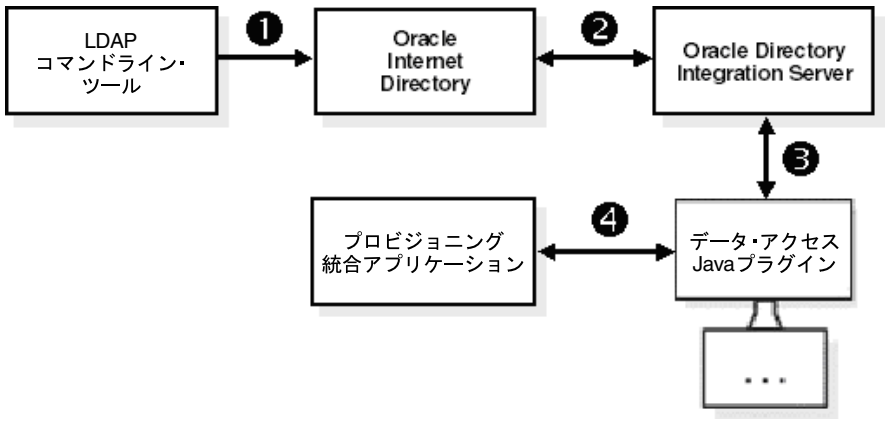


図 12-2 に示されているとおり、LDAP コマンドライン・ツールを使用した同期プロビジョニングは、次のプロセスに従います。

1. LDAP コマンドライン・ツールによって、Oracle Internet Directory に新規ユーザー・エントリが作成されます。
2. 次にスケジュールされた同期間隔で、Oracle Directory Integration Server は、プロビジョニングの必要な新規ユーザー・エントリが Oracle Internet Directory に存在することを確認します。
3. Oracle Directory Integration Server は、データ・アクセス Java プラグインを起動します。
4. データ・アクセス Java プラグインは、アプリケーションに新規ユーザー・アカウントをプロビジョニングします。

非同期プロビジョニング

Oracle Directory Integration Server は、PL/SQL イベントをプロビジョニング統合アプリケーションに伝播します。次に、プロビジョニング統合アプリケーションは、イベントを処理するために PL/SQL プラグインを実行します。PL/SQL プラグインの実行は、アプリケーション・リポジトリ内で発生し、任意の Oracle Identity Management コンポーネントのアドレス空間では発生しません。プロビジョニングは、任意の Oracle Identity Management コンポーネントではなく PL/SQL プラグインによって処理されるため、PL/SQL プラグインを実装するプロビジョニング統合アプリケーションは、非同期的にプロビジョニングされます。PL/SQL プラグインは、Oracle Directory Integration Server に対して `SUCCESS` または `FAILURE` というステータスを返します。PL/SQL プラグインで `SUCCESS` のステータスが返される場合、プロビジョニング・ステータスも返されます。このステータスは、特定のプロビジョニング統合アプリケーション用として、Oracle Internet Directory にあるユーザーのプロビジョニング・ステータス属性に記録されます。新規のユーザー・プロビジョニング・リクエストに対して `FAILURE` のステータスが返された場合、ユーザーのプロビジョニング・ステータスには、`PROVISIONING_FAILURE` という値が割り当てられます。プロビジョニング・ステータスのリストは、12-10 ページの「Oracle Internet Directory のプロビジョニング・ステータス」を参照してください。

図 12-3 に、プロビジョニング・コンソール、Directory Integration アシスタント（dipassistant）によるバルク・プロビジョニング、およびサード・パーティ・ディレクトリを使用してアプリケーションが非同期的にプロビジョニングされる場合のプロセスを示します。

図 12-3 非同期プロビジョニング・プロセス

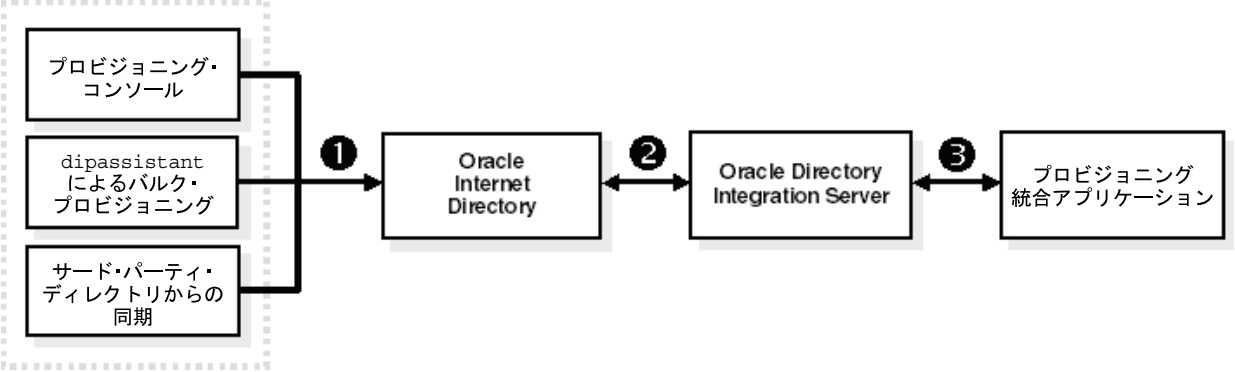


図 12-3 に示されているとおり、プロビジョニング・コンソール、Directory Integration アシスタント（dipassistant）によるバルク・プロビジョニング、およびサード・パーティ・ディレクトリを使用した非同期プロビジョニングは、次のプロセスに従います。

1. 次のソースのいずれかに基づいて、Oracle Internet Directory に新規ユーザー・エントリとアプリケーション固有のユーザー・プリファレンスを含む関連エントリが作成されます。
   - Oracle Internet Directory プロビジョニング・コンソール
   - Directory Integration アシスタントによるバルク・プロビジョニング
   - サード・パーティ・ディレクトリとの同期
2. 次にスケジュールされた同期間隔で、Oracle Directory Integration Server は、プロビジョニングの必要な新規ユーザー・エントリが Oracle Internet Directory に存在することを確認します。
3. Oracle Directory Integration Server から PL/SQL プラグインにプロビジョニング・イベントが送信されます。

図 12-4 に、LDAP コマンドライン・ツールを使用してアプリケーションが非同期的にプロビジョニングされる場合のプロセスを示します。

図 12-4 LDAP コマンドライン・ツールによる非同期プロビジョニング

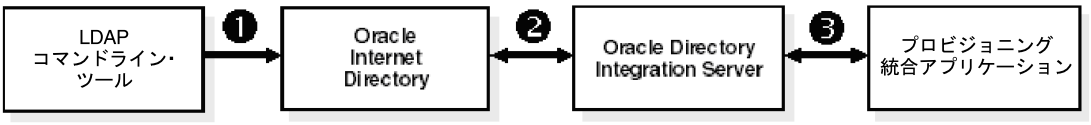


図 12-4 に示されているとおり、LDAP コマンドライン・ツールを使用した非同期プロビジョニングは、次のプロセスに従います。

1. LDAP コマンドライン・ツールを使用して、Oracle Internet Directory に新規ユーザー・エントリが作成されます。
2. 次にスケジュールされた同期間隔で、Oracle Directory Integration Server は、プロビジョニングの必要な新規ユーザー・エントリが Oracle Internet Directory に存在することを確認し、アプリケーション固有のユーザー・プリファレンスを含む関連エントリを作成します。
3. Oracle Directory Integration Server から PL/SQL プラグインにプロビジョニング・イベントが送信されます。

プロビジョニングのデータ・フロー

プロビジョニングが同期的か非同期的かにかかわらず、アプリケーションでは、プロビジョニング・インテリジェンス機能を拡張してビジネス・ポリシーを実装するために、プレデータ・エントリ・プラグインとポストデータ・エントリ・プラグインを起動できます。どちらのプラグインも、Oracle Internet Directory プロビジョニング・コンソールなどの Oracle Identity Management コンポーネントや、Directory Integration アシスタント（`dipassistant`）によるバルク・プロビジョニングによって起動されます。

プレデータ・エントリ・プラグインは、プロビジョニング・ポリシーに基づいてフィールドの移入を行います。このプラグインの主な目的は、アプリケーションにユーザーをプロビジョニングするかどうかを決定することです。たとえば、財務管理アプリケーションにはマネージャのみをプロビジョニングするというポリシーを持つ組織の場合、プレデータ・エントリ・プラグインを使用することで、どのユーザー・エントリをプロビジョニングするかを判別できます。共通のユーザー属性はこのプラグインの起動時にすでに移入されているため、プロビジョニングの決定を行うための十分な情報がすでに存在していることになります。

ポストデータ・エントリ・プラグインは、主に、ユーザーによって入力された共通属性とアプリケーション固有属性に関するデータを検証します。プロビジョニングを続けるためには、このプラグインでの検証に成功する必要があります。

図 12-5 に、プレデータ・エントリおよびポストデータ・エントリ・プラグインを使用したプロビジョニングのデータ・フローを示します。

図 12-5 プロビジョニングのデータ・フロー

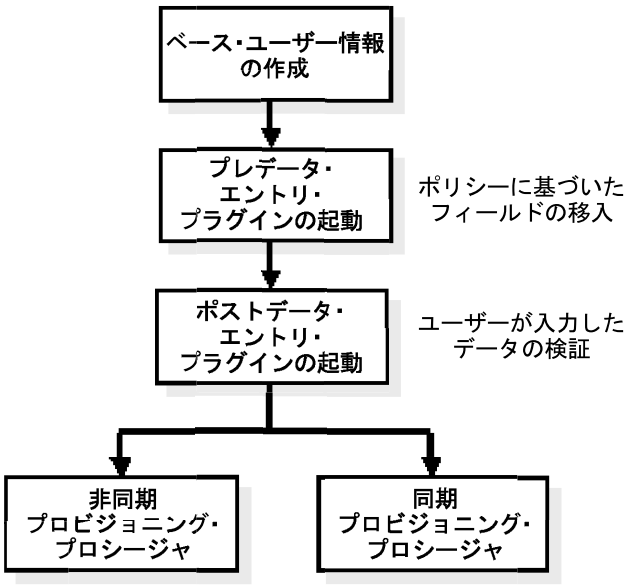


図 12-5 に示されているとおり、プロビジョニングのデータ・フローは、次のプロセスに従います。

1. ベース・ユーザー情報が作成されます。
2. プレデータ・エントリ・プラグインが起動し、ポリシーに基づいてフィールドの移入が行われます。
3. ポストデータ・エントリ・プラグインが起動し、ユーザーが入力したデータが検証されます。
4. プロビジョニング方式に応じて、非同期または同期プロビジョニング・プロシージャが起動します。

プロビジョニング・コンソールでプロビジョニングを実行する場合、管理者は、プレデータ・エントリ・プラグインが起動した後で、ポストデータ・エントリ・プラグインが起動する前にアプリケーション属性を変更できます。

プロビジョニング方式の概要

この項では、Oracle Identity Management でユーザーをプロビジョニングする手順について説明します。内容は次のとおりです。

- プロビジョニング・コンソールによるユーザーのプロビジョニング
- 外部ソースから同期化されたユーザーのプロビジョニング
- LDAP コマンドライン・ツールで作成されたユーザーのプロビジョニング
- バルク・プロビジョニング
- オンデマンド・プロビジョニング
- アプリケーション・ブートストラップ

プロビジョニング・コンソールによるユーザーのプロビジョニング

プロビジョニング・コンソールを使用すると、1 人以上のユーザーのプロビジョニングおよびプロビジョニング解除を同時に集中管理できます。このコンソールには、個別ユーザーを作成、変更および削除する場合と、任意のプロビジョニング統合アプリケーションに対してユーザーを選択的にプロビジョニングおよびプロビジョニング解除する場合に役立つウィザードベースのインタフェースがあります。プロビジョニング・コンソールは、LDIF ファイルを使用したユーザーのバルク作成、変更および削除にも対応しています。詳細は、12-8 ページの「バルク・プロビジョニング」を参照してください。

外部ソースから同期化されたユーザーのプロビジョニング

Oracle Internet Directory が中央リポジトリとして使用され、エンタープライズ・ユーザー・エントリがサード・パーティ・ディレクトリから Oracle Internet Directory に同期化される場合、各ユーザー ID は、プロビジョニング統合アプリケーションごとのデフォルト・プロビジョニング・ポリシーに従って自動的にプロビジョニングされます。

LDAP コマンドライン・ツールで作成されたユーザーのプロビジョニング

オラクル社、または標準の LDAP コマンドライン構文を利用するサード・パーティ・ベンダーによって開発された任意のツールを使用して、Oracle Internet Directory にユーザー・エントリを作成できます。外部ソースから同期化されたユーザー・エントリの場合と同様に、LDAP コマンドライン・ツールまたはその他の方法によって作成されたユーザー・エントリは、プロビジョニング統合アプリケーションごとのデフォルト・プロビジョニング・ポリシーに従ってプロビジョニングされます。

バルク・プロビジョニング

プロビジョニング・コンソールまたは Directory Integration アシスタント（`dipassistant`）では、ユーザー・データを含む LDAP Data Interchange Format（LDIF）ファイルを指定することでユーザー・エントリを作成およびプロビジョニングできます。LDIF ファイルには、LDAP 固有の属性のみが含まれている必要があります。LDIF ファイルのユーザー・エントリが Oracle Internet Directory に作成される場合、各エントリは、プロビジョニング統合アプリケーションごとのデフォルト・プロビジョニング・ポリシーに従ってプロビジョニングされます。

オンデマンド・プロビジョニング

オンデマンド・プロビジョニングは、ユーザーがアプリケーションにアクセスし、そのアプリケーションのリポジトリにユーザーの情報が存在しない場合に発生します。アプリケーションは、デフォルト・プロビジョニング・ポリシーに基づいてユーザー・アカウントをプロビジョニングするかどうかを決定します。リポジトリにユーザー・アカウントをプロビジョニングした後、アプリケーションは、Oracle Internet Directory のユーザー・エントリのプロビジョニング・ステータスを更新します。

アプリケーション・ブートストラップ

Oracle Directory Integration Platform Service は、新規登録されたアプリケーションに Oracle Internet Directory のすべての既存ユーザー・エントリを通知し、各既存ユーザー・エントリをアプリケーションの新規ユーザーであるかのようにプロビジョニングします。

Oracle Internet Directory のユーザー・プロファイルの構成

この項では、Oracle Internet Directory のユーザー・プロファイルの構成について説明します。内容は次のとおりです。

- ディレクトリ情報ツリーのプロビジョニング・エントリの構成
- ユーザー・プロビジョニング・ステータスの概要

ディレクトリ情報ツリーのプロビジョニング・エントリの構成

Oracle Directory Integration Platform は、個人情報と、ユーザーがプロビジョニングされる様々なアプリケーション用の設定を含む属性で構成されるディレクトリ情報ツリー（DIT）のユーザー・プロファイルに依存します。Oracle Directory Integration Platform Service のこれらのユーザー属性は、次のように分類されます。

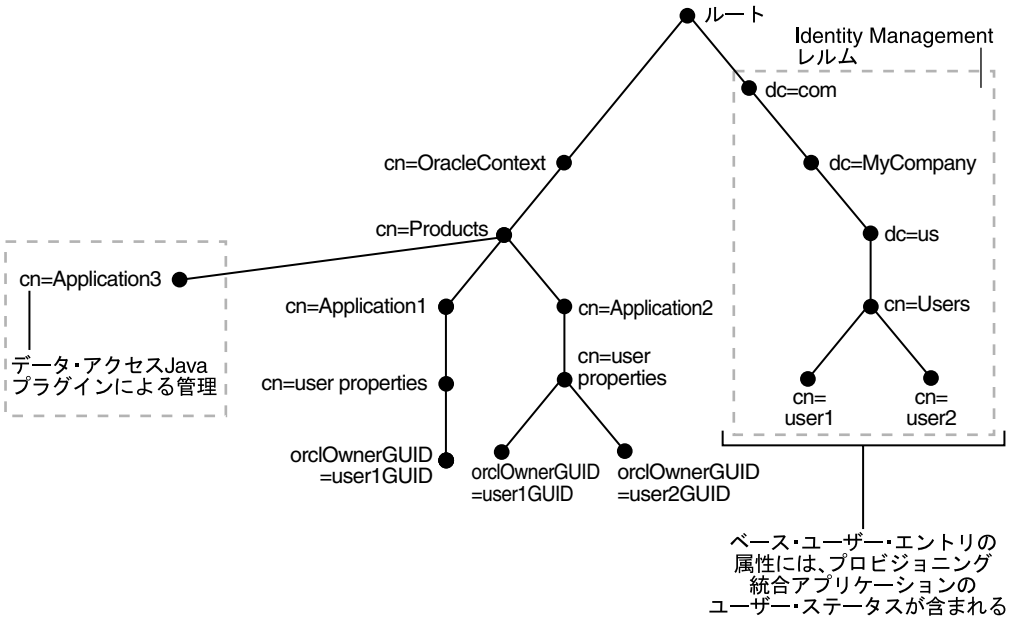
- すべてのユーザー・エントリで使用されるベース属性
- ユーザーがアプリケーションにプロビジョニングされる場合にのみ使用されるアプリケーション固有属性

ベース・ユーザー属性は、主に `organizationalPerson` や `inetOrgPerson` などの標準 LDAP オブジェクト・クラスに属し、氏名、電子メール・アドレスおよび電話番号を含む個人の詳細情報で構成されます。ベース・ユーザー属性は、`orclUserV2` 補助クラスに属する Oracle アプリケーション固有の属性でも構成されます。

Oracle Internet Directory は、ベース属性とアプリケーション固有属性のプライマリ・リポジトリです。どちらのタイプの属性も、各ユーザーのプロファイルに格納されます。ただし、アプリケーションでは、プロビジョニング・イベント通知サービスで更新されるユーザー属性がキャッシュされる場合があります。図 12-6 に示されているとおり、ユーザー属性は、DIT 内の 2 つの場所に格納されます。`inetorgperson` および `orcluserv2` に属する属性を含むベース・ユーザー・エントリは、`cn=users,`*`Realm DN`* の下に格納されます。各ユーザー・エントリのプロビジョニング・ステータスも、ベース・ユーザー・エントリに格納されます。アプリケーション固有属性は、アプリケーション・コンテナの個別エントリに含まれます。アプリケーション固有属性の定義に関連する LDAP スキーマとオブジェクト・クラスは、インストール・プロセスまたはアップグレード・プロセス中に作成されます。アプリケーション固有属性は、補助オブジェクト・クラスによって修飾されます。これにより、そのエントリのアプリケーション固有ユーザーのプロパティを検索できます。デフォルトでは、アプリケーション固有エントリは、`cn=User Properties,cn=`*`Application Type`*`,cn=Products,cn=OracleContext,`*`Realm DN`* コンテナに `orclOwnerGUID=`*`GUID of the Base User`* として格納されます。

一部のアプリケーションは、独自のアプリケーション属性を管理し、データ・アクセス Java プラグインを実装します。詳細は、12-3 ページの「プロビジョニング概念の概要」を参照してください。Oracle Directory Integration Platform Service では、ベース・ユーザー属性またはアプリケーション固有属性が変更されると、必ずこのプラグインが起動されます。

図 12-6 ベース・ユーザー属性とアプリケーション固有属性



ユーザー・プロビジョニング・ステータスの概要

この項では、Oracle Internet Directory のユーザー・プロビジョニング・ステータスについて説明します。内容は次のとおりです。

- Oracle Internet Directory のプロビジョニング・ステータス
- プロビジョニング・ステータスの遷移
- アップグレードと共存プロビジョニング・ステータス
- プロビジョニング・ステータスと例外処理

Oracle Internet Directory のプロビジョニング・ステータス

Oracle プロビジョニング・サービスでは、プロビジョニング統合アプリケーションごとに、Oracle Internet Directory にユーザーのプロビジョニング・ステータスが記録されます。プロビジョニング・ステータスは、Oracle Directory Integration Server、Directory Integration アシスタント（`dipassistant`）によるバルク・プロビジョニング、またはプロビジョニング統合アプリケーションによって設定されます。表 12-1 に、プロビジョニング・ステータスのリストを示します。

表 12-1 Oracle Internet Directory のプロビジョニング・ステータス

内部ステータス	GUI ステータス	説明
プロビジョニング・ステータス		
PROVISIONING_REQUIRED	保留	プロビジョニングが必要です。このステータスは、管理者が選択するか、アプリケーションのプロビジョニング・ポリシーに従って設定されます。このステータスにより、ユーザーがプロビジョニングされているかどうかが決定することに注意してください。
PROVISIONING_IN_PROGRESS	進行中	プロビジョニングが進行中です。スケジュールされた間隔でアプリケーションによりプロビジョニングが実行される場合、現行のステータスがこのステータスであれば、ユーザーはアプリケーションにアクセスできます。アプリケーションでは、ユーザーをオンデマンドでプロビジョニングすることが可能です。
PROVISIONING_SUCCESSFUL	成功	プロビジョニングに成功しました。このステータスは、Oracle Directory Integration Server、Directory Integration アシスタント（dipassistant）によるバルク・プロビジョニング、またはプロビジョニング統合アプリケーションによって自動的に更新されます。
PROVISIONING_NOT_REQUIRED	リクエストなし	プロビジョニングは必要ありません。このステータスは、管理者が選択するか、アプリケーションのプロビジョニング・ポリシーに従って設定されます。このステータスにより、ユーザーが今後プロビジョニングされるかどうかが決定することに注意してください。
PROVISIONING_FAILURE	失敗	プロビジョニングに失敗しました。このステータスは、Oracle Directory Integration Server、Directory Integration アシスタント（dipassistant）によるバルク・プロビジョニング、またはプロビジョニング統合アプリケーションによって自動的に更新されます。このステータスである場合、ユーザーはアプリケーションにアクセスできません。
プロビジョニング解除ステータス		
DEPROVISIONING_REQUIRED	プロビジョニング解除が保留中です	プロビジョニング解除が必要です。このステータスである場合、ユーザーはまだプロビジョニングされています。
DEPROVISIONING_IN_PROGRESS	プロビジョニング解除が進行中です	プロビジョニング解除が進行中です。
DEPROVISIONING_SUCCESSFUL	正常にプロビジョニング解除されました	プロビジョニング解除に成功しました。このステータスである場合、ユーザーはアプリケーションにアクセスできません。
DEPROVISIONING_FAILURE	プロビジョニング解除に失敗しました	プロビジョニング解除に失敗しました。このステータスである場合、ユーザーはまだプロビジョニングされています。
アップグレード・ステータス		
PENDING_UPGRADE	アップグレードが保留中です	プロビジョニングのアップグレードが保留中です。
UPGRADE_IN_PROGRESS	アップグレードが進行中です	プロビジョニングのアップグレードが進行中です。
UPGRADE_FAILURE	アップグレードに失敗しました	プロビジョニングのアップグレードに失敗しました。

各アプリケーションのプロビジョニング・ステータスは、ユーザー・エントリの orclUserApplnProvStatus 属性に格納されます。この属性は、Oracle Internet Directory で索引付けされており、検索可能です。プロビジョニング統合アプリケーションごとに、サブタイプの orclUserApplnProvStatus 属性が作成されます。たとえば、次の文には、電子メール・アプリケーションとスケジュール・アプリケーションに対するユーザーのプロビジョニング・ステータスが格納されています。電子メール・アプリケーションに対するユーザーのプロビジョニング・ステータスは PROVISIONING_SUCCESS ですが、スケジュール・アプリケーションに対するプロビジョニング・ステータスは PROVISIONING_FAILURE です。

```
orclUserApplnProvStatus;CORP-MAIL_E-MAIL:PROVISIONING_SUCCESS
orclUserApplnProvStatus;CORP-SCHEDULE_CALENDAR:PROVISIONING_FAILURE
```

アプリケーションでのユーザーのプロビジョニング・ステータスに関する追加情報は orclUserApplnProvStatusDesc 属性に格納され、各アプリケーションのプロビジョニング失敗アカウントは orclUserApplnProvFailureCount 属性に格納されます。orclUserApplnProvStatus 属性と同様に、プロビジョニング統合アプリケーションごとに個別の orclUserApplnProvStatusDesc および orclUserApplnProvFailureCount 属性が作成されます。orclUserApplnProvStatusDesc 属性の書式は orclUserApplnProvStatus 属性と同じですが、それ以外にタイムスタンプと説明的な情報がアプリケーションの名前とタイプの後に追加されます。たとえば、次のようになります。

```
orclUserApplnProvStatusDesc;CORP-MAIL_E-MAIL:20040101010101^Missing employee ID
```

orclUserApplnProvStatus、orclUserApplnProvStatusDesc および orclUserApplnProvFailureCount 属性は、オプション属性として orclUserProvStatus オブジェクト・クラスに格納されます。

プロビジョニング・ステータスの遷移

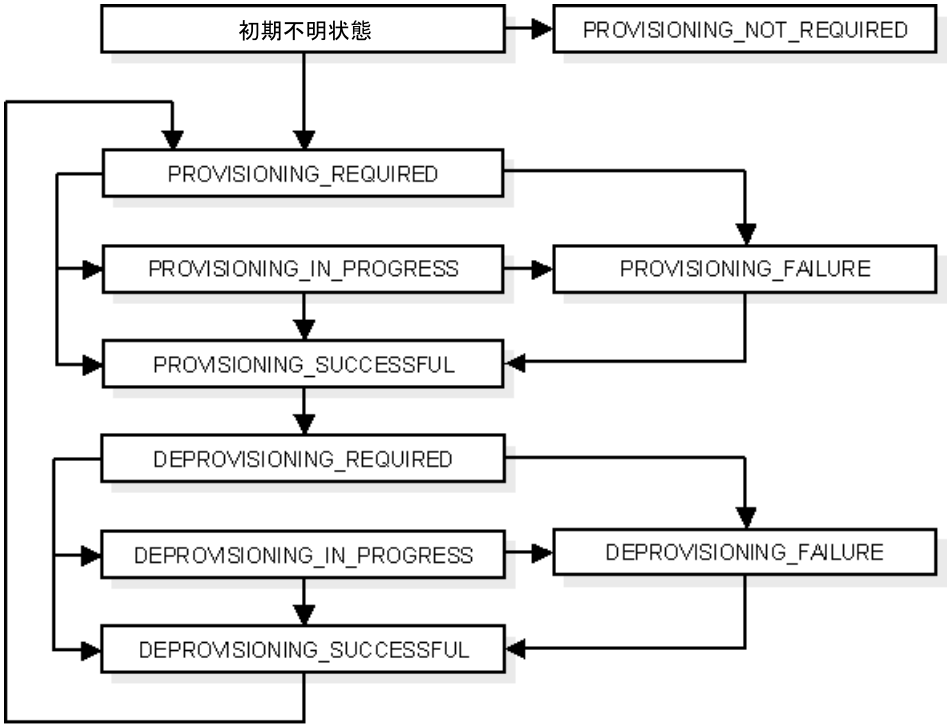
表 12-2 に、有効なプロビジョニング・ステータスの遷移を示します。

表 12-2 Oracle Internet Directory での有効なプロビジョニング・ステータスの遷移

内部ステータス	GUI ステータス	有効な遷移元
プロビジョニング・ステータス		
PROVISIONING_REQUIRED	保留	初期不明状態 DEPROVISIONING_SUCCESSFUL
PROVISIONING_IN_PROGRESS	進行中	PROVISIONING_REQUIRED
PROVISIONING_SUCCESSFUL	成功	PROVISIONING_REQUIRED PROVISIONING_IN_PROGRESS PROVISIONING_FAILURE
PROVISIONING_NOT_REQUIRED	リクエストなし	初期不明状態
PROVISIONING_FAILURE	失敗	PROVISIONING_REQUIRED PROVISIONING_IN_PROGRESS
プロビジョニング解除ステータス		
DEPROVISIONING_REQUIRED	プロビジョニング解除が保留中です	PROVISIONING_SUCCESSFUL
DEPROVISIONING_IN_PROGRESS	プロビジョニング解除が進行中です	PROVISIONING_SUCCESSFUL
DEPROVISIONING_SUCCESSFUL	正常にプロビジョニング解除されました	DEPROVISIONING_REQUIRED DEPROVISIONING_IN_PROGRESS DEPROVISIONING_FAILURE
DEPROVISIONING_FAILURE	プロビジョニング解除に失敗しました	DEPROVISIONING_REQUIRED DEPROVISIONING_IN_PROGRESS

図 12-7 に、有効なプロビジョニング・ステータスの遷移を示します。

図 12-7 有効なプロビジョニング・ステータスの遷移



アップグレードと共存プロビジョニング・ステータス

Oracle Identity Management 10*g*（10.1.4.0.1）では、Oracle Internet Directory 内の 1 つのユーザー・エントリが、複数の LDAP エントリによって物理的に示されることがあります。ベース・ユーザー・エントリ以外に、プロビジョニング統合アプリケーションごとに複数の独立した LDAP エントリが存在する可能性があります。

Oracle Identity Management の通常のアップグレードでは、複数の中間層は同時にアップグレードされません。つまり、Oracle Identity Management のアップグレード後も、旧バージョンの中間層とアップグレード・バージョンの中間層を同時に実行する必要がある場合があります。中間層をアップグレードすると、アプリケーションのメタデータ・リポジトリに格納されていたユーザーのアプリケーション固有データは、すべて必要に応じて移行されます。Oracle Directory Integration Server は、アップグレード前から Oracle Internet Directory に存在しているユーザー・エントリごとに新規ユーザー・イベントを起動し、各エントリに `PENDING_UPGRADE` というプロビジョニング・ステータスを割り当てます。新規ユーザー・エントリが、古い中間層や一部のサポートされない手順（標準の LDAP SDK を使用した既存アプリケーションなど）によって作成されると、プロビジョニング・ステータス属性は失われます。この場合も、Oracle Directory Integration Server は、新規ユーザー・イベントを起動し、各ユーザー・エントリに `PENDING_UPGRADE` というプロビジョニング・ステータスを割り当てます。

イベントを受信したプロビジョニング統合アプリケーションは、ユーザーがプロビジョニングされているかどうかを示すレスポンスを Oracle Directory Integration Platform に返します。Oracle Directory Integration Platform は、そのレスポンスに従ってユーザー・エントリのプロビジョニング・ステータスを更新します。

プロビジョニング・ステータスと例外処理

プロビジョニング・コンソールで作成されたか、外部データソースとの同期により作成された新規ユーザー・エントリに、特定のアプリケーションでユーザーをプロビジョニングするために十分な情報が含まれていない場合、プロビジョニングが失敗する可能性があります。その他様々な理由によっても、プロビジョニングは失敗します。Oracle Directory Integration Platform Service では、ユーザー・プロビジョニングの失敗が例外として識別されます。

アプリケーションが USER_ADD イベントに対して失敗のステータスを示すレスポンスを返すと、Oracle Directory Integration Server は、ユーザーのプロビジョニング・ステータスを PROVISIONING_FAILURE に変更します。次に、Oracle Directory Integration Server は、新規ユーザーの場合と同様に、失敗した場合の通知をアプリケーションに送信します。これは、プロビジョニング・リクエストの再試行になります。

ユーザーのプロビジョニング・ステータスは、プロビジョニング・コンソールに表示されます。管理者は必要な変更を加えて問題を修正でき、プロビジョニングは自動的に再試行されます。同期プロビジョニングの場合、この結果としてデータ・アクセス・プラグインが起動されます。非同期プロビジョニングの場合、イベントが伝播されます。

この一連のステップは、ユーザーがプロビジョニングに成功するまで繰り返されます。

プロビジョニング・フローの概要

この項では、様々なプロビジョニング・シナリオでの情報および制御のフローについて説明します。内容は次のとおりです。

- プロビジョニング・コンソールでのユーザーの作成および変更
- プロビジョニング・コンソールでのユーザーの削除
- 外部ソースからのユーザー・プロビジョニング

プロビジョニング・コンソールでのユーザーの作成および変更

プロビジョニング・コンソールを使用して、Oracle Internet Directory に新規ユーザー・エントリを作成およびプロビジョニングできます。コンソールでは、ウィザードベースのインタフェースを使用して、次の手順を実行します。

1. 初期ユーザー作成画面に、必要なベース・ユーザー属性のリストが表示されます。ベース・ユーザー属性は、プロビジョニング・コンソールによるプレデータ・エントリ・プラグインの起動後に移入されます。ユーザー作成の場合、プラグインによってベース・ユーザー属性が処理され、アプリケーションのデフォルト・プロビジョニング・ポリシーおよび属性が生成されます。ユーザー変更の場合、プロビジョニング・コンソールにより Oracle Internet Directory のユーザー情報が取得され、プラグインによりアプリケーション情報が取得されます。
2. ウィザードの次のステップでは、アプリケーションのデフォルト・プロビジョニング・ポリシーに基づいて、各アプリケーションでのユーザーのプロビジョニング方法が表示されます。ユーザー変更の場合、このステップで、ユーザーが現在プロビジョニングされているアプリケーションのリストと、ユーザーをプロビジョニング可能なアプリケーションのリストが表示されます。ユーザーがまだプロビジョニングされていないアプリケーションには、次のいずれかの値を選択できます。
   - **ユーザー・ポリシー:** このフィールドの選択値は、各アプリケーションのデフォルト・プロビジョニング・ポリシーに基づきます。このフィールドには、「プロビジョニング」または「プロビジョニングしない」という 2 つの値のいずれかが表示されます。
   - **ポリシーを上書きしてプロビジョニングを実行する:** このオプションを選択すると、アプリケーションのデフォルト・ポリシーが上書きされ、ユーザーがプロビジョニングされます。
   - **ポリシーを上書きしてプロビジョニングを実行しない:** このオプションを選択すると、アプリケーションのデフォルト・ポリシーが上書きされ、ユーザーがプロビジョニングされません。

ユーザーが現在プロビジョニングされているアプリケーションでは、ユーザーのプロビジョニングを解除するオプションが表示されます。

3. ユーザーがプロビジョニングされていないアプリケーションでは、ウィザードの次のステップで、プレデータ・エントリ・プラグインから返されたデフォルト値とともにプロビジョニング対象のアプリケーションの属性が表示されます。ユーザーがプロビジョニングされているアプリケーションでは、現在のアプリケーション情報がリストされます。このステップでは、「**次へ**」をクリックする前に属性に必要な変更を加えることができます。「**次へ**」をクリックすると、ポストデータ・エントリ・プラグインが起動され、入力したデータが検証されます。
4. ウィザードの最後のステップでは、アプリケーション属性とその値を確認できます。「**終了**」をクリックします。「**終了**」をクリックすると、プロビジョニング・コンソールによって Oracle Internet Directory のユーザー情報が作成または更新されます。次に、同期的にプロビジョニングされるアプリケーション用のデータ・アクセス Java プラグインが起動され、アプリケーションが作成または更新されます。

プロビジョニング・コンソールでのユーザーの削除

ユーザーの削除前に、プロビジョニング・コンソールにベース・ユーザーとアプリケーション属性をリストした読取り専用ページが表示されます。ユーザーによる削除の確認後、プロビジョニング・コンソールによって、ベース・ユーザー情報とアプリケーション固有情報が削除されるか、同期的にプロビジョニングされるアプリケーション用のデータ・アクセス Java プラグインが起動されます。非同期アプリケーションの場合、`USER_DELETE` イベントが伝播されます。

外部ソースからのユーザー・プロビジョニング

配置では、多くの場合サード・パーティのエンタープライズ・ユーザー・リポジトリなどの外部ソースからユーザーをプロビジョニングすると予想されます。このようなタイプの配置では、サード・パーティ・リポジトリによって Oracle Internet Directory がブートストラップされます。Oracle Directory Integration Platform では、Oracle Internet Directory とサード・パーティ・リポジトリの間で継続的に同期が実行されます。サード・パーティ・ユーザー・リポジトリの例には、Oracle Human Resources や、Microsoft Active Directory、Sun Java System Directory、Novell eDirectory、OpenLDAP などの LDAP ディレクトリがあります。

Oracle Directory Synchronization Service により、Oracle Internet Directory にユーザー・エントリが作成されます。外部ソースから取得される情報は、様々なアプリケーションにユーザーをプロビジョニングするには不十分である可能性があるため、アプリケーション情報の作成にはアプリケーションのデフォルトが使用されます。Oracle Directory Synchronization Service では、次のようにユーザーが作成されます。

1. Oracle Directory Synchronization Service は、アプリケーションで指定されたプロビジョニング・ポリシーを評価し、ユーザーをアプリケーションにプロビジョニングするかどうかを決定します。
2. Oracle Directory Synchronization Service は、アプリケーションに登録されているその他のプラグインを評価します。
3. Oracle Directory Integration Platform Service は、PL/SQL プラグインまたはデータ・アクセス Java プラグインを起動して、ユーザー情報をアプリケーションに送信します。
4. イベント・インタフェースの使用により、アプリケーションからユーザーのプロビジョニング・ステータスが返されます。
5. Oracle Directory Integration Platform Service は、アプリケーション用のユーザーのプロビジョニング・ステータスを更新します。

管理権限の委任方法

Oracle Delegated Administration Services の管理権限は、各管理者に委任された権限に応じて異なります。管理者は、ユーザーの管理とプロビジョニング、およびアプリケーションの管理を行うための権限をすべて付与されるか、またはこれらの権限の組合せを付与されます。権限の使用例を次に示します。

プロビジョニング管理モデル

次のタイプのプロビジョニング情報は、Oracle Internet Directory で管理されます。

- ベース・ユーザー情報。
- アプリケーション固有情報。
- 各プロビジョニング統合アプリケーションのユーザー・プロビジョニング・ステータス。この情報は、ベース・ユーザー・エントリに格納されますが、個別に管理されます。

管理者とユーザーには、それぞれ次のタイプの権限が必要です。

- 管理者は、ベース・ユーザー属性とアプリケーション固有情報を管理するための権限が必要です。
- ユーザーは、自分自身のベース属性とアプリケーション固有情報を管理するための権限が必要です。

管理権限を保持するユーザー・アカウントは、`cn=User Provisioning Admins,cn=Groups,cn=OracleContext` というグループ・エントリによって示されます。アプリケーション固有情報を管理するため、アプリケーションでは、`cn=User Provisioning Admins,cn=Groups,cn=OracleContext` グループに権限を付与する必要があります。アプリケーションですでに管理権限を保持するグループを定義している場合は、その権限を保持するグループのメンバーとしてこのグループを追加する必要があります。

Oracle Delegated Administration Services 権限

Oracle Delegated Administration Services の管理権限を保持する管理者の場合、プロビジョニング・コンソールで「**作成**」、「**削除**」、「**編集**」の各ボタンが使用可能になり、ユーザーを作成、削除および変更できます。Oracle Delegated Administration Services の管理権限のみを保持する管理者がこれらのボタンのいずれかをクリックすると、その機能を実行するために単一ステップのプロシージャが使用されます。

プロビジョニング管理権限

プロビジョニング権限を保持する管理者の場合、プロビジョニング・コンソールで「**作成**」、「**削除**」、「**編集**」の各ボタンが使用可能になり、ユーザーを作成、削除および変更できます。ただし、プロビジョニング権限を保持する管理者の場合、Oracle Delegated Administration Services 権限を保持する管理者に使用される単一ステップのプロシージャではなく、ウィザードベースのプロシージャによって作成および変更処理は実行されます。ユーザーの削除は、12-16 ページの「Oracle Delegated Administration Services 権限」に説明のある Oracle Delegated Administration Services 権限の場合と同じ単一ステップのプロシージャに基づいて実行されます。

アプリケーション管理権限

Oracle Delegated Administration Services 権限やプロビジョニング権限ではなく、アプリケーション管理権限を保持する管理者の場合、プロビジョニング・コンソールで「**作成**」および「**削除**」ボタンは使用できません。ただし、「**編集**」ボタンはあります。このボタンをクリックすると、12-17 ページの「プロビジョニング管理権限」に説明のあるプロビジョニング管理権限の場合と同じウィザードが起動します。アプリケーション管理者がプロビジョニング権限を保持していない場合、一般的なユーザー・プロビジョニングに使用するウィザードの最初のページは、読取り専用になります。ただし、アプリケーション管理者でも、ウィザードの他のページに表示されるアプリケーション・プロビジョニング属性は変更できます。

Oracle Delegated Administration Services 権限とプロビジョニング管理権限

Oracle Delegated Administration Services 権限とプロビジョニング権限を保持する管理者は、12-17 ページの「プロビジョニング管理権限」に説明のあるプロビジョニング管理権限の場合と同じ権限を保持します。

アプリケーション管理権限と Oracle Delegated Administration Services 権限

この項では、管理者に様々な Oracle Delegated Administration Services 権限が割り当てられており、同時に管理権限も割り当てられている場合、各権限がどのように委任されるかについて説明します。

アプリケーション管理権限と Oracle Delegated Administration Services のユーザー作成権限

Oracle Delegated Administration Services のユーザー作成権限を保持し、ユーザー編集またはユーザー削除権限を保持しないアプリケーション管理者の場合、プロビジョニング・コンソールで「作成」および「**編集**」ボタンは使用できますが、「削除」ボタンは使用できません。ユーザーの作成は、12-17 ページの「プロビジョニング管理権限」に説明のあるプロビジョニング管理権限の場合と同じウィザードベースのプロシージャに基づいて実行されます。ユーザーの編集権限は、12-17 ページの「アプリケーション管理権限」に説明のあるアプリケーション管理権限の場合と同じです。

アプリケーション管理権限と Oracle Delegated Administration Services のユーザー編集権限

Oracle Delegated Administration Services のユーザー編集権限を保持し、ユーザー作成またはユーザー削除権限を保持しないアプリケーション管理者の場合、プロビジョニング・コンソールで「**編集**」ボタンは使用できますが、「**作成**」または「**削除**」ボタンは使用できません。ユーザーの編集は、12-17 ページの「プロビジョニング管理権限」に説明のあるプロビジョニング管理権限の場合と同じウィザードベースのプロシージャに基づいて実行されます。

アプリケーション管理権限と Oracle Delegated Administration Services のユーザー削除権限

Oracle Delegated Administration Services のユーザー削除権限を保持し、ユーザー作成またはユーザー変更権限を保持しないアプリケーション管理者の場合、プロビジョニング・コンソールで「**削除**」および「**編集**」ボタンは使用できますが、「**作成**」ボタンは使用できません。ユーザーの削除は、12-16 ページの「Oracle Delegated Administration Services 権限」に説明のある Oracle Delegated Administration Services 権限の場合と同じ単一ステップのプロシージャに基づいて実行されます。ユーザーの編集は、12-17 ページの「プロビジョニング管理権限」に説明のあるプロビジョニング管理権限の場合と同じウィザードベースのプロシージャに基づいて実行されます。

プロビジョニング権限とアプリケーション管理権限

プロビジョニング権限とアプリケーション管理権限を保持する管理者は、12-17 ページの「プロビジョニング管理権限」に説明のあるプロビジョニング管理権限の場合と同じ権限を保持します。

Oracle Delegated Administration Services 権限、プロビジョニング権限およびアプリケーション管理権限

Oracle Delegated Administration Services 権限とアプリケーション管理権限を保持する管理者は、12-17 ページの「アプリケーション管理権限」に説明のあるプロビジョニング管理権限の場合と同じ権限を保持します。

13

プロビジョニング統合アプリケーションの配置

この章では、Oracle プロビジョニング・サービスでのプロビジョニング統合アプリケーションの配置方法について説明します。内容は次のとおりです。

- プロビジョニング統合アプリケーションの配置の概要
- プロビジョニング用のアプリケーションの登録
- アプリケーションのプロビジョニング・プロパティの構成

関連項目：

- 第 4 章「Oracle Directory Integration Platform の管理」
- C-19 ページの「プロビジョニングに関するトラブルシューティング」

プロビジョニング統合アプリケーションの配置の概要

Oracle プロビジョニング・サービスでプロビジョニング統合アプリケーションを配置するには、一般的に次の手順を実行します。

1. Oracle Directory Integration Platform が含まれる Oracle Internet Directory をインストールします。
2. ユーザー情報を Oracle Internet Directory にロードします。

   関連資料：『Oracle Internet Directory 管理者ガイド』

3. 4-8 ページの「Oracle Directory Integration Platform の起動、停止および再起動」の手順に従い、Oracle Directory Integration Server を起動します。
4. アプリケーションをインストールし、プロビジョニング・サブスクリプション・ツールを使用して各アプリケーションのプロビジョニング・プロファイルを作成します。

   関連項目： 3-8 ページの「プロビジョニング・サブスクリプション・ツール」

5. 13-2 ページの「プロビジョニング用のアプリケーションの登録」で説明されている手順に従い、アプリケーション登録を構成します。
6. 13-5 ページの「アプリケーションのプロビジョニング・プロパティの構成」で説明されている手順に従い、アプリケーション・プロビジョニングを構成します。
7. 各アプリケーションについて、プロビジョニング・イベント伝播のステータスを定期的に監視します。これは、Oracle Enterprise Manager 10*g* Application Server Control コンソールを使用して実行できます。

   関連資料：『Oracle Internet Directory 管理者ガイド』のディレクトリの記録、監査および監視に関する章

プロビジョニング用のアプリケーションの登録

アプリケーションをインストールし、プロビジョニング・サブスクリプション・ツールを使用してそのプロビジョニング・プロファイルを作成したら、次の手順を実行してプロビジョニング用にアプリケーションを登録する必要があります。

1. 初期プロビジョニング登録を実行し、プロビジョニング統合プロファイルを作成します。Oracle Directory Integration Platform Service では、プロビジョニング統合プロファイルを使用してプロビジョニング統合アプリケーションを識別します。
2. Oracle Directory Integration Platform Service に対して、アプリケーション固有属性とデフォルト値を設定し、アプリケーションにユーザーをプロビジョニングする際に属性が必須であるかどうかを指定します。
3. プロビジョニング統合アプリケーションで必要とされるプラグインを登録します。これには、ビジネス・ポリシーを適用するためにアプリケーションで使用されるアプリケーション固有のプラグインも含まれます。

注意： Oracle Directory Integration Platform Service では、複数インスタンス・アーキテクチャに対応するインスタンス・レベルのアプリケーション・プロビジョニングはサポートされません。同じアプリケーションの複数のインスタンスをインストールする場合、Oracle Directory Integration Platform Service では、各インスタンスが独立したプロビジョニング統合アプリケーションとして扱われます。

プロビジョニング・コンソールでユーザーを作成する場合、管理者は、特定のプロビジョニング統合アプリケーションのユーザー属性を割り当てることができます。Oracle Internet Directory は、プロビジョニング・コンソールが管理する属性用のプライマリ・ディレクトリであるため、アプリケーション固有属性は、アプリケーションにプロビジョニングされるユー

ザーごとに Oracle Internet Directory に格納されます。パフォーマンス向上のため、プロビジョニング統合アプリケーションでは、通常、Oracle Internet Directory からユーザー属性を取得するかわりに、属性のローカル・コピーをキャッシュします。アプリケーションには、データ・アクセス Java プラグインにより同期的に、または PL/SQL プラグインにより非同期的に、ユーザーの作成、ユーザーの削除および属性の変更が通知されます。

登録処理により、Oracle Internet Directory にアプリケーションの一意の ID が作成されます。Oracle アプリケーションは、通常、Oracle Application Server によってデフォルトで $*ORACLE_HOME*/jlib ディレクトリにインストールされる repository.jar ファイルのリポジトリ API を使用して、プロビジョニングのための自己登録を行います。リポジトリ API は、Oracle Internet Directory にアプリケーション・エントリを作成する以外に、アプリケーションを権限グループに追加する場合にも使用されます。

登録 API を使用できない Oracle 以外のアプリケーションでは、LDAP コマンドと LDIF テンプレートを使用して Oracle Internet Directory にアプリケーションの ID を作成できます。アプリケーションのコンテナは、`cn=Products,cn=OracleContext` または `cn=Products,cn=OracleContext,`*`Realm DN`* の下に作成します。アプリケーション ID を作成するコンテナは、そのアプリケーションを使用するユーザーが単一レルムにいるか複数レルムにいるかによって変化します。ほとんどの場合、アプリケーションが特定の Oracle Internet Directory ID 管理レルムの ID 管理ポリシーによってバインドされないように、`cn=Products,cn=OracleContext` コンテナにアプリケーション ID を作成する必要があります。

同じアプリケーションの複数のインスタンスをインストールすることも可能です。プロビジョニング統合アプリケーションの新規インスタンスをインストールすると、アプリケーション ID コンテナに新規インスタンス用の個別エントリが作成されます。一部の構成設定はインスタンス固有ですが、それ以外の設定は同じアプリケーションの複数のインスタンス全体で共有されます。たとえば、Oracle Files のようなアプリケーションを考えてみます。Oracle Files の複数のインスタンスは、各インスタンスが相互に独立するような環境に配置できます。この場合、各インスタンスを個別のプロビジョニング統合アプリケーションとして定義できます。アプリケーションの複数のインスタンスにユーザーをプロビジョニングすることも可能です。

アプリケーションの最初のインスタンスをインストールする場合、Oracle Internet Directory に次の例のようなエントリを作成する必要があります。この例では、`cn=Products,cn=OracleContext` コンテナにアプリケーション ID を作成しています（アプリケーションの名前とタイプは、Files-App1 と FILES であるとします）。

```
dn: cn=FILES,cn=Products,cn=OracleContext
changetype: add
objectclass: orclContainer

dn: orclApplicationCommonName=Files-App1,cn=FILES,cn=Products,cn=OracleContext
changetype: add
orclappfullname: Files Application Instance 1
userpassword: password
description: This is a test application instance.
protocolInformation: protocol information
orclVersion: 1.0
orclaci: access to entry by group="cn=odisgroup,cn=DIPAdmins,cn=Directory Integration
Platform,cn=Products,cn=OracleContext" (browse,proxy) by group="cn=User Provisioning
Admins,cn=Groups,cn=OracleContext" (browse,proxy)
orclaci: access to attr=(*) by group="cn=odisgroup,cn=DIPAdmins,cn=Directory
Integration Platform,cn=Products,cn=OracleContext" (search,read,write,compare) by
group="cn=User Provisioning Admins,cn=Groups,cn=OracleContext"
(search,read,write,compare)
```

アプリケーションの 2 番目のインスタンスをインストールする場合、Oracle Internet Directory に次の例のようなエントリを作成する必要があります。この例でも、cn=Products,cn=OracleContext コンテナにアプリケーション ID を作成しています（アプリケーションの名前は、Files-App2 であるとします）。

```
dn: orclApplicationCommonName=Files-App2,cn=FILES,cn=Products,cn=OracleContext
changetype: add
orclappfullname: Files Application Instance 2
userpassword: password
description: This is a test Appliction instance.
protocolInformation: protocol information
orclVersion: 1.0
orclaci: access to entry by group="cn=odisgroup,cn=DIPAdmins,cn=Directory Integration
Platform,cn=Products,cn=OracleContext" (browse,proxy) by group="cn=User Provisioning
Admins,cn=Groups,cn=OracleContext" (browse,proxy)
orclaci: access to attr=(*) by group="cn=odisgroup,cn=DIPAdmins,cn=Directory
Integration Platform,cn=Products,cn=OracleContext" (search,read,write,compare) by
group="cn=User Provisioning Admins,cn=Groups,cn=OracleContext"
(search,read,write,compare)
```

Oracle Internet Directory へのプロビジョニング統合アプリケーションの登録に成功したら、必要に応じてアプリケーションを各種権限グループに追加します。表 13-1 に、Oracle Internet Directory の共通権限グループを示します。

表 13-1 Oracle Internet Directory の共通権限グループ

グループ	説明
OracleDASCreateUser	ユーザー作成
OracleDASEditUser	ユーザー編集
OracleDASDeleteUser	ユーザー削除
OracleDASCreateGroup	グループ作成
OracleDASEditGroup	グループ編集
OracleDASDeleteGroup	グループ削除

次の LDIF ファイルでは、すべてのレルムにおけるユーザー作成権限を Files-App1 アプリケーションに付与しています。

```
dn:cn=OracleCreateUser,cn=Groups,cn=OracleContext
changetype: modify
add: uniquemember
uniquemember:
orclApplicationCommonName=Files-App1,cn=FILES,cn=Products,cn=OracleContext
```

アプリケーションのプロビジョニング・プロパティの構成

プロビジョニング統合アプリケーションを登録したら、そのプロパティを構成する必要があります。各アプリケーションのプロビジョニング・プロファイルでは、独自のプロビジョニング構成プロパティが管理されます。プロビジョニング統合アプリケーションでは、次のタイプのメタデータの格納にこれらのプロパティが使用されます。

- アプリケーション ID 情報
- ID レルム情報
- デフォルト・アプリケーション・プロビジョニング・ポリシー
- アプリケーション属性プロパティとデフォルト値
- アプリケーション・プロビジョニング・プラグイン
- アプリケーション・イベント・インタフェース情報
- アプリケーション・イベント伝播情報

Oracle Directory Integration Platform では、1.1、2.0、3.0 という 3 つのバージョンのプロビジョニング・プロファイルがサポートされます。バージョン 3.0 のプロビジョニング・プロファイルは、Oracle Identity Management 10*g*（10.1.4.0.1）でのみ使用できます。アプリケーションごとに、異なるプロビジョニング・プロファイル・バージョンに対応しています。たとえば、多くの Oracle アプリケーションでは、バージョン 2.0 のみがサポートされます。ただし、Oracle Collaboration Suite では、バージョン 3.0 のプロビジョニング・プロファイルがサポートされます。プロビジョニング・プロファイルのバージョン間の主な違いは、次のとおりです。

- プロビジョニング・コンソールを使用してプロビジョニングできるのは、バージョン 3.0 のプロビジョニング・プロファイルをサポートするターゲット・アプリケーションのみです。バージョン 1.1 および 2.0 のプロビジョニング・プロファイルのみをサポートするアプリケーションは、プロビジョニング・コンソールで使用できませんが、構成されたイベント通知をそれらのアプリケーションで受信することは可能です。
- バージョン 1.1 および 2.0 のプロビジョニング・プロファイルをサポートするアプリケーションのプロビジョニングは、`oidprovtool` ユーティリティに関連する単一ステップのプロセスです。このツールの詳細は、3-8 ページの「プロビジョニング・サブスクリプション・ツール」を参照してください。ただし、バージョン 3.0 のプロビジョニング・プロファイルをサポートするアプリケーションのプロビジョニングは、複数ステップのプロセスです。詳細は、『Oracle Identity Management アプリケーション開発者ガイド』の集中管理ユーザー・プロビジョニング Java API リファレンスに関する章を参照してください。
- Oracle Directory Integration Platform では、バージョン 3.0 のプロビジョニング・プロファイルをサポートするアプリケーションのユーザー・プロビジョニング・ステータスのみが管理されます。

> **関連資料：**『Oracle Identity Management アプリケーション開発者ガイド』の集中管理ユーザー・プロビジョニング Java API リファレンスに関する章

14

Oracle Internet Directory プロビジョニング・コンソールによる管理

この章では、Oracle Internet Directory プロビジョニング・コンソールを使用した管理の方法について説明します。内容は次のとおりです。

- プロビジョニング・コンソールによるユーザーの管理
- プロビジョニング・コンソールによるアプリケーションの管理

関連項目：

- 第 4 章「Oracle Directory Integration Platform の管理」
- C-19 ページの「プロビジョニングに関するトラブルシューティング」

プロビジョニング・コンソールによるユーザーの管理

この項では、プロビジョニング・コンソールを使用してユーザーを管理する方法について説明します。内容は次のとおりです。

- プロビジョニング条件に基づくユーザーの検索
- プロビジョニング・コンソールによるユーザーの作成
- プロビジョニング・コンソールによるユーザーのプロビジョニングとプロビジョニング解除

注意： ユーザーの削除など、特にプロビジョニングに関連しないユーザー管理は、Oracle Internet Directory セルフ・サービス・コンソールで処理します。詳細は、『Oracle Identity Management 委任管理ガイド』を参照してください。

プロビジョニング条件に基づくユーザーの検索

プロビジョニング条件に基づいてユーザーを検索するには、次の手順を実行します。

1. 「**ディレクトリ**」タブをクリックし、「**ユーザー**」を選択します。「ユーザー」ページで、「**プロビジョニング検索**」をクリックします。「プロビジョニング検索」ウィンドウが表示されます。

   このウィンドウの詳細は、『Oracle Identity Management 委任管理ガイド』を参照してください。

2. 次のオプションのいずれかを選択し、ユーザーの検索方法を決定します。
   - **すべての条件に一致するユーザーを検索します。**
   - **任意の条件に一致するユーザーを検索します。**
3. ユーザーのプロビジョニング・ステータスを検索する各アプリケーションの右側にある 1 番目のボックスから、次の条件のいずれかを選択します。
   - **次に一致する（デフォルト）**
   - **次に一致しない**
   - **存在する**
   - **存在しない**
4. 検索する各アプリケーションの右側にある 2 番目のボックスから、次のプロビジョニング・ステータスのいずれかを選択します。
   - **保留**
   - **リクエストなし**
   - **成功**
   - **失敗**
   - **進行中**
   - **プロビジョニング解除が保留中です**
   - **正常にプロビジョニング解除されました**
   - **プロビジョニング解除に失敗しました**
   - **プロビジョニング解除が進行中です**
   - **アップグレードが保留中です**
   - **アップグレードが進行中です**
   - **アップグレードに失敗しました**

5. 別の検索属性を追加するには、「**さらに追加**」ボックスから属性名を選択し、「**追加**」をクリックします。
6. 「**実行**」をクリックすると、入力した条件に一致するエントリが表示されます。

プロビジョニング・コンソールによるユーザーの作成

プロビジョニング・コンソールでユーザーを作成するには、次の手順を実行します。

1. Oracle Internet Directory セルフ・サービス・コンソールで、「**ディレクトリ**」タブを選択し、「**ユーザー**」をクリックします。「ユーザーの検索」ウィンドウが表示されます。

   このウィンドウの詳細は、『Oracle Identity Management 委任管理ガイド』を参照してください。
2. 「**作成**」をクリックして一般プロビジョニング・ウィンドウを表示します。

   このウィンドウの詳細は、『Oracle Identity Management 委任管理ガイド』を参照してください。
3. 一般プロビジョニング・ウィンドウで、適切な情報を入力します。既存ユーザー・エントリのパスワードをリセットするには、「**パスワード**」フィールドに新しい値を入力します。

   注意：「**ユーザー ID**」フィールドには、空白または & ' % ? \ / + = ( ) * ^ , ; | ' ~ のいずれの文字も使用することはできません。
4. 「**次へ**」をクリックしてアプリケーション・プロビジョニング・ウィンドウを表示します。

   このウィンドウの詳細は、『Oracle Identity Management 委任管理ガイド』を参照してください。
5. アプリケーション・プロビジョニング・ウィンドウで、ユーザー・エントリをプロビジョニングするアプリケーションを選択します。このウィンドウに表示される使用可能なアプリケーションは、環境に応じて変化します。デフォルト・プロビジョニング・ポリシーにより、新規ユーザーの作成時にデフォルトでプロビジョニングされるアプリケーションが決定されます。デフォルト・ポリシーによっては、1 つ以上のアプリケーションのポリシーを上書きすることが可能です。ポリシーを上書きできない場合、デフォルト設定に応じて表示される「プロビジョニング」または「プロビジョニングしない」列は、グレー表示されます。

   アプリケーションのデフォルト・プロビジョニング・ポリシーを変更するには、14-5 ページの「プロビジョニング・コンソールによるアプリケーションの管理」の説明に従ってください。

   注意： Oracle Application Server 10*g*（10.1.4.0.1）の場合、プロビジョニング・コンソールでプロビジョニングできるのは、Oracle Collaboration Suite に属するコンポーネントのみです。
6. 「**次へ**」をクリックして「アプリケーション属性」ウィンドウを表示します。

   このウィンドウの詳細は、『Oracle Identity Management 委任管理ガイド』を参照してください。
7. 「アプリケーション属性」ウィンドウで、ユーザー・エントリをプロビジョニングするために選択したアプリケーションの属性値を入力します。アプリケーションの構成状況によっては、一部の属性にデフォルト値が入力されている場合があります。

   関連項目： 14-5 ページの「プロビジョニング・コンソールによるアプリケーションの管理」

8. 「**次へ**」をクリックしてプロビジョニングの確認ウィンドウを表示します。

   このウィンドウの詳細は、『Oracle Identity Management 委任管理ガイド』を参照してください。

9. ユーザー・エントリのプロビジョニング・オプションの確認後、「**終了**」をクリックします。

プロビジョニング・コンソールによるユーザーのプロビジョニングとプロビジョニング解除

プロビジョニング・コンソールでユーザーをプロビジョニングまたはプロビジョニング解除するには、次のようにします。

1. Oracle Internet Directory セルフ・サービス・コンソールで、「**ディレクトリ**」タブをクリックし、「**ユーザー**」を選択します。「ユーザーの検索」ウィンドウが表示されます。

   このウィンドウの詳細は、『Oracle Identity Management 委任管理ガイド』を参照してください。

2. 「**ユーザーの検索**」フィールドに、ユーザーの姓、名、電子メール・アドレスまたはユーザー ID の最初の数文字を入力します。たとえば、Anne Smith を検索する場合、`Ann` または `Smi` と入力します。ディレクトリにあるすべてのユーザーのリストを表示するには、このフィールドを空白のままにしてください。

