HP Select Identity

Windows® Active Directory 用コネクタ (双方向 LDAP ベース)

コネクタバージョン : 2.20

インストールと設定ガイド

ドキュメント発行日 : 2008 年 1 月
ソフトウェア発行日 : 2008 年 1 月

invent

ご注意

保証について

HP の製品およびサービスの保証は、当該製品およびサービスに含まれる明示的保証書に明記されています。ここに記載されている内容は、その他の保証を付加するものではありません。HP は、本書の技術的または編集上の誤りに対して一切の責任を負わないものとします。

本書に記載されている内容は、予告なしに変更することがあります。

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

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のソフトウェアには以下があります。

- 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。

本製品には Waveset Technologies, Inc. (www.waveset.com) が開発したソフトウェアが含まれます。

Trademark Notices

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

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。

JAVA™ は Sun Microsystems, Inc の米国商標です。

Microsoft® および Windows® は Microsoft Corporation の米国登録商標です。

Oracle® は Oracle Corporation (Redwood City、California) の米国商標です。

UNIX® は The Open Group の登録商標です。

サポート

次の HP ソフトウェアサポート Web サイトをご利用いただけます。

http://www.hp.com/go/hpsoftwaresupport

HP ソフトウェアのオンラインサポートでは、対話形式による技術サポートツールを効率的にご利用いただけます。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
- サポートケースと改善要求の送信、および追跡
- ソフトウェアパッチのダウンロード
- サポート契約を管理する
- HP サポートの連絡先の問い合わせ
- 利用可能なサービスについての情報の参照
- 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の検索および参加登録

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

サポートの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://h20230.www2.hp.com/new_access_levels.jsp

目次

1 資料マップ

この章では、HP Select Identity コネクタのドキュメント構成について説明し、コネクタのインストールと設定にドキュメントセットを利用する方法について必要な情報を提供します。

図 1 は、HP Select Identity コネクタの資料マップを示しています。用意されている製品マニュアルの一覧については、表 1 を参照してください。

図 1　　資料マップ

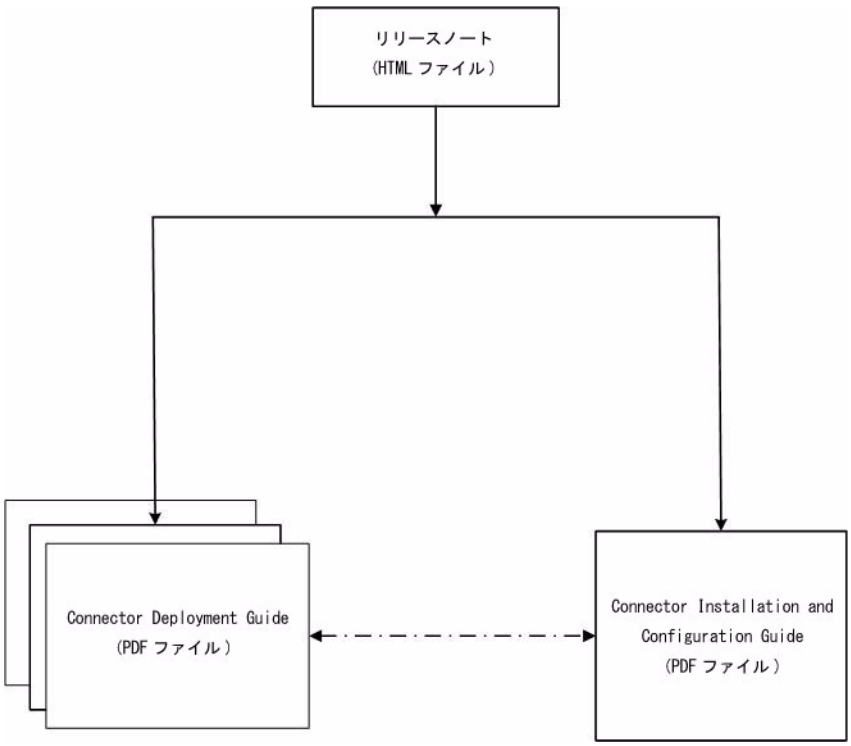


表 1　　コネクタのドキュメント

ドキュメントのタイトルとファイル名	内容	保存されている場所
リリースノート Active Directory BiLDAP Connector v2.20 Release Note.htm	このファイルには、コネクタの新機能、改善点、既知の問題点と制限、サポート情報が記載されています。	コネクタディレクトリの下の /Docs/ サブディレクトリ。
Connector Deployment Guide (Select Identity 4.20 用) connector_deploy_SI4.20.pdf	コネクタの配布ガイド。次の情報が記載されています。 • アプリケーションサーバーへのコネクタの配布。 • Select Identity によるコネクタの設定。 コネクタのインストールに関する一般的な情報については、これらのガイドを参照してください。	製品リリースフォルダ直下にある /Docs/ ディレクトリ。
Connector Deployment Guide (Select Identity 4.10 ～ 4.13 用) connector_deploy_SI4.13.pdf		
Connector Deployment Guide (Select Identity 4.0/4.01 用) connector_deploy_SI4.pdf		
Connector Installation and Configuration Guide Active_Directory_BiLDAP_guide.pdf	コネクタのインストールと設定に関するガイド。特定のコネクタのインストール方法について説明します。設定の詳細がリソースごとに示されます。	コネクタディレクトリの下の /Docs/ サブディレクトリ。

2 概要

この章では、Active Directory 用の HP Select Identity コネクタの概要について説明します。Active Directory 用の HP Select Identity コネクタを使用すると、ユーザーのプロビジョニングとアイデンティティ管理を Active Directory で行うことができます。この章で説明する内容は、以下のとおりです。

- HP Select Identity の利点
- コネクタの役割
- Active Directory 用のコネクタ

HP Select Identity について

HP Select Identity では、新しい手法のアイデンティティ管理が実現されています。Select Identity を使用すると、複数のプラットフォーム間、アプリケーション間、および企業間のユーザーアカウントとアクセス権限のプロビジョニングや管理のプロセスを自動化できます。Select Identity はコネクタを通じてエンタープライズ情報システムと通信し、アイデンティティ管理作業を自動化します。エンタープライズ情報システムは「**リソース**」とも呼ばれます。リソースには、データベース、ディレクトリサービス、ERP パッケージなどがあります。

コネクタについて

リソースと Select Identity との接続を確立するには、コネクタを使用します。コネクタはリソースによって異なります。Select Identity とコネクタを組み合わせると、一連のタスクをリソースで実行してアイデンティティを管理することができます。コネクタには「**一方向型**」と「**双方向型**」のものがあります。一方向型のコネクタでは、アイデンティティを Select Identity から管理できますが、リソースに変更が発生しても、それを Select Identity に伝えることができません。一方、双方向型のコネクタは、リソースで発生した変更を Select Identity に伝えることができます。この双方向型コネクタの特性は「**リバース同期**」と呼ばれます。

Active Directory 双方向 LDAP コネクタについて

Microsoft Active Directory 用の双方向型 LDAP コネクタ (以後 Active Directory 双方向 LDAP コネクタと呼ぶ) により、Select Identity は Active Directory サーバで次のタスクを実行できるようになります。

`user` ObjectClass の場合

- 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
- ユーザーパスワードの失効
- すべての使用権の取得
- 利用可能なユーザー属性の一覧の取得
- ユーザーに対する使用権の付与と破棄
- ユーザー名の変更 (CN 属性の変更)
- 同じドメイン内の OU 間でユーザーを移動
- マルチドメイン機能
  - AD フォレストのサポート： マルチドメイン AD フォレスト内の任意のドメインに対するユーザーのフォワードプロビジョニング
  - AD フォレスト内の複数のドメインコントローラ (DC)、およびグローバルカタログ (GC) のサポート
  - マルチドメインフォレスト内の任意のグループ (使用権) に対するユーザーの割り当て、および割り当て解除
  - AD フォレスト内のすべてのドメインにおけるユーザー更新 (追加、削除、名前の変更、プロファイルの変更、リンク / アンリンク、パスワードのリセット、OU またはドメイン間の移動) の検出
- フェイルオーバー機能
  - フォワードプロビジョニングのフェイルオーバーのサポート。1 次 DC/GC の障害時に 2 次 DC/GC へのフェイルオーバーを試行 (操作タイプに依存)
  - ドメインコントローラに対する順逆両方のポーリングが失敗した場合は、再試行を実行。再試行回数は設定可能

`contact` ObjectClass の場合

- コンタクトの追加、更新、および削除
- コンタクト属性の取得
- コンタクトに対する使用権の付与と破棄

フォレスト、ドメイン、グローバルカタログなどの Active Directory ドメインサービスの主要な概念については、次の Microsoft MSDN Web サイトを参照してください。

http://msdn2.microsoft.com/en-us/library/aa772157.aspx

その他の機能

- Select Identity コネクタインタフェース 4.x のサポート
- 相互認証のサポート
- Windows 2000のネイティブモード、およびWindows Server 2003におけるドメイン間のユーザー移動をサポート

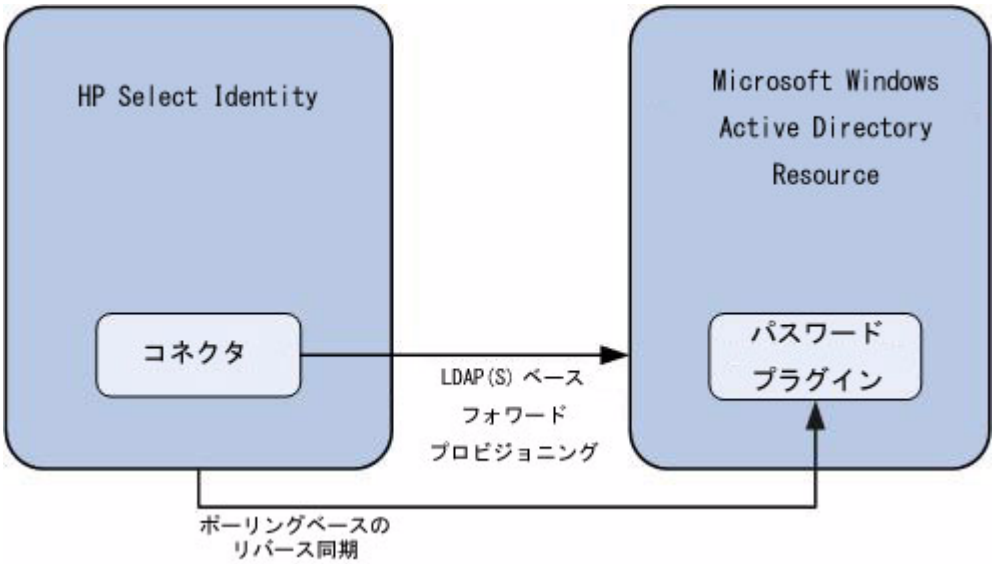
- Select Identity のユーザー名変更をサポート
- 複数値を持つ AD 属性のために複数値属性をサポート
- 32 ビットと 64 ビットの両方の AD サーバーをサポート
- 親子とピアツーピアの両方のフォレスト環境をサポート

アーキテクチャの概要

図 2 は、Active Directory 双方向 LDAP コネクタのアーキテクチャの概要を示しています。これは、双方向型 Lightweight Directory Access Protocol バージョン 3(LDAPv3) に準拠したコネクタであり、Select Identity データベース内のユーザーデータに行った変更を、ターゲットの Active Directory サーバーにプッシュします。このコネクタは、Java LDAP API(アプリケーションプログラムインタフェース) を使用して LDAP サーバーのユーザーとその使用権をプロビジョニングし、そのデータを順に Active Directory サーバーにプッシュします。

リバース同期機能は Select Identity を使用して、Active Directory リソースに行ったユーザーアカウントの変更を調整します。Select Identity は、定期的に Active Directory リソースに対してポーリングを行い、コネクタを通じて変更を取得します。

図 2　　Active Directory 双方向 LDAP コネクタのアーキテクチャ概要



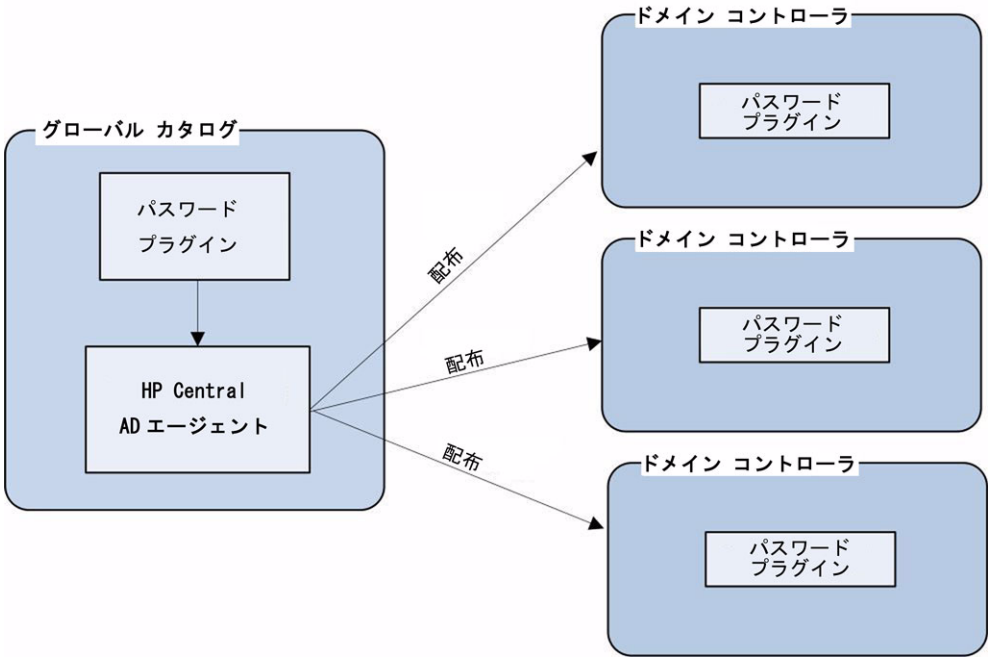
このコネクタは、Select Identity のすべてのバージョン (4.0 ～ 4.20) と組み合わせて使用できます。

パスワードプラグイン

パスワードプラグインは、Active Directory のパスワード変更を収集し、変更されたパスワードを暗号形式で Active Directory システムに格納します。この変更は、次のポーリング操作中にコネクタによりピックアップされます。このエージェントは Active Directory のみを更新し、Select Identity Web サービスと直接の通信は行いません。パスワードプラグインはオプションであり、インストールされていない場合は、パスワードの変更について Select Identity との調整は行われません。

Active Directoryのマルチドメインフォレスト環境では、HP Central AD Agentのセットアップユーティリティを実行することにより、パスワードプラグインをすべてのドメインコントローラサーバーに配布することができます。

図 3　　HP Central AD Agent のアーキテクチャ



インストールタスクの概要

コネクタのインストールを開始する前に、システム要件と、インストールに関するすべての前提条件を満たしていることを確認してください。表 2 は、インストールタスクの概要を示しています。

表 2　タスクの構成

タスク番号	タスク名	参照先
1	Select Identity サーバーにコネクタをインストール。	15 ページの「コネクタのインストール」を参照。
	— システム要件に対応。	16 ページの「システム要件」を参照。
	— インストール前のタスクを実行: Select Identity をホスティングするアプリケーションサーバーに Active Directory 証明書をインストール。	16 ページの「インストール前のタスク」を参照。
	— スキーマ JAR ファイル (コネクタのマッピングファイルを含んだファイル) の内容を Select Identity サーバー上に解凍。	32 ページの「スキーマ JAR ファイルの解凍」を参照。
	— `ActiveDirConfig.properties` ファイルの設定可能なパラメータを確認。	32 ページの「設定可能パラメータの確認」を参照。
	— コネクタのリソースアダプタアーカイブ (RAR) をアプリケーションサーバーにインストール。	38 ページの「コネクタ RAR のインストール」を参照。
	— 周期的なリクエストをブロックするように Select Identity データベースを設定。	38 ページの「周期的リクエストをブロックするための Select Identity システムデータベースの設定」を参照。
2	Active Directory 双方向 LDAP コネクタのエージェントモジュールをインストール。	41 ページの「エージェントのインストール」を参照。
	— パスワードプラグインをインストール。	41 ページの「パスワードプラグインのインストール」を参照。
	— パスワードプラグインを配布。	51 ページの「パスワードプラグインの配布」を参照。

表 2　タスクの構成 (続き)

タスク番号	タスク名	参照先
3	Select Identity でコネクタを設定。	55 ページの「Select Identity でのコネクタの設定」を参照。
	— Select Identity に新しいコネクタを追加。	55 ページの「新しいコネクタの追加」を参照。
	— Select Identity に新しいリソースを追加。	55 ページの「新しいリソースの追加」を参照。
	— Active Directory 属性を Select Identity 属性にマッピング。	60 ページの「属性のマッピング」を参照。
	— ワークフローの外部コールを設定。	63 ページの「Select Identity におけるワークフロー外部コールの設定」を参照。

3 コネクタのインストール

この章では、Select Identity サーバーに Active Directory 双方向 LDAP コネクタをインストールする手順について詳しく説明します。この章で説明する内容は次のとおりです。

- Active Directory 双方向 LDAP コネクタのインストールに必要なソフトウェア。
- Active Directory 双方向 LDAP コネクタをインストールするための前提条件。
- Active Directory 双方向 LDAP コネクタのインストール手順。

Active Directory 双方向 LDAP コネクタのファイル

Active Directory 双方向 LDAP コネクタには、次のファイルが付属します。これは、Select Identity Connector CD の `Bidirectional LDAP Connector - Active Directory` フォルダに収録されています。

表 3　Active Directory 双方向 LDAP コネクタのファイル

シリアル番号	ファイル名	説明
1	• `ActiveDirConnector.rar` (WebLogic 9.2 以外のすべてのプラットフォーム構成用) • ActiveDirConnector_WL9.rar (WebLogic 9.2 用)	コネクタが使用するバイナリファイルが含まれています。
2	`ActiveDirSchema.jar`	スキーマファイル (`ActiveDir.xml`) が含まれています。このファイルにより、Select Identity フィールドと Active Directory フィールドのマッピングを制御します。また、次のようなプロパティファイルも含まれています。`ActiveDirConfig.properties`
3	`cbc_config.zip`	周期的なリクエストをブロックするようにデータベースを設定するための DDL ファイルが含まれています。
4	`Password_Installer.zip`	パスワードプラグインをインストールする実行可能ファイルが含まれています。
5	`HP Central AD Agent.zip`	HP Central AD Agent 用の DLL ファイル、実行可能ファイル、および設定ファイルが含まれます。

システム要件

Active Directory 双方向 LDAP コネクタは、以下の環境でサポートされます。

表 4　　Active Directory 双方向 LDAP コネクタのプラットフォーム一覧

Select Identity のバージョン	アプリケーションサーバーとオペレーティングシステム	データベース
4.0-4.20	Active Directory 双方向 LDAP コネクタは、Select Identity 4.0 ～ 4.20 のすべてのプラットフォーム構成でサポートされます。	

Active Directory 双方向 LDAP コネクタは、Microsoft Windows Server 2000、および Microsoft Windows Server 2003 Service Pack 1 でサポートされます。

Active Directory 双方向 LDAP コネクタは多言語化されており、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 サーバーを多言語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 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。

インストール前のタスク

LDAP ストアに対して直接ユーザをプロビジョニングするには、コネクタは安全なチャネルを通じて Active Directory リソースと通信する必要があります。コネクタと Active Directory 間で安全に通信するには、以下のタスクを実行する必要があります。

- Active Directory サーバーから Select Identity サーバーへの CA 証明書のダウンロード
  - 証明書のダウンロード
  - 証明書のエクスポート

  CA 証明書の生成に関する詳細は、81 ページの「Active Directory におけるルート CA 証明書の作成」と 83 ページの「新しい証明書を適用するための情報の生成」を参照してください。

コネクタのインストールを始める前に、Select Identity と Active Directory サーバー間で SSL (Secure Socket Layer) 接続を有効にする必要があります。

- Select Identity と Active Directory サーバー間の SSL 接続の設定
  - Active Directory 証明書のアプリケーションサーバーへのインストール
    - WebLogic 8/9 と WebSphere 5
    - WebSphere 6.1

  Select Identity 4.20 で相互認証を可能とするには、以下のタスクを実行する必要があります。
  - Select Identity 4.20 における双方向 (相互) 認証の設定
    - 相互認証の設定
    - キーローテーション

Active Directory サーバーから Select Identity サーバーへの CA 証明書のダウンロード

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

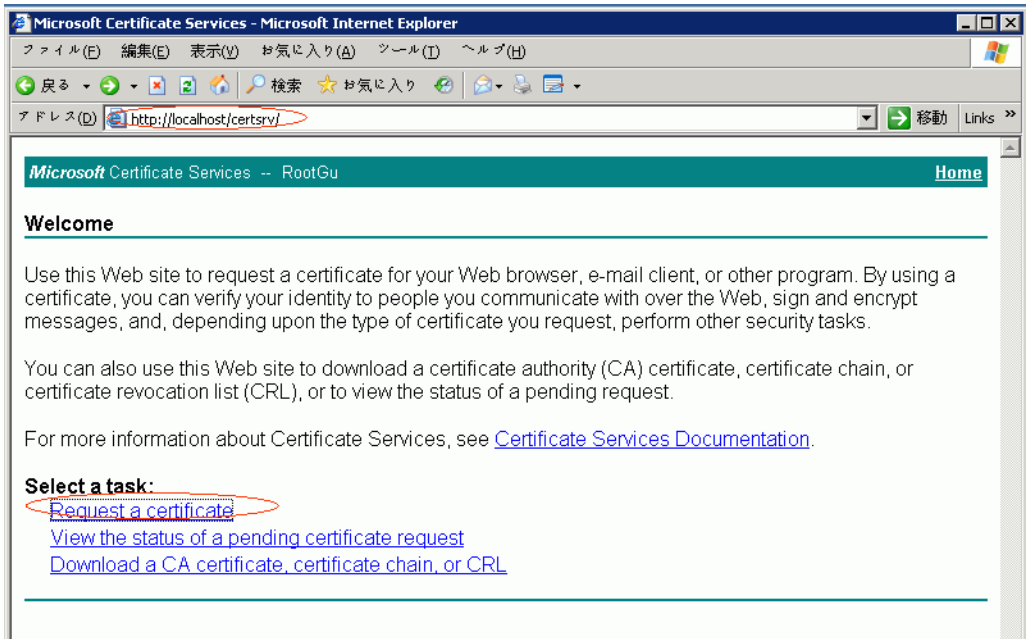
プロンプトが表示されたら、Active Directory サーバーのログイン証明書を指定します。証明書は、<アプリケーションサーバーの Java Home>`\jre\lib\security` ディレクトリにダウンロードする必要があります。

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

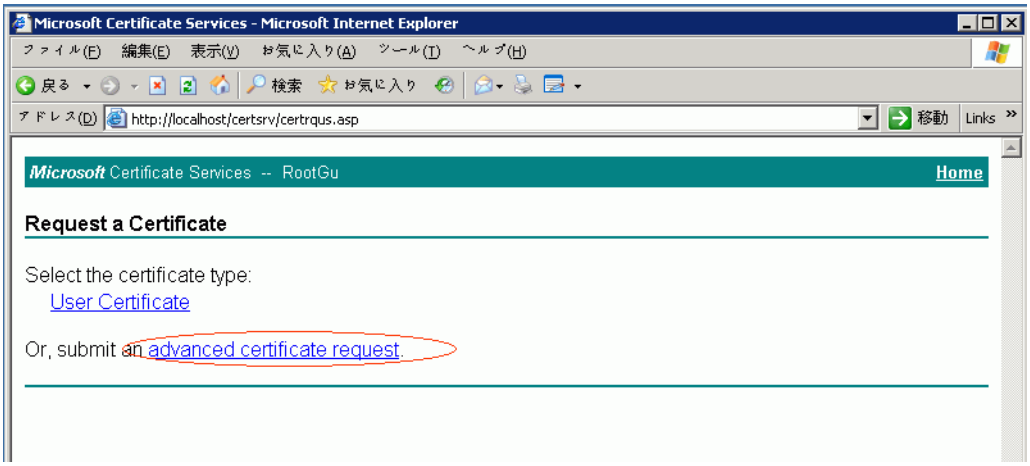
証明書のダウンロード

1 CA サーバーで Internet Explorer を開きます。

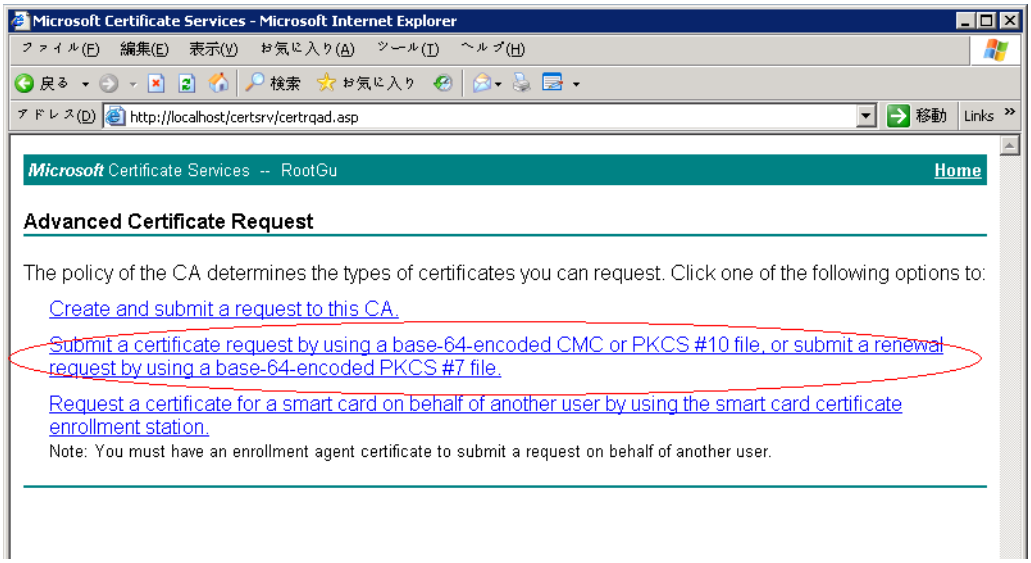
アドレスフィールドに **`http://localhost/certsrv/`** または **`http://`**<認証サーバーの IP>**`/certsrv/`** を入力し、次に **[Request a certificate]** リンクをクリックして次のページを開きます。



2 [**Request a Certificate**] ページで、**[advanced certificate request]** リンクをクリックします。

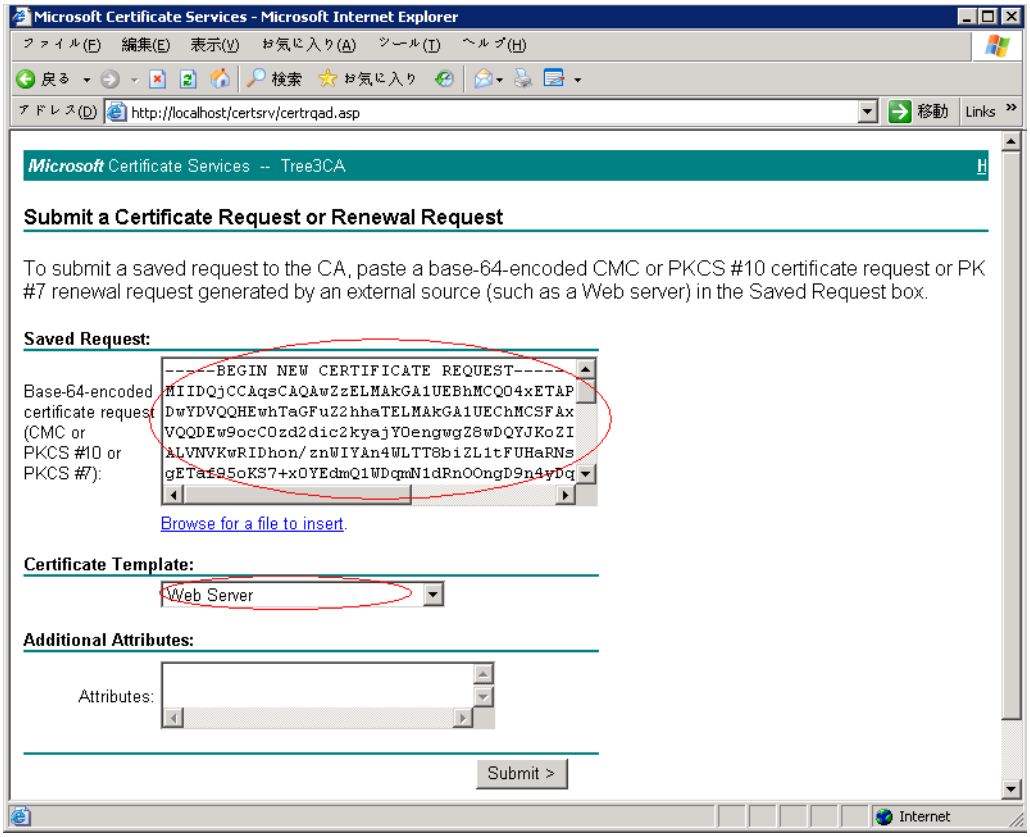


3 以下に示す 2 番目のリンクをクリックします。

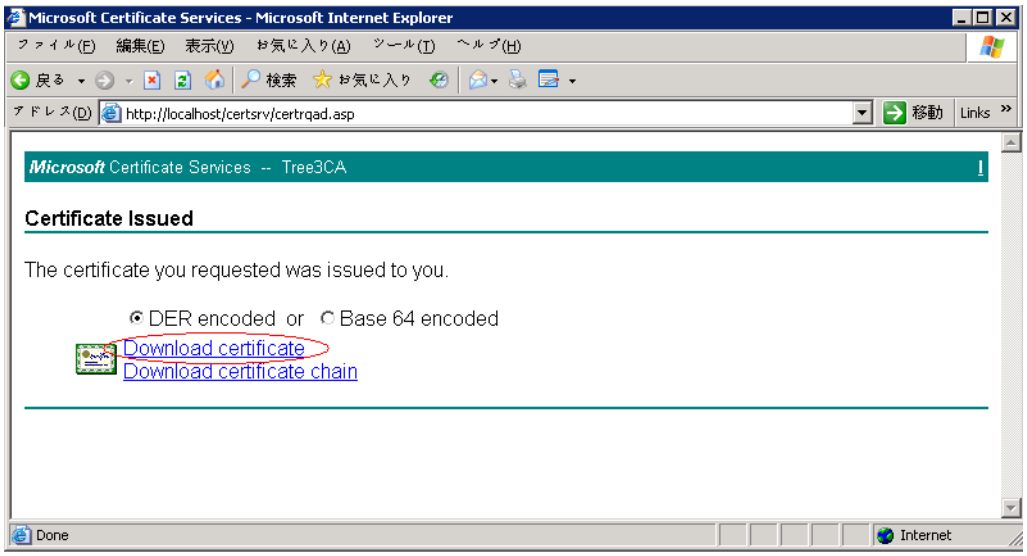


4 リクエスト情報を [保存された要求] フィールドにコピーし、[証明書テンプレート] フィールドで Web サーバーを選択します。次に、**[送信]** をクリックします。

