

HP OpenView Select Identity

Windows 2000 および Windows 2003 上の
Microsoft® Active Directory LDAP サーバー用コネクタ

インストールと設定ガイド

コネクタバージョン : 3.4
Select Identity バージョン : 3.3.1



2005 年 8 月

© 2005 Hewlett-Packard Development Company, L.P.

ご注意

1. 本書に記載した内容は、予告なしに変更することがあります。
2. 当社は、本書に関して特定目的の市場性と適合性に対する保証を含む一切の保証をいたしかねます。
3. 当社は、本書の記載事項の誤り、またはマテリアルの提供、性能、使用により発生した直接損害、間接損害、特別損害、付随的損害または結果損害については責任を負いかねますのでご了承ください。
4. 本製品パッケージとして提供した本書、**CD-ROM**などの媒体は本製品用だけにお使いください。プログラムをコピーする場合はバックアップ用だけにしてください。プログラムをそのままの形で、あるいは変更を加えて第三者に販売することは固く禁じられています。

本書には著作権によって保護される内容が含まれています。本書の内容の一部または全部を著作者の許諾なしに複製、改変、および翻訳することは、著作権法下での許可事項を除き、禁止されています。

All rights are reserved.

Restricted Rights Legend.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company

United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices

© 2005 Hewlett-Packard Development Company, L.P.

本製品には Apache Software Foundation (<http://www.apache.org/>) が開発したソフトウェアが含まれます。Portions Copyright (c) 1999-2003 The Apache Software Foundation. All rights reserved.

Select Identity は Apache Jakarta Project の以下のソフトウェアを使用しています。

- Commons-beanutils
- Commons-collections
- Commons-logging
- Commons-digester
- Commons-httpclient
- Element Construction Set (ecs)
- Jakarta-poi
- Jakarta-regexp
- Logging Services (log4j)

ほかに、Select Identity で使用されているサードパーティ製のソフトウェアには以下がありません。

- SourceForge の JasperReports
- SourceForge の iText (JasperReports 用)
- BeanShell
- Apache XML Project の Xalan
- Apache XML Project の Xerces
- Apache XML Project の Java API for XML Processing
- Apache Software Foundation の SOAP
- SUN Reference Implementation の JavaMail
- SUN Reference Implementation の Java Secure Socket Extension (JSSE)
- SUN Reference Implementation の Java Cryptography Extension (JCE)

- SUN Reference Implementation の JavaBeans Activation Framework (JAF)
- OpenSPML.org の OpenSPML Toolkit
- JGraph の JGraph
- Hibernate.org の Hibernate
- bouncycastle.org の BouncyCastle engine(キーストア管理用)

本製品には Teodor Danciu (<http://jasperreports.sourceforge.net>) が開発したソフトウェアが含まれます。Portions Copyright (C) 2001-2004 Teodor Danciu (teodord@users.sourceforge.net). All rights reserved.

Portions Copyright 1994-2004 Sun Microsystems, Inc. All Rights Reserved.

本製品には the Waveset Technologies, Inc. (www.waveset.com) が開発したソフトウェアが含まれます。Portions Copyright © 2003 Waveset Technologies, Inc. 6034 West Courtyard Drive, Suite 210, Austin, Texas 78730. All rights reserved.

Portions Copyright (c) 2001-2004, Gaudenz Alder. All rights reserved.

Trademark Notices

HP OpenView Select Identity は Hewlett-Packard Development Company, L.P. の商標です。

Microsoft、Windows、Windows ロゴおよび SQL Server は Microsoft Corporation の商標または登録商標です。

Sun ワークステーション、Solaris Operating Environment ソフトウェア、SPARCstation 20 システム、Java テクノロジ、および Sun RPC は Sun Microsystems, Inc. の登録商標または商標です。JavaScript は Sun Microsystems, Inc. の商標で、Netscape により考案および実装されたテクノロジーのライセンス下で使用されます。

本製品には Sun Java Runtime が含まれます。本製品には RSA Security, Inc. にライセンスされたコードが含まれます。IBM にライセンスされた部分は <http://oss.software.ibm.com/icu4j/> で参照できます。

IBM、DB2 Universal Database、DB2、WebSphere、および IBM ロゴは米国およびその他の国における International Business Machines Corporation の商標または登録商標です。

UNIX は The Open Group の登録商標です。

本製品には World Wide Web Consortium が提供するソフトウェアが含まれます。このソフトウェアには xml-apis が含まれます。Copyright © 1994-2000 World Wide Web Consortium, (Massachusetts Institute of Technology, Institute National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. <http://www.w3.org/Consortium/Legal/>

Intel および Pentium は米国およびその他の国における Intel Corporation の商標または登録商標です。

AMD および AMD ロゴは Advanced Micro Devices, Inc. の商標です。

BEA および WebLogic は BEA Systems, Inc. の登録商標です。

VeriSign は VeriSign, Inc. の登録商標です。Copyright © 2001 VeriSign, Inc. All rights reserved.