3. 「**実行**」をクリックして検索結果を表示します。

4. プロビジョニングする（またはプロビジョニング解除する）ユーザーを選択し、「**編集**」をクリックして一般プロビジョニング・ウィンドウを表示します。

   このウィンドウの詳細は、『Oracle Identity Management 委任管理ガイド』を参照してください。

   注意： ユーザー・エントリを編集するための十分な権限がない場合、「**編集**」ボタンは表示されません。

5. 一般プロビジョニング・ウィンドウで、適切な情報を入力します。既存ユーザー・エントリのパスワードをリセットするには、「**パスワード**」フィールドに新しい値を入力します。

   注意：「**ユーザー ID**」フィールドには、空白または & ' % ? \ / + = ( ) * ^ , ; | ' ~ のいずれの文字も使用することはできません。

6. 「**次へ**」をクリックしてアプリケーション・プロビジョニング・ウィンドウを表示します。

   このウィンドウの詳細は、『Oracle Identity Management 委任管理ガイド』を参照してください。

7. アプリケーション・プロビジョニング・ウィンドウで、ユーザー・エントリをプロビジョニングする（またはプロビジョニング解除する）アプリケーションを選択します。このウィンドウに表示される使用可能なアプリケーションは、環境に応じて変化します。デフォルト・プロビジョニング・ポリシーにより、新規ユーザーの作成時にデフォルトでプロビジョニングされるアプリケーションが決定されます。アプリケーションの構成状況によっては、1 つ以上のアプリケーションのポリシーを上書きすることが可能です。ポリシーを上書きできない場合、デフォルト設定に応じて表示される「プロビジョニング」または「プロビジョニングしない」列は、グレー表示されます。

   アプリケーションのデフォルト・プロビジョニング・ポリシーを変更するには、14-5 ページの「プロビジョニング・コンソールによるアプリケーションの管理」の説明に従ってください。

注意： Oracle Application Server 10*g*（10.1.4.0.1）の場合、プロビジョニング・コンソールでプロビジョニングできるのは、Oracle Collaboration Suite に属するコンポーネントのみです。

8. 「**次へ**」をクリックして「アプリケーション属性」ウィンドウを表示します。

   このウィンドウの詳細は、『Oracle Identity Management 委任管理ガイド』を参照してください。

9. 「アプリケーション属性」ウィンドウで、ユーザー・エントリをプロビジョニングするために選択したアプリケーションの属性値を入力します。環境によっては、一部の属性にデフォルト値が入力されている場合があります。

   関連項目： 14-5 ページの「プロビジョニング・コンソールによるアプリケーションの管理」

10. 「**次へ**」をクリックしてプロビジョニングの確認ウィンドウを表示します。

    このウィンドウの詳細は、『Oracle Identity Management 委任管理ガイド』を参照してください。

11. ユーザー・エントリのプロビジョニング・オプションの確認後、「**終了**」をクリックします。

プロビジョニング・コンソールによるアプリケーションの管理

この項では、プロビジョニング・コンソールを使用してアプリケーションを管理する方法について説明します。内容は次のとおりです。

- アプリケーション・デフォルトの管理
- アプリケーション・キャッシュのリロード

アプリケーション・デフォルトの管理

この項では、プロビジョニング統合アプリケーションのデフォルト設定を管理する方法について説明します。使用可能なプロビジョニング対応アプリケーションは、環境に応じて異なります。

注意： Oracle Application Server 10*g*（10.1.4.0.1）の場合、プロビジョニング・コンソールでプロビジョニングできるのは、Oracle Collaboration Suite に属するコンポーネントのみです。

アプリケーション・デフォルトを管理するには、次の手順を実行します。

1. 「**ディレクトリ**」タブを選択し、「**アプリケーション**」を選択して「デフォルトの管理 : アプリケーションの選択」ウィンドウを表示します。

   このウィンドウの詳細は、『Oracle Identity Management 委任管理ガイド』を参照してください。

2. 「デフォルトの管理 : アプリケーションの選択」ウィンドウで、デフォルトを管理するアプリケーションを選択します。

3. 「**管理**」をクリックして「デフォルトの管理 : 属性」ウィンドウを表示します。

   このウィンドウの詳細は、『Oracle Identity Management 委任管理ガイド』を参照してください。

4. 「デフォルトの管理 : 属性」ウィンドウで、「デフォルトの管理 : アプリケーションの選択」ウィンドウで選択したアプリケーションの属性フィールドにデフォルト値を入力します。
5. 「**発行**」をクリックします。

アプリケーション・キャッシュのリロード

アプリケーション・キャッシュにより、プロビジョニング・コンソールで使用可能なプロビジョニング統合アプリケーションが決定されます。Oracle Internet Directory でプロビジョニング統合アプリケーションが有効化または無効化された場合は、常にアプリケーション・キャッシュをリロードする必要があります。

アプリケーション・キャッシュをリロードするには、次の手順を実行します。

1. プロビジョニング・コンソールで、「**ディレクトリ**」タブを選択し、「**アプリケーション**」を選択します。「デフォルトの管理 : アプリケーションの選択」ウィンドウが表示されます。

   このウィンドウの詳細は、『Oracle Identity Management 委任管理ガイド』を参照してください。
2. 「デフォルトの管理 : アプリケーションの選択」ウィンドウで、「**リフレッシュ**」をクリックします。

15

Oracle プロビジョニング・イベント・エンジンの概要

この章では、Oracle プロビジョニング・イベント・エンジンについて説明します。内容は次のとおりです。

Oracle プロビジョニング・イベントとは

Oracle プロビジョニング・イベント・エンジンは、Oracle Internet Directory のユーザー・エントリを対象に実行された操作に応じて、USER_ADD、USER_MODIFY および USER_DELETE イベントを送信します。ユーザーは、ベース・ユーザーおよびアプリケーション固有ユーザーの情報を含む複数のエントリで示されるため、アプリケーションでは、イベントにおいてすべての属性にサブスクライブできます。

ベース・エントリまたはアプリケーション・エントリが更新されると、ユーザー・イベントも送信されます。ただし、アプリケーション・エントリが削除される場合、イベントは送信されません。管理者がアプリケーションからユーザーをプロビジョニング解除するよう要求した場合は、USER_MODIFY イベントが DEPROVISIONING_REQUIRED というプロビジョニング・ステータスとともにアプリケーションに送信されるためです。アプリケーションが SUCCESS という値を返すことでイベントを確認すると、アプリケーション・エントリは Oracle Directory Integration Server によって削除されます。

プロビジョニング・ステータスの変更通知を受信するには、アプリケーションで orclUserApplnProvStatus;*Application_Name* 属性にサブスクライブする必要があります。たとえば、CORP_EMAIL というアプリケーションのプロビジョニング・ステータスの変更にサブスクライブするには、アプリケーションで orclUserApplnProvStatus;CORP-EMAIL 属性にサブスクライブする必要があります。

Oracle プロビジョニング・イベント・エンジンの操作

Oracle プロビジョニング・イベント・エンジンは、Oracle Internet Directory で有効に定義されたオブジェクトに対する追加、変更および削除操作からイベントを生成します。Oracle プロビジョニング・イベント・エンジンでは、イベントを生成するために、オブジェクト定義とイベント生成ルールが使用されます。このイベント生成モデルは、カスタム・オブジェクトとカスタム・イベント生成ルールを定義できるため、拡張性を備えています。Oracle プロビジョニング・イベント・エンジン、オブジェクト定義およびイベント生成ルールについては、次の項目で説明します。

- カスタム・イベント・オブジェクト定義の作成
- カスタム・イベント生成ルールの定義

カスタム・イベント・オブジェクト定義の作成

表 15-1 に、イベントを生成可能なオブジェクトを識別するために使用できるプロパティを示します。

表 15-1 イベント・オブジェクトのプロパティ

プロパティ	説明
ObjectName	オブジェクトを識別する一意の名前を割り当てます。
ObjectCriteria	オブジェクトを識別するための LDAP オブジェクト・クラスを指定します。
MustAttributeCriteria	オブジェクトの識別に必要な追加の属性を指定します。
OptionalAttributeCriteria	オブジェクトの識別に必要となる可能性のあるオプションの属性を指定します。
FilterAttributeCriteria	イベントの伝播時に送信しない属性をリストします。

表 15-2 に、Oracle プロビジョニング・イベント・エンジンでイベントを生成できる定義済オブジェクトを示します。

表 15-2 事前定義されたイベント・オブジェクト

オブジェクト名	有効なオブジェクト・クラス値
Entry	*
User	orclUserV2,inetorgperson
Identity	orclUserV2,inetOrgPerson
Group	groupOfUniqueNames,orclGroup, orclPrivilegeGroup,groupOfNames
Subscription	orclServiceSubscriptionDetail
Subscriber	orclSubscriber

注意： イベント・オブジェクトのメタデータは、cn=Object Definitions,cn=Directory Integration Platform,cn=Products,cn=OracleContext コンテナに格納されます。

カスタム・イベント生成ルールの定義

イベント生成ルールは、XML 形式で指定します。イベント生成ルールの DTD は、次のとおりです。

```
<?xml version='1.0' ?>
  <!DOCTYPE EventRuleSet [
    <!ELEMENT ChangeType (#PCDATA)>
    <!ELEMENT Rule  (#PCDATA)>
    <!ELEMENT EventName  (#PCDATA)>
    <!ELEMENT ResEvent (Rule*, EventName)>
    <!ELEMENT EventRule (ChangeType, ResEvent*)>
    <!ELEMENT EventRuleSet (EventRule*) >
  ]>
```

この DTD の要素定義は、次のとおりです。

- EventRuleSet ルート要素は、個々のイベント・オブジェクトのイベント・ルールのセットを識別します。
- EventRuleSet ルート要素には、EventRule 要素のリストが含まれます。
- 各 EventRule 要素は、ChangeType 要素に割り当てられた値に応じて変化します。
- ChangeType および Rule 要素は、アプリケーションに伝播されるイベント名を決定します。

表 15-3 に、Oracle プロビジョニング・イベント・エンジンでサポートされるイベント定義を示します。

表 15-3 サポートされるイベント定義

オブジェクト名	変更タイプ	ルール	イベント名
USER	追加	OrclApplnUserProvStatus=PENDING_UPGRADE	USER_ADD
	追加	OrclApplnUserProvStatus=PROVISIONING_REQUIRED	USER_ADD
	変更	OrclApplnUserProvStatus= PENDING_UPGRADE	USER_ADD
		OrclApplnUserProvStatus=PROVISIONING_REQUIRED	USER_ADD
		OrclApplnUserProvStatus=PROVISIONING_FAILURE	USER_ADD
		OrclApplnUserProvStatus=DEPROVISIONING_REQUIRED	USER_MODIFY
		OrclApplnUserProvStatus=PROVISIONING_IN_PROGRESS	USER_MODIFY
		OrclApplnUserProvStatus=PROVISIONING_SUCCESSFUL	USER_MODIFY
	削除	OrclApplnUserProvStatus=PROVISIONING_IN_PROGRESS	USER_DELETE
		OrclApplnUserProvStatus=PROVISIONING_SUCCESSFUL	USER_DELETE
		OrclApplnUserProvStatus=DEPROVISIONING_REQUIRED	
GROUP	追加		GROUP_ADD
	変更		GROUP_MODIFY
	削除		GROUP_DELETE
IDENTITY	追加		IDENTITY_ADD
	変更		IDENTITY_MODIFY
	削除		IDENTITY_DELETE
ENTRY	追加		ENTRY_ADD
	変更		ENTRY_MODIFY
	削除		ENTRY_DELETE
SUBSCRIPTION	追加		SUBSCRIPTION_ADD
	変更		SUBSCRIPTION_MODIFY
	削除		SUBSCRIPTION_DELETE
SUBSCRIBER	追加		SUBSCRIBER_ADD
	変更		SUBSCRIBER_MODIFY
	削除		SUBSCRIBER_DELETE

注意： サポートされるイベント・オブジェクトのメタデータは、cn=Event Definitions,cn=Directory Integration Platform, cn=Products,cn=OracleContext コンテナに格納されます。

16

Oracle E-Business Suite とのプロビジョニング・データの統合

Oracle Internet Directory 10*g*（10.1.4.0.1）では、Oracle Directory Integration Platform Service を使用して、Oracle E-Business Suite のユーザー・アカウントとその他のユーザー情報を同期化できます。

関連資料： この統合の詳細および管理方法は、Oracle E-Business Suite のドキュメントを参照してください。

次の記述は Oracle*MetaLink*（`http://metalink.oracle.com/`）で参照可能です。

- 233436.1:「Installing Oracle Application Server 10*g* with Oracle E-Business Suite Release 11*i*」
- 261914.1:「Integrating Oracle E-Business Suite Release 11*i* with Oracle Internet Directory and Oracle Application Server Single Sign-On」
- 233436.1:「Installing Oracle Application Server 10*g* with Oracle E-Business Suite Release 11*i*」

第 V 部

サード・パーティ・ディレクトリとの統合

第 V 部では、様々なサード・パーティ・ディレクトリとの統合に関する概念、コンポーネントおよび手順について説明します。次の各章で構成されています。

17

サード・パーティ・ディレクトリ統合の概念と考慮事項

この章では、Oracle Identity Management とサード・パーティ・ディレクトリとの統合の基本概念と、統合プロセスの一環として行う様々な決定について説明します。

注意： この章を読む前に、次の資料の内容を理解しておく必要があります。

- 『Oracle Internet Directory 管理者ガイド』の ID 管理レルムの配置に関する章
- 『Oracle Identity Management 委任管理ガイド』

この章の内容は次のとおりです。

関連項目： サード・パーティ・ディレクトリとの同期に関する特定の実装の詳細は、次の各章を参照してください。

- 第 18 章「サード・パーティ・ディレクトリとの同期の構成」
- 第 19 章「Microsoft Active Directory との統合」
- 第 20 章「Oracle Password Filter for Microsoft Active Directory の配置」
- 第 21 章「Sun Java System Directory との統合」
- 第 22 章「Novell eDirectory または OpenLDAP との統合」
- 第 23 章「サード・パーティ・ディレクトリとの統合の管理」

サード・パーティ・ディレクトリ統合の概念とアーキテクチャ

すべての Oracle コンポーネントは、Oracle Identity Management と統合することによって、セキュリティが集中管理されます。環境内で Oracle Identity Management とサード・パーティ・ディレクトリ（Microsoft Active Directory など）の両方を使用する場合、コネクタを使用して 2 つのシステムを統合し、両方のデータを同期化することができます。コネクタとは、あらかじめパッケージされた接続ソリューションで、これを使用すると Oracle Internet Directory を接続ディレクトリと同期化できます。

この項では、Oracle Identity Management とサード・パーティ接続ディレクトリの統合に必要な Oracle コンポーネントとアーキテクチャについて説明します。内容は次のとおりです。

- サポート対象のサード・パーティのディレクトリおよびサーバー
- サード・パーティ・ディレクトリとの統合に関する Oracle Identity Management コンポーネント
- サード・パーティ・ディレクトリとの同期用の Oracle Internet Directory スキーマ要素
- サード・パーティ・ディレクトリとの統合におけるディレクトリ情報ツリー

サポート対象のサード・パーティのディレクトリおよびサーバー

Oracle Internet Directory 10*g*（10.1.4.0.1）は、次のサード・パーティのディレクトリおよびサーバーとの統合が保証されています。

- Microsoft Active Directory 2000/2003
- Microsoft Exchange 2000/2003
- Sun Java System Directory 5.2
  Sun Java System Directory は、以前の Sun ONE Directory Server、iPlanet Directory Server および Netscape Directory Server です。Oracle Internet Directory 10*g*（10.1.4.0.1）は、Netscape Directory Server 4.13 以上のすべてのバージョンとの統合が保証されています。
- Novell eDirectory 8.6.2 および 8.7
- OpenLDAP 2.2

サード・パーティ・ディレクトリとの統合に関する Oracle Identity Management コンポーネント

この項では、Oracle Identity Management とサード・パーティ・ディレクトリとの統合に使用される次のコンポーネントについて説明します。

- Oracle Internet Directory
- Oracle Directory Integration Platform
- Oracle Delegated Administration Services
- Oracle Access Manager
- Oracle Application Server Single Sign-On
- 外部認証プラグイン

> **関連項目：** Oracle Internet Directory とサード・パーティ・ディレクトリとの統合に使用されるツールの説明は、第 3 章「Oracle Directory Integration Platform 管理ツール」を参照してください。

Oracle Internet Directory

Oracle Internet Directory は、Oracle コンポーネントとサード・パーティのアプリケーションによって、ユーザー ID および資格証明が格納され、アクセスされるリポジトリです。ここでは、Oracle ディレクトリ・サーバーを使用して、ユーザーにより入力された資格証明を Oracle Internet Directory に格納された資格証明と比較することで、ユーザー認証が行われます。資格証明がサード・パーティのディレクトリに格納されていて、Oracle Internet Directory に格納されていない場合でも、ユーザーを認証することはできます。この場合は、Oracle Internet Directory では、サード・パーティのディレクトリ・サーバーに対してユーザー認証を行う外部認証プラグインが使用されます。

> **関連資料：** Oracle Internet Directory でのセキュリティについては、『Oracle Internet Directory 管理者ガイド』のセキュリティに関する章を参照してください。

Oracle Directory Integration Platform

Oracle Directory Integration Platform は、Oracle Application Server Infrastructure の一部としてインストールされます。これを Oracle Internet Directory と同じホストで実行するようにも、異なるホストで実行するようにも構成できます。

Oracle Directory Integration Platform を使用すると、次のことができます。

- Oracle Internet Directory と他のディレクトリおよびユーザー・リポジトリ間の同期
- Oracle コンポーネント用の自動プロビジョニング・サービス

Oracle Directory Integration Platform には、Oracle Internet Directory を他の LDAP ディレクトリまたはデータ・ストアと同期化するためのコネクタが含まれます。Oracle Directory Integration Platform 統合コネクタを使用すると、次のことができます。

- サード・パーティ・ディレクトリとの一方向または双方向いずれかの同期の構成
- 同期専用の属性サブセットの指定。これは、適切なマッピング・ルールを構成することによって行います。マッピング・ルールは、実行時に変更できます。

> **関連項目：** 属性マッピング・ルールの構成については、6-7 ページの「属性レベル・マッピング」を参照してください。

Oracle Delegated Administration Services

Oracle Delegated Administration Services は Web ベースの事前定義済ユニットのセットで、ユーザーのかわりにディレクトリ操作を実行します。ディレクトリ管理者は、他の管理者やエンド・ユーザーに特定の機能を委任できるようになるため、より多くの日常的なディレクトリ管理タスクから解放されます。また、ユーザー・エントリの作成、グループ・エントリの作成、エントリの検索、ユーザー・パスワードの変更など、ディレクトリ対応アプリケーションに必要な機能の大部分が提供されます。ディレクトリ内のアプリケーション・データを管理するには、Oracle Delegated Administration Services ベースのツールである Oracle Internet Directory セルフサービス・コンソールを使用します。このツールは、Oracle Internet Directory とともに使用できるようになっています。あるいは、Oracle Delegated Administration Services を使用して、アプリケーション・データを管理するための独自ツールを開発できます。

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

Oracle Access Manager

Oracle Delegated Administration Services の他に、Oracle Access Manager を使用してもディレクトリ操作を実行することができます。Oracle Access Manager（以前の Oblix NetPoint および Oblix COREid）には、Web シングル・サインオン、ユーザー・セルフサービスとユーザー自己登録、高度なワークフロー機能、ユーザー・プロビジョニング、レポート作成と監査、ポリシー管理、動的グループ管理、委任管理など、ID 管理とセキュリティの機能がフル装備されています。

> **関連資料：**『Oracle Access Manager ID および共通管理ガイド』

Oracle Application Server Single Sign-On

OracleAS Single Sign-On を使用すると、ユーザーは 1 回のみのログインで、Web ベースの Oracle コンポーネントにアクセスできます。

Oracle コンポーネントは、ログイン機能を OracleAS Single Sign-On Server に委任します。初めて Oracle コンポーネントにログインする場合は、そのコンポーネントによって OracleAS Single Sign-On Server へログインが送信されます。OracleAS Single Sign-On Server では、ユーザーが入力した資格証明を、Oracle Internet Directory に格納されている資格証明と比較します。資格証明の検証後、OracleAS Single Sign-On Server により、現行セッション中、ユーザーが使用を認可されているすべてのコンポーネントに対するユーザー・アクセス権が付与されます。

Oracle Application Server Single Sign-On を使用すると、Microsoft Windows 環境でのネイティブ認証が有効になります。ユーザーは、Windows 環境にログインすると、自動的に Oracle コンポーネントにアクセスできるようになります。OracleAS Single Sign-On が、ユーザーの Kerberos 資格証明を使用してユーザーを Oracle 環境に自動的にログインさせます。

> **関連資料：** OracleAS Single Sign-On の詳細は、『Oracle Application Server Single Sign-On 管理者ガイド』を参照してください。

外部認証プラグイン

外部認証プラグイン（Microsoft Active Directory 外部認証プラグインなど）は、Oracle ディレクトリ・サーバーの一部で、これを使用すると、ユーザーは Microsoft Windows 資格証明を使用して Oracle 環境にログインできます。外部認証プラグインがインストールされていれば、Oracle ディレクトリ・サーバーにより起動されます。このプラグインにより、サード・パーティ・ディレクトリでユーザーの資格証明が検証されます。検証が正常に実行された場合は、Oracle ディレクトリ・サーバーから OracleAS Single Sign-On に通知されます。

サード・パーティ・ディレクトリとの同期用の Oracle Internet Directory スキーマ要素

サード・パーティ・ディレクトリのオブジェクトと同期化されるオブジェクトを識別するために、Oracle Internet Directory には、サード・パーティ・ディレクトリ（Microsoft Active Directory など）に固有の属性に対応するスキーマ要素が含まれています。これらのスキーマ要素については、『Oracle Identity Management ユーザー・リファレンス』および次の項を参照してください。

- Microsoft Active Directory 用の Oracle Internet Directory スキーマ要素
- Sun Java System Directory 用の Oracle Internet Directory スキーマ要素
- Novell eDirectory 用の Oracle Internet Directory スキーマ要素
- OpenLDAP 用の Oracle Internet Directory スキーマ要素

サード・パーティ・ディレクトリとの統合におけるディレクトリ情報ツリー

この項の内容は次のとおりです。

> **関連資料 :** ディレクトリ情報ツリーの詳細は、『Oracle Internet Directory 管理者ガイド』のディレクトリの概念とアーキテクチャに関する章を参照してください。

Oracle Internet Directory のレルムの概要

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

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

複数のレルム

同じ Oracle Identity Management インフラストラクチャ内で複数の ID 管理レルムを定義できます。したがって、ユーザーの集団を区別し、各レルムで異なる ID 管理ポリシー（パスワード・ポリシー、ネーミング・ポリシー、自己変更ポリシーなど）を施行できます。これは、Oracle Application Server のホスティングされた配置で役立ちます。

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

デフォルトのレルム

すべての Oracle コンポーネントが機能するには、ID 管理レルムが必要です。Oracle Internet Directory のインストール中に作成される特別なレルムは、デフォルト ID 管理レルムと呼ばれます。これは、レルムの名前が指定されていない場合に、Oracle コンポーネントが、ユーザー、グループおよび関連付けられたポリシーを検索する場所です。このデフォルトのレルムにより、ディレクトリ内で情報の適切な編成が容易になり、適切なアクセス制御が実行されます。

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

図 17-1 に、デフォルト ID 管理レルムを示します。

図 17-1 デフォルト ID 管理レルム

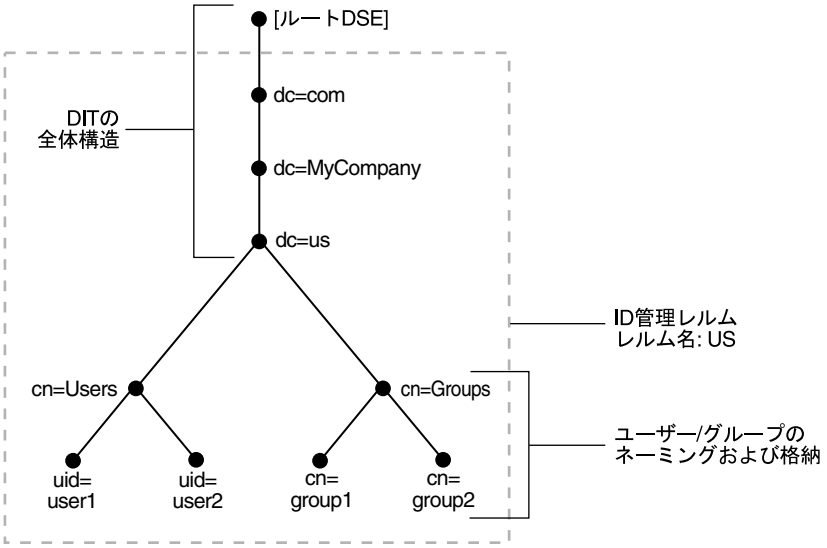


図 17-1 が示すように、デフォルト ID 管理レルムは、グローバルなディレクトリ情報ツリー（DIT）の一部です。ルート DSE に続くノードは `dc=com` で、その下に `dc=MyCompany`、`dc=us` が続きます。これらの 4 つのノードは、DIT の全体構造を表しています。`dc=us` ノードは、デフォルト ID 管理レルムのルートです。このノードには、ユーザーとグループの情報を格納するための 2 つのサブツリー、`cn=Users` と `cn=Groups` があります。説明のために、`cn=Users` ノードには 2 つのリーフ、`uid=user1` と `uid=user2` があります。同様に、`cn=Groups` ノードには、`cn=group1` と `cn=group2` があります。

レルムにおけるアクセス制御ポリシー

Oracle Directory Integration Platform で次のことを可能にするには、Oracle Internet Directory で適切な ACL を構成する必要があります。

- インポート・プロファイルにより `users` コンテナと `groups` コンテナでオブジェクトの追加、変更および削除ができるようにします。デフォルトでは、インポート・プロファイルはレルム管理グループの一部で、レルム識別名の下の任意のエントリに対してあらゆる操作を実行できます。レルム内で ACL をカスタマイズした場合、同期化されるサブツリーで、あるいは同期が行われる場所に応じて `user` コンテナまたは `group` コンテナ（あるいはその両方）で、インポート・プロファイルにこれらの操作を実行するための適切な権限があることを確認します。
- Oracle コンポーネントでレルム内のユーザーとグループを管理できるようにします。デフォルトでは、Oracle コンポーネントで `users` コンテナと `groups` コンテナのそれぞれのユーザーとグループを管理できます。レルム内で `usersearchbase` と `groupsearchbase` を更新した場合、`users` コンテナと `groups` コンテナで適切な ACL を設定します。

> **関連資料：** Oracle Internet Directory によりインストールされたデフォルト・レルムについては、『Oracle Internet Directory 管理者ガイド』の Oracle Identity Management レルムの配置に関する章を参照してください。

配置の計画

DIT を計画する際、同期の前に行う最も重要な決定は、次のとおりです。

- 中央ディレクトリとなるディレクトリ。
- 同期化するオブジェクト。たとえば、次のようなものです。
  - DIT で同期化する必要のある部分。DIT 全体またはその一部のみを同期化できます。
  - エントリごとの、同期化の必要な特定のコンテンツ。エントリのコンテンツ全体またはその一部のみを同期化できます。
- 同期化する位置。次の 2 つのオプションがあります。
  - DIT の各エントリの相対的な位置が、ソース・ディレクトリと宛先ディレクトリの両方で同じになるように同期化できます。この構成は、1 対 1 識別名マッピングと呼ばれ、最も一般的に使用されている構成です。ソース識別名が宛先識別名と同じであるため、この構成では 2 つの識別名が異なる場合よりパフォーマンスが向上します。
  - DIT の各エントリの相対的な位置が、ソース・ディレクトリと宛先ディレクトリで異なるように同期化できます。この構成では、Oracle Directory Integration Platform により、マップされるすべてのエントリ（グループ・エントリ内の参照を含む）の識別名値を変更する必要があります。これにはより集中的な計算が必要です。

    このように同期化する場合、6-10 ページの「サポートされている属性マッピング・ルールと例」で説明されているように、`dnconvert` マッピング・ルールを使用する必要があります。

    関連項目： ディレクトリ情報ツリーの計画の詳細は、17-15 ページの「ディレクトリ情報ツリーの構造の選択」の項を参照してください。

例 : 単一のサード・パーティ・ディレクトリ・ドメインとの統合

図 17-2 に、Oracle Internet Directory とサード・パーティ・ディレクトリ間での 1 対 1 マッピングの例を示します。

図 17-2 Oracle Internet Directory とサード・パーティ・ディレクトリのホストがドメイン us.MyCompany.com 下に存在する場合の両ディレクトリにおけるデフォルトの DIT 構造

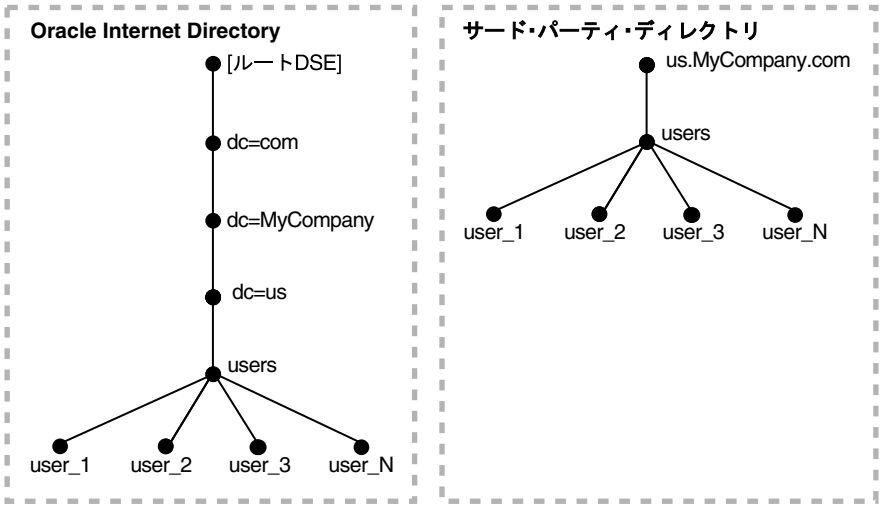


図 17-2 の 1 対 1 マッピングの場合 :

- サード・パーティ・ディレクトリと Oracle Internet Directory の両方のホストのトポロジは同じです。
- ユーザーは、サード・パーティ・ディレクトリから Oracle Internet Directory へのみ同期化されます。同期化されるすべてのユーザーが、サード・パーティ・ディレクトリ内の 1 つのコンテナ（この場合、`users.us.MyCompany.com`）に格納されます。
- 同じ DIT 構造がサード・パーティ・ディレクトリと Oracle Internet Directory の両方で保持されます。すべてのユーザーが、値 `cn=users,dc=us,dc=MyCompany,dc=com` で識別される同じ users サブツリーに表示されます。

図 17-2 に示した例では、1 対 1 のドメイン・マッピングを使用して、`users` サブツリーのみをサード・パーティ・ディレクトリから Oracle Internet Directory に同期化する必要があります。

注意 : 図 17-2 では 2 つのディレクトリのトポロジは同じですが、これは図示のためのみであるので注意してください。2 つのディレクトリは、同じドメインに存在する必要はありません。Oracle Internet Directory は、サード・パーティ・ディレクトリに接続できるのであれば、ネットワークのどこにあってもかまいません。

さらに、例では同期がサード・パーティ・ディレクトリから Oracle Internet Directory への一方向ですが、かわりに同期を双方向に行うこともできます。

統合環境の計画

この項では、統合環境の計画方法について説明します。内容は次のとおりです。

- サード・パーティ・ディレクトリとの統合に関する予備的な考慮事項
- 企業の中央ディレクトリとなるディレクトリの選択
- LDAP スキーマのカスタマイズ
- パスワードの格納場所の選択
- ディレクトリ情報ツリーの構造の選択
- ログイン名の属性の選択
- ユーザー検索ベースの選択
- グループ検索ベースの選択
- セキュリティ問題に対処する方法の決定
- Oracle Access Manager による配置の管理

サード・パーティ・ディレクトリとの統合に関する予備的な考慮事項

LDAP ディレクトリ・サーバーをすでに所有している企業に Oracle Internet Directory を配置する場合は、両方のディレクトリが同じ環境に共存するように構成する必要があります。

ディレクトリの共存には、次のいずれかの配置が必要です。

- エンタープライズ・ユーザー・セキュリティをサポートするための Oracle Internet Directory との単純な同期。データベース・サーバーの使用により、環境内でエンタープライズ・ユーザーがサポートされている場合は、この方法を使用します。
- Oracle Application Server Infrastructure との完全な統合。これにより、エンタープライズ・ユーザー全員が、Oracle Application Server スイートの各種コンポーネントを使用できるようになります。環境内で企業ディレクトリとしてサード・パーティ・ディレクトリが使用され、Oracle Application Server スイートのアプリケーションが配置されている場合は、この方法を使用します。

すべての Oracle Application Server コンポーネントが ID 管理レルムに依存するため、Oracle Application Server Infrastructure との完全な統合には、そのレルムのコンテナについていくつか決定を行う必要があります。これらの事項を決定した後、ディレクトリ間でブートストラップおよび同期を構成できます。

企業の中央ディレクトリとなるディレクトリの選択

この項では、企業の中央ディレクトリとなるディレクトリの選択方法について説明します。内容は次のとおりです。

- 企業の中央ディレクトリとしての Oracle Internet Directory
- 企業の中央ディレクトリとしてのサード・パーティ・ディレクトリ

企業の中央ディレクトリとしての Oracle Internet Directory

Oracle Internet Directory が中央ディレクトリの場合、ユーザー・オブジェクト、グループ・オブジェクトおよびレルム・オブジェクトを作成すると、Oracle Internet Directory はすべての Oracle コンポーネントおよびサード・パーティ・ディレクトリに関するプロビジョニング情報のソースになります。その後、企業全体のユーザー・オブジェクトとグループ・オブジェクトが、各種 Oracle コンポーネントおよびサード・パーティ・ディレクトリ内に Oracle Internet Directory からプロビジョニングされます。

表 17-1 に、この配置の一般的な要件を示します。

表 17-1 Oracle Internet Directory を企業の中央ディレクトリとして使用する場合の一般的な要件

要件	説明
初期起動	Directory Integration アシスタント（`dipassistant`）により、Oracle Internet Directory に格納されているユーザーおよびグループがサード・パーティ・ディレクトリに移入されます。
同期	ユーザーおよびグループ情報は、Oracle Internet Directory で管理されます。その情報への変更は、インポート・プロファイルが構成されたときに、Oracle Directory Integration Server によりサード・パーティ・ディレクトリと同期化されます。 サード・パーティ・ディレクトリから Oracle Internet Directory への同期は、インポート・プロファイルを構成することによって実行できます。
パスワードおよびパスワード・ベリファイア	パスワードは、Oracle Internet Directory セルフ・サービス・コンソールなどの Oracle ツールを使用して Oracle Internet Directory で管理されます。パスワードの変更は、Oracle Directory Integration Server によってサード・パーティ・ディレクトリと同期化されます。ただし、このサーバーでパスワードの変更を同期化する前に、マッピング・ルールにパスワードの同期を構成する必要があります。 パスワードは安全に管理されるため、パスワードを同期化するためのサード・パーティ・ディレクトリとの通信は、SSL で行う必要があります。サーバー認証モードで、サード・パーティ・ディレクトリからの適切な資格証明により、Oracle Directory Integration Server を実行します。サード・パーティ・ディレクトリも SSL に対応していることを確認してください。 Oracle 環境にパスワード・ベリファイアが必要な場合は、ユーザー・エントリを作成するか、またはパスワードを変更すると、パスワード・ベリファイアが自動的に生成されます。
Oracle Application Server Single Sign-On	ユーザーは、OracleAS Single Sign-On Sever を使用して、Oracle 環境にログインします。 Oracle ディレクトリ・サーバーは、ユーザーの認証のために OracleAS Single Sign-On Server からコールされると、ローカルで使用可能な資格証明を使用します。外部認証は起動しません。 ユーザーが Oracle 環境内の各種コンポーネントにアクセスするためにログインするのは 1 回のみです。

Oracle Internet Directory の新しいユーザーまたはグループは、Oracle Directory Integration Platform によって自動的にプロビジョニングできます。この自動プロビジョニングには、次の条件が必要です。

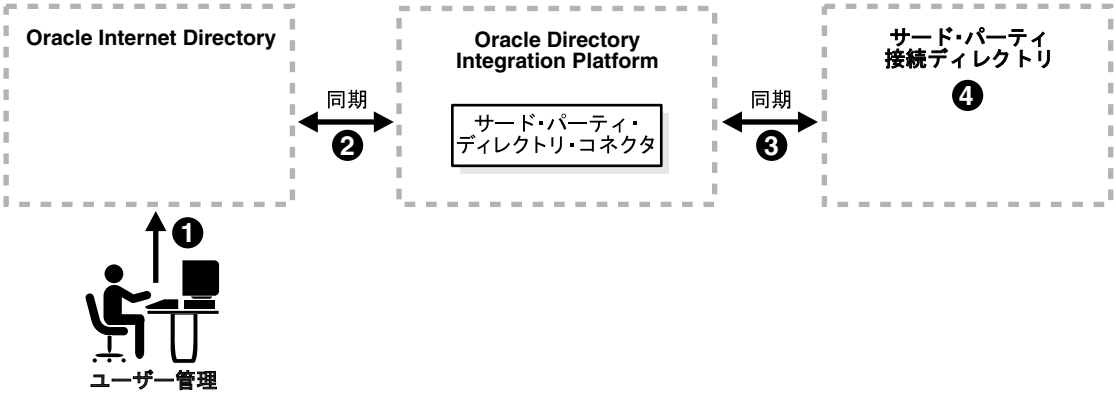
- Oracle ディレクトリ・サーバーが、変更ログが有効な状態で稼働している。
- 変更ログはパージされない。

これら 2 つの条件が満たされていない場合、Oracle Internet Directory のエントリを LDIF ファイルにダンプし、サード・パーティ・ディレクトリに対してそのデータをアップロードする必要があります。

> **関連資料：** 変更ログのパージについては、『Oracle Internet Directory 管理者ガイド』のガベージ・コレクションに関する章を参照してください。

図 17-3 に、Oracle Internet Directory が企業の中央ディレクトリとなっている場合の通常の配置を示します。

図 17-3 Oracle Internet Directory を企業の中央ディレクトリとして使用するコンポーネント間の相互作用



17-10 ページの図 17-3 が示すように、Oracle Internet Directory が企業の中央ディレクトリの場合、ユーザーまたはグループの通常のプロビジョニングは次のプロセスに従います。

1. ユーザー・エントリまたはグループ・エントリは、Oracle Internet Directory セルフ・サービス・コンソール、Oracle Directory Manager またはコマンドライン・ツールを使用して Oracle Internet Directory に作成されます。
2. 次にスケジュールされた間隔に、エントリ作成イベントが、Oracle Directory Integration Platform 内のサード・パーティ・ディレクトリ・コネクタによって読み取られます。
3. 統合プロファイル内のマッピング情報に従って、Oracle Internet Directory 内のユーザー属性またはグループ属性が、サード・パーティ・ディレクトリのスキーマで必要とされるとおりに、対応するユーザー属性またはグループ属性に適切にマップされます。
4. ユーザー・エントリおよびグループ・エントリがサード・パーティ・ディレクトリ内に作成されます。

次の場合、Oracle Internet Directory 内でユーザー・エントリが変更されます。

- 新しい属性がエントリに追加される場合
- 既存の属性の値が変更される場合
- 既存の属性が削除される場合

Oracle Internet Directory が企業の中央ディレクトリの場合、ユーザー・エントリまたはグループ・エントリの変更時に実行されるイベントの順序は次のとおりです。

1. Oracle Internet Directory セルフ・サービス・コンソール、Oracle Directory Manager またはコマンドライン・ツールを使用して、エントリが変更されます。
2. 次にスケジュールされた間隔に、エントリ変更イベントが、Oracle Directory Integration Platform 内のサード・パーティ・ディレクトリ・コネクタによって読み取られます。
3. 統合プロファイル内のマッピング情報に従って、Oracle Internet Directory 内の属性が、接続ディレクトリ内の対応する属性に適切にマップされます。
4. サード・パーティ・ディレクトリ内でユーザー・エントリが変更されます。

企業の中央ディレクトリとしてのサード・パーティ・ディレクトリ

サード・パーティ・ディレクトリが企業の中央ディレクトリの場合、ユーザー・オブジェクト、グループ・オブジェクトおよびレルム・オブジェクトを作成すると、サード・パーティ・ディレクトリはすべての Oracle コンポーネントおよびその他のディレクトリに関するプロビジョニング情報のソースになります。この場合、Oracle Internet Directory は Oracle コンポーネントのサポート用に配置されます。このサポートを提供するために、Oracle Internet Directory には、サード・パーティ・ディレクトリ内のエントリの識別を可能にするフットプリントが格納されています。

表 17-2 に、この配置の一般的な要件を示します。

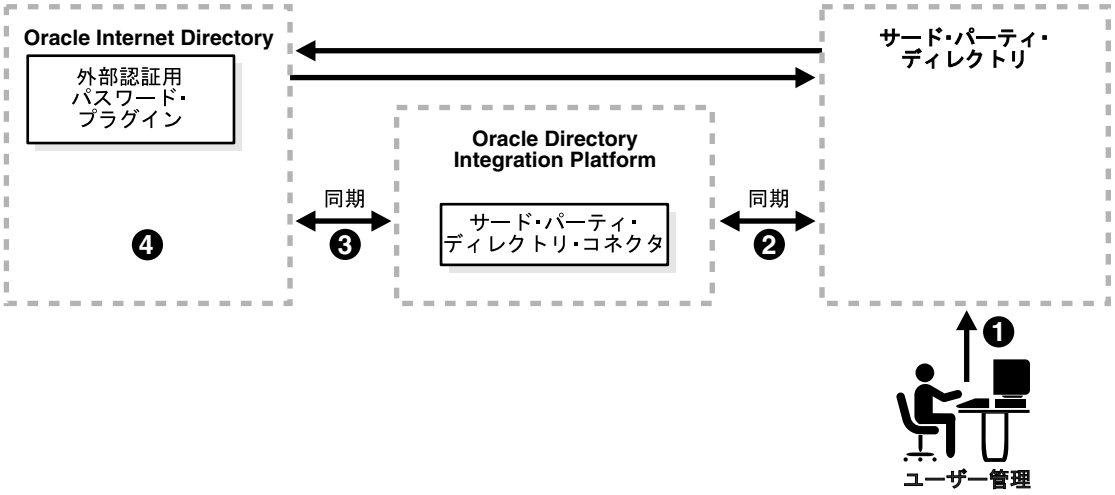
表 17-2 サード・パーティ・ディレクトリを企業の中央ディレクトリとして使用する場合の一般的な要件

要件	説明
初期起動	Directory Integration アシスタント（`dipassistant`）により、サード・パーティ・ディレクトリに格納されているユーザーおよびグループが Oracle Internet Directory に移入されます。 サード・パーティ・ディレクトリでのみ、パスワード資格証明などのユーザー情報の管理を選択できます。そのような配置では、Oracle 環境でシングル・サインオンを有効にするために、Oracle Directory Integration Server により、Oracle コンポーネントで必要なユーザー・エントリ属性のみを同期化できます。 パスワードは、サード・パーティ・ディレクトリから Oracle Internet Directory へ移行されません。
同期	ユーザーおよびグループ情報の中央ディレクトリはサード・パーティ・ディレクトリです。サード・パーティ・ディレクトリでのユーザーおよびグループ情報への変更は、インポート・プロファイルが構成されたときに、Oracle Directory Integration Server により Oracle Internet Directory と同期化されます。 Oracle Internet Directory からサード・パーティ・ディレクトリへの同期は、エクスポート・プロファイルを構成することによって実行されます。
パスワードおよびパスワード・ベリファイア	パスワードは、サード・パーティ・ディレクトリで管理されます。パスワードの変更は、Oracle Directory Integration Server によって Oracle Internet Directory に同期化されません。
Oracle Application Server Single Sign-On	ユーザーは、OracleAS Single Sign-On Sever を使用して、Oracle 環境に 1 回のみログインします。 サード・パーティ・ディレクトリでのみ資格証明を持つユーザーは、外部認証プラグインを起動する Oracle ディレクトリ・サーバーによって認証されます。 Oracle Internet Directory で資格証明を持つユーザーは、Oracle ディレクトリ・サーバーによってローカルで認証されます。
サード・パーティ・ディレクトリ外部認証プラグイン	サード・パーティ・ディレクトリでユーザーの資格証明を管理するときに、このプラグインが必要です。ユーザーを認証するために、OracleAS Single Sign-On Server により Oracle ディレクトリ・サーバーがコールされます。このプラグインによって、サード・パーティ・ディレクトリに格納されているユーザーの資格証明に対するユーザーの認証が実行されます。

サード・パーティ・ディレクトリに作成された新しいユーザーまたはグループは、Oracle Directory Integration Server によって、Oracle Internet Directory に自動的に同期化されます。プロビジョニングが実行される前に、サード・パーティ・ディレクトリと Oracle Internet Directory 間で一方向の同期が確立されている必要があります。

図 17-4 に、サード・パーティ・ディレクトリが企業の中央ディレクトリとなっている場合の通常の配置を示します。

図 17-4 サード・パーティ・ディレクトリを企業の中央ディレクトリとして使用するコンポーネント間の相互作用



ユーザーまたはグループのプロビジョニング・プロセス 図 17-4 が示すように、サード・パーティ・ディレクトリが企業の中央ディレクトリの場合、ユーザーまたはグループの通常のプロビジョニングは次のプロセスに従います。

1. ユーザー・エントリまたはグループ・エントリがサード・パーティ・ディレクトリ内に作成されます。
2. 次にスケジュールされた間隔に、エントリ作成イベントが、Oracle Directory Integration Platform 内のサード・パーティ・ディレクトリ・コネクタによって読み取られます。
3. 統合プロファイル内のマッピング情報に従って、サード・パーティ・ディレクトリのユーザー属性またはグループ属性が Oracle Internet Directory 内の対応する属性にマップされます。
4. ユーザー・エントリまたはグループ・エントリが Oracle Internet Directory 内に作成されます。

ユーザー・エントリまたはグループ・エントリの変更プロセス 次の場合、サード・パーティ・ディレクトリ内でエントリが変更されます。

- 新しい属性がエントリに追加される場合
- 既存の属性の値が変更される場合
- 既存の属性が削除される場合

サード・パーティ・ディレクトリが企業の中央ディレクトリの場合、ユーザー・エントリまたはグループ・エントリの変更は次のプロセスに従います。

1. サード・パーティ・ディレクトリ内でエントリが変更されます。
2. 次にスケジュールされた間隔に、エントリ変更イベントが、Oracle Directory Integration Platform 内のサード・パーティ・ディレクトリ・コネクタによって読み取られます。
3. 統合プロファイル内のマッピング情報に従って、サード・パーティ・ディレクトリ内の属性が Oracle Internet Directory 内の対応する属性に適切にマップされます。

4. Oracle Internet Directory 内でユーザー・エントリまたはグループ・エントリが変更されます。

図 17-4 が示すように、サード・パーティ・ディレクトリが企業の中央ディレクトリの場合、パスワード・リポジトリとして動作しているディレクトリ内でパスワードの変更が非同期的に発生します。これは、プラグインを使用することによって発生します。

LDAP スキーマのカスタマイズ

次の場合、LDAP スキーマをカスタマイズする必要があります。

- ディレクトリ配置に、カスタム・オブジェクト・クラス、カスタム属性などのスキーマ拡張が含まれている場合
- カスタム属性を、ディレクトリ・サーバー間で同期化する必要がある場合

LDAP スキーマをカスタマイズするには、次のことを行う必要があります。

- ソース・ディレクトリでスキーマ拡張を識別します。
- データの移行および同期を開始する前に、ターゲット・ディレクトリでスキーマ拡張を作成します。

注意： スキーマ拡張の作成に加えて、対応するオブジェクト・クラスと同期化させる属性も、マッピング・ルールに追加する必要があります。

関連資料：

- Oracle Internet Directory のスキーマをカスタマイズする方法は、『Oracle Internet Directory 管理者ガイド』のスキーマの管理に関する章を参照してください。
- Microsoft Active Directory のスキーマをカスタマイズする方法は、`http://msdn.microsoft.com/` にある Microsoft のドキュメントを参照してください。

パスワードの格納場所の選択

企業の中央ディレクトリとなるディレクトリに関係なく、パスワードは、一方または両方のディレクトリに格納できます。いずれのオプションにも長所と短所があります。この項では 2 つのオプションを比較します。内容は次のとおりです。

- 1 つのディレクトリにのみパスワードを格納する場合の長所と短所
- 両方のディレクトリにパスワードを格納する場合の長所と短所

1 つのディレクトリにのみパスワードを格納する場合の長所と短所

1 つのディレクトリにのみパスワードを格納すると、エントリ・ポイントの数を減らすことになるため、パスワードのセキュリティがより強力になります。また、パスワードが変更された場合の同期の問題もなくなります。

ただし、1 つのディレクトリにのみパスワードを格納すると、ネットワーク全体に対するシングル・ポイント障害の原因となります。サード・パーティ・ディレクトリで障害が発生した場合、ユーザーは、Oracle Internet Directory 内でユーザー・フットプリントが使用可能な場合でも Oracle コンポーネントにアクセスできません。

中央ディレクトリにのみパスワードを格納すると同期の問題はなくなりますが、アプリケーションでユーザーをそのディレクトリに対して認証できるようにする必要があります。これには、適切なプラグインを使用する必要があります。たとえば、企業の中央ディレクトリおよび中央パスワード・ストアの両方として Microsoft Active Directory を使用している場合は、Microsoft Active Directory に対してユーザーを認証するアプリケーションを有効にする必要があります。これには、外部認証プラグインを使用します。

注意： Oracle コンポーネントは、パスワード・ベリファイアを使用してユーザーを認証します。パスワードがサード・パーティ・ディレクトリに格納される場合、それらのベリファイアは Oracle Internet Directory に格納されません。Oracle コンポーネントを使用してパスワードが変更された場合は、Oracle Internet Directory 内でベリファイアが生成され、格納されます。

両方のディレクトリにパスワードを格納する場合の長所と短所

Oracle Internet Directory とサード・パーティ・ディレクトリの両方にパスワードを格納する場合、理想的には、リアルタイムでパスワードを同期化する必要があります。

Oracle Internet Directory 10*g*（10.1.4.0.1）の場合、パスワードはリアルタイムではなく、スケジュールに従って同期化されます。これは、企業の中央ディレクトリ内でパスワードが変更された時刻とその変更がもう 1 つのディレクトリに記録される時刻の間に、明確な差があることを意味します。

中央ディレクトリとして Oracle Internet Directory を配置した場合、パスワード値は、Oracle Internet Directory から接続ディレクトリへ定期的に同期化されます。これには、レルムのパスワード・ポリシーと可逆暗号化の両方を有効にする必要があります。

関連資料：

- パスワード・ポリシーの設定については、『Oracle Internet Directory 管理者ガイド』のパスワード・ポリシーに関する章を参照してください。
- 可逆暗号化の詳細は、『Oracle Internet Directory 管理者ガイド』のパスワード・ベリファイアのディレクトリ格納に関する章を参照してください。

通常、パスワード値はハッシュされます。両方のディレクトリが同一のハッシング・アルゴリズムを使用する場合は、そのままの状態でハッシュ値を同期化できます。たとえば、Sun Java System Directory と Oracle Internet Directory が統合されている環境があるとします。これらのディレクトリは両方とも共通のハッシング・アルゴリズムに対応しています。Oracle Internet Directory でサポートされているハッシング方法を使用して、パスワードをハッシュし、Sun Java System Directory に格納する場合、Sun Java System Directory のパスワードの Oracle Internet Directory への同期化は、その他の属性の場合と同様です。両方のディレクトリで同一のハッシング・アルゴリズムがサポートされていない場合は、クリアテキスト形式でのみパスワードを同期化する必要があります。セキュリティ上の理由から、Oracle Internet Directory とのパスワードの同期は、SSL サーバー認証モードでのみ可能です。

Oracle Internet Directory が中央ディレクトリである場合や、Oracle Internet Directory でサポートされているハッシング・アルゴリズムがその他のディレクトリでサポートされていない場合でも、パスワードの可逆暗号化が有効なときには SSL サーバー認証モードによる同期化が可能です。

Microsoft Active Directory が中央ディレクトリである場合に Microsoft Active Directory 内でパスワードを変更すると、プラグインがパスワード変更を遮断して Oracle Internet Directory に送信します。Oracle Internet Directory が中央ディレクトリで、中央パスワード・ストアである場合、Oracle Directory Integration Platform がパスワード変更を特権ユーザーとして読み取り、対応するディレクトリに送信します。

注意： 両方のディレクトリが同一のハッシング・アルゴリズムを使用しない配置では、Oracle Internet Directory のデフォルトのインストール環境ではパスワードの同期化は実行できません。構成する必要があります。

Oracle Internet Directory が中央ディレクトリではない配置では、サード・パーティ・ディレクトリによってパスワード・ポリシーが施行されます。サード・パーティ・ディレクトリに対する認証リクエストがある場合、このディレクトリから認証が成功したか失敗したかの応答があります。ただし、サード・パーティ・ディレクトリからのパスワード・ポリシーの詳細なエラーは、Oracle Internet Directory に配信されないため、クライアント・アプリケーションにも配信されません。

関連資料： プラグインの詳細は、次の章を参照してください。

- 『Oracle Internet Directory 管理者ガイド』のディレクトリ・プラグイン・フレームワークに関する章
- 『Oracle Internet Directory 管理者ガイド』の外部認証プラグインのカスタマイズに関する章

ディレクトリ情報ツリーの構造の選択

インストール時に、各ディレクトリ・サーバーがデフォルトのドメインとデフォルトの**ディレクトリ情報ツリー**構造を作成します。Oracle Internet Directory インフラストラクチャのインストールにより、企業内のユーザーおよびグループの格納用に指定されたコンテナで、デフォルトのレルムが作成されます。サード・パーティ・ディレクトリと統合する場合は、Oracle Internet Directory のデフォルトのインストールを使用するために、両方のディレクトリで同一の DIT 構造を作成する必要があります。または、ドメイン・レベルのマッピングを実行できます。

この項の内容は次のとおりです。

両方のディレクトリ上での同一ディレクトリ情報ツリー構造の作成

両方のディレクトリ上で同一のディレクトリ情報ツリーを構成することをお薦めします。これによって、すべてのユーザー・オブジェクトとグループ・オブジェクトをそのままの状態で同期化できるため、一方のディレクトリ内の識別名を持つエントリを別のディレクトリの URL にマップする必要がなくなります。また、このようなマッピングで発生する可能性があるパフォーマンスの問題も回避できます。

同一のディレクトリ情報ツリーを作成するには、まず、企業の中央ディレクトリとなるディレクトリを決定し、その後、それにあわせてもう一方のディレクトリ情報ツリーを変更します。ディレクトリ統合プロファイルを更新して、確実にドメイン・レベルのルールを反映してください。

ユーザーが Oracle Application Server Single Sign-On を介して Oracle アプリケーションにアクセスできるようにするには、ディレクトリ情報ツリーを、独自の認証および認可ドメインを持つ個別の ID 管理レルムとして識別することをお薦めします。

関連資料：『Oracle Internet Directory 管理者ガイド』の ID 管理レルムの配置に関する章

識別名のマッピングおよび制限

両方のディレクトリ上に同一のディレクトリ情報ツリーを持つことが不可能な場合は、Oracle Internet Directory と接続ディレクトリの間でドメインをマップする必要があります。たとえば、コンテナ dc=mydir,dc=com の下にあるエントリはすべて、Oracle Internet Directory 内の dc=myoid,dc=com の下で同期化する必要があります。これを実行するには、ドメイン・レベルのマッピング・ルールに指定します。

すべてのユーザーおよびグループの同期が目的の場合は、適切な識別名マッピングですべてのユーザー・エントリを同期化できます。ただし、グループ・エントリを同期化する場合は、時間がかかり、制限が追加される場合があります。この項では、識別名マッピングが行われている場合のユーザーおよびグループ両方の同期の例を示します。

例 : ユーザー・エントリ・マッピング マッピング・ファイルでは、Sun Java System Directory 内のエントリは uid=name,ou=people,o=iplanet.org という形式をとるとします。また、Oracle Internet Directory 内のエントリは、cn=name,cn=users,dc=iplanet,dc=com という形式をとるとします。Sun Java System Directory 上のネーミング属性は uid ですが、Oracle Internet Directory 上では cn です。

マッピング・ファイルには次のようなルールがあります。

```
DomainRules
ou=people,o=iplanet.org: cn=users,dc=iplanet,dc=com: cn=%, cn=users,dc=iplanet,dc=com
AttributeRules
Uid:1: :person:cn: :inetorgperson:
```

最終行の第 2 列の 1 という値は、各変更が Sun Java System Directory から Oracle Internet Directory へ伝播される場合に、uid 属性が必要であることを示しています。これは、Oracle Internet Directory 内のエントリの識別名を構成するには、uid を使用可能にする必要があるためです。

例 : グループ・エントリ・マッピング 識別名マッピングが行われている場合、グループ・エントリの同期化は複雑になります。グループ・メンバーシップ（識別名）には、同期後、有効な識別名の値が必要です。これは、ユーザー識別名に対して行われた識別名マッピングをグループ・メンバーシップの値に適用する必要があることを意味します。

たとえば、ユーザー識別名の値を次のようにマップするとします。

```
ou=people,o=iplanet.org: cn=users,dc=iplanet,dc=com:
```

これは、ou=people,o=iplanet.org の下のすべてのユーザー・エントリが cn=users,dc=iplanet,dc=com に移動することを示します。

グループ・メンバーシップは、次のようにマップする必要があります。

```
uniquemember: : : groupofuniquenames: uniquemember:
:groupofuniquenames:dnconvert(uniquemember)
```

たとえば、uniquemember の値が cn=testuser1,ou=people,o=iplanet.org の場合、その値は cn=testuser1,cn=users,dc=iplanet,dc=com になります。

また、uniquemember の値が cn=testuser1,dc=subdomain,ou=people,o=iplanet.org の場合、その値は cn=testuser1,dc=subdomain,cn=users,dc=iplanet,dc=com になります。

これは、ネーミング属性または RDN 属性が両方のディレクトリで同じ場合に適した解決方法です。ネーミング属性が ou=people,o=iplanet.org:cn=users,dc=iplanet,dc=com:cn=%,cn=users,dc=iplanet,dc=com などのようにそれぞれのディレクトリで異なる場合、グループ・メンバーシップの実際の識別名は、指定したマッピング・ルールでは導出できません。現在、このような場合に、uniquemember またはその他の識別名タイプの属性に対して識別名マッピングを行うことはできません。

グループ・メンバーシップを同期化する場合は、ソース・ディレクトリと宛先ディレクトリに同じネーミング属性を指定してください。

> **関連項目 :** マッピング・ルールの指定方法は、6-5 ページの「マッピング・ルールの構成」を参照してください。

ログイン名の属性の選択

ログイン名の属性には、Oracle コンポーネントにログインする際のエンド・ユーザーの識別情報が含まれます。この属性は、Oracle Internet Directory のコンテナ cn=common,cn=products,cn=oracleContext,*identity_management_realm* の下に、属性 orclcommonnicknameattribute の値として格納されます。

デフォルトでは、orclcommonnicknameattribute 属性の値は uid です。これは、ログインに使用される識別情報がユーザー・エントリの uid 属性に格納されることを意味します。

接続ディレクトリにログイン用の特定の属性が存在する場合は、Oracle Internet Directory 内の正しい orclcommonnicknameattribute にその属性をマップする必要があります。これは、サード・パーティ・ディレクトリとの同期に関連付けられているコネクタ用のマッピング・ファイルにある、マッピング・ルールの 1 つであることが必要です。

たとえば、Oracle Internet Directory を Microsoft Active Directory と同期させるとします。また、後者では、ログイン識別子がユーザー・エントリの userPrincipalName 属性に含まれているとします。userPrincipalName 属性の値を Oracle Internet Directory に同期させ、orclcommonnicknameattribute 属性の値である uid 属性に格納します。このマッピングは、ディレクトリ統合プロファイル内のマッピング・ルールに反映する必要があります。

