Sun Java™ System

Identity Synchronization for Windows 1 インストールおよび設定ガイド

2004Q3

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 817-7846

目 次

図目次

表目次

はじめに

Sun Java™ System Identity Synchronization for Windows 1 2004Q3 (従来の Sun™ ONE Identity Synchronization for Windows) を使用することで、Sun Java™ System Directory Server とその他のシステムの間でパスワード、および指定されているその他のユーザー属性をやり取りすることができます。

このマニュアルでは、Sun Java System Identity Synchronization for Windows を運用環境で使用できるようにインストールおよび設定する方法について説明します。

Identity Synchronization for Windows リリースの新機能および拡張機能の最新情報については、次のオンラインリリースノートを参照してください。

`http://docs.sun.com/db/doc`

注	このマニュアルに示されるユーザーインタフェースは、製品の今後のバージョンで変更される可能性があります。

ここでは、次の項目について説明します。

対象読者

この『インストールおよび設定ガイド』は、Sun Java™ System Directory Server と Windows Active Directory または NT マシンの間でパスワードとユーザー属性を双方向に同期させることを目的として、Identity Synchronization for Windows をインストールおよび設定する管理者、システムエンジニア、サービスエンジニアを対象としています。

次の事項に習熟している必要があります。

- Directory Server と Windows Active Directory/NT の設定と操作
- Lightweight Directory Access Protocol (LDAP)
- Java テクノロジ
- Extensible Markup Language (XML)
- 公開鍵暗号方式と SSL (Secure Sockets Layer) プロトコルの基本概念
- イントラネット、エクストラネット、インターネットのセキュリティの基本概念、および企業での電子証明書の役割

本書をお読みになる前に

『Sun Java System Identity Synchronization for Windows 1 2004Q3 リリースノート』には、このマニュアルに記載されている説明に優先する情報を含め、製品に関する最新の情報が記載されています。このマニュアルで説明する手順を実行する前に、『リリースノート』をお読みください。

Identity Synchronization for Windows の配備では、データストアとして Sun Java System Directory Server が使用されるため、この製品のマニュアルにも目を通しておく必要があります。Directory Server のマニュアルは、http://docs.sun.com/db/prod/entsys?l=ja で入手できます。

このマニュアルの構成

『Sun Java System Identity Synchronization for Windows 1 2004Q3 インストールおよび設定ガイド』は、次の章から構成されます。

- 第 1 章「製品について」: 製品の機能、システムコンポーネント、コマンド行ユーティリティ、システムコンポーネントの分散、配備例など、Identity Synchronization for Windows の基本概念について説明します。
- 第 2 章「インストールの準備」: インストールと設定のプロセスについて説明し、製品のインストールを準備する上で有用なその他の情報を提供します。
- 第 3 章「コアのインストール」: Identity Synchronization for Windows のインストールプログラムの使用方法と、Identity Synchronization for Windows コアコンポーネントのインストール方法について説明します。
- 第 4 章「コアリソースの設定」: コンソールを使用してコアを追加し、それを設定する方法について説明します。
- 第 5 章「コネクタと Directory Server プラグインのインストール」: Identity Synchronization for Windows コネクタと Directory Server プラグインをインストールする方法について説明します。
- 第 6 章「既存ユーザーの同期」: Identity Synchronization for Windows の新しいインストールで既存のユーザーにリンクを設定し、同期させる方法について説明します。
- 第 7 章「Identity Synchronization for Windows 1 2004Q3 への移行」: システムを Sun Java System Identity Synchronization for Windows バージョン 1.0 からバージョン 1 2004Q3 に移行する方法について説明します。
- 第 8 章「ソフトウェアの削除」: アンインストールの準備やコンソールの手動アンインストールなど、Identity Synchronization for Windows を削除する方法について説明します。
- 第 9 章「トラブルシューティング」: Identity Synchronization for Windows のインストールに関するトラブルシューティング情報を提供します。
- 第 10 章「監査とエラーのログファイルについて」: ログレベルの設定、ログファイルの表示と解釈、ディレクトリソースの状態など、監査とエラーのログ記録について説明します。
- 第 11 章「セキュリティの設定」: セキュリティ保護されたシステムの設定方法について説明します。セキュリティの強化、レプリケートされた構成の保護、SSL の有効化、証明書データベースへの Active Directory CA 証明書の追加などに関する情報を提供します。
- 付録 A「Identity Synchronization for Windows のコマンド行ユーティリティの使用」: Identity Synchronization for Windows のコマンド行ユーティリティを使用して各種タスクを実行する方法について説明します。

- 付録 B「LinkUsers XML ドキュメントのサンプル」: 環境のカスタマイズに利用できる LinkUsers XML ドキュメント (`linkusers-simple.cfg`) のサンプルを紹介します。
- 付録 C「Solaris でのルート以外のユーザーによるサービスの実行」: ルート以外のユーザーとして Identity Synchronization for Windows サービスを実行する方法について説明します。
- 付録 D「同期ユーザーリストの定義と設定」: 同期ユーザーリストの定義と複数ドメインの設定に関する情報を提供します。
- 付録 E「レプリケーション環境でのインストールに関する注意」: マルチマスターレプリケーション (MMR) の配備を設定およびセキュリティ保護する手順について簡単に説明します。

表記上の規則

この節では、このマニュアルに適用される表記規則を表形式で示します。説明する内容は、次とおりです。

- 20 ページの「フォントの表記規則」
- 21 ページの「記号」
- 21 ページの「ニーモニック」
- 22 ページの「デフォルトのパスとファイル名」

フォントの表記規則

次の表は、このマニュアルに適用されるフォントの表記規則を示しています。

表 1 フォントの表記規則

表記	意味	例
`AaBbCc123` (モノスペース)	API および言語の要素、HTML タグ、Web サイトの URL、コマンド名、ファイル名、ディレクトリパス名、画面出力の表示、サンプルコード	`.login` ファイルを編集します。 すべてのファイルをリストするときは、`ls -a` を使用します。 `% You have mail.`
`AaBbCc123` (太字のモノスペース)	画面出力の表示に対し、実際に入力する内容	`% su` `Password:`

表 1　フォントの表記規則 (続き)

表記	意味	例
AaBbCc123 (イタリック)	実際の名前や値に置き換えられる、コマンドまたはパス内のプレイスホルダ	ファイルは、*install-dir*/bin ディレクトリに格納されています。