その他の製品名は各社の商標またはサービスマークであり、ここでの記載は識別のみを目的としています。

原典

本書は『*HP OpenView Select Identity Connector for Microsoft Active Directory LDAP Servers on Windows 2000 and 2003 Installation and Configuration Guide*』 Manufacturing Part No. none (August 2005) を翻訳したものです。

サポート

次の HP OpenView の Web サイトを参照してください。

<http://openview.hp.com/> (英語)

<http://www.hp.com/jp/openview/> (日本語)

これらの Web サイトには、HP OpenView の提供する製品、サービス、サポートについてのお問い合わせ先や詳細が掲載されています。

また、直接以下のサポートサイトをご参照いただくこともできます。

<http://support.openview.hp.com/>

HP OpenView オンライン ソフトウェア サポートは、お客様の問題解決に役立つ機能を提供しています。サポートサイトでは、お客さまのビジネスの運用に役立つ対話形式の技術サポートツールに手早く効率的にアクセスできます。サポートサイトでは次のことが可能です。

- 関心のあるドキュメントを検索する
- サポートケースを登録/トラッキングする
- サポート契約を管理する
- HP サポートの問い合わせ先を調べる
- 利用可能なサービスに関する情報を確認する
- ソフトウェアを利用している他のユーザーとの情報交換
- ソフトウェア トレーニング情報の検索とお申し込み

大部分のサポートには、HP Passport へのユーザー登録とログインが必要です。また、サポート契約が必要な場合もあります。

アクセスレベルに関する詳細は、次の URL で確認してください。

http://support.openview.hp.com/access_level.jsp

HP Passport ID のご登録は、次の URL で行ってください。

<https://passport2.hp.com/hpp/newuser.do> (英語)

目次

第 1 章	コネクタのインストール	9
	システム要件	11
	Web アプリケーションサーバーでの配布	12
	セキュア LDAP の使用	14
第 2 章	コネクタの設定	19
	国際化サポート	19
	コネクタの配布	21
第 3 章	マッピングファイルの概要	27
	概説	28
	Active Directory LDAP のマッピング情報	32
第 4 章	コネクタのアンインストール	35
	WebLogic からの削除	35
	WebSphere からの削除	36

コネクタのインストール

Active Directory LDAP コネクタを使用すると、HP OpenView Select Identity は、Windows Active Directory LDAP サーバーに対してさまざまな操作が行えます。このコネクタは、LDAP とのデータの交換に JNDI (LDAP リソースプロバイダインタフェース) を使用しています。

Active Directory LDAP コネクタを使用することによって行える操作は、次のとおりです。

- ユーザーの追加、更新、および削除
- ユーザー属性の取得
- ユーザーの有効化と無効化
- ユーザーの存在の確認
- ユーザーパスワードの変更
- ユーザーパスワードのリセット
- すべてのエンタイトルメントの取得
- 利用可能なユーザー属性の一覧の取得

- ユーザーに対するエンタイトルメントの割り当てと割り当て解除 (複数の OU に対するユーザーの追加を含む)
- SSL を介したユーザーのプロビジョン



コネクタによりユーザーを **Active Directory LDAP** リソースに追加する場合、ユーザーは「ドメインユーザー」と呼ばれるデフォルトのグループに割り当てられます。このグループをエンタイトルメントとして使用しないでください。このグループはユーザーから削除できません。

Active Directory LDAP コネクタは、一方向のコネクタで、**Select Identity** データベースに格納されたユーザーデータが変更された際に、その変更を対象の **Active Directory LDAP** にも適用します。**Select Identity** フィールドと **LDAP** フィールドのマッピングには、マッピングファイルが使用されます。



このコネクタは、英語以外のプラットフォームでもサポートされています。このコネクタは、**LDAP** とのデータの交換に **JNDI (LDAP のリソースプロバイダイインタフェース)** を使用しています。

Active Directory LDAP コネクタは、次のファイルに格納されています。

- `TALDAPv3.rar` — コネクタのバイナリファイルが含まれています。
- `schema.jar` — **Select Identity** フィールドと **Active Directory LDAP** フィールドのマッピング方法が定義された、**Active Directory** システム用の属性マッピングファイル (`ActiveDir.xml`) が含まれています。

これらのファイルは、**Select Identity Connector CD** の **LDAP Active Dir** ディレクトリに収録されています。

システム要件

Active Directory LDAP コネクタは、以下の Select Identity サーバー構成でサポートされています。

Select Identity のバージョン	アプリケーションサーバー	データベース
3.0.2	WebLogic 8.1.2 (Windows 2003)	SQL Server 2000
	WebLogic 8.1.2 (Solaris 9)	Oracle 9i
	WebLogic 8.1.2 (HP-UX 11i)	Oracle 9i
	WebSphere 5.1.1 (Solaris 9)	DB2 8.2 (または DB2 8.1 Service Pack 7)
3.3	WebLogic 8.1.4 (Windows 2003)	SQL Server 2000
3.3.1	WebLogic 8.1.4 (Windows 2003)	SQL Server 2000
	WebSphere 5.1.1 (HP-UX 11i)	Oracle 9i

コネクタは、Windows 2000 および Windows 2003 にインストールされた Active Directory でサポートされています。Windows 2000 では、このコネクタにセキュア通信機能 (LDAPS) を使用できます。Windows 2003 では、LDAPS を使用しなければなりません。設定方法の詳細については、14 ページの「セキュア LDAP の使用」を参照してください。

Active Directory LDAP コネクタは、国際化されており、Java の Unicode 仕様でサポートされている言語に対応しています。英語以外のプラットフォームでコネクタを使用する場合は、以下の前提条件を満たしていることを確認する必要があります。