リクエスト情報の生成方法については、83 ページの「新しい証明書を適用するための情報の生成」を参照してください。



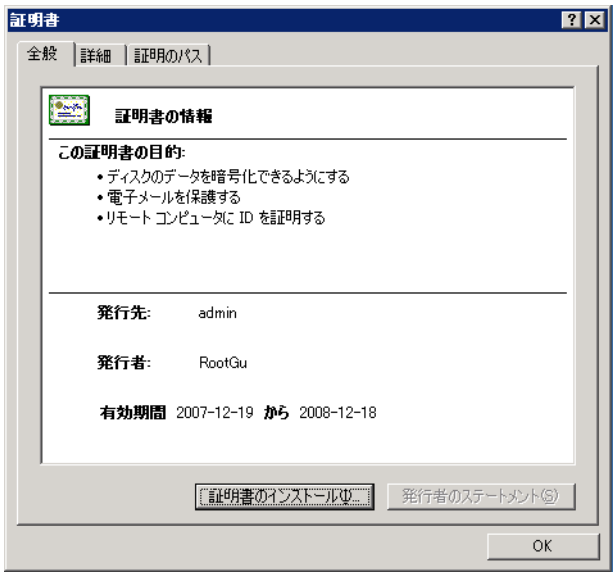
5 次のページで、**[Download certificate]** リンクをクリックします。



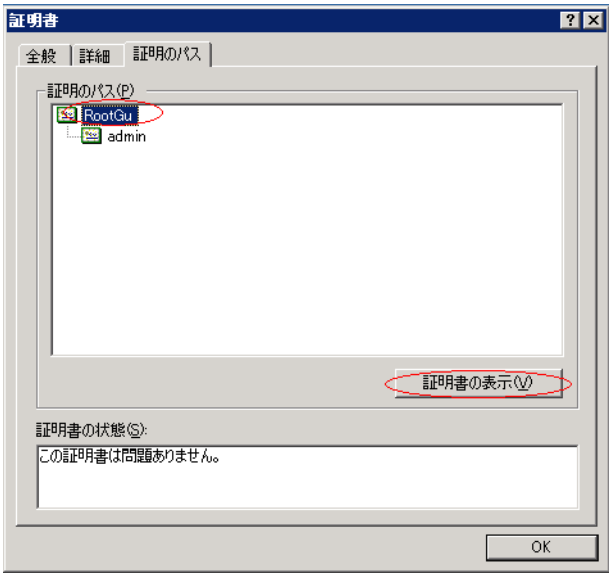
新しい証明書をダウンロードし、ローカルディスクに保存します。

証明書のエクスポート

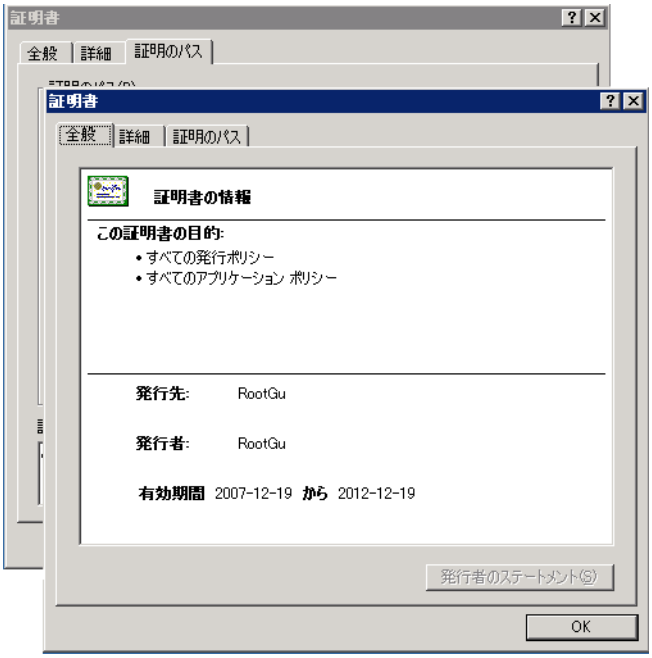
1 ダウンロードした証明書ファイルをダブルクリックして開きます。



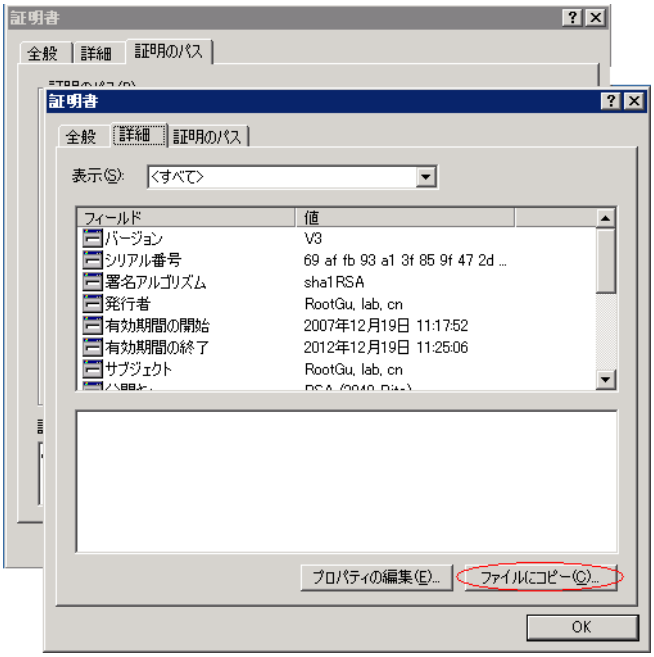
[証明のパス] タブの証明書パスを確認します。



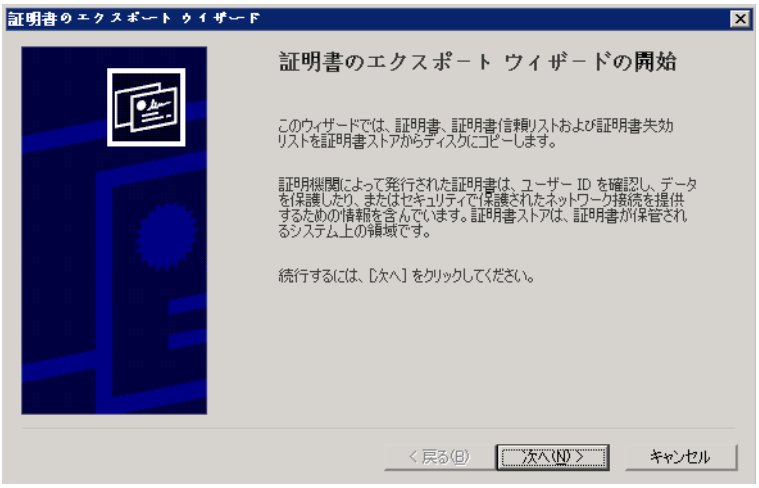
[証明書の表示] ボタンをクリックし、証明書の一般情報を表示します。



2 [詳細] タブをクリックし、次に **[ファイルにコピー]** ボタンをクリックします。



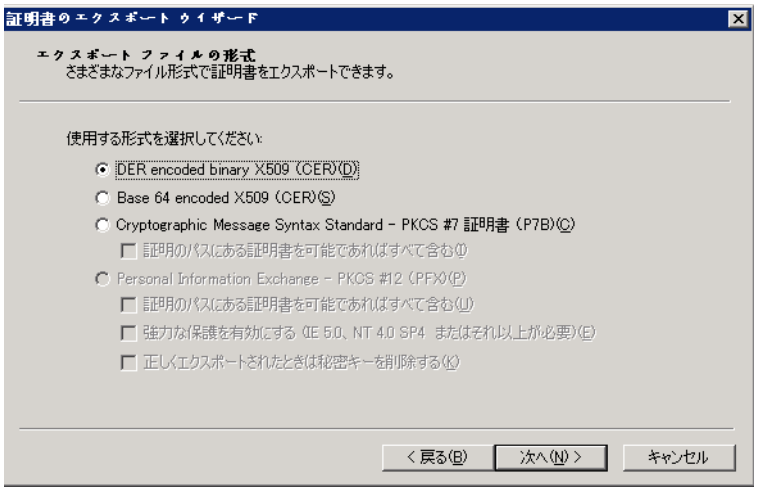
[証明書のエクスポートウィザード] が開きます。



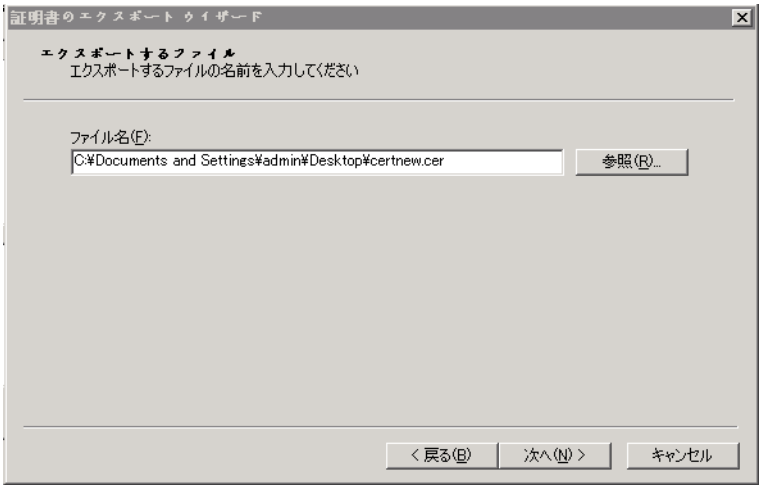
3 **[次へ]** をクリックします。

証明書のフォーマットには 3 つのオプションがありますが、最初の 2 つのみが正しく機能します。

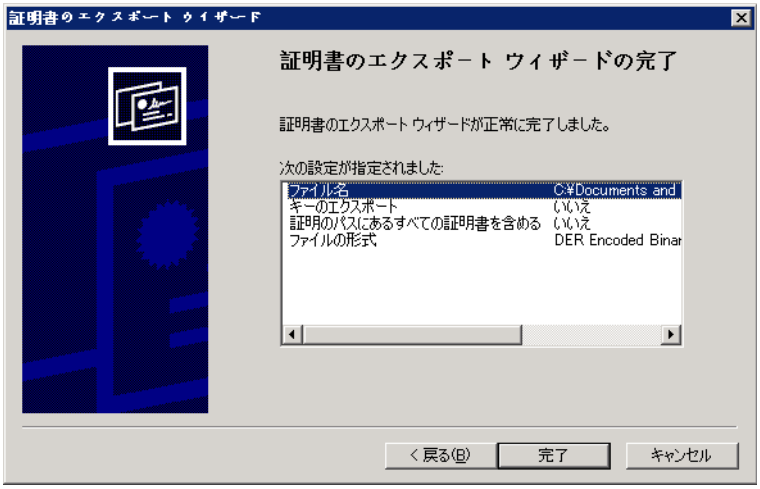
デフォルトの設定 (最初のオプション) を使用することをお薦めします。



4 **[次へ]** をクリックします。エクスポートするファイル名を指定します。



5 **[次へ]** をクリックします。



6 **[完了]** をクリックして、ルート証明書をエクスポートします。

Select Identity と Active Directory サーバー間の SSL 接続の設定

Select Identity 4.10 ～ 4.13 では、Active Directory サーバー認証のみがサポートされます。

Select Identity 4.20 では、Active Directory サーバーのみが認証される単一方向 SSL 認証と、Active Directory サーバーと Select Identity の両方が認証される双方向 (相互)SSL 認証が両方ともサポートされます。単一方向または双方向認証を可能とする方法については、58 ページの「相互認証サポートの設定」を参照してください。

単一方向 SSL 接続を通じて接続するには、Active Directory リソースを提示するサーバー証明書、またはサードパーティの証明書を Select Identity の JDK トラストストアにインポートする必要があります。

双方向 SSL 接続を通じて接続するには、Active Directory サーバーの証明書またはサードパーティの証明書を Select Identity が管理するトラストストアにインポートすることに加え、Select Identity を提示する証明書を Select Identity が管理するキーストア、および Active Directory コンピュータの信頼できるルート CA 証明書ストアにインポートする必要があります。さらに、ユーザを AD の Select Identity 証明書にマッピングする必要もあります (ユーザは、単一方向 SSL 接続で作成した権限と同じ権限を持つ必要があります)。

- [CRL の妥当性検査] と [証明書使用状況の妥当性検査] の両方が無効な場合、サーバー証明書として Active Directory 証明書、またはサードパーティの証明書を使用することを選択できます。
- [CRL の妥当性検査] または [証明書使用状況の妥当性検査] が有効な場合は、サーバー証明書としてサードパーティの証明書のみが使用できます。詳細については、58 ページの「相互認証サポートの設定」を参照してください。

表 5 は、単一方向 / 双方向 SSL 認証のために AD 証明書、またはサードパーティの証明書を使用する場合のタスク一覧を示しています。

設定タスクを開始する前に、AD SSL 接続が有効であることを確認してください。

設定タスクを終了した後で、AD サーバーを再起動してください。

表 5　　タスク一覧

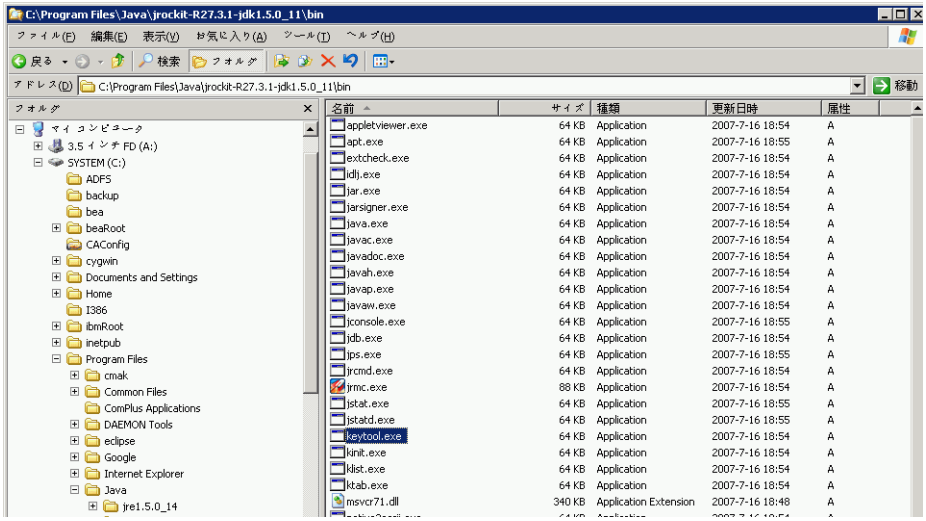
		単一方向 SSL 認証	双方向 (相互)SSL 認証
Active Directory サーバーの証明書を使用	Select Identity 側	• AD ルート証明書を JDK トラストストアにインポート 詳細については、25 ページの「Active Directory 証明書のアプリケーションサーバーへのインストール」を参照してください。	• AD ルート証明書と Select Identity ルート証明書を Select Identity トラストストアにインポート • Select Identity 証明書を Select Identity キーストアにインポート 詳細については、30 ページの「Select Identity 4.20 における双方向 (相互) 認証の設定」を参照してください。
	Active Directory 側		• Select Identity ルート証明書を AD コンピュータの信頼できるルート CA 証明書ストアにインポート • Select Identity 証明書を管理者ユーザーにマッピング 詳細については、付録 C を参照してください。
サードパーティの証明書を使用	Select Identity 側	• サードパーティのルート証明書 (AD 証明書に署名するために使用) を JDK トラストストアにインポート 詳細については、25 ページの「Active Directory 証明書のアプリケーションサーバーへのインストール」を参照してください。	• サードパーティのルート証明書 (AD 証明書に署名するために使用) と Select Identity ルート証明書を Select Identity トラストストアにインポート • Select Identity 証明書を Select Identity キーストアにインポート 詳細については、30 ページの「Select Identity 4.20 における双方向 (相互) 認証の設定」を参照してください。
	Active Directory 側	• サードパーティ証明書による署名入り AD 証明書を AD コンピュータの個人証明書ストアにインポート • サードパーティのルート証明書 (AD 証明書に署名するために使用) を AD コンピュータの信頼できるルート CA 証明書ストアにインポート 詳細については、付録 C を参照してください。	• サードパーティのルート証明書 (AD 証明書に署名するために使用) と Select Identity ルート証明書を AD コンピュータの信頼できるルート CA 証明書ストアにインポート • サードパーティの署名入り AD 証明書を AD コンピュータの個人証明書ストアにインポート • Select Identity 証明書をユーザーにマッピング 詳細については、付録 C を参照してください。

Active Directory 証明書のアプリケーションサーバーへのインストール

WebLogic 8/9 と WebSphere 5

以下の手順に従い、Active Directory 証明書を Select Identity にインストールします。

1 Active Directory 証明書をアプリケーションサーバーにインストールする前に、`keytool.exe` が使用可能かどうかを確認します。このためには、アプリケーションサーバーの Java Home に移動し、`keytool.exe` ファイルが < アプリケーションサーバーの Java Home>`/jre/bin` サブディレクトリで使用可能かどうかを確認します。Select Identity が Windows にインストールされている場合は、Windows Explorer を使用して、そのファイルを < アプリケーションサーバーの Java Home>`/jre/bin` に配置します。



2 Active Directory 証明書ファイル (< 証明書名 >`.cer`) が Select Identity システムの < アプリケーションサーバーの Java Home>`\jre\lib\security` に存在することを確認してください。

> クラスタをセットアップするために、必ず証明書をすべてのアプリケーションサーバーの < *アプリケーションサーバーの Java Home*>`\jre\lib\security` にコピーしてください。

3 コマンドプロンプトを使用し、< アプリケーションサーバーの Java Home>`jre\bin` からコマンド **`keytool -v -keystore jssecacerts -trustcacerts -import -file ..\lib\security\`**< 証明書名 >*.cer* を実行し、**jssecacerts** ファイルを生成します。

次に、生成した **jssecacerts** ファイルを < アプリケーションサーバーの Java Home>`\jre\lib\security` フォルダにコピーします。

4 パスワードを要求されたら、キーストアのパスワードを入力します (デフォルトのパスワードは **`changeit`** です)。

5 keytool は以下のメッセージを表示します。

```
Owner: CN=QA.hp.com, OU=QA, O="hp", L=abc, ST=xyz, C=mno,
EmailAddress=qa@hp.com
Issuer: CN=QA.hp.com, OU=QA, O="hp", L=abc, ST=xyz, C=mno,
EmailAddress=qa@hp.com
Serial number: 16bab38264ebda84f8011cf35d0ca6a
Valid from: Fri Jan 23 13:42:18 CST 2004 until: Fri Jan 23 13:50:22 CST
2009
```

```
Certificate fingerprints:
MD5: 60:72:A9:DD:C4:39:C4:8A:E7:42:56:0B:9E:5D:91:DB
SHA1: 38:D2:7F:33:FE:0A:AC:F3:D3:A0:2C:0F:A9:0C:6A:09:10:B5:EA:66
```

6 システムが `Trust this certificate? [no]:` と表示した場合は、**yes** または **y** を入力します。keytool は以下のメッセージを表示します。

```
Certificate was added to keystore
[Saving jssecacerts]
```

7 新しい `jssecacerts` ファイルを <アプリケーションサーバーの Java Home>`\jre\lib\security` フォルダにコピーします。

> security フォルダには上書きする必要がある `jssecacerts` ファイルがすでに存在しているので、確実にこのファイルをコピーしてください。

8 アプリケーションサーバーを再起動します。

`alias` フラグを使用することにより、新たに証明書を追加することができます。たとえば、上記の手順を実行した後、以下のコマンドを実行します。

`keytool -v -keystore jssecacerts -trustcacerts -import -file ..\lib\security\<cert-ADsample.cer>`

次のエラーメッセージが表示されます。

```
keytool error: java.lang.Exception: Certificate not imported, alias <mykey>
already exists.
```

`jssecacerts` のリストは、入力した証明書のデフォルトが `mykey` エイリアスであることを示しています。

```
mykey, Dec 22, 2004, trustedCertEntry,
Certificate fingerprint (MD5):B2:F6:42:F6:0C:88:65:EE:FB:38:3E:31:00:CA:DD:70
```

`jssecacerts` のリストを取得するには、以下のコマンドを実行します。

`keytool -list -keystore jssecacerts`

証明書 *`cert-ADsample.cer`* を新たに追加するには、以下のコマンドを実行します。

`keytool -v -keystore jssecacerts -trustcacerts -alias hp69trustca -import -file ..\lib\security\cert-ADsample.cer`

jssecacerts のリストは、次の内容になります。

```
hp69trustca, Dec 22, 2004, trustedCertEntry,
Certificate fingerprint (MD5):60:72:A9:DD:C4:39:C4:8A:E7:42:56:0B:9E:5D:91:DB
```

WebSphere 6.1

以下の手順を実行してキーストアファイルを作成し、WebShpere 6.1 が新たに作成されたキーストアを使用するように設定します。

1 キーストアファイルの作成

a LDAP 証明書ファイル (< 証明書名 >`.cer`) を < 証明書パス > 配下の Select Identity システムにコピーします。

b コマンド **`keytool -v -keystore <`** キーストア名 **`>  -import -file <`** 証明書パス **`>/<`** 証明書名 **`>.cer`** を実行します。

c パスワードを要求されたときは、キーストアのパスワードを入力します。

d keytool は以下と同様のメッセージを表示します。

```
Owner: CN=QA.hp.com, OU=QA, O="hp", L=abc, ST=efg, C=ab,
EmailAddress=qa@hp.com
Issuer: CN=QA.hp.com, OU=QA, O="hp", L=abc, ST=efg, C=ab,
EmailAddress=qa@hp.com
Serial number: 16bab38264ebda84f8011cf35d0ca6a
Valid from: Fri Jan 23 13:42:18 CST 2004 until: Fri Jan 23 13:50:22 CST
2009
Certificate fingerprints:
MD5: 60:72:A9:DD:C4:39:C4:8A:E7:42:56:0B:9E:5D:91:DB
SHA1: 38:D2:7F:33:FE:0A:AC:F3:D3:A0:2C:0F:A9:0C:6A:09:10:B5:EA:66
```

e システムが `Trust this certificate? [no]:` と表示した場合は、**`yes`** を入力します。keytool は以下のメッセージを表示します。

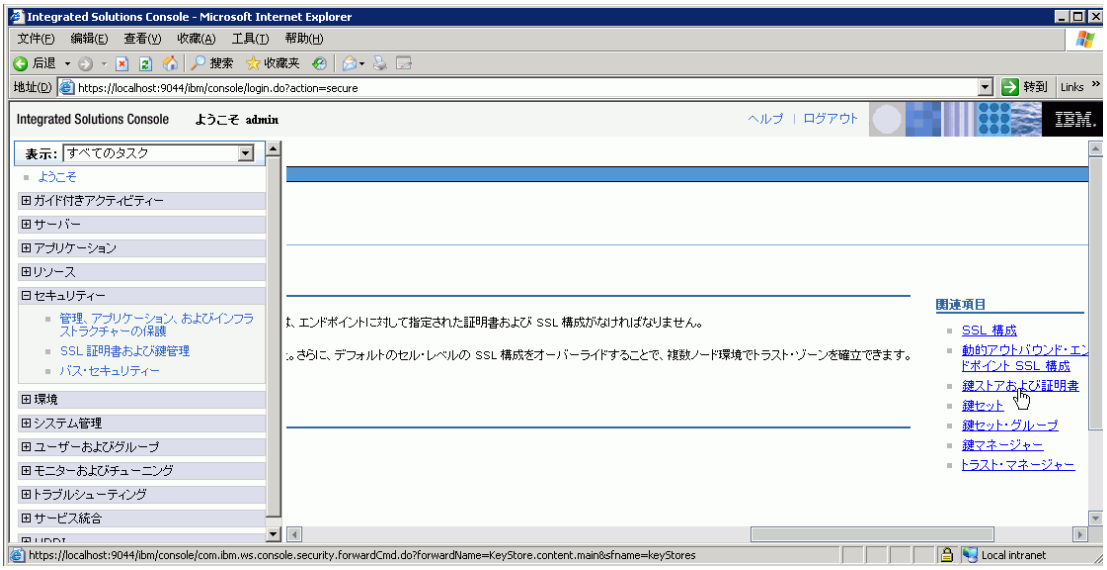
```
Certificate was added to keystore
```

2 WebSphere 6.1 が新たに作成されたキーストアを使用するための設定

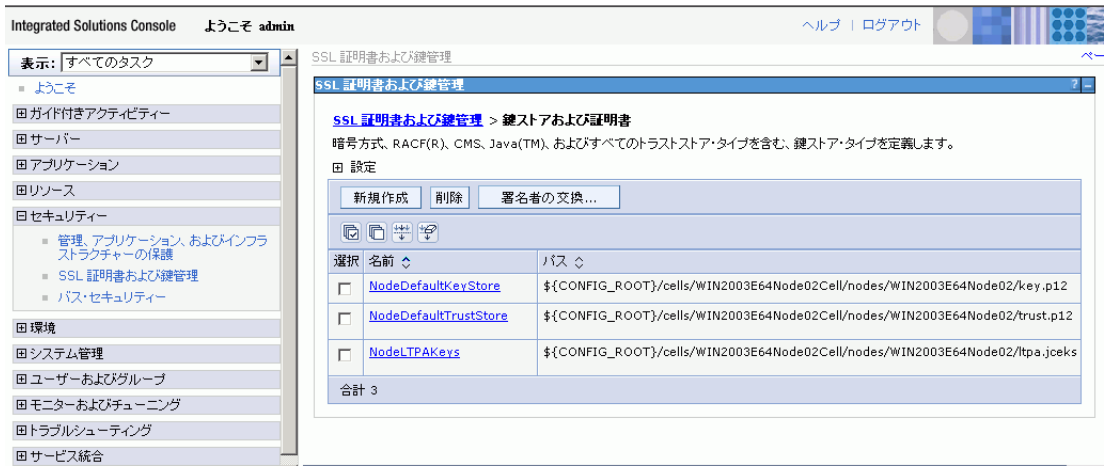
a WebSphere アプリケーションサーバーのコンソールにログオンします。

b ナビゲーションペインで、**[セキュリティ]** → **[SSL 証明書および鍵管理]** の順にクリックします。[SSL 証明書および鍵管理] ページが表示されます。

c **[関連項目]** セクションの下にある **[鍵ストアおよび証明書]** をクリックします。[鍵ストアおよび証明書] ページが表示されるので、このページですでに作成したキーストアファイルを指定する論理キーストアを定義します。



d 論理トラストストアを作成するには、**[新規作成]** をクリックします。

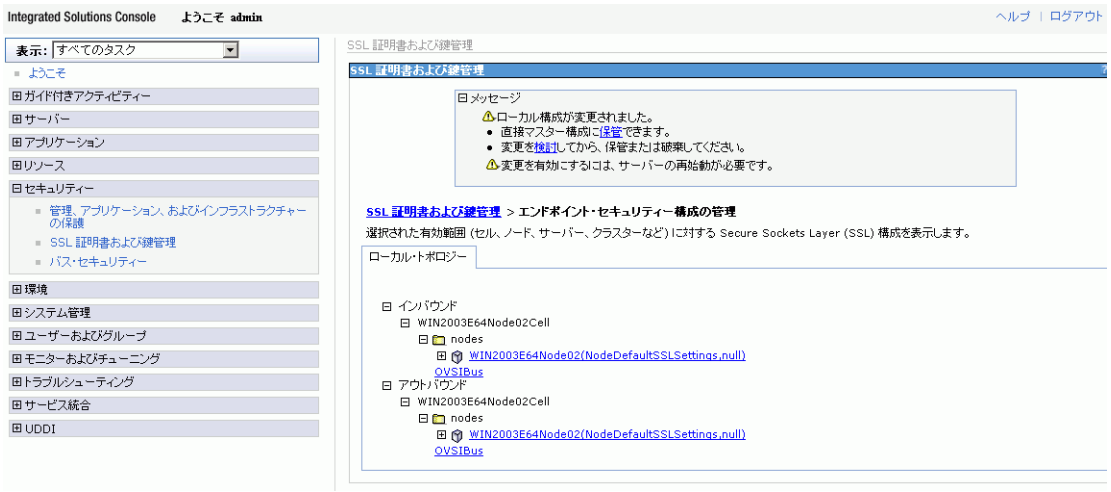


e 論理トラストストアに対して、キーストア名、キーストアパス (すでに作成したキーストアファイルを指定)、パスワード 、およびキーストアタイプ (JKS とする) を入力します。