記号

次の表は、このマニュアルで使用される記号の表記規約を示しています。

表 2　記号の表記規則

記号	説明	例	意味
[ ]	省略できるコマンドオプションを含む	ls [-l]	-l は必須オプションではない
{ | }	必須コマンドオプションの選択肢を含む	-d {y|n}	-d オプションを使用するときは、引数として y または n を指定する必要がある
-	同時に押す複数のキーの組み合わせを示す	Control-A	Control キーと A キーを同時に押す
+	連続して押す複数のキーの組み合わせを示す	Ctrl+A+N	Control キーを押してから以後のキーを押す
>	グラフィカルユーザーインタフェースで選択するメニュー項目を示す	「ファイル」>「新規」>「テンプレート」	「ファイル」メニューから「新規」を選択する。次に「新規」サブメニューから「テンプレート」を選択する

ニーモニック

Identity Synchronization for Windows のユーザーインタフェース全体でニーモニック (下線が引かれた文字) を使用できます。ニーモニックを使用することで、特定のタスクを迅速に実行できます。下線が引かれた文字を入力するだけでタスクが実行されます。ニーモニックでは、大文字と小文字は区別されません。使用するときは、同時に Alt キーを押します。

デフォルトのパスとファイル名

次の表は、このマニュアルに適用されるデフォルトのパスとファイル名の表記を示しています。

表 3　デフォルトのパスとファイル名

表記	説明
<*serverroot*>	Identity Synchronization for Windows のインストール先の親ディレクトリを示す
`isw-`<*hostname*>	Identity Synchronization for Windows のインスタンスのディレクトリを示す
<*current-working-directory*>`/cert8.db`	クライアントの証明書データベースのデフォルトのパスとファイル名を示す
<*installation_root*>`/isw-`<*machine_name*>`/logs/central/`	Identity Synchronization for Windows のセントラルログのデフォルトパスを示す
<*installation_root*>`/isw-`<*machine_name*>`/logs/`	Identity Synchronization for Windows のローカルログ (システムマネージャ、各コネクタ、セントラルロガーのログ) のデフォルトパスを示す
`/usr/sfw/bin`	Solaris 環境では、certutil はデフォルトでこのディレクトリにインストールされる

関連マニュアル

Web サイト http://docs.sun.com で Sun のオンライン技術マニュアルにアクセスできます。アーカイブを参照するか、個々の書名または件名を検索できます。

このドキュメントセットを構成するマニュアル

次の表は、Identity Synchronization for Windows のドキュメントセットを構成するマニュアルを示しています。

表 4 このドキュメントセットに含まれるマニュアル

マニュアルのタイトル	説明
『Sun Java System Identity Synchronization for Windows 1 2004Q3 インストールおよび設定ガイド』 (http://docs.sun.com/doc/817-7846)	Identity Synchronization for Windows を運用環境で使用できるようにインストールおよび設定する方法について説明する
『Sun Java System Identity Synchronization for Windows 1 2004Q3 Deployment Planning Guide』 (http://docs.sun.com/doc/817-6200)	Identity Synchronization for Windows の配備計画に関する一般的なガイドラインと実践例を示す
『Sun Java System Identity Synchronization for Windows 1 2004Q3 リリースノート』 (http://docs.sun.com/doc/817-7853)	製品のリリース後に公開される。現行リリースの新機能に関する説明、既知の問題点と制約、インストール時の注意事項、ソフトウェアまたはマニュアルに関する問題点の報告方法など、最新の情報が記載されている

その他のドキュメント

Directory Server と Sun Java™ System Message Queue を使用することになるので、それぞれの製品のマニュアルの参照が必要になるかもしれません。これらのマニュアルは、次の場所で入手できます。

- Sun Java System Directory Server のマニュアル
  http://docs.sun.com/db/prod/entsys?l=ja
- Sun Java SystemMessage Queue のマニュアル
  http://docs.sun.com/db/prod/entsys?l=ja

公開鍵暗号方式の基本概念、SSL (Secure Sockets Layer) プロトコルの基本概念、イントラネット、エクストラネット、およびインターネットのセキュリティの基本概念、企業での電子証明書の役割の基本概念については、『Managing Servers with iPlanet Console 5.0』でセキュリティ関連の付録を参照してください。

Windows 2003 サーバーおよび Windows パスワードポリシーについては、次に示す Microsoft のドキュメントを参照してください。

- 「Using Secedit.exe to Force Group Policy to Be Applied Again」Microsoft の知識ベース記事 227448
- 「グループポリシー更新ユーティリティの説明」Microsoft の知識ベース記事 298444
- Microsoft の知識ベースの記事 232690

Sun のオンラインリソースへのアクセス

製品のダウンロード、専門家によるサービス、パッチとサポート、開発者向けの追加情報は、次の場所で得られます。

- 開発者向けの情報
  http://developers.sun.com/prodtech/index.html
- ダウンロードセンター
  http://wwws.sun.com/software/download/
- 製品のデータシート
  http://www.sun.com/software/
- 製品のオンラインマニュアル
  http://docs.sun.com
- 製品のサポートと状態
  http://www.sun.com/service/support/software/
- プロフェッショナルサービス
  http://www.sun.com/service/sunps/sunone/index.html
- Sun Enterprise Services、Solaris 用パッチ、サポート
  http://sunsolve.sun.com
- サポートとトレーニング
  http://www.sun.com/supportraining/

Sun テクニカルサポートへの連絡

この製品のマニュアルを参照しても製品に関する技術的な疑問が解決しない場合は、次の場所にアクセスしてください。

http://www.sun.com/service/contacting

関連するサードパーティの Web サイト

このマニュアルでは、次のサードパーティの Web サイトが紹介されています。

- Windows 2003 のパスワードポリシーに関する情報 :

  http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dsscc_aut_xbby.asp

- Windows 2003 でのパスワードポリシーとグループポリシーの適用と変更に関する情報 :

  http://www.microsoft.com/resources/documentation/windowsserv/2003/standard/proddocs/en-us/password_grouppolicy.asp

- Microsoft Certificate Services Enterprise Root 認証局に関する情報 :

  http://support.microsoft.com/default.aspx?scid=kb;en-us;q247078

- SSL を介した LDAP の設定に関する情報 :

  http://support.microsoft.com/default.aspx?scid=kb;en-us;321051

Sun は、このマニュアルに記載されているサードパーティ Web サイトの利用可能性について責任を負いません。Sun は、このようなサイトまたはリソースで得られるあらゆる内容、広告、製品、およびその他素材を保証するものではなく、責任または義務を負いません。Sun は、このようなサイトまたはリソースで得られるあらゆるコンテンツ、製品、またはサービスによって生じる、または使用に関連して生じる、または信頼することによって生じる、または生じたと主張される、いかなる損害または損失についても責任または義務を負いません。