ログイン識別子用のその他の属性も使用できます。たとえば、ログインに employeeID を使用する場合は、それに応じてマッピング・ルールを設定できます。この設定は、構成には影響しません。

注意： orclcommonnicknameattribute 属性は Oracle Application Server Single Sign-On で広範囲に使用されるため、属性をサード・パーティ・ディレクトリの属性にどのようにマップするかを慎重に計画してください。この属性を変更した場合は、変更を有効にするために、Oracle Application Server Single Sign-On をリフレッシュする必要があります。

関連資料： ログイン名の属性の設定手順は、『Oracle Identity Management 委任管理ガイド』を参照してください。

ユーザー検索ベースの選択

ユーザー検索コンテキストは、ユーザーが存在するすべてのコンテナをリストする複数値属性によって表されます。配置に応じて、ユーザー集団全体にわたるユーザー検索コンテキスト値を設定するか、Oracle Internet Directory セルフ・サービス・コンソールを使用してユーザー検索コンテキスト属性にコンテナを追加します。

関連資料： ユーザー検索コンテキストの設定手順は、『Oracle Identity Management 委任管理ガイド』を参照してください。

グループ検索ベースの選択

グループ検索コンテキストは、グループが存在するすべてのコンテナをリストする複数値属性によって表されます。配置に応じて、すべてのグループ・エントリにわたるグループ検索コンテキスト値を設定するか、Oracle Internet Directory セルフ・サービス・コンソールを使用してグループ検索コンテキスト属性にコンテナを追加します。

関連資料： グループ検索コンテキストの設定手順は、『Oracle Identity Management 委任管理ガイド』を参照してください。

セキュリティ問題に対処する方法の決定

セキュリティ上の 3 つの主要な問題を考慮する必要があります。

- アクセス・ポリシー : ユーザー検索ベースとグループ検索ベースを不正なユーザーによるアクセスから適切に保護する必要があります。
- 同期 : Oracle Internet Directory およびサード・パーティ・ディレクトリへの接続時に SSL を使用するように Oracle Directory Integration Server を構成できます。これを実行すると、ディレクトリ・サーバー間で交換されるすべての情報が保護されます。
- パスワードの同期化 : 構成に応じて、パスワードを同期化できます。たとえば、Oracle Internet Directory が企業の中央ディレクトリの場合は、パスワードの変更を接続ディレクトリに通信できます。パスワードを同期化する場合は、ディレクトリ間の通信を SSL サーバー認証モードで構成することをお薦めします。

関連項目 : 18-11 ページの「SSL モードでの同期用サード・パーティ・ディレクトリ・コネクタの構成」

Oracle Access Manager による配置の管理

Oracle Access Manager を使用して、サード・パーティ・ディレクトリと同期する Oracle Internet Directory の配置を管理するには、同期化されたユーザーが Oracle Access Manager で表示できることを保証する必要があります。

関連資料 : Oracle Access Manager でユーザーを管理する方法の詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

Microsoft Active Directory 統合の概念

この項では、Oracle Internet Directory と Microsoft Active Directory との統合に関するその他の考慮事項について説明します。内容は次のとおりです。

- Microsoft Active Directory から Oracle Internet Directory への同期化
- Windows ネイティブ認証
- Microsoft Active Directory 用の Oracle Internet Directory スキーマ要素
- 複数の Microsoft Active Directory ドメイン・コントローラとの統合
- 複数ドメイン Microsoft Active Directory 環境との同期化
- 外部セキュリティ・プリンシパル

関連項目 : 第 19 章「Microsoft Active Directory との統合」

Microsoft Active Directory から Oracle Internet Directory への同期化

Microsoft Active Directory から Oracle Internet Directory へ変更を同期化するために、Oracle Directory Integration Platform では、Microsoft Active Directory 変更追跡メカニズムで使用可能になる増分変更をインポートします。Oracle Directory Integration Platform では、次の 2 つの Microsoft Active Directory 変更追跡メカニズムをサポートします。

- DirSync 方式。Microsoft Active Directory でサポートされる LDAP コントロールを使用します。
- USN-Changed 方式。エントリの属性を使用します。

いずれの方式でも、変更が導出されるディレクトリに対して、Microsoft Active Directory コネクタによりスケジュールされた間隔で問合せが行われます。各方式には、長所と短所があります。表 17-3 に、これら 2 つの方式の相違点を示します。

表 17-3 DirSync 方式と USN-Changed 方式の比較

考慮事項	DirSync 方式	USN-Changed 方式
キーの変更	エントリの一意の識別子である ObjectGUID に変更を渡します。	識別名に変更を渡します。ObjectGUID は識別名の変更の追跡に使用されます。
エラー処理	エラー状態の結果、同期が停止した場合、次のサイクル中に、適用済の変更がすべて読み取られ、スキップされます。	同期が原子性を持つ必要はありません。同期が停止した場合、同期が中断されたエントリから、次の同期サイクルが開始します。
検索結果の情報	変更は、変更された属性と新しい値のみです。このため USN-Changed 方式より速くなる可能性があります。	変更エントリのすべての属性が取得されます。取得された値は、Oracle Internet Directory に格納されている古い値と比較され、更新されます。このため DirSync 方式より時間がかかる可能性があります。
複数値の属性の変更	複数値の属性に加えられた増分変更を、属性値の完全置換として反映します。	複数値の属性に加えられた増分変更を、属性値の完全置換として反映します。
同期点の追跡方法	ディレクトリ内の変更を問い合せたときに、ディレクトリの状態を識別する Cookie 値に基づく増分変更が渡されます。	USNChanged 属性（長整数、すなわち 8 バイト）に基づいて、ディレクトリ内の変更を問い合せます。値を変更して、同期を開始する点を調整できます。
必須のユーザー権限	ユーザーは、対象となるネーミング・コンテキストに対する変更のレプリケート権限が必要です。これにより、Microsoft Active Directory 内のすべてのオブジェクトおよび属性を、それらに対するアクセス保護に関係なく、読み取ることができます。 関連資料 : DirSync 方式の使用時に Microsoft Active Directory ユーザーに権限を割り当てる方法については、Microsoft Knowledge Base Article 303972（http://support.microsoft.com/ で入手可能）を参照してください。このコンテキストには、この記事にある Microsoft Active Directory 管理エージェントに使用される方法を適用します。	Microsoft Active Directory ユーザーには、Oracle Internet Directory に対して同期化するすべての必須属性を読み取る権限が必要です。 関連資料 : USN-Changed 方式の使用時に、Microsoft Active Directory ユーザーに権限を割り当てる方法については、Microsoft ライブラリ（http://msdn.microsoft.com/）で入手可能な Microsoft のネットワーキングおよびディレクトリ関連のドキュメントを参照してください。
複数ドメインのサポート	異なるドメイン内のエントリに加えられた変更を読み取るには、異なるドメイン・コントローラへの個々の接続が必要です。	グローバル カタログ サーバーに接続することで、複数のドメインに加えられた変更を取得できます。 関連項目 : 17-24 ページの「複数ドメイン Microsoft Active Directory 環境との同期化」

表 17-3 DirSync 方式と USN-Changed 方式の比較（続き）

考慮事項	DirSync 方式	USN-Changed 方式
異なる Microsoft Active Directory ドメイン・コントローラへの切替え時のレプリケートされたディレクトリからの同期	同期は続行可能です。レプリケートされた環境に接続するときも同期キーは同じです。	次のことが必要です。 ■ 既知のポイントに対する完全同期化 ■ USNChanged 値の更新 ■ フェイルオーバー・ディレクトリとの同期開始 関連項目 : 19-17 ページの「同一ドメイン内の異なる Microsoft Active Directory ドメイン・コントローラへの切替え」
同期の有効範囲	ディレクトリ内のすべての変更を読み取り、必須エントリへの変更のみを Oracle Internet Directory に伝播します。	特定のサブツリーで変更の同期を有効にします。
ロード・バランサの背後に複数の Microsoft Active Directory Server を配置した環境の可用性	-	特定の Microsoft Active Directory ドメイン・コントローラに接続するか、グローバル カタログに接続します。次の場合にグローバル カタログに接続します。 ■ インポート操作のみに関心がある場合 ■ グローバル カタログに、同期化するすべてのエントリおよび属性が含まれている場合 ■ グローバル カタログのパフォーマンスが許容範囲内である場合

関連項目： 5-4 ページの「Oracle Internet Directory から接続ディレクトリへの同期」

Windows ネイティブ認証

この項では、Windows ネイティブ認証を Oracle Directory Integration Platform とともに使用する方法について説明します。内容は次のとおりです。

- Windows ネイティブ認証の概要
- 複数の Microsoft Active Directory ドメインに対するユーザーの認証
- Windows ネイティブ認証によるアプリケーション認証メカニズムの上書き

Windows ネイティブ認証の概要

Windows ネイティブ認証は、Microsoft Windows での Microsoft Internet Explorer ユーザーの認証方法です。この機能が OracleAS Single Sign-On で有効な場合、ユーザーは OracleAS Single Sign-On のパートナ・アプリケーションに自動的にログインします。このためにユーザーは、Windows のドメインへのログイン時に取得した Kerberos 資格証明を使用します。

Internet Explorer バージョン 5.0 以上では、Simple and Protected GSS-API Negotiation Mechanism（SPNEGO）プロトコルを使用して、ユーザーの Kerberos 資格証明をリクエスト先の Kerberos 対応の Web サーバーに自動的に渡すことができます。これにより、Web サーバーは資格証明を復号化してそのユーザーを認証できます。

Microsoft 統合セキュリティやその他のタイプのセキュリティ・メカニズムは、Oracle Application Server Single Sign-On を Windows ネイティブ認証と統合する際に使用できません。SPNEGO プロトコルは、Kerberos バージョン 5 と NT Lan Manager（NTLM）の両方の認証方法をサポートしますが、Oracle Application Server 10*g*（10.1.4.0.1）では、SPNEGO 使用の Kerberos V5 のみをサポートします。

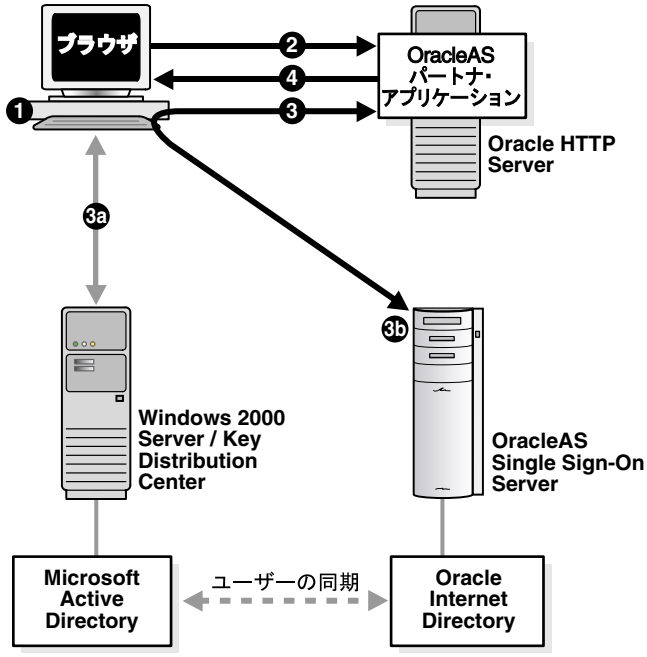
注意： この章では Windows 2000 についてのみ説明しますが、Windows XP プラットフォームも Windows ネイティブ認証をサポートしています。

ブラウザが Internet Explorer 5.0 以上でない場合、Oracle Identity Management では、OracleAS Single Sign-On を使用してユーザー認証を行います。外部ディレクトリに対する認証は、外部認証プラグインを使用して行われます。

次の手順は、シングル・サインオンで保護されたアプリケーションにユーザーがアクセスするときのプロセスを示しています（17-21 ページの図 17-5 を参照）。

1. ユーザーは Windows コンピュータで Kerberos レルム（ドメイン）にログインします。
2. ユーザーは、Internet Explorer を使用して Single Sign-On パートナ・アプリケーションへのアクセスを試みます。
3. アプリケーションは、ユーザーを認証するために Single Sign-On Server にルーティングします。このルーティングの一環として、次の動作が行われます。
   a. ブラウザは、Key Distribution Center（KDC）から Kerberos セッション・チケットを取得します。
   b. OracleAS Single Sign-On Server では、Kerberos セッション・チケットを検証し、ユーザーは、認可されると、リクエストした URL へのアクセスを許可されます。
4. このアプリケーションによって、ユーザーの必要とするコンテンツが表示されます。

図 17-5 Windows ネイティブ認証の流れ



ユーザーが Windows セッションからログアウトすると、このアプリケーションとアクセスされたすべてのシングル・サインオン・アプリケーションからも、同時にログアウトします。

Microsoft Active Directory が中央ディレクトリである配置で Windows ネイティブ認証を使用するには、ユーザーは Microsoft Active Directory 内に存在する必要があります。Windows ネイティブ認証が有効な場合、ローカルの Oracle Internet Directory ユーザーがシングル・サインオン・サーバーを起動するには、ユーザー・エントリごとに `orclsamaccountname` 属性と `krbprincipalname` 属性を移入する必要があります。

複数の Microsoft Active Directory ドメインに対するユーザーの認証

1 つのフォレストに属する複数の Microsoft Active Directory ドメインに対してユーザーを認証するには、グローバル カタログを作成し、認証のために Oracle Application Server Single Sign-On をそのグローバル カタログに接続します。しかし、ドメインが同じフォレストに属さない場合は、ドメイン間でドメイン信頼を作成する必要があります。構成手順の詳細は、19-7 ページの「Windows ネイティブ認証の構成」を参照してください。

Windows ネイティブ認証によるアプリケーション認証メカニズムの上書き

Windows ネイティブ認証は、アプリケーションの既存の認証メカニズムを自動的に上書きしません。Windows ネイティブ認証と Oracle Application Server Single Sign-On を内部認証メカニズムを含むアプリケーションで使用するには、次のタスクのいずれかを実行する必要があります。

- アプリケーションの内部認証メカニズムを削除する。
- アプリケーションを Oracle Application Server Single Sign-On の外部アプリケーションとして構成する。この作業には、有効なアプリケーション・ユーザーの名前とパスワードをアプリケーション構成に格納し、ユーザーが Oracle Application Server Single Sign-On を使用してログインした後に、認証プロセスをユーザーに対して透過的にする必要があります。詳細は、『Oracle Application Server Single Sign-On 管理者ガイド』を参照してください。

Microsoft Active Directory 用の Oracle Internet Directory スキーマ要素

表 17-4 に、Microsoft Active Directory からインポートされるユーザー用の Oracle Internet Directory スキーマ要素を示します。

表 17-4 Microsoft Active Directory 用の Oracle Internet Directory スキーマ要素

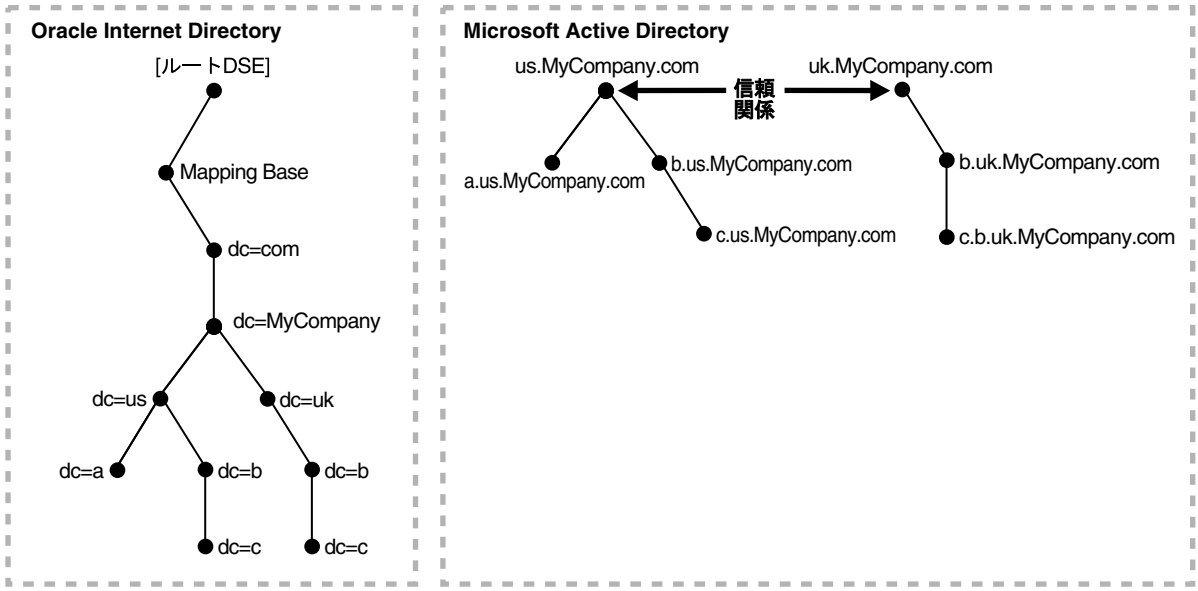
スキーマ要素	説明
`orclObjectGUID`	Microsoft Active Directory から Oracle Internet Directory に移行されたユーザーおよびグループに対する Microsoft Active Directory の `OBJECTGUID` 属性値を格納します。
`orclObjectSID`	Microsoft Active Directory から Oracle Internet Directory に移行されたユーザーおよびグループに対する Microsoft Active Directory の `OBJECTSID` 属性値を格納します。
`orclSAMAccountName`	Microsoft Active Directory の `SAMAccountName` 属性値を格納します。Oracle Internet Directory では、この属性はディレクトリ文字列型として定義されます。しかし、Microsoft Active Directory では、この属性に特殊文字または印刷不可能文字を使用できません。この属性を保持するエントリを Oracle Internet Directory に追加する場合は、単純なテキスト文字列しか入力できず、そうしないと Oracle Internet Directory から Microsoft Active Directory への同期は失敗します。
`orclUserPrincipalName`	Microsoft Active Directory ユーザーの Kerberos ユーザー・プリンシパル名を格納します。
`orclADGroup`	Microsoft Active Directory のグループ属性を格納します。これらのグループ属性は、Oracle Directory Integration 環境における Microsoft Active Directory のグループ・オブジェクトと Oracle Internet Directory のグループ・オブジェクトの同期に使用されます。
`orclADUser`	Microsoft Active Directory のユーザー属性を格納します。これらのユーザー属性は、Oracle Directory Integration 環境における Microsoft Active Directory のユーザー・オブジェクトと Oracle Internet Directory のユーザー・オブジェクトの同期に使用されます。
`orclSourceObjectDN`	Microsoft Active Directory の各エントリに対する識別名を表します。この値は、両方のディレクトリ間に異なるドメインがマップされている場合の外部認証の実行に必要です。

関連資料： Microsoft Active Directory 用の Oracle Internet Directory スキーマ要素の詳細は、『Oracle Identity Management ユーザー・リファレンス』を参照してください。

複数の Microsoft Active Directory ドメイン・コントローラとの統合

複数のドメインを持つ Microsoft Active Directory の配置では、単一の DIT にすることも、複数の DIT を組み合せることもできます。Microsoft Active Directory では、DIT のグループをフォレストと呼びます。図 17-6 に、Microsoft Active Directory のフォレストが Oracle Internet Directory にどのように反映されるかを示します。

図 17-6 Oracle Internet Directory と Microsoft Active Directory 内のフォレストとのマッピング



このディレクトリでは、2 つのドメイン・ツリーが 1 つのフォレストを構成しています。これらのツリーは信頼関係にあります。つまり、一方のドメインのユーザーは、他方のドメインのドメイン・コントローラにより認証されます。Microsoft Active Directory のこのフォレストは、Oracle Internet Directory 内の同一構造のサブツリーにマップされます。

Oracle Internet Directory が中央ディレクトリである配置の考慮事項

複数の Microsoft Active Directory ドメインが存在する場合は、Microsoft Active Directory ドメインの数と同じ回数 Directory Integration アシスタント（`dipassistant`）を実行する必要があります。これを実行するたびに、ターゲットの Microsoft Active Directory Server で必要な特定のデータ・セットを選択します。

Oracle Directory Integration Platform によって、それぞれの Microsoft Active Directory ドメイン内のユーザーおよびグループがプロビジョニングされます。プロビジョニングが行われるには、Oracle Internet Directory から Microsoft Active Directory ドメインへの一方向の同期を構成する必要があります。

Microsoft Active Directory が中央ディレクトリである配置の考慮事項

複数の Microsoft Active Directory サーバーがある場合、Microsoft Active Directory の各ドメインからデータをブートストラップする必要があります。Microsoft Active Directory から Oracle Internet Directory への一方向の同期にグローバル カタログを使用する場合は、グローバル カタログ サーバーから 1 回だけブートストラップする必要があります。

Oracle Directory Integration Platform によって、それぞれの Microsoft Active Directory ドメインから Oracle Internet Directory にユーザーおよびグループが同期化されます。プロビジョニングが実行される前に、Oracle Internet Directory と各 Microsoft Active Directory ドメインのドメイン・コントローラ間で一方向の同期が確立されている必要があります。

複数ドメイン Microsoft Active Directory 環境との同期化

この項では、複数ドメイン Microsoft Active Directory 環境との同期化の考慮事項について説明します。内容は次のとおりです。

Microsoft Active Directory から Oracle Internet Directory へのインポートに必要な構成

通常、インポートを行うには、DirSync 方式または USN-Changed 方式のいずれを使用しているかに関係なく、Microsoft Active Directory ドメインごとに 1 つインポート・プロファイルを構成する必要があります。ただし、USN-Changed 方式を使用している場合は、グローバル カタログを使用すれば、Microsoft Active Directory フォレスト全体からインポートできます。グローバル カタログを使用するにはインポート・プロファイルを 1 つ構成するだけですが、次の考慮事項に注意してください。

- グローバル カタログは読取り専用であるため、Oracle Internet Directory にデータをインポートする場合にのみ使用できます。
- グローバル カタログにはすべての属性は含まれていませんが、使用可能な属性は Microsoft Active Directory で構成できます。
- グローバル カタログは認証のポイントであるため、このポイントから同期が開始されると追加のオーバーヘッドが発生する可能性があります。

> **関連資料 :** Microsoft Active Directory スキーマ内のグローバル カタログの属性については、Microsoft Help and Support（`http://support.microsoft.com/`）にある Microsoft Knowledge Base Article 256938 を参照してください。

Oracle Internet Directory から Microsoft Active Directory へのエクスポートに必要な構成

複数ドメイン Microsoft Active Directory 環境と統合するために、Oracle Directory Integration Platform では、各 Microsoft Active Directory ドメインから構成情報を取得します。Microsoft Active Directory ドメインの数と同数のエクスポート・プロファイルを構成する必要があります。

例 : 複数のサード・パーティ・ディレクトリ・ドメインとの統合

複数のドメインを持つサード・パーティ・ディレクトリの配置では、単一の DIT にすることも、複数の DIT を組み合せることもできます。図 17-7 に、サード・パーティ・ディレクトリの複数のドメインがどのように Oracle Internet Directory の DIT にマップされるかを示します。

図 17-7 Oracle Internet Directory と Microsoft Active Directory 内の複数のドメイン間のマッピングの例

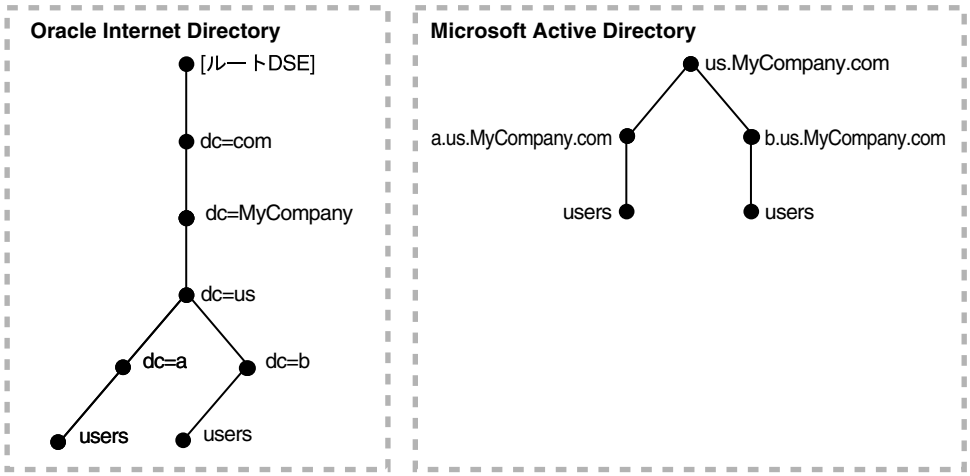


図 17-7 では、サード・パーティ・ディレクトリ環境に 1 つの親ドメインと 2 つの子ドメインがあります。

最初の子ドメイン `a.us.MyCompany.com` は、Oracle Internet Directory の `dc=a,dc=us,dc=MyCompany,dc=com` にマップされます。2 番目の子ドメイン `b.us.MyCompany.com` は、Oracle Internet Directory の `dc=b,dc=us,dc=MyCompany,dc=com` にマップされます。サード・パーティ・ディレクトリ環境の共通ドメイン・コンポーネント `us.MyCompany.com` は、Oracle Internet Directory のデフォルト ID 管理レルム、この場合は `dc=us,MyCompany,dc=com` にマップされます。

外部セキュリティ・プリンシパル

Microsoft Active Directory のユーザーやコンピュータ・アカウントは、コンピュータや人などの物理エンティティを表します。ユーザー・アカウントおよびコンピュータ・アカウントは、グループと同様に、セキュリティ・プリンシパルと呼ばれます。セキュリティ・プリンシパルは、自動的にセキュリティ識別子を割り当てられるディレクトリ・オブジェクトです。セキュリティ識別子を持つオブジェクトは、ネットワークにログインし、ドメイン・リソースにアクセスできます。ユーザー・アカウントまたはコンピュータ・アカウントは、次のことに使用されます。

- ユーザーまたはコンピュータの識別情報の認証
- ドメイン・リソースへのアクセス権の認可または否認
- 他のセキュリティ・プリンシパルの管理
- ユーザー・アカウントまたはコンピュータ・アカウントを使用して実行されるアクションの監査

たとえば、エンタープライズ管理者グループのメンバーであるユーザー・アカウントまたはコンピュータ・アカウントは、フォレスト内のすべてのドメイン・コントローラで、ログインの許可を自動的に付与されます。

ユーザー・アカウントおよびコンピュータ・アカウントは、Microsoft Active Directory Users and Computers を使用して、追加、無効化、リセットおよび削除されます。

Microsoft Active Directory の信頼関係では、あるドメインのユーザーは、別のドメインのドメイン・コントローラにより認証されます。信頼関係は、推移的にも非推移的にもなります。

- 推移的な信頼関係では、あるドメインに拡張された信頼関係は、そのドメインを信頼する他のすべてのドメインに自動的に拡張されます。たとえば、A、B、C の 3 つのドメインがあり、B と C は A と直接の信頼関係にあるとします。この場合、B と C の間にも信頼関係が生じます。これは、B と C の間には直接の信頼関係はありませんが、どちらも A と直接の信頼関係にあるためです。
- 非推移的な信頼関係では、信頼は直接関係のある 2 つのドメインに限定され、フォレスト内の他のドメインには適用されません。

あるフォレストの Windows 2000 ドメインと、そのフォレスト外の Windows 2000 ドメインの間に信頼関係が確立されている場合、外部ドメインからのセキュリティ・プリンシパルは、フォレスト内のリソースへのアクセス権を付与されます。外部ドメインからのセキュリティ・プリンシパルは、外部セキュリティ・プリンシパルと呼ばれ、Microsoft Active Directory では外部セキュリティ・プリンシパル・オブジェクトとして表されます。これらの外部セキュリティ・プリンシパルは、フォレスト外のドメインからメンバーを受け入れるドメイン・ローカル・グループのメンバーになることができます。

外部セキュリティ・プリンシパルは、Microsoft Active Directory 環境の 2 つのドメイン間に非推移的な信頼関係がある場合に使用されます。

Microsoft Active Directory 環境の非推移的な信頼関係では、あるドメインが別のドメインからの外部セキュリティ・プリンシパルを認識すると、そのエンティティは識別名エントリのように表されます。そのエントリでは、RDN コンポーネントは、信頼関係のドメインにおける元のエントリの SID に設定されます。グループの場合は、外部セキュリティ・プリンシパルの識別名が、信頼関係のドメインにおける元のエントリの識別名としてではなく、メンバーの値として表されます。このため、外部セキュリティ・プリンシパルが Oracle Internet Directory と同期化されるときに問題が発生する可能性があります。

Sun Java System Directory 統合の概念

この項では、Oracle Internet Directory と Sun Java System Directory との統合に関するその他の考慮事項について説明します。内容は次のとおりです。

- Sun Java System Directory から Oracle Directory Integration Platform への同期
- Sun Java System Directory 用の Oracle Internet Directory スキーマ要素

関連項目： 第 21 章「Sun Java System Directory との統合」

Sun Java System Directory から Oracle Directory Integration Platform への同期

Sun Java System Directory は、ディレクトリ・オブジェクトへの増分変更が保存される変更ログを保持します。Sun Java System Directory から Oracle Internet Directory への同期は、この変更ログを活用します。

関連資料：

- 5-4 ページの「Oracle Internet Directory から接続ディレクトリへの同期」
- 変更ロギングを有効にして Oracle ディレクトリ・サーバーを起動する方法は、『Oracle Identity Management ユーザー・リファレンス』の Oracle Internet Directory サーバー管理ツールに関する章を参照してください。
- 変更ロギングの構成方法については、Sun Java System Directory のドキュメントを参照してください。Sun Java System Directory バージョン 5.0 以上と同期させる場合は、Retro Change Log プラグインを有効にする必要があります。

Sun Java System Directory 用の Oracle Internet Directory スキーマ要素

Oracle Internet Directory には、Sun Java System Directory からインポートされるユーザー用の `orclSourceObjectDN` 要素があります。`orclSourceObjectDN` 要素は、Sun Java System Directory の各エントリの識別名を表します。この値は、両方のディレクトリ間に異なるドメインがマップされている場合の外部認証の実行に必要です。

Novell eDirectory および OpenLDAP 統合の概念

この項では、Oracle Internet Directory と Novell eDirectory または OpenLDAP との統合に関するその他の考慮事項について説明します。内容は次のとおりです。

- Novell eDirectory または OpenLDAP から Oracle Internet Directory への同期
- Novell eDirectory 用の Oracle Internet Directory スキーマ要素
- OpenLDAP 用の Oracle Internet Directory スキーマ要素

関連項目： 第 22 章「Novell eDirectory または OpenLDAP との統合」

Novell eDirectory または OpenLDAP から Oracle Internet Directory への同期

Novell eDirectory または OpenLDAP から Oracle Internet Directory へ変更を同期化するために、Oracle Directory Integration Platform では、Novell eDirectory または OpenLDAP の各エントリの変更タイムスタンプを評価します。最後の同期の実行時間よりも新しいタイムスタンプを持つエントリが Oracle Internet Directory で更新されます。

Novell eDirectory または OpenLDAP で削除されたエントリについて、Oracle Directory Integration Platform では、Oracle Internet Directory のエントリと Novell eDirectory または OpenLDAP との間で線形比較して削除済エントリを識別します。つまり、両方のディレクトリのエントリが指定された間隔で比較されます。Oracle Internet Directory と Novell eDirectory または OpenLDAP の両方で使用できないエントリは削除されます。ディレクトリ・エントリが比較される際にサーバーでのパフォーマンスの低下を回避するために、DIT の特定のサブセットを検索するように比較をカスタマイズできます。

関連項目：

- 5-4 ページの「Oracle Internet Directory から接続ディレクトリへの同期」
- Oracle Internet Directory と Novell eDirectory または OpenLDAP との間での削除の同期時に DIT の特定のサブセットを検索する方法の詳細は、22-4 ページの「手順 6: 削除を同期化するための Novell eDirectory または OpenLDAP コネクタのカスタマイズ」を参照してください。

Novell eDirectory 用の Oracle Internet Directory スキーマ要素

表 17-5 に、Novell eDirectory からインポートされるユーザー用の Oracle Internet Directory スキーマ要素を示します。

表 17-5 Novell eDirectory 用の Oracle Internet Directory スキーマ要素

スキーマ要素	説明
orclSourceObjectDN	Novell eDirectory の各エントリに対する識別名を表します。この値は、両方のディレクトリ間に異なるドメインがマップされている場合の外部認証の実行に必要です。
orclndsobjectguid	Novell eDirectory の各エントリに対する GUID 値を表します。この値は、同期キーとして使用されます。
orclsourcemodifytimestamp	Novell eDirectory の各エントリの modifytimestamp 属性を表します。この値は、同期化する必要があるエントリの取得に使用されます。
orclsourceCreateTimestamp	Novell eDirectory の各エントリの createtimestamp 属性を表します。この値は、削除済エントリの同期に使用されます。
orclndsobject	Novell eDirectory の NDS オブジェクトを表します。

関連資料： Novell eDirectory 用の Oracle Internet Directory スキーマ要素の詳細は、『Oracle Identity Management ユーザー・リファレンス』を参照してください。

OpenLDAP 用の Oracle Internet Directory スキーマ要素

表 17-6 に、OpenLDAP からインポートされるユーザー用の Oracle Internet Directory スキーマ要素を示します。

表 17-6 OpenLDAP 用の Oracle Internet Directory スキーマ要素

スキーマ要素	説明
orclSourceObjectDN	OpenLDAP の各エントリに対する識別名を表します。この値は、両方のディレクトリ間に異なるドメインがマップされている場合の外部認証の実行に必要です。
orclOpenLdapEntryUUID	OpenLDAP の各エントリに対する entryUUID 値を表します。この値は、同期キーとして使用されます。
orclsourcemodifytimestamp	OpenLDAP の各エントリの modifytimestamp 属性を表します。この値は、同期化する必要があるエントリの取得に使用されます。
orclsourceCreateTimestamp	OpenLDAP の各エントリの createtimestamp 属性を表します。この値は、削除済エントリの同期に使用されます。
orclopenldapobject	OpenLDAP オブジェクトを表します。

関連資料： OpenLDAP 用の Oracle Internet Directory スキーマ要素の詳細は、『Oracle Identity Management ユーザー・リファレンス』を参照してください。

Oracle Internet Directory 10*g*（10.1.4.0.1）でのサード・パーティ統合の制限事項

Oracle Internet Directory 10*g*（10.1.4.0.1）では、スキーマおよび ACL の同期はサポートされません。スキーマまたは ACL を変更する場合は、手動で変更を適用する必要があります。Oracle Internet Directory とサード・パーティ・ディレクトリ間でスキーマを同期化するには、`schemasync` ツールを使用します。

関連資料：『Oracle Identity Management ユーザー・リファレンス』の Oracle Directory Integration Platform ツールの章の `schemasync` に関する項を参照してください。

18

サード・パーティ・ディレクトリとの同期の構成

この章では、Oracle Internet Directory とサード・パーティ・ディレクトリとの同期の一般的な方法について説明します。内容は次のとおりです。

- 同期要件の確認
- Express 構成による同期プロファイルの作成
- 拡張統合オプションの構成

注意： この章を読む前に、第 17 章「サード・パーティ・ディレクトリ統合の概念と考慮事項」の内容を理解しておく必要があります。

関連項目： Oracle Internet Directory と特定のサード・パーティ・ディレクトリ間の統合の構成に関する手順については次の各章を参照してください。

- 第 19 章「Microsoft Active Directory との統合」
- 第 21 章「Sun Java System Directory との統合」
- 第 22 章「Novell eDirectory または OpenLDAP との統合」

同期要件の確認

Oracle Internet Directory とサード・パーティ・ディレクトリ間の同期を準備するには、次のようにします。

1. Oracle Internet Directory とサード・パーティ・ディレクトリが稼働していることを確認します。
2. 同期化するコンテナ内の関連エントリの読取りおよび書込みに十分な権限を持つユーザー・アカウントをサード・パーティ・ディレクトリに作成します。ディレクトリで tombstone がサポートされている場合、アカウントには tombstone エントリの読取りに十分な権限も必要です。

   - **サード・パーティ・ディレクトリからのインポート操作 :** ユーザー・アカウントにサブツリー・ルートに対する読取りアクセス権限を付与します。ユーザー・アカウントは、Oracle Directory Integration Platform との同期化が行われるサード・パーティ・ディレクトリ内のソース・コンテナ（サブツリー・ルート）下のすべてのオブジェクトを読み取れることが必要です。サード・パーティ・ディレクトリのユーザー・アカウントに、Oracle Internet Directory と同期化されるすべてのオブジェクトに対する必要な権限があるかどうかを確認するには、次のようにコマンドライン・ユーティリティ `ldapsearch` を使用してサブツリー検索を実行します。

     ```
     $ORACLE_HOME/bin/ldapsearch -h directory host -p directory port -b "DN of
     subtree" -s sub -D "DN of privileged directory user"
     -w "password for privileged directory user" "objectclass=*"
     ```

     `ldapsearch` ユーティリティから返される結果には、同期化されるすべての属性および値を含む、対象の全オブジェクトが含まれている必要があります。

   - **サード・パーティ・ディレクトリへのエクスポート操作 :** ユーザー・アカウントに、Oracle Directory Integration Platform からユーザーをエクスポートする全コンテナの親であるサブツリー・ルートに対する、次の権限を付与します。

     – 書込み
     – すべての子オブジェクトの作成
     – すべての子オブジェクトの削除

     関連資料 : ユーザー・アカウントに対する権限の付与方法については、使用しているサード・パーティ・ディレクトリのドキュメントを参照してください。

     変更ロギングが有効な状態で Oracle Internet Directory が稼働していることと、変更ログのパージ期間が 7 日以上に設定されていることを確認する必要もあります。

     関連資料 :

     - 変更ロギングを有効にして Oracle ディレクトリ・サーバーを起動する方法は、『Oracle Identity Management ユーザー・リファレンス』の Oracle Internet Directory サーバー管理ツールに関する章を参照してください。
     - 変更ログのパージ期間の設定方法は、『Oracle Identity Management ユーザー・リファレンス』の `orclPurgeTargetAge` に関する項を参照してください。

Express 構成による同期プロファイルの作成

この項では、Express 構成による同期プロファイルの作成および構成の方法を説明します。内容は次のとおりです。

Express 構成の概要

Directory Integration アシスタント（dipassistant）には、Express 構成オプションがあります。このオプションでは、事前定義の仮定を使用して、インポート用とエクスポート用の 2 つの同期プロファイルが作成されます。Directory Integration Server がすでに稼働している場合は、プロファイルを有効にすると、ユーザーおよびグループがサード・パーティ・ディレクトリに格納されているコンテナと Oracle Internet Directory 内の cn=users,*default_realm*/cn=groups,*default_realm* との間で、ユーザーおよびグループの同期化をすぐに開始できます。

構成を簡単にするために、Express 構成オプションでは次のことを仮定します。

- Oracle Internet Directory のデフォルト・レルムのユーザー・エントリは、cn=users,*default_realm_DN* コンテナにあります。
- Oracle Internet Directory のデフォルト・レルムのグループ・エントリは、cn=groups,*default_realm_DN* コンテナにあります。
- インストール時に作成された Oracle Directory Integration Platform マスター・マッピング・ルール・ファイルは、$*ORACLE_HOME*/ldap/odi/conf にあります。
- マスター・ドメイン・マッピング・ルールは $*ORACLE_HOME*/ldap/odi/samples にあります。
- ログイン証明書は、Oracle ディレクトリ・サーバー内のユーザー・コンテナに対して、プロファイル、レルムおよびアクセス制御を構成するために十分な権限を持つ Oracle Directory Integration Platform 管理者のものです。Oracle Directory Integration Platform 管理者グループのメンバー（cn=dipadmingrp,cn=dipadmin,cn=directory integration platform,cn=products,cn=oraclecontext）には、必要な権限があります。

次の手順に従い、Express 構成を実行し、サード・パーティ・ディレクトリの cn=users,default_naming_context と Oracle Internet Directory の cn=users,*default_realm* との間で、ユーザーとグループが同期していることを確認します。

1. 18-5 ページの「Express 構成の実行」の指示に従い、Express 構成を実行します。
2. Express 構成により、*profile_name*Import および *profile_name*Export という 2 つのプロファイルが作成されます。デフォルトでは、プロファイルはいずれも無効になっています。サード・パーティ・ディレクトリから Oracle Internet Directory への同期が必要な場合は、*profile_name*Import プロファイルを有効にします。Oracle Internet Directory からサード・パーティ・ディレクトリへの同期が必要な場合は、*profile_name*Export プロファイルを有効にします。プロファイルを有効にするには、Directory Integration アシスタント（dipassistant）ユーティリティで modifyprofile 操作を使用します。たとえば、次のコマンドにより、myprofileImport というインポート・プロファイルが有効になります。

   ```
   $ORACLE_HOME/bin/dipassistant modifyprofile -host myhost -port myport
   -file import.profile -dn bind_DN -passwd password_of_bind_DN
   -profile myprofileImport odip.profile.status=ENABLE
   ```

3. 4-8 ページの「Oracle Directory Integration Platform の起動、停止および再起動」の指示に従い、Oracle Directory Integration Platform を起動します。

4. スケジューリングの間隔が経過するまで待ち、次のコマンドを入力して同期が開始されたことを確認します。

```
$ORACLE_HOME/bin/ldapsearch -h OID host -p OID port
-D "DN of privileged OID user" -w "password of privileged OID user"
-b "orclodipagentname=import profile,cn=subscriber profile,cn=changelog
subscriber,cn=oracle internet directory" -s base "objectclass=*"
orclodipsynchronizationstatus orclodiplastsuccessfulexecutiontime
```

> **注意：** デフォルトのスケジューリング間隔は 60 秒（1 分）です。Directory Integration アシスタント（dipassistant）を使用すると、デフォルトのスケジューリング間隔を変更できます。詳細は、第 3 章「Oracle Directory Integration Platform 管理ツール」を参照してください。

同期が正常に開始された場合は、次のようになります。

- 「同期ステータス」属性の値は、「同期成功」です。
- 「最終正常実行時間」属性の値は、その実行の具体的な日時です。この値は、現在の日時に近い値である必要があります。

次に、正常な同期を示す結果の例を示します。

```
Synchronization successful 20060515012615
```

> **注意：**
>
> - 日時は、現在の日時に近い値である必要があります。
> - ldapsearch コマンドを実行する場合は、インストール時に指定された、orcladmin パスワードと同一の dipadmin パスワードが必要です。

5. 同期が開始されていることを確認した後、Oracle Internet Directory とサード・パーティ・ディレクトリ内のエントリを調べ、サード・パーティ・ディレクトリの cn=users,default_naming_context と Oracle Internet Directory の cn=users,*default_realm* 間で、ユーザーおよびグループが同期していることを確認します。

Express 構成の実行

Express 構成は、Directory Integration アシスタント（dipassistant）または Oracle Directory Integration Server 管理ツールを使用して実行できます。Oracle Directory Integration Server 管理ツールでの Express 構成オプションは、Microsoft Active Directory との統合の場合のみ使用できます。その他すべてのサポート対象のサード・パーティ・ディレクトリでは、Directory Integration アシスタントを使用して Express 構成を実行する必要があります。各ツールの Express 構成の実行方法は、次の項目を参照してください。

- Directory Integration アシスタントによる Express 構成の実行
- Oracle Directory Integration Server 管理ツールによる Express 構成の実行（Microsoft Active Directory のみ）

注意： 自分の環境用の同期プロファイルをカスタマイズする際に、配置作業を容易にするためにテスト・ユーザーとテスト・グループを追加することが必要になる場合があります。同期プロファイルのカスタマイズとテストが終了したときには、必ずテスト・ユーザーとテスト・グループを削除してください。

注意：インポートとエクスポートの同期プロファイルをうまくカスタマイズするためには、その他の構成タスクがすべて終了するまで、SSL を有効にしないでください。

Directory Integration アシスタントによる Express 構成の実行

この項では、Directory Integration アシスタント（dipassistant）を使用して Express 構成を実行する方法について説明します。サポート対象のサード・パーティ・ディレクトリのいずれにもこのコマンドを使用できます。

Directory Integration アシスタントを使用して Express 構成を実行するには、次のようにします。

1. Directory Integration の Express 構成ツールを次のように起動します。

```
$ORACLE_HOME/bin/dipassistant expressconfig
[-h oracle_internet_directory_host
-p oracle_internet_directory_port -3rdpartyds directory_name
-configset configuration_set_entry]
```

この例の引数は、表 18-1 のとおりです。

表 18-1 Directory Integration の Express 構成ツールの引数

引数	説明
oracle_internet_directory_host	Oracle ディレクトリ・サーバーのホスト。デフォルトはローカル・ホストです。
oracle_internet_directory_port	Oracle Internet Directory の非 SSL ポート。デフォルトは 389 です。
directory_name	サード・パーティ・ディレクトリの名前。次のいずれかの値を入力します。 ■ Active Directory ■ Iplanet ■ Novell eDirectory ■ Openldap ■ adforexchange

表 18-1 Directory Integration の Express 構成ツールの引数（続き）

引数	説明
configuration_set_entry	Oracle Directory Integration Platform の構成設定。デフォルトは 1 です。

2. 要求されたら、次の情報を入力します。
   - Oracle Internet Directory の資格証明。スーパー・ユーザー（cn=orcladmin）か、または Oracle Directory Integration Platform 管理者グループのメンバーである任意のユーザー（cn=dipadmingrp,cn=dipadmin,cn=directory integration platform,cn=products,cn=oraclecontext）を指定する必要があります。
   - 特権ユーザーのサード・パーティ・ディレクトリの接続詳細と資格証明。Microsoft Active Directory との同期化の場合、特権ユーザーは削除済エントリを読み取るために必要な管理権限を持つ必要があります。
   - Novell eDirectory、OpenLDAP、Sun Java System Directory の場合、同期化するコンテナを指定する必要もあります。
   - 作成される同期プロファイルを識別する名前。たとえば、abc という名前を指定した場合、ツールにより abcImport と abcExport という 2 つのプロファイルが作成されます。
   - （オプション）cn=users コンテナでの適切な ACL。ユーザーおよびグループが、cn=users コンテナにある Oracle コンポーネントによって管理されるように選択できます。このように ACL をカスタマイズすると、元の ACL は $*ORACLE_HOME*/ldap/odi/archive/profile_name_prefix_useracl.ldif に保存されます。

Oracle Directory Integration Server 管理ツールによる Express 構成の実行（Microsoft Active Directory のみ）

この項では、Oracle Directory Integration Server 管理ツールを使用して Express 構成を実行する方法について説明します。このコマンドは、Microsoft Active Directory と統合する配置の場合のみ使用できます。

Oracle Directory Integration Server 管理ツールを使用して Express 構成を実行するには、次のようにします。

1. 次のコマンドを入力して、Oracle Directory Integration Server 管理ツールを起動します。

   $*ORACLE_HOME*/bin/dipassistant -gui

2. Oracle Directory Integration Server 管理ツールで、「***directory_server***」、「**統合プロファイルの構成**」の順に展開し、**Microsoft Active Directory コネクタの構成**を選択します。対応するタブ・ページが、右側のペインに表示されます。
3. Microsoft Active Directory コネクタ Express 同期タブ・ページで、適切な値を入力します。
4. 「**適用**」を選択します。

拡張統合オプションの構成

Oracle Directory Integration Platform をインストールすると、サポート対象のサード・パーティ・ディレクトリごとにインポートおよびエクスポートの同期プロファイルのサンプルが自動的に作成されます。18-5 ページの「Express 構成の実行」で説明されているように、Directory Integration アシスタント（dipassistant）の Express 構成オプションを使用して同期プロファイルを追加作成することもできます。インストール・プロセス時または Express 構成によって作成されたインポートおよびエクスポートの同期プロファイルは、Oracle Internet Directory とサード・パーティ・ディレクトリの統合を配置する際に使用する開始点としてのみ利用されます。デフォルトの同期プロファイルは事前定義の仮定を使用して作成されるため、次の項目で説明されているように、環境に合せてそれらをさらにカスタマイズする必要があります。

- レルムの構成
- Access 制御リストのカスタマイズ
- マッピング・ルールのカスタマイズ
- SSL モードでの同期用サード・パーティ・ディレクトリ・コネクタの構成
- Oracle Internet Directory からサード・パーティ・ディレクトリへのパスワードの同期の有効化
- 外部認証プラグインの構成

> **関連項目：** インストール・プロセス時に作成されたサンプルの同期プロファイルの詳細は、個々のサード・パーティ・ディレクトリ統合に関する章を参照してください。

インストール・プロセス時に作成された同期プロファイルのサンプルをカスタマイズするには、Directory Integration アシスタントの createprofilelike（cpl）コマンドでそれらのプロファイルをコピーし、Directory Integration アシスタントの modifyprofile コマンドでそのコピーを有効にします。

レルムの構成

レルムを構成する手順は、次のとおりです。

1. 17-15 ページの「ディレクトリ情報ツリーの構造の選択」での説明や、17-7 ページの「配置の計画」でのより具体的な説明のように、レルム識別名構造を選択します。
2. ユーザーのログイン名の属性を選択します。この属性には、ログインに使用される属性の名前が含まれます。デフォルトでは uid です。詳細は、17-17 ページの「ログイン名の属性の選択」を参照してください。
   - Microsoft Active Directory と統合して、userprincipalname 属性をログインに使用する場合は、userprincipalname を Oracle Internet Directory の uid 属性にマップします。
   - Novell eDirectory または OpenLDAP と統合して、mail 属性をログインに使用する場合は、mail を Oracle Internet Directory の uid 属性にマップします。
3. Oracle Internet Directory で usersearchbase 値と groupsearchbase 値を設定します。これらの値によって、Oracle Internet Directory 内でユーザーおよびグループを検索する場所が、各種 Oracle コンポーネントに指定されます。これらの値は、インストール時にデフォルトの値に設定されます。ただし、2 つのディレクトリ内の DIT 構造に対応するように、これらの値をリセットすることが必要になる場合があります。これらを正しく設定してください。間違って設定すると、同期が正常に機能していても、コンポーネントが Oracle Internet Directory のユーザーやグループにアクセスできないままになる可能性があります。

   ユーザー検索ベースとグループ検索ベースの構成方法は、17-7 ページの図 17-2 を例に説明します。ここで usersearchbase の値は、cn=users,dc=us,dc=MyCompany,dc=com

かその親の 1 つに設定します。同様に、DIT に groups というサブツリーがあるとすると、複数の値のある groupsearchbase 属性は、次の両方に設定します。

- cn=groups,dc=us,dc=MyCompany,dc=com またはその親の 1 つ
- cn=users,dc=us,dc=MyCompany,dc=com

ユーザー検索ベースとグループ検索ベースを構成するには、Oracle Internet Directory セルフ・サービス・コンソールを使用します。

4. Oracle Internet Directory で usercreatebase 値と groupcreatebase 値を設定します。これらの値は、各種 Oracle コンポーネントに、ユーザーおよびグループを作成できる場所を指定します。これらの値は、インストール時にデフォルトの値に設定されます。

   ユーザー作成ベースとグループ作成ベースの構成方法は、17-7 ページの図 17-2 を例に説明します。ここで usercreatebase の値は、cn=users,dc=us,dc=MyCompany,dc=com かその親の 1 つに設定します。同様に、groupcreatebase は cn=groups,dc=us,dc=MyCompany,dc=com またはその親の 1 つに設定します。

   ユーザー作成ベースとグループ作成ベースを構成するには、Oracle Internet Directory セルフ・サービス・コンソールを使用します。

   関連資料：『Oracle Identity Management 委任管理ガイド』の ID 管理レルムの構成設定の変更に関する項

Access 制御リストのカスタマイズ

この項では、インポート・プロファイル、エクスポート・プロファイルおよびその他の Oracle コンポーネント用に、ACL をカスタマイズする方法を説明します。内容は次のとおりです。

- インポート・プロファイル用 ACL のカスタマイズ
- エクスポート・プロファイル用 ACL のカスタマイズ
- その他の Oracle コンポーネント用 ACL

インポート・プロファイル用 ACL のカスタマイズ

インポート・プロファイルは、Oracle Directory Integration Platform で Oracle Internet Directory へのアクセスに使用される識別情報です。ACL により、ユーザー・コンテナおよびグループ・コンテナ、またはアクセスするエントリのあるサブツリーで、インポート・プロファイルによるオブジェクトの追加、変更および削除ができるようにする必要があります。デフォルトでは、インポート・プロファイルは、デフォルト・レルムのレルム管理者グループ（cn=RealmAdministrators, cn=groups,cn=OracleContext,*realm_DN*）の一部です。このグループは、デフォルト・レルムの識別名の下にある任意のエントリに対してあらゆる操作を実行する権限を持ちます。

Oracle Internet Directory 10*g*（10.1.4.0.1）でインストールされるデフォルト・レルムとのインポート同期のために、ACL をカスタマイズする必要はありません。それより前のリリースの Oracle Internet Directory からアップグレードする場合、あるいはデフォルト以外の Oracle Internet Directory レルムと同期が行われる場合、適切なサブツリーまたはコンテナで必要な権限が、同期を処理するインポート・プロファイルに付与されていることを確認します。

LDIF 形式の ACL テンプレートは、$*ORACLE_HOME*/ldap/schema/oid/oidRealmAdminACL.sbs ファイルを参照してください。デフォルト・レルムで ACL を変更しなかった場合、このテンプレート・ファイルは、置換変数をインスタンス化し、%s_SubscriberDN% を Oracle Internet Directory のデフォルト・レルム識別名と、%s_OracleContextDN% を cn=OracleContext,*default_realm_DN* とそれぞれ置換すると、直接適用できます。たとえば、realmacl.ldif がインスタンス化されたファイルの場合、次の ldapmodify コマンドを使用して、このファイルをアップロードできます。

```
$ORACLE_HOME/bin/ldapmodify -h OID host -p OID port
-D "DN of privileged OID user" -w "password of privileged OID user"
-v -f realmacl.ldif
```

関連資料：『Oracle Internet Directory 管理者ガイド』のアクセス制御に関する章

エクスポート・プロファイル用 ACL のカスタマイズ

Oracle Directory Integration Platform でサード・パーティ・ディレクトリにアクセスできるようにするには、サード・パーティ・ディレクトリで識別情報を作成する必要があります。この識別情報は、各エクスポート・プロファイルで構成されます。

その他の Oracle コンポーネント用 ACL

デフォルトの ACL により、ユーザーおよびグループの作成、変更、削除ができますが、それはデフォルト・レルムの下のユーザー・コンテナとグループ・コンテナに限られます。その他のコンテナのオブジェクトを同期化するには、ACL をカスタマイズする必要があります。

Oracle コンポーネント用に ACL をカスタマイズするために使用できるサンプル ACL ファイルがあります。これらのサンプル・ファイルは、$*ORACLE_HOME*/ldap/schema/oid ディレクトリにインストールされています。これには、次のようなものがあります。

- `oidUserAdminACL.sbs`: Oracle コンポーネントのサブツリーに対して、ユーザーの管理やアクセスに必要な権限を付与します。
- `oidGroupAdminACL.sbs`: Oracle コンポーネントのサブツリーに対して、グループの管理やアクセスに必要な権限を付与します。
- `oidUserAndGroupAdminACL.sbs`: Oracle コンポーネントでサブツリー内のユーザーとグループを管理およびアクセスするための権限を付与します。

コンテナごとに必要な権限を付与するように、ACL ポリシーをカスタマイズできます。

関連資料： ACL をカスタマイズする方法は、『Oracle Internet Directory 管理者ガイド』のアクセス制御に関する章を参照してください。

マッピング・ルールのカスタマイズ

同期プロファイルの重要な要素であるマッピング・ルールは、同期化されるディレクトリ情報、および同期化されたときのディレクトリ情報の変換方法を決定します。マッピング・ルールは、要件にあわせて実行時に変更できます。

サンプルの同期プロファイルには、それぞれデフォルトのマッピング・ルールが含まれています。これらのルールには、デフォルトで同期用に構成された、最小限のデフォルトのユーザー属性およびグループ属性が含まれています。

注意： 進行中の同期は、ディレクトリ内の変更より前に構成されたマッピング・ルールに依存します。マッピングの一貫性を確実にするには、同期化済のエントリを削除するか、完全同期を実行することが必要な場合があります。

マッピング・ルールにより、ソース・ディレクトリと宛先ディレクトリが同期化されるときに、データを変換する方法が決定されます。次の変更を行う必要がある場合は、サンプル・プロファイルにあるデフォルトのマッピング・ルールをカスタマイズします。

- 識別名マッピングの変更。識別名マッピングにより、サード・パーティ・ディレクトリの DIT を Oracle Internet Directory の DIT にマップする方法を決定します。
- 同期化する必要がある属性の変更。
- 同期時に発生する変換（マッピング・ルール）の変更。

宛先ディレクトリで変換の結果得られたデータがそのディレクトリのスキーマに一致すれば、どのようなマッピングでも実行できます。

関連資料：

- マッピング・ルールの詳細は、6-5 ページの「マッピング・ルールの構成」を参照してください。
- 一方のディレクトリから他方のディレクトリに同期化する際に、属性値がどのように変換されるかの例は、6-10 ページの「サポートされている属性マッピング・ルールと例」を参照してください。
- インポート・マッピング・ルールの例は、$*ORACLE_HOME*/ldap/odi/conf/activeimp.map.master ファイルを参照してください。

Oracle Internet Directory とサード・パーティ・ディレクトリ間の同期を確立すると、同期プロファイルの属性マッピング・ルールを、配置の要件を満たすようにカスタマイズできます。Express 構成を使用してインポートおよびエクスポートの同期プロファイルを作成すると、各プロファイル用のマッピング・ファイルが、$*ORACLE_HOME*/ldap/conf ディレクトリに作成されます。マッピング・ファイルの名前は、*profile_name*Import.map と *profile_name*Export.map です。たとえば、Express 構成でプロファイル名の指定を要求されたときに abc と入力すると、マッピング・ファイルの名前は abcImport.map と abcExport.map になります。

同期プロファイルの属性マッピング・ルールをカスタマイズする手順は、次のとおりです。

1. サンプルのマッピング・ルール・ファイルの複製を作成します。サンプルのマッピング・ルール・ファイルは、$*ORACLE_HOME*/ldap/odi/conf ディレクトリにあり、各種プロファイル用に map.master の拡張子が付いています。
2. 前述の変更を行うために、サンプル・マッピング・ルール・ファイルを編集します。マッピング・ルールの編集方法は、6-5 ページの「マッピング・ルールの構成」を参照してください。
3. 変更後、次のコマンドを入力します。

   ```
   $ORACLE_HOME/bin/dipassistant modifyprofile -profile profile_name
   -host oid_host -port oid_port -dn DN -passwd password
   odip.profile.mapfile=path_name
   ```

   たとえば、次のようになります。

   ```
   $ORACLE_HOME/bin/dipassistant modifyprofile -profile my_profile
   -host my_host -port 3060 -dn cn=orcladmin -passwd welcome1
   odip.profile.mapfile=my_profile.map
   ```

   関連資料：『Oracle Identity Management ユーザー・リファレンス』の Oracle Directory Integration Platform ツールの章の `dipassistant` に関する項

4. スケジューリングの間隔が経過するまで待ってから、同期化されたユーザーおよびグループをチェックし、属性マッピング・ルールが要件を満たしていることを確認します。

   ヒント： 属性マッピング・ルールをカスタマイズする際に、テスト・ユーザーとテスト・グループを Oracle Internet Directory またはサード・パーティ・ディレクトリに追加すると便利です。

SSL モードでの同期用サード・パーティ・ディレクトリ・コネクタの構成

デフォルトでは、Express 構成により作成されたインポートおよびエクスポート同期プロファイルに対して、SSL は使用できません。SSL モードで同期化するかどうかは、配置要件によって決まります。たとえば、SSL は、パブリック・データの同期化には必要ありませんが、パスワードなどの機密情報の同期化には必要です。Oracle Internet Directory とサード・パーティ・ディレクトリ間で、パスワードの変更を同期化するには、SSL サーバー認証モードを使用する必要があります。

注意： 同期プロファイルを SSL 用に構成する前に、非 SSL モードでユーザーを正常に同期化できることを確認してください。

チャネルを保護するには、次のことが必要です。

- Oracle Internet Directory と Oracle Directory Integration Platform 間の SSL の有効化
- Oracle Directory Integration Platform とサード・パーティ・ディレクトリ間の SSL の有効化

Oracle Internet Directory と Oracle Directory Integration Platform 間の SSL またはそのサーバーとサード・パーティ・ディレクトリ間の SSL を有効にできますが、機密情報を同期化する前に、完全にチャネルを保護することをお薦めします。パスワードの同期化などの場合は、SSL を介してのみ同期化を行うことができます。