- Select Identity サーバーを国際化に対応するように設定する必要があります。詳細については、『*HP OpenView Select Identity インストールガイド*』を参照してください。
- 各地域の言語で使用する文字をサポートするようにリソースを設定する必要があります。

詳細については、19 ページの「国際化サポート」を参照してください。

Web アプリケーションサーバーでの配布

Active Directory LDAP コネクタを Select Identity サーバーにインストールするには、以下の手順を実行します。

- 1 Select Identity ホームディレクトリに、コネクタの RAR ファイルを格納するサブディレクトリを作成します。たとえば、Windows 上に `C:\¥Select_Identity¥connectors` フォルダを作成します (コネクタのサブディレクトリは既に存在している場合があります)。
- 2 TALDAPv3.rar ファイルを Select Identity Connector CD からコネクタのサブディレクトリにコピーします。
- 3 WebLogic にコネクタを配布するには、以下の手順に従います。WebSphere にコネクタを配布する場合は、[13 ページの手順 4](#)に進みます。
 - a Select Identity ホームディレクトリにスキーマのサブディレクトリを作成します。このディレクトリには、コネクタのマッピングファイルを格納します。たとえば、`C:\¥Select_Identity¥schema` フォルダを作成します (このサブディレクトリは既に存在している場合があります)。
 - b `schema.jar` ファイル (Select Identity Connector CD に収録) を解凍して、解凍されたフォルダをスキーマのサブディレクトリに配置します。
 - c WebLogic サーバーの起動スクリプトで指定されている環境変数 `CLASSPATH` に、このスキーマのサブディレクトリが含まれていることを確認します。
 - d アプリケーションサーバーが起動していない場合は起動します。
 - e WebLogic サーバーのコンソールにログインします。
 - f **[My_domain]** → **[デプロイメント]** → **[コネクタモジュール]** に移動します。
 - g **[新しいコネクタモジュールのデプロイ]** をクリックします。
 - h TALDAPv3.rar ファイルの格納場所に移動し、TALDAPv3.rar を選択します。このファイルは、コネクタのサブディレクトリに格納されています。
 - i **[モジュールの割り当て]** をクリックします。
 - j **[myserver]**(配布先のサーバーインスタンス)チェックボックスをオンにします。

- k **[続行]** をクリックします。設定内容を確認します。
 - l デフォルトの設定をすべてそのまま使用して、**[デプロイ]** をクリックします。**[最後のアクションのステータス]** 列に「成功」と表示されます。
- 4 WebSphere にコネクタを配布するには、以下の手順に従います。
- a アプリケーションサーバーを停止します。
 - b schema.jar ファイル (Select Identity Connector CD に収録) を解凍して、解凍されたフォルダを WebSphere¥AppServer¥lib¥ext ディレクトリに配置します。
 - c アプリケーションサーバーを起動します。
 - d WebSphere アプリケーションサーバーコンソールにログオンします。
 - e **[リソース]** → **[リソース・アダプタ]** に移動します。
 - f **[RAR のインストール]** をクリックします。
 - g **[ローカルパス]** フィールドに、TALDAPv3.rar ファイルへのパスを入力します。このファイルは、**手順 1** で作成したサブディレクトリに保存されています。
 - h **[次へ]** をクリックします。
 - i **[名前]** フィールドに、コネクタ名を入力します。
 - j **[OK]** をクリックします。
 - k **[保存]** リンク (ページの上部) をクリックします。
 - l 変更をマスター構成に保管するページで、**[保管]** ボタンをクリックします。
 - m **[リソース]** → **[リソース・アダプタ]** をクリックします。
 - n 新しいコネクタをクリックします。
 - o **[追加プロパティ]** テーブルで **[J2C 接続ファクトリ]** をクリックします。
 - p **[新規作成]** をクリックします。
 - q **[名前]** フィールドに、コネクタのファクトリ名を入力します。SQL コネクタの場合は、「**eis/LDAPv3**」と入力します。
 - r **[OK]** をクリックします。
 - s **[保存]** リンクをクリックします。
-

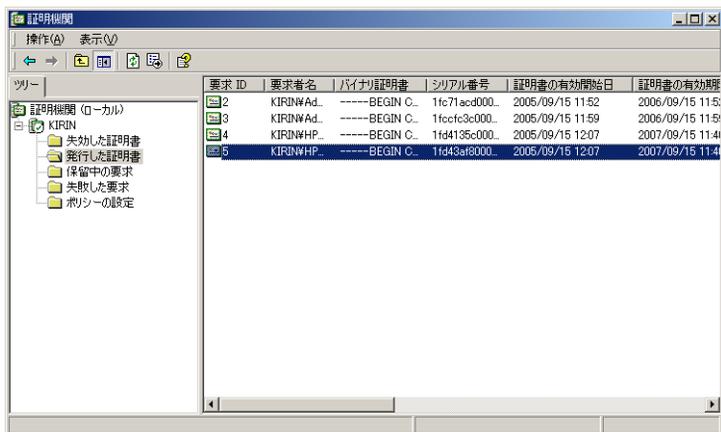
- t 変更をマスター構成に保管するページで、**[保管]** ボタンをクリックします。
 - u **WebSphere** を再起動します。
- 5 必要に応じて、マッピングファイルを変更します。このファイルについては、[27 ページ](#)の「マッピングファイルの概要」で詳しく説明されています。
- コネクタをインストールしたら、[19 ページ](#)の「コネクタの設定」の記述に従って、**Select Identity** のコネクタの登録と構成を行ってください。