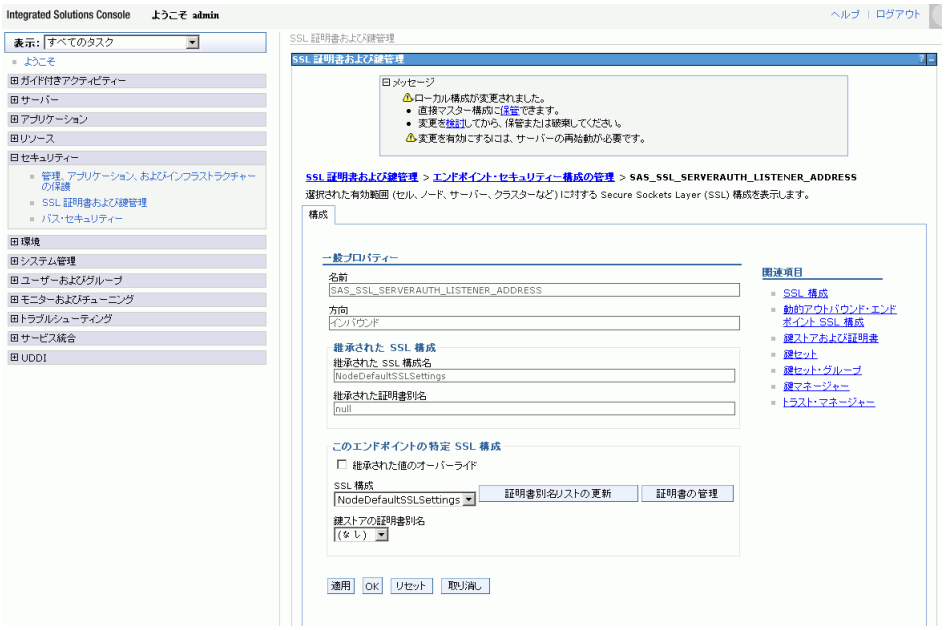
f [SSL 証明書および鍵管理] ページに戻り、**[関連項目]** セクションの **[SSL 構成]** をクリックします。[SSL 構成] ページが表示されます。

g **[新規作成]** をクリックします。新しい SSL 設定をニーズに合わせて定義します。SSL 設定は、すでに定義した新しい論理トラストストアを指定しています。

h [SSL 証明書および鍵管理] ページに戻り、**[構成]** セクションの下にある **[エンドポイント・セキュリティー構成の管理]** をクリックし、次に **[アウトバウンド]** を展開します。



i SSL 設定と証明書エイリアスを選択します。



j 変更を適用し、設定が WebSphere により保存されたことを確認します。

Select Identity 4.20 における双方向 (相互) 認証の設定

相互認証の設定

以下の手順に従って、Active Directory 双方向 LDAP 証明書をインストールします。

1 まだ作成していない場合は、Select Identity のトラストストアを作成し、プロパティを設定します。

a トラストストアを作成します。

b トラストストアファイルに対応するプロパティファイルを生成します。

キーストア、トラストストア、およびプロパティの作成に関する詳細は、『HP Select Identity インストールガイド』の「トラストストアの作成」セクションを参照してください。

2 Active Directoryリソースを示す証明書を Select Identityトラストストアにインポートします。

a Active Directory 証明書を取得します。

b 前の手順で作成したトラストストアファイルに、証明書をインポートします。

キーストア、トラストストア、およびプロパティの作成に関する詳細は、『HP Select Identity インストールガイド』の「トラストストアの作成」セクションを参照してください。

3 リソースが特定のクライアント証明書を必要とする場合は、クライアント証明書を作成するか、キーストアにインポートします。

a キーストアファイルを作成します。

b 使用できる証明書がない場合は、Select Identity サーバーを示す証明書を生成します。また、証明書がすでに存在する場合は、Select Identity サーバーを示す証明書をインポートします。

c キーストアに対応するプロパティファイルを生成します。

詳細は、『HP Select Identity インストールガイド』の「相互認証とセキュアなオブジェクト移行のキーストアならびにキーペア」セクションを参照してください。

4 まだ実行していない場合は、キーストアとトラストストアを登録し、Select Identity クライアント証明書を選択します。

a Select Identity のセキュリティセットアップツールを開きます。

b Select Identity にキーストアプロパティを登録します。

c Select Identity にトラストストアプロパティを登録します。

d 必要に応じて、Select Identity サーバーを示す証明書を選択します。

詳細は、HP Select Identity 管理者向けオンラインヘルプのシステムセキュリティの設定というトピックを参照してください。

キーローテーション

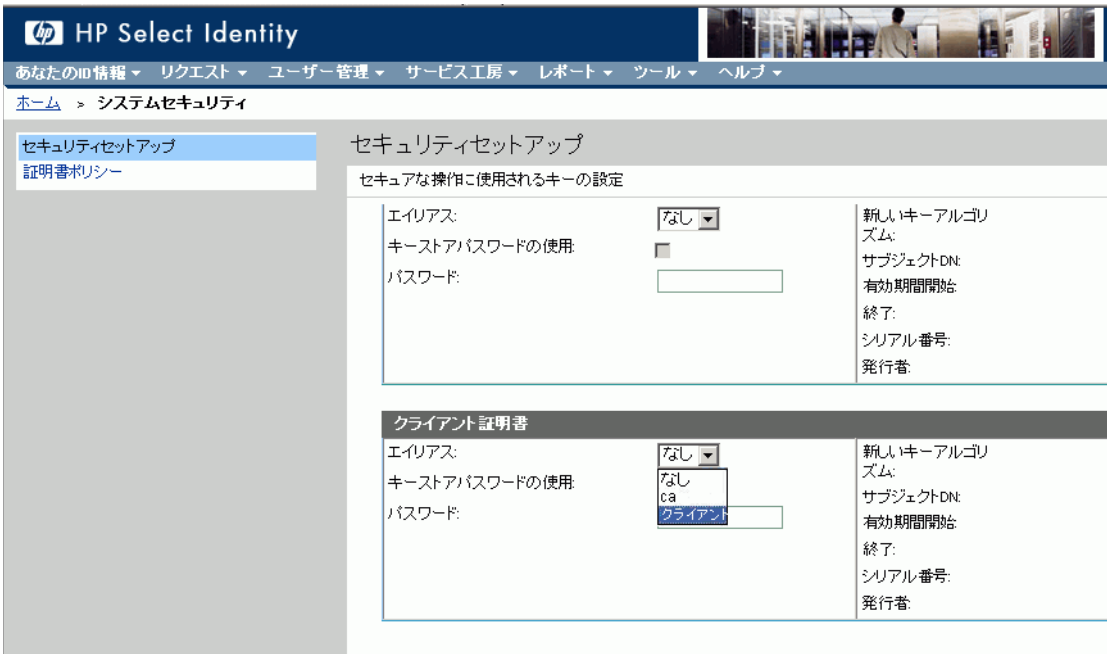
キーローテーションは、Select Identity がさまざまなキーを使用してリソースに接続するための手順です。その手順は以下のとおりです。

1 キーストアの新しいキーペアを生成します。

詳細は、『HP Select Identity インストールガイド』の「相互認証キーの作成」セクションを参照してください。

2 システムセキュリティセットアップでキーアライアスを変更します。

a [**ツール**] メニューから [**システムセキュリティ**] → [**セキュリティセットアップ**] を選択します。[セキュリティセットアップ] ページが開きます。



b [クライアント証明書] セクションで、新たに生成された証明書を選択します。

スキーマ JAR ファイルの解凍

コネクタのスキーマ JAR ファイルには、リソース属性を Select Identity にマッピングするのに必要なマッピング情報が含まれています。ActiveDirSchema.jar ファイルをアプリケーションサーバーの CLASSPATH 内にあるディレクトリに解凍します。スキーマ JAR ファイル解凍の詳細な手順については、『HP Select Identity Connector Deployment Guide』を参照してください。

XML およびプロパティファイルを解凍し、それらを Select Identity インストールディレクトリの**スキーマ**フォルダに配置することをお薦めします。

設定可能パラメータの確認

ActiveDirSchema.jar ファイル内に存在する ActiveDirConfig.properties ファイルなどのプロパティファイルには、以下に示すような設定可能パラメータが含まれています。これらのパラメータは手動で変更可能です。コネクタをインストールする前にパラメータの値を確認し、以下に示す値と一致しない場合は値を変更してください。

ほとんどの場合、ActiveDirSchema.jar ファイルには 1 つのプロパティファイルのみが存在し、通常そのファイルは ActiveDirConfig.properties という名前です。ファイル名は、利用しやすい名前にカスタマイズできます。たとえば、***ActiveDirConfig***.properties を ***ADConfigNew***.properties に変更し、特定のリソースに対応させることができます。特に複数のリソースが存在する場合は便利です。ファイルの拡張子は変更できないので注意してください。

属性を手動で追加する方法については、95 ページの「スキーマファイルのカスタマイズ」を参照してください。

カスタマイズできないパラメータ

以下のパラメータと説明は、参考のための情報です。これらのパラメータの値は、変更しないことをお薦めします。

- `entitlement-delimiter=|`

  使用権のタイプと名前の間に表示される区切り文字を指定します。

- `modify_replace=false`

  true または false をセットする設定パラメータです。false に設定すると、Active Directory 双方向 LDAP コネクタは変更 / 追加および変更 / 削除操作を使用して、複数値属性をサポートします。true を設定すると、Active Directory 双方向 LDAP コネクタは変更 / 置換操作を使用して、複数値属性をサポートします。

- `attribute-begins=[[`

  Select Identity からコネクタへの送信中に、base64 で特別にエンコードされた属性値を囲むための開始パラメータです。

- `attribute-ends=]]`

  Select Identity からコネクタへの送信中に、base64 で特別にエンコードされた属性値を囲むための終了パラメータです。

- `dualLink-support=2`

  リンクがユーザーリンクか、またはグループリンクかを指定します。1 の場合はユーザーリンクであり、2 の場合はグループリンクです。

- `unlink-before-terminate=false`

  ユーザー操作の停止中に使用権をアンリンクしたい場合は、このフラグに false を設定します。

- `null-entitlement-support=true`

  このパラメータには `true` を設定します。

- `entitlement-provisioning=true`

  このパラメータに true を設定した場合、コネクタは使用権のプロビジョニングをサポートします。それ以外の場合は、使用権はプロビジョニングされません。

- `ldapv3-pageSize=900`

  LDAP API を照会するときに返されるエントリの数です。

- `number-of-retries=3`

  フェイルオーバーの再試行回数です。

- `retry-delay=1`

  再試行の間隔 (秒) です。

カスタマイズ可能なパラメータ：

以下のパラメータは、カスタマイズ可能です。ニーズに合わせて、以下のパラメータの *italic* (斜体) 部分を変更できます。

> システムが実稼動環境に移行した後は、しばらくの間何も変更しないことをお薦めします。

- PSSync_ATTRIBUTE=*description*

  この Active Directory 属性は、パスワードプラグインがユーザーの暗号化パスワードを一時的に格納するために使用します。この属性名は、Select Identity AD コネクタのプロパティファイル、およびパスワードプラグインのプロパティファイルの両方に保存されます。エージェント ini ファイル (ADProperties.ini) の設定に関する詳細は、47 ページの手順 12 を参照してください。

  パスワードプラグインがインストールされていない場合は、値は空になります (たとえば、PSSync_ATTRIBUTE= のように設定できます)。

- OVSI.ADConnector.groupid.attribute=

  ここでは、Select Identity グラフィカルユーザーインタフェースにおける OVSI AD コネクタグループの表示名を指定します。このパラメータには、以下の 4 つの値を指定できます。

  — *dotFormat* – グループ名のデフォルトフォーマットが表示されます。グループの distinguishedName を表示するために、区切り文字として“.”が使用されます。たとえば、AD でグループの distinguishedName が“cn=group1,OU=Test,DC=root,DC=sicf”だった場合、“Group|group1.Test.root.sicf”と表示されます。

  — *cn* – グループの共通名が表示されます。共通名は、マルチドメインと同様に、フォレスト内で**一意**である必要があります。ただし、異なったドメインでは重複が可能です。したがって、共通名をグループ表示名として使用したい場合は、**フォレスト内で一意であることを確認してください**。以上が、共通名をグループの表示名として使用する場合の制限です。

  — *distinguishedName* – グループの識別名が表示されます。

  — *description* – グループの説明が表示されます。この説明はフォレスト内で**一意**である必要があり、最大文字数は 100 文字です。説明が空の場合は、パラメータはグループの表示名として *cn* (共通名) を使用します。以上が、説明をグループの表示名として使用する場合の制限です。

  > パラメータ値として dotFormat または distinguishedName を使用することをお薦めします。

以下の 5 つのパラメータは、ドメイン間でユーザーを移動する機能のためのものです。

- OVSI.Command.Message.Request.Attribute=info

  ユーザーをドメイン間で移動するためのリクエスト情報を一時的に格納するために、Active Directory 属性を指定します。

- OVSI.Command.Message.Response.Attribute=info

  ユーザーをドメイン間で移動するためのレスポンス情報を一時的に格納するために、Active Directory 属性を指定します。

- OVSI.Command.Message.Delimeter=#####

ユーザーをドメイン間で移動するためのパラメータを分割するために、リクエストおよびレスポンス情報で使用します。

以下に示すように、上記 3 つの属性には PasswordAgent-config.xml 内の属性と同じ属性値を持たせてください (この xml は、ユーザーのドメイン間の移動をサポートするコンピュータの System32 ディレクトリに存在します)。

```
<?xml version="1.0" encoding="utf-8" ?>
- <PasswordAgent-config>
  - <constants-config>
      <constant name="request" attribute="info" />
      <constant name="response" attribute="info" />
      <constant name="delimiter" value="#####" />
    </constants-config>
  - <action-mappings>
      <action message="moveUserAcrossDomains" assembly="HP.AD.WNF.MoveUser"
        className="HP.AD.WNF.MoveUser.MoveUserAction" />
    </action-mappings>
  </PasswordAgent-config>
```

- OVSI.Command.Message.DeleteTransientUser=true

  ドメイン間のユーザーの移動が完了したときに、Active Directory 内の一時的なユーザーを削除するかどうかを指定します。

- OVSI.Command.Message.Retrieve.Intervals=10

  再試行の間隔 (秒) です。

- OVSI.Command.Message.Retrieve.Times=8

  再試行の回数です。

- # AD forest configuration

  # ------------------------

  OVSI.ADConnector.gc.count=***1***

  OVSI.ADConnector.gc.0=*rootdc1.root.sicf*

  OVSI.ADConnector.gc.0.port=*3268*

  OVSI.ADConnector.gc.0.domain=*dc=root,dc=sicf*

  OVSI.ADConnector.domain.count=***3***

  # Domain 1

  OVSI.ADConnector.domain.0=*dc=root,dc=sicf*

  OVSI.ADConnector.domain.0.userSuffix=*ou=selectidentity,ou=openview*

  OVSI.ADConnector.domain.0.groupSuffix=*ou=selectidentity,ou=openview*

  OVSI.ADConnector.domain.0.transientUserSuffix=ou=*transientuserSuffix*

  OVSI.ADConnector.domain.0.dc.count=*2*

  OVSI.ADConnector.domain.0.dc.0=*rootdc1.root.sicf*

  OVSI.ADConnector.domain.0.dc.0.port=*636*

```
OVSI.ADConnector.domain.0.dc.1=rootdc2.root.sicf
OVSI.ADConnector.domain.0.dc.1.port=636

# Domain 2
OVSI.ADConnector.domain.1=dc=child1,dc=root,dc=sicf
OVSI.ADConnector.domain.1.userSuffix=ou=selectidentity,ou=openview
OVSI.ADConnector.domain.1.groupSuffix=ou=selectidentity,ou=openview
OVSI.ADConnector.domain.1.transientUserSuffix=ou=transientuserSuffix
OVSI.ADConnector.domain.1.dc.count=1
OVSI.ADConnector.domain.1.dc.0=child1dc1.child1.root.sicf
OVSI.ADConnector.domain.1.dc.0.port=636

# Domain 3
OVSI.ADConnector.domain.2=dc=child2,dc=root,dc=sicf
OVSI.ADConnector.domain.2.userSuffix=ou=selectidentity,ou=openview
OVSI.ADConnector.domain.2.groupSuffix=ou=selectidentity,ou=openview
OVSI.ADConnector.domain.2.transientUserSuffix=ou=transientuserSuffix
OVSI.ADConnector.domain.2.dc.count=1
OVSI.ADConnector.domain.2.dc.0=child2dc1.child2.root.sicf
OVSI.ADConnector.domain.2.dc.0.port=636
```

以下は、上記プロパティの説明です。

1) OVSI.ADConnector.gc.count=*1*

2) OVSI.ADConnector.gc.0=*rootdc1.root.sicf*

3) OVSI.ADConnector.gc.0.port=*3269*

4) OVSI.ADConnector.gc.0.domain=*dc=root,dc=sicf*

5) OVSI.ADConnector.domain.count=*3*

この 5 行は、AD フォレストの設定情報です。

— 1) **OVSI.ADConnector.gc.count** プロパティは、フォレスト内のグローバルカタログ数を決定します。この例では、フォレスト内に 1 つのグローバルカタログのみが存在します。

OVSI.ADConnector.gc.count プロパティ値が 2 の場合は、2 番目のグローバルカタログ用コンピュータの省略しない名前とポート番号、およびドメイン名を示すために、新たに 3 行が追加されます。

— 2) **OVSI.ADConnector.gc.0**=rootDC1.root.sicf プロパティは、グローバルカタログが存在するコンピュータの省略しない名前が rootDC1.root.sicf であることを示しています。

— 3) **OVSI.ADConnector.gc.0.port**=*3268* プロパティは、コンピュータのポート番号が 3268 であることを示しています。

単一方向認証が有効な場合、グローバルカタログのポートは 3268 に設定する必要があります。双方向認証が有効な場合、グローバルカタログのポートは **3269** に設定する必要があります。

— 4) **OVSI.ADConnector.gc.0.domain**=DC=root,DC=sicf プロパティは、ドメイン名が DC=root,DC=sicf であることを示しています。

— 5) **OVSI.ADConnector.domain.count** プロパティは、フォレスト内のドメイン数を決定しますが、このプロパティ値はそれぞれの環境によって異なります。この例では、プロパティ値が 3 であり、この環境に 3 つのドメインが存在することを示しています。

6) # Domain 1

7) OVSI.ADConnector.domain.0=*dc=root,dc=sicf*

8) OVSI.ADConnector.domain.0.userSuffix=*ou=selectidentity,ou=openview*

OVSI.ADConnector.domain.0.groupSuffix=*ou=selectidentity,ou=openview*

9) OVSI.ADConnector.domain.0.transientUserSuffix=*ou=transientuserSuffix*

10) OVSI.ADConnector.domain.0.dc.count=*2*

11) OVSI.ADConnector.domain.0.dc.0=*rootdc1.root.sicf*

...

OVSI.ADConnector.domain.count プロパティに続くコード行は、ドメイン特有のプロパティ情報です。

Domain 1 の場合

— 7) OVSI.ADConnector.domain.0=*dc=root,dc=sicf* プロパティは、ドメイン名が dc=root,dc=sicf であることを示しています。

— 8) OVSI.ADConnector.domain.0.userSuffix プロパティと OVSI.ADConnector.domain.0.groupSuffix プロパティは、それぞれドメイン内のユーザー接尾辞とグループ接尾辞を示しています。

UserSuffix は、コネクタがプロビジョニングや変更の検出が可能なユーザーの先頭位置です。UserSuffix が空に設定されている場合、コネクタはドメイン内のすべてのユーザーを管理できます。たとえば、親として“*ou=openview*”が存在し、コネクタにその配下のユーザーのみを管理させたい場合は、プロパティファイルに“*ou=openview*”を設定します。ユーザー属性 (Select Identity の UserSuffix) が“ou=ca, ou=openview”に設定されている場合、ユーザーは子の“ou=ca”に対してプロビジョニングされます (ドメインコントローラに子の OU が既に存在していることを確認してください。)

GroupSuffix は、コネクタがユーザー使用権を取得し、メンバーの変更を検出できるグループの先頭位置です。このリリースの制限として、1 つのグループ位置のみが指定可能です。また、空の設定をすることはできません。

— 9) OVSI.ADConnector.domain.0.transientUserSuffix= プロパティは、ドメインの一時的なユーザーの接尾辞を示しています。ドメイン間でユーザーを移動した場合、コネクタは自動的に transientUserSuffix OU 配下に一時的なユーザーを作成します。**この OU が AD サーバーに存在することだけを確認してください。**

— 10) OVSI.ADConnector.domain.0.dc.count プロパティは、ドメイン内のドメインコントローラ数を示します。

— 11) `OVSI.ADConnector.domain.0.dc.0` プロパティは、DC が存在するコンピュータの省略しない名前を示します。

残りのプロパティについては、これまでのプロパティから類推できます。

フォワードプロビジョニング、またはリバースプロビジョニングを行う場合、**`groupSuffix`** で指定した範囲のグループのみが Select Identity サーバーに表示されます。

コネクタ RAR のインストール

コネクタの RAR ファイル (`ActiveDirConnector.rar` または `ActiveDirConnector_WL9.rar`) を Select Identity サーバーにインストールするには、まずそのファイルを Select Identity のローカルサブディレクトリにコピーし、その上でアプリケーションサーバーにファイルを配布する必要があります。アプリケーションサーバーへの RAR ファイルの配布については、『HP Select Identity Connector Deployment Guide』の第 4 章を参照してください。

WebSphere に RAR を配布するときは、JNDI プール名を次のように入力します。
`eis/ActiveDirConnector`

周期的リクエストをブロックするための Select Identity システムデータベースの設定

Active Directory 双方向 LDAP コネクタは、フォワードプロビジョニングと変更検出の両方をサポートします。リソースでフォワード操作を実行した場合、あたかも Active Directory システムで直接実行されたかのように、コネクタの次のポーリングサイクルでこの操作が検出されます。これは周期的リクエストと呼ばれます。周期的リクエストをブロックするには、Select Identity データベースの設定が必要となります。

以下の手順に従って、周期的リクエストをブロックします。

1. Select Identity データベースで DDL ファイル (Microsoft SQL Server データベースの場合は `mssql_cbc_ddl.sql`、Oracle データベースの場合は `Oracle_cbc_ddl.sql`) を実行します。このファイルは、`cbc_config.zip` に存在します。
2. `ActiveDirConfig.properties` ファイルを変更します。

   `CBCDatasource – JNDIName`、および `CBCDatasource – Repository` パラメータを以下のように設定します。2 つのパラメータは `ActiveDirConfig.properties` ファイルに格納されます。

   ```
   CBCDatasource – JNDIName=jdbc/TruAccess
   CBCDatasource – Repository=< データベースタイプ >
   ```

   この場合、< *データベースタイプ* > は Select Identity のデータベースです (Oracle データベースの場合は `Oracle`、Microsoft SQL Server データベースの場合は `mssql` です)。

   Select Identity の接続プール、および JDBC データソースを使用して、データベースの読み込み / 書き込みを行います。

- コネクタを V2.01 から上位バージョンにアップグレードする場合、コネクタリリースフォルダに含まれる以下の SQL スクリプトを実行して、DB テーブルをアップグレードします。

  Oracle の場合：

  `Oracle_cbc_upgrade_ddl.sql` スクリプトファイルを実行します。

  SQL Server の場合：

  `mssql_cbc_upgrade_ddl.sql` スクリプトファイルを実行します。

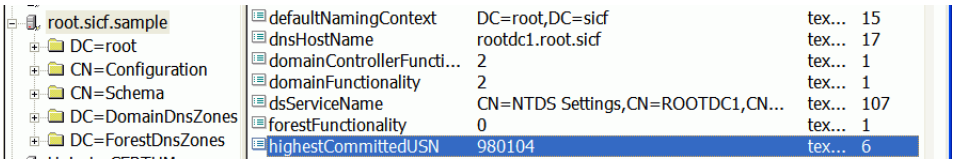
- リソースの作成を完了するたびに、データベースで以下のスクリプトを実行し、対応するエントリを `ovsi_bidirldap_lcln` テーブルに追加してください。エントリの数は、フォレスト全体のドメインコントローラの数により決定されます。

  ```
  insert into ovsi_bidirldap_lcln values('rootDC3.root.sicf','330612','ELDAPADsample')
  ```

  この例の説明

  - *'rootDC3.root.sicf'* は、調整を実行するドメインコントローラの省略しないドメイン名です。
  - *'330612'* は、各ドメインコントローラの最後に変更したログ番号です。

    Active Directory サーバーの最後に変更したログ番号を取得するには、以下の例に示すように、LDAP ブラウザを使用してパラメータ `highestCommittedUSN` の値を取得します。

  - *'ELDAPADsample'* は、Select Identity サーバーで作成したリソース名です。

  このスクリプトは `config.sql` という名前で `cbc_config.zip` パッケージにも存在します。

  この SQL 文は、設定ファイルに定義されたドメインに 1 つだけドメインコントローラが存在する場合のみ適用されます。

JBoss サポートの構成

コネクタを JBoss アプリケーションサーバーで使用するには、コネクタの `<ActiveDirConnector-ds.xml>` ファイル (*<JBoss_HOME_DIR>*`/server/profile/deploy/` フォルダに格納) を変更します。`conectorName` および `jndiName` の 2 つの `config-property` 属性を追加して、JNDI 名を設定します。

変更後、xml ファイルは以下のサンプルのようになるはずです。

```
<?xml version="1.0" encoding="UTF-8"?>


<connection-factories>

    <no-tx-connection-factory>
```

```
        <jndi-name>eis/ActiveDirConnector</jndi-name>
        <use-java-context>false</use-java-context>
        <rar-name>ActiveDirConnector.rar</rar-name>
        <connection-definition>com.trulogica.truaccess.connector.SIConnectorFactory</
        connection-definition>
        <config-property name="connectorName"
        type="java.lang.String">ActiveDir</config-property>
        <config-property name="jndiName" type="java.lang.String">eis/
        ActiveDirConnector</config-property>
    </no-tx-connection-factory>
</connection-factories>
```

4　エージェントのインストール

この章では、Active Directory 双方向 LDAP コネクタ用エージェントの概要について説明します。この章で説明する内容は以下のとおりです。

- エージェントの役割。
- エージェントのインストール手順。

エージェントについて

Active Directory 双方向 LDAP コネクタは、パスワードプラグインエージェントモジュールに同梱されています。パスワードプラグインは、Active Directory システムでのあらゆるパスワードの変更を検出します。

パスワードプラグインのインストール

エージェントインストールウィザードを使用して、パスワードプラグインを Active Directory サーバー (グローバルカテゴリ) にインストールしてください。

パスワードプラグインはパスワードの調整を行うために、Active Directory システムでのあらゆるパスワードの変更を検出します。

インストール中に **[Support move user across domain]** を選択すれば、パスワードプラグインはドメイン間のユーザーの移動をサポートします。

現在、エージェントには、32 ビットと 64 ビットの両方の AD サーバーで使用できる別のバージョンが存在します。

Active Directory のマルチドメインフォレスト環境では、HP Central AD Agent のセットアッププユーティリティを実行し、パスワードプラグインをすべてのドメインコントローラサーバーに配布します。

HP Central AD Agent をインストールする際には、必ずパスワードプラグインをインストールしたときと同じコンピュータにインストールしてください。

準備作業

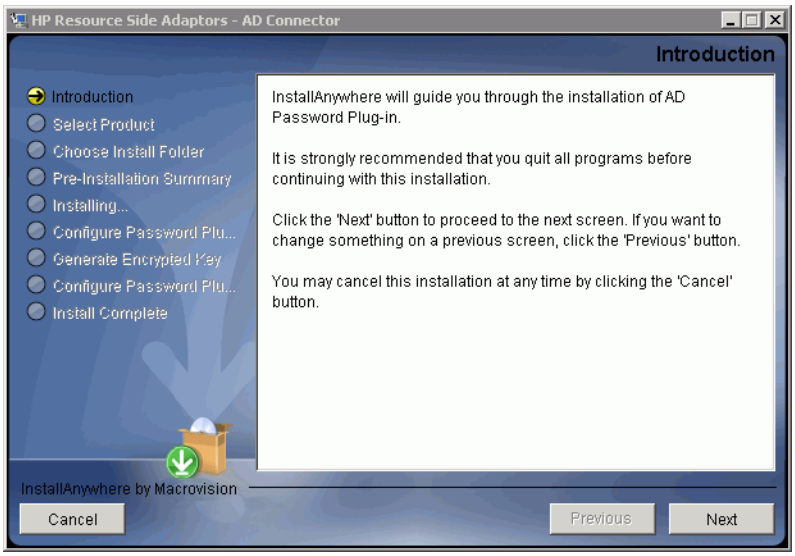
インストーラを起動する前に、以下の手順を実行します。

`Password_Installer.zip` ファイルを、Active Directory システムのローカルディレクトリ (< インストーラディレクトリ >) に解凍します。すると、自動フォルダインストーラプログラム `setup.exe` が、< インストーラディレクトリ >`\Disk1\InstData\NoVM` に格納されます。