SSL を構成するには、次のことを実行する必要があります。

- Oracle ディレクトリ・サーバーを SSL モードで実行します（『Oracle Internet Directory 管理者ガイド』の Secure Sockets Layer（SSL）に関する章を参照）。
- Oracle Directory Integration Platform を SSL モードで実行します（第 2 章「Oracle Directory Integration Platform のセキュリティ機能」を参照）。SSL モードは、Oracle Internet Directory サーバーの起動時と同じモードであることが必要です。Oracle Directory Integration Platform の起動時に、`sslauth` パラメータを、認証なしの場合は `1`、サーバー認証の場合は `2` に指定します。`sslauth` パラメータを指定しない場合は、SSL モードはデフォルトで認証なしに設定されます。
- サード・パーティ・ディレクトリ・サーバーを SSL モードで実行します。SSL を介したサード・パーティ・ディレクトリとの通信では、SSL サーバー認証が必要です。これには、Oracle Internet Directory と Oracle Directory Integration Platform の両方を SSL サーバー認証モードで実行する必要があります。

次の手順を実行し、SSL モードでの接続ディレクトリとの通信を構成します。

1. 統合プロファイルで、通信モードが SSL であることを示すには、`connectedDirectoryURL` 属性を `host:port:1` の形式で構成します。ポート番号が SSL ポートであることを確認します。デフォルトの SSL ポート番号は 636 です。
2. 接続ディレクトリから証明書を生成します。サーバーからのトラスト・ポイント証明書が必要です。外部の証明書サーバーを使用する必要はありません。
3. 証明書を BASE64 エンコード形式にエクスポートします。
4. Oracle Wallet Manager を使用して、Oracle Wallet 内のトラスト・ポイントとして証明書をインポートします。ウォレットを保存する際に、メニュー・バーから「**ウォレット**」を選択した後、「**自動ログイン**」メニュー項目の横のチェック・ボックスを選択して自動ログインを有効にします。
5. $*ORACLE_HOME*/ldap/odi/conf 内の `odi.properties` ファイルにウォレットの場所を指定します。

6. 次のように Directory Integration アシスタントの `modifyprofile` コマンドを使用して、サード・パーティ・ディレクトリの接続情報（ホスト名、プロファイルなど）を変更します。

```
$ORACLE_HOME/bin/dipassistant modifyprofile -h hostName -p ssl_port
-U ssl_mode -profile profile_name
odip.profile.condirurl=ad_host_name:636:1
```

7. 次のコマンドを入力して certWalletPwd ファイルを作成します。

```
dipassistant wpasswd
```

このコマンドにより、certWalletPwd ファイルの作成先となる場所について odi.properties ファイルが読み取られます。要求されたら、ウォレット・パスワードを入力します。

8. `odisrvreg` ユーティリティを使用してサーバーを登録します。次のコマンドは、`odisrvreg` ユーティリティを使用した非 SSL モードでのサーバーの登録方法を示しています。

```
odisrvreg -h hostname -p port -D bindDN -w password
```

関連資料： `odisrvreg` ユーティリティの使用方法の詳細は、『Oracle Identity Management ユーザー・リファレンス』を参照してください。

9. 4-8 ページの「Oracle Directory Integration Platform の起動、停止および再起動」の指示に従い、Oracle Directory Integration Platform を SSL モードで再起動します。

10. テスト・ユーザーを追加し、正常に同期することを確認します。テスト・ユーザーが正常に同期しない場合、SSL 構成のトラブルシューティングを行います。

注意： Oracle Directory Integration Platform では、クライアント / サーバー認証モードでの SSL はサポートされていません。

関連資料：

- `dipassistant` コマンドを SSL モードで実行する方法の詳細は、『Oracle Identity Management ユーザー・リファレンス』を参照してください。
- 4-7 ページの「Oracle Internet Directory と接続ディレクトリの SSL 証明書の管理」

Oracle Internet Directory からサード・パーティ・ディレクトリへのパスワードの同期の有効化

Oracle Internet Directory からサード・パーティ・ディレクトリにパスワードを同期化するには、Oracle ディレクトリ・サーバーでパスワード・ポリシーとパスワードの可逆暗号化を有効にする必要があります。これを行うには、`1` の値を、`cn=PwdPolicyEntry,cn=common,cn=products,cn=oraclecontext,DN_of_realm` エントリの `orclPwdPolicyEnable` 属性と `orclpwdEncryptionEnable` 属性に指定します。そのためには、Oracle Directory Manager を使用するか、`ldapmodify` を使用して次の内容の LDIF ファイルをアップロードします。

```
dn:cn=PwdPolicyEntry,cn=common,cn=products,cn=oraclecontext,DN_of_realm.
changetype: modify
replace: orclpwdpolicyenable
orclpwdpolicyenable: 1
-
replace: orclpwdencryptionenable
orclpwdencryptionenable: 1
```

関連資料： パスワード・ポリシーの設定方法の詳細は、『Oracle Internet Directory 管理者ガイド』を参照してください。

外部認証プラグインの構成

10*g*（10.1.4.0.1）から、Oracle Directory Integration Platform では、Java ベースの外部認証プラグインがサポートされます。Microsoft Active Directory と Sun Java System Directory にしか対応していない以前の PL/SQL ベースのプラグインのかわりに、Java プラグインを使用することをお薦めします。

新しいプラグイン用の構成ツールは `oidexcfg` という Java プログラムです。このプログラムを使用して、Microsoft Active Directory、Sun Java System Directory、Novell eDirectory および OpenLDAP の Java ベースの外部認証プラグインを構成します。ツールでは、単一ドメインで機能するようにしか外部認証プラグインを設定しません。複数ドメインで機能するように外部認証プラグインを設定するには、追加手順を実行する必要があります。

この項の内容は次のとおりです。

外部認証プラグインの構成

外部認証プラグインを構成するには、Directory Integration アシスタント（`dipassistant`）ユーティリティの `extauth` 操作を使用します。`extauth` 操作の使用方法の詳細は、『Oracle Identity Management ユーザー・リファレンス』の Oracle Directory Integration Platform ツールの章の `dipassistant` に関する項を参照してください。

複数のドメインに対する外部認証の構成

複数の外部認証ドメインで機能するように外部認証プラグインを設定する場合は、外部構成ツールの実行後にいくつかの手順を手動で実行する必要があります。次のように設定を続行します。

1. 「外部認証プラグインの構成」で説明されているように、外部認証プラグインを構成します。
2. 手順 1 で構成ツールにより作成されたプラグイン構成エントリを検索し、検索結果をファイルに出力します。次のような `ldapsearch` コマンドを使用します。

```
ldapsearch -p 3060 -D cn=orcladmin -w welcome -s sub -L \
    -b "cn=plugin,cn=subconfigsubentry" cn="oidexplg_*_ad" >> output.ldif
```

この例では、Microsoft Active Directory の `cn` が表示されます。表 18-2 に示すように、構成したプラグインのタイプに正しいプラグインの `cn` を使用します。例に示すように、`*` をワイルドカードとして使用できます。

表 18-2 外部認証プラグインの識別名

プラグイン・タイプ	識別名
Microsoft Active Directory	`cn=oidexplg_compare_ad, cn=plugin,cn=subconfigsubentry` `cn=oidexplg_bind_ad, cn=plugin,cn=subconfigsubentry`
Sun Java System Directory	`cn=oidexplg_compare_iplanet, cn=plugin,cn=subconfigsubentry` `cn=oidexplg_bind_iplanet, cn=plugin,cn=subconfigsubentry`
Novell eDirectory	`cn=oidexplg_compare_Novell eDirectory, cn=plugin,cn=subconfigsubentry` `cn=oidexplg_bind_Novell eDirectory, cn=plugin,cn=subconfigsubentry`

表 18-2 外部認証プラグインの識別名（続き）

プラグイン・タイプ	識別名
OpenLDAP	cn=oidexplg_compare_openldap, cn=plugin,cn=subconfigsubentry cn=oidexplg_bind_openldap, cn=plugin,cn=subconfigsubentry

3. 出力ファイルを調べます。Microsoft Active Directory プラグインの場合、出力ファイルは次のようになります。

```
dn: cn=oidexplg_compare_ad,cn=plugin,cn=subconfigsubentry
cn: oidexplg_compare_ad
objectclass: orclPluginConfig
objectclass: top
orclpluginname: oidexplg.jar
orclplugintype: operational
orclpluginkind: Java
orclplugintiming: when
orclpluginldapoperation: ldapcompare
orclpluginsecuredflexfield;walletpwd: welcome1
orclpluginsecuredflexfield;walletpwd2: welcome
orclpluginversion: 1.0.1
orclpluginisreplace: 1
orclpluginattributelist: userpassword
orclpluginentryproperties: (!(&(objectclass=orcladobject)(objectclass=orcluserv2)))
orclpluginflexfield;host2: host.domain.com
orclpluginflexfield;port2: 636
orclpluginflexfield;isssl2: 1
orclpluginflexfield;host: host.domain.com
orclpluginflexfield;walletloc2: /location/wallet
orclpluginflexfield;port: 389
orclpluginflexfield;walletloc: /tmp
orclpluginflexfield;isssl: 0
orclpluginflexfield;isfailover: 0
orclpluginclassreloadenabled: 0
orclpluginenable: 0
orclpluginsubscriberdnlist: cn=users,dc=us,dc=oracle,dc=com

dn: cn=oidexplg_bind_ad,cn=plugin,cn=subconfigsubentry
cn: oidexplg_bind_ad
objectclass: orclPluginConfig
objectclass: top
orclpluginname: oidexplg.jar
orclplugintype: operational
orclpluginkind: Java
orclplugintiming: when
orclpluginldapoperation: ldapbind
orclpluginversion: 1.0.1
orclpluginisreplace: 1
orclpluginentryproperties: (!(&(objectclass=orcladobject)(objectclass=orcluserv2)))
orclpluginclassreloadenabled: 0
orclpluginflexfield;walletloc2: /location/wallet
orclpluginflexfield;port: 389
orclpluginflexfield;walletloc: /tmp
orclpluginflexfield;isssl: 0
orclpluginflexfield;isfailover: 0
orclpluginflexfield;host2: host.domain.com
orclpluginflexfield;port2: 636
orclpluginflexfield;isssl2: 1
orclpluginflexfield;host: host.domain.com
orclpluginenable: 0
```

```
orclpluginsecuredflexfield;walletpwd: welcome1
orclpluginsecuredflexfield;walletpwd2: welcome
orclpluginsubscriberdnlist:
cn=users,dc=us,dc=oracle,dc=com
```

4. 次のように、出力ファイルから LDIF ファイルを新規作成します。

   a. エントリ名を変更します。前の手順で示した例では、`cn=oidexplg_compare_ad,cn=plugin, cn=subconfigsubentry` を `cn=oidexplg_compare_ad1, cn=plugin,cn=subconfigsubentry` に、`cn=oidexplg_bind_ad, cn=plugin,cn=subconfigsubentry` を `cn=oidexplg_bind_ad1, cn=plugin,cn=subconfigsubentry` に変更します。

   b. `orclpluginenable` の値を変更します。有効にする場合は値 `1` を、無効にする場合は値 `0` を使用します。

   c. 外部ディレクトリのホスト名とポート番号について、`orclpluginflexfield;host` と `orclpluginflexfield;port` の値を変更します。

   d. `orclpluginflexfield;isssl` の値を変更します。外部ディレクトリに対して SSL 接続を有効にする場合は値 `1` を、無効にする場合は値 `0` を使用します。値 `1` を使用する場合は、ウォレット・ロケーションとパスワードについて、`orclpluginflexfield;walletloc` と `orclpluginsecuredflexfield;walletpwd` の値も変更する必要があります。

   e. `orclpluginflexfield;isfailover` の値を変更します。バックアップ外部ディレクトリに対してフェイルオーバーを設定する場合は、値 `1` を使用します。値 `1` を使用する場合は、ホスト名とポート番号について、`orclpluginflexfield;host2` と `orclpluginflexfield;port2` の値も変更する必要があります。バックアップ・ディレクトリ・サーバーに対して SSL 接続を使用するには、`orclpluginflexfield;walletloc2` と `orclpluginsecuredflexfield;walletpwd2` の値を変更する必要があります。

   f. プラグインの起動ネーミング・コンテキストについて、`orclpluginsubscriberdnlist` を変更します。

   g. プラグインのリクエスト・グループについて、`orclPluginRequestGroup` を変更します。この属性が検索結果の出力にない場合は、LDIF ファイルに属性と値を追加します。

5. 変更したプラグイン構成エントリを Oracle Internet Directory サーバーに追加します。次のようなコマンドを使用します。

```
$ORACLE_HOME/ldap/bin/ldapadd -h host -p port -D cn=orcladmin \
     -w orcladminPwd -v -f input.ldif
```

19

Microsoft Active Directory との統合

この章では、本番環境で Oracle Identity Management と Microsoft Active Directory を統合する手順について説明します。内容は次のとおりです。

- Microsoft Active Directory の同期要件の確認
- Microsoft Active Directory との基本同期の構成
- Microsoft Active Directory との拡張統合の構成
- インポート操作変更追跡での DirSync 方式の使用
- Windows ネイティブ認証の構成
- Oracle Internet Directory 外部セキュリティ・プリンシパル参照と Microsoft Active Directory との同期の構成
- 同一ドメイン内の異なる Microsoft Active Directory ドメイン・コントローラへの切替え
- Microsoft Exchange Server 用の Microsoft Active Directory コネクタの構成

注意： この章を読む前に、『Oracle Internet Directory 管理者ガイド』の Oracle Internet Directory の概念とアーキテクチャに関する章を理解しておく必要があります。また、このマニュアルのここまでの章、特に次の章を理解していることを前提としています。

- 第 1 章「Oracle Identity Management 統合の概要」
- 第 4 章「Oracle Directory Integration Platform の管理」
- 第 5 章「Oracle Directory Synchronization Service」
- 第 17 章「サード・パーティ・ディレクトリ統合の概念と考慮事項」

Microsoft Active Directory との統合のデモンストレーションを構成する場合は、Oracle Identity Management 10*g*（10.1.4.0.1）の Oracle By Example シリーズを参照してください。Oracle Technology Network（`http://www.oracle.com/technology/`）で参照可能です。

Microsoft Active Directory の同期要件の確認

Microsoft Active Directory で基本同期または拡張同期を構成するには、18-2 ページの「同期要件の確認」の指示に従い、使用する環境で必要な同期要件が満たされていることを確認してください。

Microsoft Active Directory との基本同期の構成

Express 構成コマンドを使用すると、Oracle Internet Directory と Microsoft Active Directory 間の同期を迅速に確立できます。Express 構成では、デフォルトの設定を使用してすべての必須構成を自動的に実行し、インポート用とエクスポート用の 2 つの同期プロファイルも作成します。Express 構成を使用して Microsoft Active Directory と同期化するには、18-3 ページの「Express 構成による同期プロファイルの作成」の指示に従ってください。

注意： 18-3 ページの「Express 構成による同期プロファイルの作成」に示す一般的な仮定に加えて、Microsoft Active Directory との統合の場合、Express 構成オプションでは次のことを仮定します。

- 組織単位、ユーザーおよびグループの作成と変更のみが同期化されます。
- サード・パーティ・ディレクトリのユーザーおよびグループのエントリは、`cn=users,default_naming_context` コンテナにあります。

Microsoft Active Directory との拡張統合の構成

Oracle Directory Integration Platform をインストールすると、サポート対象のサード・パーティ・ディレクトリごとにインポートおよびエクスポートの同期プロファイルのサンプルが自動的に作成されます。Microsoft Active Directory 用に作成された同期プロファイルのサンプルは、次のとおりです。

- `ActiveImport`: DirSync 方式を使用して、Microsoft Active Directory から Oracle Internet Directory へ変更をインポートするためのプロファイル
- `ActiveChgImp`: USN-Changed 方式を使用して、Microsoft Active Directory から Oracle Internet Directory へ変更をインポートするためのプロファイル
- `ActiveExport`: Oracle Internet Directory から Microsoft Active Directory へ変更をエクスポートするためのプロファイル

注意： `ActiveImport` または `ActiveChgImp` のいずれを使用するかは、変更の追跡方法で DirSync 方式か USN-Changed 方式のどちらを選択したかによって決まります。

19-2 ページの「Microsoft Active Directory との基本同期の構成」で説明されているように、Directory Integration アシスタント（`dipassistant`）の Express 構成オプションを使用して同期プロファイルを追加作成することもできます。インストール・プロセス時または Express 構成によって作成されたインポートおよびエクスポートの同期プロファイルは、Oracle Internet Directory と Microsoft Active Directory の統合を配置する際に使用する開始点としてのみ利用されます。デフォルトの同期プロファイルは事前定義の仮定を使用して作成されるため、次の手順を順序どおりに実行して、環境に合せてそれらをさらにカスタマイズする必要があります。

- 手順 1: 統合の計画
- 手順 2: レルムの構成
- 手順 3: Microsoft Active Directory から情報を取得する検索フィルタのカスタマイズ
- 手順 4: ACL のカスタマイズ
- 手順 5: 属性マッピングのカスタマイズ
- 手順 6: 複数の Microsoft Active Directory ドメインとの同期

手順 1: 統合の計画

第 17 章「サード・パーティ・ディレクトリ統合の概念と考慮事項」、特に 17-18 ページの「Microsoft Active Directory 統合の概念」を読んで、統合を計画します。

手順 2: レルムの構成

18-7 ページの「レルムの構成」の指示に従い、レルムを構成します。

手順 3: Microsoft Active Directory から情報を取得する検索フィルタのカスタマイズ

デフォルトで、Microsoft Active Directory コネクタにより、同期用に構成されたコンテナ内のすべてのオブジェクトに対する変更が取得されます。特定のタイプの変更のみ（ユーザーやグループに対する変更のみなど）を取得する場合は、LDAP 検索フィルタを構成する必要があります。このフィルタにより、Microsoft Active Directory コネクタの Microsoft Active Directory に対する問合せの際に、不要な変更が排除されます。フィルタは、同期プロファイルの `searchfilter` 属性に格納されます。

サンプル・プロファイルの `activeChgImp` と `activeImport` では、グループとユーザーのみが Microsoft Active Directory から取得されます。コンピュータは取得されません。`searchfilter` 属性の値は、`searchfilter=(|(objectclass=group)(&(objectclass=user)(!(objectclass=computer))))` のように設定されます。

`searchfilter` 属性を更新するには、Oracle Directory Integration Server 管理ツールまたは Directory Integration アシスタント（`dipassistant`）を使用します。

Directory Integration アシスタントを使用して検索フィルタをカスタマイズするには、次のようにします。

1. 「接続されたディレクトリ一致フィルタ」（`orclODIPConDirMatchingFilter`）属性をカスタマイズするために、次のコマンドを入力します。

   ```
   $ORACLE_HOME/bin/dipassistant modifyprofile -D bindDn -w password -profile
   profName odip.profile.condirfilter=searchfilter=(|(objectclass=group)
   (objectclass=organizationalunit)(&(objectclass=user)(!(objectclass=computer))))
   ```

2. 「OID 一致フィルタ」（`orclODIPOIDMatchingFilter`）属性をカスタマイズするために、次のコマンドを入力します。

   ```
   $ORACLE_HOME/bin/dipassistant modifyprofile -D bindDn -w password
   -profile profName odip.profile.oidfilter=orclObjectGUID
   ```

Oracle Directory Integration Server 管理ツールを使用して検索フィルタをカスタマイズするには、次のようにします。

1. 次のコマンドを入力して、Oracle Directory Integration Server 管理ツールを起動します。

   ```
   $ORACLE_HOME/bin/dipassistant -gui
   ```

2. ナビゲータ・ペインで、「***directory_integration_server***」を展開した後、「**統合プロファイルの構成**」を展開します。

3. 構成設定を選択し、右側のペインで、カスタマイズするプロファイルを選択します。「統合プロファイル」ウィンドウが表示されます。

4. 「統合プロファイル」ウィンドウでは、「**マッピング**」タブを選択します。このタブ・ページのフィールドの説明は、A-8 ページの「マッピング」を参照してください。
5. 「マッピング」タブ・ページで、「接続されたディレクトリ一致フィルタ」（orclODIPConDirMatchingFilter）フィールドおよび「OID 一致フィルタ」（orclODIPOIDMatchingFilter）フィールドに searchfilter 属性の適切な値を入力します。searchfilter 属性を指定する方法は、6-14 ページの「LDAP 検索による変更のフィルタ処理」を参照してください。
6. 「**OK**」を選択します。

注意： searchfilter 属性に指定する属性はすべて、Microsoft Active Directory の索引付き属性のように構成する必要があります。

関連資料： LDAP 検索フィルタを構成する方法は、『Oracle Internet Directory 管理者ガイド』の LDAP フィルタ定義に関する付録を参照してください。

手順 4: ACL のカスタマイズ

18-8 ページの「Access 制御リストのカスタマイズ」で説明されているように、ACL をカスタマイズします。

手順 5: 属性マッピングのカスタマイズ

Microsoft Active Directory と統合する場合は、次の属性レベル・マッピングがすべてのオブジェクトに対して必須です。

```
ObjectGUID:  :  : :orclObjectGUID:
ObjectSID:  :  : :orclObjectSID:
```

例 19-1 Microsoft Active Directory のユーザー・オブジェクト用の属性レベル・マッピング

```
SAMAccountName:1: :user:orclADSAMAccountName: :orclADUser
userPrincipalName: : :user:orclADUserPrincipalName::orclADUser:userPrincipalName
```

例 19-2 Microsoft Active Directory のグループ・オブジェクト用の属性レベル・マッピング

```
SAMAccountName:1: :group:orclADSAMAccountName: :orclADGroup
```

この例では、Microsoft Active Directory の SAMAccountName および userPrincipalName は、それぞれ Oracle Internet Directory の orclADSAMAccountName および orclADUserPrincipalName にマップされます。

18-9 ページの「マッピング・ルールのカスタマイズ」の指示に従い、属性マッピングをカスタマイズします。

手順 6: 複数の Microsoft Active Directory ドメインとの同期

複数の Microsoft Active Directory ドメインと同期化する場合は、通常、ドメインごとに別々のインポートおよびエクスポート同期プロファイルが必要です。ただし、各ドメインのプロファイルは非常に似たものにします。唯一の例外は、グローバル カタログをインポート同期プロファイルとともに使用する場合です。この場合、Microsoft Active Directory フォレスト用の 1 つのインポート同期プロファイルを作成するのみです。詳細は、17-24 ページの「Microsoft Active Directory から Oracle Internet Directory へのインポートに必要な構成」を参照してください。

> **注意 :** 属性および識別名マッピングは、必ず複数のドメインとの同期化を行う前に実行してください。

複数ドメインに個別のインポートおよびエクスポート同期プロファイルを作成する最善の方法は、次のとおりです。

1. 単一ドメイン用のインポートおよびエクスポート同期プロファイルを、この項で前述した手順を使用して、カスタマイズします。
2. 最初のドメイン用のインポートおよびエクスポートの同期プロファイルのカスタマイズを終了したら、Directory Integration アシスタントの `createprofilelike` コマンドを使用して、プロファイルを次のように複製します。

   ```
   $ORACLE_HOME/bin/dipassistant createprofilelike [-h hostName] [-p port]
   [-D bindDn] [-w password] -profile origProfName -newprofile newProfName
   ```

3. Directory Integration アシスタントの `modifyprofile` コマンドを使用して、その他の Microsoft Active Directory ドメインごとに、プロファイルを次のようにカスタマイズします。

   ```
   $ORACLE_HOME/bin/dipassistant modifyprofile [-h hostName] [-p port]
   [-D bindDn] [-w password] {-f fileName | -profile profName [-updlcn] }
   [propName1=value] [propName2=value]...
   ```

4. 必要な場合は、6-3 ページの「接続詳細の構成」の指示に従い、ドメインごとに接続詳細を更新します。
5. 次のコマンドを実行して、各ドメインのインポートおよびエクスポート同期プロファイルの最終変更番号を更新します。

   ```
   $ORACLE_HOME/bin/dipassistant modifyprofile -profile profile_name -updcln
   ```

6. 同期が必要な Microsoft Active Directory ドメインごとに、手順 2 ～ 5 を繰り返します。

手順 7: Microsoft Active Directory からの削除の同期化

Microsoft Active Directory での削除を Oracle Internet Directory と同期化するには、Oracle Directory Integration Server で Microsoft Active Directory との同期を実行するために使用される Microsoft Active Directory ユーザー・アカウントに必要な権限を付与する必要があります。Microsoft Active Directory での削除は、Microsoft Active Directory で削除を問い合せることで、Oracle Internet Directory と同期化できます。この方法は、DirSync 方式または USN-Changed 方式のいずれを使用しているかによって決まります。

DirSync 方式の場合、Oracle Directory Integration Platform で Microsoft Active Directory へのアクセスに使用される Microsoft Active Directory ユーザー・アカウントは、Domain Administrators グループに属するドメイン管理者権限を持つか、「ディレクトリの変更の複製」権限を明示的に付与される必要があります。

> **関連資料 :**「ディレクトリの変更の複製」権限を付与する方法については、`http://support.microsoft.com` で Article ID 303972 を参照してください。

USN-Changed 方式の場合、Oracle Directory Integration Platform で Microsoft Active Directory へのアクセスに使用される Microsoft Active Directory ユーザー・アカウントには、指定したド

メインの cn=Deleted Objects コンテナに対する「内容の一覧表示」権限と「プロパティの読み取り」権限が必要です。これらの権限を設定するには、Microsoft Active Directory Application Mode（ADAM）の最新のバージョンで使用可能な dsacls.exe コマンドを使用する必要があります。ADAM の最新バージョンは、http://www.microsoft.com/downloads/ でダウンロードできます。

Microsoft Active Directory での削除を Oracle Internet Directory と同期化するために DirSync 方式または USN-Changed 方式のどちらを使用する場合であっても、ActiveImport プロファイル（DirSync 方式用）または ActiveChgImp プロファイル（USN-Changed プロファイル用）の一致フィルタを作成する場合は、必ず次の Microsoft Active Directory のキー属性のみを含めます。

- ObjectGUID
- ObjectSID
- ObjectDistName
- USNChanged

これらのキー属性以外の属性を一致フィルタに指定すると、Microsoft Active Directory での削除は Oracle Internet Directory に伝播されません。

関連資料：

- Microsoft Active Directory からアイテムを削除する方法については、http://support.microsoft.com で Article ID 230113 を参照してください。
- Oracle Internet Directory でサポートされる標準の LDAP 属性のリストについては、『Oracle Identity Management ユーザー・リファレンス』の属性リファレンスに関する章を参照してください。

手順 8: SSL モードでの同期

18-11 ページの「SSL モードでの同期用サード・パーティ・ディレクトリ・コネクタの構成」の指示に従い、SSL モードでの同期用に Microsoft Active Directory コネクタを構成します。

手順 9: パスワードの同期化

Oracle Internet Directory から Microsoft Active Directory にパスワードの変更を同期化するには、次のようにします。

1. 18-11 ページの「SSL モードでの同期用サード・パーティ・ディレクトリ・コネクタの構成」で説明されているように、Oracle Internet Directory、Oracle Directory Integration Platform および Microsoft Active Directory を SSL サーバー認証モードで稼働するように構成します。
2. 18-12 ページの「Oracle Internet Directory からサード・パーティ・ディレクトリへのパスワードの同期の有効化」の指示に従い、Oracle Internet Directory から Microsoft Active Directory へのパスワードの同期を有効にします。
3. 第 20 章「Oracle Password Filter for Microsoft Active Directory の配置」で説明されているように、Oracle Password Filter for Microsoft Active Directory をインストールおよび構成して、パスワードを同期化するように Microsoft Active Directory コネクタを構成します。

手順 10: Microsoft Active Directory 外部認証プラグインの構成

18-13 ページの「外部認証プラグインの構成」の指示に従い、Microsoft Active Directory 外部認証プラグインを構成します。

手順 11: 構成後タスクおよび管理タスクの実行

構成後タスクおよび継続的な管理タスクの詳細は、第 23 章「サード・パーティ・ディレクトリとの統合の管理」を参照してください。

インポート操作変更追跡での DirSync 方式の使用

デフォルトでは、Express 構成で作成されたインポート同期プロファイルでは、変更追跡に USN-Changed 方式を使用します。DirSync 方式の変更追跡を使用する場合は、同期化を開始する前に、必ずこの項の手順を実行してください。

注意： 次の手順を実行する前に、現行のインポート同期プロファイルのバックアップを取ります。プロファイルのバックアップ・コピーは、Directory Integration アシスタントの `createprofilelike` コマンドを使用すると作成できます。詳細は、『Oracle Identity Management ユーザー・リファレンス』の Oracle Directory Integration Platform ツールの章の `dipassistant` に関する項を参照してください。

インポート同期プロファイルで DirSync 変更追跡方式が使用されるように変更する手順は、次のとおりです。

1. $*ORACLE_HOME*/ldap/odi/conf ディレクトリにある activeimp.cfg.master ファイルを使用すれば、インポート同期プロファイルを USN-Changed 方式から DirSync 方式に変更できます。プロファイルを更新するには、次のコマンドを使用します。

   ```
   $ORACLE_HOME/bin/dipassistant modifyprofile -profile profile_name
   odip.profile.configfile=$ORACLE_HOME/ldap/odi/conf/activeimp.cfg.master
   ```

2. 次のコマンドを実行して、最終変更番号を更新します。

   ```
   $ORACLE_HOME/bin/dipassistant modifyprofile -profile profile_name -updcln
   ```

Windows ネイティブ認証の構成

この項では、Windows ネイティブ認証を構成するためのシステム要件とタスクについて説明します。内容は次のとおりです。

- Windows ネイティブ認証のシステム要件
- 単一の Microsoft Active Directory ドメインでの Windows ネイティブ認証の構成
- 複数の Microsoft Active Directory ドメインまたはフォレストでの Windows ネイティブ認証の構成
- フォールバック認証の実装
- 可能なログインの例

関連項目： 19-7 ページの「Windows ネイティブ認証の構成」

Windows ネイティブ認証のシステム要件

Windows ネイティブ認証は、イントラネットの Web アプリケーションを対象にしています。イントラネットでの配置に必要な要素は、次のとおりです。

- Microsoft Active Directory を搭載した Windows 2000 Server
- OracleAS Single Sign-On Server 用に設定された Kerberos サービス・アカウント
- インストール済の Oracle Application Server 10*g*（10.1.4.0.1）Infrastructure

> **注意：** この項のサンプル構成は UNIX/Linux 用ですが、Oracle Application Server は Microsoft Windows にもインストールできます。

- Kerberos レルム用に構成した OracleAS Single Sign-On 中間層
- Microsoft Active Directory の Oracle Internet Directory との同期
- Windows 外部認証プラグイン用に構成した Oracle Internet Directory

単一の Microsoft Active Directory ドメインでの Windows ネイティブ認証の構成

Windows ネイティブ認証を設定するには、次のタスクを順序どおりに実行して、Oracle Internet Directory、OracleAS Single Sign-On Server およびユーザーのブラウザを構成します。

タスク 1: OracleAS Single Sign-On Server の構成

Single Sign-On Server を構成するには、次の項目で説明されているタスクを完了します。

- OracleAS Single Sign-On Server の Kerberos サービス・アカウントの設定
- 各 Oracle Application Server Single Sign-On ホストでの OracleAS Single Sign-On Configuration Assistant の実行

OracleAS Single Sign-On Server の Kerberos サービス・アカウントの設定　Microsoft Active Directory で OracleAS Single Sign-On Server のサービス・アカウントを作成し、次にそのサーバー用の keytab ファイルを作成して、サービス・プリンシパル（サーバー）をアカウント名にマップします。keytab ファイルには、サーバーの秘密鍵が格納されます。このファイルにより、サーバーでは KDC に対する認証が可能になります。サービス・プリンシパルはエンティティであり、この場合は、KDC によりセッション・チケットが付与されるシングル・サインオン・サーバーです。

1. システム・クロックを同期化します。OracleAS Single Sign-On 中間層と Windows 2000 Server が一致する必要があります。この作業を省略すると、システム時間に違いが生じるために、認証が失敗します。必ず時刻、日付、タイム・ゾーンを同期化してください。
2. Microsoft Active Directory ホストで Kerberos サーバーのポート番号を確認します。Kerberos サーバーがリスニングするポートは、デフォルトでは /etc/services から選択されます。Windows システムでは、サービス・ファイルは、*system_drive*:¥WINNT¥system32¥drivers¥etc にあります。サービス名は Kerberos です。通常、ポートは Windows 2000 Server で `88/udp` および `88/tcp` に設定されます。services ファイルに正しく追加すると、これらのポート番号のエントリは次のようになります。

```
kerberos5       88/udp          kdc             # Kerberos key server
kerberos5       88/tcp          kdc             # Kerberos key server
```

3. services ファイルと同じディレクトリにある hosts ファイルで、シングル・サインオン中間層のエントリを確認します。Oracle Application Server Single Sign-On Server の物理ホスト名を示す完全修飾ホスト名が、IP アドレスと短縮名の間に配置されている必要があります。正しいエントリの例を次に示します。

```
130.111.111.111 sso.MyCompany.com sso loghost
```

4. 次のタスクを実行して、Oracle Application Server Single Sign-On の論理ホストで使用されるユーザー・アカウントと keytab ファイルを Microsoft Active Directory に作成します。

a. Windows 2000 Server で Microsoft Active Directory 管理ツールにログインし、「**ユーザー**」、「**新規**」、「**ユーザー**」の順に選択します。

OracleAS Single Sign-On ホストの名前を、ドメイン名を省略して入力します。たとえば、ホスト名が `sso.MyCompany.com` の場合は、`sso` と入力します。これは、Microsoft Active Directory のアカウント名です。

アカウントに割り当てたパスワードを書き留めておいてください。このパスワードは後で必要になります。「**ユーザーは次回ログオン時にパスワードの変更が必要**」を選択しないでください。

b. OracleAS Single Sign-On Server の kyetab ファイルを作成し、アカウント名をサービス・プリンシパル名にマップします。これら 2 つのタスクを行うには、次のコマンドを Windows 2000 Server で実行します。

```
C:> Ktpass -princ HTTP/sso.MyCompany.com@MyCompany.com -pass password -mapuser
sso -out sso.keytab
```

`-princ` 引数はサービス・プリンシパルです。
`HTTP/single_sign-on_host_name@KERBEROS_REALM_NAME` の書式を使用して、この引数の値を指定します。`HTTP` と Kerberos レルムは大文字で指定します。

`single_sign-on_host_name` は、OracleAS Single Sign-On ホスト自体でも、複数の OracleAS Single Sign-On 中間層が配置されているロード・バランサの名前でもかまいません。`MyCompany.com` は、Microsoft Active Directory 内の架空の Kerberos レルムです。ユーザー・コンテナは、このレルム内にあります。`-pass` 引数はアカウント・パスワード、`-mapuser` 引数は OracleAS Single Sign-On 中間層のアカウント名です。`-out` 引数はサービス・キーを格納する出力ファイルです。

例の値をそれぞれのインストール環境に適した値に置き換えてください。置き換える値は、例の中では太字で示されています。

注意：

- コンピュータで Ktpass が見つからない場合は、Microsoft 社から Windows リソース・キットをダウンロードしてこのユーティリティを取得します。
- Microsoft Kerberos チケットのデフォルトの暗号化タイプは RC4-HMAC です。Microsoft では、MIT 準拠の実装で使用される DES-CBC と DES-CBC-MD5 の 2 つの DES 変数もサポートします。Ktpass により、KDC アカウントの鍵のタイプは、RC4_HMAC から DES に変換されます。

---

5. 各 Oracle Application Server Single Sign-On ホストを対象に、keytab ファイル（sso.keytab）を OracleAS Single Sign-On 中間層にコピーまたは FTP 転送し、$*ORACLE_HOME*/j2ee/OC4J_SECURITY/config に配置します。FTP を使用する場合、ファイルをバイナリ・モードで送信してください。

Web サーバーに OracleAS Single Sign-On 中間層の一意識別子（UID）を指定し、keytab ファイルに対する読取り権限を必ず付与します。

各 Oracle Application Server Single Sign-On ホストでの OracleAS Single Sign-On Configuration Assistant の実行　この時点で ossoca.jar ツールを実行すると、次のようになります。

- Sun JAAS ログイン・モジュールを使用するように、Oracle Application Server Single Sign-On Server が構成されます。
- サーバーを保護されたアプリケーションとして構成します。

ossoca.jar ツールを OracleAS Single Sign-On 中間層で実行するには、次のようにします。

1. 次の構成ファイルのバックアップを作成します。
   - $*ORACLE_HOME*/sso/conf/policy.properties
   - $*ORACLE_HOME*/j2ee/OC4J_SECURITY/config/jazn.xml
   - $*ORACLE_HOME*/opmn/conf/opmn.xml
   - $*ORACLE_HOME*/j2ee/OC4J_SECURITY/config/jazn-data.xml
   - $*ORACLE_HOME*/j2ee/OC4J_SECURITY/applications/sso/web/WEB-INF/web.xml
   - $*ORACLE_HOME*/j2ee/OC4J_SECURITY/applications-deployments/sso/orion-application.xml
2. ossoca.jar ツールを次のように実行します。
   - UNIX/Linux:

     ```
     $ORACLE_HOME/sso/bin/ssoca
     wna -mode sso
     -oh $ORACLE_HOME
     -ad_realm AD_REALM
     -kdc_host_port kerberos_server_host:port
     -verbose
     ```

   - Windows:

     ```
     %ORACLE_HOME%¥jdk¥bin¥java -jar %ORACLE_HOME%¥sso¥lib¥ossoca.jar
     wna -mode sso
     -oh %ORACLE_HOME%
     -ad_realm AD_REALM
     -kdc_host_port kerberos_server_host:port
     -verbose
     ```

   AD_REALM は、Microsoft Active Directory の Kerberos レルムです。これはユーザー・コンテナです。構文からわかるように、この値は大文字で入力します。KDC のデフォルト・ポート番号は通常 88 です。これを確認するには、19-8 ページの「OracleAS Single Sign-On Server の Kerberos サービス・アカウントの設定」の手順 2 を参照してください。
3. 手順 2 で、OracleAS Single Sign-On Server は停止します。次のコマンドで再起動します。

   ```
   $ORACLE_HOME/opmn/bin/opmnctl startall
   ```

タスク 2: Windows ネイティブ認証用の Internet Explorer の構成

Windows ネイティブ認証を使用できるように Internet Explorer を構成します。構成方法は、使用するバージョンによって異なります。

- Internet Explorer 5.0 以上
- Internet Explorer 6.0 のみ

Internet Explorer 5.0 以上

Internet Explorer 5.0 以上を構成するには、次の手順を実行します。

1. メニュー・バーから「**ツール**」を選択し、「**ツール**」メニューから「**インターネット オプション**」を選択します。
2. 「インターネット オプション」ダイアログ・ボックスで、「**セキュリティ**」タブを選択します。
3. 「セキュリティ」タブ・ページで、「**イントラネット**」を選択し、「**サイト**」を選択します。
4. 「イントラネット」ダイアログ・ボックスで「**プロキシ サーバーを使用しないサイトをすべて含める**」を選択し、「**詳細設定**」をクリックします。
5. もう 1 つの「イントラネット」ダイアログ・ボックスで、OracleAS Single Sign-On 中間層の URL を入力します。たとえば、次のようになります。

   ```
   http://sso.mydomain.com
   ```

6. 「**OK**」をクリックし、「イントラネット」ダイアログ・ボックスを終了します。
7. 「インターネット オプション」ダイアログ・ボックスで「**セキュリティ**」タブを選択し、「**イントラネット**」、「**レベルのカスタマイズ**」を選択します。
8. 「セキュリティの設定」ダイアログ・ボックスで「ユーザー認証」セクションまでスクロールし、「**イントラネット ゾーンでのみ自動的にログオンする**」を選択します。
9. 「**OK**」をクリックし、「セキュリティの設定」ダイアログ・ボックスを終了します。
10. メニュー・バーから「**ツール**」を選択し、「**ツール**」メニューから「**インターネット オプション**」を選択します。
11. 「インターネット オプション」ダイアログ・ボックスで、「**接続**」タブを選択します。
12. 「**接続**」タブで「**LAN の設定**」を選択します。
13. プロキシ・サーバーの正しいアドレスとポート番号が入力されていることを確認してから、「**詳細設定**」を選択します。
14. 「プロキシの設定」ダイアログ・ボックスで、「**例外**」セクションに、OracleAS Single Sign-On Server のドメイン名（例では `MyCompany.com`）を入力します。
15. 「**OK**」をクリックし、「プロキシの設定」ダイアログ・ボックスを終了します。

Internet Explorer 6.0 のみ

Internet Explorer 6.0 を使用している場合は、「Internet Explorer 5.0 以上」の手順 1 ～ 12 の実行後に、次の手順を実行します。

1. メニュー・バーから「**ツール**」を選択し、「**ツール**」メニューから「**インターネット オプション**」を選択します。
2. 「インターネット オプション」ダイアログ・ボックスで、「**詳細設定**」タブを選択します。
3. 「**詳細設定**」タブ・ページで「セキュリティ」セクションまでスクロールします。
4. 「**統合 Windows 認証を使用する（再起動が必要）**」を選択します。

タスク 3: ローカル・アカウントの再構成

Windows ネイティブ認証の構成後、Oracle Internet Directory 管理者（orcladmin）と、アカウントが Oracle Internet Directory にあるその他の Windows ローカル・ユーザーのアカウントを再構成する必要があります。このタスクを省略すると、これらのユーザーがログインできなくなります。

Oracle Internet Directory の Oracle Directory Manager を使用して、次の手順を実行します。

1. Oracle Internet Directory のローカル・ユーザー・エントリに orclADUser クラスを追加します。
2. ユーザー・エントリの orclSAMAccountName 属性にローカル・ユーザーのログイン ID を追加します。たとえば、orcladmin アカウントのログイン ID は orcladmin です。
3. 外部認証プラグインの exceptionEntry プロパティにローカル・ユーザーを追加します。

複数の Microsoft Active Directory ドメインまたはフォレストでの Windows ネイティブ認証の構成

この項では、次のタイプの配置において、複数の Microsoft Active Directory ドメインまたはフォレストで Windows ネイティブ認証を構成する方法について説明します。

- 親子関係のある Microsoft Active Directory ドメイン
- ツリー・ルート信頼タイプが確立された同一フォレスト内の Microsoft Active Directory ドメイン
- フォレスト信頼タイプが確立された異なるフォレスト内のドメイン

> **注意：** フォレスト信頼タイプは、Windows Server 2003 以上の Windows オペレーティング・システムでのみサポートされます。

複数の Microsoft Active Directory ドメインまたはフォレストで Windows ネイティブ認証を構成するには、次のタスクを順序どおりに実行します。

タスク 1: Microsoft Active Directory ドメイン間で信頼が確立していることの検証

複数の Microsoft Active Directory ドメイン間の信頼を検証する方法の詳細は、使用している Microsoft Active Directory のドキュメントを参照してください。

タスク 2: ロード・バランサまたはリバース・プロキシを介した Oracle Application Server Single Sign-On での Windows ネイティブ認証の有効化

『Oracle Application Server Single Sign-On 管理者ガイド』の拡張配置オプションに関する章の指示に従い、Oracle Application Server Single Sign-On Server をロード・バランサの背後で稼働するように、またはリバース・プロキシを介して稼働するように構成します。

タスク 3: OracleAS Single Sign-On Server の構成

19-8 ページの「タスク 1: OracleAS Single Sign-On Server の構成」の指示に従い、各 Oracle Application Server Single Sign-On Server を構成します。各 Oracle Application Server Single Sign-On Server の物理インスタンスを構成する際は、必ず同一の Microsoft Active Directory レルムおよび対応する Key Distribution Center（KDC）を使用してください。また、Oracle Application Server Single Sign-On の論理ホスト名として、ロード・バランサまたはリバース・プロキシの名前を使用してください。

注意： 複数の Microsoft Active Directory フォレストでは、Oracle Application Server Single Sign-On Server の論理ホスト名は、Microsoft Active Directory ドメインのいずれかに属している必要があります。たとえば、2 つの Microsoft Active Directory フォレストがあり、各フォレストには 1 つのドメインが含まれているとします。1 番目のフォレストのドメイン名は `engineering.mycompany.com` で、2 番目のフォレストのドメイン名は `finance.mycompany.com` です。Oracle Application Server Single Sign-On Server の論理ホスト名は、`engineering.mycompany.com` または `finance.mycompany.com domain` のいずれかに存在する必要があります。

タスク 4: Windows ネイティブ認証用の Internet Explorer の構成

19-11 ページの「タスク 2: Windows ネイティブ認証用の Internet Explorer の構成」の指示に従い、Oracle Application Server Single Sign-On Server を構成します。

フォールバック認証の実装

SPNEGO-Kerberos 認証をサポートするブラウザは、Internet Explorer 5.0 以上のみです。OracleAS Single Sign-On では、Netscape Communicator などのサポート外のブラウザでフォールバック認証を利用できます。ブラウザのタイプと構成内容に応じて、OracleAS Single Sign-On ログイン・フォームまたは HTTP Basic 認証のダイアログ・ボックスが表示されます。いずれの場合でも、ユーザーはユーザー名とパスワードを入力する必要があります。ユーザー名は Kerberos レルム名とユーザー ID を連結したものです。デフォルトでは、ユーザー名を次の例のように入力します。

`domain_name¥user_id`

次の例では、19-8 ページの「OracleAS Single Sign-On Server の Kerberos サービス・アカウントの設定」で示した例に基づいて、ユーザー名の入力方法を示しています。

`MyCompany.COM¥jdoe`

ユーザー名とパスワードは、大文字と小文字が区別されます。また、Microsoft Active Directory のパスワード・ポリシーは適用されません。Oracle Directory Integration Platform を使用すると、別の同期プロファイルを構成できます。その場合、前述のログイン書式は適用されません。

フォールバック認証は、Oracle Internet Directory の外部認証プラグインによって Microsoft Active Directory に対して実行されます。

注意：

- HTTP Basic 認証は、ログアウトをサポートしていません。ブラウザのキャッシュから資格証明を消去する場合、ユーザーは開いているブラウザ・ウィンドウをすべて閉じる必要があります。あるいは、Windows コンピュータからログアウトします。
- Basic 認証が起動している場合、ユーザーは使用する言語を Internet Explorer で手動設定する必要があります。「ツール」メニューから「**インターネット オプション**」、「**言語**」の順に選択し、必要な言語を入力します。

可能なログインの例

使用している Internet Explorer のバージョンに応じて、ログインの方法が異なる場合があります。19-14 ページの表 19-1 に、自動サインオンとフォールバック認証が起動する状況を示します。

表 19-1 Internet Explorer での Single Sign-On ログインのオプション

ブラウザのバージョン	デスクトップ・プラットフォーム	デスクトップの認証タイプ	Internet Explorer ブラウザの統合認証	OracleAS Single Sign-On ログイン・タイプ
5.0.1 以上	Windows 2000/XP	Kerberos V5	オン	自動サインオン
5.0.1 以上、ただし 6.0 より前	Windows 2000/XP	Kerberos V5	オフ	シングル・サインオン
6.0 以上	Windows 2000/XP	Kerberos V5 または NTLM	オフ	HTTP Basic 認証
5.0.1 以上、ただし 6.0 より前	Windows NT/2000/XP	NTLM	オンまたはオフ	シングル・サインオン
6.0 以上	NT/2000/XP	NTLM	オン	シングル・サインオン
5.0.1 以上	Windows 95、Windows ME、Windows NT 4.0	該当なし	該当なし	シングル・サインオン
5.0.1 より前	該当なし	該当なし	該当なし	シングル・サインオン
他のすべてのブラウザ	他のすべてのプラットフォーム	該当なし	該当なし	シングル・サインオン

Oracle Internet Directory 外部セキュリティ・プリンシパル参照と Microsoft Active Directory との同期の構成

この項では、Oracle Internet Directory 外部セキュリティ・プリンシパル参照を Microsoft Active Directory と同期化する方法について説明します。

Microsoft Active Directory では、グループ・メンバーの情報が信頼関係のドメインに外部セキュリティ・プリンシパル参照として格納されますが、Oracle Internet Directory では、これらのメンバーの識別名が Oracle Internet Directory での表示どおりに格納されます。このため、エントリとグループのメンバーとしてのその値が一致しなくなります。Oracle Internet Directory では、ユーザーとグループとの関係を直接確立することはできません。

ユーザーとグループとの関係を確立するには、外部セキュリティ・プリンシパルを参照するメンバー識別名を、グループの同期中にエントリの識別名に置き換える必要があります。これは外部キー参照の解決と呼ばれます。

注意： 外部セキュリティ・プリンシパル参照の同期は、Windows 2003 でのみサポートされています。

例 19-3 外部キー参照の解決方法

この項の例は、外部キー参照がどのように解決されるかを示しています。

A、B、C の 3 つのドメインがあるとします。

ドメイン A には、ドメイン B に対する一方向の非推移的な信頼があります。ドメイン A では、ドメイン B のユーザーおよびグループに対して、外部セキュリティ・プリンシパル参照を設定できます。

ドメイン A には、ドメイン C に対する一方向の非推移的な信頼があります。ドメイン A では、ドメイン C のユーザーおよびグループに対して、外部セキュリティ・プリンシパル参照を設定できます。

ドメイン B には、ドメイン C に対する一方向の非推移的な信頼があります。ドメイン B では、ドメイン C のユーザーおよびグループに対して、外部セキュリティ・プリンシパル参照を設定できます。

この例では、ドメイン A からドメイン B、ドメイン A からドメイン C、ドメイン B からドメイン C に対して一方向の非推移的な信頼があります。

外部キー参照を解決するタスク

この項では、外部キー参照を解決する手順を説明します。

タスク 1: エージェント構成情報の更新　外部セキュリティ・プリンシパル参照が設定されている可能性のあるプロファイルごとに、次の手順を実行します。ここで言及するサンプル構成ファイルは、$*ORACLE_HOME*/ldap/odi/samples ディレクトリにあります。

1. activeimp.cfg.fsp ファイルをコピーします。次に activeimp.cfg.fsp ファイルの例を示します。

```
[INTERFACEDETAILS]
   Package: gsi
   Reader: ActiveReader
[TRUSTEDPROFILES]
   prof1 : <Name of the profile1>
   prof2 : <Name of the profile2>
[FSPMAXSIZE]
   val=10000
```

   この例では、DirSync 変更追跡方式を使用しているものと仮定しています。変更対的に USN-Changed 方式を使用している場合、Reader パラメータに `ActiveChgReader` の値を指定します。

2. activeimp.cfg.fsp ファイルの `[TRUSTEDPROFILES]` タグの下で、このドメインに外部セキュリティ・プリンシパル参照を持つその他のドメインのプロファイル名を指定します。

   19-14 ページの例 19-3 を参照すると、ドメイン A のエージェント構成情報は、次のようになります。

```
[INTERFACEDETAILS]
   Package: gsi
   Reader: ActiveReader
[TRUSTEDPROFILES]
   prof1: profile_name_for_domain_B
   prof2: profile_name_for_domain_C
```

   ドメイン B のエージェント構成情報は、次のようになります。

```
[INTERFACEDETAILS]
   Package: gsi
   Reader: ActiveReader
[TRUSTEDPROFILES]
   prof1: profile_name_for_domain_C
```

   ドメイン C には外部キー参照がないため、ドメイン C のエージェント構成情報ファイルには変更がありません。

3. `[FSPMAXSIZE]` タグの下で、外部セキュリティ・プリンシパルのキャッシュ・サイズを指定します。これは、設定できる外部セキュリティ・プリンシパルの平均値でかまいません。activeimp.cfg.fsp ファイルでは、サンプルの値 `1000` が指定されています。

4. Directory Integration アシスタントを使用して、次のように新しいエージェント構成情報ファイルをロードします。

```
$ORACLE_HOME/bin/dipassistant modifyprofile
-profile profile_name_for_domain_A_or_B
-host host_name
-port port_name
-dn bind_DN
-passwd password_of_bind_DN
odip.profile.configfile=activeimp.cfg.fsp
```

5. 対象となるすべてのプロファイルについて、このタスクを繰り返します。

タスク 2: 外部セキュリティ・プリンシパル参照を解決するためのブートストラップ前の入力データ変更　これには、次の手順を実行します。

1. Microsoft Active Directory から LDIF ダンプを取得します。適切なフィルタを使用して、取得した LDIF ファイルには、必要なオブジェクト（ユーザーやグループなど）のみが含まれるようにします。

> **注意：** Microsoft Active Directory から Oracle Internet Directory にエントリをダンプするコマンドは、`ldifde` です。このコマンドは、Microsoft Windows 環境からのみ実行できます。

2. 次のコマンドを入力して、外部セキュリティ・プリンシパル参照を解決します。

```
$ORACLE_HOME/ldap/odi/admin/fsptodn
host=oid_host
port=oid_port
dn= OID_privileged_DN (that is, superuser or dipadmin user)
pwd=OID_password
profile=profile_name_for_domain_A_or_B
infile=input_filenameo_of_the_LDIF_dump_from_Active_Directory
outfile=output_filename
[sslauth=0|1]
```

デフォルトで、`host` は *`local_host`* に、`port` は `389` に、`sslauth` は `0` に設定されています。

> **注意：** コマンドの実行が成功したかどうかは、出力ファイルにメンバー属性の `cn=foreignsecurityprincipals` に対する参照が含まれていないことを確認することで検証できます。このコマンドでは、外部セキュリティ・プリンシパル参照の解決以外に、属性レベルのマッピングは実行されません。

3. Directory Integration アシスタントの `-bootstrap` オプションを使用して、Microsoft Active Directory から Oracle Internet Directory にデータをブートストラップします。

関連項目： 23-3 ページの「ディレクトリ間でのデータのブートストラップ」

タスク 3: 同期中に外部セキュリティ・プリンシパルを解決するためのマッピング・ルールの更新　ブートストラップ後、グループに対する変更は、正しいグループ・メンバーシップの値で Oracle Internet Directory に反映する必要があります。`fsptodn` マッピング・ルールにより、同期化の際にこれが可能になります。外部セキュリティ・プリンシパルの解決が必要なすべてのプロファイルで、このマッピング・ルールを変更します。19-14 ページの例 19-3 を参照すると、ドメイン A と B について、マッピング・ルールを変更する必要があります。

識別名マッピングがない場合は、`member` 属性のマッピング・ルールを次のように変更します。

```
member: : :group:uniquemember: :groupofUniqueNames: fsptodn(member)
```

識別名マッピングがある場合は、マッピング・ルールを次のように変更します。

1. 信頼関係の各ドメインに対応する識別名マッピング・ルールを追加します。これは、正しいドメイン・マッピングを解決するために使用されます。19-14 ページの例 19-3 を参照すると、ドメイン A のマッピング・ファイルの domainrules は、次のような内容になります。

   ```
   DOMAINRULES
   <Src Domain A >:<Dst domain A1 in OID>
   <Src Domain B >:< Dst domain B1 in OID>
   <Src Domain C>:<Dst domain C1 in OID>
   ```

2. member 属性のマッピング・ルールを次のように変更します。

   ```
   member:::group:uniquemember::groupofUniqueNames:dnconvert(fsptodn(member))
   ```

3. Directory Integration アシスタント（dipassistant）を使用して、様々なプロファイルのマッピング・ファイルをアップロードします。

同一ドメイン内の異なる Microsoft Active Directory ドメイン・コントローラへの切替え

この項では、変更のエクスポート先である Microsoft Active Directory ドメイン・コントローラを変更する方法を説明します。USN-Changed 方式用と DirSync 方式用の 2 つの方法があります。

USN-Changed 方式を使用して Microsoft Active Directory ドメイン・コントローラを変更する方法

USN-Changed 方式を使用している場合は、次の手順を実行します。

1. 現在実行中のプロファイルを停止します。Microsoft Active Directory ホスト接続情報（ホスト、ポート、ユーザー、パスワード）を、新規ホストを指すように変更します。通常、更新が必要なアイテムは、ホスト名のみです。

2. 新しいドメイン・コントローラのルート DSE で、現行の最大の USNChanged 値（ルート DSE の highestCommittedUSN 属性の属性値）を検索することにより、highestCommittedUSN の現行値を取得します。

   ```
   ldapsearch -h host -p port -b "" -s base -D user
   DN -w password "objectclass=*" highestCommittedUSN
   ```

3. Oracle Directory Integration Platform を使用して、Microsoft Active Directory から完全同期化を実行します。

   a. 目的とする LDAP 検索の範囲と検索フィルタを使用して、Microsoft Active Directory から Oracle Internet Directory にエントリをダンプする ldifde コマンドを実行します。通常、検索フィルタは、実行中のプロファイルで指定されているものと同じです。たとえば、サンプルのプロパティ・ファイルでは、次の検索フィルタが設定されています。ldifde を実行できるのは、Microsoft Windows 環境からのみです。

      ```
      searchfilter=(&(|(objectclass=user)(objectclass=organizationalunit))(!(obje
      ctclass=group)))
      ```

      基本的に、実行中のプロファイルにより Microsoft Active Directory と同期化されるように構成された、Oracle Internet Directory オブジェクト（エントリ）をすべて取得する検索範囲と検索フィルタを使用して、ldifde を実行します。

   b. Oracle Directory Integration Platform を実行して、同じプロファイルを使用して手順 a で生成された LDIF ファイルをアップロードします。

4. 完全同期が完了した後、lastchangenumber 属性を、手順 2 で取得された highestCommittedUSN 値により更新します。

5. USNChanged 属性を使用して、Microsoft Active Directory から通常の同期（増分同期）を再開します。

DirSync 方式を使用して Microsoft Active Directory ドメイン・コントローラを変更する方法

DirSync 方式を使用している場合は、次の手順を実行します。

1. 実行中の現行プロファイルを停止します。
2. Directory Integration アシスタントの `createlike` オプションを使用して、すでに使用しているプロファイルとまったく同じプロファイルを新たに作成します。新たに作成したプロファイルで、Microsoft Active Directory ホスト接続情報（ホスト、ポート、ユーザー、パスワード）を、新規ホストを指すように変更します。通常、更新が必要なアイテムは、ホスト名のみです。
3. 変更したプロファイルで、通常の同期を再開します。ドメイン・コントローラはすべて、同じ Microsoft Active Directory ドメインに存在することが必要です。

Microsoft Exchange Server 用の Microsoft Active Directory コネクタの構成

Microsoft Active Directory コネクタは、Microsoft Exchange でのユーザーのプロビジョニングに使用できます。これは、Microsoft Active Directory Server 2000 以上を ID ストアとして使用する配置に適用できます。

Microsoft Active Directory コネクタを Microsoft Exchange Server 用に構成するには、18-5 ページの「Express 構成の実行」で説明されているように、Directory Integration アシスタント（`dipassistant`）ユーティリティで Express 構成を実行します。`dipassistant` コマンドを実行する際には、`-3rdpartyds` パラメータに割り当てられる値として `adforexchange` を必ず指定してください。Microsoft Exchange との統合をさらにカスタマイズするには、19-2 ページの「Microsoft Active Directory との拡張統合の構成」の指示に従います。

関連資料：『Oracle Application Server MS Office Developer's Guide』

20

Oracle Password Filter for Microsoft Active Directory の配置

この章では、Oracle Password Filter for Microsoft Active Directory のインストールおよび構成の方法について説明します。内容は次のとおりです。

- Oracle Password Filter for Microsoft Active Directory の概要
- SSL サーバー側認証での Oracle Internet Directory の構成およびテスト
- Microsoft Active Directory ドメイン・コントローラへの信頼できる証明書のインポート
- Oracle Internet Directory と Microsoft Active Directory 間の SSL 通信のテスト
- Oracle Password Filter for Microsoft Active Directory のインストールおよび再構成
- Oracle Password Filter for Microsoft Active Directory の削除

注意： Oracle Password Filter for Microsoft Active Directory の setup.exe インストール・ファイルは、Windows 版 Oracle Application Server の CD の utils/adpwdfilter ディレクトリにあります。

Oracle Password Filter for Microsoft Active Directory の概要

この項では、Oracle Password Filter for Microsoft Active Directory の目的と動作について説明します。内容は次のとおりです。