コメントをお待ちしております

Sun はマニュアル類の改善に努めるため、お客様からのコメントやご意見をお待ちしております。

コメントをお寄せいただく場合は、http://docs.sun.com/db/prod/entsys?l=ja にアクセスし、「コメントの送信」をクリックしてください。オンラインフォームには、マニュアルのタイトルとパート番号を記載してください。パート番号は、マニュアルのタイトルページまたは最上部に記載されている 7 桁または 9 桁の番号です。

たとえば、このマニュアルのタイトルは『Sun Java System Identity Synchronization for Windows 1 2004Q3 インストールおよび設定ガイド』で、パート番号は 817-7846 です。

第 1 部

インストールと設定

第 1 章

製品について

Identity Synchronization for Windows を使用することで、Sun Java™ System Directory Server 5 2005Q1 と次の製品の間で、パスワードとユーザー属性を双方向で同期させることができます。

- Windows 2000 または Windows 2003 Server Active Directory
- Windows NT SAM レジストリ

Identity Synchronization for Windows は同期イベントを処理します。

- **セキュリティ** : Identity Synchronization for Windows は、いかなる場合もパスワードを「クリアテキスト」形式で送信しない。また、システムへのアクセスは管理者に限定される
- **信頼性** : Identity Synchronization for Windows は、個々のコンポーネントが一時的に使用不可能な状態になっても、ディレクトリの同期を維持する
- **効率** : Identity Synchronization for Windows の同期メソッドがディレクトリサーバーに与える負荷はごく小規模である

Sun Java System Identity Synchronization for Windows バージョン 1 2004Q3 をインストールする、または同製品に移行する前に、この章で説明する概念について理解する必要があります。この章で説明する内容は次のとおりです。

製品の機能

Identity Synchronization for Windows が提供する機能は次のとおりです。

- **パスワードの双方向同期** : Sun Java System ディレクトリソースと、Windows Active Directory および Windows NT ディレクトリソースの間でユーザーパスワードを同期させることができる

  パスワードを同期させることで、ユーザーはログイン認証にこれらのディレクトリソースを使用してアプリケーションにアクセスできるため、複数のパスワードを覚える必要がなく、1 つのパスワードだけを使用できる。また、パスワードの定期的な更新が必要な場合でも、パスワードの更新を一方の環境だけで完了できる

- **ユーザー属性の双方向同期** : 1 つのディレクトリ環境で選択した属性を作成、修正、削除し、その値を自動的に他のディレクトリ環境に伝達することができる
- **ユーザーアカウント作成の双方向同期** : 1 つのディレクトリ環境でユーザーアカウントを作成または削除し、それを自動的に他のディレクトリ環境に伝達することができる
- **双方向のオブジェクト削除、有効化、無効化** : Directory Server と Active Directory ディレクトリソースの間で、オブジェクトの削除、有効化、無効化の流れを制御できる (Windows NT では利用できない)
- **複数ドメインとの同期** : Active Directory と Windows NT の複数のドメイン、および Active Directory フォレストと同期させることができる
- **一元的なシステム監査** : インストールと設定の状態、日常のシステム動作、配備に関連するエラー状態を一元的に監視することができる

Windows ディレクトリ内のエントリを修正したり、ディレクトリを使用するアプリケーションを変更したりする必要はありません。

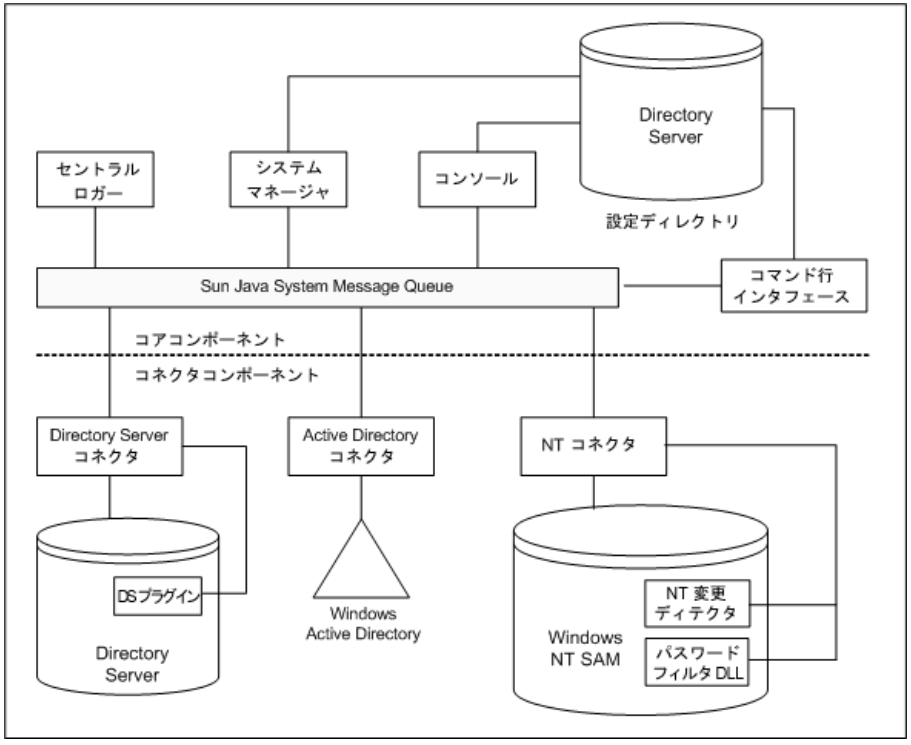
Identity Synchronization for Windows を使用して Directory Server と Active Directory を同期させる場合、Windows 環境に追加コンポーネントをインストールする必要はありません。

Directory Server と Windows NT を同期させる場合は、製品の NT コンポーネントを Windows NT 環境にインストールする必要があります。

システムコンポーネント

Identity Synchronization for Windows は、コアコンポーネントのセット、任意の組み合わせのコネクタ、およびコネクタサブコンポーネントから構成されます (図 1-1 を参照)。コネクタサブコンポーネントは、Sun Java System Directory Server と Windows ディレクトリの間でパスワードとユーザー属性の更新を同期させる場合に必要とされます。

図 1-1　システムコンポーネント



ここでは、Identity Synchronization for Windows の各コンポーネントとその構成を定義し、それぞれについて説明します。

- 32 ページの「Watchdog プロセス」
- 32 ページの「コア」
- 35 ページの「コネクタ」
- 36 ページの「コネクタサブコンポーネント」

Watchdog プロセス

Watchdog は個々のバックグラウンド Java プロセスの起動、再起動、停止を担当する Identity Synchronization for Windows Java プロセスです。Watchdog は、セントラルロガー、システムマネージャ、コネクタを起動し、それを監視します。ただし、サブコンポーネント、Message Queue、Identity Synchronization for Windows コンソールの監視は行いません。