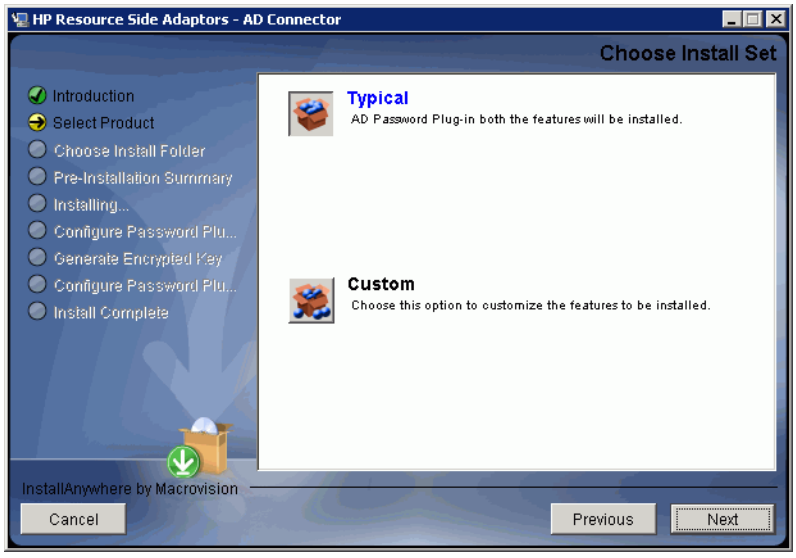
パスワードプラグインをインストール。

以下の手順を実行し、ウィザードに従ってパスワードプラグインをインストールします。

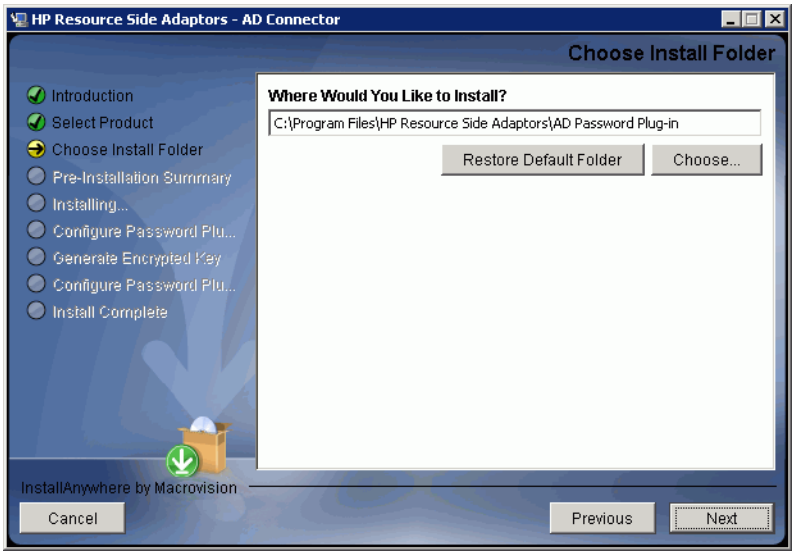
1 リソースシステムの < インストーラディレクトリ >\Disk1\InstData\NoVM ディレクトリに存在する setup.exe を実行します。インストールウィザードが表示されます。



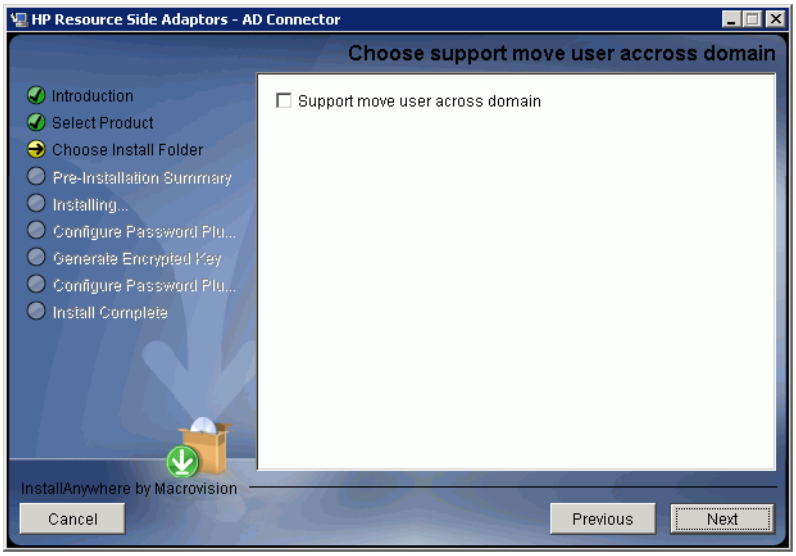
2 **[Next]** をクリックして、インストールを開始します。[Choose Install Set] 画面が表示されます。



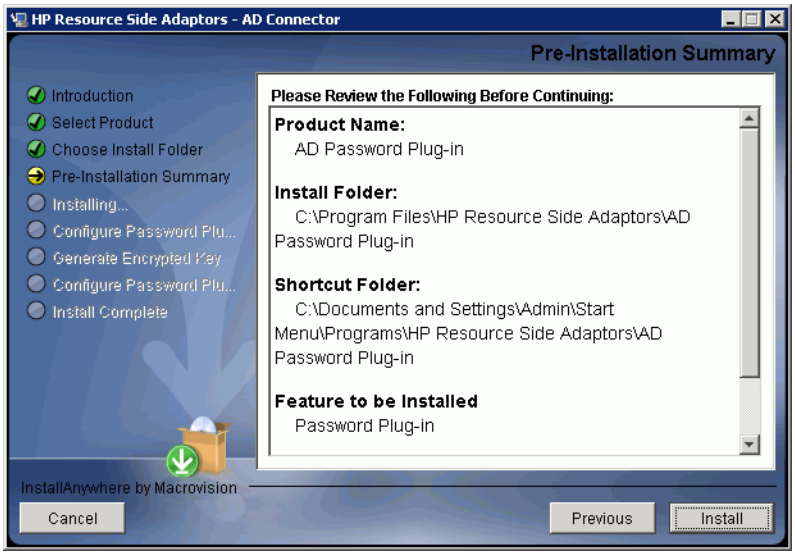
3 [Typical] インストールセットを選択し、**[Next]** をクリックします。[インストール先フォルダの選択] 画面が表示されます。



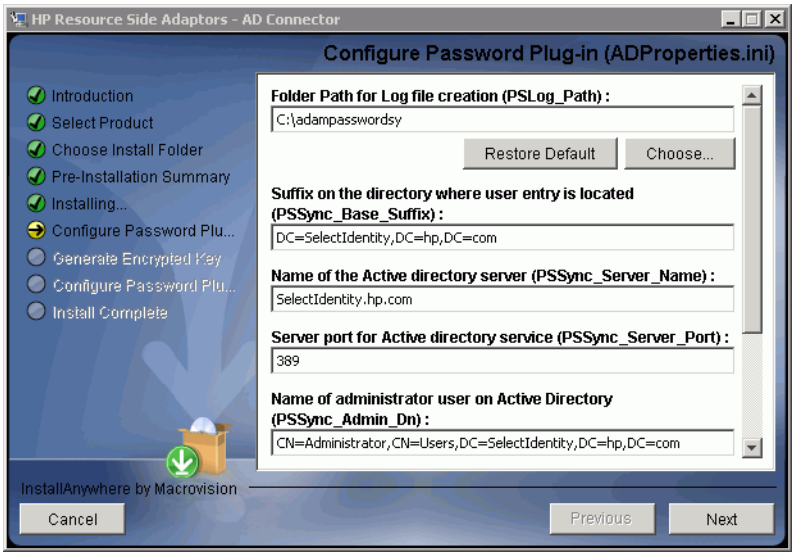
4 ドメイン間のユーザー移動のサポートを希望する場合は、**[Support move user across domain]** を選択し、それ以外の場合は未選択のままにします。

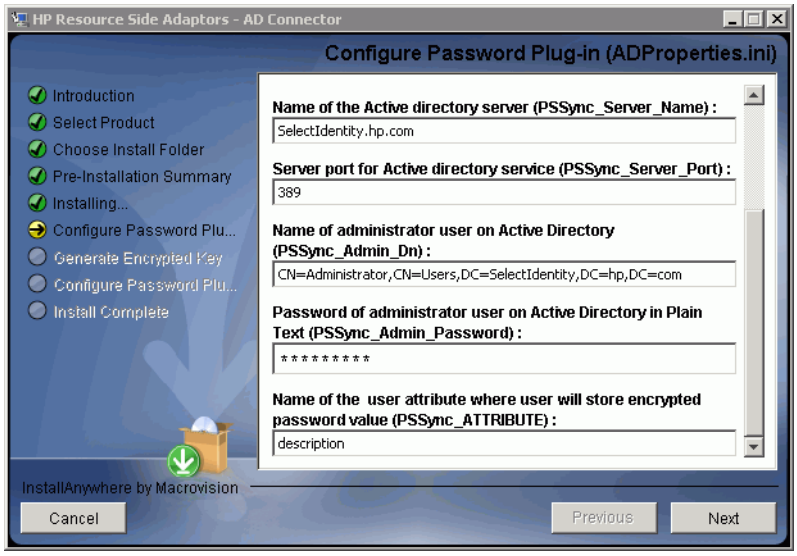


5 パスワードプラグインの場所を指定し、**[Next]** をクリックします。[Pre-Installation Summary] 画面が表示されます。



6 概要情報を確認し、**[Install]** をクリックしてインストールを開始します。[Configure Password Plug-in (ADProperties.ini)] 画面が表示されます。



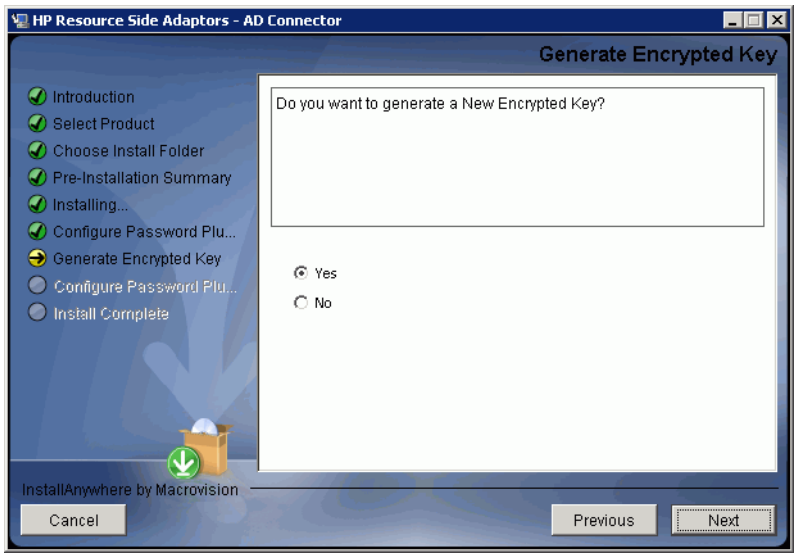


テキストフィールドに、以下のパラメータを入力する必要があります。

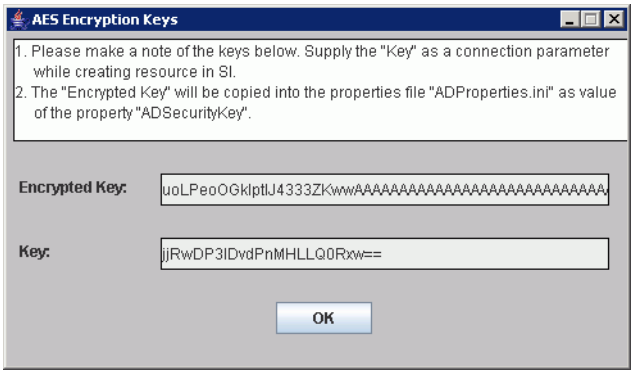
- `PSLog_Path`: ログファイルを作成するフォルダ名 (ファイル名ではない) です。このフィールドに Active Directory サーバーの既存の場所を指定するか、または Active Directory サーバーに新しいフォルダを作成し、そのフォルダのパスを入力します。
- `PSSync_Base_Suffix`: ユーザーエントリが配置された Active Directory のベース接尾辞です。(例 : DC=SelectIdentity,DC=hp,DC=com)
- `PSSync_Server_Name`: Active Directory サーバーの名前です (例 : SelectIdentity.hp.com)。
- `PSSync_Server_Port`: Active Directory サービスのサーバーポートです (例 : 389)。
- `PSSync_Admin_Dn`: Active Directory の管理者ユーザーの名前です (例 : CN=Administrators,CN=Users,DC=SelectIdentity,DC=hp,DC=com)。
- `PSSync_Admin_Password`: Active Directory の管理者ユーザーの暗号化されたパスワードです。
- `PSSync_ATTRIBUTE`: Active Directory でユーザーが暗号化されたパスワードを格納するための、ユーザー属性の名前です。指定したフィールドは、180 文字以上を保持できる必要があります。そうでない場合、AD は暗号化されたパスワードを保持することができません。たとえば、Active Directory の `description` 属性などを指定します。

これは、ユーザーの暗号化されたパスワードを含んだ機密性の高い属性です。他のアプリケーションで使用されない、簡単に表示したり利用できない属性を選択することを、強くお薦めします。この属性を隠蔽するには、Active Directory スキーマを拡張して属性を追加するのがよい方法です。

7 **[Next]** をクリックします。[Generate Encrypted Key] 画面が表示されます。

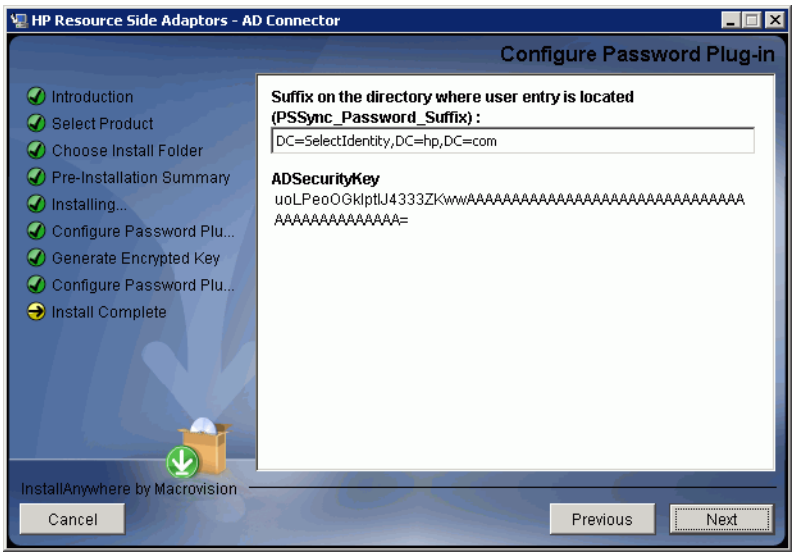


8 [Yes] ラジオボタンをチェックし、**[Next]** をクリックします。[AES Encryption Keys] ポップアップが表示されます。



- [Key] フィールドの値を書きとめ、キーを保存してください。Select Identity のリソースアクセス情報パラメータの入力時に、[Encryption Key] フィールドにこの値を入力する必要があります。
- このキーは、変更しないことをお薦めします。変更する必要がある場合は、必ずすべてのユーザーパスワードを再設定してください。

9 [Configure Password Plug-in] 画面が表示されます。



10 ユーザーエントリが配置されているディレクトリの接尾辞を、`[PSSYnc_Password_Suffix]` に入力します。(例 : DC=SelectIdentity,DC=hp,DC=com)。**[Next]** をクリックします。

11 インストールの完了後、**[Done]** をクリックします。

12 エージェントは、パスワードプラグインの操作に関する情報をログファイルに記録します。`ADProperties.ini` ファイルの `PSLog_Level` 属性を設定することにより、この情報をフィルタできます。以下の手順に従って、この属性を設定します。

a `C:\WINDOWS\system32` に存在する `ADProperties.ini` ファイルを開きます。

b `PSLog_Level` 属性に 0、1、2、または 3 を設定します。

- `PSLog_Level` に `0` を設定すると、基本情報のみを記録します。
- `PSLog_Level` に `1` を設定すると、中間レベルの情報を記録します。
- `PSLog_Level` に `2` を設定すると、詳細レベルの情報を記録します。
- `PSLog_Level` に `3` を設定すると、開発者レベルの情報を記録します。

13 インストール後に、コンピュータを再起動してください。また、忘れずに `ADProperties.ini` ファイルをバックアップしてください。

`Description` は、パスワードプラグインが暗号化パスワードを格納するために使用する、デフォルトの Active Directory 属性です。

暗号化パスワードの格納に別の属性を使用したい場合は、以下の手順を実行します。

- パスワードプラグイン側の作業

  パスワードプラグインのプロパティファイル (`ADProperties.ini`) を変更し、“`PSSync_ATTRIBUTE=`*`description`*”の“`description`”を別の属性名に置き換えます。

- Select Identity 側の作業

  アプリケーションサーバーを停止し、`ActiveDirSchema.jar` の `ActiveDirConfig.properties` を変更して、`PSSync_ATTRIBUTE=description` の *`description`* を別の属性に置き換えます。次に、アプリケーションサーバーを再起動します。

Exchange 2007 プラグインのインストール

Exchange 2007 Server 上の操作

以下の手順に従って、Exchange 2007 プラグインをインストールします。

1 Exchange 2007 Server 設定ファイルを変更します。

HP.AD.ExchangeWindowsService.vshost.exe.config ファイルで ExchangeWCFService サービスの正しいポート番号を設定します。**8000** など、1024 以上のポート番号を必ず指定してください。ExchangeWCFService サービスを起動すると、ポート 8000 をリッスンします。

```
<services>
   <service name="HP.AD.ExchangeWindowsService.ExchangeWCFService"
behaviorConfiguration="ExchangeServiceBehavior">
      <host>
          <baseAddresses>
             <add baseAddress="http://localhost:8000/ExchangeWCFService"/>
          </baseAddresses>
      </host>
   <!-- this endpoint is exposed at the base address provided by host:
http://localhost:8000/ServiceModelSamples/service  -->
    <endpoint address=""
         binding="basicHttpBinding"
         contract="HP.AD.ExchangeWindowsService.IExchangeWCFService" />
   </service>
</services>
```

2 Windows サービスをインストールします。

a コネクタリリースフォルダの下の Installer/Exchange2007/Exchange Agent.zip パッケージを解凍して、Exchange 2007 Server 上のパスにコピーします。

b コンピュータ上に .Net Framework 3.0 が事前にインストールされていることを確認します。

c コマンドプロンプトから以下のコマンドを実行して、Windows サービスをインストールします。

InstallUtil HP.AD.ExchangeWindowsService.exe

InstallUtil.exe は C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727 など、.NET framework セットアップパスに格納されています。

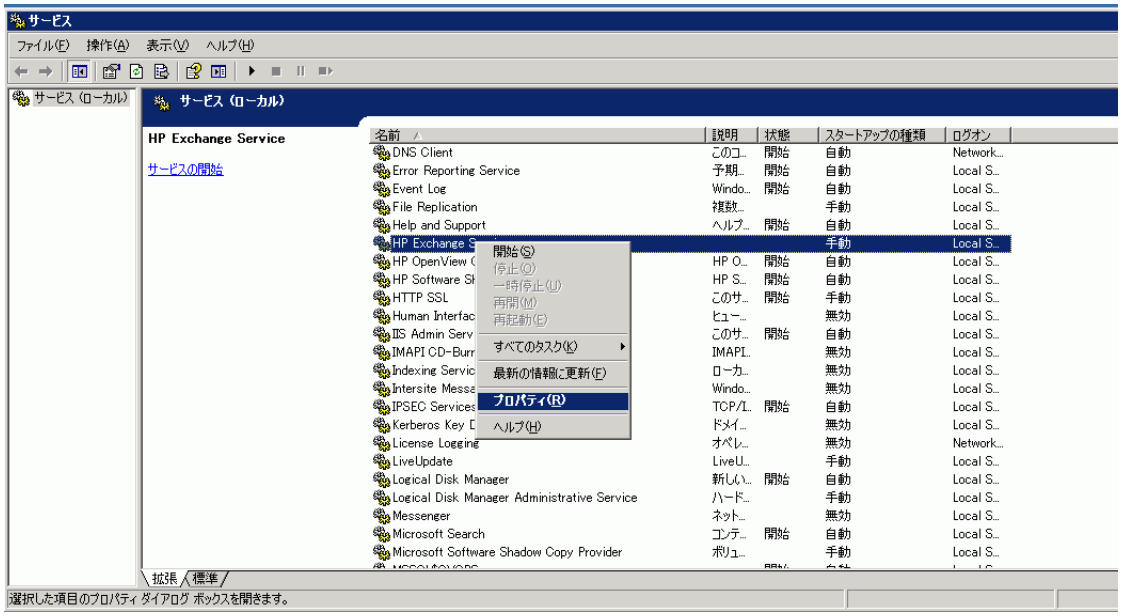
コマンドをパスに追加して、InstallUtil.exe を解析できるようにします。また、HP.AD.ExchangeWindowsService.exe も解析可能であることを確認します。

Windows サービスをアンインストールするには、次のコマンドを使用します。

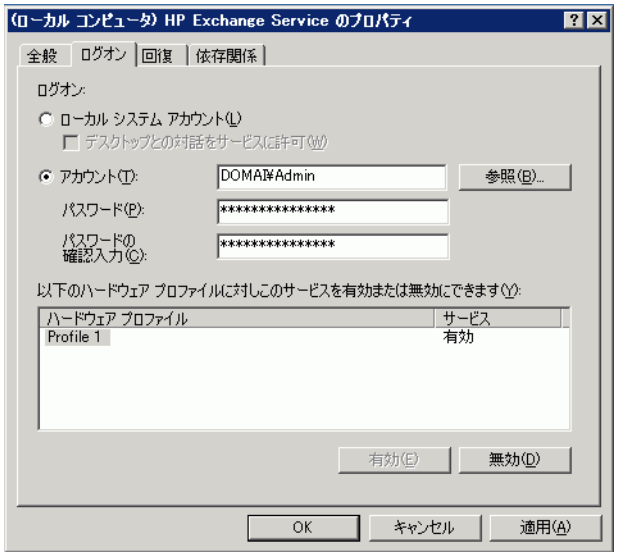
InstallUtil /u HP.AD.ExchangeWindowsService.exe

d インストール後、Exchange 2007 Server で Windows サービスを起動します。Exchange Organization Administrators グループに所属するユーザーアカウントを使用してください。また、ユーザーアカウントは Exchange 2007 Server と同じドメインに属する必要があります。

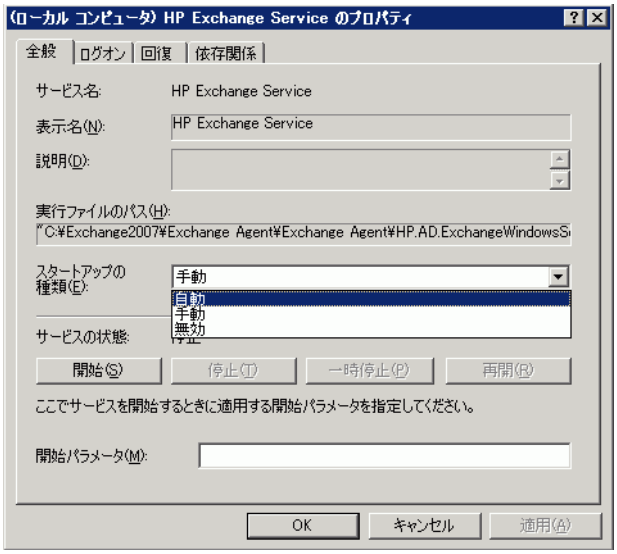
[スタート] → **[コントロールパネル]** → **[管理ツール]** → **[サービス]** を開き、[サービス] ウィンドウで [HP Exchange Service] を右クリックして、コンテキストメニューから **[プロパティ]** を選択します。



[HP Exchange Service のプロパティ] ウィンドウで [ログオン] タブをクリックして、適切な権限を持ったアカウントを指定します。**[OK]** をクリックします。



次に、適切な権限を持ったユーザーアカウントを使用して、[サービス] コンソールから HP Exchange Service を手動で開始、または自動的に起動するように設定します。



Active Directory サーバー上の操作

1 パスワードプラグインをインストール後、Exchange 2007 Server でのメールボックス作成をサポートするため、コネクタリリースフォルダの下の `Installer/Exchange2007/AD Agent.zip` パッケージから以下の 2 つのファイルを解凍して、AD サーバー上の `%SystemRoot%\system32` にコピーする必要があります。

```
HP.AD.WNF.CreateMailBoxClientAction.dll
HP.AD.WNF.CreateMailBoxClientAction.dll.config
```

2 `PasswordAgent-config.xml` ファイルに以下の太字の行を追加します。このファイルは、Active Directory サーバーの `%SystemRoot%\system32` に格納されています。

```
<action-mappings>
    <action message="moveUserAcrossDomains" assembly="HP.AD.WNF.MoveUser"
className="HP.AD.WNF.MoveUser.MoveUserAction" />
    <action message="CreateMailBox"
assembly="HP.AD.WNF.CreateMailBoxClientAction"
className="HP.AD.WNF.Action.CreateMailBoxClientAction" />
</action-mappings>
```

3 `HP.AD.WNF.CreateMailBoxClientAction.dll.config` ファイルを変更します。タグ `<value>` の値をサーバーの IP アドレスおよび ExchangeWCFService サービスが実行中のポート番号に設定します。

```
<configuration>
 <configSections>
  <sectionGroup name="applicationSettings"
type="System.Configuration.ApplicationSettingsGroup, System,
Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >
    <section
name="HP.AD.WNF.CreateMailBoxClientAction.Properties.Settings"
type="System.Configuration.ClientSettingsSection, System, Version=2.0.0.0,
Culture=neutral, PublicKeyToken=b77a5c561934e089"
requirePermission="false" />
```

```
  </sectionGroup>
 </configSections>
<applicationSettings>
<HP.AD.WNF.CreateMailBoxClientAction.Properties.Settings>
   <setting
name="HP_AD_WNF_CreateMailBoxClientAction_WCFService_ExchangeWCFService"
serializeAs="String">
    <value> http://[ExchangeWCFService サーバーの IP アドレス]:8000/
ExchangeWCFService </value>
   </setting>
  </HP.AD.WNF.CreateMailBoxClientAction.Properties.Settings>
 </applicationSettings>
</configuration>
```

複数ドメイン環境の場合、上の 3 つの手順を各 Active Directory サーバーで実施します。

パスワードプラグインの配布

HP Central AD Agent のセットアップユーティリティを実行すれば、フォレスト内のすべてのドメインコントローラにパスワードプラグインを配布することができます。

準備作業

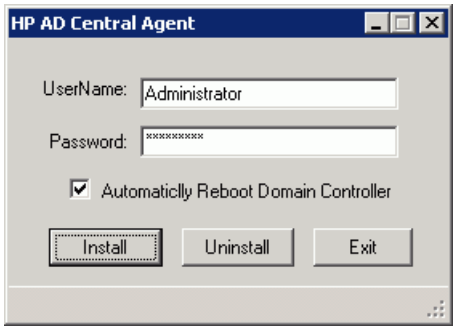
1. Microsoft .Net Framework 2.0 をダウンロードしてインストールし、次にシステム変数 Path に RegAsm.exe が存在するパスを追加します (例 : C:\WINDOWS\microsoft.net\Framework64\v2.0.50727)。
2. 以下の 4 ファイルが %SystemRoot%\system32 ディレクトリに存在することを確認し、パスワードプラグインがインストーラウィザードにより正常にインストールされたことをチェックします。

   ADProperties.ini
   ADPassfilt.dll
   libeay32.dll
   libssl32.dll (32 ビット用)/ssleay32.dll (64 ビット用)
3. HP_Central_AD_Agent.zip ファイルを、同じ AD ドメインコントローラサーバーのローカルディレクトリ (< インストーラディレクトリ >) に解凍します。すると、HP Central AD Agent Setup.exe が、< インストーラディレクトリ >\HP_Central_AD_Agent ディレクトリに格納されます。
4. ドメインコントローラのログオンで使用する資格証明が、以下のタスクを実行するための権限を、フォレスト内のすべてのドメインコントローラに対して持っていることを確認してください。
   - リモートコンピュータの %systemroot%\system32 ディレクトリに対するアクセスおよび書き込み権限
   - リモートコンピュータのレジストリに対する書き込みおよび更新権限

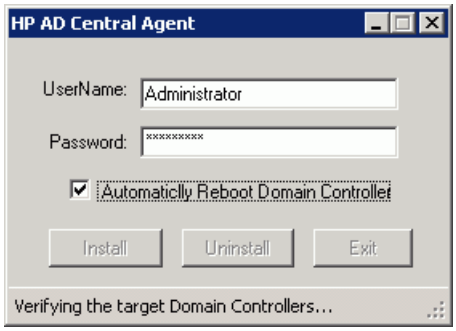
インストール手順

以下の手順に従って、HP Central AD Agent を実行します。

1 HP Central AD Agent のインストールフォルダに存在する `HP Central AD Agent Setup.exe` を実行し、組み込みの管理者権限を持つ管理者ユーザーアカウントとパスワードを入力します。



2 **[Install]** ボタンをクリックし、インストールを開始します。



ステータスバーに、インストールの進捗状況が表示されます。

3 インストールが完了したら、**[OK]** をクリックして終了します。

4 インストールを開始する前に [Automatically Reboot Domain Controller] を選択しなかった場合は、必要なすべての操作を終了後、手動ですべてのドメインコントローラを再起動し、パスワードプラグインを有効にする必要があります。

インストールが完了すると、HP Central AD Agent が稼動するドメインコントローラには以下のアイテムが追加されます。

- < インストーラディレクトリ >`\HP_Central_AD_Agent\Log` フォルダに 3 つのファイルが追加されます。
  - `Reached.txt` - パスワードプラグインが正常にインストールされた、すべての対応済ドメインコントローラのコンピュータ名のリスト

- Unreached.txt - 手動でパスワードプラグインのインストールが必要となる、すべての未対応ドメインコントローラのコンピュータ名のリスト
- LogInfo.txt - ログメッセージのリスト

- インストールフォルダに、以下のファイルを含んだデータフォルダが追加されます。
  - ADProperties.ini、ADPassfilt.dll、libeay32.dll、および libssl32.dll - これらのファイルは、%SystemRoot%\System32 ディレクトリからコピーされます。
  - DC_List.txt - 対応済みのすべてのドメインコントローラ名のリスト
  - DCFull_List.txt - 対応済みのすべてのドメインコントローラの省略しない名前のリスト