Oracle Password Filter for Microsoft Active Directory の概要

Oracle Directory Integration Platform を使用すると、Oracle Internet Directory と Microsoft Active Directory 間の同期が可能になります。Oracle Directory Integration Platform では、ユーザー・パスワードを除いたすべての Microsoft Active Directory の属性を取得できます。Oracle Application Server Single Sign-On では、外部認証プラグインを使用して Microsoft Active Directory のユーザーの資格証明を検証します。Oracle Application Server Single Sign-On を使用しない環境では、Oracle Password Filter for Microsoft Active Directory を使用して、Microsoft Active Directory から Oracle Internet Directory にパスワードを取り出します。ユーザーがデスクトップからパスワードを変更すると、更新されたパスワードは Oracle Internet Directory と自動的に同期化されます。つまり、Oracle Password Filter for Microsoft Active Directory は、パスワードの変更について Microsoft Active Directory を監視し、その変更を Oracle Internet Directory に格納します。これにより、Oracle Internet Directory ユーザーは Microsoft Active Directory の資格証明で認証され、Oracle Internet Directory に格納された情報を使用してリソースへのアクセスを認可されます。また、Microsoft Active Directory ユーザーの資格証明を Oracle Internet Directory に格納すると、Microsoft Active Directory サーバーが停止した場合には可用性の高いソリューションが提供されます。Oracle Password Filter は、各 Microsoft Active Directory サーバーにインストールされ、パスワードの変更を Oracle Internet Directory に自動的に転送します。

注意： エンタープライズ・ユーザー・セキュリティは、Oracle Internet Directory に格納されているユーザーの資格証明しか検証できません。このため、Microsoft Active Directory のユーザーの資格証明をエンタープライズ・ユーザー・セキュリティを使用して検証するには、Oracle Password Filter を使用して Microsoft Active Directory から Oracle Internet Directory にパスワードを取り出す必要があります。

Oracle Password Filter for Microsoft Active Directory では、Oracle Directory Integration Platform による Microsoft Active Directory から Oracle Internet Directory へのパスワードの同期は必要ありません。唯一の要件は、Microsoft Active Directory から Oracle Internet Directory に同期化されたユーザーに、両方のディレクトリでユーザーを識別するための `ObjectGUID` 属性値が含まれている必要があることです。Oracle Password Filter for Microsoft Active Directory は、Microsoft Active Directory と Oracle Internet Directory 間に複数のパスワード・ポリシー（すなわち異なるパスワード・ポリシー）を施行しません。かわりに、システム管理者が両方のディレクトリのパスワード・ポリシーが一致するようにする必要があります。

パスワード変更リクエストは、アカウントが作成されるとき、管理者がユーザーのパスワードをリセットするとき、ユーザーが自分のパスワードを変更するときに発生します。Oracle Password Filter for Microsoft Active Directory で Microsoft Active Directory のパスワードを取得するには、これらのイベントのいずれかが発生する必要があります。Oracle Password Filter for Microsoft Active Directory のインストール前に設定されたパスワードは、システム管理者がすべてのユーザーに対してパスワード変更のグローバル・リクエストを強制しないかぎり取得できません。

注意： Oracle Password Filter for Microsoft Active Directory は、Microsoft Active Directory と統合されている 32 ビット以上の Windows システムに対するパスワードの変更のみを取得します。

Oracle Password Filter for Microsoft Active Directory の動作

この項では、Oracle Password Filter for Microsoft Active Directory の動作について説明します。内容は次のとおりです。

- 取得されるクリアテキストのパスワードの変更
- Oracle Internet Directory の使用不可時に格納されるパスワードの変更
- Microsoft Active Directory ユーザーが Oracle Identity Management と同期化されるまで遅延されるパスワードの同期
- パスワードのブートストラッピング

取得されるクリアテキストのパスワードの変更

パスワード変更リクエストが作成されると、Windows オペレーティング・システムの Local Security Authority（LSA）は、システムに登録されている Oracle Password Filter for Microsoft Active Directory パッケージをコールします。LSA は、Oracle Password Filter for Microsoft Active Directory パッケージをコールすると、ユーザー名と変更されたパスワードを渡します。次に、Oracle Password Filter for Microsoft Active Directory は同期を実行します。

Oracle Internet Directory の使用不可時に格納されるパスワードの変更

Oracle Internet Directory が使用できないとき、パスワード変更イベントは安全にアーカイブされ、暗号化されたパスワードは Microsoft Active Directory に格納されます。Oracle Password Filter for Microsoft Active Directory は、指定された最大再試行回数に達するまでこれらのエントリの同期を試みます。

Microsoft Active Directory ユーザーが Oracle Identity Management と同期化されるまで遅延されるパスワードの同期

Oracle Password Filter for Microsoft Active Directory には、ユーザーが Microsoft Active Directory に新規作成されるとすぐに通知されます。しかし、Oracle Directory Integration Platform は次にスケジュールされた同期間隔までエントリを同期化しません。このため、次の同期まで、新規ユーザー・エントリのパスワードは暗号化された形式で Microsoft Active Directory に格納されます。その後、Oracle Password Filter for Microsoft Active Directory は、指定された最大再試行回数に達するまでこれらのエントリの同期を試みます。

パスワードのブートストラッピング

元のクリアテキスト形式のパスワードは、Oracle Password Filter for Microsoft Active Directory では取得できないため、Microsoft Active Directory から Oracle Internet Directory にパスワードを同期化するための最初のブートストラッピングを実行できません。しかし、ユーザーにパスワードの変更を指示するか、またはパスワードの有効期限ポリシーを変更して Microsoft Active Directory 内のすべてのユーザーに対してパスワードの変更を強制することができます。

Oracle Password Filter for Microsoft Active Directory の配置方法

Oracle Password Filter for Microsoft Active Directory のインストールおよび構成の一般的な手順は、次のとおりです。

1. 第 19 章「Microsoft Active Directory との統合」の指示に従い、Oracle Internet Directory と Microsoft Active Directory 間の同期を有効にします。
2. 20-4 ページの「SSL サーバー側認証での Oracle Internet Directory の構成およびテスト」の指示に従い、SSL サーバー認証モードで Oracle Internet Directory を構成およびテストします。
3. 20-5 ページの「Microsoft Active Directory ドメイン・コントローラへの信頼できる証明書のインポート」の指示に従い、Microsoft Active Directory ドメイン・コントローラに Oracle Internet Directory の信頼できるサーバー証明書をインポートします。
4. 20-6 ページの「Oracle Internet Directory と Microsoft Active Directory 間の SSL 通信のテスト」の指示に従い、Oracle Internet Directory と Microsoft Active Directory が SSL サーバー認証で通信できることを確認します。
5. 20-8 ページの「Oracle Password Filter for Microsoft Active Directory のインストール」の指示に従い、Oracle Password Filter for Microsoft Active Directory をインストールします。
6. 20-16 ページの「Oracle Password Filter for Microsoft Active Directory の再構成」の指示に従い、Oracle Password Filter for Microsoft Active Directory を構成します。

SSL サーバー側認証での Oracle Internet Directory の構成およびテスト

Oracle Password Filter は、TCP/IP 接続に対してデータの暗号化とメッセージの整合性を提供する Secure Sockets Layer（SSL）プロトコルを使用して、Microsoft Active Directory から Oracle Internet Directory にパスワードの変更を通信します。つまり、Oracle Internet Directory と Microsoft Active Directory 間でパスワードの変更を同期化するには、SSL サーバー認証モードを使用して、クライアントでサーバーの識別情報を確認できるようにする必要があります。また、デジタル証明と組み合せると、SSL はサーバー認証とクライアント認証の両方を提供します。SSL によるサーバー認証では、通信リンクのサーバー側にデジタル証明をインストールする必要があります。SSL トランザクションがクライアントによって開始されると、サーバーはデジタル証明をクライアントに送信します。クライアントは証明書を調べ、証明書が信頼できる認証局（CA）によって発行されていることを含め、サーバーが正しく自身を証明していることを確認します。Oracle Internet Directory と Microsoft Active Directory の統合の場合、Oracle Internet Directory がサーバーで、Microsoft Active Directory がクライアントです。Oracle Password Filter for Microsoft Active Directory では、Microsoft Active Directory ドメイン・コントローラと Oracle Internet Directory サーバー間の送信時、SSL を使用してパスワードを保護します。

注意： Oracle Password Filter for Microsoft Active Directory とともに使用する証明書は、PKCS#10 規格の証明書リクエストを受け入れ、X.509 バージョン 3、ISO 規格および RFC2459 に準拠した証明書を作成できる X.509 準拠の認証局であればどれでも生成できます。

Oracle Internet Directory を SSL サーバー側認証で構成およびテストするには、『Oracle Internet Directory 管理者ガイド』を参照してください。

Microsoft Active Directory ドメイン・コントローラへの信頼できる証明書のインポート

Microsoft Active Directory ドメイン・コントローラと Oracle Internet Directory 間のサーバー認証された SSL 通信は、ドメイン・コントローラが Oracle Internet Directory の SSL 証明書を有効と認識しないと障害が発生します。ドメイン・コントローラが Oracle Internet Directory の SSL 証明書を受け入れるようにするには、Microsoft 管理コンソールを使用して認証局の信頼できる証明書をドメイン・コントローラにインポートする必要があります。

Microsoft 管理コンソールを使用して認証局の信頼できる証明書をドメイン・コントローラにインポートするには、次のようにします。

1. Windows の「**スタート**」メニューから「**ファイル名を指定して実行**」を選択します。「ファイル名を指定して実行」ダイアログ・ボックスが表示されます。「ファイル名を指定して実行」ダイアログ・ボックスに **mmc** と入力し、「**OK**」をクリックします。「Microsoft 管理コンソール」ウィンドウが表示されます。
2. 「**ファイル**」メニューから「**スナップインの追加と削除**」を選択します。「スナップインの追加と削除」ダイアログ・ボックスが表示されます。
3. 「スナップインの追加と削除」ダイアログ・ボックスで、「**追加**」をクリックします。「スタンドアロン スナップインの追加」ダイアログ・ボックスが表示されます。
4. 「スタンドアロン スナップインの追加」ダイアログ・ボックスで「**証明書**」を選択した後、「**追加**」をクリックします。「証明書スナップイン」ダイアログ・ボックスが表示され、このスナップインで管理する証明書のオプションを選択するように要求されます。
5. 「証明書スナップイン」ダイアログ・ボックスで「**コンピュータ名**」を選択した後、「**次へ**」をクリックします。「コンピュータの選択」ダイアログ・ボックスが表示されます。
6. 「コンピュータの選択」ダイアログ・ボックスで「**ローカル コンピュータ**」を選択した後、「**完了**」をクリックします。
7. 「スタンドアロン スナップインの追加」ダイアログ・ボックスで「**閉じる**」をクリックした後、「スナップインの追加と削除」ダイアログ・ボックスで「**OK**」をクリックします。新しいコンソールのコンソール・ツリーに「証明書 (ローカル コンピュータ)」と表示されます。
8. コンソール・ツリーで「**証明書 (ローカル コンピュータ)**」を開き、「**信頼されたルート証明機関**」をクリックします。
9. 「**操作**」メニューの「**すべてのタスク**」をポイントした後、「**インポート**」を選択します。「証明書のインポート ウィザードの開始」ページが表示されます。「**次へ**」をクリックして「インポートする証明書ファイル」ページを表示します。
10. 「**インポートする証明書ファイル**」ページで、認証局の信頼できるルート証明書のパスとファイル名を入力するか、「**参照**」をクリックしてファイルを検索して、「**次へ**」をクリックします。「証明書ストア」ページが表示されます。
11. 「証明書ストア」ページで、「**証明書をすべて次のストアに配置する**」を選択します。「信頼されたルート証明機関」が証明書ストアとして選択されていない場合は、「**参照**」をクリックして選択します。「**次へ**」をクリックします。「証明書のインポート ウィザードの完了」ページが表示されます。
12. 「証明書のインポート ウィザードの完了」ページで、「**完了**」をクリックします。インポートが成功したことを示すダイアログ・ボックスが表示されます。「**OK**」をクリックします。
13. 「**ファイル**」メニューから「**上書き保存**」をクリックします。「名前を付けて保存」ダイアログ・ボックスが表示されます。新しいコンソールの名前を入力した後、「**保存**」をクリックします。
14. 「**Microsoft 管理コンソール**」を閉じます。

注意： Microsoft 管理コンソールを使用した信頼できる証明書のインポートに関するヘルプは、Windows 製品のドキュメントを参照するか、Microsoft 社のサポート オンライン（http://support.microsoft.com）を参照してください。

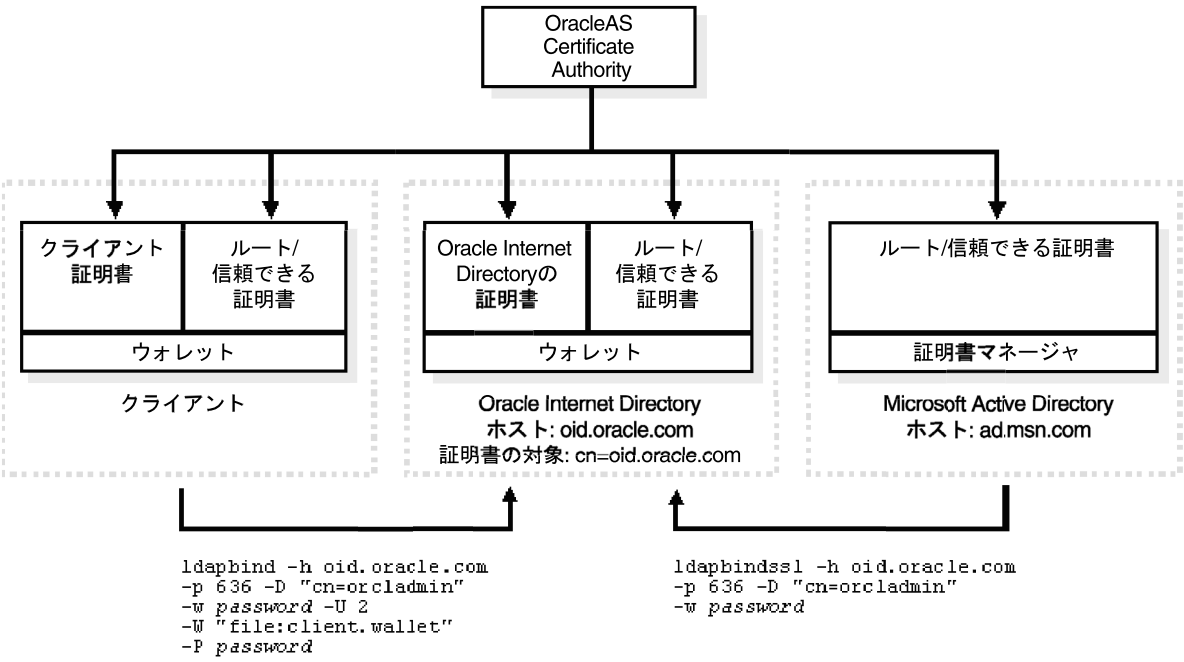
Oracle Internet Directory と Microsoft Active Directory 間の SSL 通信のテスト

Oracle Password Filter for Microsoft Active Directory は、ldapbindssl コマンドをドメイン・コントローラにインストールします。このコマンドは、Oracle Internet Directory と Microsoft Active Directory 間の SSL 通信のテストに使用できます。ldapbindssl の構文は、次のとおりです。

```
ldapbindssl -h oid_hostname -p ssl_port -D account -w password
```

図 20-1 に、ldapbindssl コマンドと ldapbind コマンドを使用して、Oracle Internet Directory と Microsoft Active Directory 間の SSL 通信をテストする方法を概念的に示します。

図 20-1 Oracle Internet Directory と Microsoft Active Directory 間の SSL 通信のテスト



Microsoft Active Directory から Oracle Internet Directory への SSL 通信をテストするには、次のようにします。

1. ドメイン・コントローラで「コマンド プロンプト」ウィンドウを開き、Oracle Password Filter for Microsoft Active Directory をインストールしたフォルダにナビゲートします。
2. ldapbindssl コマンドを入力して Oracle Internet Directory との SSL 通信をテストします。たとえば、次のコマンドでは、SSL ポート 636 で oraas.mycompany.com という Oracle Internet Directory ホストにバインドしようとします。

   ```
   ldapbindssl -h oraas.mycompany.com -p 636 -D cn=orcladmin -w welcome1
   ```

   ldapbindssl コマンドが成功した場合は、次のレスポンスが返されます。

   ```
   bind successful
   ```

`ldapbindssl` コマンドが失敗した場合は、次のレスポンスが返されます。

```
Cannot connect to the LDAP server
```

Microsoft Active Directory から Oracle Internet Directory に SSL モードで接続できない場合は、20-5 ページの「Microsoft Active Directory ドメイン・コントローラへの信頼できる証明書のインポート」で説明されているように、Microsoft Active Directory ドメイン・コントローラに信頼できる証明書が正常にインポートされていることを確認してください。

3. 「コマンド プロンプト」ウィンドウを閉じます。

Oracle Password Filter for Microsoft Active Directory のインストールおよび再構成

この項では、Oracle Password Filter for Microsoft Active Directory のインストールおよび再構成の方法について説明します。内容は次のとおりです。

- Oracle Password Filter for Microsoft Active Directory のインストール
- Oracle Password Filter for Microsoft Active Directory の再構成

Oracle Password Filter for Microsoft Active Directory をインストールまたは再構成する前に、Microsoft Active Directory および Oracle Internet Directory に必要な構成パラメータの情報を必ず収集してください。表 20-1 に、Microsoft Active Directory に必要な構成パラメータを示します。また、表 20-2 には、Oracle Internet Directory に必要な構成パラメータを示します。

表 20-1 Microsoft Active Directory 用の Oracle Password Filter の構成パラメータ

パラメータ	説明
ドメイン	このドメイン・コントローラの Microsoft Active Directory ドメイン。この値は、通常、*mycompany.com* 形式の DNS ドメイン名です。
ベース DN	Oracle Password Filter が変更済パスワードのエントリを検索する Microsoft Active Directory の DIT 内のコンテナ。パスワード伝播が失敗した場合、失敗したパスワードの DNS は、指定されたコンテナ内の `organizationalUnit` というエントリに格納されます。このため、指定されたコンテナは `organizationalUnit` オブジェクトを保持できる必要があります。このフィールドの形式は、通常、*cn=%,l=%,o=oracle,dc=com* です。
ポート	Microsoft Active Directory の LDAP ポート（通常 389）。
ホスト	Microsoft Active Directory ドメイン・コントローラの IP アドレス（ホスト名ではありません）。
Microsoft Active Directory ユーザー	Microsoft Active Directory の DIT 全体に対しての読取り権限と、Microsoft Active Directory のベース DN の下に組織単位およびサブツリーのエントリを作成する権限を持つユーザー名。管理ユーザーの DN ではなく、ユーザー名を入力する必要があります。この値の形式は、通常、*administrator@machine_name* です。
Microsoft Active Directory ユーザー・パスワード	指定された Microsoft Active Directory ユーザーのパスワード。
ログ・ファイル・パス	ログ・ファイルが作成されるディレクトリ（E:¥ADPasswordFilter¥Log など）。

表 20-2 Oracle Internet Directory 用の Oracle Password Filter の構成パラメータ

パラメータ	説明
ベース DN	Oracle Password Filter が Microsoft Active Directory から同期化されたエントリを検索する Oracle Internet Directory の DIT 内のコンテナ。`o=Microsoft Active Directory,c=us` など。
ホスト	Oracle Internet Directory の LDAP プロセスが実行されるホスト名を指定します。高可用性構成で稼働する Oracle Internet Directory の場合、ロード・バランサの仮想ホスト名を使用します。
SSL ポート	SSL サーバー認証用に構成された Oracle Internet Directory のポート。
非 SSL ポート	暗号化されていない通信用の Oracle Internet Directory。
Oracle Internet Directory ユーザー	ベース DN のユーザー・パスワードを更新する権限を持つ Oracle Internet Directory ユーザーの識別名。`cn=orcladmin` など。
Oracle Internet Directory ユーザー・パスワード	指定された Oracle Internet Directory ユーザーのパスワード。

Oracle Password Filter for Microsoft Active Directory のインストール

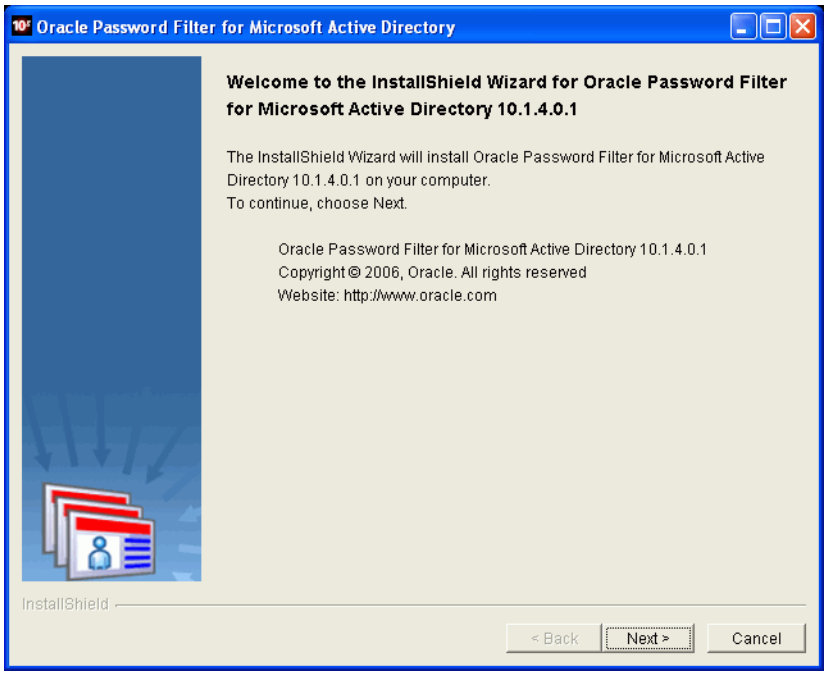
この項では、Oracle Password Filter for Microsoft Active Directory をドメイン・コントローラにインストールする方法について説明します。

注意： 次の手順に示す Microsoft Active Directory と Oracle Internet Directory の構成パラメータについては、表 20-1 および表 20-2 を参照してください。

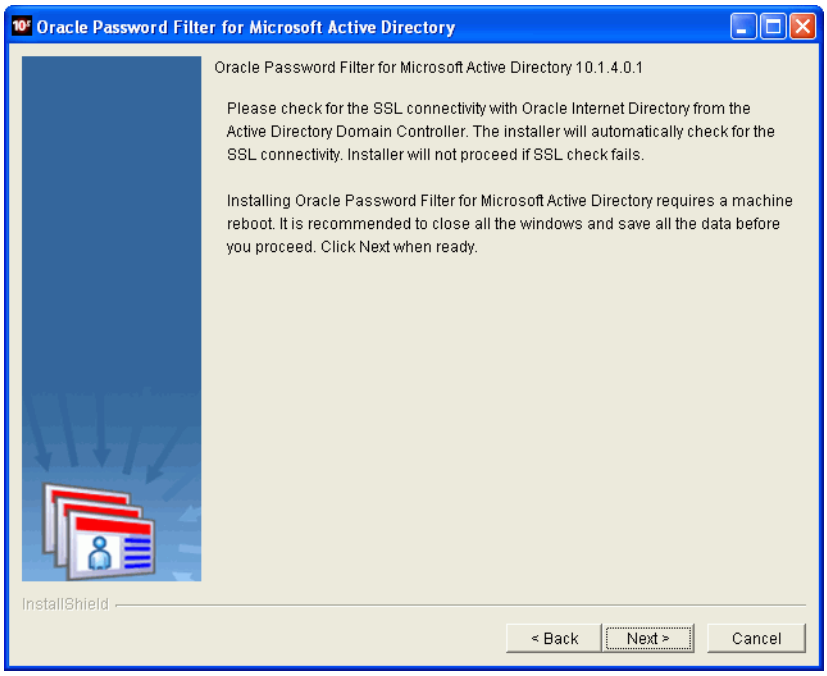
Oracle Password Filter for Microsoft Active Directory をドメイン・コントローラにインストールするには、次のようにします。

1. Oracle Application Server の CD の utils/adpwdfilter ディレクトリ内で setup.exe ファイルを探します。**setup.exe** コマンドを実行して、インストール・ファイルをドメイン・コントローラのディレクトリに解凍します。

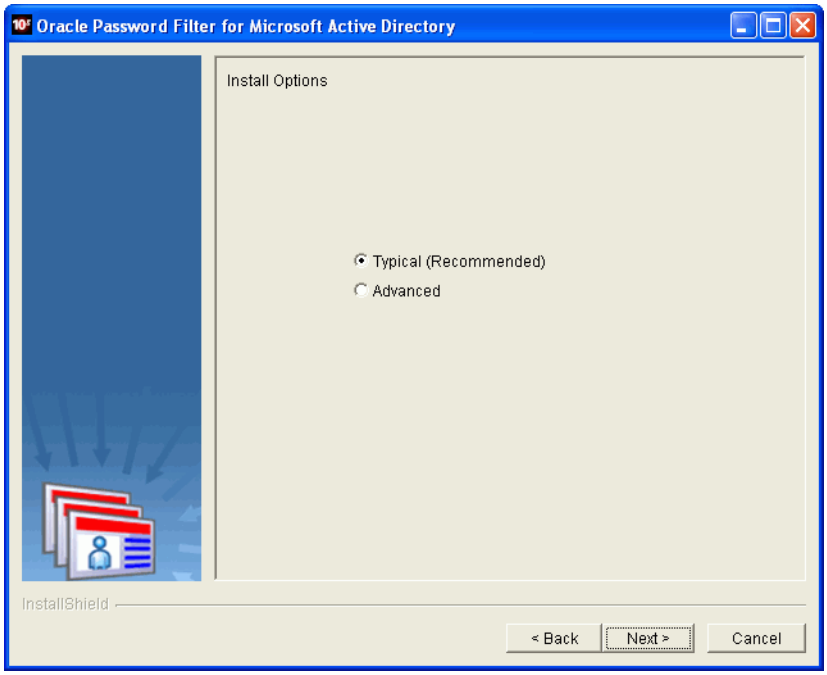
2. インストール・ファイルを解凍したディレクトリにナビゲートし、**setup.exe** をダブルクリックします。Oracle Password Filter for Microsoft Active Directory インストール・プログラムの「ようこそ」ページが表示され、プログラムによる Oracle Password Filter for Microsoft Active Directory のインストールが通知されます。



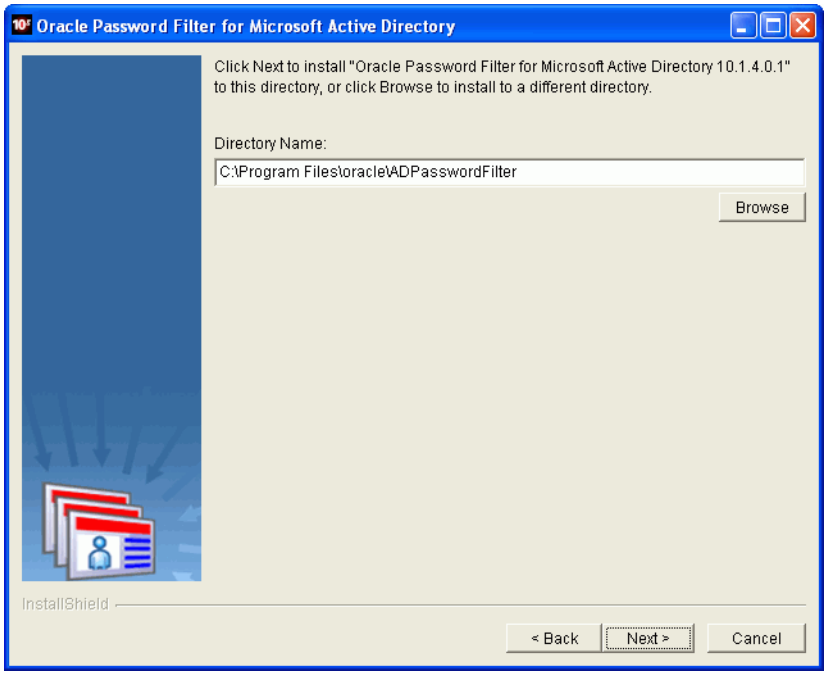
3. 「ようこそ」ページで、「**次へ**」をクリックします。インストール要件のページが表示され、Oracle Internet Directory と Microsoft Active Directory 間の SSL が有効である必要があり、インストール・プロセスの最後に Oracle Password Filter for Microsoft Active Directory によるコンピュータの再起動が必要であることが通知されます。



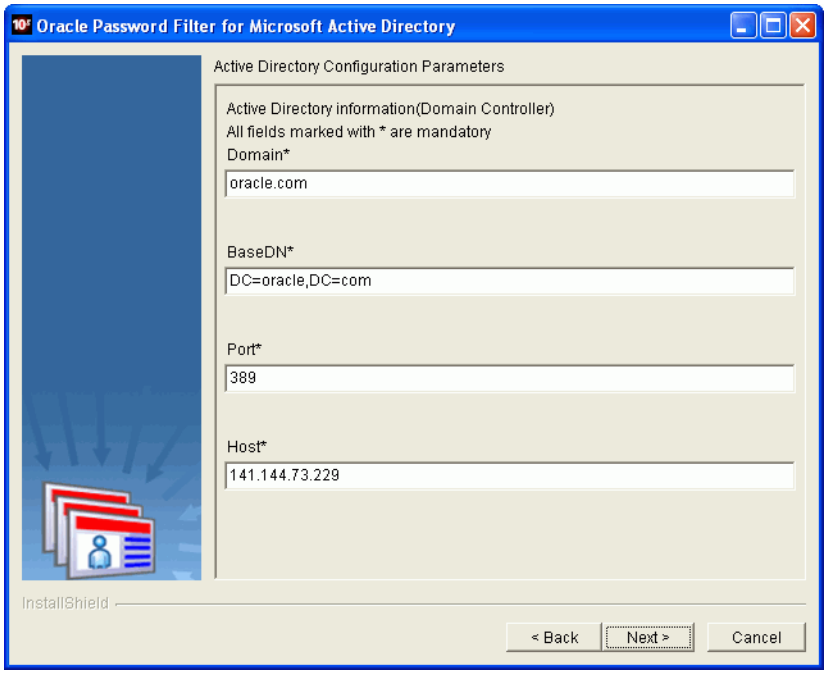
4. インストール要件のページで、「**次へ**」をクリックします。「インストール・オプション」ページが表示されます。



5. 「インストール・オプション」ページで、「**標準 (推奨)**」または「**拡張**」を選択します。拡張インストールの実行を選択すると、インストール・プロセスの後半（手順 14）で Oracle Internet Directory および Microsoft Active Directory の属性を指定できます。「**次へ**」をクリックします。インストール場所のページが表示され、Oracle Password Filter for Microsoft Active Directory をインストールするフォルダを指定するように要求されます。

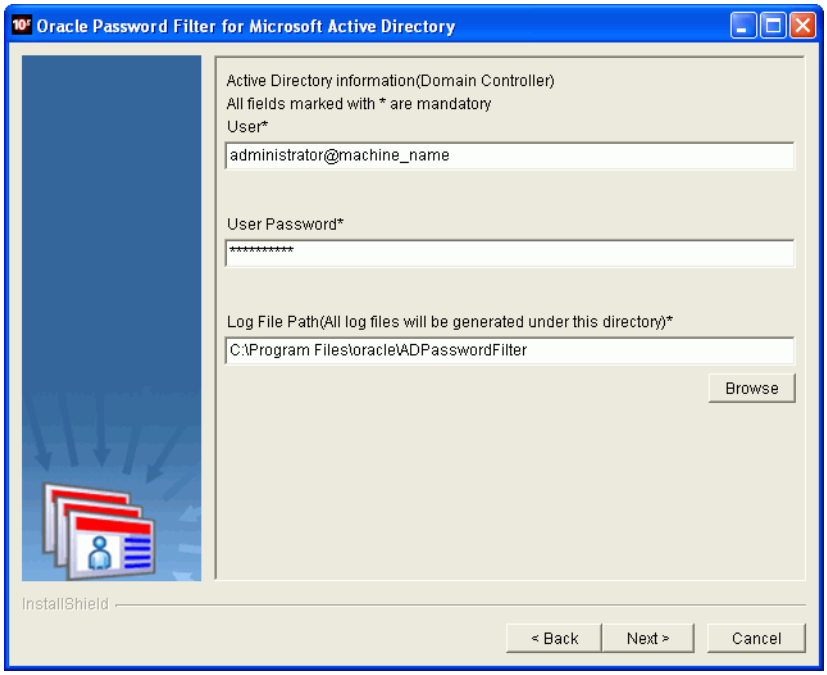


6. インストール場所のページで、デフォルトのインストール・ディレクトリを使用するか、別のディレクトリを入力します。「**参照**」をクリックして別のディレクトリを探すこともできます。インストール・ディレクトリを選択したら、「**次へ**」をクリックします。「Active Directory 構成パラメータ」ページが表示されます。



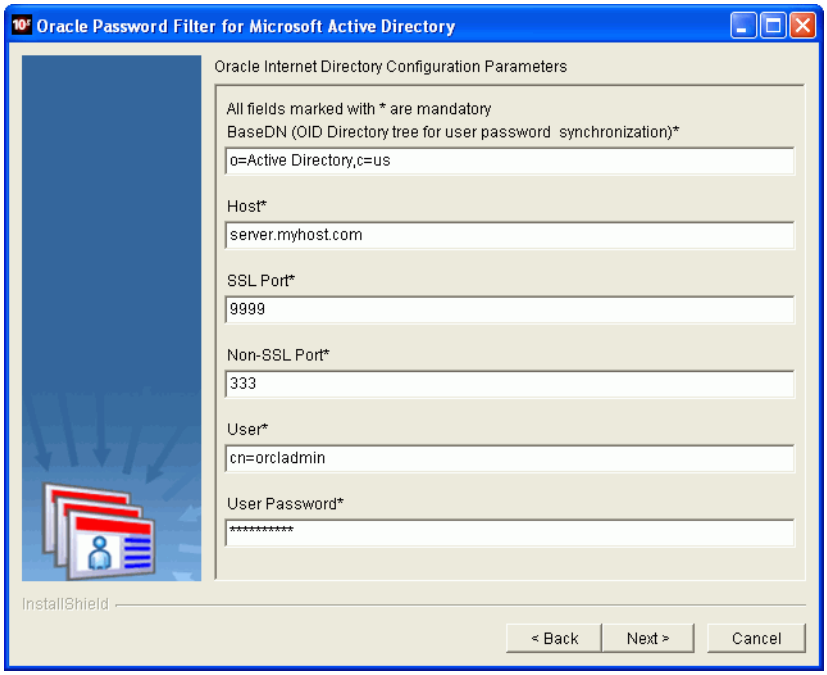
7. 「Active Directory 構成パラメータ」ページで、次のパラメータの値を入力します。
   - **ドメイン**
   - **ベース DN**
   - **ポート**
   - **ホスト**

8. 「**次へ**」をクリックします。「Active Directory 情報 (ドメイン・コントローラ)」ページが表示されます。



9. 「Active Directory 情報 (ドメイン・コントローラ)」ページで、次のパラメータの値を入力します。
   - **ユーザー**
   - **ユーザー・パスワード**
   - **ログ・ファイル・パス**

10. 「**次へ**」をクリックして続行します。「Oracle Internet Directory 構成パラメータ」ページが表示されます。

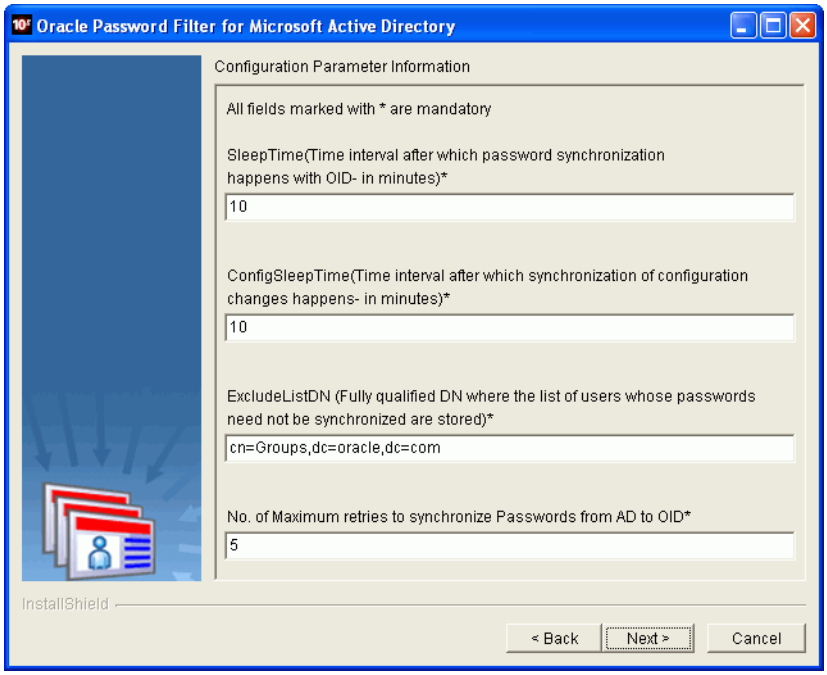


11. 「Oracle Internet Directory 構成パラメータ」ページで、次のパラメータの値を入力します。
    - **ベース DN**
    - **ホスト**
    - **SSL ポート**
    - **非 SSL ポート**
    - **ユーザー**
    - **ユーザー・パスワード**

重要： Oracle Internet Directory と Microsoft Active Directory 間にインポート同期とエクスポート同期の両方を構成した場合、Microsoft Active Directory から Oracle Internet Directory に値をインポートする同期プロファイルに指定されているものと同じバインド DN とパスワードを、ユーザー・パラメータとユーザー・パスワード・パラメータとして入力してください。この指定は、Oracle Internet Directory と Microsoft Active Directory 間でのパスワード更新のループを回避するために必要です。

---

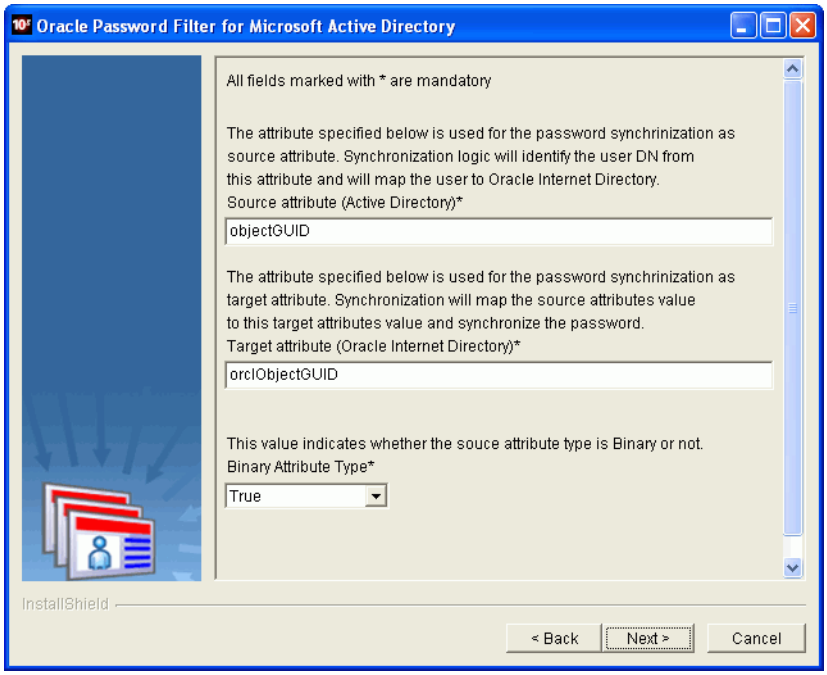
12. 「**次へ**」をクリックして続行します。「構成パラメータ情報」ページが表示されます。



13. 「構成パラメータ情報」ページで、次のパラメータの値を入力します。

- **SleepTime**: Oracle Internet Directory と Microsoft Active Directory 間でパスワードの変更を同期化する試行の時間間隔（分）。
- **ConfigSleepTime**: Oracle Internet Directory と Microsoft Active Directory 間で構成の変更を同期化する試行の時間間隔（分）。
- **ExcludeListDN**: 同期化する必要がないパスワードを持つユーザーのリストが格納されている完全修飾識別名。
- **再試行最大数** : パスワードの同期化を試行する最大回数。

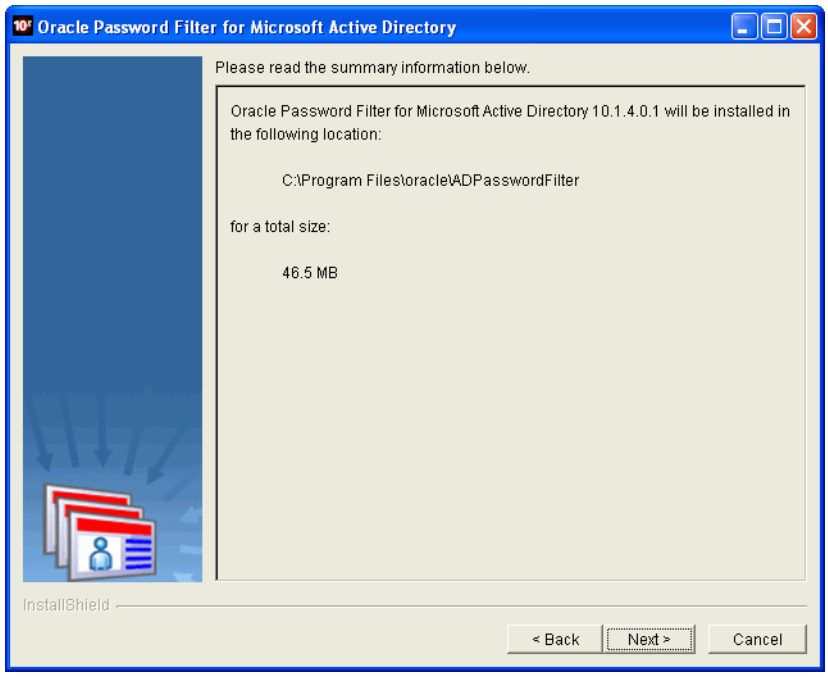
14. 「**次へ**」をクリックして続行します。「インストール・オプション」ページで「拡張」を選択した場合は、属性の指定ページが表示されます。



拡張インストールの場合、次の手順を実行します。

a. 属性の指定ページで、2 つのディレクトリ間で同期化する属性について、「**ソース属性 (Active Directory)***」ボックスと「**ターゲット属性 (Oracle Internet Directory)***」ボックスに値を入力します。また、「**バイナリ属性タイプ ***」ボックスで「`True`」または「`False`」の値を選択し、ソースの属性タイプがバイナリかどうかを指定します。

b. 「**次へ**」をクリックして続行します。サマリー・ページが表示され、Oracle Password Filter for Microsoft Active Directory がインストールされるパスが表示されます。



15. サマリー・ページで、「**次へ**」をクリックし、Oracle Password Filter をインストールします。
16. 今回初めて Oracle Password Filter をインストールする場合は、「**はい**」を選択し、要求されたらスキーマ拡張機能を Oracle Internet Directory にアップロードします。2 回目以降の場合は、「**いいえ**」を選択します。ドメイン・コントローラの再起動ページが表示されます。
17. ドメイン・コントローラの再起動ページで、「**次へ**」をクリックしてコンピュータを再起動します。
18. コンピュータが再起動したら、管理者としてログインします。ログインすると、Oracle Password Filter の残りの構成タスクが自動的に実行されます。

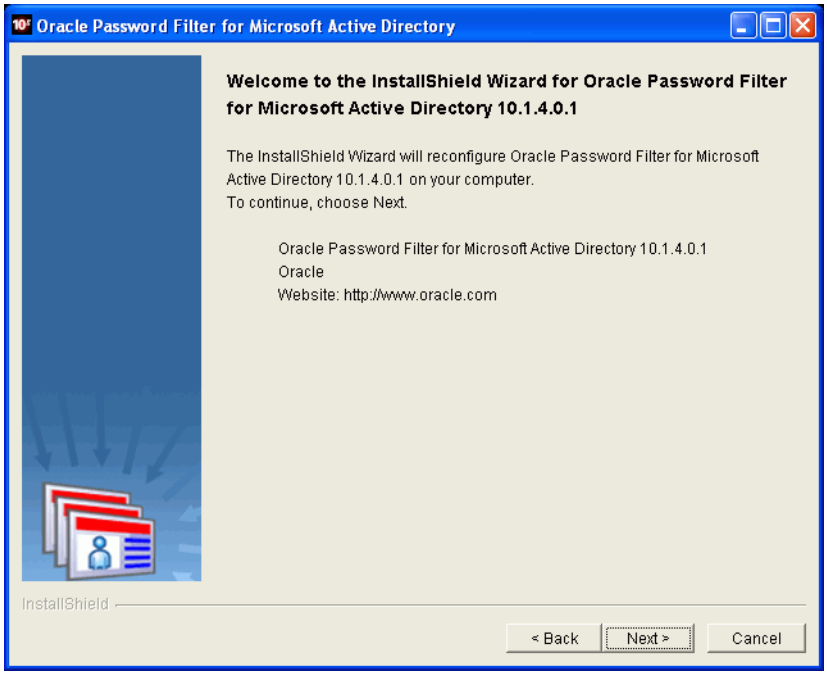
Oracle Password Filter for Microsoft Active Directory の再構成

ほとんどの場合、インストール・プロセス後に Oracle Password Filter を再構成する必要はありません。しかし、Oracle Password Filter for Microsoft Active Directory インストール・プログラムを実行すると、Oracle Password Filter for Microsoft Active Directory を再構成できます。

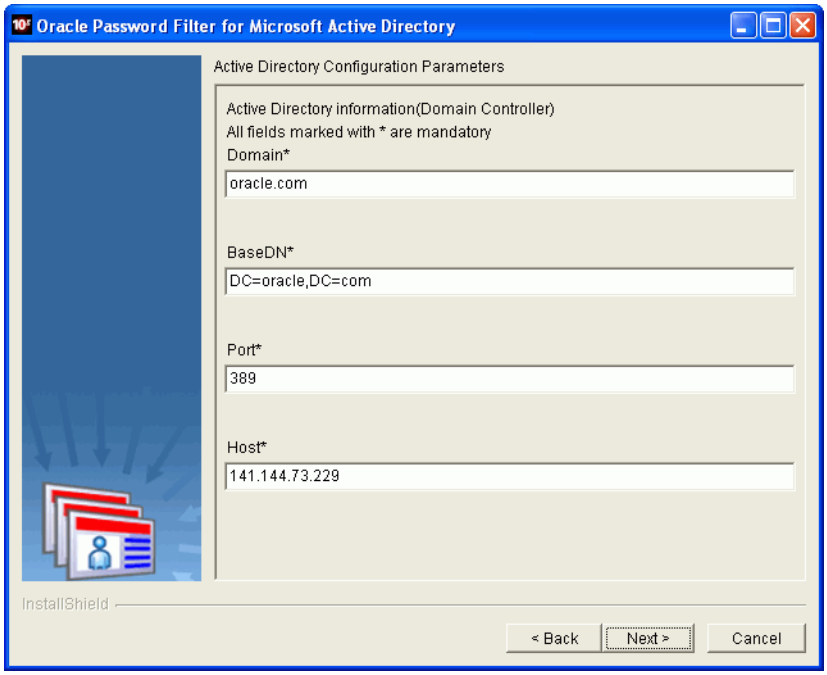
注意： 次の手順に示す Microsoft Active Directory と Oracle Internet Directory の構成パラメータについては、表 20-1 および表 20-2 を参照してください。

Oracle Password Filter for Microsoft Active Directory を再構成するには、次のようにします。

1. インストール・ファイルを解凍したディレクトリにナビゲートし、**setup.exe** をダブルクリックします。Oracle Password Filter for Microsoft Active Directory 構成プログラムの「ようこそ」ページが表示され、プログラムによる Oracle Password Filter for Microsoft Active Directory の再構成が通知されます。

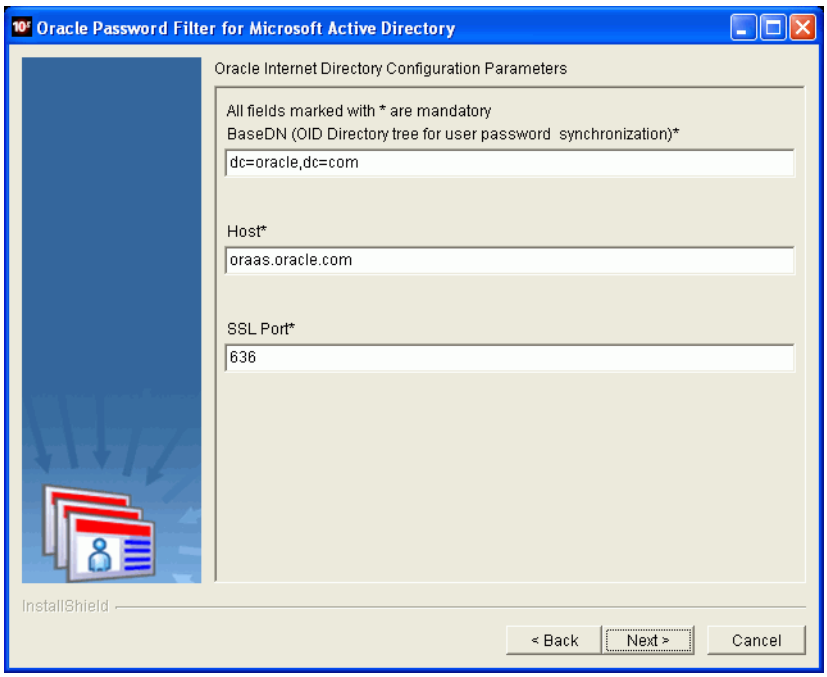


2. 「ようこそ」ページで、「**次へ**」をクリックします。「Active Directory 構成パラメータ」ページが表示されます。

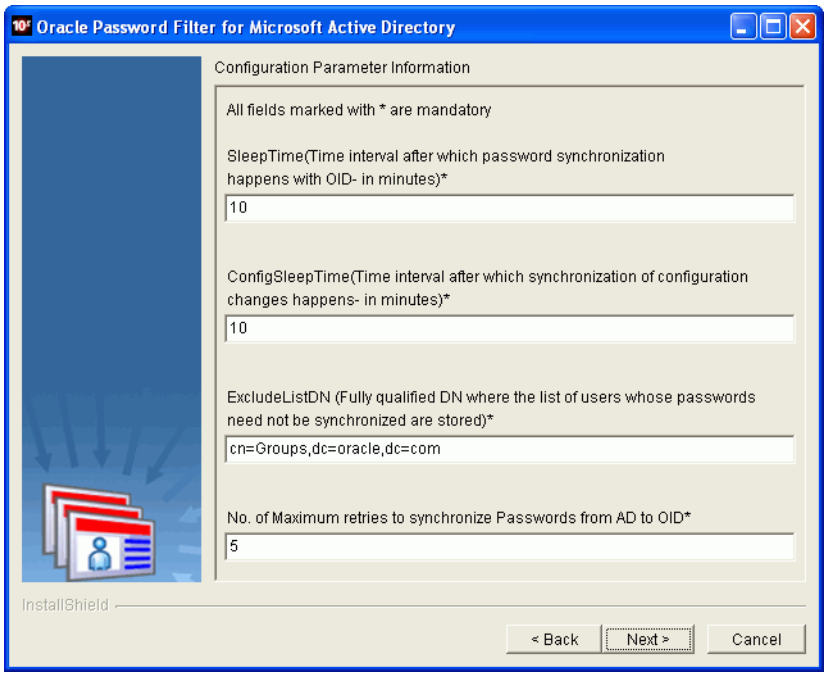


3. 「Active Directory 構成パラメータ」ページで、次のパラメータの値を変更します。
   - **ドメイン**
   - **ベース DN**
   - **ポート**
   - **ホスト**

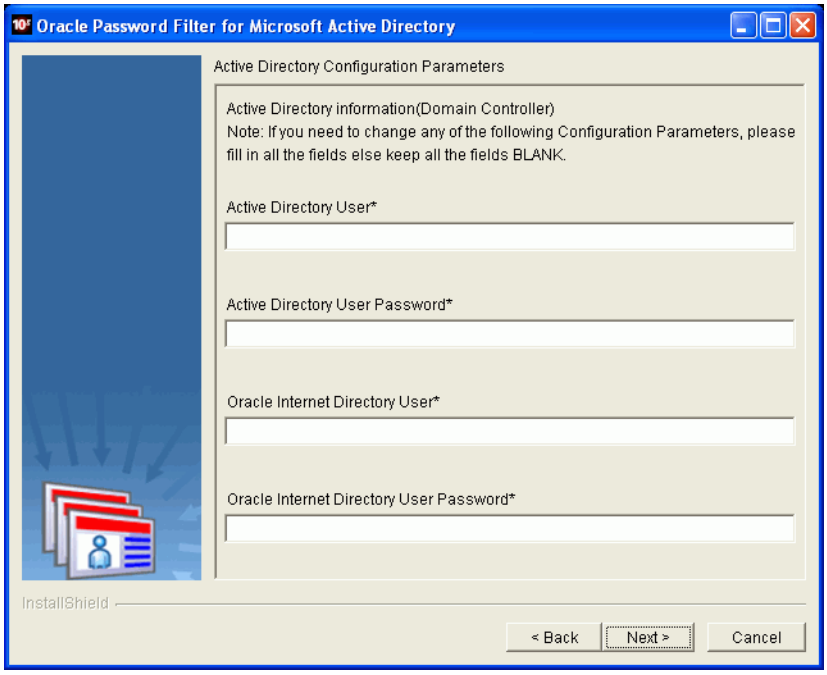
4. 「**次へ**」をクリックします。「Oracle Internet Directory 構成パラメータ」ページが表示されます。



5. 「Oracle Internet Directory 構成パラメータ」ページで、次のパラメータの値を変更します。
   - **ベース DN**
   - **ホスト**
   - **SSL ポート**
6. 「**次へ**」をクリックして続行します。「構成パラメータ情報」ページが表示されます。



7. 「構成パラメータ情報」ページで、次のパラメータの値を変更します。
   - **SleepTime**: Oracle Internet Directory と Microsoft Active Directory 間でパスワードの変更を同期化する試行の時間間隔（分）。
   - **ConfigSleepTime**: Oracle Internet Directory と Microsoft Active Directory 間で構成の変更を同期化する試行の時間間隔（分）。
   - **ExcludeListDN**: 同期化する必要がないパスワードを持つユーザーのリストが格納されている完全修飾識別名。
   - **再試行最大数** : パスワードの同期化を試行する最大回数。
8. 「**次へ**」をクリックして続行します。「Active Directory 構成パラメータ」ページが表示されます。



9. 「Active Directory 構成パラメータ」ページで、次のパラメータの値を変更します。
   - **Microsoft Active Directory ユーザー**
   - **Microsoft Active Directory ユーザー・パスワード**
   - **Oracle Internet Directory ユーザー**
   - **Oracle Internet Directory ユーザー・パスワード**

   重要： Oracle Internet Directory と Microsoft Active Directory 間にインポート同期とエクスポート同期の両方を構成した場合、Microsoft Active Directory から Oracle Internet Directory に値をインポートする同期プロファイルに指定されているものと同じバインド DN とパスワードを、ユーザー・パラメータとユーザー・パスワード・パラメータとして入力してください。この指定は、Oracle Internet Directory と Microsoft Active Directory 間でのパスワード更新のループを回避するために必要です。

10. 「**次へ**」をクリックして続行します。「再構成は正常に完了しました」ページが表示されます。
11. 「再構成は正常に完了しました」ページで、「**終了**」をクリックして Oracle Password Filter を再構成します。

Oracle Password Filter for Microsoft Active Directory の削除

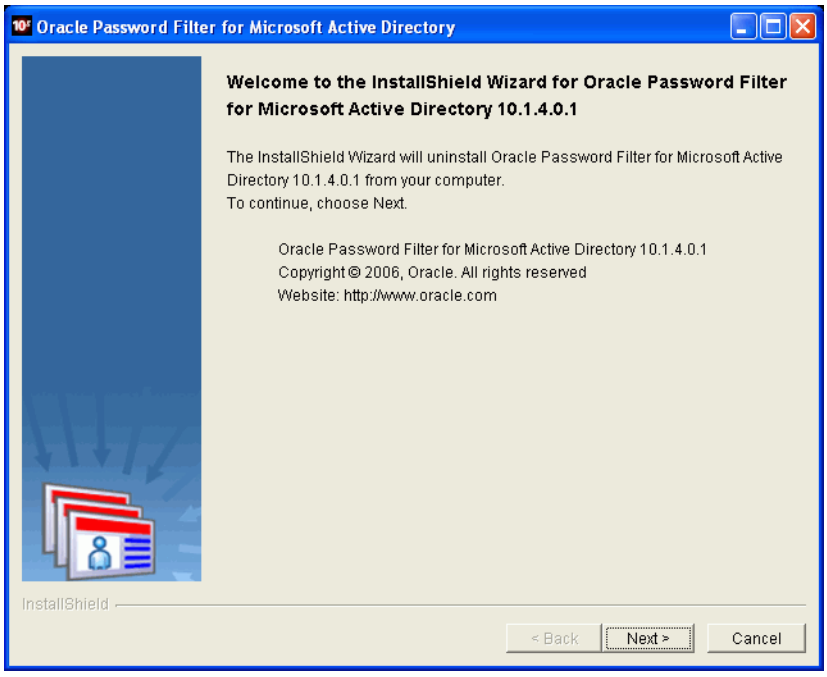
この項では、Oracle Password Filter for Microsoft Active Directory の削除方法について説明します。

Oracle Password Filter for Microsoft Active Directory を削除するには、次のようにします。

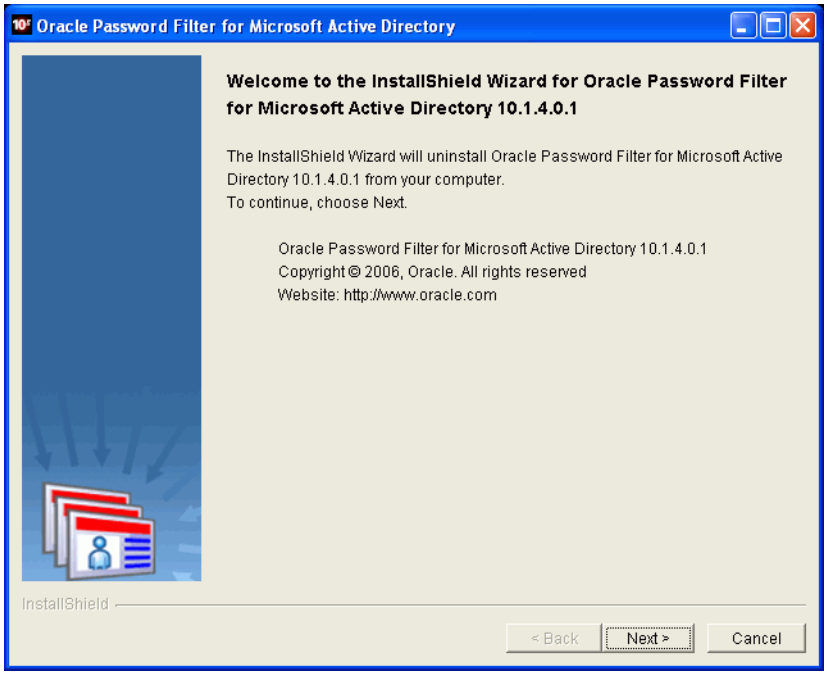
1. テキスト・エディタで **prepAD.ldif** ファイルを開きます。このファイルは、Oracle Password Filter for Microsoft Active Directory をインストールしたディレクトリにあります。prepAD.ldif ファイルにリストされたエントリとコンテナを Microsoft Active Directory 環境から削除します。
2. Windows の「**スタート**」メニューをクリックして「**ファイル名を指定して実行**」を選択します。「ファイル名を指定して実行」ダイアログ・ボックスが表示されます。
3. 「ファイル名を指定して実行」ダイアログ・ボックスに **regedt32** と入力し、「**OK**」をクリックします。「レジストリ エディタ」ウィンドウが表示されます。
4. 次のレジストリ・キーにナビゲートします。

   ```
   HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥Lsa¥orclidmpwf¥OIDConfig
   ```

5. `OidSinkNode` エントリに割り当てられたコンテナをメモします。このエントリに割り当てられたデフォルト値は `cn=Products,cn=OracleContext` です。
6. Windows の「**スタート**」メニューから「**コントロール パネル**」を選択します。「コントロール パネル」ウィンドウが表示されます。「コントロール パネル」ウィンドウで、「**プログラムの追加と削除**」を選択します。「プログラムの追加と削除」ウィンドウが表示されます。
7. 「プログラムの追加と削除」ウィンドウで、現在インストールされているプログラムのリストから「**Oracle Password Filter for Microsoft Active Directory**」を選択した後、「**変更**」または「**削除**」をクリックします。Oracle Password Filter for Microsoft Active Directory インストール・プログラムの「ようこそ」ページが表示され、プログラムによる Oracle Password Filter for Microsoft Active Directory の削除が通知されます。