Watchdog は、コアをインストールするすべてのマシンにインストールされ、Solaris デーモンまたは Windows サービスとして実行できます。サービスの起動と停止については、184 ページの「サービスの開始と停止」を参照してください。

コア

Identity Synchronization for Windows のインストールでは、最初にコアコンポーネントをインストールし、次に環境に合わせてそれを設定します。

コアは次のコンポーネントから構成されます。各コンポーネントは独立した Java プロセスです。各コンポーネントについて、次の各ページで説明します。

- 32 ページの「設定ディレクトリ」
- 33 ページの「コンソール」
- 33 ページの「コマンド行ユーティリティ」
- 34 ページの「システムマネージャ」
- 34 ページの「セントラルロガー」

注 Watchdog はコアのインストール先にインストールされ、セントラルロガーとシステムマネージャの起動、監視を行います。

詳細は、32 ページの「Watchdog プロセス」を参照してください。

設定ディレクトリ

Identity Synchronization for Windows は、設定データを Directory Server 設定ディレクトリに格納します。設定ディレクトリは、プログラムによってインストールされません。

コンソール、システムマネージャ、コマンド行ユーティリティ、インストーラは、いずれも設定ディレクトリに対して製品の次のような設定データの書き込みと読み込みを行います。

- 各コンポーネントの状態に関するインストール情報

- すべてのディレクトリ、ドメイン、コネクタ、Directory Server プラグインの設定情報
- コネクタの状態
- ユーザー作成、ユーザー削除、属性修正の方向を示す同期設定
- 同期の対象となる属性、および 2 つのディレクトリ環境 (Active Directory と Directory Server、または Windows NT と Directory Server) の間の属性マッピング
- 各ディレクトリトポロジの同期ユーザーリスト
- ログ設定

コンソール

Identity Synchronization for Windows には、製品コンポーネントのすべての設定タスクと管理タスクを集中的に行えるコンソールが用意されています。

コンソールには次の機能があります。

- 同期の対象となるディレクトリソースを設定する
- パスワード以外に同期させるユーザーエントリ属性のマッピングを定義する
- ディレクトリまたはドメイントポロジ内のどのユーザーおよび属性を同期させるか (または同期させないか) を指定する
- システムの状態を監視する
- 同期を開始および終了する

コマンド行ユーティリティ

Identity Synchronization for Windows には、次のタスクをコマンド行から直接実行するためのコマンド行ユーティリティも用意されています。

- 設定と SSL 設定に基づく証明書情報を表示する
- Identity Synchronization for Windows の設定パスワードを変更する
- エクスポートされた Identity Synchronization for Windows バージョン 1.0 の設定 XML ドキュメントをインポートする
- Identity Synchronization for Windows が使用できるように Sun Java System Directory Server ソースを準備する
- インストールと設定のプロセスを完了させるための手順と、インストールされているコネクタ、システムマネージャ、Message Queue の状態を確認するための手順を表示する
- 設定ディレクトリ内のコネクタの状態をアンインストール済みにリセットする

- 2 つのディレクトリ内の既存ユーザーを同期させてリンクを設定し、インストールプロセスの一部としてディレクトリを事前に取り込む
- 同期を開始する
- 同期を終了する

製品のコマンド行ユーティリティの詳細な説明と使用方法については、付録 A「Identity Synchronization for Windows のコマンド行ユーティリティの使用」を参照してください。

システムマネージャ

Identity Synchronization for Windows のシステムマネージャは独立した Java プロセスで、次の機能を持ちます。

- 製品のバックエンドでネットワーク化された機能を使用して、設定の更新を動的にコネクタに伝達する
- 各コネクタと、すべてのコネクタサブコンポーネントの状態を維持する
- 2 つのディレクトリの初期同期に使用される `idsync resync` の動作を調整する

セントラルロガー

コネクタは、地理的に離れた複数の場所にまたがってインストールできます。このため、すべてのログ情報を集約することは、管理上の大きな利点となります。これにより管理者は、同期アクティビティの監視、エラーの検出、システム全体の状態の評価を 1 つの場所で行うことができます。

管理者は、セントラルロガーを使用して次の管理を行えます。

- システムが正常に稼動していることを確認する
- 個々のコンポーネントおよびシステム全体の問題を検出し、それを解決する
- 個々の同期アクティビティおよびシステム全体の同期アクティビティを監査する
- ディレクトリ環境間でのユーザーパスワードの同期を追跡する

ログには、次の 2 種類があります。

- **監査ログ**は、システムの毎日の動作に関する情報を提供する。これには、ディレクトリ間でのユーザーパスワードの同期などの重要なイベントも含まれる。監査ログに記録される情報のレベルは、ログメッセージの詳細度を上下することで制御できる

注	その他のイベントとの相関関係を容易に確認できるように、Identity Synchronization for Windows はすべてのエラーログメッセージを監査ログにも記録します。

- **エラーログ**は、重大なエラーおよび警告として評価される状況に関する情報を提供する。エラーログのすべてのエントリは重要度が高いため、エラーをログに記録しないように設定することはできない。エラー状態が発生すると、それは常にエラーログに記録される

コネクタ

コネクタは、1 つのデータソースタイプで同期プロセスを管理する Java プロセスです。コネクタはユーザーによる変更をデータソースから検出し、Message Queue 経由でその変更をリモートコネクタに伝達します。

Identity Synchronization for Windows には、ディレクトリの種類別に次のコネクタがあります。これらのコネクタは、ディレクトリ間およびドメイン間でユーザー属性とパスワードの更新を双方向に同期させます。

- Directory Server **コネクタ** : Directory Server 内の単一ルートサフィックス (たとえば サフィックス / データベースなど) をサポートする
- Active Directory **コネクタ** : Windows 2000 または Windows 2003 Server Active Directory 環境内の単一インスタンスをサポートする。追加ドメイン用に複数のコネクタを使用することができる
- Windows NT **コネクタ** : Windows NT 環境内の単一ドメインをサポートする

注	コネクタのインストール先には Watchdog がインストールされ、コネクタの起動、再起動、停止を行います。詳細については、32 ページの「Watchdog プロセス」を参照してください。

コネクタサブコンポーネント

サブコンポーネントは、コネクタから独立して実行される軽量のプロセスまたはライブラリです。コネクタは、Directory Server または Windows NT 内のパスワードの取り込みのように、リモートアクセスできないネイティブリソースへのアクセスにサブコンポーネントを使用します。