セキュア LDAP の使用

Windows Active Directory に接続してユーザーパスワードを変更する場合は、セキュア LDAP (LDAPS) を使用する必要があります。これを使用しないと、Active Directory LDAP コネクタは Active Directory のパスワードを更新できません。また、Windows 2003 上の Active Directory の場合は、すべてのタスクで LDAPS を使用する必要があります。

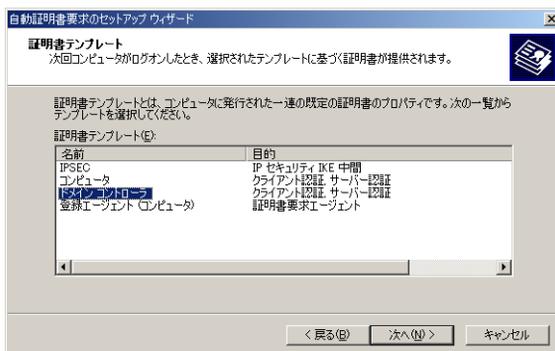
Active Directory システム上でセキュア通信 (LDAPS) を有効にするには、以下の手順に従います。

- 1 Windows CD から証明書サービスコンポーネントをインストールします。
- 2 システム上で HTTPS を構成します。
- 3 証明機関を作成します([管理ツール] → [証明機関] を選択します)。これにより、ルート証明書も作成されます。以下に Windows 2003 上に作成された証明書を示します。

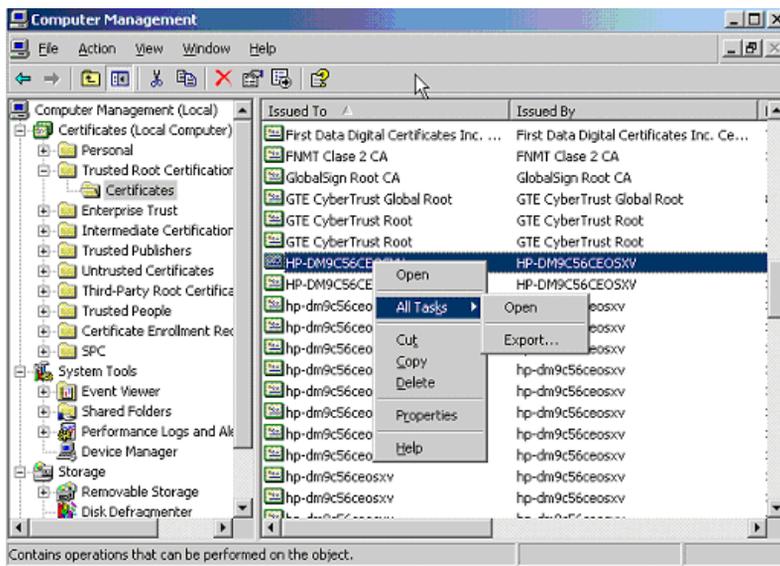


- 4 自動証明書要求を作成します([管理ツール]→[ドメインコントローラセキュリティポリシー]→[公開キーのポリシー]を選択します)。

プロンプトが表示されたら、以下のとおりに[ドメインコントローラ]を選択します。



- 5 [管理ツール] → [証明機関] → [発行した証明書]を選択して新しいエントリを表示した後、[信頼されたルート証明機関] → [証明書]の下にある、CAと同じ名前前の付いた証明書を開きます (mmc からのスナップインを使用)。



- 6 証明書をエクスポートして、拡張子 **.cer** のファイル名を指定します。
- 7 Select Identity サーバー上でブラウザに以下の URL を読み込み、証明書を Active Directory サーバーから Select Identity サーバーにダウンロードします。

http://AD_host/certsrv

プロンプトが表示されたら、Active Directory サーバーのログイン証明書を指定します。証明書を必ず %JAVA_HOME%\jre\lib\security ディレクトリにダウンロードします。

Select Identity サーバーに証明書をコピーすることもできます。

- 8 コマンド行で、%JAVA_HOME%\jre\lib\security ディレクトリに移動し、次のコマンドを使用して証明書を出力して確認します。

```
keytool -printcert -v -file filename.cer
```

以下のように表示されるはずです。

```
C:\bea\jdk-142_05\jre\lib\security>keytool -printcert -v -file AD_03_28_1.cer
所有者: CN=KIRIN, C=JP
実行者: CN=KIRIN, C=JP
シリアル番号: 2d4b5db8a11d7ba8433216395d98bfff0
有効日: Thu Sep 15 11:33:07 JST 2005 有効期限: Sat Sep 15 11:40:18 JST 2007
証明書のフィンガープリント:
MD5: D1:A2:FB:06:A9:73:3F:A6:1E:41:7B:10:A1:DD:4B:59
SHA1: 37:85:65:03:B1:CD:DC:8A:A7:63:EC:60:D6:4D:B4:AA:67:E8:5A:3D
```