8. 「ようこそ」ページで、「**次へ**」をクリックします。サマリー・ページが表示され、Oracle Password Filter for Microsoft Active Directory が削除されるパスが表示されます。



9. サマリー・ページで、「**次へ**」をクリックします。「再起動が必要」ページが表示され、Oracle Password Filter for Microsoft Active Directory の削除には削除プロセスの最後に再起動が必要であることが通知されます。

10. 「再起動が必要」ページで、「**次へ**」をクリックします。最後のページが表示され、コンピュータを再起動する必要があることが通知されます。「**次へ**」をクリックしてコンピュータを再起動します。

11. Oracle Internet Directory をインストールしたコンピュータで、次のコマンドを実行して Oracle Directory Manager を起動します。

```
oidadmin
```

12. **cn=PWSync,*OidSinkNode*** コンテナにナビゲートし、次のエントリとそのサブエントリを削除します。

```
CN=Active_Directory_Host, cn=PWSync,OidSinkNode
```

13. 次の内容のテキスト・ファイルを deleteOIDSchema.ldif という名前で新規作成します。

```
dn: cn=subschemasubentry
changetype: modify
delete: objectclasses
objectclasses: ( 2.16.840.1.113894.8.2.1002 NAME 'adconfig' SUP top STRUCTURAL MUST
( cn ) MAY ( ADBaseDN $ deleteomain $ ADHost $ ADPort $ Log $ ResourceFilePath ) )

dn: cn=subschemasubentry
changetype: modify
delete: objectclasses
objectclasses: ( 2.16.840.1.113894.8.2.1001 NAME 'oidconfig' SUP top STRUCTURAL
MUST ( cn ) MAY ( OIDBaseDN $ OIDHost $ OIDPort $ passwdattr $ MSDEDSN $
OIDObjectClass $ OIDLog $ ExcludeListDN $ MAX_RETRIES $ OIDSSLType $ OIDWalletLoc $
OidSinkNode $ SleepTime $ stop $ ConfigSleepTime $ OIDConfigSynchKey ) )
```

```
dn: cn=subschemasubentry
changetype: modify
delete: attributetypes
attributetypes: ( 2.16.840.1.113894.8.1.1001  NAME 'OIDBaseDN' DESC 'OID Base
Search DN' SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )

dn: cn=subschemasubentry
changetype: modify
delete: attributetypes
attributetypes: ( 2.16.840.1.113894.8.1.1002  NAME 'OIDHost' DESC 'OID Host' SYNTAX
'1.3.6.1.4.1.1466.115.121.1.15' )

dn: cn=subschemasubentry
changetype: modify
delete: attributetypes
attributetypes: ( 2.16.840.1.113894.8.1.1003  NAME 'OIDPort' DESC 'OID Port' SYNTAX
'1.3.6.1.4.1.1466.115.121.1.15' )

dn: cn=subschemasubentry
changetype: modify
delete: attributetypes
attributetypes: ( 2.16.840.1.113894.8.1.1004  NAME 'passwdattr' DESC 'Pass
Attribute' SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )

dn: cn=subschemasubentry
changetype: modify
delete: attributetypes
attributetypes: ( 2.16.840.1.113894.8.1.1005  NAME 'MSDEDSN' DESC 'DB DSN' SYNTAX
'1.3.6.1.4.1.1466.115.121.1.15' )

dn: cn=subschemasubentry
changetype: modify
delete: attributetypes
attributetypes: ( 2.16.840.1.113894.8.1.1006  NAME 'OIDObjectClass' DESC 'AD Object
Class' SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )

dn: cn=subschemasubentry
changetype: modify
delete: attributetypes
attributetypes: ( 2.16.840.1.113894.8.1.1007  NAME 'OIDLog' DESC 'OID Log' SYNTAX
'1.3.6.1.4.1.1466.115.121.1.15' )

dn: cn=subschemasubentry
changetype: modify
delete: attributetypes
attributetypes: ( 2.16.840.1.113894.8.1.1008  NAME 'ExcludeListDN' DESC 'Exclude
List' SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )

dn: cn=subschemasubentry
changetype: modify
delete: attributetypes
attributetypes: ( 2.16.840.1.113894.8.1.1009  NAME 'MAX_RETRIES' DESC 'Max Retries'
SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )

dn: cn=subschemasubentry
changetype: modify
delete: attributetypes
attributetypes: ( 2.16.840.1.113894.8.1.1010  NAME 'OIDSSLType' DESC 'OID SSL Type'
SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

```
dn: cn=subschemasubentry
changetype: modify
delete: attributetypes
attributetypes: ( 2.16.840.1.113894.8.1.1011  NAME 'OIDWalletLoc' DESC 'OID Wallet
Loc' SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )

dn: cn=subschemasubentry
changetype: modify
delete: attributetypes
attributetypes: ( 2.16.840.1.113894.8.1.1012  NAME 'OidSinkNode' DESC 'Config Sync
Node' SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )

dn: cn=subschemasubentry
changetype: modify
delete: attributetypes
attributetypes: ( 2.16.840.1.113894.8.1.1013  NAME 'SleepTime' DESC 'Sleep Time for
store thread' SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )

dn: cn=subschemasubentry
changetype: modify
delete: attributetypes
attributetypes: ( 2.16.840.1.113894.8.1.1014 NAME 'stop' DESC 'Stop flag for store
thread' SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )

dn: cn=subschemasubentry
changetype: modify
delete: attributetypes
attributetypes: ( 2.16.840.1.113894.8.1.1015 NAME 'ConfigSleepTime' DESC 'Sleep
Time for config thread' SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )

dn: cn=subschemasubentry
changetype: modify
delete: attributetypes
attributetypes: ( 22.16.840.1.113894.8.1.1016 NAME 'OIDConfigSynchKey' DESC 'Config
Sync key' SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )

dn: cn=subschemasubentry
changetype: modify
delete: attributetypes
attributetypes: ( 2.16.840.1.113894.8.1.1017 NAME 'ADBaseDN' SYNTAX
'1.3.6.1.4.1.1466.115.121.1.15' )

dn: cn=subschemasubentry
changetype: modify
delete: attributetypes
attributetypes: ( 2.16.840.1.113894.8.1.1018 NAME 'ADPort' SYNTAX
'1.3.6.1.4.1.1466.115.121.1.15' )

dn: cn=subschemasubentry
changetype: modify
delete: attributetypes
attributetypes: ( 2.16.840.1.113894.8.1.1019 NAME 'ADHost' SYNTAX
'1.3.6.1.4.1.1466.115.121.1.15' )

dn: cn=subschemasubentry
changetype: modify
delete: attributetypes
attributetypes: ( 2.16.840.1.113894.8.1.1020 NAME 'ADDomain' SYNTAX
'1.3.6.1.4.1.1466.115.121.1.15' )
```

```
dn: cn=subschemasubentry
changetype: modify
delete: attributetypes
attributetypes: ( 2.16.840.1.113894.8.1.1021 NAME 'Log' SYNTAX
'1.3.6.1.4.1.1466.115.121.1.15' )

dn: cn=subschemasubentry
changetype: modify
delete: attributetypes
attributetypes: ( 2.16.840.1.113894.8.1.1022 NAME 'ResourceFilePath' SYNTAX
'1.3.6.1.4.1.1466.115.121.1.15' )
```

14. ldapmodify コマンドを使用して、deleteOIDSchema.ldif ファイルをロードします。

```
$ORACLE_HOME/bin/ldapmodify -h OID host -p OID port
-D "DN of privileged OID user" -w "password of privileged OID user"
-f deleteOIDSchema.ldif
```

21

Sun Java System Directory との統合

この章では、本番環境で Oracle Identity Management と Sun Java System Directory（以前の SunONE iPlanet）を統合する手順について説明します。内容は次のとおりです。

- Sun Java System Directory の同期要件の確認
- Sun Java System Directory との基本同期の構成
- Sun Java System Directory との拡張統合の構成

注意： この章を読む前に、『Oracle Internet Directory 管理者ガイド』の Oracle Internet Directory の概念とアーキテクチャに関する章を理解しておく必要があります。また、このマニュアルのここまでの章、特に次の章を理解していることを前提としています。

- 第 1 章「Oracle Identity Management 統合の概要」
- 第 4 章「Oracle Directory Integration Platform の管理」
- 第 5 章「Oracle Directory Synchronization Service」
- 第 17 章「サード・パーティ・ディレクトリ統合の概念と考慮事項」

Sun Java System Directory との統合のデモンストレーションを構成する場合は、Oracle Identity Management 10*g*（10.1.4.0.1）の Oracle By Example シリーズを参照してください。Oracle Technology Network（`http://www.oracle.com/technology/`）で参照可能です。

Sun Java System Directory の同期要件の確認

Sun Java System Directory で基本同期または拡張同期を構成するには、18-2 ページの「同期要件の確認」の指示に従い、使用する環境で必要な同期要件が満たされていることを確認してください。また、Sun Java System Directory と統合する前に、次の手順を実行する必要があります。

- インポート操作とエクスポート操作の実行に十分な権限を持つユーザー・アカウントを Sun Java System Directory に作成する際に、tombstone の読取りに十分な権限を必ず割り当てます。
- Sun Java System Directory で変更ログを有効にします。
- Retro Change Log プラグインを有効にします。

Sun Java System Directory との基本同期の構成

Express 構成コマンドを使用すると、Oracle Internet Directory と Sun Java System Directory 間の同期を迅速に確立できます。Express 構成では、デフォルトの設定を使用してすべての必須構成を自動的に実行し、インポート用とエクスポート用の 2 つの同期プロファイルも作成します。Express 構成を使用して Sun Java System Directory と同期化するには、18-3 ページの「Express 構成による同期プロファイルの作成」の指示に従ってください。

Sun Java System Directory との拡張統合の構成

Oracle Directory Integration Platform をインストールすると、サポート対象のサード・パーティ・ディレクトリごとにインポートおよびエクスポートの同期プロファイルのサンプルが自動的に作成されます。Sun Java System Directory 用に作成された同期プロファイルのサンプルは、次のとおりです。

- `iPlanetImport`: Sun Java System Directory から Oracle Internet Directory へ変更をインポートするためのプロファイル
- `iPlanetExport` : Oracle Internet Directory から Sun Java System Directory へ変更をエクスポートするためのプロファイル

21-2 ページの「Sun Java System Directory との基本同期の構成」で説明されているように、Directory Integration アシスタント（`dipassistant`）の Express 構成オプションを使用して同期プロファイルを追加作成することもできます。

インストール・プロセス時または Express 構成によって作成されたインポートおよびエクスポートの同期プロファイルは、Oracle Internet Directory と Sun Java System Directory の統合を配置する際に使用する開始点としてのみ利用されます。デフォルトの同期プロファイルは事前定義の仮定を使用して作成されるため、次の手順を順序どおりに実行して、環境に合せてそれらをさらにカスタマイズする必要があります。

- 手順 1: 統合の計画
- 手順 2: レルムの構成
- 手順 3: ACL のカスタマイズ
- 手順 4: 属性マッピングのカスタマイズ
- 手順 5: 削除を同期化するための Sun Java System Directory コネクタのカスタマイズ
- 手順 6: パスワードの同期化
- 手順 7: SSL モードでの同期
- 手順 8: Sun Java System Directory 外部認証プラグインの構成
- 手順 9: 構成後タスクおよび管理タスクの実行

手順 1: 統合の計画

第 17 章「サード・パーティ・ディレクトリ統合の概念と考慮事項」、特に 17-26 ページの「Sun Java System Directory 統合の概念」を読んで、統合を計画します。

手順 2: レルムの構成

18-7 ページの「レルムの構成」の指示に従い、レルムを構成します。

手順 3: ACL のカスタマイズ

18-8 ページの「Access 制御リストのカスタマイズ」で説明されているように、ACL をカスタマイズします。

手順 4: 属性マッピングのカスタマイズ

Sun Java System Directory と統合する場合は、次の属性レベル・マッピングがすべてのオブジェクトに対して必須です。

```
Targetdn:1: : :orclsourceobjectdn: : orclSUNOneobject:
```

例 21-1 Sun Java System Directory のユーザー・オブジェクト用の属性レベル・マッピング

```
Cn:1: : :person: cn: :person:
sn:1: : :person: sn: :person:
```

例 21-2 Sun Java System Directory のグループ・オブジェクト用の属性レベル・マッピング

```
Cn:1: : :groupofname: cn:groupofuniquenames
```

この例では、Sun Java System Directory の Cn および sn は、それぞれ Oracle Internet Directory の cn および sn にマップされます。

18-9 ページの「マッピング・ルールのカスタマイズ」の指示に従い、属性マッピングをカスタマイズします。

手順 5: 削除を同期化するための Sun Java System Directory コネクタのカスタマイズ

削除の同期が必要で、マッピング・ルールに必須属性がある場合、tombstone が正しく構成されていることを確認してください。

Sun Java System Directory で tombstone が構成されていることを確認するには、次のコマンドを実行します。

```
$ORACLE_HOME/bin/ldapsearch -h connected_directory_host
-p connected_directory_port -D  connected_directory_account
-w connected_directory_password -b source_domain
-s sub "objectclass=nstombstone"
```

このコマンドにより、すべての削除済エントリの情報が得られます。

関連資料： tombstone の構成の詳細は、Sun Java System Directory のドキュメントを参照してください。

注意： レプリケーションが有効な場合、tombstone は Sun Java System Directory に対して自動的に構成されます。

手順 6: パスワードの同期化

Oracle Internet Directory および Sun Java System Directory では、同じ一連のパスワード・ハッシング技術をサポートしています。Oracle Internet Directory と Sun Java System Directory 間でパスワードを同期化するには、両方のディレクトリに対して SSL サーバー認証モードが構成され、次のマッピング・ルールがマッピング・ファイルに存在する必要があります。

```
Userpassword: : :person:userpassword: :person
```

手順 7: SSL モードでの同期

18-11 ページの「SSL モードでの同期用サード・パーティ・ディレクトリ・コネクタの構成」の指示に従い、SSL モードでの同期用に Sun Java System Directory を構成します。

手順 8: Sun Java System Directory 外部認証プラグインの構成

18-13 ページの「外部認証プラグインの構成」の指示に従い、Sun Java System Directory 外部認証プラグインを構成します。

手順 9: 構成後タスクおよび管理タスクの実行

構成後タスクおよび継続的な管理タスクの詳細は、第 23 章「サード・パーティ・ディレクトリとの統合の管理」を参照してください。

22

Novell eDirectory または OpenLDAP との統合

この章では、本番環境で Oracle Identity Management と Novell eDirectory または OpenLDAP を統合する手順について説明します。内容は次のとおりです。

- Novell eDirectory または OpenLDAP の同期要件の確認
- Novell eDirectory または OpenLDAP との基本同期の構成
- Novell eDirectory または OpenLDAP との拡張統合の構成

注意： この章を読む前に、『Oracle Internet Directory 管理者ガイド』の Oracle Internet Directory の概念とアーキテクチャに関する章を理解しておく必要があります。また、このマニュアルのここまでの章、特に次の章を理解していることを前提としています。

- 第 1 章「Oracle Identity Management 統合の概要」
- 第 4 章「Oracle Directory Integration Platform の管理」
- 第 5 章「Oracle Directory Synchronization Service」
- 第 17 章「サード・パーティ・ディレクトリ統合の概念と考慮事項」

同期は、Oracle Application Server 10*g*（10.1.4.0.1）以上と、Novell eDirectory 8.6.2 以上または OpenLDAP 2.2 以上との間でサポートされます。

Novell eDirectory または OpenLDAP の同期要件の確認

Novell eDirectory または OpenLDAP で基本同期または拡張同期を構成するには、18-2 ページの「同期要件の確認」の指示に従い、使用する環境で必要な同期要件が満たされていることを確認してください。

Novell eDirectory または OpenLDAP との基本同期の構成

Express 構成コマンドを使用すると、Oracle Internet Directory と Novell eDirectory または OpenLDAP 間の同期を迅速に確立できます。Express 構成では、デフォルトの設定を使用してすべての必須構成を自動的に実行し、インポート用とエクスポート用の 2 つの同期プロファイルも作成します。Express 構成を使用して Novell eDirectory または OpenLDAP と同期化するには、18-3 ページの「Express 構成による同期プロファイルの作成」の指示に従ってください。

Novell eDirectory または OpenLDAP との拡張統合の構成

Oracle Directory Integration Platform をインストールすると、サポート対象のサード・パーティ・ディレクトリごとにインポートおよびエクスポートの同期プロファイルのサンプルが自動的に作成されます。Novell eDirectory 用に作成された同期プロファイルのサンプルは、次のとおりです。

- `Novell eDirectoryImp`: Novell eDirectory から Oracle Internet Directory へ変更をインポートするためのプロファイル
- `Novell eDirectoryExp`: Oracle Internet Directory から Novell eDirectory へ変更をエクスポートするためのプロファイル

OpenLDAP 用に作成された同期プロファイルのサンプルは、次のとおりです。

- `OpenLDAPImport`: OpenLDAP から Oracle Internet Directory へ変更をインポートするためのプロファイル
- `OpenLDAPExport`: Oracle Internet Directory から OpenLDAP へ変更をエクスポートするためのプロファイル

22-2 ページの「Novell eDirectory または OpenLDAP との基本同期の構成」で説明されているように、Directory Integration アシスタント（`dipassistant`）の Express 構成オプションを使用して同期プロファイルを追加作成することもできます。インストール・プロセス時または Express 構成によって作成されたインポートおよびエクスポートの同期プロファイルは、Oracle Internet Directory と Novell eDirectory または OpenLDAP の統合を配置する際に使用する開始点としてのみ利用されます。デフォルトの同期プロファイルは事前定義の仮定を使用して作成されるため、次の手順を順序どおりに実行して、環境に合せてそれらをさらにカスタマイズする必要があります。

- 手順 1: 統合の計画
- 手順 2: レルムの構成
- 手順 3: Novell eDirectory または OpenLDAP から情報を取得する検索フィルタのカスタマイズ
- 手順 4: ACL のカスタマイズ
- 手順 5: 属性マッピングのカスタマイズ
- 手順 6: 削除を同期化するための Novell eDirectory または OpenLDAP コネクタのカスタマイズ
- 手順 7: 追加構成情報の属性用の同期パラメータの指定
- 手順 8: パスワードを同期化するための OpenLDAP コネクタの構成
- 手順 9: SSL モードでの同期
- 手順 10: Novell eDirectory または OpenLDAP 外部認証プラグインの構成
- 手順 11: 構成後タスクおよび管理タスクの実行

手順 1: 統合の計画

第 17 章「サード・パーティ・ディレクトリ統合の概念と考慮事項」、特に 17-27 ページの「Novell eDirectory および OpenLDAP 統合の概念」を読んで、統合を計画します。

手順 2: レルムの構成

18-7 ページの「レルムの構成」の指示に従い、レルムを構成します。

手順 3: Novell eDirectory または OpenLDAP から情報を取得する検索フィルタのカスタマイズ

デフォルトでは、Novell eDirectory または OpenLDAP コネクタにより、`modifytimestamp` 属性に基づいてコンテナ内のすべてのオブジェクトに対する変更が取得されます。特定のタイプのオブジェクトに対する変更（ユーザーやグループに対する変更など）を取得する場合は、LDAP 検索フィルタを構成する必要があります。このフィルタにより、Novell eDirectory または OpenLDAP コネクタの Novell eDirectory または OpenLDAP に対する問合せの際に、不要な変更が排除されます。フィルタは、同期プロファイルの「接続されたディレクトリー致フィルタ」属性（`orclodipcondirmatchingfilter`）に格納されます。

Novell eDirectory または OpenLDAP のサンプルのインポート・プロファイルは、それぞれ Novell eDirectory および OpenLDAP のユーザー、グループおよびコンテナ・オブジェクトに対する変更を取得するように構成されています。コンピュータは取得されません。`searchfilter` 属性の値は、次のように設定されます。

```
searchfilter=(&(!(modifiersname=connected_dir_account))
(|(objectclass=domain)(objectclass=organizationalunit)
(objectclass=organization)(objectclass=person) (objectclass=groupofnames)))
```

ユーザーまたはグループ以外のエントリを同期化する場合は、Directory Integration アシスタント（`dipassistant`）を使用して `searchfilter` 属性を更新します。たとえば、次のコマンドは、`searchfilter` 属性を更新してユーザーとグループのみを同期化します。

```
dipassistant mp -h host -p port -D binddn -w bindpass -profile profilename
odip.profile.condirfilter=searchfilter=
(|(objectclass=groupofnames)(objectclass=person))
```

注意： `searchfilter` 属性に指定する属性はすべて、Novell eDirectory または OpenLDAP の索引付き属性のように構成する必要があります。

関連資料： LDAP 検索フィルタを構成する方法は、『Oracle Internet Directory 管理者ガイド』の LDAP フィルタ定義に関する付録を参照してください。

手順 4: ACL のカスタマイズ

18-8 ページの「Access 制御リストのカスタマイズ」で説明されているように、ACL をカスタマイズします。

手順 5: 属性マッピングのカスタマイズ

Novell eDirectory と統合する場合は、次の属性レベル・マッピングがすべてのオブジェクトに対して必須です。

```
GUID:1: : :orclNDSObjectGUID: :orclndsObject:bin2b64(guid)
Modifytimestamp:1 : : :orclsourcemodifytimestamp: :orclndsobject:
Createtimestamp:1 : : :orclsourcecreatetimestamp: :orclndsobject:
Targetdn:1: : :orclsourceobjectdn: : orclndsobject:
```

OpenLDAP と統合する場合は、次の属性レベル・マッピングがすべてのオブジェクトに対して必須です。

```
entryuuid:1: : : orclOpenLdapEntryUUID: : orclOpenLdapObject
Modifytimestamp:1 : : :orclsourcemodifytimestamp: : orclOpenLdapObject
Createtimestamp:1 : : :orclsourcecreatetimestamp: : orclOpenLdapObject
Targetdn:1: : :orclsourceobjectdn: : orclOpenLdapObject:
```

例 22-1 Novell eDirectory または OpenLDAP のユーザー・オブジェクト用の属性レベル・マッピング

```
Cn:1: : :person: cn: :person:
sn:1: : :person: sn: :person:
```

例 22-2 Novell eDirectory または OpenLDAP のグループ・オブジェクト用の属性レベル・マッピング

```
Cn:1: : :groupofname: cn:groupofuniquenames
```

この例では、Novell eDirectory または OpenLDAP の `Cn` および `sn` は、それぞれ Oracle Internet Directory の `cn` および `sn` にマップされます。

18-9 ページの「マッピング・ルールのカスタマイズ」の指示に従い、属性マッピングをカスタマイズします。

手順 6: 削除を同期化するための Novell eDirectory または OpenLDAP コネクタのカスタマイズ

17-27 ページの「Novell eDirectory または OpenLDAP から Oracle Internet Directory への同期」で説明されているように、Oracle Internet Directory での Novell eDirectory または OpenLDAP からの削除の同期化はリコンシリエーション方式で処理されます。Oracle Internet Directory で Novell eDirectory または OpenLDAP からの削除を同期化する際にサーバーでのパフォーマンスの低下を回避するために、DIT の特定のサブセットを検索するように比較をカスタマイズできます。`ReconciliationRules` キーワードを使用して、サブセットの検索条件をマッピング・ファイルの一部として指定します。

Novell eDirectory のデフォルトのリコンシリエーション・ルールは、次のとおりです。

```
inetorgperson:cn:*
groupofnames:cn:*
```

OpenLDAP のデフォルトのリコンシリエーション・ルールは、次のとおりです。

```
inetorgperson:cn:*
groupofuniquenames:cn:*
```

これらのルールで指定される検索条件は、次の 2 つの手順に該当します。

1. `inetorgperson` オブジェクト・クラス内のすべてのエントリを検索します。属性値に応じて、このルール内に異なるサブセットを指定することもできます。
2. Novell eDirectory の `groupofnames` オブジェクト・クラス内または OpenLDAP の `groupofuniquenames` オブジェクト・クラス内のすべてのエントリを検索します。

リコンシリエーション・ルールの定義方法

リコンシリエーション・ルールは、1 つのオブジェクト・クラス、1 つの属性、任意の数の値を使用して定義します。Oracle Internet Directory と同期化される任意の属性を使用してリコンシリエーション・ルールを定義できます。ただし、次の 2 つの要件に従う必要があります。

- 指定されたオブジェクト・クラスの属性は、マッピング・ルールに定義されている必要があります。
- 対応する Oracle Internet Directory の属性は、索引付けされている必要があります。

たとえば、次のリコンシリエーション・ルールを考えてみます。

```
myobjclass:myattr:val1:val2:val3
```

このリコンシリエーション・ルールでは、オブジェクト・クラス名は myobjclass、属性名は myattr です。val1、val2 または val3 の値を myattr 属性に指定できます。myattr 属性を使用するには、次のマッピング・ルールを定義する必要があります。

```
myattr: : : myobjclass:attr: :objclass:
```

このマッピング・ルールは、myattr 属性を myattr オブジェクト・クラスに定義します。attr は Oracle Internet Directory の対応する属性で、索引付けする必要があります。

リコンシリエーション・ルールを使用して削除を同期化する方法

リコンシリエーション・ルールを定義すると、Novell eDirectory または OpenLDAP に問い合せて削除エントリ数を特定する検索フィルタが生成されます。たとえば、前の項の myobjclass および attr リコンシリエーション・ルールの例では、次の検索フィルタが Novell eDirectory または OpenLDAP に生成されます。

- `(&(objectclass= myobjclass) (createtimestamp<=orclodipreconciliationtimestamp) (myattr=val1))`
- `(&(objectclass= myobjclass) (createtimestamp<= orclodipreconciliationtimestamp) (myattr=val2))`
- `(&(objectclass= myobjclass)(createtimestamp<= orclodipreconciliationtimestamp)(myattr=val3))`

また、リコンシリエーション・ルールとマッピング・ルールによって、対応するフィルタが Oracle Internet Directory に生成されます。たとえば、myobjclass および attr リコンシリエーション・ルールについて、次の Oracle Internet Directory のフィルタが生成されます。

- `(&(objectclass= objclass) (orclndsobjectguid=*)(orclSourceCreateTimeStamp<= orclodipreconciliationtimestamp)(attr=val1))`
- `(&(objectclass= objclass) (orclndsobjectguid=*)(orclSourceCreateTimeStamp<= orclodipreconciliationtimestamp)(attr=val2))`
- `(&(objectclass= objclass) (orclndsobjectguid=*)(orclSourceCreateTimeStamp<= orclodipreconciliationtimestamp)(attr=val3))`

手順 7: 追加構成情報の属性用の同期パラメータの指定

同期プロファイルの「追加構成情報」（orclodipAgentConfigInfo）属性には、コネクタで Oracle Internet Directory と接続ディレクトリの同期化を行うために必要な追加の構成情報が格納されます。6-4 ページの「追加構成情報」で説明されているように、SearchDeltaSize および SkipErrorToSyncNextChange パラメータは任意の接続ディレクトリとともに使用できます。Novell eDirectory と OpenLDAP では、表 22-1 に示すパラメータを使用して追加構成情報を指定することもできます。

表 22-1「追加構成情報」属性用の Novell eDirectory と OpenLDAP の同期パラメータ

パラメータ	説明
AttributeType	UniqueAttribute パラメータのタイプを示します。このパラメータには、Novell eDirectory の場合は Binary 値、OpenLDAP の場合は nonBinary 値を指定します。このパラメータは、マッピング・ファイルに定義されている属性に対応する Oracle Internet Directory の属性を取得するために使用します。
CheckAllEntries	Novell eDirectory または OpenLDAP の削除済エントリを Oracle Internet Directory と同期化する方法を決定します。このパラメータに true 値を指定すると、Oracle Directory Integration Platform では、Oracle Internet Directory のエントリと Novell eDirectory または OpenLDAP との間で線形比較して削除済エントリを識別します。エントリが Novell eDirectory または OpenLDAP に存在しない場合、そのエントリは Oracle Internet Directory から削除されます。このパラメータに false 値を指定すると、接続ディレクトリのエントリ数と Oracle Internet Directory のエントリ数の差によって削除済エントリは同期化されます。削除済エントリ数が 0 以下の場合、同期化する削除済エントリはありません。しかし、削除済エントリ数が 1 以上の場合は、Oracle Directory Integration Platform は Oracle Internet Directory の各エントリを Novell eDirectory または OpenLDAP と比較して同期化する削除済エントリを識別します。Oracle Directory Integration Platform では、接続ディレクトリのエントリ数と Oracle Internet Directory のエントリ数の差と同じ数の削除済エントリを検出するまでエントリの比較を続けます。パフォーマンスを向上させるには、このパラメータに false 値を指定します。
ReduceFilterTimeInSeconds	Oracle Internet Directory を実行しているコンピュータと Novell eDirectory を実行しているコンピュータの間の時間差を指定します。Novell eDirectory のコンピュータ上の時間が Oracle Internet Directory のコンピュータの時間より早い場合、Oracle Internet Directory と Novell eDirectory 間の同期が正しく機能しないため、このパラメータが必要になります。このパラメータには、2 つのコンピュータ間の時間差と等しい値を秒単位で指定します。デフォルト値は 0 です。
UniqueAttribute	エントリの検索に使用できる Novell eDirectory または OpenLDAP の一意の属性を指定します。このパラメータには、Novell eDirectory の場合は GUID 値、OpenLDAP の場合は entryuuid 値を指定します。

手順 8: パスワードを同期化するための OpenLDAP コネクタの構成

Oracle Directory Integration Platform では、ディレクトリが SSL サーバー側認証を実行している場合にかぎり、Oracle Internet Directory から Novell eDirectory または OpenLDAP にパスワードの変更を同期化できます。Novell eDirectory から Oracle Internet Directory には、パスワードを同期化できません。しかし、OpenLDAP から Oracle Internet Directory には、次のタスクを実行するとパスワードを同期化できます。

- パスワードの同期を有効にするマッピング・ルールの追加。たとえば、次のようになります。

  ```
  userpassword: : : inetorgperson: userpassword: person
  ```

- Oracle ディレクトリ・サーバーでのパスワード・ポリシーおよびパスワードの可逆暗号化の有効化。これを行うには、1 の値を、`cn=PwdPolicyEntry,cn=common,cn=products,cn=oraclecontext,`*`DN_of_realm`* エントリの `orclPwdPolicyEnable` 属性と `orclpwdEncryptionEnable` 属性に指定します。そのためには、Oracle Directory Manager を使用するか、`ldapmodify` を使用して次の内容の LDIF ファイルをアップロードします。

  ```
  dn:cn=PwdPolicyEntry,cn=common,cn=products,cn=oraclecontext,DN_of_realm.
  changetype: modify
  replace: orclpwdpolicyenable
  orclpwdpolicyenable: 1
  -
  replace: orclpwdencryptionenable
  orclpwdencryptionenable: 1
  ```

  関連資料 :

  - 18-11 ページの「SSL モードでの同期用サード・パーティ・ディレクトリ・コネクタの構成」
  - マッピング・ルールを追加する方法は、6-5 ページの「マッピング・ルールの構成」を参照してください。
  - 可逆暗号化の有効化の詳細は、『Oracle Internet Directory 管理者ガイド』のパスワード・ベリファイアのディレクトリ格納に関する章を参照してください。

手順 9: SSL モードでの同期

18-11 ページの「SSL モードでの同期用サード・パーティ・ディレクトリ・コネクタの構成」の指示に従い、SSL モードでの同期用に Novell eDirectory または OpenLDAP コネクタを構成します。

手順 10: Novell eDirectory または OpenLDAP 外部認証プラグインの構成

18-13 ページの「外部認証プラグインの構成」の指示に従い、Novell eDirectory または OpenLDAP 外部認証プラグインを構成します。

手順 11: 構成後タスクおよび管理タスクの実行

構成後タスクおよび継続的な管理タスクの詳細は、第 23 章「サード・パーティ・ディレクトリとの統合の管理」を参照してください。

23

サード・パーティ・ディレクトリとの統合の管理

この章では、構成後タスクおよび継続的な管理タスクについて説明します。内容は次のとおりです。

- サード・パーティ・ディレクトリでの構成後のタスク
- サード・パーティ・ディレクトリとの統合の一般的な管理

サード・パーティ・ディレクトリでの構成後のタスク

構成の完了後、次のタスクを実行します。

1. 一方のディレクトリから他方のディレクトリに、必要に応じてデータを移行します。詳細は、23-3 ページの「ディレクトリ間でのデータのブートストラップ」を参照してください。
2. Directory Integration アシスタントを使用して次のコマンドを入力し、同期プロファイルを有効にします。

   ```
   $ORACLE_HOME/bin/dipassistant modifyprofile
   [-h host name] [-p port_number] [-D bind_DN] [-w password]
   -profile profile_name_in_OID odip.profile.status=ENABLE
   ```

3. プロファイルの構成設定に対応する構成設定を使用して、Oracle Directory Integration Server を起動します。4-8 ページの「Oracle Directory Integration Platform の起動、停止および再起動」を参照してください。

サード・パーティ・ディレクトリとの統合の一般的な管理

管理タスクには一般に次のものがあります。

- 同期プロファイルおよびマッピング・ルールの管理
  - 新しいプロファイルの作成。複数ドメイン環境で追加のドメイン・コントローラと同期化する必要がある場合は、新しいプロファイルを作成します。

    新しいプロファイルは、既存のプロファイルをテンプレートとして使用することで作成できます。これには、Directory Integration アシスタント（`dipassistant`）ユーティリティの `createlike` コマンドを使用します。
  - プロファイルの構成（属性）の変更。
  - プロファイルによるメンテナンス許可の無効化およびその再有効化。プロファイルを無効にすると、そのプロファイルに関連する同期が停止されます。
- マッピング・ルールの管理
  - 新しいルールの作成（追加の属性を同期化する必要がある場合）
  - 既存ルールの変更（属性を同期化する方法を変更する必要がある場合）
  - 不要なルールの削除またはコメント化（特定の属性を同期化する必要がない場合）
- アクセス制御の管理
- Oracle ディレクトリ・サーバーおよび Oracle Directory Integration Server の起動と停止

この項の内容は次のとおりです。

- ディレクトリ間でのデータのブートストラップ
- サード・パーティ・ディレクトリ外部認証プラグインの管理

関連資料：

- プロファイル、マッピング・ルールおよびアクセス制御の管理方法は、18-7 ページの「拡張統合オプションの構成」を参照してください。
- サーバーの起動方法および停止方法と Directory Integration アシスタント（`dipassistant`）ユーティリティの使用方法は、『Oracle Identity Management ユーザー・リファレンス』を参照してください。
- Identity Management Grid Control Plug-in を使用したサード・パーティ・ディレクトリとの統合の管理方法は、『Oracle Identity Management インフラストラクチャ管理者ガイド』を参照してください。

ディレクトリ間でのデータのブートストラップ

ブートストラップは、データの移行と呼ばれることがあります。データをブートストラップするには、サード・パーティ・ディレクトリのコネクタおよびプラグインの構成完了後に次の手順を実行します。

1. 移行するデータを識別します。ディレクトリ内のデータ全体またはサブセットのみの移行を選択できます。
2. 次のコマンドを使用して、インポートおよびエクスポート同期プロファイルを無効にします。

   ```
   $ORACLE_HOME/bin/dipassistant modifyprofile -host myhost -port myport
   -file import.profile -dn bind_DN -passwd password_of_bind_DN
   -profile profile_name odip.profile.status=DISABLE
   ```

3. `-bootstrap` オプションを指定した Directory Integration アシスタント（`dipassistant`）を使用して、ディレクトリ間でデータをブートストラップします。ブートストラップの詳細は、第 8 章「Oracle Directory Integration Platform におけるディレクトリのブートストラップ」を参照してください。

   ブートストラップが完了すると、Directory Integration アシスタント（`dipassistant`）によって同期プロファイルのプロファイル・ステータス属性が適切に更新されます。
4. LDIF ファイルベースのブートストラップを使用した場合、Directory Integration アシスタント（`dipassistant`）を使用して、次のように `lastchangekey` 値を初期化します。

   ```
   $ORACLE_HOME/bin/dipassistant modifyprofile -updlcn
   ```

   この `lastchangekey` 属性は、ブートストラップを開始する前に、ソース・ディレクトリの最終変更番号の値に設定する必要があります。
5. 双方向同期が必要な場合は、エクスポート・プロファイルを有効にし、Oracle ディレクトリ・サーバーで変更ロギング・オプションが有効になっていることを確認します。変更ロギングは、Oracle Internet Directory の起動時に `-l` オプションによって制御されます。デフォルトでは、変更ロギングが有効なことを意味する `TRUE` に設定されています。`FALSE` に設定されている場合は、OID 制御ユーティリティを使用して Oracle ディレクトリ・サーバーを停止した後、変更ログを有効にしてサーバーを再起動します。

サード・パーティ・ディレクトリ外部認証プラグインの管理

この項では、サード・パーティの外部認証プラグインを削除、無効化および再有効化する方法について説明します。

サード・パーティ・ディレクトリ外部認証プラグインの削除

サード・パーティの外部認証プラグインを削除するには、次のコマンドを入力します。

```
ldapdelete -h host -p port -D cn=orcladmin -w password
"cn=adwhencompare,cn=plugin,cn=subconfigsubentry"

ldapdelete -h host -p port -D cn=orcladmin -w password
"cn=adwhenbind,cn=plugin,cn=subconfigsubentry"
```

サード・パーティの外部認証プラグインの無効化

サード・パーティの外部認証プラグインを無効にするには、次のようにします。

1. 次の内容で、LDIF ファイルを作成します。

```
dn: cn=adwhencompare,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclpluginenable
orclpluginenable: 0

dn: cn=adwhenbind,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclpluginenable
orclpluginenable: 0
```

2. 次のように、`ldapmodify` コマンドを使用して LDIF ファイルをロードします。

```
ldapmodify -h host -p port -D cn=orcladmin -w password -f fileName
```

サード・パーティの外部認証プラグインの再有効化

サード・パーティの外部認証プラグインを再度有効にするには、次の 2 つのコマンドを使用します。

1. 次の内容で、LDIF ファイルを作成します。

```
dn: cn=adwhencompare,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclpluginenable
orclpluginenable: 1

dn: cn=adwhenbind,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclpluginenable
orclpluginenable: 1
```

2. 次のように、`ldapmodify` コマンドを使用して LDIF ファイルをロードします。

```
ldapmodify -h host -p port -D cn=orcladmin -w password -f fileName
```

第 VI 部

付録

第 VI 部は、次の各付録で構成されています。

- 付録 A「Oracle Directory Integration Server 管理ツールの要素」
- 付録 B「事例 : Oracle Directory Integration Platform の配置」
- 付録 C「Oracle Directory Integration Platform のトラブルシューティング」

A

Oracle Directory Integration Server 管理ツールの要素

この付録では、Oracle Directory Integration Server 管理ツールのタブ・ページと対応するフィールドについて説明します。内容は次のとおりです。

- ディレクトリ・サーバーに接続するためのウィンドウとフィールド
- サーバー情報を表示するためのウィンドウとフィールド
- ディレクトリ統合プロファイルを登録および編集するためのウィンドウとフィールド
- Microsoft Active Directory コネクタを構成するためのウィンドウとフィールド

ディレクトリ・サーバーに接続するためのウィンドウとフィールド

この項では、ディレクトリ・サーバーへの接続に使用するウィンドウとフィールドについて説明します。

資格証明

表 A-1 に、「資格証明」タブ・ページのフィールドを示します。

表 A-1「資格証明」タブ・ページのフィールド

フィールド名	説明
ユーザー	ユーザー名のデフォルト値は dipadmin です。これは、エントリが cn=dipadmin,cn=odi,cn=oracle internet directory であるユーザーのニックネームです。 LDAP のコマンドライン・ツールを使用してユーザーのエントリをすでに設定している場合は、次の 2 つの方法いずれかでそのユーザーのエントリを入力できます。 ■ 「**ユーザー**」フィールドの右側のボタンを使用し、そのエントリを参照して選択します。 ■ そのユーザーのエントリに対する**識別名**を、次の例のように正しい書式で入力します。 cn=Susie Brown,ou=HR,o=acme,c=us 正しい権限を持っていない場合は、ツールへのアクセスが拒否されます。このツールを使用するには、cn=dipadmingrp,cn=dipadmin,cn=directory integration platform,cn=products,cn=oraclecontext グループのメンバーであることが必要です。
パスワード	スーパー・ユーザーでログインし、インストール時にスーパー・ユーザー用のパスワードを指定している場合は、そのパスワードを「**パスワード**」フィールドに入力します。パスワードを指定していない場合は、デフォルトのパスワード welcome を入力します。Oracle Directory Integration Server 管理にログインし、ディレクトリ・サーバーに接続した後、ディレクトリを保護するためにこのパスワードを変更してください。 匿名でログインする場合は、「**パスワード**」フィールドを空白のままにします。 特定のディレクトリ・ユーザーとしてログインする場合は、対応するパスワードを入力してください。 **関連資料 :** パスワードの変更方法については、『Oracle Internet Directory 管理者ガイド』のディレクトリ・サーバー管理に関する章を参照してください。

表 A-1「資格証明」タブ・ページのフィールド（続き）

フィールド名	説明
サーバー	初めてログインすると、Oracle Directory Integration Server 管理ツールにより、Oracle Application Server インストール時に指定したデフォルトの Oracle ディレクトリ・サーバーの名前が表示されます。 ディレクトリ・サーバーの情報は、最初に $*ORACLE_HOME*/config ディレクトリにある `ias.properties` ファイルの `oidhost` パラメータの値をチェックして取得されます。パラメータに値が指定されていない場合は、`osdadmin.ini` ファイルの `host` パラメータの値をチェックします。そこにも値が指定されていない場合は、「**サーバー**」フィールドの値 `localhost` が表示されます。 別のホスト上のサーバーに接続する場合の手順は、次のとおりです。 1. 「サーバー」リストの右側のボタンをクリックします。使用可能なサーバーのリストが、「ディレクトリ・サーバーの選択」ダイアログ・ボックスに表示されます。 2. サーバーを選択します。 3. 「**OK**」をクリックします。 ディレクトリ・サーバーをリストに追加する手順は、次のとおりです。 1. 「ディレクトリ・サーバーの選択」ダイアログ・ボックスで、「**追加**」をクリックします。「ディレクトリ・サーバーの接続」ダイアログ・ボックスが表示されます。 2. 「**サーバー**」フィールドに、追加するディレクトリ・サーバーの名前を入力します。 3. 「**ポート**」フィールドに、追加するサーバーのポート番号を入力します。 4. 「**OK**」をクリックします。追加したディレクトリが、「ディレクトリ・サーバーの選択」ダイアログ・ボックスのリストに表示されます。 リストにあるディレクトリ・サーバーを変更する手順は、次のとおりです。 1. 変更するディレクトリ・サーバーを選択します。 2. 「**編集**」をクリックします。「ディレクトリ・サーバーの接続」ダイアログ・ボックスが表示されます。 3. 「**サーバー**」フィールドおよび「**ポート**」フィールドを変更して、「**OK**」をクリックします。サーバーに対する変更が、「ディレクトリ・サーバーの選択」ダイアログ・ボックスのリストに表示されます。
ポート	初めてログインすると、Oracle Directory Integration Server 管理ツールにより、Oracle Application Server インストール時に指定したデフォルトの Oracle ディレクトリ・サーバー・ポートの名前が表示されます。この情報は、`ias.properties` ファイルの `oidport` パラメータの値をチェックすることで取得されます。パラメータに値が指定されていない場合は、`osdadmin.ini` ファイルの `port` パラメータの値をチェックします。そこにも値が指定されていない場合は、`389` の値が表示されます。 このポート番号を変更する手順は、次のとおりです。 1. 「**サーバー**」フィールドの右側のボタンをクリックします。 2. 「ディレクトリ・サーバーの選択」ダイアログ・ボックスで、ディレクトリ・サーバーを選択します。 3. 「**編集**」をクリックします。「ディレクトリ・サーバーの接続」ダイアログ・ボックスが表示されます。 4. 「ディレクトリ・サーバーの接続」ダイアログ・ボックスの「**ポート**」フィールドにポート番号を入力して、「**OK**」をクリックします。

SSL

表 A-2 に、「SSL」タブ・ページのフィールドを示します。

表 A-2「SSL」タブ・ページのフィールド

フィールド名	説明
SSL パスワード	ユーザーのウォレットをオープンするパスワード。
SSL 認証	認証レベルを次の中から選択します。 ■ SSL 認証なし : クライアントとサーバーのいずれも、相手に対して自己認証を行いません。証明書の送信または交換は行われません。「資格証明」タブの「SSL 使用可能」チェック・ボックスを選択して、このオプションを選択した場合は、SSL 暗号化 / 復号化のみが使用されます。 ■ SSL クライアントとサーバー認証 : 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・サーバーのみがクライアントに対してサーバー認証を行います。

エントリ管理の構成

このウィンドウを使用して、次の指定を行います。

- Oracle Directory Integration Server 管理ツールで 1 回の検索結果に表示されるエントリ数
- 検索の期間

このツールまたはディレクトリ・サーバー、あるいはその両方でこれらの構成を行えます。

ツールとディレクトリ・サーバーの両方で構成を行い、その 2 つの構成が一致しない場合は、Oracle Internet Directory によりこの不一致が次のように解決されます。

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

アクセス制御ポリシー管理の構成

このタブ・ページを使用して、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。

ディレクトリ・サーバーの接続

このダイアログ・ボックスを使用して、「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ディレクトリ・サーバーを追加します。

識別名 (DN) パスの選択 : ツリー表示

このダイアログ・ボックスを使用して、ディレクトリ情報ツリー（DIT）のエントリの階層を表示します。

トップ・レベルのエントリの横にあるプラス記号（+）をクリックし、ツリーを展開します。プラス記号をクリックしてツリーを展開し、従属エントリを表示します。プラス記号をクリックしてエントリを展開すると、そのプラス記号はマイナス記号（-）になります。

注意 : 従属エントリがないエントリがプラス記号付きで表示される場合がありますが、そのプラス記号はクリックすると消えます。横にプラス記号もマイナス記号もないエントリは、ツリーのリーフ・ノードです。

必要なエントリを選択し、「**OK**」をクリックします。このエントリは、「検索」ウィンドウの「**検索のルート**」フィールドに表示されます。

ディレクトリ・サーバーの選択

このダイアログ・ボックスには、過去に接続したすべてのディレクトリ・サーバーのリストが表示されます。このリストからディレクトリ・サーバーを選択すれば、そのサーバーに対する接続、削除、編集の他、サーバーを別の管理接続用のテンプレートとして使用することもできます。このリストにサーバーを追加するには、「**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。

サーバー情報を表示するためのウィンドウとフィールド

この項で説明するウィンドウとフィールドは、アクティブ・サーバー・プロセスに関する情報を提供します。

アクティブ・プロセス

このウィンドウには、Microsoft Active Directory 統合サーバー・インスタンスのリストが表示されます。読みやすい形式で構成設定エントリを表示するには、エントリの 1 つを選択し、「**プロパティの表示**」をクリックします。パラメータを変更するには、ナビゲータ・ペインで構成設定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。

構成設定 : 統合プロファイル

このダイアログ・ボックスには、構成設定エントリに関連付けられたディレクトリ統合プロファイルの情報が表示されます。「統合プロファイル」タブ・ページが空の場合、この構成設定エントリに関連付けられたディレクトリ統合プロファイルはありません。このダイアログ・ボックスの「統合プロファイル」タブ・ページの列は、次のとおりです。

- プロファイル名 : このディレクトリ統合プロファイルの識別名の相対識別名コンポーネント。
- 同期モード : プロファイルがインポートまたはエクスポートのどちらに使用されるかを指定します。インポート操作は、変更を接続ディレクトリから Oracle Internet Directory に取り込みます。エクスポート操作は、Oracle Internet Directory から接続ディレクトリに変更を送信します。
- プロファイルのステータス : プロファイルが使用可能か使用禁止かを指定します。

ディレクトリ統合プロファイルを登録および編集するためのウィンドウとフィールド

この項では、ディレクトリ統合プロファイルを登録および編集する際に使用するウィンドウとフィールドについて説明します。

統合コネクタ

このダイアログ・ボックスを使用して、ディレクトリ統合プロファイルを作成または変更します。次の操作が可能です。

- 既存のものをコピーして統合プロファイルを作成します。これには、コピーするディレクトリ統合プロファイルを選択し、「**類似項目の作成**」をクリックします。「統合プロファイル」ダイアログ・ボックスに「一般」タブ・ページが表示されます。
- 既存のものをコピーせずに統合プロファイルを作成します。これには、「**新規作成**」をクリックします。「統合プロファイル」ダイアログ・ボックスに「一般」タブ・ページが表示されます。
- 統合プロファイルを編集します。これには、プロファイルを選択し、「**編集**」をクリックします。その結果「一般」タブ・ページが表示されます。

一般

表 A-3 に、「一般」タブ・ページのフィールドを示します。

表 A-3「一般」タブ・ページのフィールド

フィールド名	説明
プロファイル名	プロファイルの名前を指定します。入力した名前は、この統合プロファイルの識別名の相対識別名コンポーネントとして使用されます。たとえば、プロファイル名 `MSAccess` を指定して、`orclodipagentname=MSAccess,cn=subscriber profile, cn=changelog subscriber, cn=oracle internet directory` という名前の統合プロファイルを作成します。 このフィールドは必須です。このフィールドにデフォルトの設定はありません。
プロファイルのバージョン	このプロファイルが作成された Oracle Directory Integration Platform のバージョン。
同期モード	インポート操作かエクスポート操作かを指定します。インポート操作は、変更を接続ディレクトリから Oracle Internet Directory に取り込みます。エクスポート操作は、Oracle Internet Directory から接続ディレクトリに変更を送信します。 このフィールドは必須です。デフォルトは `IMPORT` です。
プロファイルのステータス	プロファイルが使用可能か使用禁止かを指定します。 このフィールドは必須です。デフォルトは `ENABLE` です。
プロファイルのパスワード	Oracle Directory Integration Server がプロファイルのかわりに Oracle Internet Directory にバインドするときに使用するパスワードを指定します。このフィールドは必須で、デフォルトは `welcome` です。
スケジューリングの間隔	接続ディレクトリと Oracle Internet Directory の同期の、試行間隔の秒数を指定します。 このフィールドは必須です。デフォルトは `60` です。

表 A-3「一般」タブ・ページのフィールド（続き）

フィールド名	説明
最大再試行回数	Directory Integration Server が同期を無効化するまでに同期を試行する回数の、最大数を指定します。このフィールドは必須です。 デフォルトは 5 です。最初の再試行は最初の失敗の 1 分後に行われます。2 回目の再試行は 2 回目の失敗の 2 分後に、後続の再試行は *n* 回目の失敗の *n* 分後に行われます。
デバッグ・レベル	デバッグのロギング・レベルを、『Oracle Internet Directory 管理者ガイド』で説明されているように指定します。

実行

表 A-4 に、「実行」タブ・ページのフィールドを示します。

表 A-4「実行」タブ・ページのフィールド

フィールド名	説明

エージェントの実行コマンド	Oracle Directory Integration Server がエージェントを実行するために使用するエージェント実行可能ファイルの名前と引数を指定します。
	このフィールドはオプションです。このフィールドにデフォルトの設定はありません。
	一般的な実行コマンドは、次の形式です。
	`odicmd user=%orclodipcondirAccessAccount pass=%orclodipcondiraccesspassword`
	`odicmd` は、実行するコマンドです（パスに指定されている場合に使用可能、またはフルパス名で指定）。
	`user=%orclodipcondirAccessAccount pass=%orclodipcondiraccesspassword`
	はコマンドライン引数です。ユーザー（user）に渡される値は `orclodipcondiraccessaccount` 属性から、パス（pass）に渡される値は `orclodipcondiraccesspassword` 属性から導出されます。
	一般的な例は、Oracle Human Resources エージェントにあります。

接続されたディレクトリ・アカウント	コネクタ・エージェントが接続ディレクトリにアクセスするために使用するアカウントを指定します。たとえば、接続ディレクトリがデータベースの場合、アカウントは `Scott` などになります。接続ディレクトリが別の LDAP 準拠ディレクトリの場合は、アカウントは `cn=Directory Manager` などになります。 このフィールドはオプションです。このフィールドにデフォルトの設定はありません。
接続されたディレクトリ・アカウントのパスワード	コネクタまたはエージェントが接続ディレクトリにアクセスするときに使用するパスワードを指定します。このフィールドはオプションです。このフィールドにデフォルトの設定はありません。
追加構成情報	このフィールドには、Oracle Directory Integration Server がエージェントに渡す追加情報が表示されます。このフィールドは Oracle Directory Integration Server 管理ツールで変更できません。変更するには、Directory Integration アシスタント（`dipassistant`）を使用します。

表 A-4「実行」タブ・ページのフィールド（続き）

フィールド名	説明
接続されたディレクトリ URL	接続ディレクトリへの接続に必要な接続情報。このパラメータは、ホスト名とポート番号を `host:port:sslmode` の形式で示します。 SSL を使用して接続するには、*`host:port`*:1 を入力します。 ディレクトリに接続するための証明書がウォレットに格納され、その場所が `odi.properties` ファイルに指定されていることを確認します。 **注意 :** SSL を使用して Sun Java System Directory に接続するには、サーバー証明書をウォレットにロードする必要があります。 **関連資料 :**『Oracle Advanced Security 管理者ガイド』の Oracle Wallet Manager に関する章
インタフェース・タイプ	インポート・ファイルまたはエクスポート・ファイルが使用する形式。オプションは、`DB`、`LDAP`、`LDIF` および `TAGGED` です。このフィールドはオプションです。デフォルトは `TAGGED` です。

マッピング

表 A-5 に、「マッピング」タブ・ページのフィールドを示します。

表 A-5「マッピング」タブ・ページのフィールド

フィールド名	説明
マッピング・ルール	このフィールドには、接続ディレクトリと Oracle Internet Directory の間でデータを変換するためのマッピング・ルールが表示されます。このフィールドにデフォルトの設定はありません。 **注意 :** マッピング・ルール・ファイルは、Oracle Directory Integration Server 管理ツールでは編集できません。ファイルのマッピング・ルールは手動で編集し、Oracle Directory Integration Platform を使用してプロファイルにアップロードします。
接続されたディレクトリ一致フィルタ	接続ディレクトリのエントリを一意に識別する属性を指定します。
OID 一致フィルタ	Oracle Internet Directory のレコードを一意に識別する属性を指定します。この属性は、Oracle Internet Directory と接続ディレクトリを同期化するためのキーとして使用されます。このフィールドはオプションです。

ステータス

表 A-6 に、「ステータス」タブ・ページのフィールドを示します。

表 A-6「ステータス」タブ・ページのフィールド

フィールド名	説明
OID 前回適用された変更番号（インポート操作のみ）	エクスポート操作に、接続ディレクトリに適用された Oracle Internet Directory からの最後の変更の識別子を指定します。デフォルトは 0 です。エンド・ユーザーはこのフィールドを必要に応じて意識的に変更できます。プロファイルは、使用禁止モードにしてください。番号が増加した場合、元の値と新しい値の間に番号付けされた変更ログ・エントリは適用されません。
最終実行時間	エージェントが実行された最新の絶対日時。デフォルトは、コネクタの作成日時です。このフィールドを変更すると誤解を招く恐れがあります。
最終正常実行時間	エージェントの実行が成功した最新の絶対日時。デフォルトは、コネクタの作成日時です。このフィールドを変更すると誤解を招く恐れがあります。
同期ステータス	同期の成功または失敗。
同期エラー	最後のエラー・メッセージ。このフィールドは変更できません。このフィールドにデフォルトの設定はありません。
前回適用された変更番号（エクスポート操作のみ）	接続ディレクトリに正常に適用された最新の変更ログ・エントリの数。エンド・ユーザーはこのフィールドを必要に応じて意識的に変更できます。プロファイルは、使用禁止モードにしてください。番号が増加した場合、元の値と新しい値の間に番号付けされた変更ログ・エントリは適用されません。

Microsoft Active Directory コネクタを構成するためのウィンドウとフィールド

この項では、Microsoft Active Directory コネクタの構成時に使用するウィンドウとフィールドについて説明します。

Microsoft Active Directory コネクタ Express 同期設定

このタブ・ページを使用して、Microsoft Active Directory コネクタの Express 構成を実行します。この構成は、Oracle Application Server のデフォルトのインストールに基づいています。その他のタイプのディレクトリ統合プロファイルの作成には、この方法を使用しないでください。

表 A-7 に、Microsoft Active Directory コネクタ Express 同期設定タブ・ページのフィールドを示します。

表 A-7 Microsoft Active Directory コネクタ Express 同期設定タブ・ページのフィールド

フィールド名	説明
Microsoft Active Directory ホスト	Microsoft Active Directory がインストールされているホスト。
Microsoft Active Directory ポート	Microsoft Active Directory インストールのポート番号。
アカウント名	Microsoft Active Directory にログインするためのユーザー名。
アカウント・パスワード	Microsoft Active Directory にログインするためのパスワード。
コネクタ名	ディレクトリ統合プロファイルの名前。
インポート・プロファイル名	読取り専用。値はコネクタのプロファイルから導出されます。
エクスポート・プロファイル名	読取り専用。値はコネクタのプロファイルから導出されます。
構成設定	デフォルトは 1 です。別の構成設定を指定すると、その構成設定が自動的に作成され、このプロファイルに関連付けられます。

アクセス制御ポリシーの指定を選択することもできます。

B

事例 : Oracle Directory Integration Platform の配置

この付録では、MyCompany という企業内の様々なアプリケーションが Oracle Directory Integration Platform によって統合されている配置例を説明します。

内容は次のとおりです。

企業 MyCompany 内のコンポーネント

この仮想の企業には、次のコンポーネントがあります。

- Oracle Human Resources システム。すべての従業員と契約社員が管理されています。
- Sun Java System Directory。特定のアプリケーションで使用されています。
- OracleAS Portal。全従業員のイントラネット・ポータルとして使用されています。
- Oracle Collaboration Suite。社内の全ドキュメントのドキュメント・リポジトリとして使用されています。

企業 MyCompany の要件

企業 MyCompany の要件は次のとおりです。

- すべての従業員と契約社員を Oracle Human Resources で作成すること。作成後の情報は、企業内のすべてのアプリケーションが Oracle Internet Directory を介して共有する必要があります。
- シングル・サインオン・サービスなど、企業内のすべてのアプリケーションが、Oracle Human Resources で作成された従業員を認識できること。
- ユーザー・プロパティの変更が発生したときには、影響を受けるすべてのアプリケーションにその変更が通知されること。
- Oracle Human Resources でユーザーが期限切れのときは、そのユーザーのすべてのアクセス権限が取り消されること。

企業 MyCompany 内の全体的な配置

図 B-1 は、様々なコンポーネントとそれらの相互関係を示しています。

図 B-1 MyCompany での Oracle Directory Integration Platform の配置例

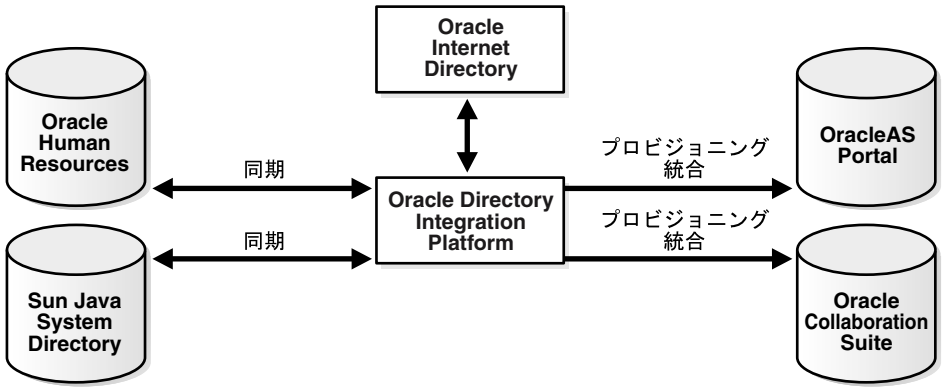


図 B-1 の例では、次のようになっています。

- Oracle Internet Directory は、企業の全アプリケーションの中央ユーザー・リポジトリです。
- Oracle Human Resources は、すべてのユーザー関連情報の基礎となります。Oracle Directory Synchronization Service を使用して Oracle Internet Directory と同期化されます。
- Sun Java System Directory は、すでに企業内に配置されており、Oracle Directory Synchronization Service を使用して Oracle Internet Directory と同期化されます。
- OracleAS Portal は、Oracle Directory Integration Platform Service を使用して、Oracle Internet Directory 内の変更に関する通知を受けます。

- Oracle Collaboration Suite は、Oracle Directory Integration Platform Service を使用して、Oracle Internet Directory 内の変更に関する通知を受けます。

企業 MyCompany でのユーザーの作成とプロビジョニング

この例では、MyCompany という企業が、すべてのユーザーを Oracle Human Resources で作成する必要があるとします。Oracle Directory Integration Platform は、企業内のその他のすべてのリポジトリに新規ユーザー・レコードを伝播する必要があります。

図 B-2 は、Oracle Directory Integration Platform によりこのタスクがどのように実行されるかを示しています。

図 B-2 ユーザーの作成とプロビジョニング

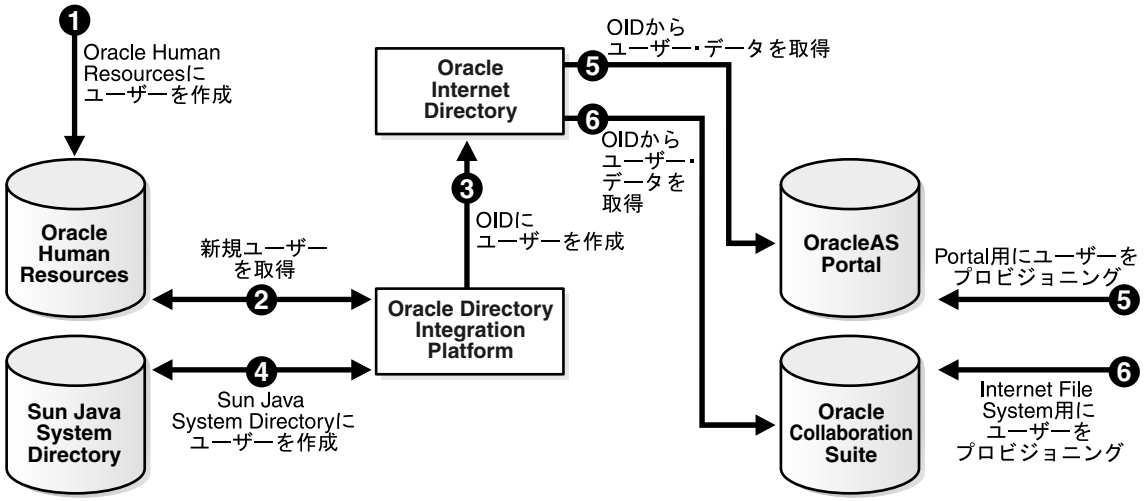


図 B-2 は、Oracle Human Resources での新規ユーザーの作成を示しています。この作成によって、そのユーザーのエントリが Oracle Internet Directory と Sun Java System Directory に作成されます。また、企業内に配置されている 2 つのアプリケーション、つまり OracleAS Portal および Oracle Collaboration Suite にアクセスするユーザーのプロビジョニング・プロセスも示しています。ユーザーの作成とプロビジョニングは、次の方法で行われます。

1. Oracle Human Resources 管理者は、ユーザーを Oracle Human Resources データベースに作成します。
2. Oracle Directory Integration Platform は、Oracle Directory Synchronization Service を介して新規ユーザーの作成を検出します。
3. Oracle Directory Integration Platform は、Oracle Directory Synchronization Service を介してユーザーのエントリを Oracle Internet Directory に作成します。
4. Oracle Directory Integration Platform は、Oracle Directory Synchronization Service を介して Sun Java System Directory にエントリを作成します。
5. このユーザー・エントリは Oracle Internet Directory で使用可能なため、OracleAS Portal の管理者は、OracleAS Portal のサービスを使用するユーザーをプロビジョニングできます。このタスクの実行時、OracleAS Portal ソフトウェアは、Oracle Internet Directory からユーザー情報を自動的に取得します。
6. Oracle Collaboration Suite の管理者も、同様のプロセスを使用して、Oracle Collaboration Suite のサービスを使用するユーザーをプロビジョニングします。

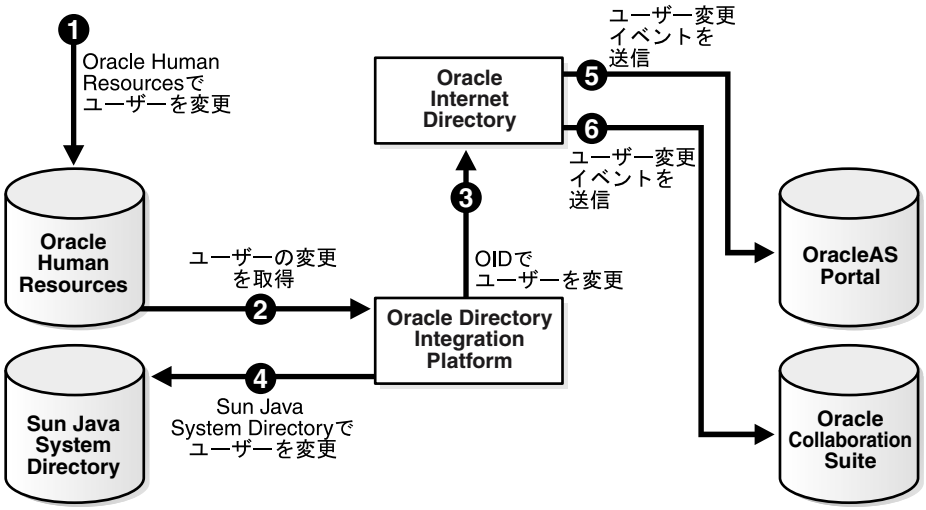
Oracle Directory Integration Platform は、新規ユーザーについて OracleAS Portal または Oracle Collaboration Suite に直接通知しないことに注意してください。これは、Oracle Human Resources で作成されたすべてのユーザーが、すべてのサービスへのアクセスを必要とすると

はかぎらないためです。この場合の配置では、これらのサービスを使用するユーザーを、手順 5 と 6 に従って、明示的にプロビジョニングする必要があります。

企業 MyCompany でのユーザー・プロパティの変更

この例の企業 MyCompany では、ユーザー・プロパティに対するあらゆる変更が、その変更に関連するすべてのコンポーネントに伝達される必要があります。図 B-3 は、この要件を満たすために Oracle Directory Integration Platform が実行するアクションを示しています。

図 B-3 ユーザー・プロパティの変更



このプロセスは、次のとおりです。

1. ユーザーは、最初に Oracle Human Resources で変更されます。
2. Oracle Directory Integration Platform は、Oracle Directory Synchronization Service を介してこれらの変更を取得します。
3. Oracle Directory Integration Platform は、Oracle Internet Directory 内で対応するユーザーを変更します。
4. Oracle Directory Synchronization Service は、Sun Java System Directory 内でユーザーを変更します。
5. Oracle Directory Integration Platform は、Oracle Directory Integration Platform Service を介してユーザー・プロパティの変更を OracleAS Portal に通知します。
6. Oracle Directory Integration Platform は、Oracle Directory Integration Platform Service を介してユーザー・プロパティの同じ変更を Oracle Collaboration Suite に通知します。

企業 MyCompany でのユーザーの削除

この例の企業 MyCompany では、Oracle Human Resources で削除または期限切れになったユーザーは、ディレクトリ・サービスに基づいた企業のすべてのリソースへのアクセスを自動的に拒否される必要があります。

図 B-4 は、ユーザーが削除されたときのイベントの流れを示しています。

図 B-4 企業の Human Resources からのユーザーの削除

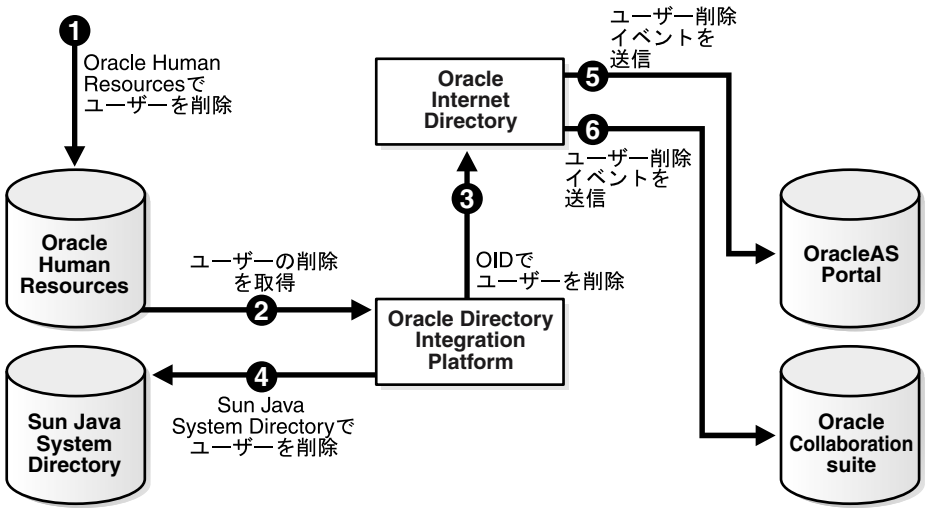


図 B-4 は、Oracle Directory Integration Platform がユーザーの削除を企業内のすべてのシステムに通信するプロセスを示しています。このプロセスは、次のとおりです。

1. ユーザーは、最初に Oracle Human Resources で削除されます。
2. Oracle Directory Integration Platform は、Oracle Directory Synchronization Service を介してこれらの変更を取得します。
3. Oracle Directory Integration Platform は、Oracle Directory Synchronization Service を介して Oracle Internet Directory 内の対応するユーザーを削除します。
4. Oracle Directory Integration Platform は、Oracle Directory Synchronization Service を介して Sun Java System Directory 内でユーザーを削除します。
5. Oracle Directory Integration Platform は、Oracle Directory Integration Platform Service を介してユーザーの削除を OracleAS Portal に通知します。
6. Oracle Directory Integration Platform は、Oracle Directory Integration Platform Service を介してユーザーの削除を Oracle Collaboration Suite に通知します。

すべての手順が終了すると、Oracle Human Resources で削除されたユーザーは、OracleAS Portal や Oracle Collaboration Suite にアクセスできなくなります。

C

Oracle Directory Integration Platform のトラブルシューティング

この付録では、Oracle Directory Integration Platform の使用時に発生する可能性のある一般的な問題とその解決策について説明します。内容は次のとおりです。

関連資料：

- Oracle Technology Network（`http://www.oracle.com/technology/index.html`）で参照可能な Oracle Identity Management の「Oracle by Example」
- 『Oracle Identity Management ユーザー・リファレンス』

Oracle Directory Integration Platform の問題のトラブルシューティング

この項では、Oracle Directory Integration Server の問題を診断するための一般的な方法について説明します。内容は次のとおりです。

インフラストラクチャ・インストール環境の Oracle Directory Integration Platform の診断

Oracle Directory Integration Server が起動後、稼働しているかどうかを確認するには、次の手順に従います。

1. UNIX/Linux の場合、次のコマンドを使用して、`odisrv` プロセスが実行されていることを確認します。

   ```
   ps -ef | grep odisrv
   ```

   Windows オペレーティング・システムの場合、*$ORACLE_HOME*/ldap/log/oidmon.log から `odisrv` プロセスのプロセス ID（PID）の値を取得します。次にタスク マネージャを起動し、「**プロセス**」タブをクリックして、プロセスが実行されていること確認します。

2. Oracle Directory Integration Server が稼働していない場合は、*$ORACLE_HOME*/ldap/log/oidmon.log ファイルを調べ、サーバーが起動しなかった理由を特定します。

3. ログ・ファイルにデータベース関連のエラーが表示されている場合は、次のように対処します。

   a. `ORACLE_`*`SID`* に値が設定されていることを確認します。

   b. `ORACLE_`*`SID`* に指定されている接続文字列が、*$ORACLE_HOME*/network/admin/tnsnames.ora ファイルに指定されていることを確認します。

4. ログ・ファイルに、サーバーの `instance` 番号と `configset` 番号の引数がリストされていることを確認します。値が正しく設定されている場合は、*$ORACLE_HOME*/ldap/log/odisrv_*nn*.log ファイルを調べます。*nn* は起動されたインスタンスの番号です。odisrv_*xx*.log ファイルに登録エラーが示されている場合は、`odisrvreg` ユーティリティを使用して Oracle Directory Integration Platform を再登録します。

5. 前の手順でエラーが見つからない場合は、*$ORACLE_HOME*/ldap/log/odisrv_jvm_*yyy*.log ファイルを調べます。*yyy* は、起動した `odisrv` プロセスのプロセス識別子です。最新のタイムスタンプが含まれているファイルを検索します。

Oracle Directory Integration Platform インストール環境の Oracle Directory Integration Platform の診断

Oracle Directory Integration Server が起動後稼働しているかどうかを確認するには、次の手順に従います。

1. UNIX/Linux の場合、次のコマンドを使用して、odisrv プロセスが実行されていることを確認します。

   ```
   ps -ef | grep odisrv
   ```

   Windows オペレーション・システムの場合、*$ORACLE_HOME*/ldap/log/odisrv_*nn*.log ファイルから odisrv プロセスのプロセス ID（PID）の値を取得します。nn は、起動されたインスタンスの番号です。次に、タスク マネージャを起動し、「**プロセス**」タブをクリックして、そのプロセスが実行されていることを確認します。

2. Oracle Directory Integration Server が稼働していない場合は、odisrv_*xx*.log ファイルを調べます。ファイルに登録エラーが含まれている場合は、odisrvreg ユーティリティを使用して Oracle Directory Integration Server を再登録します。

3. 前の手順でエラーが見つからない場合は、*$ORACLE_HOME*/ldap/log/odisrv_jvm_*yyy*.log ファイルを調べます。*yyy* は、起動した odisrv プロセスのプロセス識別子です。最新のタイムスタンプが含まれているファイルを検索します。

トラブルシューティングのユーティリティ

この項では、同期問題のトラブルシューティングに使用できる oditest ユーティリティと DIP Tester ユーティリティについて説明します。

oditest ユーティリティ

多数のプロファイルが実行されている場合や、特定のプロファイルに対して同期の間隔があまりにも長く設定されている場合は、同期のトラブルシューティングは複雑になる可能性があります。このような場合は、oditest ユーティリティを使用して、次の手順でコネクタの動作をテストできます。

1. 多数のプロファイルが実行されている場合は、Directory Integration アシスタント（dipassistant）を使用して、トラブルシューティングを行うプロファイルを選択して無効にします。実行されているプロファイルが 1 つの場合は、Directory Integration Server を停止します。

2. *$ORACLE_HOME*/bin に移動し、次の構文を使用して oditest ユーティリティを実行します。

   ```
   oditest sync | prov profile_name host=host_of_Oracle_Internet_Directory \
   port=port_for_Oracle_Internet_Directory binddn=bind_DN \
   bindpass=password_for_the_bind_DN sslauth=0 debug=63
   ```

   次の例は、Sun Java System Directory 同期プロファイルで oditest ユーティリティを実行する方法を示しています。

   ```
   oditest sync IplanetImport host=my-oidhost port=3060 binddn=cn=orcladmin
   bindpass=welcome1 sslauth=0 debug=63
   ```

   関連項目： 監査ログとトレース・ファイルの確認方法の詳細は、4-13 ページの「ログ・ファイルの検索」を参照してください。

DIP Tester ユーティリティ

DIP Tester ユーティリティは、Oracle Directory Integration Platform コネクタと同期する Oracle Internet Directory 実装の構成、テストおよびデバッグに役立つプラットフォームに依存しないスタンドアロン Java アプリケーションです。このユーティリティでは、プロファイルの変更に Directory Integration アシスタント（`dipassistant`）を使用し、多くの内部操作に標準の LDAP ツール（`ldapadd`、`ldapmodify`、`ldapdelete` および `ldapsearch`）を使用します。DIP Tester ユーティリティは、Solaris、Linux および Windows プラットフォーム用の Oracle Application Server 10*g*（10.1.4.0.1）において、Oracle Internet Directory 10*g*（9.0.4）上でテストされています。DIP Tester は、Oracle Technology Network（`http://www.oracle.com/technology/index.html`）からダウンロードできます。ダウンロードの内容には、グラフィカル・ユーザー・インタフェース（GUI）版とコマンドライン版の DIP Tester ユーティリティが含まれます。どちらのバージョンも、単一のインストール・スクリプトで自動的にインストールされます。

この項のトラブルシューティングの手順に従うと、DIP Tester ユーティリティを使用して、次のことができます。

- ディレクトリ統合プロファイルの変更
- ログ・ファイルの表示
- テスト・エントリの作成
- 最後に適用された変更キーの取得または設定
- エントリ・プロファイルの内容のダンプ
- マップ・ファイルのリロード
- Directory Integration Server の起動と停止
- トレース・ファイルでのオラクル社カスタマ・サポート・センターにアップロードするためのエラーの取得
- ユーザーの初期ブートストラップの実行

注意： Oracle Directory Integration Server では、同期を実行する際、最後に適用された変更キーを読み取り、値をキャッシュします。次の同期の間隔で、Oracle Directory Integration Server は、最終実行時間と、最後に適用された変更キーのキャッシュされた値により、Oracle Internet Directory を更新します。

最後に適用された変更キーを同期プロファイル内で手動で変更する前に、必ず Oracle Directory Integration Server を停止してください。停止しないと、次の間隔で、変更がキャッシュ内の値により上書きされてしまいます。実際、同期プロファイルで値を変更する場合には、その前に必ず Oracle Directory Integration Server を停止してください。

DIP Tester ユーティリティは、*$ORACLE_HOME*/bin ディレクトリにインストールされます。

関連資料： DIP Tester ユーティリティのインストール先ディレクトリにある README.txt と『DIP Tester User's Guide』

問題と解決策

この項では、Oracle Directory Integration Platform の一般的な問題とその解決策について説明します。内容は次のとおりです。

注意： Oracle Directory Integration Platform では、6-15 ページの「ファイルの場所とネーミング」に示した適切なファイルにエラー・メッセージが格納されます。

Oracle Directory Integration Server のエラー

この項では、Oracle Directory Integration Server で発生する可能性のあるエラーおよび問題の解決策を示します。

問題

パスワード・ポリシー・エラー :9000: GSL_PWDEXPIRED_EXCP。

解決策

Oracle Internet Directory 10*g*（9.0.4）から、パスワードの期限切れ時間は、`pwdmaxage` 属性に指定され、デフォルトは 60 日に設定されています。この問題を解決するには、次の手順を実行します。

1. `oidpasswd` ユーティリティを使用して、次のように `cn=orcladmin` スーパー・ユーザー・アカウントのロックを解除します。

   ```
   oidpasswd connect=asdb unlock_su_acct=true
   OID DB user password:
   OID super user account unlocked successfully.
   ```

   これにより、スーパー・ユーザー・アカウント `cn=orcladmin` のみがロック解除されます。このアカウントを、デフォルト・レルム `cn=orcladmin,cn=users,dc=xxxxx,dc=yyyyy` 内の cd=orcladmin アカウントと混同しないでください。これら 2 つは別々のアカウントです。

2. Oracle Internet Directory 10*g*（10.1.4.0.1）の Oracle Directory Manager を起動し、「パスワード・ポリシー管理」にナビゲートします。ここには、`cn=PwdPolicyEntry` と、自分のレルムのパスワード・ポリシー（*`password_policy_entry`*`,dc=acme,dc=com` など）の 2 つのエントリがあります。

   各パスワード・ポリシーの `pwdmaxage` 属性を、適切な値に変更します。

   - 5184000 = 60 日（デフォルト）
   - 7776000 = 90 日
   - 10368000 = 120 日
   - 15552000 = 180 日
   - 31536000 = 1 年

注意： 両方のパスワード・ポリシーでこの値を変更することが重要です。

---

3. Oracle Directory Manager を起動し、レルム固有の orcladmin アカウントにナビゲートします。userpassword 属性を探し、新しい値を指定します。これにより OracleAS Single Sign-On を使用する Oracle コンポーネントを起動し、orcladmin としてログインできるようになります。

4. odisrvreg ユーティリティに戻り、ランダムに生成された Oracle Directory Integration Platform のパスワードをリセットします。