同期対象のディレクトリには次のコネクタサブコンポーネントがインストールされ、暗号化された接続を通じて対応するコネクタと通信します。

- 36 ページの「Directory Server プラグイン」
- 36 ページの「Windows NT コネクタサブコンポーネント」

注	Active Directory コネクタにはサブコンポーネントは必要ありません。

Directory Server プラグイン

Directory Server プラグインは、Directory Server コネクタのサブコンポーネントです。Directory Server プラグインは、同期対象となるそれぞれの Directory Server にインストールされます。

このプラグインの機能は次のとおりです。

- 暗号化されたパスワードを旧バージョン形式の更新履歴ログ (Retro Changelog) に格納することで、Directory Server コネクタの変更検出機能を強化する
- Active Directory と Directory Server の間での、ユーザー属性とパスワードの同期を双方向にサポートする (44 ページの「オンデマンドパスワード同期によるクリアテキスト形式パスワードの取得」を参照)

注	Directory Server プラグインは、4 方向のマルチマスターレプリケーション (MMR) 環境でも機能します。従来の Identity Synchronization for Windows では 2 方向の MMR だけがサポートされていました。

Windows NT コネクタサブコンポーネント

Windows NT SAM Registry との同期が必要なインストールでは、Identity Synchronization for Windows のインストールプログラムによって Windows NT コネクタ以外に次の主ドメインコントローラ (PCD) がインストールされます。

- **変更ディテクタ** : セキュリティログを監視することでユーザーエントリとパスワードの変更イベントを検出し、変更をコネクタに伝達する
- **パスワードフィルタ** : NT ドメインコントローラで加えられたパスワードの変更を検出し、それを安全に NT コネクタに伝達する

Message Queue

Identity Synchronization for Windows は、ディレクトリソース間での属性とパスワードの変更の伝達、およびディレクトリソースの同期を管理するコネクタへの管理情報と設定情報の伝達に、Message Queue を使用します。Message Queue は、パブリッシュ / サブスクライブのモデルを持つ持続的メッセージキューメカニズムです。

Message Queue は、オープンな標準規格である JMS (Java Message Service) を実装する企業向けのメッセージングシステムです。JMS 仕様は、Java アプリケーションが分散環境でメッセージの作成、送受信、および読み取りを行う共通の方法を提供するためのプログラミングインタフェースを規定しています。

Message Queue は、共通のメッセージサービスを使用してメッセージを交換する、メッセージパブリッシャとサブスクライバから構成されます。このメッセージサービスは、1 つまたは複数の専用メッセージブローカから構成され、これらのブローカは Message Queue に対するアクセスの制御、アクティブなパブリッシャとサブスクライバに関する情報の維持、メッセージ配信の確認を行います。

Message Queue を利用した伝達には次のような利点があります。

- コネクタ間に信頼のシステムを確立する
- すべてのコンポーネントのセキュリティアクセス制御を簡略化する
- パスワードが最初から最後まで暗号化されている
- すべてのパスワード更新メッセージを確実に配信できる
- コネクタ間通信の複雑さとセキュリティリスクを軽減する
- 一元的な権限で設定情報を各所に伝達できる
- すべてのコネクタのログを一元的に集約できる

システムコンポーネントの分散

効率的な配備を開発するには、Identity Synchronization for Windows のコンポーネントがどのように組織化され、製品がどのように機能するかについて事前に理解する必要があります。ここで説明する内容は次のとおりです。

この項および配備例 (48 ページ) で説明する基本概念を理解することで、Active Directory 環境と Windows NT 環境の混合環境や複数サーバー環境のように、より複雑で洗練された配備に必要な戦略を策定するための情報を推測できるようになります。

コア

まず、サポートされるオペレーティングシステムのディレクトリサーバーに、すべてのコアコンポーネントを一度だけインストールします。管理サーバーは、コアと同じマシンに存在します。コアをインストールするには、事前に Message Queue 3.5 SP1 Enterprise Edition をインストールしておく必要があります。

Directory Server コネクタとプラグイン

Directory Server コネクタは、サポートされている任意のオペレーティングシステム (54 ページの「オペレーティングシステムの要件」を参照) にインストールできます。Directory Server コネクタは、同期対象の Directory Server が稼動しているマシンにインストールする必要はありません。ただし、設定されている Directory Server ソースごとに 1 つの Directory Server コネクタをインストールする必要があります。

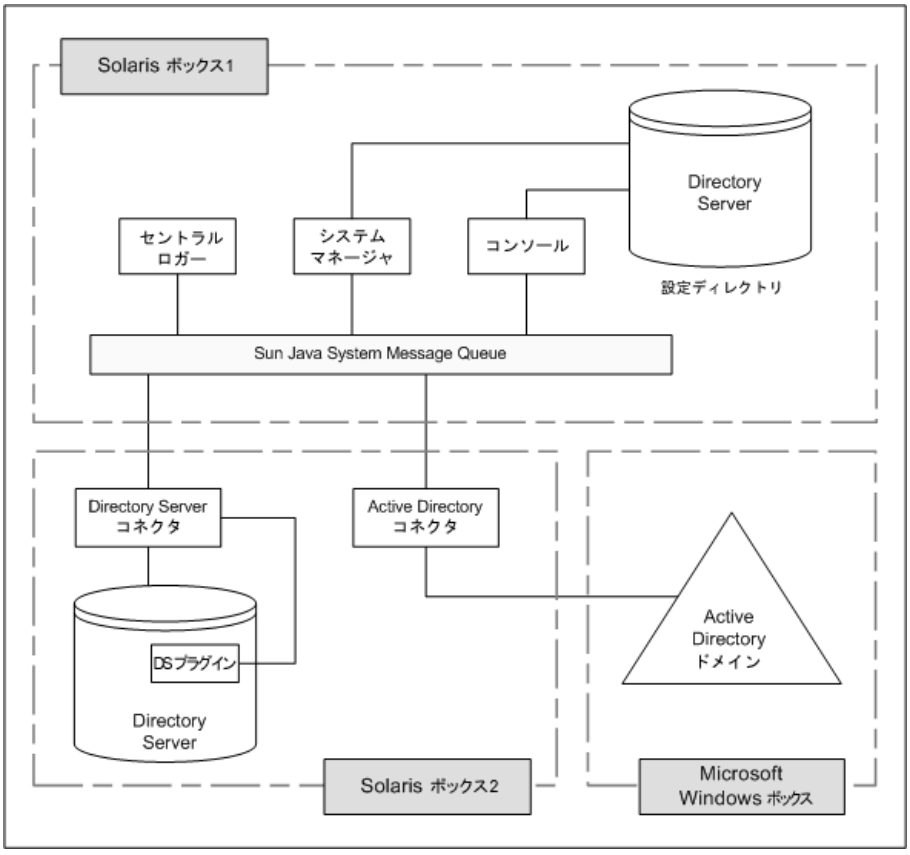
Directory Server プラグインは、同期対象となる Directory Server がインストールされているすべてのホストにインストールする必要があります。