パスワードプラグインが正常にインストールされた、ターゲット AD ドメインコントローラサーバーには、以下のアイテムが作成されます。

- ADProperties.ini の <PSLog_Path> で指定したとおりに、ログフォルダが作成されます。
- ADProperties.ini、ADPassfilt.dll、libeay32.dll、および libssl32.dll が、%SystemRoot%\System32 ディレクトリにコピーされます。また、ADProperties.ini に以下の LDAP 情報が追加されます。

```
PSSync_Base_Suffix=DC=root, DC=sicf          '(Target DC's Domain Name)
PSSync_Server_Name=rootdc1.root.sicf         '(Target DC's Full DC Name)
```

- レジストリの HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa 配下にある "Notification Packages" に、文字列 "ADPassfilt" が追加されます。

Central AD Agent について

- エンタープライズ管理者アカウントを使用した場合は、パスワードプラグインを各ドメインコントローラにインストールできます。
- ドメイン管理者アカウントを使用した場合は、パスワードプラグインを同じドメインのドメインコントローラにのみインストールできます。
- 組み込みの管理者アカウントを使用した場合は、パスワードプラグインをローカルマシンにのみインストールできます。
- その他のアカウントを使用した場合は、いずれのドメインコントローラにもパスワードプラグインをインストールすることはできません。

5 Select Identity でのコネクタの設定

この章では、Select Identity で Active Directory 双方向 LDAP コネクタを設定する手順と、Select Identity でコネクタを設定する際に指定するコネクタ特有のパラメータについて説明します。

設定手順

アプリケーションサーバーにコネクタの RAR ファイルを配布したら、Select Identity 側でコネクタを設定してください。Select Identity で Active Directory 双方向 LDAP コネクタを設定するには、以下の手順を実行します。

1 新しいコネクタの追加

2 新しいリソースの追加

3 属性のマッピング

4 Select Identity におけるワークフロー外部コールの設定

5 Exchange に関連する属性の設定

新しいコネクタの追加

ユーザーインタフェースを使用して Select Identity に新しいコネクタを追加します。コネクタを追加するときは、以下のように操作します。

- [コネクタ名] テキストボックスにコネクタの名前を入力します。
- [プール名] テキストボックスに「**`eis/ActiveDirConnector`**」と入力します。
- [利用できるマッパー] セクションで **[いいえ]** を選択します。

Select Identity に新しいコネクタを追加する方法については、『HP Select Identity Connector Deployment Guide』を参照してください。

新しいリソースの追加

新たに追加したコネクタを使用する新しいリソースを Select Identity に追加します。Select Identity にリソースを追加する方法については、『HP Select Identity Connector Deployment Guide』を参照してください。

次の表を参照し、[基本情報] ページと [アクセス情報] ページにパラメータを入力します。

表 6　　リソース設定パラメータ

フィールド名	値の例	説明	コメント
Resource Name	ELDAPADsample	リソースに付ける名前。	
Connector Name	ELDAPADsample	新たに配布したコネクタ。	
Login Name	CN=Administrator, CN=Users,DC=sis, DC=com	管理者ユーザーのログイン名。	調整の実行時に管理者ユーザーが削除されたユーザーを見つけることができない場合は、次の URL のトラブルシューティング情報を確認する必要があります。 **http://support.microsoft.com/kb/892806/en-us**
Password		管理ユーザーのパスワード。	双方向認証が有効な場合、Login Name と Password は使用されません。 ドメイン間でユーザーを移動する場合、必ずパスワードを AD パスワードの複雑性要件に準拠させてください。
Mapping File	ActiveDir.xml	属性のマッピングを指定するファイルの名前です。このファイルは、アプリケーションサーバーの classpath に存在する必要があります。**[表示]** をクリックし、ブラウザでファイルを開きます。このファイルが表示できない場合は、Select Identity はこのファイルを検出できません。	
configFile	ActiveDirConfig	設定情報とフォレスト全体の情報が含まれています。具体的な情報は、顧客の環境により変わります。	
objectClass	User	プロビジョニングを行うエンティティのタイプです。 各リソースは、2 つのエンティティタイプ (コンタクトまたはユーザー) のうち 1 つのみをサポートします。	ユーザーまたはコンタクトのいずれかを値に設定できます。

表 6　　リソース設定パラメータ (続き)

フィールド名	値の例	説明	コメント
Select Identity Locale	en_US	ロケール特有の情報です。Country=US および Language=English の場合、現在のロケール文字列は en_US です。	
encryptionKey	6PqwwkfRTxaEJgW/cFuIUA==	パスワードプラグインのインストーラプログラムが生成したキーのコピーです。	
CRL Flag	false	リソースが CRL チェックを実行するかどうかを示します。このフラグは、**[ツール] → [システムセキュリティ] → [セキュリティセットアップ] → [証明書ポリシー]** ページの CRL チェックフラグと連携して機能します。これら 2 つのフラグが両方とも true の場合、コネクタは CRL チェックを実行します。	
Usage Flag	false	コネクタが使用状況チェックを実行するかどうかを示します。このフラグは、**[ツール] → [システムセキュリティ] → [セキュリティセットアップ] → [証明書ポリシー]** ページの使用状況チェックフラグと連携して機能します。これら 2 つのフラグが両方とも true の場合、コネクタは使用状況チェックを実行します。	
Delete Group Detection	false	コネクタが、削除されたグループの調整と検出をサポートするかどうかを示します。	現在のコネクタバージョンでは使用できません。

リバース同期用ポーリングの設定

リソースアクセス情報の入力後、[ユーザーの調整ポリシー] ページが表示されます。このページで以下の操作を行います。

a　[ポーリング有効] チェックボックスをチェックします。ポーリング間隔に希望する値を設定します。

b　[変更] セクションの下のドロップダウンボックスを使用して、[調整のワークフロー] に [SI Recon User Enable Disable Workflow] を設定します。

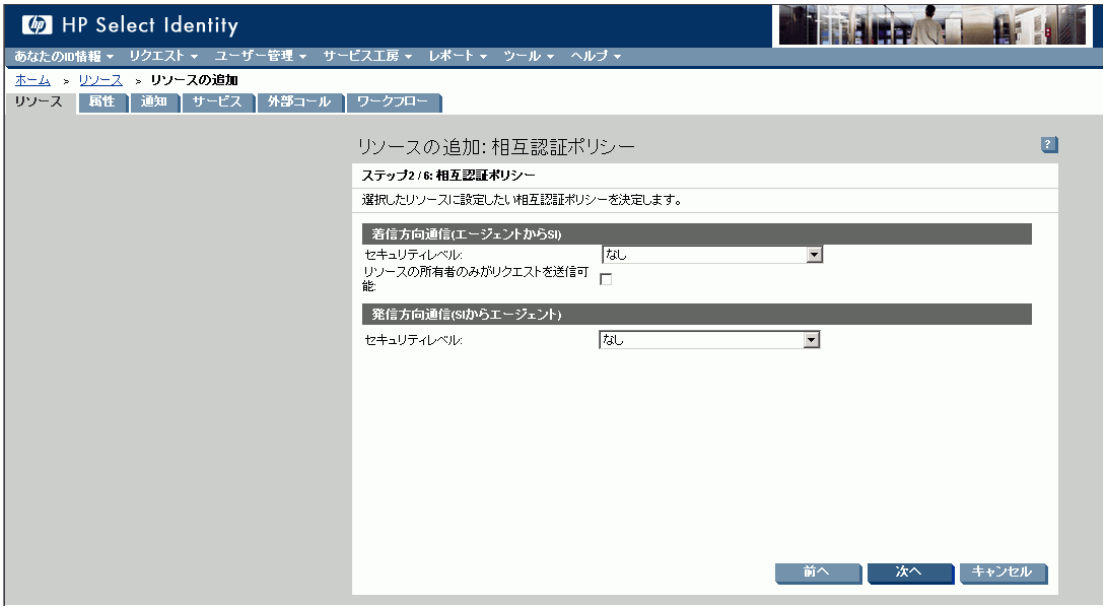
c　このページの他のデフォルト設定は、すべてそのまま保持します。

相互認証サポートの設定

Active Directory の相互認証をサポートするには、共通的な設定 (26 ページで示すように、キーストアとトラストストアプロパティに Select Identity のセキュリティレベルを設定) に加えて、いくつか特別な設定が必要となります。

以下の手順を実行します。

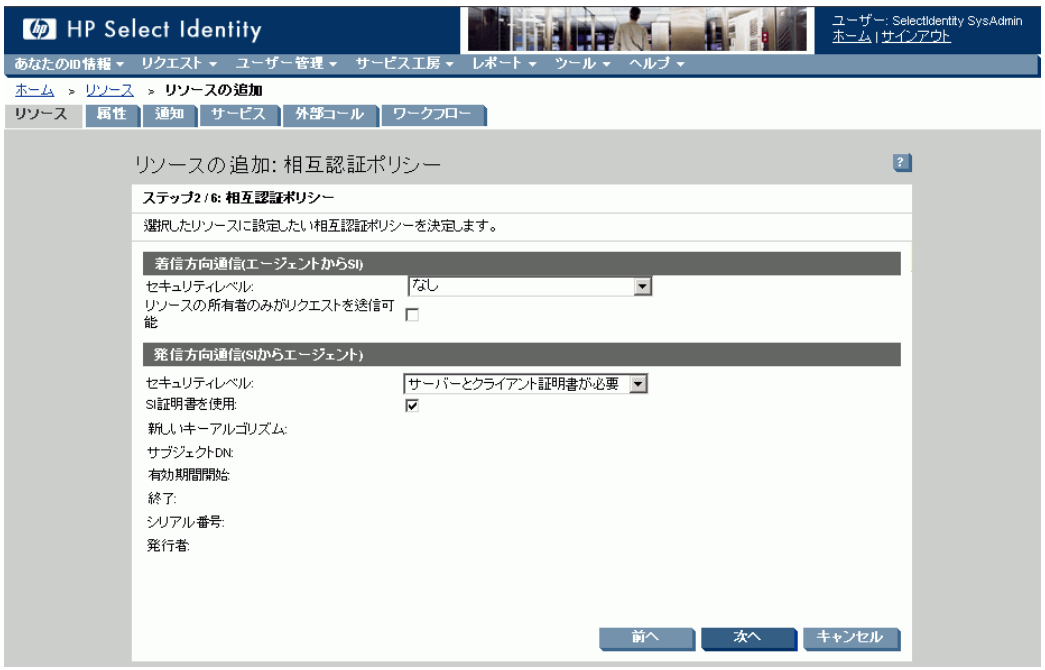
1 リソースを追加する場合、**[リソースの追加 : 相互認証ポリシー]** ページで着信と発信のセキュリティ設定を指定し、相互認証ポリシーを設定します。



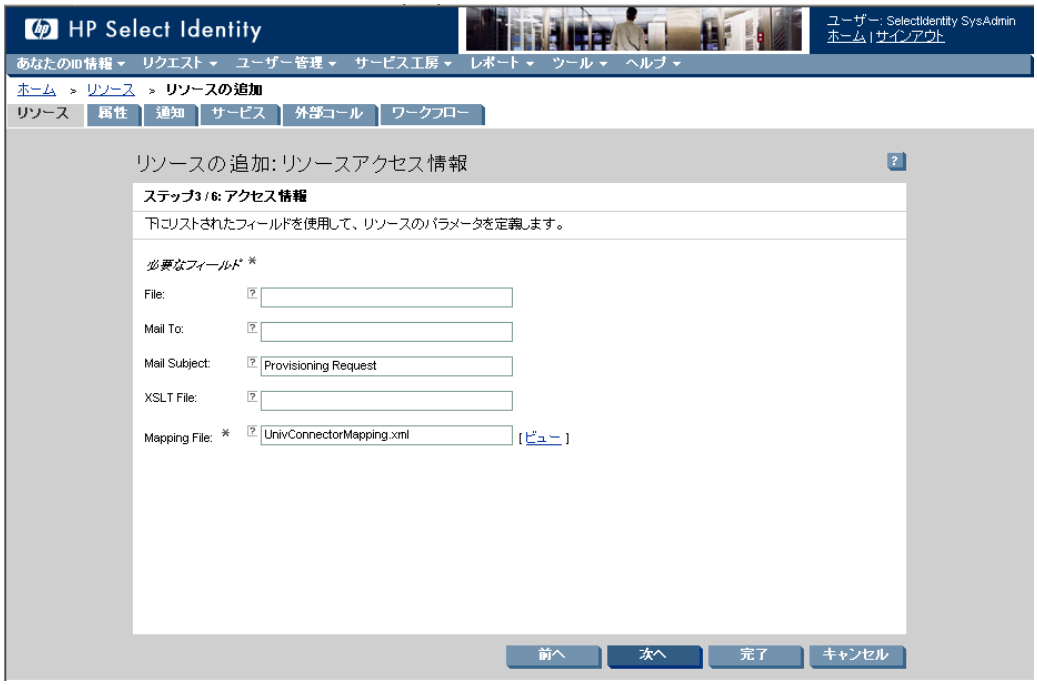
2 Select Identity とリソースの間で単一方向認証を使用したい場合は、**[発信方向通信 (SI からエージェント)]** セクションの **[セキュリティレベル]** ドロップダウンリストから **[サーバー証明書が必要]** を選択します。

Select Identity とリソースの間で双方向認証を使用したい場合は、[発信方向通信 (SI からエージェント)] セクションの **[セキュリティレベル]** ドロップダウンリストから **[サーバーおよびクライアント証明書が必要]** を選択し、**[SI 証明書を使用]** にチェックを付けます。すると、Select Identity の証明書情報が表示されます。

[セキュリティレベル] に**なし**という値は適用できません。



3 **[次へ]** をクリックします。



前のページで双方向認証が選択された場合、Login Name 属性と Password 属性は相互認証には使用されません。

3 つの新しいフィールド (CRL Flag、Usage Flag、Delete Group Detection) が追加されることに注意してください。

— CRL Flag が true に設定され、**[ツール]** → **[システムセキュリティ]** → **[セキュリティセットアップ]** → **[証明書ポリシー]** ページの [証明書使用状況の妥当性検査] にチェックを付けた場合は、CRL の妥当性検査が有効になります。

— Usage Flag が true に設定され、**[ツール]** → **[システムセキュリティ]** → **[セキュリティセットアップ]** → **[証明書ポリシー]** ページの [CRL の妥当性検査] にチェックを付けた場合は、証明書使用状況の妥当性検査が有効になります。

属性のマッピング

Active Directory 双方向 LDAP コネクタのリソースを正しく追加したら、リソースの属性を Select Identity の属性にマッピングしてください。属性のマッピングと作成については、『HP Select Identity Connector Deployment Guide』を参照してください。属性をマッピングするときは、以下の表を参照してリソース固有のマッピング情報を確認してください。

コンタクトをサポートするには、ユーザーの memberAttributes 定義で新しい属性 entityType を使用します。この属性は、ユーザーとコンタクトを区別するために使用されます。この属性にユーザーのみを指定する場合は、`"entityType=user"` と設定します。この属性にコンタクトのみを指定する場合は、`"entityType=contact"` と設定します。また、この属性にユーザーとコンタクトを指定する場合は、`"entityType=user|contact"` と設定します。

表 7　　Active Directory 双方向 LDAP マッピング情報

Select Identity リソース属性	**コネクタ属性**	**Active Directory の属性**	**説明**
Street	streetAddress	streetAddress	*entityType= user|contact*
PhHome	homePhone	homePhone	*entityType= user|contact*
Email	Mail	mail	*entityType= user|contact*
PhMobile	mobile	mobile	*entityType= user|contact*
UserName	sAMAccountName	sAMAccountName	*entityType= user* これは、ユーザーの作成に必須の属性です。
CN	cn	Cn	*entityType= user|contact* これは、ユーザーの作成に必須の属性です。
Zip	postalCode	postalCode	*entityType= user|contact*
PhBus	telephoneNumber	telephoneNumber	*entityType= user|contact*
Password	unicodePwd	unicodePwd	*entityType= user* これは、ユーザーの作成に必須の属性です。
Title	title	title	*entityType= user|contact*
DisplayName	displayName	displayName	*entityType= user|contact*
LastName	sn	Sn	*entityType= user|contact* これは、ユーザーの作成に必須の属性です。

表 7　　Active Directory 双方向 LDAP マッピング情報 (続き)

Select Identity リソース属性	コネクタ属性	Active Directory の属性	説明
ObjectGUID	objectGUID	objectGUID	*entityType*= *user*|*contact* これは、ユーザーの作成に必須の属性です。 Active Directory 双方向 LDAP リソースがサービスと関連付けられている間は、この属性をサービスに追加しないでください。
Groups	memberOf	memberOf	*entityType*= *user*|*contact*
FirstName	givenName	givenName	*entityType*= *user*|*contact*
UserPrincipalName	userPrincipalName	userPrincipalName	*entityType*= *user*
State	st	St	*entityType*= *user*|*contact*
Usersuffix	userSuffix	userSuffix	*entityType*= *user*|*contact* これはユーザーの作成に必須の属性であり、有効な値を指定する必要があります。 **UserSuffix を Select Identity サービスの固定属性として設定する必要がある場合は、必ず値をすべて小文字にしてください。**
Domain	domain	domain	*entityType*= *user*|*contact* これは、ユーザーの作成に必須の属性です。 マルチドメイン環境では、フォレスト内に複数のドメインを保有することができます。したがって、どのドメインに現在の操作が割り当てられているのかを指定する必要があります。1 つのドメインが指定された場合、操作はそのドメインのみに割り当てられます。コネクタを期待どおり十分に機能させるには、この属性を設定する必要があります。 **Domain を Select Identity サービスの固定属性として設定する必要がある場合は、必ず値をすべて小文字にしてください。** コネクタを v1.x から v2.x に移行する場合は、属性名はすべて小文字にする必要があります (domain など)。

表 7　　Active Directory 双方向 LDAP マッピング情報 (続き)

Select Identity リソース属性	コネクタ属性	Active Directory の属性	説明
City	l	L	*entityType*= *user*|*contact*
POBox	postOfficeBox	postOfficeBox	*entityType*= *user*|*contact*
userAccount Control	userAccount Control	userAccount Control	*entityType*= *user* Active Directory 双方向 LDAP リソースがサービスと関連付けられている間は、この属性をサービスに追加しないでください。

userSuffix は、ドメインコントローラにユーザーが格納された場所を指定します。userSuffix が空の場合、コネクタはプロパティファイルに定義されたデフォルトの userSuffix を使用します。たとえば、userSuffix を ***ou=test,ou=selectidentity,ou=openview*** と入力した場合、ユーザーはドメインコントローラの OU に作成されます。

スキーマファイル (`ActiveDir.xml`) を変更する場合、必ずリソースキーに `objectGUID` を設定してください。

ユーザーを Exchange メールボックスにプロビジョニングしたい場合は、以下の属性をマッピングします。

表 7A　　Exchange マッピング情報

Select Identity リソース属性	コネクタ属性	Active Directory 双方向 LDAP の属性	説明
Email	Mail	mail	*entityType*= *user*
MailBoxStore	homeMDB	homeMDB	*entityType*= *user* メールボックスサポートを提供する場合、この属性を Select Identity で指定する必要があります。
mailNickName	mailNickname	mailNickname	*entityType*= *user* メールボックスサポートを提供する場合、この属性を Select Identity で指定する必要があります。
AlternateRecipient	altRecipient	altRecipient	*entityType*= *user*
HomeDirectory	homeDirectory	homeDirectory	*entityType*= *user*
AddressBook	showInAddressBook	showInAddressBook	*entityType*= *user*

表 7A　　Exchange マッピング情報

Select Identity リソース属性	コネクタ属性	Active Directory 双方向 LDAP の属性	説明
proxyAddresses	proxyAddresses	proxyAddresses	*entityType= user* 値は、以下の形式で指定する必要があります。 [メールのタイプ][アドレス値] たとえば、 「SMTP:test@domain.com」 や 「smtp:test2@domain.com」 など
userPrincipalName	userPrincipalName	userPrincipalName	*entityType= user* 値は、「user@test.com」などの電子メールアドレス形式で指定する必要があります。
msExchHideFromAddressLists	msExchHideFromAddressLists	msExchHideFromAddressLists	*entityType= user* Select Identity で TRUE または FALSE に設定する必要があります。大文字を必ず指定します。

Select Identity におけるワークフロー外部コールの設定

リバース同期を実行するには、Active Directory 双方向 LDAP コネクタに対するユーザーの有効化 / 無効化操作を行うためのワークフロー外部コールを設定する必要があります。ユーザーがリソース (Active Directory) に対して有効化または無効化された場合は、特定の Active Directory 属性値 (`PSSync_ATTRIBUTE`) が変化します。コネクタはこの属性値の変更を検出し、このイベントをユーザー変更として登録します。

ユーザーを有効化 / 無効化するワークフロー外部コールについては、『HP Select Identity Connector Deployment Guide』を参照してください。設定においては、以下の表 8 で示すパラメータを入力してください。

表 8　　Active Directory 双方向 LDAP コネクタに対するユーザーの有効化 / 無効化パラメータ

シリアル番号	パラメータ名	パラメータ値
1.0	AttributeName	userAccountControl
2.0	EnableValue	512
3.0	DisableValue	514

表 8　Active Directory 双方向 LDAP コネクタに対するユーザーの有効化 / 無効化パラメータ (続き)

シリアル番号	パラメータ名	パラメータ値
4.0	UserName	Select Identity の管理者ユーザー名 (例 : sisa)
5.0	Password	Select Identity の管理者パスワード (例 : abc123)
6.0	Url	Select Identity Web サービスの URL (例 : http://localhost:7001/lmz/webservice)

これらのパラメータの入力においては、Password の場合のみ [機密] チェックボックスにチェックを付けてください。

Exchange に関連する属性の設定

このコネクタを使用すれば、ユーザーを Exchange メールボックスにプロビジョニングすることができます。これを可能にするには、Exchange に関連する属性をマッピングする必要があります。これらの属性は、ユーザーのプロビジョニング時に入力する必要があり、以下に属性値の例を示して説明しています。

- `Mail` ― ユーザーの電子メールアドレスです (例 : *user01@sitest.com*)。
- `homeMDB` ― これは ExchangeFolderDN であり、いくつかのサーバーの値を連結したものです。以下に例を示します。

  CN=Mailbox Store (TLNT3),CN=First Storage Group,CN=InformationStore,CN=TLNT3,CN=Servers,CN=First Administrative Group,CN=Administrative Groups,CN=SITestOrg,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=sitest,DC=com

  これはテスト DN です。同等の値を指定する必要があります。
- `mailNickname` ― このニックネームは `User name` または `sAMAccountName` として使用できます (例 : *User01nick)*。

  ユーザーの追加時にこの値を入力すると、ユーザーの電子メール ID は *User01nick@sitest.com* になります。
- `altRecipient` ― これは、他のユーザーエントリの DN であり、User01 から User02 へメールを転送するために使用されます (例 : *CN=User02,CN=Users,DC=sitest,DC=com*)。

  この属性を設定すると、User01 へ送信されたどのメールも User02 へ転送されます。
- `homeDirectory` ― これは、仮想的なホームフォルダです。この場所に、Exchange ユーザーのホームディレクトリが格納されます (例 : *D:\temp*)。

  このフォルダはユーザー属性としてのみ表示され、物理的にサーバー上に作成されることはありません。
- `showInAddressBook` ― これは、いくつかのサーバーの値を連結したものです。以下に例を示します。

CN=All Users,CN=All Address Lists,CN=Address Lists Container,CN=SITestOrg,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=sitest,DC=com | CN=Default Global Address List,CN=All Global Address Lists,CN=Address Lists Container,CN=SITestOrg,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=sitest,DC=com

これはテスト用の値であり、同等の値を指定する必要があります。

- `proxyAddresses` ー
  a. Exchange 2007 Server で値を自動的に生成するようにこの属性を設定した場合、Select Identity で空欄のままにします。Select Identity で値を指定すると、自動的に生成された値が置換されます。
  b. この属性の値を Select Identity で空欄にして、Exchange 2007 Server で自動的に値を生成するように後から属性を構成した場合、ユーザーアカウントが正しく作成されたときに Exchange 2007 Server で生成される値は Select Identity で表示できません。ただし、Select Identity は調整を行うことでフィールドの値を取得できます。調整が行われた後にフィールドの値が Select Identity に表示されます。
- `userPrincipalName` ー この属性は、「user@test.com」などの電子メールアドレス形式で指定する必要があります。
- `msExchHideFromAddressLists` ー この属性を Select Identity でマッピングした場合、Select Identity で値を TRUE または FALSE に設定する必要があります。値は大文字を必ず指定します。

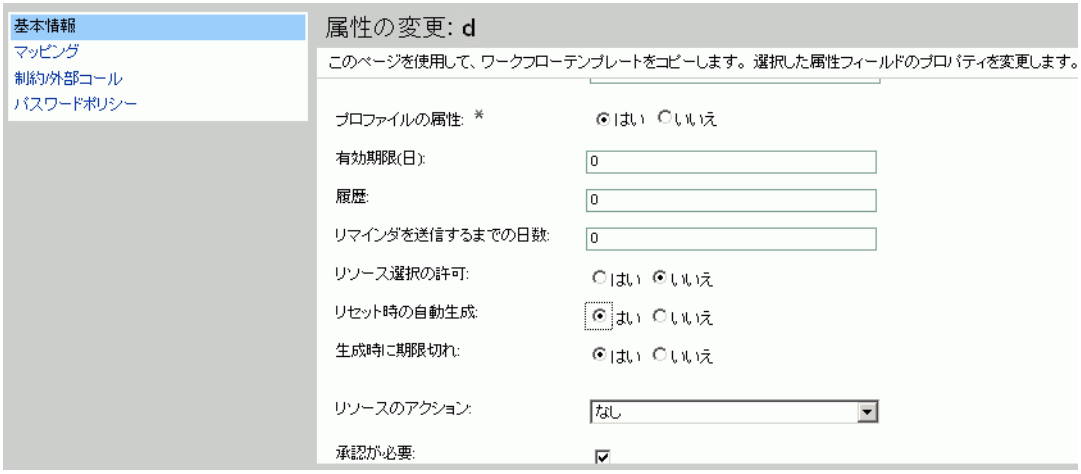
パスワードの失効操作の設定

Select Identity を設定し、新たに作成したユーザーのパスワードを自動的に失効させることができます (このパスワードは、ユーザーの作成時に Select Identity が自動的に作成します)。

以下の手順に従って、Select Identity 4.0 ～ 4.20 でパスワードの失効操作を設定します。

1. Select Identity のホームページで、**[サービス工房] → [属性]** の順にクリックします。属性リストが表示されます。

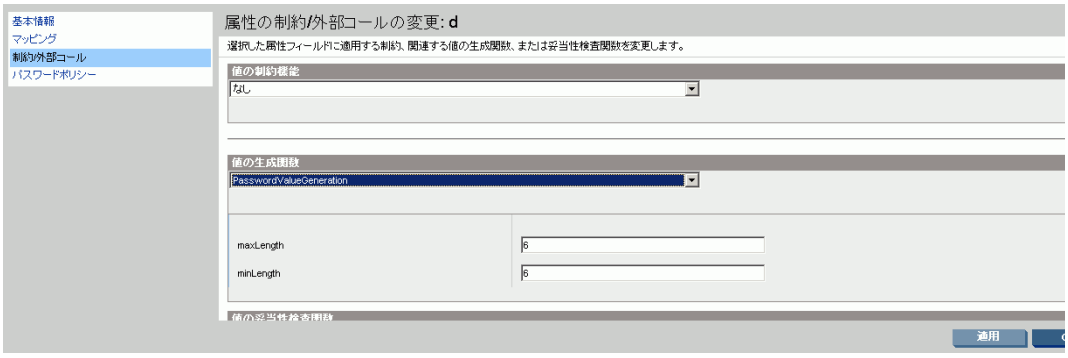
2 Password 属性を選択し、**[変更]** をクリックします。[属性の変更 : < パスワード >] ページが表示されます。



3 [生成時に期限切れ] フィールドで [はい] を選択します。

4 [リセット時の自動生成] フィールドで [はい] を選択します。

5 左側のペインで **[制約 / 外部コール]** リンクをクリックします。[属性の制約 / 外部コールの変更 : < パスワード >] ページが表示されます。



6 [値の生成関数] ドロップダウンボックスから、[PasswordValueGeneration] を選択します。

7 **[適用]** をクリックします。

Password 属性は、サービスフォームには含まれません。

8 テキストエディタを使用してスキーマファイル (ActiveDir.xml) を開き、User セクションに以下の XML 文字列が存在するかどうか確認します。

```
<attributeDefinitionReferenceattrFunction="provision|post|pre"attributeTy
pe="Read/write"
concero:isKey="false"concero:resfield="pwdLastSet"concero:tafield="{0}"
defaultValue="0"encrypt="false" encrypted="false"
encryptionAlgorithm=""expirePassword="true" expireValue="0"
isPassword="false"linktoentity=""
multivalued="false"mustOnResource="false"name="objectclassuserattributepw
dLastSet"objectclass="user" objectclasstype="structural"ordering=""
```

```
remexpireValue="-1" renamekey="false"required="false"
resourcekey="false"supportedOperations="UNLINK,LINK,GETATTRIBUTES,GETPARE
NT,GETCHILDREN,GETALL,RESETPASSWORD,CHANGEPASSWORD,EXPIREPASSWORD,DISABLE
,ENABLE,CREATE,DELETE,UPDATE"transform="NO" type="java.lang.String"/>
```

6 コネクタのアンインストール

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。

- すべてのリソースの依存関係を Select Identity から削除します。
- Select Identity からコネクタを削除します。
- アプリケーションサーバーからコネクタを削除します。
- ドメインコントローラでパスワードプラグインウィザードを実行し、パスワードプラグインをアンインストールします。
- マルチドメイン環境に HP Central AD Agent がインストールされている場合、インストールされているサーバーで HP Central AD Agent を実行すれば、他のすべてのドメインコントローラから自動的にパスワードプラグインを削除することができます。

アプリケーションサーバーと Select Identity からのコネクタの削除については、『HP Select Identity Connector Deployment Guide』を参照してください。