```
odisrvreg -D cn=orcladmin -w welcome1 -p 3060
Already Registered...Updating DIS password...
DIS registration successful.
```

プロビジョニングのエラーと問題

この項では、プロビジョニングのエラーと問題の解決策を示します。

問題

GUID からエントリを取得できません。致命的なエラー ...

解決策

Oracle Directory Integration Server が、削除されてまだパージされていないエントリを取得しようとしています。Oracle Directory Manager の「ガベージ・コレクション管理」ノードで、tombstone パージ構成設定を更新します。

問題

LDAP 接続失敗

解決策

Oracle Directory Integration Platform がディレクトリ・サーバーへの接続に失敗しました。ディレクトリ・サーバーへの接続をチェックしてください。

> **関連資料：** ディレクトリ・サーバーの接続については、『Oracle Internet Directory 管理者ガイド』のディレクトリ・サーバーの管理に関する章を参照してください。

問題

LDAP 認証失敗。

解決策

管理者権限で、プロビジョニング・プロファイルを LDAP サーバーに接続できません。ディレクトリの Oracle Directory Integration Server エントリを確認してください。odisrvreg ユーティリティを使用して、Oracle Directory Integration Server を再登録します。

> **関連項目：** 4-13 ページの「Oracle Directory Integration Platform の手動登録」

問題

初期化失敗。

解決策

JNDI を使用したディレクトリ・サーバーへの接続に関する問題です。$*ORACLE_HOME*/ldap/odi/log ディレクトリにあるトレース・ファイル（*profile_name*.trc）および監査ファイル（*profile_name*.aud）を調べてください。

問題
データベース接続失敗。

解決策
データベースを指定したアカウント情報で接続する際の問題です。データベースが稼働していないか、認証に問題があります。$*ORACLE_HOME*/ldap/odi/log ディレクトリにあるトレース・ファイル（*profile_name*.trc）および監査ファイル（*profile_name*.aud）を調べてください。

問題
SQL 操作をコール中の例外。

解決策
パッケージを実行する際の問題です。パッケージの有用性を検査してください。$*ORACLE_HOME*/ldap/odi/log ディレクトリにあるトレース・ファイル（*profile_name*.trc）および監査ファイル（*profile_name*.aud）を調べてください。

問題
プロビジョニング・プロファイルを DIP プロビジョニング・サーバーで実行できません。

解決策
プロビジョニング・プロファイルは、Oracle Directory Integration Platform が構成設定 0 で起動された場合にのみ実行されます。Oracle Directory Integration Server が、引数 `configset=0` で起動されているか確認します。

問題
アプリケーション・データベースに接続できません。

解決策
プロビジョニング・プロファイルで、アプリケーション・データベースの接続要件が正しく指定されていない可能性があります。`sqlplus` を使用して、接続要件を確認します。

問題
ユーザーまたはグループの変更イベントおよび削除イベントがアプリケーションで使用されません。

解決策
Oracle Directory Integration Platform Service では、まずアプリケーション・データベースに対して、ユーザーまたはグループの存在について問い合せます。アプリケーション・データベースが負の値を返した場合は、ユーザーまたはグループは存在せず、イベントはアプリケーションに伝播されません。$*ORACLE_HOME*/ldap/odi/log ディレクトリにあるトレース・ファイル（*profile_name*.trc）および監査ファイル（*profile_name*.aud）を調べ、アプリケーション・データベースにユーザーまたはグループが存在するかどうかを確認します。

問題
バイナリ属性に対するサブスクリプションにより、イベント伝播エラーが発生しました。

解決策
バイナリ属性の伝播はサポートされていません。プロビジョニング・ファイルのイベント・サブスクリプションから、バイナリ属性の指定を削除します。

問題
アプリケーション識別名としてプロキシの役割を果すには不十分なアクセス権限。

解決策
Oracle Directory Integration Platform Server グループは、アプリケーション識別名によって参照権限を付与されていません。`ldapmodify` コマンドを使用して、次の ACI をロードします。これにより、アプリケーション識別名から Oracle Directory Integration Platform グループに対する参照権限を付与します。

```
orclaci: access to attr=(*) by group="cn=odisgroup,cn=odi,cn=oracle internet
directory"(read,write,search,compare)
orclaci: access to entry by group="cn=odisgroup,cn=odi,cn=oracle internet
directory"(browse,proxy)
```

問題
アプリケーション識別名をプロキシとして使用するには不十分なアクセス権限。

解決策
Oracle Directory Integration Platform Server グループは、アプリケーション識別名によってプロキシ権限を付与されていません。`ldapmodify` コマンドを使用して、次の ACI をロードします。これにより、アプリケーション識別名から Oracle Directory Integration Platform グループに対するプロキシ権限を付与します。

```
orclaci: access to entry by group=" cn=odisgroup, cn=odi,cn=oracle internet directory"
(browse,proxy)
```

同期のエラーと問題

この項では、同期のエラーと問題の解決策を示します。

> **関連資料：** Oracle*MetaLink* Note: 276481.1:「Troubleshooting OID DIP Synchronization Issues」（Oracle*MetaLink*（`http://metalink.oracle.com/`）で参照可能）

問題
LDAP: エラー・コード 50 - 不十分なアクセス権限 ; 残りの名前 'CN=Users,dc=mycompany,dc=com'

解決策
レコード・ターゲットがデフォルトのコンテナにありません。`DST CHANGE RECORD` を検索します。ACI でターゲット・コンテナをチェックします。ACI がブランクの場合は、DIP Tester を使用して、既知の ACI のセットを新しいコンテナに適用します。

問題
LDAP: エラー・コード 50 - 不十分なアクセス権限 ; ACTIVECHGIMP マッピング、インポート操作失敗 ; エージェント実行成功、マッピング /IMPORT 操作に失敗しました。

解決策
デフォルトでは、`cn=Users,`*`default realm`* に適切な ACI が含まれています。ただし、このエラーは、デフォルト・レルム内の別のコンテナで同期化を試みると発生する可能性があります。トレース・ファイルを開き、エラーの原因となっている変更レコードを探し、そのレコードの親コンテナの ACI をチェックします。同じ ACI をターゲット・コンテナに適用します。

問題

トレース・ファイル・エラー : Not able to construct DN Output ChangeRecord ChangeRecord : Changetype: 1 ChangeKey: cn=users, dc=us,dc=oracle,dc=com Exception javax.naming. ContextNotEmptyException: [LDAP: error code 66 - Not Allowed On Non-leaf]; remaining name 'cn=users,dc=us,dc=oracle,dc=com' Missing mandatory attribute(s).

解決策

マッピング・ファイルの問題です。Oracle*MetaLink*（`http://metalink.oracle.com/`）で参照可能な Oracle*MetaLink* Note: 261342.1「Understanding DIP Mapping Files」の指示に従います。

問題

トレース・ファイル・エラー : IPlanetImport:Error in Mapping Enginejava.lang.NullPointerException java.lang.NullPointerException at oracle.ldap.odip.engine.Connector.setValues(Connector.java:101).

解決策 1

マッピング・ファイルがロードされていません。Oracle Directory Integration Server 管理ツールで、「マッピング」タブに自分のマッピング・ファイルからの値が含まれていることを確認します。自分の値がない場合は、DIP Tester ユーティリティを使用してマッピング・ファイルをリロードします。

解決策 2

`orclcondirlastappliedchgnum` 属性は NULL か、値がないかです。これは、ブートストラップが失敗した場合、または手動で Oracle Internet Directory にデータを移入し、`orclcondirlastappliedchgnum` 属性に値を指定しなかった場合に発生する可能性があります。`orclcondirlastappliedchgnum` 属性に値が指定されていることを確認します。値が指定されていない場合は、`DIP Tester` ユーティリティを使用して、`orclcondirlastappliedchgnum` 属性を設定します。

問題

トレース・ファイル・エラー : Command exec successful IPlanetImport:Error in Mapping Enginejava.lang.NullPointerException java.lang.NullPointerException at oracle.ldap.odip.engine.Connector.setValues(Connector.java:101) at oracle.ldap.odip.gsi.LDAPReader.initialise(LDAPReader.java:169) Updated Attributes orclodipLastExecutionTime: 20040601143204.

解決策

接続ディレクトリの URL 属性値（`hostname:port`）で LDAP ポートがありません。接続ディレクトリの URL 属性に LDAP ポートを指定します。

問題

トレース・ファイル・エラー : LDAP URL : (xxxxxx.com:389<login credentials to 3rd party ldap server> LDAP Connection success ActiveChgImp:Error in Mapping EngineODIException: DIP_GEN_INITIALIZATION_EXCEPTION ODIException: DIP_GEN_INITIALIZATION_EXCEPTION at oracle.ldap.odip.util.DirUtils.getLastChgNum(DirUtils.java:48) at oracle.ldap.odip.gsi.LDAPReader.initAvailableChgKey(LDAPReader.java:719) at oracle.ldap.odip.gsi.LDAPReader.initialise(LDAPReader.java:212) at oracle.ldap.odip.engine.AgentThread.mapInitialise(AgentThread.java:327) at oracle.ldap.odip.engine.AgentThread.execMapping(AgentThread.java:253) at oracle.ldap.odip.engine.AgentThread.run(AgentThread.java:149) ActiveChgImp:about to Update exec status Error in proxy connection : java.lang.NullPointerException.

解決策

$ORACLE_HOME/ldap/odi/conf のファイルの権限および所有権は、Oracle インストーラ ID が所有する必要があります。`ldapmodify` ユーティリティを使用して、次の 2 つのエントリを修正します。

```
dn: orclODIPAgentName=profile_name,cn=subscriber profile,
  cn=changelog subscriber, cn=oracle internet directory
changetype: modify
replace: orclaci
orclaci: access to attr = (*) by group="cn=odisgroup,cn=odi,cn=oracle
  internet directory"  (read,write,search,compare)
orclaci: access to entry by group="cn=odisgroup,cn=odi,cn=oracle
  internet directory"  (browse,proxy)

dn: orclodipAgentName=ActiveChgImp,cn=subscriber profile,cn=changelog
subscriber,cn=oracle internet directory
orclodipagentconfiginfo:: W0lOVEVSRkFDRURFVEFJTFNdClBhY2thZ2U6IGdzaQpSZWFkZXI
6IEFjdGl2ZUNoZ1JlYWRlcgo=
```

注意： 前述のエントリは、アクティブ変更リーダーのインポート・プロファイルを表すバイナリ・オブジェクトです。Sun Java System Directory のエクスポート・プロファイルを修正している場合は、既存のプロファイルまたは別のノードから、対応するプロファイル用の `orclodipagentconfiginfo` 属性をダンプする必要があります。

関連資料： LDAP エラー・コード 49 およびエラー 9000: GSL_PWDEXPIRED_EXCP については、次の資料を参照してください。

- C-5 ページの「Oracle Directory Integration Server のエラー」
- Oracle*MetaLink* Note: 265397.1: 「Password Policy Expires」（Oracle*MetaLink*（`http://metalink.oracle.com/`）で参照可能）

問題

Oracle Directory Integration Server 管理ツールの「マッピング」タブに、マッピング・ルールのかわりにファイル名が表示されています。

解決策

マッピング・ファイルがロードされたときに、絶対パスが含まれていませんでした。完全な絶対パスを使用して、マッピング・ファイルをリロードします。マッピング・ファイルは、Directory Integration アシスタント（`dipassistant`）または DIP Tester ユーティリティを使用してリロードできます。

問題

LDAP: エラー・コード 50 - 不十分なアクセス権限

解決策

odi エージェント `orclODIPAgentName=IPlanetImport,cn=subscriber profile,cn=changelog subscriber,cn=oracle internet directory` に、Oracle Internet Directory で同期化されたエントリに対する十分な読取り / 書込みアクセス権限がありません。`cn=oracleDASCreateUser,cn=groups,cn=oraclecontext,identity_management_realm` グループですでに必須 ACL が定義されているため、このエントリはこのグループのメンバーです。この場合、<subscriber DN> が *`identity_management_realm`* に設定されています。`orclODIPAgentName=IPlanetImport,cn=subscriber profile,cn=changelog subscriber,cn=oracle internet directory` ユーザー・エントリを、`cn=oracleDASCreateUser,cn=groups,cn=oraclecontext,identity_management_realm` グループに追加する必要があります。すると、エントリには更新を実行するために必要な ACL アクセス権限が付与されます。Oracle Directory Manager で、「エントリ管理」→「dc=com,*`identity_management_realm`*,cn=oraclecontext」→「cn=groups」→「cn=oracleDASCreateUser」にナビゲートします。ここから、属性 uniquemember に対して、`orclODIPAgentName=IPlanetImport,cn=subscriber profile,cn=changelog subscriber,cn=oracle internet directory` を追加します。

問題

追加操作と変更操作は成功しますが、削除操作は失敗し、トレース・ファイルに記録されません。

解決策 1

Sun Java System Directory の場合 : tombstone は無効です。tombstone が有効であることを、Oracle*MetaLink* Note: 219835.1 で説明されているように確認します。Oracle*MetaLink* Note は Oracle*MetaLink*（`http://metalink.oracle.com/`）で参照できます。

解決策 2

Microsoft Active Directory の場合 : プロファイルに使用されるアカウントが、DIR SYNCH ADMIN グループのメンバーではありません。これは、Microsoft Active Directory 管理者アカウントを使用していない場合のみ発生します。Microsoft から適切なパッチをインストールします。

問題

Oracle Directory Integration インポート・コネクタまたはエクスポート・コネクタをサード・パーティ LDAP ディレクトリに対して構成した後、データの同期の問題が発生しました。

解決策

`oditest` ユーティリティを実行して原因を特定します。`oditest` ユーティリティを、C-3 ページの「oditest ユーティリティ」で説明されているように実行します。

問題

Oracle Directory Manager の Oracle Internet Directory プロファイルは、「同期成功」と表示されますが、ディレクトリではまだ変化が見られません。

解決策

同期の間隔の設定が長すぎて、テストに役立ちません。デフォルトでは、同期の間隔は 60 秒ごとに発生するように設定されています。しかし、パフォーマンスを向上させるために、同期の間隔を長くすることができます。たとえば、同期の間隔を 300 秒（5 分）や 600 秒（10 分）に増やすことができます。次の手順に従い、同期の間隔を減らします。

注意：同期の間隔を減らすと、接続ディレクトリ・サーバーのパフォーマンスに深刻な影響を与える可能性があります。同期の間隔を変更する前に、`oditest` ユーティリティを使用して、コネクタをデバッグしてみてください。同期の間隔を変更する場合は、テストの手順が終了したら、必ず元の値にリセットしてください。

1. Oracle Directory Integration Server 管理ツールのナビゲータ・ペインで、「統合サーバー」にナビゲートし、プロファイルの「スケジューリングの間隔」属性を 20 秒に変更します。
2. `odisrv` コマンドを使用して Oracle Directory Integration Server を停止し、パラメータ `debug=63` で再起動します。
3. 接続ディレクトリにテスト・エントリを追加します。
4. Oracle Internet Directory で、*$ORACLE_HOME*/ldap/odi/log ディレクトリに移動し、`cat` コマンドを使用して、ActiveChgImp.trc ファイルを表示します。Oracle Directory Integration Server が稼働中で、接続ディレクトリの変更ログからのレコードを処理しているとき、IplanetImport.trc または ActiveChgImp.trc ファイルの詳細が表示されます。
5. トレース・ファイルを調べて、実際に起こっていることに関して考えられる手掛かりを探ります。接続ディレクトリ・サーバーに対するハンドシェイクやログイン、次に、取得されてマッピング・ルールに応じて形式が改められた変更、最後に、Oracle Internet Directory で試みられた変更が記述されています。ハンドシェイクやマッピングに問題がある場合は、このファイルに現れます。

一般的なミスは、接続ディレクトリ「接続されたディレクトリ・アカウント」の識別名を「管理者」に設定することです。このフィールドには、Microsoft Active Directory 管理者の完全な識別名を入力する必要があります。たとえば次のようになります。

```
cn=Administrator,cn=Users,dc=myoracle,dc=com
```

最初のドメイン・コンポーネントは、Windows のログイン・ページの「ユーザー名」、「パスワード」、「ログオン先」の 3 番目のフィールドの値です。

次の `ldapsearch` コマンドは、構成での問題の特定に役立つ場合があります。

デフォルト ID 管理レルムをチェックするには、次のようにします。

```
ldapsearch -h host -p port -D cn=orcladmin -w password -b "cn=common,cn=products,
cn=oraclecontext" -L -s
base "objectclass=*" orcldefaultsubscriber
```

Oracle Directory Integration Server 構成設定をダンプするには、次のようにします。

```
ldapsearch -h host -p port -D cn=orcladmin -w password -b cn=instance1,cn=odisrv,
cn=subregistrysubentry
-s base -v "objectclass=*"
```

プロファイルをチェックするには、次のようにします。

```
ldapsearch -h host -p port -D cn=orcladmin -w password -b
"orclODIPAgentName=profile,cn=subscriber profile,cn=changelog Subscriber,cn=oracle
internet directory" -s sub objectclass=*
```

エージェントの資格証明をチェックするには、次のようにします。

```
ldapsearch -p port -D cn=orcladmin -w password -b "orclODIPAgentName=profile,
cn=subscriber profile,cn=changelog subscriber,cn=oracle internet directory"
-s sub "objectclass=*"
```

このコマンドは、`orcladmin` 資格証明を使用して実行した場合のみ、パスワードをクリアテキストで返します。

問題

のブートストラップ・エラー : DIP_GEN_AUTHENTICATION_FAILURE（Microsoft Active Directory と Oracle Internet Directory の同期化の試行時）

解決策

資格証明が無効です。同期プロファイルをチェックし、Microsoft Active Directory サーバーにログインするための適切な資格証明が含まれていることを確認します。

Windows ネイティブ認証のエラーと問題

この項では、Oracle Identity Management を Windows ネイティブ認証と統合する際に発生する可能性のあるエラーと問題の解決策を示します。

問題

サーバーの内部エラーです。管理者に通知してください。

解決策

中間層コンピュータで、Windows ネイティブ認証が正しく構成されていません。この問題を解決するには、次の手順を実行します。

1. opmn.log ファイルでエラーをチェックします。
2. ssoServer.log ファイルでエラーをチェックします。
3. keytab ファイルが $*ORACLE_HOME*/j2ee/OC4J_SECURITY/config ディレクトリにあり、jazn-data.xml ファイルで構成されたプリンシパル名が正しいことを確認します。
4. Key Distribution Center にアクセスできるように、シングル・サインオンの中間層コンピュータが正しく構成されていることを確認します。19-8 ページの「OracleAS Single Sign-On Server の Kerberos サービス・アカウントの設定」を参照してください。

問題

KDC で認証できませんでした。

解決策

krb5.conf のレルム名が正しく構成されていない場合に、このエラー・メッセージが表示されることがあります。/etc/krb5/krb5.conf で `default_realm` と `domain_realm` の値をチェックします。レルム名では、大文字と小文字を区別します。

問題

ブラウザが Windows の Kerberos 認証をサポートしていないか適切に構成されていません。

解決策

ユーザーの Web ブラウザがサポートされていないか、正しく構成されていません。19-11 ページの「タスク 2: Windows ネイティブ認証用の Internet Explorer の構成」の指示に従ってください。

問題

「アクセスが許可されていません」、HTTP エラー・コード 403、または「Windows のネイティブ認証に失敗しました。管理者に連絡してください。」

解決策

これらのエラー・メッセージは、同じ原因、つまりユーザー・エントリが Oracle Internet Directory にないことに起因します。Windows デスクトップで作業するローカル管理者が、Oracle Internet Directory と同期化されていないエントリを持つシングル・サインオンのパートナ・アプリケーションへのアクセスを試みている可能性があります。ユーザー・エントリがディレクトリに存在するかどうか、そのユーザーの Kerberos プリンシパル属性が Microsoft Active Directory から正しく同期化されているかどうかを確認します。

問題

パートナ・アプリケーションにアクセスすると、Windows のログイン・ダイアログ・ボックスが（ユーザー名、パスワードおよびドメイン・フィールド付きで）表示されます。

解決策

Oracle Internet Directory で対応するユーザー・エントリが見つからないため、Single Sign-On Server で Kerberos トークンを認証できませんでした。ディレクトリにユーザー・エントリを追加します。

問題

Single Sign-On Server が起動しません。ログ・ファイルに「Credential not found.」というメッセージの例外があります。

解決策

`kerberos-servicename` パラメータが正しく構成されていない可能性があります。この問題を解決するには、次の手順を実行します。

1. orion-application.xml ファイルと jazn-data.xml ファイルで `kerberos-servicename` が正しく構成されていることを確認します。orion-application.xml ファイルでは、このパラメータの書式は `HTTP@sso.mycompany.com` です。jazn-data.xml ファイルでは、書式は `HTTP/sso.mycompany.com` です。
2. ssoServer.log ファイルでエラーをチェックします。
3. keytab ファイルが $*ORACLE_HOME*/j2ee/OC4J_SECURITY/config ディレクトリにあり、jazn-data.xml で構成されたプリンシパル名が正しいことを確認します。
4. Kerberos ドメイン・コントローラにアクセスできるように、シングル・サインオンの中間層コンピュータが構成されていることを確認します。19-8 ページの「OracleAS Single Sign-On Server の Kerberos サービス・アカウントの設定」を参照してください。

問題

OracleAS Single Sign-On Configuration Assistant の実行時に、次の例外が発生します。

```
Repository Access API throws exception :
oracle.ias.repository.schema.SchemaException: Unable to establish secure
connection to Oracle Internet Directory Server
ldap://server.mycompany.com:636/ Base Exception :
javax.naming.CommunicationException: server.mycompany.com:636 [Root
exception is java.lang.UnsatisfiedLinkError: no njssl10 in java.library.path]
        at
oracle.ias.repository.directory.DirectoryReader.connectSsl(DirectoryReader.java:
98)
        at
oracle.ias.repository.directory.DirectoryReader.connect(DirectoryReader.java:106
)
        at oracle.ias.repository.IASSchema.getDBPassword(IASSchema.java:440)
        at
oracle.ias.repository.SchemaManager.getDBPassword(SchemaManager.java:310)
        at oracle.security.sso.IMWNAConfig.getSSOHost(IMWNAConfig.java:903)
        at oracle.security.sso.IMWNAConfig.parseArgs(IMWNAConfig.java:168)
        at oracle.security.sso.IMWNAConfig.init(IMWNAConfig.java:194)
        at oracle.security.sso.IMWNAConfig.work(IMWNAConfig.java:60)
        at
oracle.security.sso.SSOConfigAssistant.wnaConfig(SSOConfigAssistant.java:243)
        at
oracle.security.sso.SSOConfigAssistant.main(SSOConfigAssistant.java:218)
```

解決策

この例外は、Windows バージョンの OracleAS Single Sign-On Configuration Assistant を UNIX および Linux プラットフォームで実行した場合に発生します。19-10 ページの「各

Oracle Application Server Single Sign-On ホストでの OracleAS Single Sign-On Configuration Assistant の実行」の指示に従い、UNIX/Linux バージョンの OracleAS Single Sign-On Configuration Assistant を実行してください。

問題

Windows ネイティブ認証で、Internet Explorer が Kerberos 資格証明のかわりに NT Lan Manager（NTLM）認証を送信しています。

解決策

この問題は、Microsoft Active Directory が正しく構成されていないことが原因で発生します。この問題の解決方法について Microsoft Active Directory のドキュメントを参照するか、Microsoft 社に問い合せてください。

問題

個別ユーザーが、Windows ネイティブ認証を使用して特定のコンピュータからログインできません。

解決策

ユーザーが別のコンピュータを使用してログインできる場合は、元のコンピュータでの Windows または Internet Explorer に構成の問題があります。この問題の解決方法について Microsoft Developer Network（`http://msdn.microsoft.com`）を参照するか、Microsoft 社に問い合せてください。

Novell eDirectory と OpenLDAP の同期のエラーと問題

この項では、Novell eDirectory と OpenLDAP で発生する可能性のある同期のエラーと問題に対する解決策を示します。

問題

インポート同期の構成後、プロファイルの同期ステータスは成功で、トレース・ファイルに例外が示されていないにもかかわらず、Novell eDirectory または OpenLDAP から Oracle Internet Directory にエントリが同期化されません。

考えられる原因と解決策は、次のとおりです。

原因　誤った値がインポート・プロファイルの `odip.profile.condirfilter` プロパティの `modifiersname` パラメータに割り当てられています。

解決策　接続識別名を、Novell eDirectory または OpenLDAP のエクスポート・プロファイルからインポート・プロファイルの `odip.profile.condirfilter` プロパティの `modifiersname` パラメータにコピーします。

原因　Oracle Directory Integration Server が同期化しようとしたエントリが、インポート・ファイルの `odip.profile.condirfilter` プロパティの `modifiersname` パラメータに割り当てられたものと同じ識別名を使用して作成されています。

解決策　インポート・ファイルの `odip.profile.condirfilter` プロパティの `modifiersname` パラメータに割り当てられている識別名を、Novell eDirectory または OpenLDAP でエントリを作成しない識別名に変更します。

原因　Oracle Internet Directory を実行しているコンピュータと、Novell eDirectory または OpenLDAP を実行しているコンピュータとの間に時間差があります。

解決策　インポート・ファイルの `odip.profile.configfile` プロパティの `ReduceFilterTimeInSeconds` パラメータに、2 つのコンピュータ間の時間差と等しい秒数を値として割り当てます。

問題
通信例外。

解決策
ディレクトリ・サーバーの 1 つが稼働していません。`ldapbind` ユーティリティを使用して、稼働していないサーバーを確認し、そのサーバーを再起動します。

問題
リコンシリエーション時にスローされたサポート外の例外。

解決策
Novell eDirectory または OpenLDAP のリコンシリエーション・ルールに指定されている Oracle Internet Directory の属性の 1 つ以上が索引付けされていません。Oracle Internet Directory の対応する属性を索引付けします。

問題
プロファイルのリコンシリエーション・ステータスは成功であるにもかかわらず、Novell eDirectory または OpenLDAP から Oracle Internet Directory に削除済エントリが同期化されません。

考えられる原因と解決策は、次のとおりです。

原因　削除済エントリが Novell eDirectory または OpenLDAP のリコンシリエーション・ルールに指定されていません。

解決策　Novell eDirectory または OpenLDAP のリコンシリエーション・ルールを変更して、削除済エントリを含めます。

原因　Novell eDirectory または OpenLDAP に特定のリコンシリエーション・ルールに関するエントリが Oracle Internet Directory よりも多くあります。

解決策　次のメッセージがないか、$*ORACLE_HOME*/ldap/odi/log/*profile_name*.trc ファイルを調べてください。

```
No. of entries are less in destination directory compared to source directory.
```

このメッセージは通常、Novell eDirectory または OpenLDAP の DIT 全体が Oracle Internet Directory と同期化される必要がある場合に生成されます。この問題を解決するには、`odip.profile.configfile` プロパティの `CheckAllEntries` パラメータに `true` 値を指定します。

注意： `odip.profile.configfile` プロパティの `CheckAllEntries` パラメータに `true` 値を指定すると、パフォーマンスが低下します。

Oracle Password Filter for Microsoft Active Directory のエラーと問題

この項では、Oracle Password Filter for Microsoft Active Directory で発生する可能性のあるエラーと問題に対する解決策を示します。

問題
ログ・ファイル・パスが見つかりません。

原因
ログ・ファイル・パスが無効です。

解決策
20-16 ページの「Oracle Password Filter for Microsoft Active Directory の再構成」の指示に従い、有効なログ・ファイル・パスを指定します。

問題
非 SSL モードで Oracle Internet Directory に接続できません。

原因
Oracle Internet Directory の構成設定が無効です。

解決策
20-16 ページの「Oracle Password Filter for Microsoft Active Directory の再構成」の指示に従い、Oracle Internet Directory の構成設定を修正します。

問題
SSL モードで Oracle Internet Directory に接続できません。

原因
Oracle Internet Directory の認証局の信頼できる証明書が Microsoft Active Directory ドメイン・コントローラにインポートされていません。

解決策
20-5 ページの「Microsoft Active Directory ドメイン・コントローラへの信頼できる証明書のインポート」の指示に従い、Microsoft Active Directory に信頼できる証明書をインポートします。

問題
Microsoft Active Directory に接続できません。

原因
Microsoft Active Directory の構成設定が無効です。

解決策
20-16 ページの「Oracle Password Filter for Microsoft Active Directory の再構成」の指示に従い、Microsoft Active Directory の構成設定を修正します。

問題

prepAD.ldif ファイルをアップロードできません。

原因

指定された Microsoft Active Directory のベース DN コンテナに `organizationalUnit` オブジェクトを格納できません。

解決策

20-16 ページの「Oracle Password Filter for Microsoft Active Directory の再構成」の指示に従い、`organizationalUnit` オブジェクトを格納できる Microsoft Active Directory のベース DN を指定します。

問題

パスワード更新が Oracle Internet Directory と Microsoft Active Directory の間でループしています。

原因

Oracle Password Filter が、Microsoft Active Directory から Oracle Internet Directory に値をインポートする同期プロファイルに指定されているものと同じバインド DN とパスワードを使用するように構成されていません。

解決策

20-16 ページの「Oracle Password Filter for Microsoft Active Directory の再構成」の指示に従い、Microsoft Active Directory から Oracle Internet Directory に値をインポートする同期プロファイルに指定されているものと同じバインド DN とパスワードを使用するように Oracle Password Filter を構成します。

問題

一部のパスワードが、Oracle Internet Directory と Microsoft Active Directory の間で同期化されません。

原因

Oracle Internet Directory と Microsoft Active Directory で、競合するパスワード・ポリシーを指定しています。

解決策

Oracle Internet Directory のパスワード・ポリシーを Microsoft Active Directory に設定されているものと同じポリシーに設定するか、Oracle Internet Directory からパスワード・ポリシーを削除します。

問題

一部のユーザーについて、パスワードが同期化されません。

原因

Oracle Password Filter の拡張インストールを実行して、Oracle Internet Directory と Microsoft Active Directory の間で同期化する属性に異なる値を指定しています。

解決策

20-16 ページの「Oracle Password Filter for Microsoft Active Directory の再構成」の指示に従い、Oracle Internet Directory と Microsoft Active Directory の間で同期化する属性に同じ値を指定します。

問題

ユーザー・データは同期化されますが、パスワードの同期化が遅延します。

原因

ユーザー・データの同期とパスワードの同期に、異なる時間間隔が指定されています。

解決策

Oracle Password Filter の `SleepTime` パラメータに指定された値が、同期プロファイルのデフォルトのスケジューリング間隔と同じであることを確認します。Oracle Directory Integration Server 管理ツールまたは Directory Integration アシスタント（`dipassistant`）を使用すると、同期プロファイルのデフォルトのスケジューリング間隔を表示および変更できます。`SleepTime` パラメータに指定された値を変更するには、20-16 ページの「Oracle Password Filter for Microsoft Active Directory の再構成」の指示に従います。

> **関連項目：** Oracle Directory Integration Server 管理ツールまたは Directory Integration アシスタント（`dipassistant`）の詳細は、第 3 章「Oracle Directory Integration Platform 管理ツール」を参照してください。

プロビジョニングに関するトラブルシューティング

この項では、Oracle Internet Directory プロビジョニング・コンソールでプロビジョニング問題をトラブルシューティングする方法について説明します。内容は次のとおりです。

診断設定の表示

Oracle Delegated Administration Services の診断設定を使用すると、ログ・ファイルを調べずに Oracle Internet Directory プロビジョニング・コンソールでプロビジョニング問題をデバッグできます。診断設定の表示および構成の詳細は、『Oracle Identity Management 委任管理ガイド』の Oracle Internet Directory セルフ・サービス・コンソールによるユーザーおよびグループの管理に関する章を参照してください。

プロビジョニング統合アプリケーションがプロビジョニング・コンソールに表示されない場合

Oracle Internet Directory に新しいプロビジョニング統合アプリケーションをインストールしても、アプリケーション・キャッシュをリロードするまでそのアプリケーションはプロビジョニング・コンソールに表示されません。Oracle Internet Directory でプロビジョニング統合アプリケーションが有効化または無効化された場合も、常にアプリケーション・キャッシュをリロードする必要があります。アプリケーション・キャッシュをリロードするには、14-6 ページの「アプリケーション・キャッシュのリロード」の手順に従います。

ユーザーを作成できない場合

Oracle プロビジョニング・サービスでは、プラグインを使用して新規ユーザーを作成します。この項では、Oracle プロビジョニング・サービスのプラグインをトラブルシューティングしてユーザー作成の問題を解決する方法について説明します。内容は次のとおりです。

- データ・エントリ・プラグインのトラブルシューティング
- プロビジョニング・プラグインのトラブルシューティング

データ・エントリ・プラグインのトラブルシューティング

プロビジョニング統合アプリケーションでは、プロビジョニング・インテリジェンス機能を拡張してビジネス・ポリシーを実装するために、プレデータ・エントリ・プラグインとポストデータ・エントリ・プラグインを起動できます。この項では、これら 2 つのプラグインの問題をトラブルシューティングする方法について説明します。

プレデータ・エントリ・プラグインに関する問題の識別 14-3 ページの「プロビジョニング・コンソールによるユーザーの作成」の指示に従う場合、プロビジョニング・コンソールでは、一般プロビジョニング・ウィンドウの「次へ」をクリックすると、プレデータ・エントリ・プラグインが起動します。このプラグインの主な目的は、一般プロビジョニング・ウィンドウで選択されたアプリケーションにユーザーをプロビジョニングするかどうかを決定することです。ユーザーがアプリケーションに対するプロビジョニング権限を保持している場合、アプリケーションのプロビジョニング・ポリシーに従って、プレデータ・エントリ・プラグインにより、次のウィンドウ（アプリケーション・プロビジョニング・ウィンドウ）のフィールドが移入されます。

プレデータ・エントリ・プラグインに問題が発生すると、例外メッセージとスタック・トレースを含むエラーが一般プロビジョニング・ウィンドウに表示されます。スタック・トレースで次の行を検索して、プラグインに渡されたユーザー属性を確認できます。

```
******preplugin base user prop set for <Application Name> …
```

次の行を検索して、ログ・ファイルでエラーを確認できます。

```
oracle.idm.provisioning.plugin.PluginException
```

ポストデータ・エントリ・プラグインに関する問題の識別 14-3 ページの「プロビジョニング・コンソールによるユーザーの作成」の指示に従う場合、プロビジョニング・コンソールでは、「アプリケーション属性」ウィンドウの「**次へ**」をクリックすると、ポストデータ・エントリ・プラグインが起動します。ポストデータ・エントリ・プラグインは、ユーザーによって入力された共通属性とアプリケーション固有属性に関するデータを検証します。プロビジョニング作業を続けるためには、このプラグインでの検証に成功する必要があります。

ポストデータ・エントリ・プラグインに問題が発生すると、エラーが「アプリケーション属性」ウィンドウに表示されます。例外スタック・トレースは、次の行に続いています。

```
UserPlguInMgmt::postPlugInProcess(): apptype <Application Type> appname <Application
Name> error when executing plugin logics
```

プロビジョニング・プラグインのトラブルシューティング

プロビジョニング統合アプリケーションは、PL/SQL プラグインまたはデータ・アクセス Java プラグインを通じてプロビジョニングされます。PL/SQL プラグインは、Oracle Directory Integration Platform によって起動されますが、データ・アクセス Java プラグインは、Oracle Delegated Administration Services によって直接起動されます。

14-3 ページの「プロビジョニング・コンソールによるユーザーの作成」の指示に従う場合、特定のアプリケーションに対するプロビジョニングに失敗しても、ユーザーの作成は成功することがあります。プロビジョニングの失敗は、「確認」ウィンドウの「**発行**」をクリックして、プロビジョニング・エラー・メッセージとともに警告ステータスを受信した場合にそのことがわかります。失敗の詳細を確認するには、ログ・ファイルで「Data Access plug-in execution failure」を検索します。この文に続く行に、プロビジョニングに失敗した詳細な理由がリストされています。

プロビジョニング・ステータスを使用した問題の識別

ユーザー・エントリのプロビジョニング・ステータスは、プロビジョニング問題の識別に役立ちます。

ユーザー・エントリのプロビジョニング・ステータスを参照するには、次の手順を実行します。

1. プロビジョニング・コンソールで、「**ディレクトリ**」タブを選択し、「**ユーザー**」を選択します。「ユーザーの検索」ウィンドウが表示されます。
2. 「**ユーザーの検索**」フィールドに、ユーザーの姓、名、電子メール・アドレスまたはユーザー ID の最初の数文字を入力します。たとえば、Anne Smith を検索する場合、Ann または Smi と入力します。ディレクトリにあるすべてのユーザーのリストを表示するには、このフィールドを空白のままにしてください。
3. 「**実行**」をクリックして検索結果を表示します。
4. 参照するエントリを保持するユーザーを選択し、「**表示**」をクリックして「ユーザーの表示」ウィンドウを表示します。

   このウィンドウの詳細は、『Oracle Identity Management 委任管理ガイド』を参照してください。
5. 「**ユーザーの表示**」ウィンドウで、「**プロビジョニング・ステータス**」表のエントリを調べます。アプリケーションの「プロビジョニング・ステータス」列に PROVISIONING_FAILURE という値が含まれている場合、「プロビジョニング・ステータスの説明」列に失敗の原因を説明する次のいずれかの値が含まれます。

   - PROVISIONING_REQUIRED
   - PENDING_UPGRADE
   - PROVISIONING_NOT_REQUIRED
   - PROVISIONING_FAILURE

   関連項目： ユーザー・プロビジョニング・ステータスの詳細は、12-10 ページの「ユーザー・プロビジョニング・ステータスの概要」を参照してください。

アカウント作成後にユーザーがログインできない場合

アカウント作成後にユーザーがログインできないという典型的な問題を解決するには、次の手順を実行します。

1. C-21 ページの「プロビジョニング・ステータスを使用した問題の識別」の指示に従い、ユーザー・プロビジョニング・ステータスを調査してユーザーが適切にプロビジョニングされていないアプリケーションを特定します。
2. ユーザーが適切にプロビジョニングされていないアプリケーションのプロビジョニング方式を特定します。

   - Oracle Internet Directory プロビジョニング・コンソールで作成されたユーザー・アカウントの場合、Oracle Delegated Administration Services の次のログ・ファイルを調べます。

     $*ORACLE_HOME*/opmn/logs/OC4J~OC4J_SECURITY~default_island~1

   - PL/SQL プラグインまたはデータ・アクセス Java プラグインで作成されたユーザー・アカウントの場合、次のトレース・ファイルまたは監査ファイルを調べます。

     $ORACLE_HOME/ldap/odi/log/*applicationType_realmName*_E.trc
     $ORACLE_HOME/ldap/odi/log/*applicationType_realmName*_E.aud

Oracle Enterprise Manager 10*g* Application Server Control コンソールによるプロビジョニング実行ステータスの監視

Oracle Enterprise Manager 10*g* Application Server Control コンソールを使用して、プロビジョニング統合プロファイルのプロビジョニング実行ステータスを監視できます。

1. Application Server Control コンソールのメイン・ページの「スタンドアロン・インスタンス」セクションで、管理する Oracle Application Server インスタンスの名前を選択します。選択したインスタンスについて、Oracle Application Server ホームページが開きます。
2. 「**システム・コンポーネント**」表の「名前」列で、「**OID**」を選択します。「Oracle Internet Directory」ページが開きます。必要なパッケージが正しくインストールされている場合、ステータスは緑色になります。これは、Oracle Directory Integration Server が稼働中かどうかを示すものではありません。
3. サーバーのステータスをチェックするには、「**ディレクトリ統合**」を選択して、「ディレクトリ統合プラットフォーム・ステータス」ページを表示します。このページには、プロビジョニング用と同期用のものも含め、Oracle Directory Integration Server の様々な実行中インスタンスが表示されます。プロビジョニング統合プロファイルに関してこのウィンドウに表示される主なデータは次のとおりです。
   - サブスクライブ・アプリケーションの名前
   - サブスクリプションが行われた企業の名前
   - プロファイルのステータス（ENABLED または DISABLED）
   - プロファイルで示されるアプリケーションへのイベント伝播に使用された Oracle Internet Directory 内の変更キー
   - 最終実行時間
   - プロファイルの最終正常実行時間
   - エラー（存在する場合）

   注意：「ディレクトリ統合プラットフォーム・ステータス」ページには、このプロファイルの各種イベント・サブスクリプションは表示されません。

操作の引数 `status` を指定して `oidprovtool` ユーティリティを実行することで、プロビジョニング統合ステータスに関する詳細出力も取得できます。`oidprovtool` ユーティリティは、*$ORACLE_HOME*/bin ディレクトリにあります。

関連資料： `oidprovtool` ユーティリティの使用方法の詳細は、『Oracle Identity Management ユーザー・リファレンス』の Oracle Directory Integration Platform ツールに関する章を参照してください。

プロビジョニングのトラブルシューティング用チェックリスト

プロビジョニングをトラブルシューティングする際は、次のチェックリストを使用します。

- UNIX/Linux の場合、次のコマンドを使用して、Oracle Directory Integration Server プロセス（odisrv）が実行されていることを確認します。