注 Directory Server コネクタは、Directory Server ソースごとに 1 つずつインストールされます。一方、Directory Server プラグインは、同期対象となるマスター、ハブ、およびコンシューマレプリカごとにインストールする必要があります。

Active Directory コネクタ

Active Directory コネクタは、サポートされている任意のオペレーティングシステムにインストールできます (図 1-2 を参照)。Windows 環境に Active Directory コネクタをインストールする必要はありませんが、Active Directory ドメインごとに 1 つの Active Directory コネクタをインストールする必要があります。

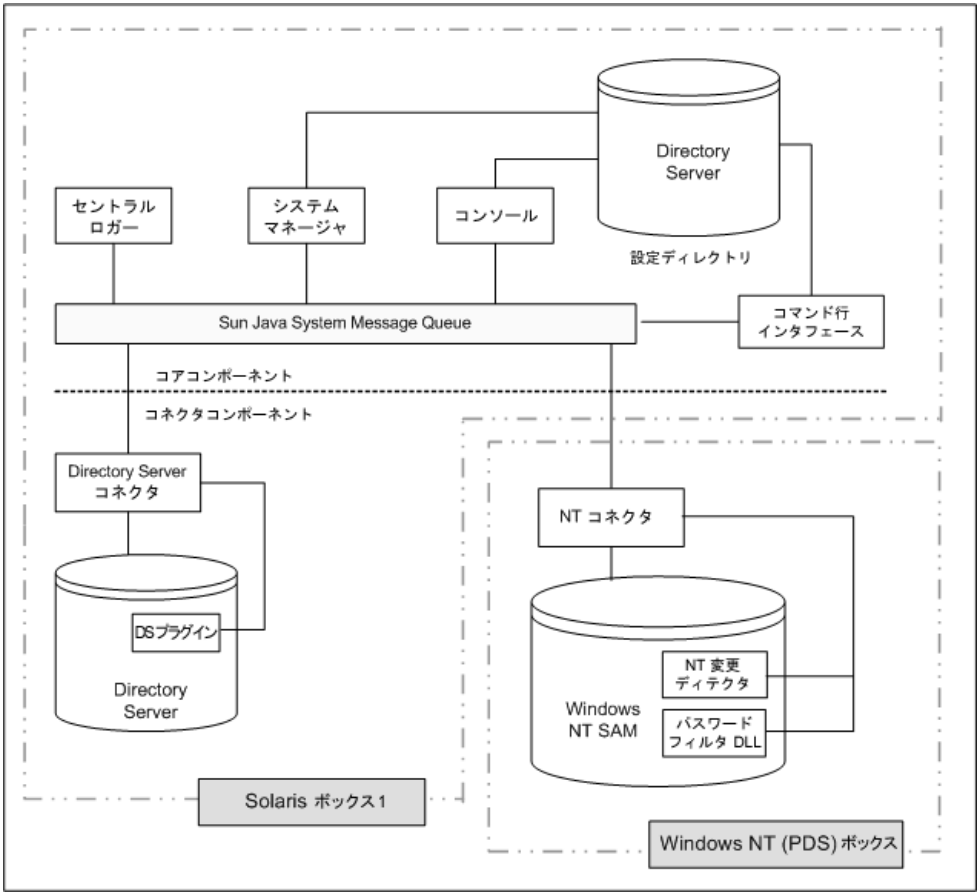
図 1-2　Directory Server と Active Directory コンポーネントの分散



Windows NT コネクタとサブコンポーネント

Windows NT SAM Registry との同期を行うには (図 1-3 を参照)、主ドメインコントローラに Windows NT コネクタ (PDC) をインストールする必要があります。また、インストールプログラムは、コネクタ以外にも 2 つの NT コネクタサブコンポーネント (変更ディテクタとパスワードフィルタの DLL) を NT ドメインの PDC にインストールします。1 つの NT コネクタは、1 つの NT ドメインのユーザーとパスワードを同期させます。

図 1-3 Directory Server と NT コンポーネントの分散



Identity Synchronization for Windows がディレクトリソース内の変更を検出するしくみ

ここでは、Sun Java System Directory Server (Directory Server)、Windows Active Directory、Windows NT のコネクタが、ユーザーエントリとパスワードの変更を検出するしくみについて説明します。

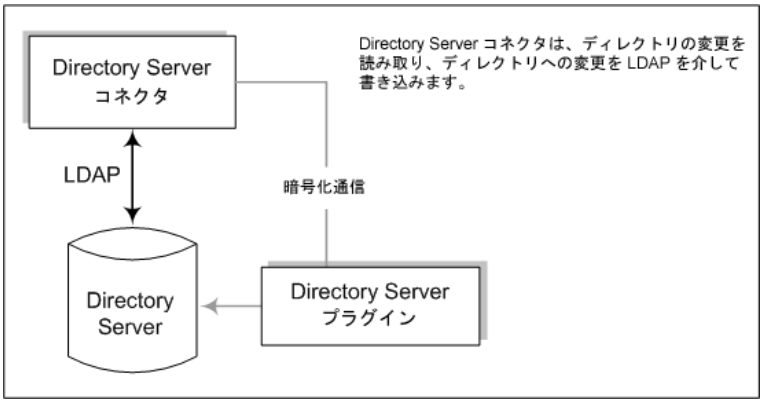
ここで説明する内容は、次のとおりです。

Directory Server コネクタによる変更の検出

Directory Server コネクタは LDAP を介して Directory Server の旧バージョン形式の更新履歴ログを調べ、ユーザーエントリとパスワードの変更イベントを検出します。このとき、Directory Server プラグインはコネクタによる次の処理を支援します。

- クリアテキスト形式のパスワードを取り込んで暗号化し、旧バージョン形式の更新履歴ログで使用できるようにする。プラグインを使用しない場合、旧バージョン形式の更新履歴ログで利用できるパスワードはハッシュ化されており、ハッシュ化されたパスワードを同期させることはできない
- Windows 環境に Identity Synchronization for Windows コンポーネントをインストールする必要をなくすため、Active Directory とのオンデマンドパスワード同期を行う (44 ページの「オンデマンドパスワード同期によるクリアテキスト形式パスワードの取得」を参照)