- 9 以下の手順に従って、**Select Identity** サーバーに証明書をインストールします。
 - a 次の **keytool** コマンドを使用して、証明書を **cacerts** キーストアにインポートします。


```
keytool -import -v -trustcacerts -alias alias -file filename.cer -keystore cacerts
```
 - b キーストアのパスワードの入力を求められたら、パスワードを入力します。
 - c 証明書を信頼するかどうかを確認するプロンプトが表示されたら、**yes** を入力します。
 - d 次のコマンドを入力し、証明書がインポートされていることを確認します。


```
keytool -list -alias CA123 -keystore file_name
```
 - e キーストアファイルを `%JAVA_HOME%\jre\lib\security` ディレクトリにコピーします。既存のファイルが上書きされる場合があります。
 - f アプリケーションサーバーを再起動します。
- 10 セキュア接続 (LDAPS) を使用して **Select Identity** サーバーを **Active Directory** サーバーに接続できることを確認するには、コネクタのリソースの作成時にアクセス URL に **ldaps://AD_host:636** を指定します。詳細については、[22 ページの手順 3](#) を参照してください。

構成および手順の詳細情報やヘルプが必要な場合は、システム管理者に連絡してください。

コネクタの設定

アプリケーションサーバーにコネクタを配布したら、**Select Identity** クライアントでコネクタを配布して、そのコネクタを使用するように **Select Identity** を設定する必要があります。ここでは、コネクタを配布するために必要な手順の概要を説明します。また、コネクタを使用するように **Select Identity** を設定する際に必要なコネクタに固有の情報について説明します。

国際化サポート

コネクタを英語以外のプラットフォームにインストールする場合、コネクタを配布および設定する前に、この項の情報を理解しておく必要があります。コネクタの国際化サポートによって利用できる機能と国際化サポートに関する制限事項は次のとおりです。

- (Select Identity クライアントで) ユーザー属性を入力してプロビジョニングする場合、以下の属性を除き、各地域の言語で使用する文字を入力できます。
 - UserName
 - Password
 - Email

下図は、属性値に中国語（漢字）を使用した場合の例です。

用户属性	
FirstName	中文
UserName	OraEvf003
Password	***** [No expiration]
GUID	E19A27C5-C66E-4F60-11DD-363488491677
Email	yilei.zhang@hp.com
Business Phone	null
Home Phone	null
Address 1	地址1
Country	中国ABC
Gen_Ora_I18N_KEY	OraEvf003

- 各地域の言語で使用する文字を含むソースとの調整処理はサポートされています。**LDAP** リソース上でユーザーをプロビジョニングする場合、各地域の言語で使用する文字を入力データとして入力できます。これらの文字は、**SPML** ファイルを通じて **Select Identity** に調整処理の際に取り込まれます。ただし、以下のユーザー属性には、**ASCII** 文字しか使用できません。

— **UserName**

— **Password**

— **Email**

- リソースの属性名には、非 **ASCII** 文字を含めることができません。したがって、非 **ASCII** 文字をマッピングファイルに含めることはできません。下図はマッピングファイルに含まれる属性を示しています。**ASCII** 文字の属性名のみが表示されています。

Resource Name=Gen_Ora_I18N				
<< < 頁 1 / 1 > >>				总记录数:10
Name	Min Length	Max Length	Attribute Mapped To	Authoritative
Address	0	255	Addr1	N
Country	0	255	Country	N
E-Mail	0	255	Email	N
FirstName	0	255	FirstName	N
Gen_Ora_I18N_ENTITLEMENTS	1	255	Gen_Ora_I18N_ENTITLEMENTS	Y
Gen_Ora_I18N_KEY	1	255	Gen_Ora_I18N_KEY	Y
Password	0	255	Password	N
PhOffice	0	255	PhBus	N
UserName	0	255	UserName	N
phHome	0	255	PhHome	N

- 非 ASCII 文字を含むエンタイトルメントは、このコネクタではサポートされていません。
- すべての設定ファイル名とプロパティファイル名には、ASCII 文字を使用する必要があります。
- リソースからの例外メッセージはすべて英語で表示されます。
- ログメッセージはすべて英語で表示されます。

コネクタの配布

コネクタを配布して設定するには、以下の手順を実行します。

- 1 **Select Identity** にコネクタを配布する前に、LDAP ブラウザまたはその他のユーティリティを使用して LDAP に接続します。これにより、**Select Identity** にリソースを配布する前に、LDAP リソースが利用可能であることと、パラメータが正しく設定されていることを確認できます。
- 2 [コネクタ]ホームページで**[新規コネクタの配布]**ボタンをクリックして、**Select Identity** にコネクタを登録します。『*HP OpenView Select Identity Administrator Guide*』の「Connectors」の章の説明に従って、この手順を実行します。

コネクタを配布すると、コネクタのプロパティは以下のように表示されます。

ホーム > コネクタ : LDAP

コネクタ情報	
*コネクタ名:	LDAP
*プール名:	eisLDAPv3
利用できるマッパ:	いはいえ

- 3 新たに作成したコネクタを使用するリソースを配布します。[リソース]ホームページで、**[新規リソースの配布]** ボタンをクリックします。リソースの設定時には、以下の表を参照して、このコネクタに固有のパラメータに関する情報を確認してください。