A トラブルシューティング

この付録では、コネクタのインストール時または実行時によく見られる問題について説明します。

- ユーザーの作成時にパスワードが設定されていない場合、コード 5003 で例外がスローされました。

  解決方法 :

  ユーザーに送信されたパスワードが、パスワードポリシーを満たしているかどうかを確認します。

  たとえば、デフォルトのパスワードポリシーは、少なくとも 1 つの大文字と数字を含んだ 8 または 9 文字のパスワードを認めています (Password1 など)。

- リソースを作成して保存しようとしたときに、次のエラーが発生しました : `The following resource failed to save: Reason: Unable to test connector`。

  解決方法 :

  コネクタの配布時に、アプリケーションサーバーの classpath に以下の設定ファイルが存在するかどうかを確認します。

  — `com\hp\ovsi\connector\bidirldap\activedir\ActiveDirConfig.properties`

- リンク / アンリンク操作のバイパスが機能しません。

  解決方法 :

  `ActiveDirConfig.properties` ファイルで `dualLink-support` パラメータに 2 を設定し、コネクタスキーマファイルで `byPass` を `User` と `Group/Computer` エンティティの両方に設定します。

- 短時間の中断後、ユーザーが操作しようとすると WebSphere で通信例外が発生し、ログファイルに以下のエラーメッセージが表示されました。

  `javax.naming.CommunicationException`

  原因 :

  アプリケーションサーバーにおける JCA 接続の接続タイムアウトが、リソースに対するコネクタの接続タイムアウトと一致していません。

  解決方法 :

  Active Directory では、リソースタイムアウト (`MaxConnIdleTime`) は、WebSphere 接続プールパラメータの Unused timeout と Reap time の合計よりも大きくする必要があります。また、Minimum connections はゼロに設定する必要があります。WebSphere コンソールで以下の手順を実行し、接続プール設定を変更してください。

  a WebSphere コンソールにログオンします。

  b 左側のペインで、**[リソース] → [リソース・アダプター]** の順にクリックします。

  c 右側のペインで、[設定] セクションの下にあるコネクタ名をクリックします。

d 右側のペインで、**[J2C 接続ファクトリー]** をクリックします。

e [設定] セクションの下にあるコネクタ名をクリックします。

f 右側のペインで、**[接続プールプロパティー]** をクリックします。

g [一般プロパティー] セクションで、以下の変更を行います。

- [最大接続数] をゼロに設定します。
- [経過時間タイムアウト] にゼロより大きな値を設定します。
- [リープ時間] と [未使用タイムアウト] を設定し、これらの合計が Active Directory サーバーの `MaxConnIdleTime` の値よりも小さくなるようにします。

- 時々、調整が失敗する場合があります。

  解決方法 :

  すべてのリソース属性を SI にマッピングされていることを確認してください。

- パスワードプラグインをアンインストールし、再度インストールする場合、この作業が既存のユーザーに影響を与えてしまいます。

  解決方法 :

  パスワードプラグインを再インストールするときに、`ADProperties.ini` ファイルの古いキーを手動で変更します。このキーは、Select Identity リソースプロパティの encryptionKey フィールドに格納されています。

  または

  パスワードプラグインの再インストール時に、[Generate a New Key] を選択しないでください。

- ユーザーのグループへのリンクに失敗しました。

  AD には、Domain Local、Global、および Universal の 3 種類のグループが存在します。ユーザーを、異なったドメインの Global Group にリンクすることはできません。

- 削除されたユーザーの調整に失敗しました。

  解決方法 :

  ユーザーを削除する前に、新たに作成されたユーザーが Select Identity に取り込まれたことを確認してください。そうでない場合、コネクタは削除の調整を無視します。

  または

  Active Directory の削除されたオブジェクトを非管理者が照会できるようにしたい場合は、削除されたオブジェクトコンテナの権限を変更し、非管理者が Active Directory Application Mode (ADAM) Administration Tools に含まれている DSACLS.exe を実行して、このコンテナを照会できるようにしてください。

  ADAM Administration Tools をインストールすれば、削除されたオブジェクトコンテナの権限を変更することができます。

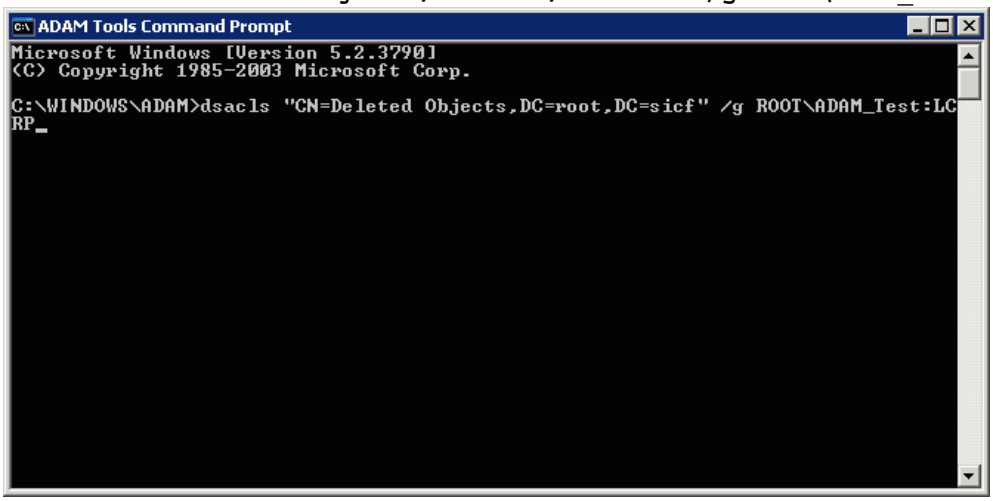
  a Domain Admins グループのメンバーのユーザーアカウントを使用して、ログオンします。

  b **[スタート] → [すべてのプログラム] → [ADAM] → [ADAM Tools Command Prompt]** の順にクリックします。

  [ADAM Tools Command Prompt] ウィンドウが表示されます。

c コマンドプロンプトで、以下の例に従ってコマンドを入力します。

```
dsacls "CN=Deleted Objects,DC=root,DC=sicf" /g ROOT\ADAM_Test:LCRP
```



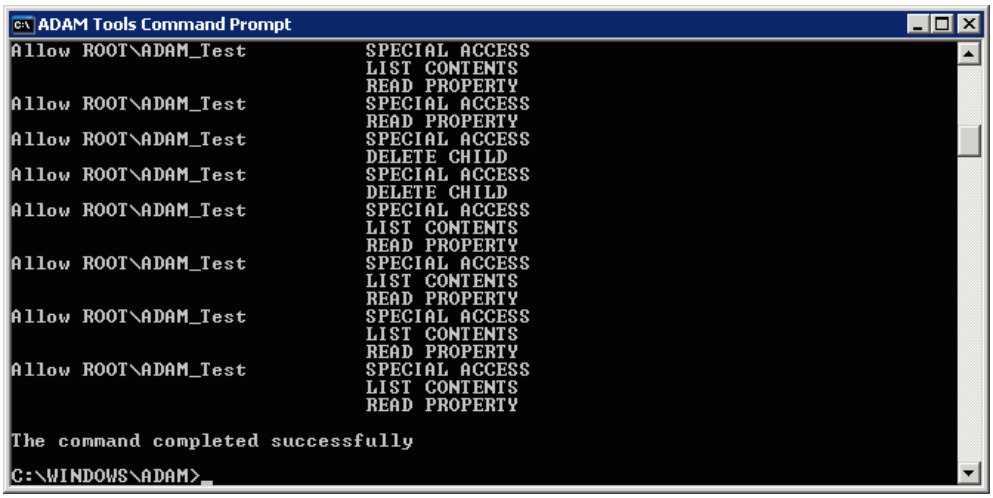
コマンドを入力するとき、必ず自分のドメインの削除されたオブジェクトコンテナ名を使用してください。

フォレスト内の各ドメインは、削除されたオブジェクトに対して独自のコンテナを保有しています。

また、ADAM Administration Tools をインストールせずに、ADAM インストールフォルダをターゲット DC にコピーすることも可能です。インストールフォルダで DSACLS.exe を探し、以下の例に従ってコマンドプロンプトにコマンドを入力します。

```
dsacls "CN=Deleted Objects,DC=root,DC=sicf" /g ROOT\ADAM_Test:LCRP
```

Enter キーを押すと、出力ウィンドウが表示されます。



ユーザーの ROOT\ADAM_Test により、ROOT ドメインの削除されたオブジェクトコンテナに対して List Contents と Read Property 権限が与えられました。これらの権限により、ユーザーは削除されたコンテナの内容を照会することができますが、コンテナのオブジェクトに何らかの変更を加えることはできません。これらの権限は、管理者グループに与えられたデフォルトの権限と同等のものです。

- Active Directory 双方向 LDAP コネクタ v2.0 またはそれ以降のバージョンが配布された後、Select Identity の属性リストから domain 属性がなくなりました。

  解決方法 :

  詳細は、103 ページの「Select Identity における属性の追加 / 削除の確認」を参照してください。

- Select Identity のバージョンアップを行った後、使用権を持ったユーザーの作成要求が正常に送信できません。以下のようなエラーメッセージが表示される場合があります。

  ERRORS

  Parameter constraints violation. <Resource_ENTITLEMENT>

  原因 :

  Select Identity のバージョンアップ後、cbc_config.zip に存在するデータベーススクリプト (MS SQL データベースの場合は mssql_cbc_ddl.sql、Oracle の場合は Oracle_cbc_ddl.sql) が実行されませんでした。

  解決方法 :

  データベーススクリプトを再実行します。

- CRL チェックを行うことができません。

  解決方法 :

  Sun JDK のバージョン 1.5.0_06-b05 はバージョンが低すぎるので、Sun JDK のバージョン 1.5.0_09-b03 またはバージョン 1.5 よりも高いバージョンにアップグレードしてください。

- Select Identity サービスに userSuffix 属性が存在しない場合、Windows 2000 AD Server の Webshpere におけるグループメンバーシップ変更の調整が失敗しました。

  解決方法 :

  Select Identity サービスに userSuffix 属性が存在し、有効な値が指定されていることを確認してください。

- ドメイン間のユーザーの移動が失敗しました。

  解決方法 :

  以下の手順を実行します。

  a Windows Native Function(WNF) フレームワークが正しくインストールされているかどうかを確認します。

  b ターゲット OU が存在することを確認します。

  c transientUserSuffix 属性が AD サーバーに存在するかどうかを確認します。

d コネクタのプロパティファイル (通常は ActiveDirConfig.properties) をチェックし、リクエスト / レスポンス属性が、エージェント側の PasswordAgent-config.xml で定義されたリクエスト / レスポンス属性と一致するかどうかを確認します。

e 相互認証モードで稼動している場合、リソース作成用のパスワードが AD サーバーに対して有効であることを確認します。

- 相互認証モードで、リソースの作成が失敗しました。

  解決方法 :

  以下の手順を実行します。

  a AD サーバーがアクティブであり、配置および接続が可能かどうかを確認します。

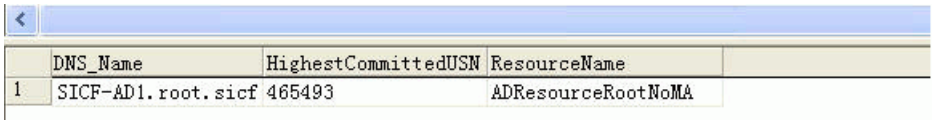
  b 相互認証が Select Identity で正しく設定されていることを確認します。

  c グローバルカタログポートが、コネクタプロパティファイルで **3269** に設定されているかどうかを確認します。

- Select Identity に調整要求が送信されません。

  解決方法 :

  以下の例に示すように、OVSI_BIDIRLDAP_LCLN が正しく設定されているかどうか確認します。



	DNS_Name	HighestCommittedUSN	ResourceName
1	SICF-AD1.root.sicf	465493	ADResourceRootNoMA

- パスワードプラグインが正常にインストールされたことを検証します。

  解決方法 :

  以下の手順を実行して、検証を行います。

  a 以下のファイルが System32 ディレクトリに存在することを確認します。

  ```
  ADPassfilt.dll
  ADProperties.ini
  libeay32.dll
  libssl32.dll (32 ビット AD サーバー )/ssleay32.dll (64 ビット AD サーバー )
  ```

  b レジストリの HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages に文字列 ADPassfilt が存在することを確認します。

- ドメイン間のユーザーの移動が正常にインストールされたことを検証します。

  解決方法 :

  以下の手順を実行して、検証を行います。

  a 以下のファイルが System32 ディレクトリに存在することを確認します。

  ```
  PasswordAgent-config.xml
  Interop.ActiveDs.dll
  log4net.dll
  HP.AD.Logging.config
  HP.AD.Common.Logging.dll
  HP.AD.WNF.ActionInterface.dll
  ```

```
HP.AD.WNF.Delegate.dll
HP.AD.WNF.MoveUser.dll
HP.AD.WNF.Utilities.dll
```

b レジストリの HKEY_CLASSES_ROOT に HP.AD.WNF.CommandDelegate が存在することを確認します。

- パスワードプラグインと Windows Native Function フレームワークのバージョンを確認します。

  解決方法 :

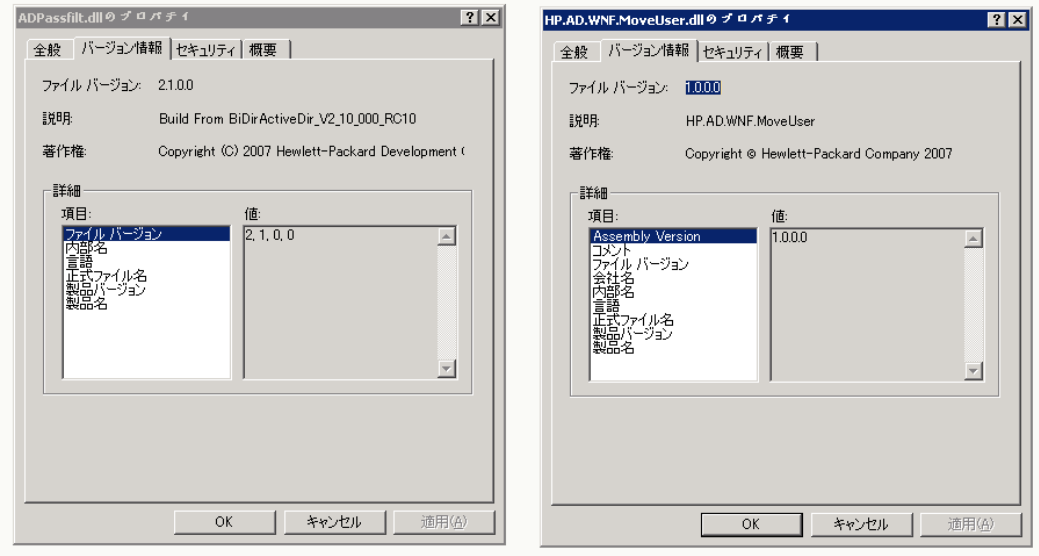
  — パスワードプラグイン

  ADPassfilt.dll ファイルを System32 ディレクトリに配置し、それを右クリックしてポップアップメニューから **[プロパティ]** を選択します。[ADPassfilt.dll プロパティ] ウィンドウが表示されます。以下に示すように、[バージョン] タブにパスワードプラグインのバージョンが表示されます。

  — Windows Native Function フレームワークのバージョン

  ドメイン間のユーザー移動機能は、Windows Native Function(WNF) フレームワークを通じて機能します。

  WNF のバージョンを確認するには、System32 ディレクトリに HP.AD.WNF.MoveUser.dll ファイルを配置し、それを右クリックしてポップアップメニューから **[プロパティ]** を選択します。[ADPassfilt.dll プロパティ] ウィンドウが表示されます。以下に示すように、[バージョン] タブに WNF のバージョンが表示されます。



- メールボックスの作成時に、System.Net.WebException 例外がスローされて、ログファイルに以下の内容が記録されます。

```
System.Net.WebException: Unable to connect to the remote server --->
System.Net.Sockets.SocketException: No connection could be made because
the target machine actively refused it

   at System.Net.Sockets.Socket.DoConnect(EndPoint endPointSnapshot,
SocketAddress socketAddress)

   at System.Net.Sockets.Socket.InternalConnect(EndPoint remoteEP)
```

```
   at System.Net.ServicePoint.ConnectSocketInternal(Boolean
connectFailure, Socket s4, Socket s6, Socket& socket, IPAddress& address,
ConnectSocketState state, IAsyncResult asyncResult, Int32 timeout,
Exception& exception)

   --- End of inner exception stack trace ---

   at System.Net.HttpWebRequest.GetRequestStream()

   at System.Web.Services.Protocols.SoapHttpClientProtocol.Invoke(String
methodName, Object[] parameters)

   at
HP.AD.WNF.CreateMailBoxClientAction.WCFService.ExchangeWCFService.DoComma
nd(String messageName, String[] parameters)

   at HP.AD.WNF.Action.CreateMailBoxClientAction.Execute(String message)
```

原因：

Windows サービスが開始されていません。

解決方法：

Windows サービスを開始します。

- メールボックス付きのユーザーを作成するとき、プロビジョニングが初回時に失敗して、メールボックスが Exchange Server 2007 に正しく作成されません。

  a Select Identity の情報：

	Mode	Operation	Operation Arg	Operation Status	Op Last Update Time	Detail
0	INITIAL	USER_ADD	david1204_Ex5	FAILED	12/04/2007 02:27 PM	com.trulogica.truaccess.connector.exception.TAConnectorException: Errors: Active Directory operation faile IDSMWIN23.domaina.sicf. This error is not retriable. Additional information: Insufficient access rights to pe Active directory response: 00002098: SecErr: DSID-03150A45, problem 4003 (INSUFF_ACCESS_RIGHTS 0:TAConnectorException, [Errors: Active Directory operation failed on IDSMWIN23.domaina.sicf. This error i Additional information: Insufficient access rights to perform the operation. Active directory response: 00002 03150A45, problem 4003 (INSUFF_ACCESS_RIGHTS), data 0]:
0	INITIAL	USER_RESET_PASSWORD	david1204_Ex5	FAILED	12/04/2007 02:27 PM	com.trulogica.truaccess.connector.exception.TAConnectorException: Errors: Active Directory operation faile IDSMWIN23.domaina.sicf. This error is not retriable. Additional information: Insufficient access rights to pe Active directory response: 00002098: SecErr: DSID-03150A45, problem 4003 (INSUFF_ACCESS_RIGHTS 0:TAConnectorException, [Errors: Active Directory operation failed on IDSMWIN23.domaina.sicf. This error i Additional information: Insufficient access rights to perform the operation. Active directory response: 00002 03150A45, problem 4003 (INSUFF_ACCESS_RIGHTS), data 0]:

  b AD サーバーの system32 のログ：

```
...

2007-12-04 12:20:59,640 [15] ERROR -
HP.AD.WNF.Action.CreateMailBoxClientAction - There are some errors in
Execute(string message),The Errot is: Errors:

This task does not support recipients of this type. The specified
recipient domaina.sicf/OpenView/SelectIdentity/TISU/Ad_exchange_da1 is
of type MailUser. Please make sure that this recipient matches the
required recipient type for this task.
```

  c Exchange Server のログ：

```
...

2007-12-04 12:20:59,225 [7] INFO  -
HP.AD.WNF.Plugin.CreateMailBoxServerAction - There are exceptions, the
exceptions are System.Exception: Errors:
```

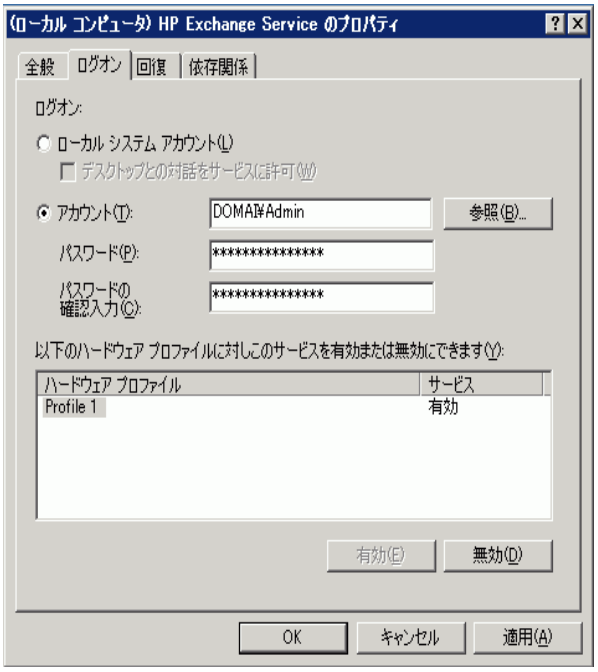
```
This task does not support recipients of this type. The specified
recipient domaina.sicf/OpenView/SelectIdentity/TISU/Ad_exchange_da1 is
of type MailUser. Please make sure that this recipient matches the
required recipient type for this task.


   at HP.AD.WNF.Plugin.ExchangeBridge.RunPowerShellScript(String
script)

   at HP.AD.WNF.Plugin.CreateMailBoxServerAction.Execute(BaseModel
model)
```

原因：

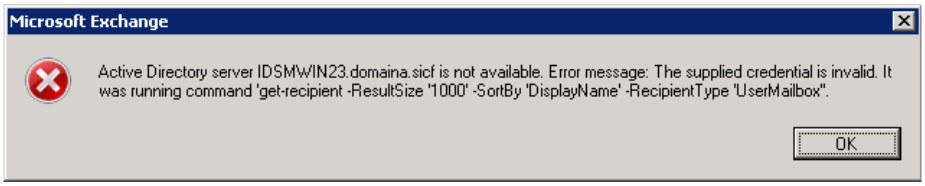
HP Exchange Service のログオンユーザーアカウントのドメイン権限が不足しています。

解決方法：

以下に示すように、十分な権限を持った HP Exchange Service ログオンユーザーアカウントを指定します。



- Exchange Server でメールボックスを更新するとき、次のエラーメッセージが表示されました。[Active Directory server IDSMWIN23.domaina.sicf is not available. Error message: The supplied credential is invalid] .



原因：

構成が正しく行われていません。

解決方法 :

Exchange Organization Administrators グループに所属するユーザーアカウント を使用して Exchange 2007 Server の [ツールボックス] の [構成管理ツール] を実行してください。また、ユーザーアカウント は Exchange 2007 Server と 同じドメインに属する必要があります。

B　証明書のインストール

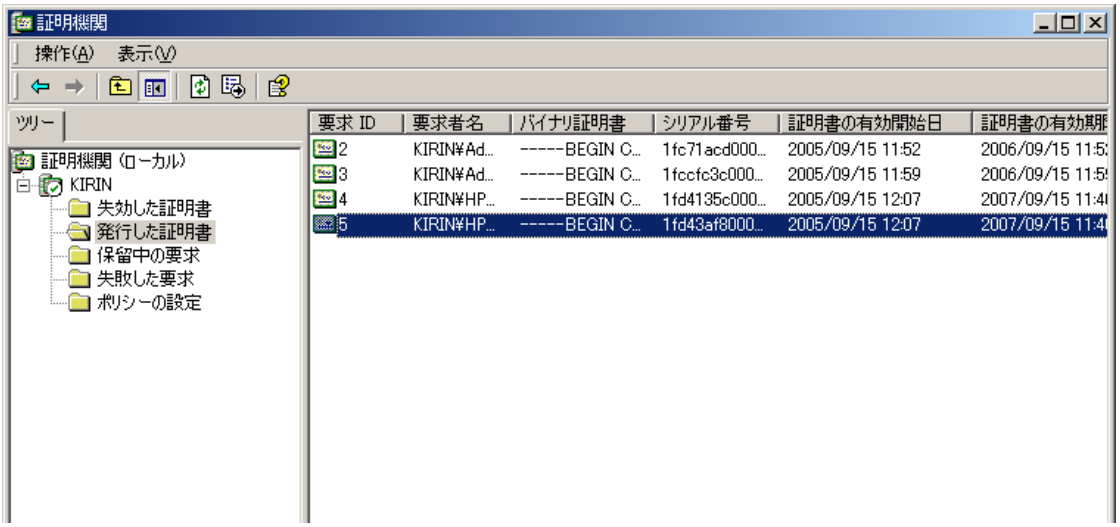
Active Directory におけるルート CA 証明書の作成

以下の手順に従って、Active Directory でルート CA 証明書を作成します。

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。

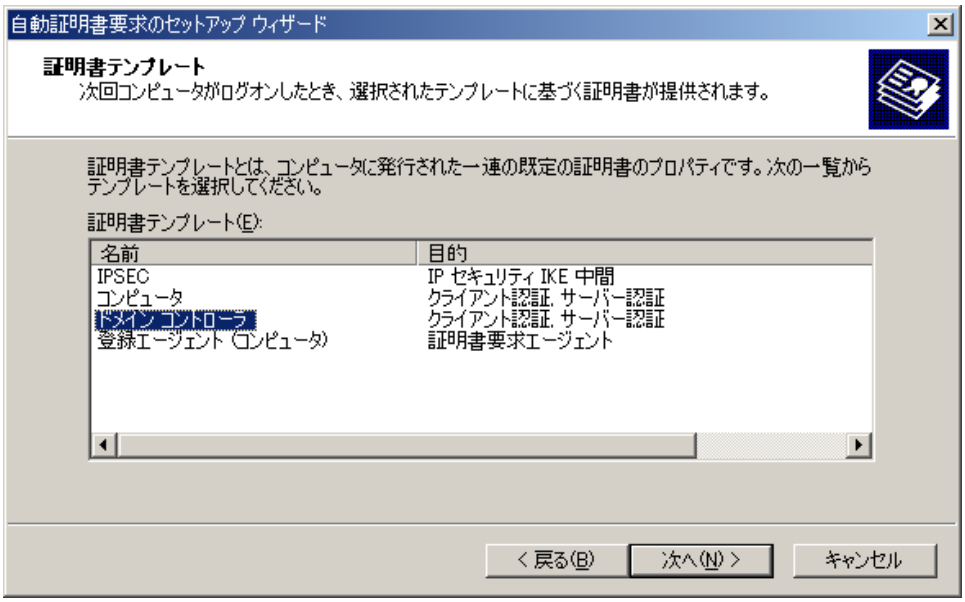
2　システム上で HTTPS を構成します。

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。Windows Server 2003 上に作成された証明書を以下に示します。



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、mmc からのスナップインを使用して [信頼されたルート証明機関] → [証明書] の下にある、CA と同じ名前の付いた証明書を開きます。

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。

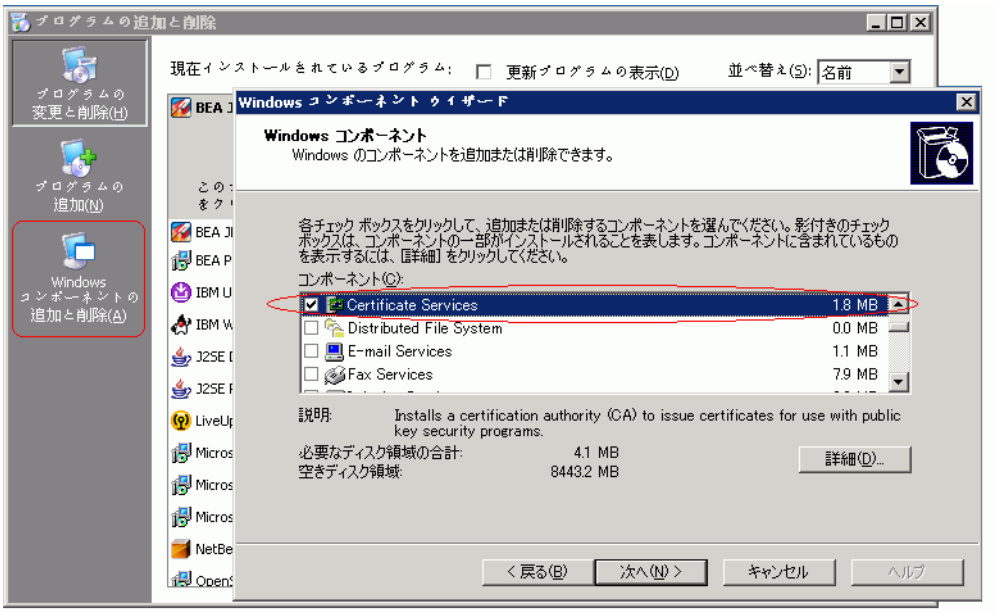
証明書サービスの設定

以下の手順に従って、証明書サービスを設定します。

1 [スタート] メニューから、**[コントロールパネル]** → **[プログラムの追加と削除]** の順にクリックします。[プログラムの追加と削除] ウィンドウが開きます。