図 1-4　Directory Server コネクタによる変更の検出



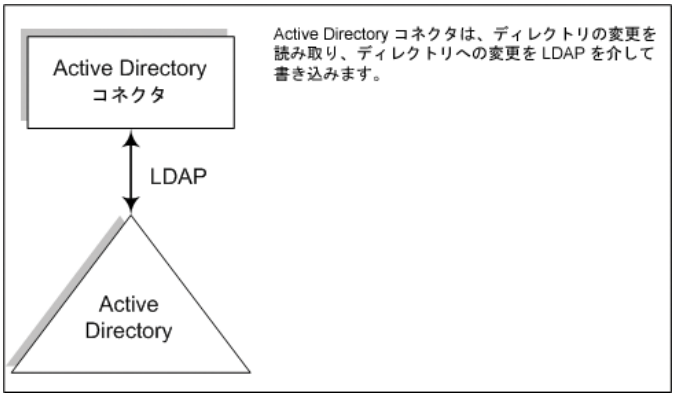
Active Directory コネクタによる変更の検出

Windows 2000/2003 Server Active Directory コネクタは、Active Directory の属性 `USNChanged` および `PwdLastSet` の値を調べることで、ユーザーエントリとパスワードの変更を検出します。

Directory Server の旧バージョン形式の更新履歴ログとは異なり、エントリの属性に変更を加えても、Active Directory はどの属性が変更されたかをレポートしません。その代わりに、Active Directory は `USNchanged` 属性の値を繰り上げることでエントリの変更を識別します。個々の属性の変更を検出するために、Active Directory と Windows NT のコネクタはオブジェクトキャッシュというプロセス内データベースを使用します。オブジェクトキャッシュには、Active Directory の各エントリのハッシュ化されたコピーが格納され、コネクタはこのコピーを使用して、エントリ内のどの属性が変更されたかを特定します。

Windows 環境に Active Directory コネクタをインストールする必要はありません。Active Directory コネクタは、Solaris コンピュータを含め、あらゆる環境で実行することができ、LDAP 経由でリモートに検出、変更を行うことができます。

図 1-5　Active Directory コネクタによる変更の検出

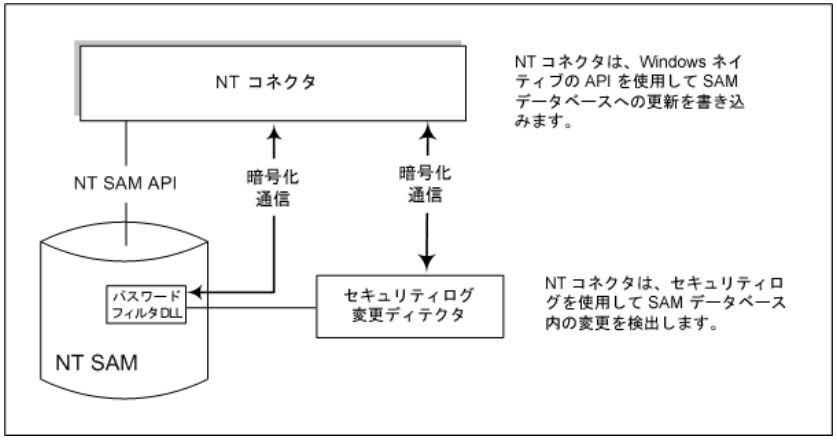


Windows NT コネクタによる変更の検出

Windows NT コネクタは、ユーザーオブジェクトに関する監査イベントのセキュリティログを調べることで、ユーザーエントリとパスワードの変更を検出します。

Windows NT SAM Registry との同期を行うには (図 1-3 を参照)、主ドメインコントローラに Windows NT コネクタ (PDC) をインストールする必要があります。また、インストーラは、コネクタ以外にも 2 つの NT コネクタサブコンポーネント (変更ディテクタとパスワードフィルタの DLL) を NT ドメインの PDC にインストールします。1 つの NT コネクタは、1 つの NT ドメインのユーザーとパスワードを同期させます。

図 1-6　Windows NT コネクタによる変更の検出



注 配備に Windows NT マシンが含まれる場合、監査を有効にしない限り、Identity Synchronization for Windows はそのマシンからのメッセージをログに記録できません。Windows NT マシンで監査のログ記録が有効化されているかどうかを確認する方法については、277 ページの「Windows NT マシンでの監査の有効化」を参照してください。

変更ディテクタおよびパスワードフィルタ DLL の各サブコンポーネントについては、36 ページの「Windows NT コネクタサブコンポーネント」を参照してください。

パスワード更新の伝達

ここでは、パスワードの変更を Windows システムと Directory Server システムの間で相互に伝達するために必要な、クリアテキスト形式パスワードの取得方法について説明します。

パスワードフィルタ DLL によるクリアテキスト形式パスワードの取得

Windows NT コネクタがパスワードの変更を Sun Java System Directory Server に伝達するには、クリアテキスト形式のパスワードを取得する必要があります。しかし、パスワードはディレクトリへの格納時にすでに暗号化されているため、Windows ディレクトリからクリアテキスト形式のパスワードを抽出することはできません。

Windows NT には、パスワードフィルタ DLL インタフェースが用意されています。コンポーネントはこのインタフェースを使用して、パスワードがディレクトリに永続的に格納される前に、クリアテキスト形式のパスワードを取得します。

オンデマンドパスワード同期によるクリアテキスト形式パスワードの取得

Active Directory は Windows NT と同じパスワードフィルタをサポートするため、すべてのドメインコントローラに主ドメインコントローラ (PDC) だけでなく、パスワードフィルタ DLL をインストールする必要があります。このインストール作業は大きな負担となるため、Identity Synchronization for Windows は Active Directory から Directory Server へのパスワード変更の同期にオンデマンドパスワード同期という別の方法を使用します。

オンデマンドパスワード同期により、Windows 2000 環境でユーザーがパスワードを変更した後に、そのユーザーが Directory Server にログインするときに新しいパスワードの値を Directory Server 側で取得することができます。