フィールド名	値のサンプル	説明
リソース名	ActiveDirectory	ターゲットリソース名。
リソースタイプ	AD LDAP	21 ページの手順 2 で配布したコネクタ。
信頼できるソース	いいえ	このリソースが、ご使用の環境でユーザーデータの信頼できるソースとして運用されているシステムかどうかを示しています。このコネクタでは、 Select Identity サーバーとアカウントデータを同期できないため、 [いいえ] を指定しなければなりません。
グループに関連付け	選択	システムがグループの概念を使用しているかどうかを示しています。この LDAP コネクタの場合、このオプションを選択します。
Access URL	ldap://136.168.1.20:389 ldaps://192.168.1.19:636	リソースにアクセスするための URL。セキュア LDAP (LDAPS) をパスワードの変更に使用する場合、プロトコルに ldaps を、ポートに 636 を指定します。
Suffix	dc=qa,dc=hp,dc=com	ユーザーがプロビジョニングされるドメイン。
Login Name	cn=Administrator,cn=Users, dc=qa, dc=hp,dc=com	ユーザーを追加および削除する管理者権限が与えられたログインアカウント。リソースにログインする際に必要です。

フィールド名	値のサンプル	説明
Password	Password123	ログインアカウントに対応するパスワード。
User Suffix*	cn=users	ユーザーの識別名の接尾辞。プロビジョニングされたユーザーが追加されるツリーの場所。
User Object Class	top, Person, organizationalPerson, user	ユーザーのオブジェクトクラス。
Group Suffix*	cn=users	グループの識別名の接尾辞。プロビジョニングされたユーザーグループが追加されるツリーの場所。
Group Object Class	top, group	ユーザーグループのオブジェクトクラス。
Mapping File	ActiveDir.xml	リソース属性を Select Identity 属性に割り当てるために使用されるコネクタマッピングファイルの場所。

* このコネクタは、別の OU へのユーザーの追加をサポートします。これを設定するには、リソースの作成時に **User Suffix** と **Group Suffix** に適切な値を指定します。

『*HP OpenView Select Identity Administrator Guide*』の「**Resources**」の章の説明に従って、この手順を実行します。

Active Directory LDAP コネクタのリソースを配布すると、[リソースアクセス情報] ページは以下のように表示されます。

> [Home](#) > [Resources](#) > [View Resource : AD-LDAP](#)

Resource Access Information	
* Resource Name:	AD-LDAP
Access URL:	ldap://16.73.17.69:389
Suffix:	dc=qa,dc=trulogica,dc=com
Login Name:	cn=administrator,cn=users,dc=qa,dc=trulogica,dc=com
Password:	*****
* User Suffix:	cn=users
* User Object Class:	top,person,organizationalPerson,user
* Group Suffix:	cn=users
* Group Object Class:	top,groupofuniquenames
* Mapping File:	ActiveDir.xml

- 4 **Select Identity** をコネクタにリンクする属性を作成します。コネクタのマッピングファイル内のマッピングごとに、**Select Identity** クライアント上で属性機能を使用して属性を作成します。

詳細情報は、『*HP OpenView Select Identity Administrator Guide*』の「Attributes」の章を参照してください。Active Directory LDAP コネクタの

属性を作成した後、リソースの [属性の表示] ページは以下のように表示されます。

Resource Name=AD-LDAP				
				合計レコード: 20
名前	最小長	最大長	属性のマップ先	権威
Address 1	1	128		
Address 2	1	128		
AD-LDAP_ENTITLEMENTS	1	255	AD-LDAP_ENTITLEMENTS	Y
AD-LDAP_KEY	1	255	AD-LDAP_KEY	Y
Business Phone	1	20		
City	1	128		
Description	1	256		
Directory	0	128		
Email	1	256		
First Name	1	64	FirstName	N
Home Phone	1	20		
Last Name	1	64	LastName	N
Mobile Phone	1	20		
Password	1	64	Password	N
Profile Path	1	128		
Script Path	1	128		
State	1	128		
Title	1	50		
User Name	1	64	UserName	N
Zip	1	50		

- 5 新たに作成したリソースを使用するサービスを作成します。サービスを作成するには、[サービス] ホームページの [新しいサービスの配布] ボタンをクリックします。『*HP OpenView Select Identity Administrator Guide*』の「Services」の章の説明に従って、この手順を実行します。このサービスの作成時に手順3で作成した新しいリソースを参照します。

必要に応じて、コネクタによってユーザーが作成されたか、またはパスワードが変更されたかを検証することができます。以下のコマンドを使用して、プロビジョニングされたユーザーにパスワードが正しく設定されたことを確認します。

```
net use \\IP_addr * /user:ユーザー名
```

以下に例を示します。

```
net use \\16.73.17.69 * /user:aa25
```

パスワードを入力すると、以下のメッセージのいずれかが表示されます。

- **成功した場合:**
コマンドは正常に終了しました。
- **ログオンに失敗した場合:**
システムエラー 1326 が発生しました。
- **ログオン失敗:**
ユーザー名を認識できないか、またはパスワードが間違っています。
- **特定のユーザーの接続が存在する場合 (net use が別の場所で発行されている場合):**
システムエラー 1219 が発生しました。

同じユーザーによる、サーバーまたは共有リソースへの複数のユーザー名での複数の接続は許可されません。サーバーまたは共有リソースへの以前の接続をすべて切断してから、再試行してください。

接続を削除するには、次のコマンドを入力します。

```
net use \\IP_Addr /delete
```

マッピングファイルの概要

Active Directory LDAP コネクタには、ActiveDir.xml マッピングファイルが付属しています。これは SPML を標準仕様とした、XML で記述されたファイルで、schema.jar ファイルにバンドルされています。ActiveDir.xml ファイルには、リソースアプリケーションに必要な属性が含まれています。このファイルは、Select Identity で行われたユーザーアカウントの追加と変更を Active Directory に適用する際のマッピングに使用されます。このファイルの内容は、Select Identity の [リソース] ページを使用してリソースを配布するときに表示できます。