2 左側のパネルで **[Windows コンポーネントの追加と削除]** をクリックし、Windows コンポーネントウィザードを起動します。

3 [証明書サービス] にチェックを付け、ウィザードに従って証明書サービスを設定します。

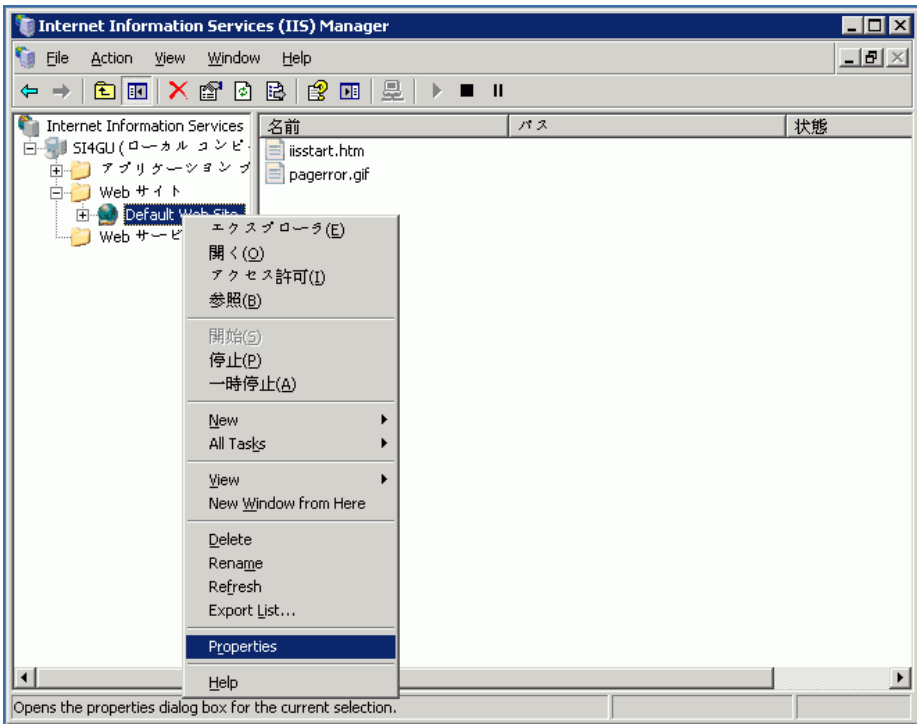


新しい証明書を適用するための情報の生成

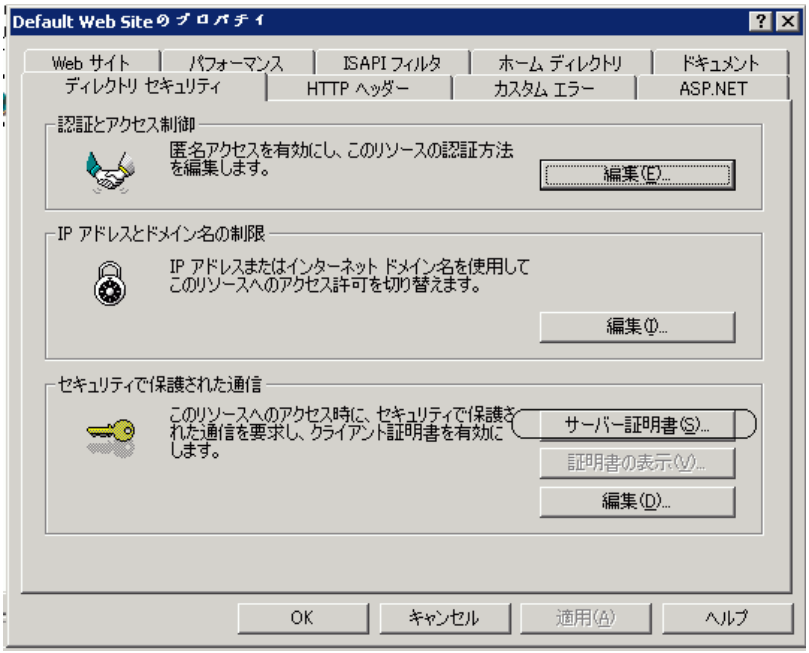
以下の手順に従って、新しい証明書を適用するための情報を生成します。

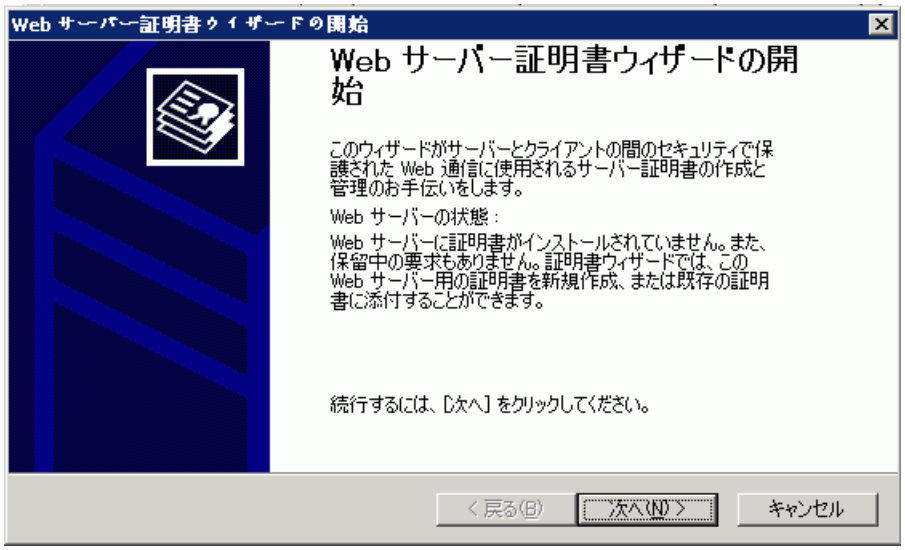
1 Active Directory サーバーで、[スタート] メニューから **[管理者ツール]** → **[インターネットインフォメーションサービス (IIS) マネージャ]** の順にクリックします。[インターネットインフォメーションサービス (IIS) マネージャ] ウィンドウが開きます。

左側のパネルでローカルコンピュータノードを展開し、**[Web サイト]** を表示します。[既定の Web サイト] を右クリックし、コンテキストメニューから [プロパティ] を選択し、[既定の Web サイトのプロパティ] ウィンドウを開きます。

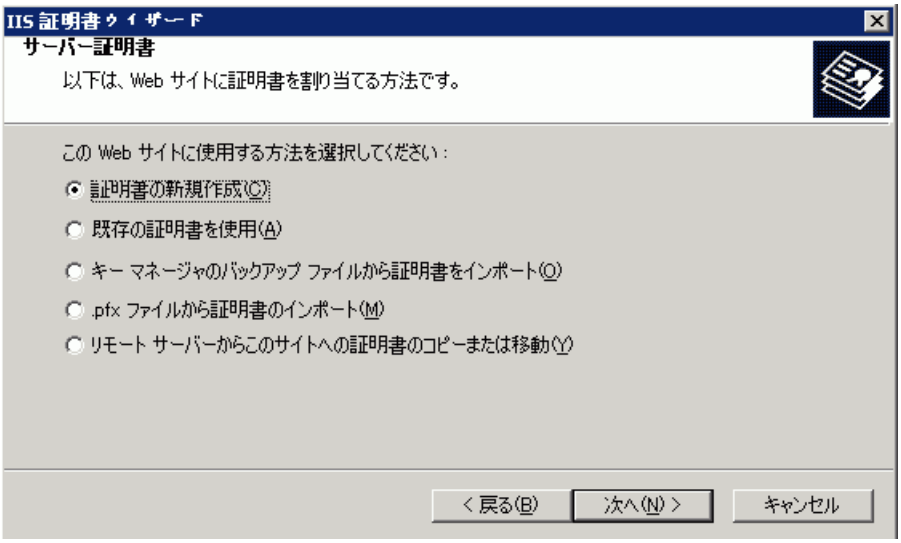


[既定の Web サイトのプロパティ] ウィンドウの [ディレクトリセキュリティ] タブで、**[サーバー証明書]** をクリックして [Web サーバー証明書ウィザード] を起動します。

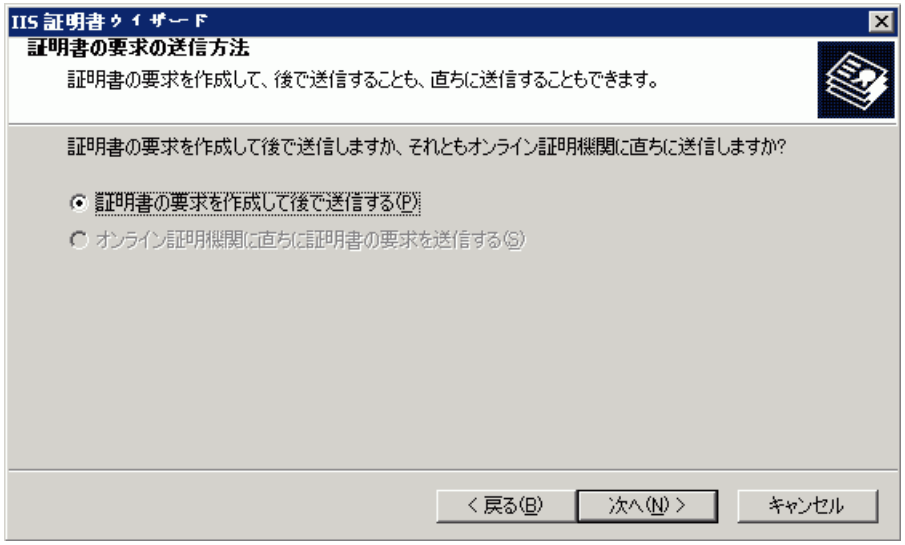




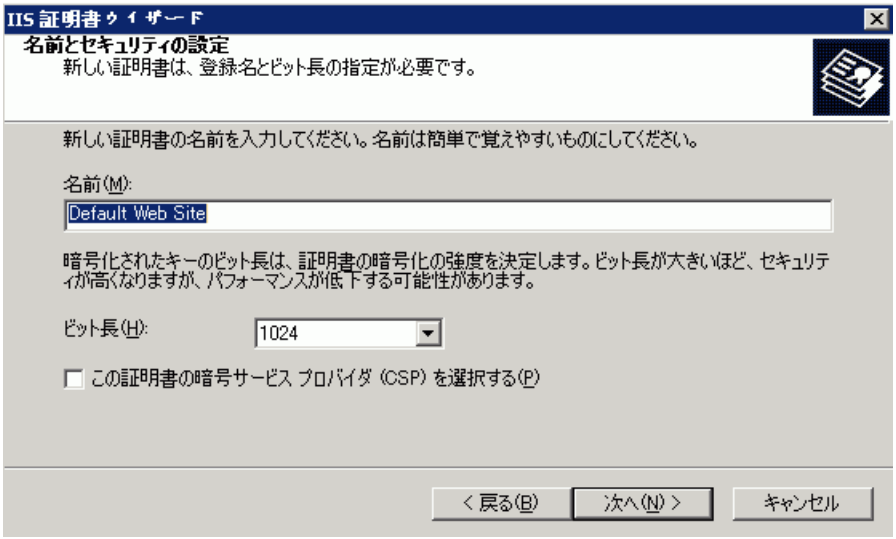
2 **[次へ]** をクリックして [サーバー証明書] ページへ移動し、**[証明書の新規作成]** を選択します。



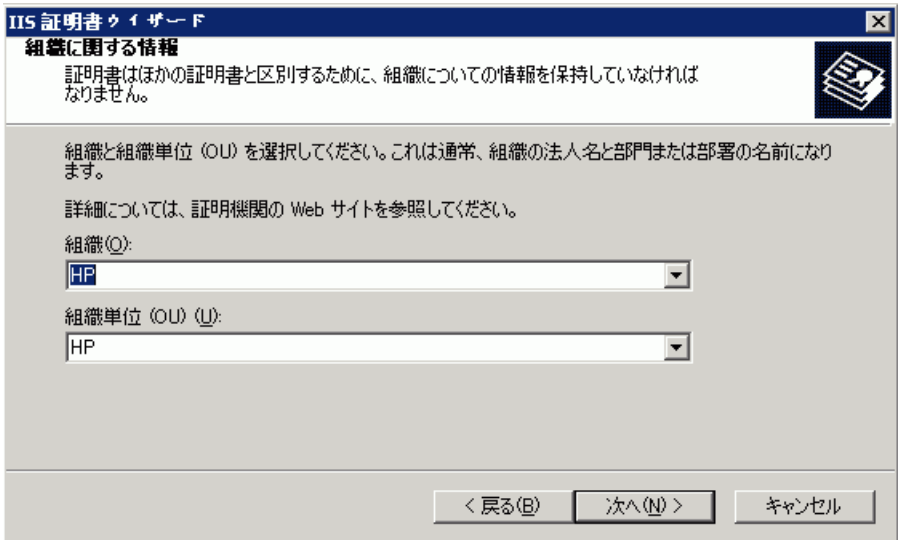
[次へ] をクリックして　[証明書の要求の送信方法] ページへ移動し、**[証明書の要求を作成して後で送信する]** を選択します。



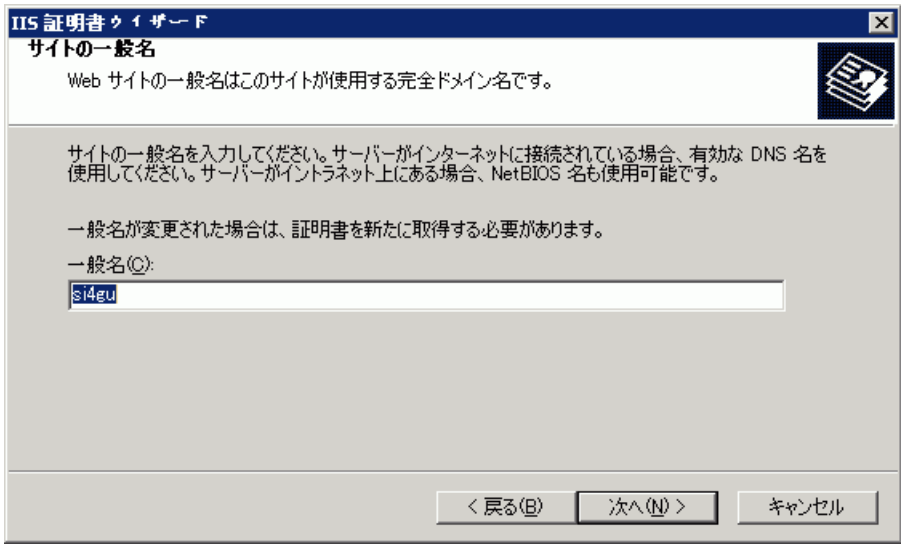
[次へ] をクリックして [名前とセキュリティの設定] ページに移動します。名前を指定するか、またはデフォルトの設定をそのまま使用します。



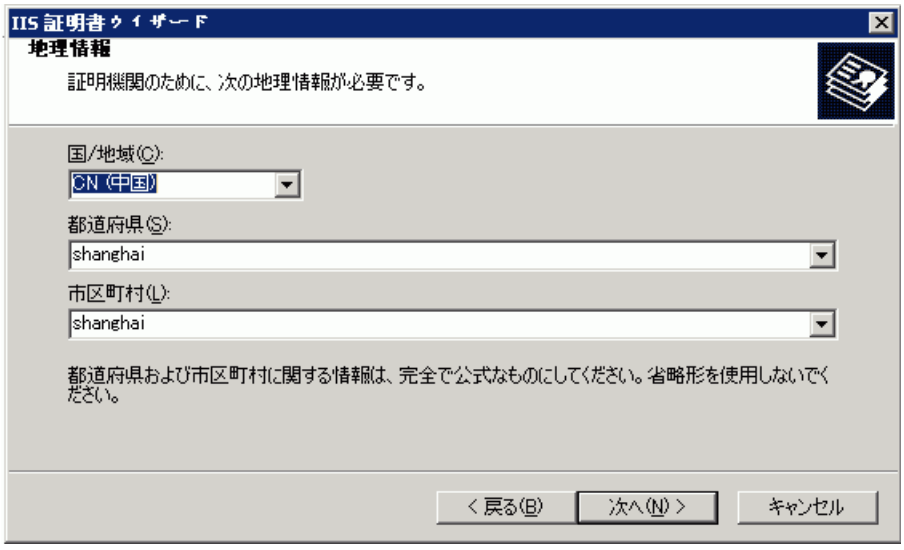
[次へ] をクリックして次のページに移動します。プロンプトに従って、必要な組織情報を入力します。



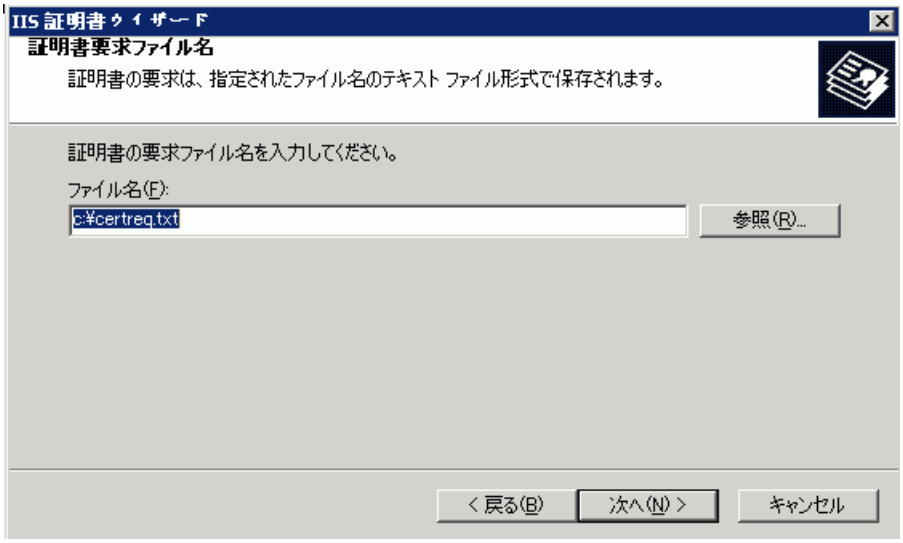
[次へ] をクリックして次のページに移動します。必要に応じて、共通の名前を指定するか、またはデフォルトの設定をそのまま使用します。



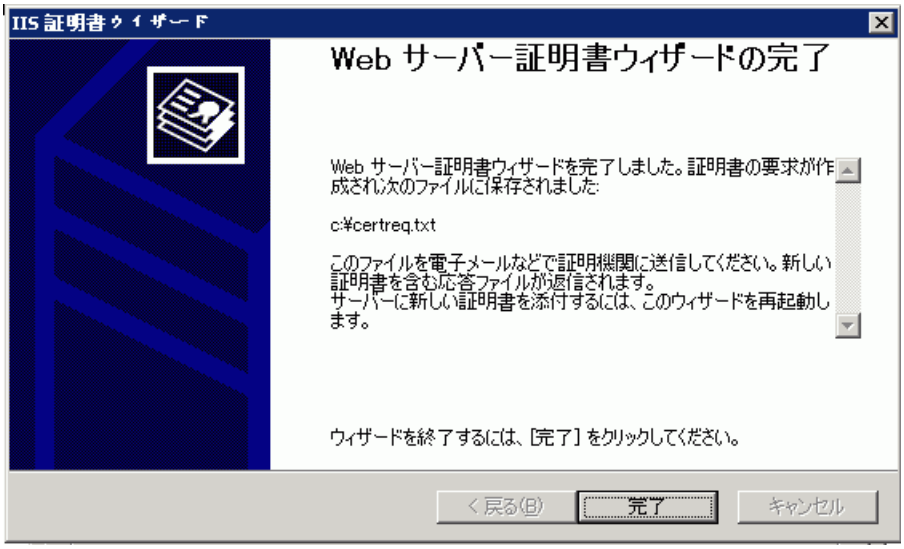
[**次へ**] をクリックして、地理情報を選択します。



[**次へ**] をクリックします。証明書の名前を指定します。



[次へ] をクリックして、要求ファイルの要約を確認します。再度、**[次へ]** をクリックします。



[完了] をクリックすると、要求情報がテキストファイル `c:\certreq.txt` に保存されます。

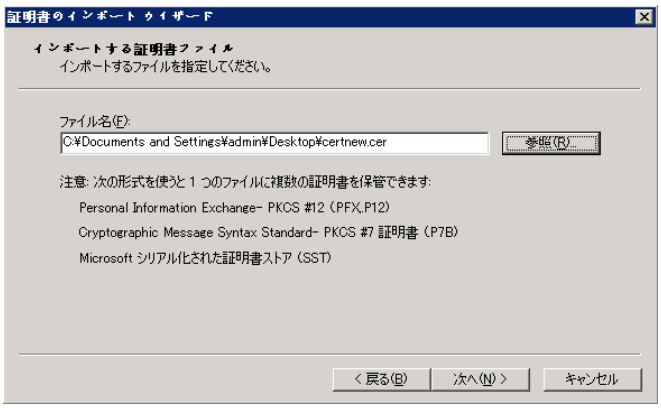
C Active Directory サーバーへの証明書のインポート

Select Identity と Active Directory サーバー間の SSL 接続では、Active Directory サーバーの手動設定が必要となります。

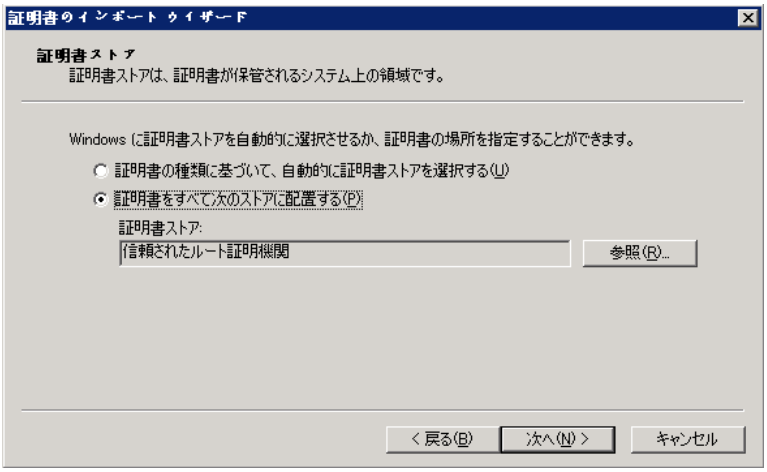
証明書を Active Directory コンピュータの信頼できるルート CA 証明書ストアへインポート

以下の手順に従って、証明書を AD コンピュータの信頼できるルート CA 証明書ストアにインポートします。

1. **mmc** を [ファイル名を指定して実行] ボックスに入力し、**[OK]** をクリックして MMC スナップインを起動します。
2. **[ファイル]** → **[スナップインの追加と削除]** の順に選択します。[スナップインの追加と削除] ウィンドウが開きます。
3. **[追加]** をクリックすると、[スタンドアロンスナップインの追加] ウィンドウが表示されます。
4. **[証明書]** を選択し、**[追加]** をクリックします。[証明書スナップイン] ポップアップウィンドウが開きます。
5. **[コンピュータアカウント]** を選択し、**[次へ]** をクリックします。[コンピュータの選択] ウィンドウが表示されます。
6. **[ローカルコンピュータ]** を選択し、**[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] ウィンドウで **[閉じる]** をクリックします。
8. [スナップインの追加と削除] ウィンドウで **[OK]** をクリックします。
9. MMC コンソールで、**[証明書 (ローカルコンピュータ)]** → **[信頼されたルート証明機関]** → **[証明書]** の順に展開します。**[証明書]** を右クリックし、**[すべてのタスク]** → **[インポート]** の順に選択すると、[証明書のインポートウィザード] が表示されます。
10. **[次へ]** をクリックすると、[インポートする証明書ファイル] ページが表示されます。証明書を探します。



11 **[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。



12 **[次へ]** をクリックし、**[完了]** をクリックします。インポートは正常に終了しました。

証明書を Active Directory コンピュータの個人証明書ストアへインポート

以下の手順に従って、証明書を AD コンピュータの個人証明書ストアにインポートします。

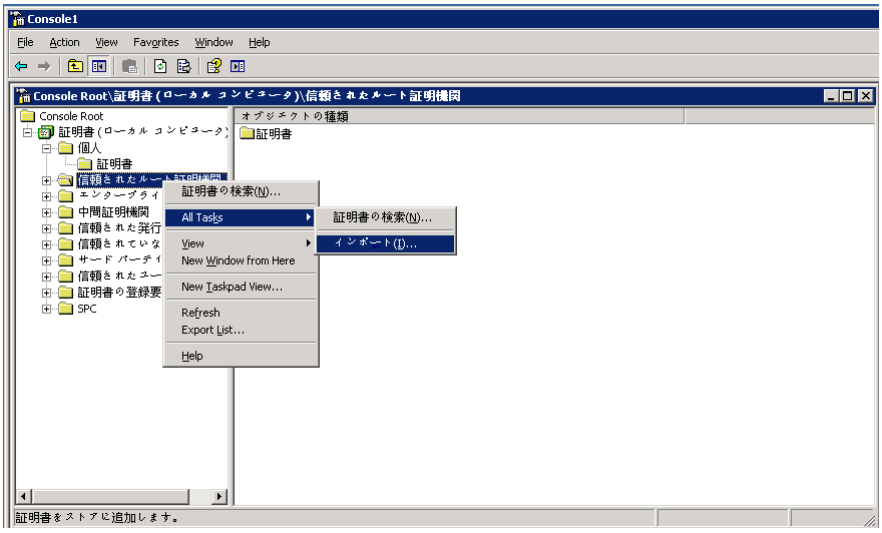
1 証明書を取得します (例 : *thirdParty*.crt)。

2 コマンドを使用して *thirdParty*.crt を *thirdParty*.pfx に変換します。

```
openssl pkcs12 -export -inkey server.key -in thirdParty.crt -out
thirdParty.pfx
```

3 *thirdParty*.pfx を AD コンピュータの個人証明書ストアのリソースにインポートします。

MMC コンソールで、**[証明書 (ローカルコンピュータ)]** → **[信頼されたルート証明機関]** → **[証明書]** の順に展開します。**[証明書]** を右クリックし、**[すべてのタスク]** → **[インポート]** の順に選択します。

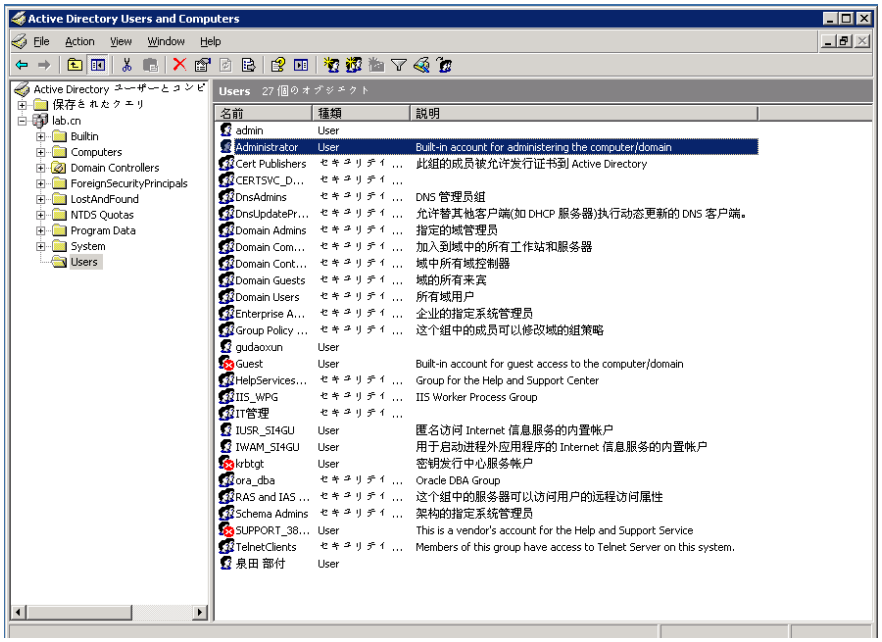


手順 10 から手順 12 までを繰り返します。

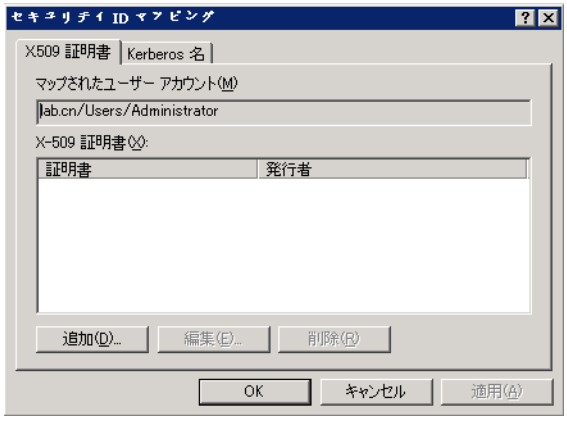
AD におけるユーザーの Select Identity 証明書へのマッピング

AD でオプションを選択し、以下の手順に従ってユーザーを Select Identity 証明書にマッピングしてください。

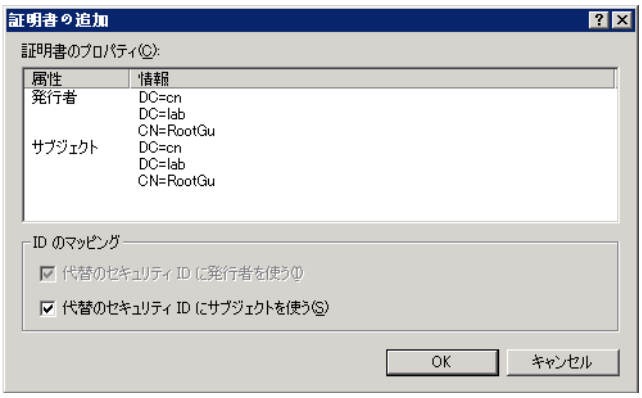
1. **[Active Directory ユーザーとコンピュータ]** を開きます。[Active Directory ユーザーとコンピュータ] ウィンドウが表示されます。
2. **[表示]** → **[詳細設定]** の順にクリックします。
3. ナビゲーションペインで **[ユーザー]** ノードをクリックし、リソースの操作を行うために Select Identity に対するアクセス権を持つユーザーを選択します (例 : Administrator)。



4 ユーザーを右クリックし、**[名前のマッピング]** を選択します。[セキュリティ ID マッピング] ウィンドウが表示されます。



5 **[追加]** をクリックして、Select Identity 証明書ファイルを探します。



6 **[OK]** をクリックします。

7 **[OK]** をクリックします。ユーザーが Select Identity 証明書にマッピングされました。

D スキーマファイルのカスタマイズ

ActiveDirSchema.jar ファイルには、ActiveDirConfig.properties などのプロパティファイルに加えて、スキーマファイル (ActiveDir.xml) が存在します。このファイルは属性の関係を定義し、Select Identity とコネクタ間をマッピングします。このスキーマファイルは、ニーズに合わせて変更可能です。