  ```
  ps -ef | grep odisrv
  ```

  Windows の場合、*$ORACLE_HOME*/ldap/log/oidmon.log ファイルから odisrv プロセスのプロセス ID（PID）の値を取得します。次に、タスク マネージャを起動し、「**プロセス**」タブをクリックして、そのプロセスが実行されていることを確認します。

- Oracle Directory Integration Server インスタンスも実行されているかどうかチェックします。

  OracleAS Portal、Oracle Collaboration Suite または別のコンポーネントでプロビジョニングが必要な場合は、構成設定 0 でインスタンス 1 として実行されている Oracle Directory Integration Server プロビジョニング・プロセスがあります。この場合、自分の Oracle Directory Integration Server をインスタンス 2 として、デフォルトの configset=1 引数か、自分で作成したカスタム構成設定番号を指定して起動する必要があります。

  $ORACLE_HOME/ldap/log/odisrv0*x*.log をチェックします。プロビジョニング統合サービスが実行されている場合、ログは odisrv01.log ファイルに記録されます。次に、ディレクトリ同期サービスは odisrv02.log ファイルに記録します。

- Oracle Directory Integration Server 管理ツールまたは DIP Tester ユーティリティを使用して、プロファイルが有効かどうかを確認します。

- トレース・ファイルが生成されていることを確認します。トレース・ファイルは、*$ORACLE_HOME*/ldap/odi/log/*profile_name*.trc にあります。

  トレース・ファイルが生成されていない場合は、Oracle Directory Integration Server の起動にこのリストでこれまで説明してきたような問題がないか、odisrv0*x*.log をチェックします。

- Oracle Directory Integration Server の起動に正しい構文が使用されていることを確認します。たとえば、次のようになります。

  ```
  oidctl connect=asdb server=odisrv instance=2 configset=1 flags="host=myhost
  port=3060" start
  ```

- デバッグの場合、Oracle Directory Integration Server の起動時に、次のようにデバッグ・フラグの値が 63 に設定されていることを確認します。

  ```
  oidctl connect=asdb server=odisrv instance=2 configset=1 flags="host=myhost
  port=3060 debug=63" start
  ```

- Oracle Directory Integration Server 管理ツールまたは DIP Tester ユーティリティを使用して、プロファイルを編集し、デバッグ・レベルを 63 に設定します。

- プロファイルのすべての必須パラメータを検証します。

  関連資料：

  - Oracle*MetaLink* Note: 261342.1「Understanding DIP Mapping Files」（Oracle*MetaLink*（http://metalink.oracle.com/）で参照可能）
  - 6-5 ページの「マッピング・ルールの構成」

- プロファイルの更新に、Oracle Internet Directory 10*g*（10.1.4.0.1）の Oracle Directory Integration Server 管理ツールまたは Oracle Directory Manager を使用していることを確認します。これらのユーティリティの前のリリースでは、「プロファイル」タブ・ページで異なる情報が表示されるため、使用しないでください。

- PL/SQL プラグインを使用している場合、sqlplus を使用してプロビジョニング統合アプリケーションへの接続状況を検証します。

関連資料： Oracle*MetaLink* Note: 265397.1: 「Password Policy Expires」（Oracle*MetaLink*（`http://metalink.oracle.com/`）で参照可能）

同期に関するトラブルシューティング

この項では、Oracle Directory Integration Platform との同期に関する問題をトラブルシューティングする方法について説明します。内容は次のとおりです。

- Oracle Directory Integration Platform の同期プロセスの流れ
- 同期のトラブルシューティング用チェックリスト
- デバッグ・レベル 63 モードでの有効なサンプル・トレース・ファイル

Oracle Directory Integration Platform の同期プロセスの流れ

Oracle Internet Directory と接続ディレクトリ間の同期に関する問題をデバッグする場合、Oracle Directory Integration Server の同期プロセスの流れを理解することが役立ちます。

インポート・プロファイルに関する Oracle Directory Integration Platform の同期プロセスの流れ

Oracle Directory Integration Server では、起動時にすべてのインポート・プロファイルを読み取ります。`ENABLE` に設定されているプロファイルごとに、同期プロセスの間に、Oracle Directory Integration Server により次のタスクが実行されます。

1. サード・パーティ・ディレクトリに接続します。
2. 接続ディレクトリから最終変更キーの値を取得します。
3. Oracle Internet Directory に接続します。
4. プロファイルの最後に適用された変更キーの値を Oracle Internet Directory から取得します。
5. Sun Java System Directory 接続の場合、Oracle Directory Integration Server は、リモートの変更ログで、最後に適用された変更キーの値より大きいエントリと、最終変更キーの値以下のエントリを検索します。Microsoft Active Directory 接続の場合、Oracle Directory Integration Server は、この情報をリモート・ディレクトリの `USNChanged` 値で検索します。Novell eDirectory コネクタと OpenLDAP コネクタの場合、変更は各エントリの `modifytimestamp` 属性に基づいて識別されます。Oracle Human Resources コネクタなど、その他のタイプのコネクタの場合、Oracle Directory Integration Server では同様のタイプの検索を実行しますが、データが交換される方法は、接続のタイプによって異なります。
6. データ値を接続ディレクトリから Oracle Internet Directory の値へマップします。
7. Oracle Internet Directory 変更レコードを作成します。
8. Oracle Internet Directory で変更を適用（追加、変更、削除）します。
9. Oracle Internet Directory インポート・プロファイルを、最終実行時間と接続ディレクトリから最後に適用された変更キーで更新します。
10. 同期の間隔として指定された秒数のスリープ・モードに入ります。

エクスポート・プロファイルに関する Oracle Directory Integration Platform の同期プロセスの流れ

Oracle Directory Integration Server では、起動時にすべてのエクスポート・プロファイルを読み取ります。ENABLE に設定されているプロファイルごとに、同期プロセスの間に、Oracle Directory Integration Platform により次のタスクが実行されます。

1. サード・パーティ・ディレクトリに接続します。
2. Oracle Internet Directory に接続します。
3. 最終変更キーの値を Oracle Internet Directory から取得します。
4. プロファイルの最後に適用された変更キーの値を Oracle Internet Directory から取得します。
5. Oracle Directory Integration Server は、Oracle Internet Directory の変更ログで、最後に適用された変更キーの値より大きいエントリと、最終変更キーの値以下のエントリを検索します。
6. データ値を Oracle Internet Directory から接続ディレクトリの値へマップします。
7. 変更レコードを作成します。
8. 接続ディレクトリに変更を適用（追加、変更、削除）します。
9. Oracle Internet Directory エクスポート・プロファイルを、最終実行時間と Oracle Internet Directory から最後に適用された変更キーで更新します。
10. 同期の間隔として指定された秒数のスリープ・モードに入ります。

同期のトラブルシューティング用チェックリスト

同期をトラブルシューティングする際は、次のチェックリストを使用します。

- UNIX/Linux の場合、次のコマンドを使用して、Oracle Directory Integration Platform プロセス（odisrv）が実行されていることを確認します。

  ```
  ps -ef | grep odisrv
  ```

  Windows オペレーティング・システムの場合、*$ORACLE_HOME*/ldap/log/oidmon.log から odisrv プロセスのプロセス ID（PID）の値を取得します。次にタスク マネージャを起動し、「**プロセス**」タブをクリックして、プロセスが実行されていること確認します。

- Oracle Directory Integration Server インスタンスも実行されているかどうかチェックします。

  OracleAS Portal、Oracle Collaboration Suite または別のコンポーネントでプロビジョニングが必要な場合は、構成設定 0 でインスタンス 1 として実行されている Oracle Directory Integration Server プロビジョニング・プロセスがあります。この場合、自分の Directory Integration Server をインスタンス 2 として、デフォルトの configset=1 引数か、自分で作成したカスタム構成設定番号を指定して起動する必要があります。

  $ORACLE_HOME/ldap/log/odisrv0*x*.log をチェックします。プロビジョニング統合サービスが実行されている場合、ログは odisrv01.log ファイルに記録されます。次に、ディレクトリ同期サービスは odisrv02.log に記録します。

- Oracle Directory Integration Server 管理ツールまたは DIP Tester ユーティリティを使用して、プロファイルが有効かどうかを確認します。

- トレース・ファイルが生成されていることを確認します。トレース・ファイルは、*$ORACLE_HOME*/ldap/odi/log/*profile_name*.trc にあります。

  トレース・ファイルが生成されていない場合は、Directory Integration Server の起動にこのリストでこれまで説明してきたような問題がないか、odisrv0*x*.log をチェックします。

- 監査ログが生成されていることを確認し、失敗がないか監査ログを定期的に調べます。監査ログは、$*ORACLE_HOME*/ldap/odi/log/*profile_name*.aud にあります。

- Oracle Directory Integration Server の起動に正しい構文が使用されていることを確認します。たとえば、次のようになります。

  ```
  oidctl connect=asdb server=odisrv instance=2 configset=1 flags="host=myhost
  port=3060" start
  ```

- デバッグの場合、Directory Integration Server の起動時に、次のようにデバッグ・フラグの値が 63 に設定されていることを確認します。

  ```
  oidctl connect=asdb server=odisrv instance=2 configset=1 flags="host=myhost
  port=3060 debug=63" start
  ```

- Oracle Directory Integration Server 管理ツールまたは DIP Tester ユーティリティを使用して、プロファイルを編集し、デバッグ・レベルを 63 に設定します。
- プロファイルのすべての必須パラメータを検証します。

  関連資料：

  - Oracle*MetaLink* Note: 261342.1「Understanding DIP Mapping Files」（Oracle*MetaLink*（`http://metalink.oracle.com/`）で参照可能）
  - 6-5 ページの「マッピング・ルールの構成」

- プロファイルの更新に、Oracle Internet Directory 10*g*（10.1.4.0.1）の Oracle Directory Integration Server 管理ツールまたは Oracle Directory Manager を使用していることを確認します。これらのユーティリティの前のリリースでは、「プロファイル」タブ・ページで異なる情報が表示されるため、使用しないでください。
- 次のコマンドを実行して、サード・パーティの LDAP ディレクトリ・サーバーが稼働しているかどうかを確認します。

  ```
  ldapbind -h ldap_host -p ldap_port -D account -w password
  ```

- Oracle Directory Integration Server が起動していない場合、または起動後障害が発生した場合は、次のことをチェックします。
  - インスタンス番号と使用されている構成設定
  - `flags="host=xxx port=xxxx"` パラメータが `oidctl` を指定して使用されているかどうか
  - odisrv0*x*.log で次のことを確認
    - コネクタが正常に起動しているかどうか
    - パスワードが期限切れになっているかどうか

  コネクタを再登録するには、次のコマンドを入力します。

  ```
  odisrvreg -p port -D cn=orcladmin -w passwd -h host
  ```

  関連資料： Oracle*MetaLink* Note: 265397.1: 「Password Policy Expires」（Oracle*MetaLink*（`http://metalink.oracle.com/`）で参照可能）

デバッグ・レベル 63 モードでの有効なサンプル・トレース・ファイル

次に、Microsoft Active Directory コネクタの同期化された追加操作用の、有効なサンプル・トレース・ファイルの最初と終わりの部分を示します。

```
--------------------------------------------------------------------------------
Trace Log Started at Tue Jun 08 11:22:25 EDT 2004
--------------------------------------------------------------------------------
Command exec succesful
LDAP URL : (activedir.oracle.com:389 administrator@oracle.com
LDAP Connection success
Applied ChangeNum : 28017Available chg num = 28019
Reader Initialised !!
LDAP URL : (sun1:3060 cn=odisrv+orclhostname=sun1,cn=odi,cn=oracle internet directory
LDAP Connection success
Writer Initialised!!
MapEngine Initialised!!
Filter Initialised!!
searchF :
CHGLOGFILTER : (&(USNChanged>=28018)(USNChanged<=28022))
Search Time 8
Search Successful till # 28022
Search Changes Done
Changenumber USNChanged: 28022
targetdn distinguishedName: CN=Test User56,CN=Users,DC=US,DC=ORACLE,DC=com
ChangeRecord : ----------
Changetype: 4
ChangeKey: CN=Test User56,CN=Users,DC=US,DC=ORACLE,DC=com
Attributes:
Class: null Name: ou Type: null ChgType: 1 Value: [ ]
Class: null Name: objectGUID Type: null ChgType: 2 Value: [[B@d0a5d9]

...

Class: null Name: mail Type: null ChgType: 1 Value: [ ]
Class: null Name: displayname Type: null ChgType: 2 Value: [Test User56]
Class: null Name: cn Type: null ChgType: 2 Value: [Test User56]
Class: null Name: sn Type: null ChgType: 2 Value: [Test User56]
Class: null Name: krbprincipalname Type: null ChgType: 1 Value: [@ ]
Class: null Name: uid Type: null ChgType: 1 Value: [ ]
Class: null Name: orcluserprincipalname Type: null ChgType: 1 Value: [ ]
Class: null Name: orclsamaccountname Type: null ChgType: 2 Value: [$Test User56]
-----------
DN : CN=Test User56,cn=users,dc=us,dc=oracle,dc=com
Normalized DN : CN=Test User56,cn=users,dc=us,dc=oracle,dc=com
Processing modifyRadd Operation ..
Entry Not Found. Converting to an ADD op..
Processing Insert Operation ..
Performing createEntry..
Entry Added Successfully : CN=Test User56,cn=users,dc=us,dc=oracle,dc=com
Updated Attributes
orclodipLastExecutionTime: 20040608112226
orclOdipSynchronizationStatus: Synchronization Successful
orclodipLastSuccessfulExecutionTime: 20040608112226
```

次に、Microsoft Active Directory コネクタの同期化された削除操作用の、有効なサンプル・トレース・ファイルの最初と終わりの部分を示します。

```
--------------------------------------------------------------------------------
 Trace Log Started at Wed Aug 18 09:10:05 EDT 2004
--------------------------------------------------------------------------------
Command exec succesful
LDAP URL : (sun1.mycompany.com:389 administrator@mycompany.com
LDAP Connection success
Applied ChangeNum : 31940Available chg num = 31940
Reader Initialised !!
LDAP URL : (sun2.mycompany.com:3060 cn=odisrv+orclhostname=sun2,cn=odi,cn=oracle
internet directory
LDAP Connection success
Writer Initialised!!
MapEngine Initialised!!
Filter Initialised!!
searchF :
CHGLOGFILTER : (&(USNChanged>=31941)(USNChanged<=31941))
Search Time 10
Search Successful till # 31941
Search Changes Done
Changenumber USNChanged: 31941
Deleted isDeleted: TRUE
Deleted isDeleted: TRUE
ChangeRecord : ----------
Changetype: 1
ChangeKey: *
Attributes:
Class: null Name: objectGUID Type: null ChgType: 3 Value: [[B@ece65]

...

Output ChangeRecord ChangeRecord : ----------
Changetype: 1
ChangeKey: *
Attributes:
Class: null Name: objectclass Type: null ChgType: 3 Value: [organizationalunit,
orclcontainer, orcladuser, orcluserv2, orcladgroup]
Class: null Name: krbprincipalname Type: null ChgType: 3 Value: [@ ]
Class: null Name: orclsamaccountname Type: null ChgType: 3 Value: [$ ]
Class: null Name: orclobjectguid Type: null ChgType: 3 Value:
[2xR7Nas8UUKtzmPk0jpSFg==]
-----------
DN : *
Normalized DN : cn=TUser2007,cn=users,dc=us,dc=oracle,dc=com
Processing Delete Operation ..
Deleted entry Successfully : cn=TUser2007,cn=users,dc=us,dc=oracle,dc=com
Updated Attributes
orclodipLastExecutionTime: 20040818091005
orclOdipSynchronizationStatus: Synchronization Successful
orclodipLastSuccessfulExecutionTime: 20040818091005
```

次に、Microsoft Active Directory コネクタの同期化された変更操作用の、有効なサンプル・トレース・ファイルの最初と終わりの部分を示します。

```
--------------------------------------------------------------------------------
 Trace Log Started at Wed Sep 29 09:40:18 EDT 2004
--------------------------------------------------------------------------------
Command exec succesful
LDAP URL : (server.mycompany.com:389 administrator@mycompany.com
LDAP Connection success
Applied ChangeNum : 35322Available chg num = 35322
Reader Initialised !!
LDAP URL : (sun2.mycompany.com:3060 cn=odisrv+orclhostname=sun2,cn=odi,cn=oracle
internet directory
LDAP Connection success
Writer Initialised!!
MapEngine Initialised!!
Filter Initialised!!
searchF :
CHGLOGFILTER : (&(USNCreated>=35323)(USNCreated<=35323))
Search Time 7
Search Successful till # 35323
Search Changes Done
searchF :
CHGLOGFILTER : (&(USNChanged>=35323)(USNChanged<=35323)(USNCreated<=35322))
Search Time 15
Search Successful till # 35323
Changenumber USNChanged: 35323
targetdn distinguishedName: CN=Test User111,CN=Users,DC=US,DC=ORACLE,DC=com
ChangeRecord : ----------
Changetype: 4
ChangeKey: CN=Test User111,CN=Users,DC=US,DC=ORACLE,DC=com
Attributes:
Class: null Name: distinguishedname Type: null ChgType: 1 Value: [ ]
Class: null Name: samaccountname,userprincipalname Type: null ChgType: 1 Value: [ ]
Class: null Name: userprincipalname Type: null ChgType: 1 Value: [ ]

...

 Output ChangeRecord ChangeRecord : ----------
Changetype: 4
ChangeKey: cn=TUser111,cn=users,dc=us,dc=oracle,dc=com
Attributes:
Class: null Name: objectclass Type: null ChgType: 3 Value: [orcluserv2, orcladuser,
inetorgperson, person]
Class: null Name: orclObjectSID Type: null ChgType: 2 Value:
[AQUAAAAAAAUVAAAAiqcyP8CFOF0VJa9HCAYAAA==]
Class: null Name: orclObjectGUID Type: null ChgType: 2 Value:
[6uEo05+F/0CHj4PTpPCchQ==]
Class: null Name: mail Type: null ChgType: 2 Value: [Tuser111@oracle.com]
Class: null Name: displayName Type: null ChgType: 2 Value: [Test User111]
Class: null Name: cn Type: null ChgType: 2 Value: [TUser111]
Class: null Name: sn Type: null ChgType: 2 Value: [TUser111]
Class: null Name: krbPrincipalName Type: null ChgType: 1 Value: [@ ]
Class: null Name: uid Type: null ChgType: 2 Value: [TUser111]
Class: null Name: orclUserPrincipalName Type: null ChgType: 1 Value: [ ]
Class: null Name: orclSAMAccountName Type: null ChgType: 2 Value: [$TUser111]
Class: null Name: orclDefaultProfileGroup Type: null ChgType: 1 Value: [ ]
-----------
DN : cn=TUser111,cn=users,dc=us,dc=oracle,dc=com
Normalized DN : cn=TUser111,cn=users,dc=us,dc=oracle,dc=com
Processing modifyRadd Operation ..
Entry found. Converting To a Modify Operation..
Proceeding with checkNReplace..
```

```
Performing checkNReplace..
Naming attribute: cn
Naming attribute value: orclDefaultProfileGroup
Naming attribute value: orclSAMAccountName
Naming attribute value: orclUserPrincipalName
Naming attribute value: uid
Naming attribute value: krbPrincipalName
Naming attribute value: sn
Naming attribute value: cn
Naming attribute value: displayName
Naming attribute value: mail
Adding Attribute in OID : mail
Naming attribute value: orclObjectGUID
Naming attribute value: orclObjectSID
Total # of Mod Items : 1
Modified Entry Successfully : cn=TUser111,cn=users,dc=us,dc=oracle,dc=com
Replacing Attribute orclodipLastSuccessfulExecutionTime in the Profile with value :
20040929094018
Removed Existing attribute
RePopulated Attribute..
Updated Attributes
orclodipLastExecutionTime: 20040929094018
orclOdipSynchronizationStatus: Synchronization Successful
orclodipLastSuccessfulExecutionTime: 20040929094018
```

Microsoft Active Directory との統合に関するトラブルシューティング

この項では、Microsoft Active Directory との統合に関する問題をトラブルシューティングする方法について説明します。内容は次のとおりです。

- Windows ネイティブ認証のデバッグ
- Oracle Internet Directory の使用不可期間後の変更の同期

Windows ネイティブ認証のデバッグ

Windows ネイティブ認証を構成すると（19-7 ページの「Windows ネイティブ認証の構成」を参照）、実行時にこの機能のロギングを有効にできます。*$ORACLE_HOME*/opmn/conf にある opmn.xml ファイルを開き、次のパラメータを追加します。

```
-Djazn.debug.log.enable = {true | false}
```

パラメータに `true` の値を指定するとデバッグが有効になり、`false` の値を指定すると無効になります。

次の例の太字は、opmn.xml ファイルでパラメータを置く位置を示しています。

```
<process-type id="OC4J_SECURITY" module-id="OC4J">
  <environment>
    <variable id="DISPLAY" value="sun1.us.oracle.com:0.0"/>
    <variable id="LD_LIBRARY_PATH" value="/private/ora1012/OraHome1/lib"/>
  </environment>
  <module-data>
    <category id="start-parameters">
      <data id="java-options" value="-server -Djazn.debug.log.enable=true
      -Djava.security.policy=/private/ora1012/OraHome1/j2ee/OC4J_SECURITY/
      config/java2.policy -Djava.awt.headless=true -Xmx512m
      -Djava.awt.headless=true"/>
      <data id="oc4j-options" value="-properties"/>
    </category>
    <category id="stop-parameters">
      <data id="java-options" value="-Djava.security.policy=/private/ora1012/
      OraHome1/j2ee/OC4J_SECURITY/config/java2.policy  -Djava.awt.headless=true"/>
    </category>
```

ログは、*$ORACLE_HOME*/opmn/logs にある OC4J~OC4J_SECURITY~default_island~1 ファイルに書き込まれます。

関連資料： Oracle*MetaLink* Note: 283268.1: 「Troubleshooting Oracle Application Server Single Sign-On Windows Native Authentication」（Oracle*MetaLink*（`http://metalink.oracle.com/`）で参照可能）

注意： 保護されたアプリケーションに Windows ネイティブ認証でアクセスすると、Web ブラウザは「401 - Unauthorized」エラーを自動的に返します。このエラーは Oracle Enterprise Manager によって記録されます。これは通常の動作で、無視してもかまいません。

Oracle Internet Directory の使用不可期間後の変更の同期

Oracle Internet Directory が使用できないとき、変更は Microsoft Active Directory に格納されます。Oracle Password Filter for Microsoft Active Directory は、Oracle Internet Directory との接続が復元された後にこれらのエントリを同期化しようとします。`SearchDeltaSize` パラメータにより、同期サイクルの各反復中に処理される増分変更数が決まります。デフォルトでは、`SearchDeltaSize` パラメータに 500 の値が割り当てられています。Oracle Internet Directory が使用できない期間の長さによっては、`SearchDeltaSize` のデフォルト値 500 は、同期化されていない変更すべてを取り込むには低すぎる場合があります。この問題を解決するには、既存の Microsoft Active Directory のインポート同期プロファイルをコピーし、`SearchDeltaSize` パラメータに指定されている値を変更して、遡及プロファイルを作成する必要があります。

遡及同期プロファイルを作成するには、次のようにします。

1. 4-8 ページの「Oracle Directory Integration Platform の起動、停止および再起動」の指示に従い、Oracle Directory Integration Platform を停止します。
2. 次のコマンドを使用して、Microsoft Active Directory のインポート同期プロファイルを無効にします。

   ```
   $ORACLE_HOME/bin/dipassistant modifyprofile -host host -port port
   -file import.profile -dn bind_DN -passwd password_of_bind_DN
   -profile profile_name odip.profile.status=DISABLE
   ```

3. 次のコマンドを使用して Microsoft Active Directory のインポート同期プロファイルをコピーし、遡及同期プロファイルを作成します。

   ```
   $ORACLE_HOME/bin/dipassistant createprofilelike -h host -p port -U ssl_mode -D
   bindDN -w password -profile orig_profile_name -newprofile catchup_profile_name
   ```

4. 次のコマンドを使用して、元の Microsoft Active Directory のインポート同期プロファイルを有効にします。

   ```
   $ORACLE_HOME/bin/dipassistant modifyprofile -h host -p port
   -file import.profile -dn bind_DN -passwd password_of_bind_DN
   -profile profile_name odip.profile.status=ENABLE
   ```

5. 4-8 ページの「Oracle Directory Integration Platform の起動、停止および再起動」の指示に従い、Oracle Directory Integration Platform を起動します。
6. 新しいドメイン・コントローラのルート DSE で、現行の最大の `USNChanged` 値（ルート DSE の `highestCommittedUSN` 属性の属性値）を検索することにより、`highestCommittedUSN` の現行値を取得します。

   ```
   ldapsearch -h host -p port -b "" -s base -D user
   DN -w password "objectclass=*" highestCommittedUSN
   ```

7. 100 超のエントリ（ただし 200 未満）を取得するまで、次の ldapsearch コマンドを試行します。200 超のエントリを取得すると、内部バッファのオーバーランを招くことがあります。

```
ldapsearch -v -h adhost -p adport -D administrator@domain -w password
-b cn=users,dc=acme,dc=com -s sub
"(&(objectclass=*)(usnChanged>=delta)(&(usnChanged<=highestCommittedUSN)))" dn
```

たとえば、次のコマンドにより、デフォルトの検索デルタ・サイズ 500 を使用して検索を実行します。

```
ldapsearch -v -h adhost -p adport -D administrator@domain -w password
-b cn=users,dc=acme,dc=com -s sub
"(&(objectclass=*)(usnChanged>=55010)(&(usnChanged<=55510)))" dn
```

8. 次の内容を指定した profile_config.txt というテキスト・ファイルを作成します。

```
[INTERFACEDETAILS]
Package: gsi
Reader: ActiveChgReader
SkipErrorToSyncNextChange: true
SearchDeltaSize: 100000
```

> **注意：** SkipErrorToSyncNextChange パラメータを設定して、同期中に変更を処理するときに Oracle Directory Integration Platform でエラーを処理する方法を決定することもできます。詳細は、6-4 ページの「SkipErrorToSyncNextChange パラメータ」を参照してください。

9. 次のコマンドを使用して、profile_config.txt ファイルを遡及同期プロファイルにロードします。

```
dipassistant modifyprofile -h oidhost -port oidport -dn cn=orcladmin
-passwd password -profile catchup_profile_name
odip.profile.configfile=path/profile_config.txt
```

10. 次のコマンドを使用して、遡及同期プロファイルを有効にします。

```
$ORACLE_HOME/bin/dipassistant modifyprofile -host host -port port
-file import.profile -dn bind_DN -passwd password_of_bind_DN
-profile catchup_profile_name odip.profile.status=ENABLE
```

> **注意：** 元の Microsoft Active Directory のインポート同期プロファイルが遡及同期プロファイルとともに実行され続けていることを確認してください。

11. 遡及同期プロファイルを 12 時間以上実行して、$*ORACLE_HOME*/ldap/odi/log/*catchup_profile_name*.aud ファイルを監視します。バックログされた変更がすべて同期化された後、次のコマンドを使用して遡及同期プロファイルを無効にします。

```
$ORACLE_HOME/bin/dipassistant modifyprofile -host host -port port
-file import.profile -dn bind_DN -passwd password_of_bind_DN
-profile catchup_profile_name odip.profile.status=DISABLE
```

それでも解決しない場合

Oracle *MetaLink*（`http://metalink.oracle.com`）で、さらに多くの解決策を見つけることができます。問題の解決策が見つからない場合は、オラクル社カスタマ・サポート・センターに問い合せてください。

関連資料： Oracle Application Server のリリース・ノート。
Oracle Technology Network
（`http://www.oracle.com/technology/documentation/index.html`）
で入手可能。

用語集

ACI

「アクセス制御情報項目」を参照。

ACL

「アクセス制御リスト」を参照。

ACP

「アクセス制御ポリシー・ポイント」を参照。

API

「Application Program Interface」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。

ASR

「Oracle Database アドバンスト・レプリケーション」を参照。

configset

「構成設定エントリ」を参照。

DES

「データ暗号化規格」を参照。

DIB

「ディレクトリ情報ベース」を参照。

Directory Integration Server

Oracle Directory Integration Platform 環境で、Oracle Internet Directory と接続ディレクトリとの間でデータの同期化を実行するサーバー。

DIS

「Directory Integration Server」を参照。

DIT

「ディレクトリ情報ツリー」を参照。

DN

「識別名」を参照。

DRG

「ディレクトリ・レプリケーション・グループ」を参照。

DSA

「ディレクトリ・システム・エージェント」を参照。

DSE

「ディレクトリ固有のエントリ」を参照。

Global Unique Identifier（GUID）

エントリがディレクトリに追加されると、システムで生成され、エントリに挿入される識別子。マルチマスター・レプリケート環境で、DN ではなく GUID がエントリを一意に識別する。エントリの GUID をユーザーが変更することはできない。

GUID

「Global Unique Identifier」を参照。

ID 管理（identity management）

組織でネットワーク・エンティティのセキュリティ・ライフ・サイクル全体を管理するプロセス。通常、組織のアプリケーション・ユーザーの管理を指す。セキュリティ・ライフ・サイクルの手順には、アカウント作成、一時停止、権限変更およびアカウント削除が含まれる。管理されるネットワーク・エンティティには、デバイス、プロセス、アプリケーション、またはネットワーク環境で対話する必要があるその他のすべてのものが含まれる。ID 管理プロセスで管理されるエンティティには、組織外のユーザー（顧客、取引先、Web サービスなど）も含まれる。

ID 管理レルム（identity management realm）

すべてが同じ管理ポリシーによって管理されている識別情報の集合。企業では、イントラネットへのアクセス権限を所有しているすべての従業員は 1 つのレルムに属し、企業の公開アプリケーションにアクセスするすべての外部ユーザーは別のレルムに属する。ID 管理レルムは、特別なオブジェクト・クラスが関連付けられた特定のエントリでディレクトリ内に表される。

ID 管理レルム固有の Oracle コンテキスト（identity management realm-specific Oracle Context）

各 ID 管理レルムに含まれた Oracle コンテキスト。これには、次の情報が格納されている。

- ID 管理レルムのユーザー・ネーミング・ポリシー（ユーザーに名前を付け、配置する方法）
- 必須認証属性
- ID 管理レルム内のグループの場所
- ID 管理レルムに対する権限の割当て（レルムにユーザーを追加する権限の割当てなど）
- レルムに関するアプリケーション固有のデータ（認可など）

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」を参照。

LDAP Data Interchange Format（LDIF）

LDAP コマンドライン・ユーティリティに使用する入力ファイルの形式を設定するための一連の規格。

LDIF

「**LDAP Data Interchange Format**」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 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ある。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**」を参照。

MTS

「**共有サーバー**」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**のプロセスによって解析され、実行される。

OID データベース・パスワード・ユーティリティ（OID Database Password Utility）

Oracle Internet Directory が Oracle データベースに接続するときのパスワードの変更に使用されるユーティリティ。

OID モニター（OID Monitor）

Oracle ディレクトリ・サーバー・プロセスの開始、監視および終了を実行する Oracle Internet Directory のコンポーネント。レプリケーション・サーバー（インストールされている場合）および Oracle Directory Integration Server の制御も行う。

Oracle Call Interface（OCI）

Application Program Interface（API）の 1 つ。これにより、第三世代言語のネイティブ・プロシージャやファンクション・コールを使用して、Oracle データベース・サーバーにアクセスし、SQL 文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 Database アドバンスト・レプリケーション（Oracle Database Advanced Replication）

2 つの Oracle データベース間で、データベースの表を継続的に同期化できる Oracle Database の機能。

Oracle Delegated Administration Services

Oracle Delegated Administration Services ユニットと呼ばれる個々の事前定義済サービスのセットで、ユーザーのかわりにディレクトリ操作を実行する。Oracle Internet Directory セルフ・サービス・コンソールによって、Oracle Internet Directory を使用する Oracle アプリケーションおよびサードパーティ・アプリケーションの両方の管理ソリューションを容易に開発および配布できる。

Oracle Directory Integration Platform

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

Oracle Directory Integration Platform 環境で、Oracle Internet Directory の変更イベントを監視し、**ディレクトリ統合プロファイル**の情報に基づいてアクションを行うデーモン・プロセス。

Oracle Directory Manager

Oracle Internet Directory を管理するための、Graphical User Interface（GUI）を備えた Java ベースのツール。

Oracle Enterprise Manager

Oracle 製品の 1 つ。グラフィカルなコンソール、エージェント、標準的なサービスおよびツールを組合せ、Oracle 製品を管理するための統合された包括的なシステム管理プラットフォームを提供する。

Oracle Identity Management

すべての企業識別情報および企業内の様々なアプリケーションへのアクセスを集中的かつ安全に管理するための配置を可能にするインフラストラクチャ。

Oracle Internet Directory

分散ユーザーやネットワーク・リソースに関する情報の検索を可能にする、汎用のディレクトリ・サービス。LDAP バージョン 3 と Oracle Database の高度のパフォーマンス、スケーラビリティ、耐久性および可用性を組み合せたもの。

Oracle 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 証明書使用条件（Oracle PKI certificate usages）

証明書でサポートされる Oracle アプリケーション・タイプを定義する。

Oracle Wallet Manager

セキュリティ管理者が、クライアントとサーバー上での公開鍵セキュリティ資格証明の管理に使用する Java ベースのアプリケーション。

peer-to-peer レプリケーション（peer-to-peer replication）

マルチマスター・レプリケーションまたは n-way レプリケーションとも呼ばれる。同等に機能する複数サイトがレプリケートされたデータのグループを管理できるようにするレプリケーションのタイプ。このようなレプリケーション環境では、各ノードはサプライヤ・ノードであると同時にコンシューマ・ノードであり、各ノードでディレクトリ全体がレプリケートされる。

PKCS #12

公開鍵暗号規格（PKCS）。RSA Data Security, Inc. の PKCS #12 は、個人的な認証資格証明を、通常**ウォレット**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。

point-to-point レプリケーション（point-to-point replication）

ファンアウト・レプリケーション（fan-out replication）とも呼ばれる。サプライヤがコンシューマに直接レプリケートするレプリケーションのタイプ。コンシューマは 1 つ以上の他のコンシューマにレプリケートできる。レプリケーションには、完全レプリケーションと部分レプリケーションがある。

RDN

「**相対識別名**」を参照。

SASL

「**Simple Authentication and Security Layer**」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 よりも若干速度が遅くなるが、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る。

Secure Sockets Layer（SSL）

ネットワーク接続を保護するために Netscape Communications Corporation が開発した業界標準プロトコル。SSL では公開鍵インフラストラクチャ（PKI）を使用して、認証、暗号化およびデータ整合性を実現している。

SGA

「**システム・グローバル領域**」を参照。

SHA

「**Secure Hash Algorithm**」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、以降のプロトコル対話に使用するセキュリティ・レイヤーを規定す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**」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る特定のタイプの**サブエントリ**。

TLS

「**Transport Layer Security**」を参照。

Transport Layer Security（TLS）

インターネット上の通信プライバシを提供するプロトコル。このプロトコルによって、クライアント / サーバー・アプリケーションは、通信時の盗聴、改ざんまたはメッセージの偽造を防止できる。

Unicode

汎用キャラクタ・セットのタイプ。16 ビットの領域にエンコードされた 64,000 個の文字の集合。既存のほとんどのキャラクタ・セット規格の文字をほとんどすべてエンコードする。世界中で使用されているほとんどの記述法を含む。Unicode は Unicode Inc. によって所有および定義される。Unicode は標準的なエンコーディングであり、異なるロケールで値を伝達できることを意味する。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。以前から広くグリニッジ標準時（GMT）または世界時と呼ばれており、UTC は名目上は地球の子午線に沿った平均太陽時を表す。UTC 形式である場合、値の最後に z が示される（例 : 200011281010z）。

UTF-16

Unicode の 16 ビット・エンコーディング。Latin-1 文字は、この規格の最初の 256 コード・ポイントである。

UTF-8

文字ごとに連続した 1、2、3 または 4 バイトを使用する **Unicode** の可変幅 8 ビット・エンコーディング。0 ～ 127 の文字（7 ビット ASCII 文字）は 1 バイトでエンコードされ、128 ～ 2047 の文字では 2 バイト、2048 ～ 65535 の文字では 3 バイト、65536 以上の文字は 4 バイトを必要とする。このための Oracle キャラクタ・セット名は AL32UTF8（Unicode 3.1 規格用）となる。

X.509

公開鍵の署名に使用される ISO の一般的な形式。

アクセス制御情報項目（Access Control Information Item: ACI）

どのディレクトリ・データに対して、誰がどのタイプのアクセス権限を持っているかを判断する属性。この属性には、エントリに関係する構造型アクセス項目と、属性に関係するコンテント・アクセス項目に関する 1 組の規則が含まれている。両方のアクセス項目に対するアクセス権限を、1 つ以上のユーザーまたはグループに付与できる。

アクセス制御ポリシー・ポイント（Access Control Policy Point: ACP）

セキュリティ・ディレクティブを含むエントリ。このディレクティブは、**ディレクトリ情報ツリー**内のすべての下位エントリに適用される。

アクセス制御リスト（Access Control List: ACL）

アクセス・ディレクティブのグループ。管理者が定義する。ディレクティブは、特定のクライアントまたはクライアントのグループ、あるいはその両方に対して、特定データへのアクセスのレベルを付与する。

アドバンスト・レプリケーション（Advanced Replication: AR）

「**Oracle Database アドバンスト・レプリケーション**」を参照。

暗号化（cryptography）

データのエンコードとデコードを行い、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）に変換する処理。

暗号スイート（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暗号スイートを確認する。

一方向関数（one-way function）

一方向への計算は容易だが、逆の計算（反対方向への計算）は非常に難しい関数。

一方向ハッシュ関数（one-way hash function）

可変サイズの入力を取得して、固定サイズの出力を作成する**一方向関数**。

一致規則（matching rule）

検索または比較操作における、検索対象の属性値と格納されている属性値との間の等価性の判断。たとえば、`telephoneNumber` 属性に関連付けられた一致規則では、(650) 123-4567 を (650) 123-4567 または 6501234567 のいずれか、あるいはその両方と一致させることができる。属性の作成時に、その属性を一致規則と対応付けることができる。

委任管理者（delegated administrator）

ホスティングされた環境では、アプリケーション・サービス・プロバイダなどの 1 企業が、他の複数の企業に Oracle コンポーネントを使用可能にして、それらの企業の情報を格納する。この種の環境では、グローバル管理者はディレクトリ全体にまたがるアクティビティを実行する。委任管理者と呼ばれる他の管理者は、特定の ID 管理レルムで、または特定のアプリケーションに対してロールを実行できる。

インスタンス（instance）

「**ディレクトリ・サーバー・インスタンス**」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**によってインポートされたデータを格納するファイル。

ウォレット（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、ウォレットの場所を特定するために必要な情報をすべて提供する。

エクスポート・エージェント（export agent）

Oracle Directory Integration Platform 環境で、Oracle Internet Directory からデータをエクスポートするエージェント。

エクスポート・データ・ファイル（export data file）

Oracle Directory Integration Platform 環境で、**エクスポート・エージェント**によってエクスポートされたデータを格納するファイル。

エクスポート・ファイル（export file）

「**エクスポート・データ・ファイル**」を参照。

エントリ（entry）

ディレクトリの基本単位で、ディレクトリ・ユーザーに関係のあるオブジェクトに関する情報が含まれている。

オブジェクト・クラス（object class）

名前を持った属性のグループ。属性をエントリに割り当てるときは、その属性を保持しているオブジェクト・クラスをそのエントリに割り当てる。

同じオブジェクト・クラスに関連するオブジェクトはすべて、同じ属性を共有する。

介在者（man-in-the-middle）

第三者によるメッセージの不正傍受などのセキュリティ攻撃。第三者、つまり介在者は、メッセージを復号化して再暗号化し（元のメッセージを変更する場合と変更しない場合がある）、元のメッセージの宛先である受信者に転送する。これらの処理はすべて、正当な送受信者が気付かないうちに行われる。この種のセキュリティ攻撃は、**認証**が行われていない場合にのみ発生する。

外部エージェント（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）

公開鍵とそれに対応する**秘密鍵**のペア。

「**公開鍵と秘密鍵のペア**」を参照。

仮想 IP アドレス（virtual IP address）

Oracle Application Server Cold Failover Cluster（Infrastructure）では、各物理ノードには独自の物理 IP アドレスと物理ホスト名が割り振られる。単一のシステムであるというイメージを外部に示すために、クラスタは、クラスタ内のどの物理ノードにも変更できる動的 IP アドレスを使用する。これは、仮想 IP アドレスと呼ばれる。

仮想ホスト名（virtual host name）

Oracle Application Server Cold Failover Cluster（Infrastructure）で、仮想 IP アドレスに対応するホスト名。

簡易認証（simple authentication）

ネットワークでの送信時に暗号化されない識別名とパスワードを使用して、クライアントがサーバーに対して自己認証を行うプロセス。簡易認証オプションでは、クライアントが送信した識別名とパスワードと、ディレクトリに格納されている識別名とパスワードが一致していることをサーバーが検証する。

管理領域（administrative area）

ディレクトリ・サーバー上の 1 つのサブツリー。そのエントリは、1 つの管理認可レベル（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、サポートできるユーザー数が増える。共有サーバー構成では、多数のユーザー・プロセスがディスパッチャに接続する。ディスパッチャは、複数の着信ネットワーク・セッション・リクエストを共通キューに送る。サーバー・プロセスの共有プールでアイドル状態である共有サーバー・プロセスが、共通キューからリクエストを取り出す。これは、サーバー・プロセスの小規模プールで大量のクライアントを処理できることを意味する。専用サーバーと対比。

クラスタ（cluster）

単一のコンピューティング・リソースとして使用される、相互接続されたコンピュータの集合。ハードウェア・クラスタによって、高可用性およびスケーラビリティが実現する。

グループ検索ベース（group search base）

Oracle Internet Directory のデフォルトのディレクトリ情報ツリーで、すべてのグループを検索できる ID 管理レルムのノード。

グローバル管理者（global administrator）

ホスティングされた環境では、アプリケーション・サービス・プロバイダなどの 1 企業が、他の複数の企業に Oracle コンポーネントを使用可能にして、それらの企業の情報を格納する。この種の環境では、グローバル管理者はディレクトリ全体にまたがるアクティビティを実行する。

継承（inherit）

オブジェクト・クラスが別のクラスから導出されたときに、導出元のオブジェクト・クラスの多数の特性も導出（継承）されること。同様に、属性のサブタイプも、そのスーパータイプの特性を継承する。

ゲスト・ユーザー（guest user）

匿名ユーザーではなく、特定のユーザー・エントリも持っていないユーザー。

コールド・バックアップ（cold backup）

データベース・コピー・プロシージャを使用して、新規 **DSA** ノードを既存のレプリケート・システムに追加する手順。

公開鍵（public key）

公開鍵暗号において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**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・コンテキストのルートの **DN**。

サービス時間（service time）

リクエストの開始から、そのリクエストに対するレスポンスの完了までの時間。

サブエントリ（subentry）

サブツリー内のエントリ・グループに適用可能な情報が含まれているエントリのタイプ。情報には次の 3 つのタイプがある。

- アクセス制御ポリシー・ポイント
- スキーマ規則
- 共通属性

サブエントリは、管理領域のルートのすぐ下に位置している。

サブクラス（subclass）

別のオブジェクト・クラスから導出されたオブジェクト・クラス。導出元のオブジェクト・クラスは、その**スーパークラス**と呼ばれる。

サブスキーマ DN（subschema DN）

独立したスキーマ定義を持つディレクトリ情報ツリー領域のリスト。

サブタイプ（subtype）

オプションを持たない同じ属性に対して、1 つ以上のオプションを持つ属性。たとえば、American English をオプションとして持つ commonName（cn）属性は、そのオプションを持たない commonName（cn）属性のサブタイプである。逆に、オプションを持たない commonName（cn）属性は、オプションを持つ同じ属性の**スーパータイプ**である。

サプライヤ（supplier）

レプリケーションにおいて、ネーミング・コンテキストのマスター・コピーを保持しているサーバー。マスター・コピーから**コンシューマ**・サーバーに更新を供給する。

参照（referral）

ディレクトリ・サーバーがクライアントに提供する情報。リクエストする情報を見つけるためにクライアントが接続する必要がある他のサーバーを示す。

「**ナレッジ参照**」も参照。

識別名（distinguished name: DN）

ディレクトリ・エントリの一意名。親エントリの個々の名前がすべて、下からルート方向へ順に結合されて構成されている。

思考時間（think time）

ユーザーが実際にプロセッサを使用していない時間。

システム・グローバル領域（System Global Area: SGA）

共有メモリー構造の 1 グループ。1 つの Oracle データベース・インスタンスに関するデータと制御情報が含まれている。複数のユーザーが同じインスタンスに同時に接続した場合、そのインスタンスの SGA 内のデータはユーザー間で共有される。したがって、SGA は共有グローバル領域と呼ばれることもある。バックグラウンド・プロセスとメモリー・バッファの組合せは、Oracle インスタンスと呼ばれる。

システム固有のエージェント（native agent）

Oracle Directory Integration Platform 環境において、**Directory Integration Server** の制御下で実行されるエージェント。**外部エージェント**とは対照的。

システム操作属性（system operational attribute）

ディレクトリ自体の操作に関係する情報を保持する属性。一部の操作情報は、サーバーを制御するためにディレクトリによって指定される（例：エントリのタイムスタンプ）。アクセス情報などのその他の操作情報は、管理者が定義し、ディレクトリ・プログラムの処理時に、そのプログラムによって使用される。

従属参照（subordinate reference）

エントリの直下から始まるネーミング・コンテキストまで、ディレクトリ情報ツリー内で下位方向を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、参照側の 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 まで、上位方向を指し示すナレッジ参照。

証明書（certificate）

公開鍵に対して識別情報を安全にバインドする ITU x.509 v3 の標準データ構造。証明書は、エンティティの公開鍵が、信頼できる機関（**認証局**）によって署名されたときに作成される。この証明書は、そのエンティティの情報が正しいこと、および公開鍵がそのエンティティに実際に属していることを保証する。

証明連鎖（certificate chain）

エンド・ユーザーまたはサブスクライバの証明書とその認証局の証明書を含む、順序付けられた証明書のリスト。

信頼できる証明書（trusted certificate）

一定の信頼度を有すると認定された第三者の識別情報。信頼できる証明書は、識別情報の内容がそのエンティティと一致していることを検証するときに使用される。一般的に、信頼されている認証局によってユーザーの証明書が発行される。

スーパークラス（superclass）

別のオブジェクト・クラスが導出される元のオブジェクト・クラス。たとえば、オブジェクト・クラス `person` は、オブジェクト・クラス `organizationalPerson` のスーパークラスである。後者の `organizationalPerson` は、`person` の**サブクラス**であり、`person` に含まれている属性を継承する。

スーパータイプ（supertype）

1 つ以上のオプションを持つ同じ属性に対して、オプションを持たない属性。たとえば、オプションを持たない `commonName`（`cn`）属性は、オプションを持つ同じ属性のスーパータイプである。逆に、American English をオプションとして持つ `commonName`（`cn`）属性は、そのオプションを持たない `commonName`（`cn`）属性の**サブタイプ**である。

スーパー・ユーザー（super user）

一般的には、ディレクトリ情報へのあらゆるアクセスが可能な特別なディレクトリ管理者。

スキーマ（schema）

属性、オブジェクト・クラスおよびそれらに対応する一致規則の集合。

スケーラビリティ（scalability）

使用可能なハードウェア・リソースに比例して、そのハードウェア・リソースによってのみ制限されるスループットを提供するシステムの機能。

スポンサ・ノード（sponsor node）

レプリケーションにおいて、新規ノードに初期データを設定するために使用されるノード。

スマート・ナレッジ参照（smart knowledge reference）

ナレッジ参照エントリが検索の有効範囲内にあるときに返される**ナレッジ参照**。リクエストされた情報を格納しているサーバーを示す。

スループット（throughput）

Oracle Internet Directory が単位時間ごとに処理するリクエストの数。通常、操作 / 秒（1 秒当たりの操作件数）で表される。

スレーブ（slave）

「コンシューマ」を参照。

整合性（integrity）

受信メッセージの内容が、元の送信メッセージの内容から変更されていないことの保証。

セカンダリ・ノード（secondary node）

Oracle Application Server Cold Failover Cluster（Infrastructure）で、フェイルオーバー時にアプリケーションが移動される先のクラスタ・ノード。

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中に使用される、対称鍵暗号方式の鍵。

接続記述子（connect descriptor）

特別に書式が設定された、ネットワーク接続の接続先の説明。接続記述子には、宛先サービスとネットワーク・ルート情報が含まれる。

宛先サービスを示すには、その Oracle Database に対応するサービス名、あるいは Oracle リリース 8.0 またはバージョン 7 のデータベースに対応する Oracle システム識別子（SID）を使用する。ネットワーク・ルートは、少なくとも、ネットワーク・アドレスによってリスナーの場所を提供する。

接続ディレクトリ（connected directory）

Oracle Directory Integration Platform 環境で、それ自体（たとえば、Oracle Human Resource データベース）と Oracle Internet Directory との間で完全なデータの同期が必要な情報リポジトリ。

相対識別名（relative distinguished name: RDN）

ローカルの最下位レベルのエントリ名。エントリのアドレスを一意に識別するために使用される他の修飾エントリ名は含まれない。たとえば、`cn=Smith,o=acme,c=US` では、`cn=Smith` が相対識別名である。

属性（attribute）

エントリの性質を説明する情報項目。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**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。

属性一意性（attribute uniqueness）

指定した 2 つの属性が同じ値にならないようにする Oracle Internet Directory 機能。企業ディレクトリと同期しているアプリケーションで、属性を一意キーとして使用することを可能にする。

属性構成ファイル（attribute configuration file）

Oracle Directory Integration Platform 環境で、接続ディレクトリの属性を指定するファイル。

属性値（attribute value）

エントリで出現する情報の特定の値。たとえば、jobTitle 属性に対する値には manager がある。

属性のタイプ（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**として機能する。

待機時間（latency）

指定したディレクトリ操作が完了するまでのクライアントの待機時間。待機時間は、空費時間として定義される場合がある。ネットワーク通信では、待機時間は、ソースから宛先へパケットが移動する時間として定義される。

待機時間（wait time）

リクエストの発行からレスポンスの開始までの時間。

単一鍵ペア・ウォレット（single key-pair wallet）

単一のユーザー**証明書**とその関連する**秘密鍵**が含まれる **PKCS #12** 形式の**ウォレット**。**公開鍵**は証明書に埋め込まれている。

中央ディレクトリ（central directory）

Oracle Directory Integration Platform 環境で、中央リポジトリとして機能するディレクトリ。Oracle Directory Integration Platform 環境では、Oracle Internet Directory が中央ディレクトリになる。

データ暗号化規格（Data Encryption Standard: DES）

1970 年代に IBM 社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。

データ整合性（data integrity）

受信メッセージの内容が、元の送信メッセージの内容から変更されていないことの保証。

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付け、異なる内容を格納できる。つまり、内容は DSE を保持するディレクトリに固有のものにできる。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持つエントリである。

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。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**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行方法を記述した特殊な**ディレクトリ統合プロファイル**。

ディレクトリ統合プロファイル（directory integration profile）

Oracle Directory Integration Platform 環境での、Oracle Directory Integration Platform による外部システムとの通信方法および通信内容を示す Oracle Internet Directory のエントリ。

ディレクトリ・ネーミング・コンテキスト（directory naming context）

「ネーミング・コンテキスト」を参照。

ディレクトリ・プロビジョニング・プロファイル（directory provisioning profile）

Oracle Directory Integration Platform がディレクトリ対応アプリケーションに送信するプロビジョニング関連通知の性質を記述した特殊な**ディレクトリ統合プロファイル**。

ディレクトリ・レプリケーション・グループ（directory replication group: DRG）

レプリケーション承諾のメンバーであるディレクトリ・サーバーの集合。

デフォルト ID 管理レルム（default identity management realm）

ホスティングされた環境では、アプリケーション・サービス・プロバイダなどの 1 つの企業が、複数の企業で Oracle コンポーネントを使用できるようにし、それらの企業の情報を格納する。このようなホスティングされた環境では、ホスティングしている企業はデフォルト ID 管理レルムと呼ばれ、ホスティングされている企業はそれぞれディレクトリ情報ツリー内のその企業独自の ID 管理レルムに関連付けられる。

デフォルト・ナレッジ参照（default knowledge reference）

ベース・オブジェクトがディレクトリになく、操作がサーバーによってローカルに保持されていないネーミング・コンテキストで実行されたときに返される**ナレッジ参照**。デフォルト・ナレッジ参照は、一般的にディレクトリ・パーティション化対策についてより多くのナレッジを持つサーバーにユーザーを送信する。

デフォルト・レルムの場所（default realm location）

デフォルト ID 管理レルムのルートを識別するルート Oracle コンテキストでの属性。

同時クライアント数（concurrent clients）

Oracle Internet Directory とのセッションを確立しているクライアントの総数。

同時実行性（concurrency）

複数のリクエストを同時に処理できる機能。同時実行性メカニズムの例には、スレッドおよびプロセスなどがある。

同時操作数（concurrent operations）

すべての同時クライアント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 つの管理側面のうち 1 つが制御される。特定管理領域は、自律型管理領域の一部である。

匿名認証（anonymous authentication）

ディレクトリがユーザー名とパスワードの組合せを要求せずにユーザーを認証するプロセス。各匿名ユーザーは、匿名ユーザー用に指定された権限を行使する。

トラスト・ポイント（trustpoint）

「**信頼できる証明書**」を参照。

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。

ニックネーム属性（nickname attribute）

ディレクトリ全体のユーザーを一意に識別するために使用する属性。この属性のデフォルト値は `uid`。アプリケーションでは、この属性を使用して単純なユーザー名が完全な識別名に変換される。ユーザー・ニックネーム属性は複数値を保持できない。つまり、ユーザーは同じ属性名で格納される複数のニックネームを所有できない。

認可（authorization）

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、信頼できるサード・パーティ。認証局は、ユーザーの識別情報を検証し、認証局の秘密鍵を使用して署名した証明書を発行する。

ネーミング・コンテキスト（naming context）

完全に 1 つのサーバーに常駐しているサブツリー。サブツリーは連続している必要がある。つまり、サブツリーの最上位の役割を果すエントリから始まり、下位方向にリーフ・エントリまたは従属ネーミング・コンテキストへの**ナレッジ参照**（参照とも呼ばれる）まで伸びていく必要がある。単一のエントリからディレクトリ情報ツリー全体までを範囲とすることができる。

ネーミング属性（naming attribute）

Oracle Delegated Administration Services または Oracle Internet Directory Java API を使用して作成した新規ユーザー・エントリの相対識別名を構成するために使用する属性。この属性のデフォルト値は `cn`。

ネット・サービス名（net service name）

接続記述子に変換されるサービスの単純な名前。ユーザーは、接続するサービスに対する接続文字列内のネット・サービス名とともに、ユーザー名とパスワードを渡すことによって、接続リクエストを開始する。次に例を示す。

```
CONNECT username/password@net_service_name
```

必要に応じて、ネット・サービス名は次のような様々な場所に格納できる。

- 各クライアントのローカル構成ファイル（`tnsnames.ora`）
- ディレクトリ・サーバー
- Oracle Names Server
- NDS、NIS、CDS などの外部ネーミング・サービス

パーティション（partition）

一意の重複していないディレクトリ・ネーミング・コンテキスト。1 つのディレクトリ・サーバーに格納されている。

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。

平文（plaintext）

暗号化されていないメッセージ・テキスト。

ファンアウト・レプリケーション（fan-out replication）

point-to-point レプリケーションとも呼ばれる。サプライヤがコンシューマに直接レプリケートするレプリケーションのタイプ。コンシューマは 1 つ以上の他のコンシューマにレプリケートできる。レプリケーションには、完全レプリケーションと部分レプリケーションがある。

フィルタ（filter）

データ（通常、検索対象のデータ）を限定する方法。フィルタは、`cn=susie smith,o=acme,c=us` のように常に識別名で表される。

フェイルオーバー（failover）

障害を認識し、リカバリする処理。Oracle Application Server Cold Failover Cluster（Infrastructure）では、1 つのクラスタ・ノードで稼働しているアプリケーションは透過的に別のクラスタ・ノードに移行される。この移行時に、クラスタ上のサービスにアクセスするクライアントは一時的に接続できず、フェイルオーバーが完了した後、再接続する必要がある場合がある。

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。

プライマリ・ノード（primary node）

Oracle Application Server Cold Failover Cluster（Infrastructure）で、指定した時刻にアプリケーションが実行されるクラスタ・ノード。

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 内のその情報に対する変更に関係がある。

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」を参照。

変更ログ（change logs）

ディレクトリ・サーバーに加えられた変更を記録するデータベース。

マスター・サイト（master site）

レプリケーションにおいて、マスター定義サイト以外のサイトで、LDAP レプリケーションのメンバーであるサイト。

マスター定義サイト（master definition site: MDS）

レプリケーションにおいて、管理者が構成スクリプトを実行する Oracle Internet Directory のデータベース。

マッピング・ルール・ファイル（mapping rules file）

Oracle Directory Integration Platform 環境で、Oracle Internet Directory 属性と接続ディレクトリの属性との間のマッピングを指定するファイル。

マルチマスター・レプリケーション（multimaster replication）

peer-to-peer または n-way レプリケーションとも呼ばれる。同等に機能する複数のサイトがレプリケートされたデータのグループを管理できるようにするレプリケーションのタイプ。マルチマスター・レプリケーション環境では、各ノードはサプライヤ・ノードであると同時にコンシューマ・ノードであり、各ノードでディレクトリ全体がレプリケートされる。

メタディレクトリ（metadirectory）

企業のすべてのディレクトリ間で情報を共有するディレクトリ・ソリューション。すべてのディレクトリを 1 つの仮想ディレクトリに統合する。集中的に管理できるため、管理コストを削減できる。ディレクトリ間でデータが同期化されるため、企業内のデータに一貫性があり最新であることが保証される。

ユーザー検索ベース（user search base）

Oracle Internet Directory のデフォルトのディレクトリ情報ツリーで、すべてのユーザーが配置される ID 管理レルムのノード。

猶予期間ログイン（grace login）

パスワード期限切れ前の指定された期間内に行われるログイン。

リモート・マスター・サイト（remote master site: RMS）

レプリケート環境におけるマスター定義サイト以外のサイトで、Oracle Database アドバンスト・レプリケーションのメンバーであるサイト。

リレーショナル・データベース（relational database）

構造化されたデータの集合。同一の列のセットを持つ 1 つ以上の行で構成される表にデータが格納される。Oracle では、複数の表のデータを容易にリンクできる。このため、Oracle はリレーショナル・データベース管理システム、すなわち RDBMS と呼ばれる。Oracle はデータを複数の表に格納し、さらに表間の関係を定義できる。このリンクは両方の表に共通の、1 つ以上のフィールドに基づいて行われる。

ルート DSE（root DSE）

「ルート・ディレクトリ固有のエントリ」を参照。

ルート Oracle コンテキスト（Root Oracle Context）

Oracle Identity Management インフラストラクチャでは、ルート Oracle コンテキストは、インフラストラクチャのデフォルト ID 管理レルムへのポインタを含む Oracle Internet Directory のエントリである。単純な名前を指定して ID 管理レルムの場所を特定する方法の詳細も含まれる。

ルート・ディレクトリ固有のエントリ（root directory specific entry）

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**と呼ばれる）に関連する実行時情報が含まれているエントリ。レジストリ・エントリはディレクトリ自体に格納され、対応するディレクトリ・サーバー・インスタンスが停止するまで保持される。

レスポンス時間（response time）

リクエストの発行からレスポンスの完了までの時間。

レプリカ（replica）

ネーミング・コンテキストの個々のコピー。1 つのサーバー内に格納されている。

レプリケーション承諾（replication agreement）

ディレクトリ・レプリケーション・グループ内のディレクトリ・サーバー間におけるレプリケーションの関係を記述する特別なディレクトリ・エントリ。

レルム検索ベース（realm search base）

すべての ID 管理レルムを含むディレクトリ情報ツリー内のエントリを識別するルート Oracle コンテキストでの属性。この属性は、単純なレルム名をディレクトリ内の対応するエントリにマッピングする際に使用される。

論理ホスト（logical host）

Oracle Application Server Cold Failover Cluster（Infrastructure）で、1 つ以上のディスク・グループおよびホスト名と IP アドレスのペア。論理ホストは、クラスタ内の物理ホストにマップされる。この物理ホストは、論理ホストのホスト名と IP アドレスを使用する。

索引

P

S

U

W

あ

い

う

え

す

せ

そ

た

つ

て

と

な

に

は

ひ

ふ

へ

ほ

ま

め

も

ゆ

る

れ

ろ