Select Identity クライアントの [属性] ページで、Select Identity に固有の属性を作成できます。これらの属性は、この章で説明するとおりにコネクタマッピングファイルを編集することによって、Select Identity ユーザーアカウントとシステムリソースの関連付けに使用できます。このような処理は、1つの属性(たとえば、"username")がリソースごとに異なる名前(たとえば、UNIX では "login"、データベースでは "UID"、Windows サーバーでは "userID")で表されるため、必要になります。

このファイルは、追加の属性をリソースに割り当てない限り、編集する必要はありません。このマッピングファイルで定義されていない属性と値は、Select Identity を介してリソースに保存することはできません。

概説

マッピングファイルでは、以下の作業を行います。

- 新しい属性マッピングを追加する
- 既存の属性マッピングを削除する
- 属性マッピングの変更

ここでは、Active Directory LDAP コネクタが提供する XML マッピングファイルの各要素について説明します。

- **<Schema>**、**<providerID>**、および **<schemalD>**

ヘッダー情報の標準要素を提供します。

- **<objectClassDefinition>**

特定のオブジェクトに対して実行可能なアクションとそのオブジェクトに含まれる各フィールドの **Select Identity** とリソース間でのマッピングを定義します。実行可能なアクションは、**<properties>** 要素のブロック内の **name** 属性で、各フィールドのマッピングは **<memberAttributes>** 要素のブロック内で定義します。たとえば、ユーザーのオブジェクトクラスの定義では、LDAP で管理されているユーザーの作成、読み込み、更新、削除、リセット、失効などが行えるように定義します。

- **<properties>**

オブジェクトに対して実行可能な操作を定義します。この要素は、**Select Identity** を通じて実行される操作を制御するために使用されます。以下の操作を制御できます。

- 作成 (CREATE)
- 読み込み (READ)
- 更新 (UPDATE)
- 削除 (DELETE)
- 有効化 (ENABLE)
- 無効化 (DISABLE)
- パスワードのリセット (RESET_PASSWORD)
- パスワードの失効 (EXPIRE_PASSWORD)

— パスワードの変更 (CHANGE_PASSWORD)

操作は <attr> 要素の name 属性で指定し、操作が利用可能かどうかは対応する <value> 要素で指定します。値は以下のように設定できます。

- true — 操作はコネクタによってサポートされます。
- false — 操作はコネクタによってサポートされず、`PermissionException` をスローします。
- bypass — 操作はコネクタによってサポートされませんが、例外をスローしません。操作は単にバイパスされます。

以下に例を示します。

```
<objectClassDefinition name="User" description="Active
Directory User">
  <properties>
    <attr name="CREATE">
      <value>true</value>
    </attr>
    <attr name="READ">
      <value>true</value>
    </attr>
```

- **<memberAttributes>**

属性マッピングを定義します。この要素には、各属性のマッピングを表す <attributeDefinitionReference> 要素が含まれています。各 <attributeDefinitionReference> について、最大/最小文字数などの詳細情報を定義する <attributeDefinition> 要素をこの要素の後で定義する必要があります。

各 <attributeDefinitionReference> 要素には、以下の属性が含まれます。

- name — 参照名
- required — プロビジョニングにおけるこの属性の必要性 (true または false に設定)
- concero:tafield — Select Identity のリソース属性名。一般的に、tafield に指定する属性名は、物理リソースの属性名か、少なくともコネクタの属性名と同一にする必要があります。たとえば、以下のようにするをお勧めします。

```
<attributeDefinitionReference name="FirstName"
required="false" concero:tafield="[givenname]"
concero:resfield="givenname" concero:init="true"
concero:isMulti="true"/>
```

以下はお勧めしません。

```
<attributeDefinitionReference name="FirstName"
required="false" concero:tafield="[FirstName]"
concero:resfield="givenname" concero:init="true"
concero:isMulti="true"/>
```

- **concero:resfield** — リソースのスキーマから流用した物理リソース属性名。リソースが明示的なスキーマ (UNIX など) をサポートしない場合、このフィールドは、リソースの属性をマッピングしていることを示すタグフィールドになります。

また、属性名は大文字と小文字の区別がある場合があります。たとえば、リソースで定義されている属性の名前に含まれる文字がすべて大文字の場合、ここでもすべて大文字で指定するようにしてください。

- **concero:isKey** — 省略可能。この属性を指定して値に **true** に指定すると、このフィールドがリソース上のオブジェクトを特定するキーフィールドになります。**isKey="true"** を指定できる

<attributeDefinitionReference> 要素は、1 つだけです。このキーフィールドは、**Select Identity** のアイデンティティオブジェクトのキーフィールドと同じである必要はありません。

キーフィールドをマッピングする場合、**isKey="true"** を指定した要素の **tafield** に **UserName** 属性の値が指定されていない場合、**UserName** を他のマッピングで使用しないようにしてください。つまり、**UserName** は、リソースのキーフィールドにマップされている場合にのみ、**tafield** に割り当てることができます。以下に例を示します。

```
<attributeDefinitionReference name="UserName"
required="true" concero:tafield="[UserName]"
concero:resfield="uid" concero:isKey="true"
concero:init="true"/>
```

- **concero:init** — 省略可能。この属性を指定すると、オブジェクトの属性が **Select Identity** から渡された **Identity** オブジェクトの属性値で初期化されることを示しています。