新しい属性マッピングの追加

スキーマファイルの新しい属性を追加するには、2 つのタグを追加する必要があります。

1 最初に、スキーマファイルの <Schema>\<objectClassDefintion description="" name="User">\<memberAttributes> に新しいタグ <attributeDefinitionReference> を追加します。

```
+ <objectClassDefinition description="" name="Group">
+ <objectClassDefinition description="" name="Computer">
- <objectClassDefinition description="" name="User">
  + <properties>
  - <memberAttributes>
      <attributeDefinitionReference attrFunction="provision|post|pre" attributeType="Read/write" concero:isKey="false"
        concero:resfield="userAccountControl" concero:tafield="userAccountControl" defaultValue="" encrypt="false"
        encrypted="false" encryptionAlgorithm="" expirePassword="false" expireValue="" isPassword="false" linktoentity=""
        multivalued="false" mustOnResource="false" name="objectclassuserattributeuserAccountControl" objectclass="user"
        objectclasstype="structural" ordering="" remexpireValue="" renamekey="false" required="false" resourcekey="false"
        entityType="user"
        supportedOperations="UNLINK,LINK,GETATTRIBUTES,GETPARENT,GETCHILDREN,GETALL,RESETPASSWORD,CHANGEPASSWORD,EX
        transform="NO" type="java.lang.String" />
    - <!--
                    <attributeDefinitionReference
                        attrFunction="provision|post|pre"
```

2 タグ <attributeDefinition> を、スキーマファイルのタグ <Schema> に追加します。

```
+ <objectClassDefinition description="" name="Group">
+ <objectClassDefinition description="" name="Computer">
+ <objectClassDefinition description="" name="User">
- <attributeDefinition description="Group_objectclassgroupattributemember" name="Group_objectclassgroupattributemember"
    type="java.lang.String">
  - <properties>
    - <attr name="minLength">
        <value>0</value>
      </attr>
    - <attr name="maxLength">
        <value>255</value>
      </attr>
    - <attr name="defaultValue">
        <value />
      </attr>
    - <attr name="pattern">
      - <value>
          <![CDATA[ [a-zA-Z0-9@]+  ]]>
        </value>
      </attr>
    </properties>
  </attributeDefinition>
- <attributeDefinition description="Group_objectclassldapv3ConnectorattributegroupSuffix"
    name="Group_objectclassldapv3ConnectorattributegroupSuffix" type="java.lang.String">
  - <properties>
```

3 さらに属性を追加する場合は、上記の 2 つの手順を繰り返します。

以下に、属性のパラメータを記述する <attributeDefinitionReference> タグの例を示します。

```
<attributeDefinitionReference attrFunction="provision|post|pre"
attributeType="Read/write" concero:isKey="false"
concero:resfield="userAccountControl" concero:tafield="userAccountControl"
defaultValue="" encrypt="false" encrypted="false" encryptionAlgorithm=""
expirePassword="false" expireValue="" isPassword="false" linktoentity=""
multivalued="false" mustOnResource="false"
name="objectclassuserattributeuserAccountControl" objectclass="user"
objectclasstype="structural" ordering="" remexpireValue="" renamekey="false"
required="false" resourcekey="false" entityType="user"
supportedOperations="UNLINK,LINK,GETATTRIBUTES,GETPARENT,GETCHILDREN,GETALL,
RESETPASSWORD,CHANGEPASSWORD,EXPIREPASSWORD,DISABLE,ENABLE,CREATE,DELETE,UPD
ATE" transform="NO" type="java.lang.String" />
```

それぞれの説明に従って、属性パラメータの値を変更することができます。

- `attrFunction="provision|post|pre"`

  このパラメータは、属性のプロビジョニングタイプを指定します。文字列 `"provision|post|pre"` はデフォルト値として使用され、Select Identity の 3 つのワークフロー (プロビジョニング、ポストプロビジョニング、プレプロビジョニング) を示します。この属性値を変更することにより、属性がサポートするワークフローを選択することができます。

- `attributeType="Read/Write"`

  このパラメータは、属性がリソースに対して読み込み / 書き込み権限を持つかどうかを指定します。文字列 `"Read/Write"` はデフォルト値として使用され、属性がリソースに対して読み込みと書き込みができることを意味します。このパラメータ値は、リソースに対する属性の権限に従って設定してください。

- `concero:isKey="false"`

  このパラメータは、属性が Select Identity のオブジェクトを一意に識別するためのキーであるかどうかを指定します。

  スキーマファイルのすべての属性の中で、1 つの属性のみに `true` 値を指定することができます。

- `concero:resfield="userAccountControl"`

  このパラメータは、リソースの属性に対応する属性名を指定します。

- `concero:tafield="userAccountControl"`

  このパラメータは、Select Identity の属性に対応する属性名を指定します。

- `defaultValue=""`

  このパラメータは、デフォルト値を指定します。

- `encrypt="false"`

  このパラメータは、属性の暗号化が必要かどうかを指定します。パラメータ `encrypt` が true の場合、属性値はコネクタにより暗号化される必要があります。

- `encrypted="false"`

  このパラメータは、Select Identity から受け取る値が暗号化されているかどうかを指定します。パラメータ `encrypted` が true の場合、属性値はコネクタにより再度暗号化される必要はありません。

- `encryptionAlgorithm=""`

パラメータ encrypt が true に設定されている場合、このパラメータは暗号化に使用されるアルゴリズムを指定します。

- expirePassword="false"

  このパラメータは expireValue と一緒に使用し、パスワードを期限切れに設定します。

- expireValue="-1"

  このパラメータは、パスワードを期限切れに設定するためのデフォルト値を指定します。expirePassword が true であり、かつ expireValue が -1 の場合、パスワードは期限切れに設定されます。

- isPassword="false"

  このパラメータは、この属性がパスワードかどうかを指定します。これは、パラメータ password に対しては特別な注意が必要なためです。

  スキーマファイルのすべての属性の中で、1 つの属性のみに true 値を指定することができます。

- linktoentity=""

  このパラメータは、属性にリンクされるエンティティを指定します。この例では、パラメータの値として Computer、User、および Group の 3 つが使用できます。これは、タグ <ObjectClassDefinition> で指定します。

  一般的に、group 値を指定できるのは属性 memberof に対してのみであり、空値は他の属性に使用されます。

- multivalued="false"

  このパラメータは、属性が単一値を持つか、複数値を持つかを指定します。true が設定された場合は属性は複数値を持ち、false が設定された場合は属性は単一値を持ちます。

- mustOnResource="false"

  このパラメータは、この属性がリソースに対して必須か、またはオプションかを指定します。このパラメータがリソースで必要となる場合は、パラメータ値を true に設定する必要があります。たとえば、属性 cn は Active Directory で必要となるので、mustOnResource は true に設定します。

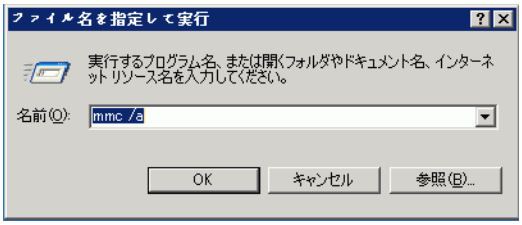
- name="objectclassuserattributeuserAccountControl"

  このパラメータは、タグ <attributeDefinition> に接続するためにスキーマファイル内で一意である必要がある属性名を指定します。このタグは、このスキーマファイル内の同じ属性を記述しています。属性名は、文字列 objectclass、文字列 attributeuser、およびパラメータ concero:tafield の値を連結した形式にすることをお薦めします。

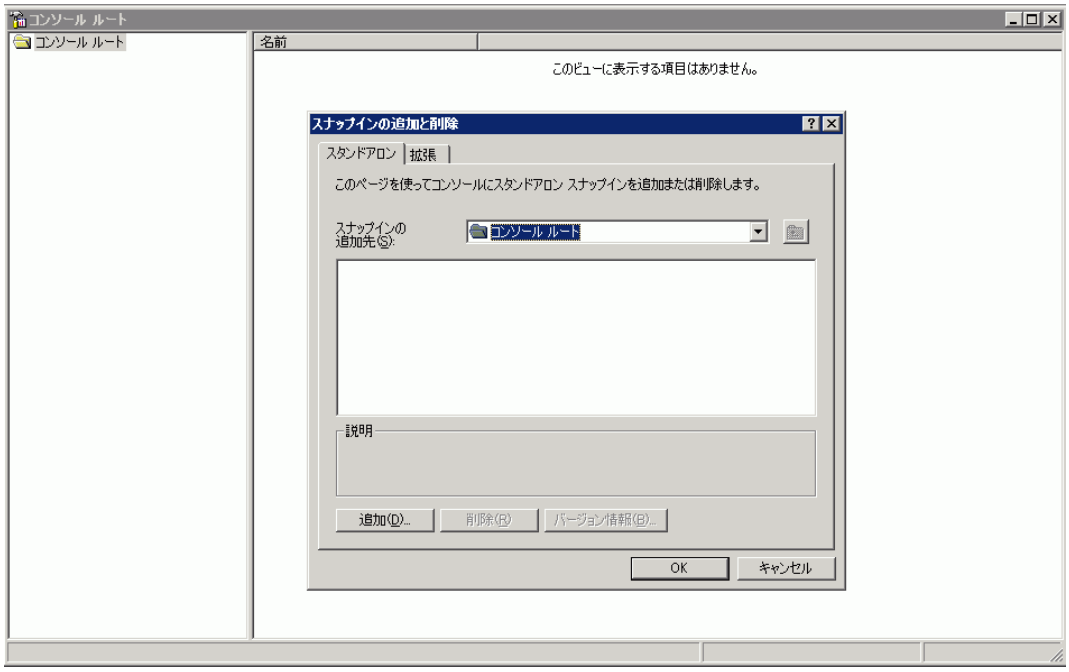
- objectClass="user"

  このパラメータは、属性が属する objectClass を指定します。以下の手順を実行すれば、Active Directory スキーマから objectClass の値を取得できます。

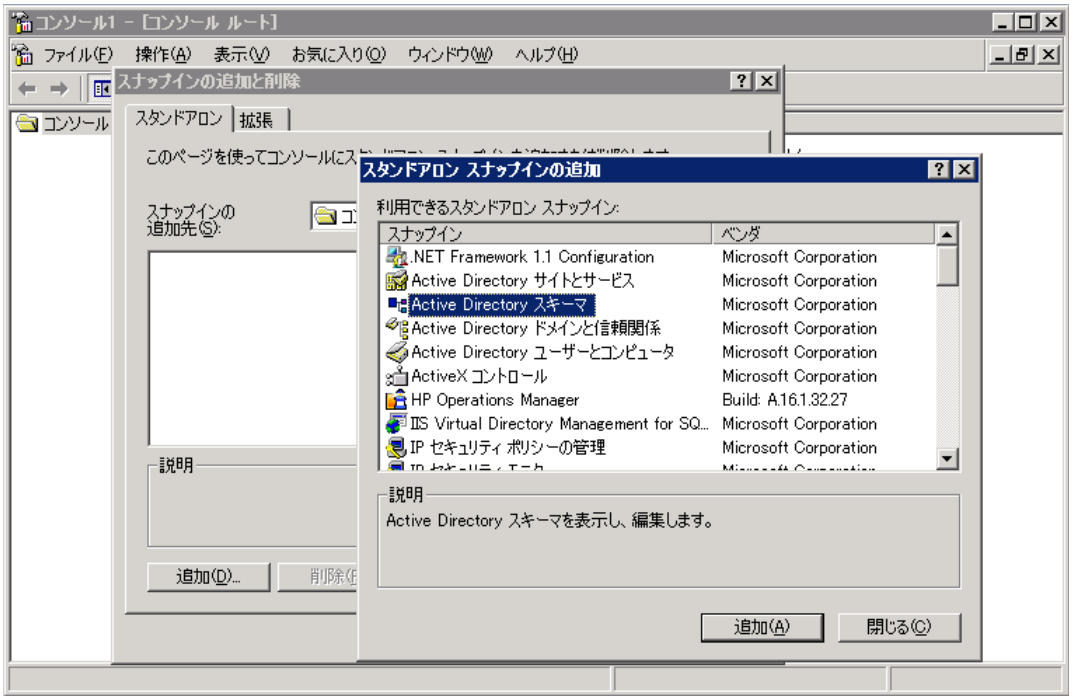
  a Active Directory サーバーで **mmc /a** を実行します。



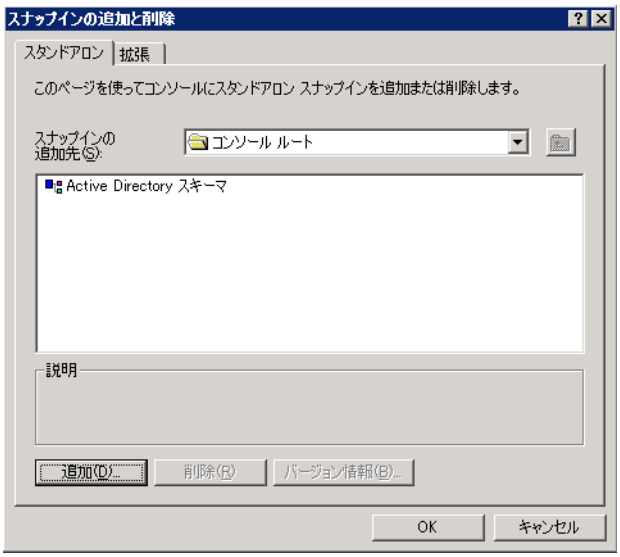
b コンソールウィンドウで、**[ファイル]** → **[スナップインの追加と削除]** の順にクリックします。[スナップインの追加と削除] ウィンドウが表示されます。



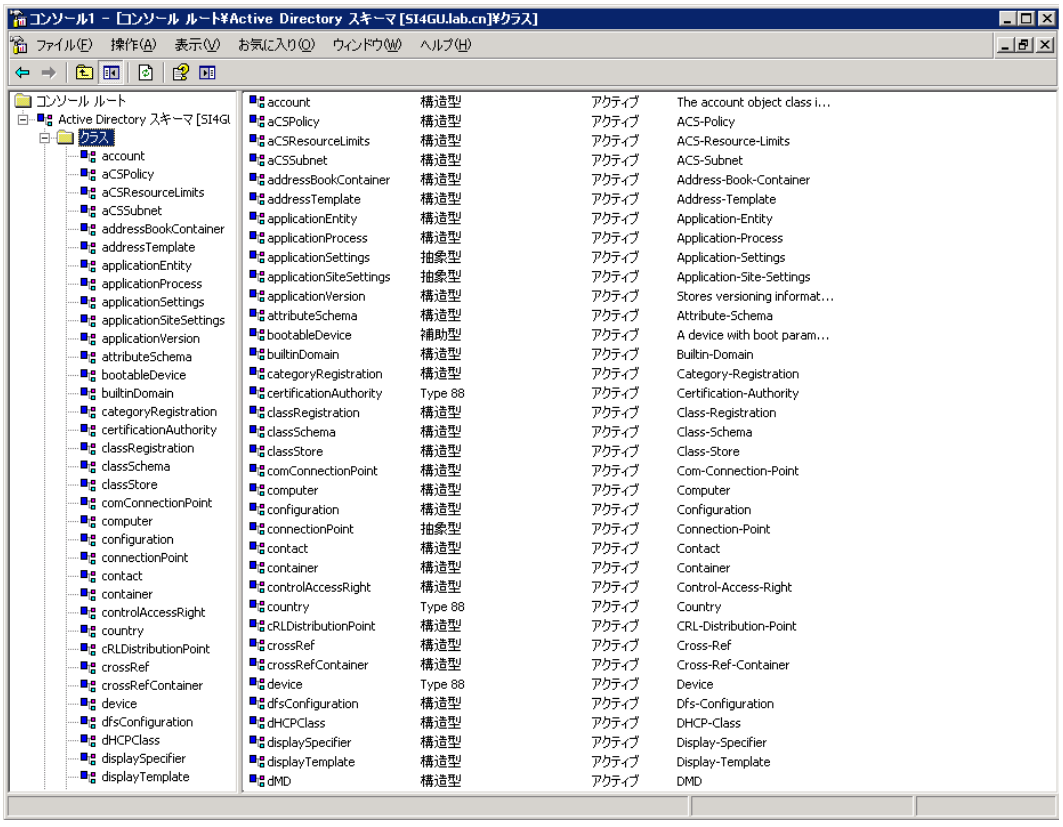
c **[追加]** をクリックします。[スタンドアロンスナップインの追加] ウィンドウが表示されるので、スナップインリストから Active Directory スキーマを選択し、**[追加]** をクリックします。



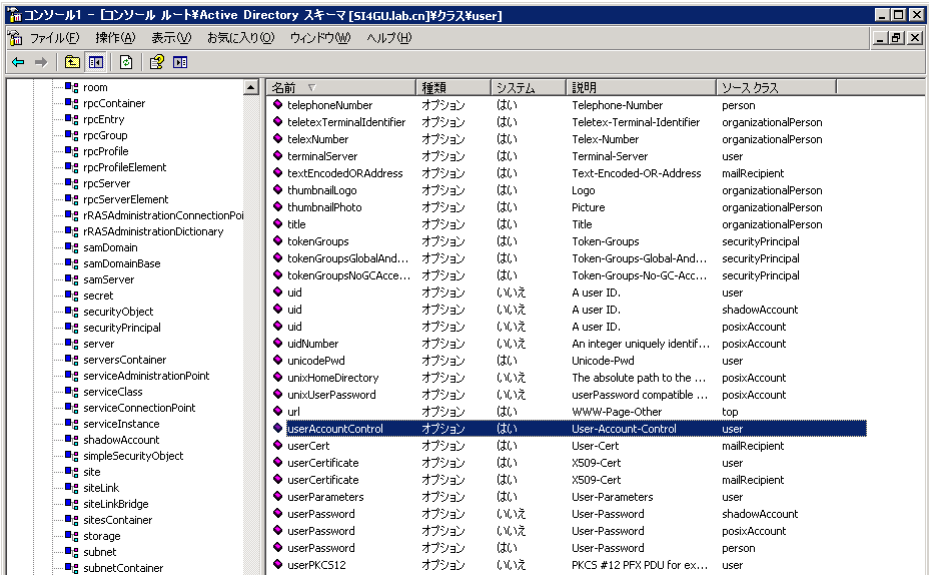
d **[OK]** をクリックします。Active Directory スキーマのスナップインが追加されました。



e 表示された [Active Directory スキーマ] ウィンドウの左側のパネルで、Classes ノードを展開します。



f スクロールダウンして **user** クラスを選択し、次に右側のパネルで userAccountControl を探します。Source Class カラムで属性の objectClass を見つけることができます。たとえば、以下に示すように、userAccountControl の objectClass は“user”です。



- `objectclasstype="structural"`

  このパラメータは、この属性の objectclasstype を指定します。Active Directory では objectclasstype に次の 3 つの値を使用できます。

  — *`Structural`*: ディレクトリのオブジェクト (ユーザー、サーバーなど) をインスタンス化するために使用します。これがデフォルト値です。

  — *`Abstract`*: 構造化クラスを導出するためのテンプレートを提供します。

  — *`Auxiliary`*: `structural` および `abstract` クラスに含まれる属性のあらかじめ定義されたリストを保有します。

- `ordering=""`

  このパラメータは、現在のバージョンではまだ実装されていません。

- `remexpireValue="0"`

  このパラメータは、パスワードの有効期限を削除するかどうかを指定します。属性がゼロの場合は、パスワードの有効期限は削除されます。

- `renameKey="false"`

  このパラメータは、属性値が変更可能かどうかを指定します。

  現在のバージョンでは、属性 cn のみに `true` 値 (`renameKey="true"`) を指定することができます。

- `required="false"`

  このパラメータは、Select Identity で属性をプロビジョニング処理する必要があるかどうかを指定します。このパラメータが Select Identity で必要となる場合は、パラメータ値を `true` に設定する必要があります。たとえば、属性 `sAMAccountName` は Select Identity で必要となるので、`required` を `true` に設定します。

- `resourceKey="false"`

  このパラメータは、属性がリソースのオブジェクトを一意に識別するためのリソースキーであるかどうかを指定します。

スキーマファイル内の 1 つの属性に対してのみ、このパラメータに true 値を指定することができます (resourceKey="true")。

- entityType="user"

  このパラメータは、属性を使用するエンティティを指定します。entityType には次の 3 つの値を使用できます。

  — user: この属性は、user のみが使用できます。

  — contact: この属性は、contact のみが使用できます。

  — user|contact: この属性は、user と contact の両方で使用できます。

- supportedOperations ="UNLINK,LINK,GETATTRIBUTES,GETPARENT,GETCHILDREN,GETALL,RESETPASSWORD,CHANGEPASSWORD,EXPIREPASSWORD,DISABLE,ENABLE,CREATE,DELETE,UPDATE"

  このパラメータは、リソースで属性がサポートする操作を指定します。

  上記のパラメータ値がデフォルト値です。

- transform="NO"

  このパラメータは、属性のタイプを他のタイプに変換可能かどうかを指定します。現在のバージョンではまだ実装されていません。

- type="java.lang.String"

  このパラメータは、リソースの属性タイプを指定します。

以下に、属性のパラメータを記述する <attributeDefinition> タグの例を示します。

```
- <attributeDefinition description="Group_objectclassgroupattributemember"
    name="Group_objectclassgroupattributemember" type="java.lang.String">
   - <properties>
     - <attr name="minLength">
         <value>0</value>
       </attr>
     - <attr name="maxLength">
         <value>255</value>
       </attr>
     - <attr name="defaultValue">
         <value />
       </attr>
     - <attr name="pattern">
       - <value>
           <![CDATA[ [a-zA-Z0-9@]+  ]]>
         </value>
       </attr>
    </properties>
  </attributeDefinition>
```

属性の詳細を、それぞれの説明に従って変更することができます。

- description: 属性の説明です。
- name: 属性の名前です。
- type: 属性のタイプです。

  name と type 値は、タグ <attributeDefinitonReference> のパラメータ name と type と同じ値にしてください。

- minLength: 属性の最小の長さです (デフォルト値はゼロ)。
- maxLength: 属性の最大の長さです (デフォルト値は "255")。
- defaultValue: 属性のデフォルト値です (デフォルト値は空の文字列)。
- pattern: 属性値のフォーマットをチェックするパターンです (デフォルト値は "![CDATA[[a-zA-Z0-9@]+]]")。

既存の属性マッピングの変更

スキーマファイル内の属性を変更するには、スキーマファイルの以下の 2 つのタグを変更してください。

- <attributeDefinitionReference>
- <attributeDefinition>

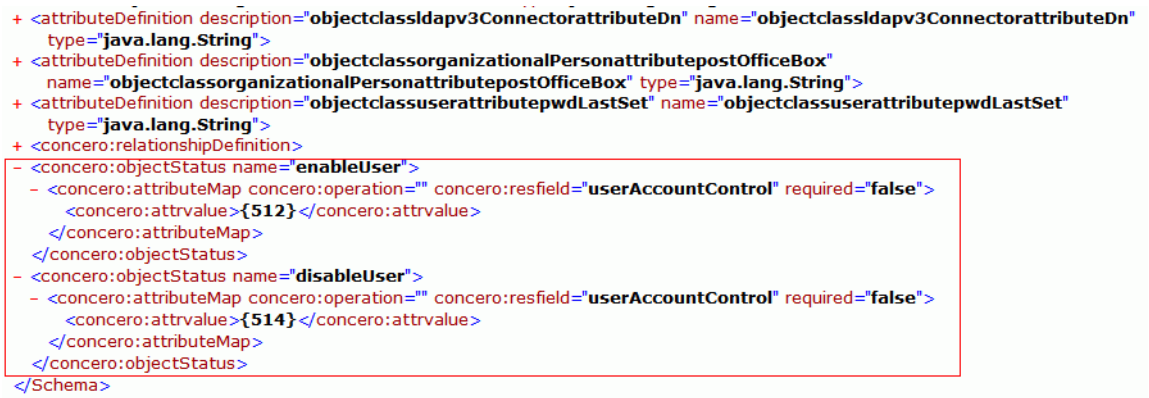
既存の属性マッピングの削除

スキーマファイルから属性を削除するには、スキーマファイルの以下の 2 つのタグを削除してください。

- <attributeDefinitionReference>
- <attributeDefinition>

マッピングの有効化 / 無効化のカスタマイズ

下図で示すように、ActiveDir.xml ファイルのタグ <concero:objectStatus name="enableUser"> とタグ <concero:objectStatus name="disableUser"> は、ユーザーの enable(有効化) および disable(無効化) で使用する属性とその値を定義します。



以下に、属性のパラメータを記述するタグ <concero:objectStatus name="enableUser"> とタグ <concero:objectStatus name="disableUser"> の例を示します。

```
- <concero:objectStatus name="enableUser">
  - <concero:attributeMap concero:operation="" concero:resfield="userAccountControl"
      required="false">
      <concero:attrvalue>{512}</concero:attrvalue>
    </concero:attributeMap>
  </concero:objectStatus>
- <concero:objectStatus name="disableUser">
  - <concero:attributeMap concero:operation="" concero:resfield="userAccountControl"
      required="false">
      <concero:attrvalue>{514}</concero:attrvalue>
    </concero:attributeMap>
  </concero:objectStatus>
```

ユーザーを有効化または無効化するときの操作をカスタマイズしたい場合は、それぞれの説明に従って、属性の名前とその値を変更できます。

- concero:resfield: ユーザーの enable(有効化) および disable(無効化) におけるユーザーのステータスを示すための属性です。現在のバージョンでは、属性 userAccountControl のみがサポートされます。
- required: 属性が Select Identity で必要かどうかを指定します。現在のバージョンでは、required には false が設定されます。
- concero:attvalue: Active Directory において、ユーザーのステータスを示す値です。以下に例を示します。

  ユーザーが有効な場合、属性 userAccountControl の値は 512 です。

  ユーザーが無効な場合、属性 userAccountControl の値は 514 です。

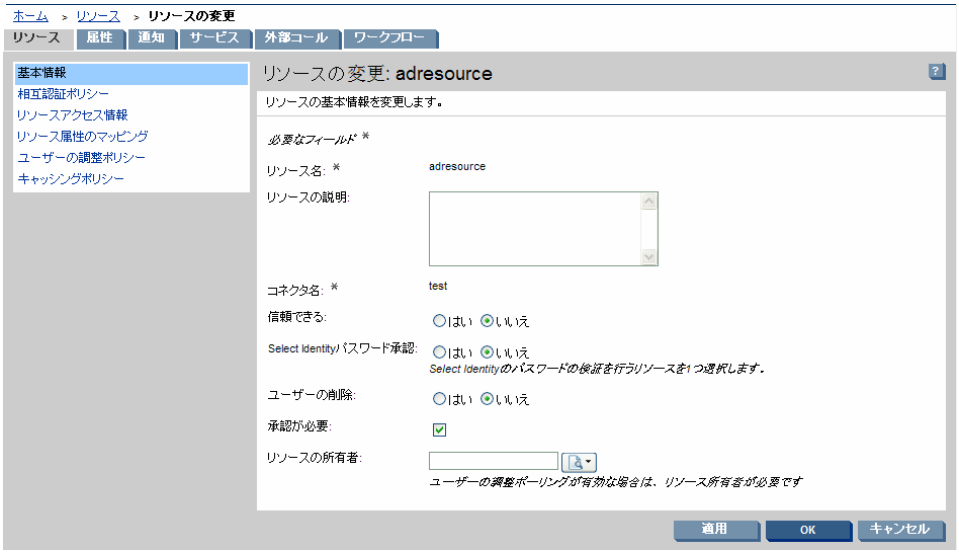
Select Identity における属性の追加 / 削除の確認

以下の手順に従って、Select Identity で属性が追加または削除されたかどうかを確認します。

1 Select Identity の [サービス工房] セクションで、**[リソース]** をクリックします。

[リソース] ウィンドウで、リソースリストからコネクタが使用するリソースを選択します。この例では、ADResource が選択されています。

2 **[変更]** をクリックします。[基本情報] ウィンドウが表示されたときは、**[OK]** をクリックします。



3 再度、リソースを選択して、**[表示]** をクリックします。

[基本情報] ウィンドウが表示されたら、左側のパネルで **[リソース属性のマッピング]** をクリックします。

右側のウィンドウで、属性がすでに追加 / 削除されたかどうかを確認します。この例では、属性 `userAccountControl` が追加されています。

Exchange 2007 用の新しい属性の追加

Exchange 2007 Server 用の属性を `ActiveDir.xml` ファイルに追加する場合、以下の手順を実行します。

1 スキーマファイルの **`User`** セクションに新しい属性を追加します。

スキーマファイルの変更方法の詳細については、新しい属性マッピングの追加 95 ページを参照してください。

2 新しい属性を追加した後、新しい属性に category="Exchange2007" を追加して、Exchange 2007 で必須であることを示します。以下に例を示します。

```
<attributeDefinitionReference
      attrFunction="provision|post|pre"
      attributeType="Read/write" concero:isKey="false"
      concero:resfield="homeMDB" concero:tafield="homeMDB"
      defaultValue="" encrypt="false" encrypted="false"
      encryptionAlgorithm="" expirePassword="false"
      expireValue="" isPassword="false" linktoentity=""
      multivalued="false" mustOnResource="false"
      name="User_objectclassmsExchMailStorageattributehomeMDB"
      objectclass="msExchMailStorage"
      objectclasstype="auxiliary" ordering=""
      remexpireValue="" renamekey="false" required="false"
      resourcekey="false"
            entityType="user|contact"
            category="Exchange2007"
supportedOperations="UNLINK,LINK,GETATTRIBUTES,GETPARENT,GETCHILDREN,GETA
LL,RESETPASSWORD,CHANGEPASSWORD,EXPIREPASSWORD,DISABLE,ENABLE,CREATE,DELE
TE,UPDATE"
      transform="NO" type="java.lang.String"/>
```

3 ActiveDir.xml ファイルの変更が終わり、Select Identity の属性マッピングを更新すると、Exchange 2007 Server 用の新フィールドが Select Identity ユーザー作成ページに表示されます。新しいフィールドに必ず値を入力します。