以下に例を示します。

```
<memberAttributes>
  <attributeDefinitionReference name="User Name"
    required="true" concero:tafield="[User Name]"
    concero:resfield="cn" concero:isKey="true"
    concero:init="true" />
```

コネクタフィールド (**concero:tafield** 属性で指定された) とリソースフィールド (**concero:resfield** 属性で指定された) の間のマッピングの解析方法は、コネクタによって異なります。**Active Directory LDAP** コネクタは、以下のようなマッピングを解析するようにプログラミングされています。

- コネクタの属性名は、角括弧で囲んで指定します (例: [xyz])。属性 xyz の値は、プロビジョニングの時に **UserModel** から取得されます。
- **ActiveDir.xml** マッピングファイルでは、複数の要素を結合した属性を指定できます。複数の要素を結合した属性を指定するには、コネクタの属性を 「[attr1] xxxx [attr2]」 のように指定します。この場合、特定のリソースのフィールドとのマッピングに、**attr1** および **attr2** 属性の値を文字列 xxxx と組み合わせたフィールドを使用することを示しています。**Active Directory LDAP** コネクタは、このような複数の要素を結合した属性のマッピングを処理するようにプログラミングされています。

• <attributeDefinition>

各オブジェクトの属性のプロパティを定義します。たとえば、**HomeDir** 属性の属性定義は、0 ~ 100 文字までの長さで指定する必要があり、**a-z**、**A-Z**、**0-9**、**@**、および **+** の文字、数字、記号とスペースを使用できることを定義します。

以下に **ActiveDir.xml** ファイルからの抜粋を示します。

```
<attributeDefinition name="HomeDir" description="User Home
directory" type="xsd:string" >
  <properties>
    <attr name="minLength">
      <value>0</value>
    </attr>
    <attr name="maxLength">
      <value>128</value>
    </attr>
```

```

    <attr name="pattern">
      <value><![CDATA[[a-zA-Z0-9@]+]]> </value>
    </attr>
  </properties>
</attributeDefinition>

```

- **<concerro:entitlementMappingDefinition>**
ユーザーにエンタイトルメントをマッピングする方法を定義します。
- **<concerro:objectStatus>**
ユーザーにステータスを割り当てる方法を定義します。
- **<concerro:relationshipDefinition>**
複数のユーザーを関連付ける方法を定義します。

Active Directory LDAP のマッピング情報

以下に **Active Directory** でサポートされている属性マッピングを示します。これらは **ActiveDir.xml** マッピングファイルにリストされています。このファイルの内容に精通すれば、属性を追加、変更、または削除できます。**Select Identity** リソース属性を編集できます。これらの属性は、**Select Identity** に表示されるアイデンティティ情報に反映されます。物理リソースの属性は、**Active Directory** 上のユーザーアカウントの属性で、リテラルとして扱われています。これらの属性は変更できません。

Select Identity リソース属性	Active Directory LDAP 属性	説明
User Name	cn	リソース上のキーフィールド
Password	UnicodePwd	
First Name	givenname	
Last Name	sn	
User Name	samaccountname	
FirstName + LastName	displayname	
Directory	homeDirectory	

Select Identity リソース属性	Active Directory LDAP 属性	説明
Last Name + First Name	userPrincipalName	
Address 1	streetAddress	
Address 2	postOfficeBox	
City	l	
State	st	
Zip	postalCode	
Title	title	
Business Phone	telephoneNumber	
Home Phone	homePhone	
Profile Path	profilePath	
Script Path	scriptPath	
Description	description	
Disable function	userAccountControl=514	ユーザーを無効化
Enable function	userAccountControl=512	ユーザーを有効化

また、LDAPS ではなく LDAP を使用している場合、マッピングファイルの以下の属性を編集します。

```
<attributeDefinitionReference name="userAccountControl"
  required="true" concero:tafield="546"...
```

512 を tafield 属性に割り当てるには、以下の属性を編集します。

```
<attributeDefinitionReference name="userAccountControl"
  required="true" concero:tafield="512"...
```

これにより、パスワードが未設定のアカウントが作成されます。ただし、このアカウントは無効です。

コネクタのアンインストール

Select Identity からコネクタをアンインストールする場合は、以下の項目を確認する必要があります。

- すべてのリソースの依存が削除されている
- Select Identity クライアント上で [コネクタ] ページを使用してコネクタが削除されている

WebLogic からの削除

コネクタを削除するには、以下の手順に従います。

- 1 WebLogic サーバーのコンソールにログインします。
- 2 **[mydomain]** → **[デプロイメント]** → **[コネクタモジュール]** に移動します。
- 3 アンインストールするコネクタの隣の **[削除]** アイコンをクリックします。
- 4 削除を確認するメッセージが表示されたら、**[はい]** をクリックします。
- 5 **[続行]** をクリックします。

WebSphere からの削除

WebSphere からコネクタをアンインストールするには、以下の手順に従います。

- 1 WebSphere アプリケーションサーバーコンソールにログオンします。
- 2 **[リソース]** → **[リソース・アダプタ]** に移動します。
- 3 アンインストールするコネクタを選択します。
- 4 **[削除]** をクリックします。
- 5 **[保管]** リンク (ページの上部) をクリックします。
- 6 変更をマスター構成に保管するページで、**[保管]** ボタンをクリックします。