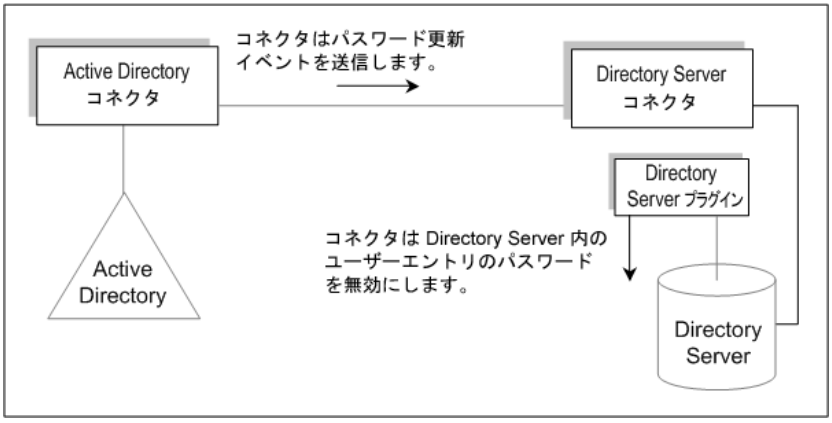
また、オンデマンドパスワード同期により、パスワードフィルタ DLL なしでパスワードを Active Directory と同期させることができます。

オンデマンドパスワード同期は次のように行われます。

1. ユーザーは Windows ワークステーションで Ctrl-Alt-Del キーを押し、パスワードを変更します。新しいパスワードは Active Directory に格納されます。
2. Active Directory コネクタは、設定された間隔でシステムをポーリングします。

   `USNchanged` (更新シーケンス番号) 属性と `PwdLastSet` 属性の変更に基づいてコネクタがパスワードの変更を検出すると、コネクタはパスワードの変更に関するメッセージを Message Queue でパブリッシュします。メッセージは、SSL で暗号化されたチャネルを通じて転送されます。

図 1-7 オンデマンドパスワード同期 (第 1 部)



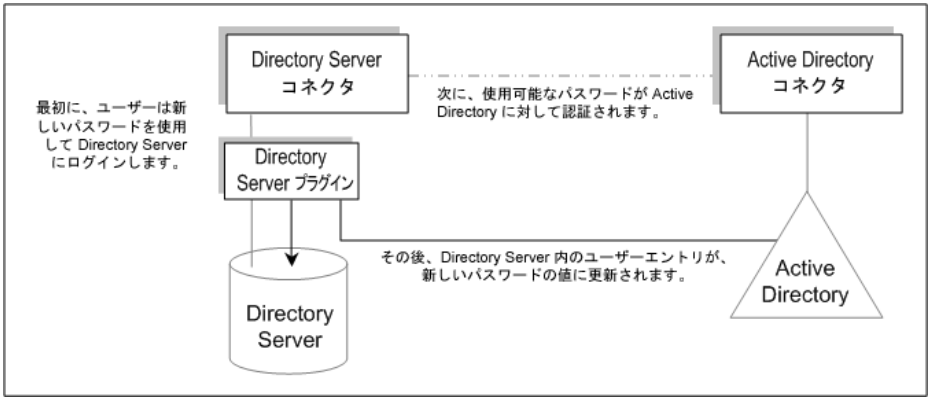
3. Directory Server コネクタは、パスワード変更に関するメッセージを Message Queue から SSL 経由で受信します。
4. Directory Server コネクタは、ユーザーエントリの `dspswvalidate` 属性を `true` に設定します。これにより、古いパスワードは無効化され、Directory Server プラグインにパスワードの変更が伝達されます。
5. ユーザーがログインを試みると、Portal Server などの LDAP アプリケーションを使用して Directory Server に対する認証が行われ、Sun Java System Directory Server プラグインは Directory Server エントリ内のパスワード値が無効になっていることを検出します。

6. Directory Server プラグインは Active Directory 内で対応するユーザーを検索します。ユーザーを見つけると、プラグインは Directory Server へのログイン試行時にユーザーが入力したパスワードを使用して Active Directory へのバインドを試みます。

注	オンデマンドパスワード同期では、アプリケーションは Directory Server に対する認証に SASL Digest-MD5 などの複雑なメカニズムではなく、単純なメカニズムを使用する必要があります。

7. Active Directory へのバインドが成功した場合は、ユーザーが Active Directory の新しいパスワードを入力したことが確認され、Directory Server プラグインは Directory Server のユーザーエントリに新しいパスワードを設定し、無効パスワードのフラグを削除します。

図 1-8　オンデマンドパスワード同期 (第 2 部)



注	ユーザー認証に失敗した場合、Directory Server 側ユーザーエントリのパスワードはそのまま残されるため、Active Directory に対する認証に使用する正しいパスワードをユーザーが入力してログインするまで、Directory Server と Active Directory の間で非同期が生じます。

信頼性の高い同期

コンポーネントが一時的に使用不可能な状態になってもユーザーによる変更のイベントが失われないように、Identity Synchronization for Windows は数多くの対策を講じています。Identity Synchronization for Windows の信頼性は、TCP ネットワークプロトコルの信頼性に似ています。TCP は、不可逆的で断続的に接続されたネットワークであっても、最終的にすべてのデータを順番に配信します。ネットワークが一時的に使用不可能な状態にある最中に送信されたデータは、ネットワークの停止中はキューに蓄積され、接続が回復した時点で再配信されます。Identity Synchronization for Windows は、次のいずれかのコンポーネントが一時的に使用不可能になった場合でも、ユーザーによる変更のイベントを最終的に検出し、それを適用します。

- コネクタ
- Directory Server
- Message Queue
- Active Directory ドメインコントローラ
- Windows NT 主ドメインコントローラ
- システムマネージャ
- 設定ディレクトリ

いずれかのコンポーネントが使用不可能になった場合、Identity Synchronization for Windows は変更 (パスワードの変更を含む) を失うことなく、該当コンポーネントが使用可能な状態に復元されるまで同期を遅延させます。Identity Synchronization for Windows のこのバージョンは、Sun Cluster などの本来の意味での高可用性ソリューションをサポートしていません。Identity Synchronization for Windows は、ユーザーが直接操作することのない、背後で実行されるアプリケーションであるため、通常は高可用性は必要ありません。致命的な障害が発生してしまった場合は、Identity Synchronization for Windows コンポーネントを再インストールし、`idsync resync` コマンドを使用してすべてのディレクトリソースを再同期させることができます。

ほとんどの状況では、コンポーネントが使用不可能になると、プログラムは同期イベントをキューに蓄積し、コンポーネントが使用可能に復元された場合にだけそのイベントを適用します。このプロセスには、次の 2 つの例外があります。

- マルチマスターレプリケーション (MMR) の Directory Server 環境では、Windows ユーザーに対する外部からの変更は、優先または二次 Directory Server を対象に同期できる

  優先 Directory Server が使用不可能な状態にある場合、Directory Server コネクタは変更を二次サーバーに適用する。Identity Synchronization for Windows は、優先マスターが使用可能になるまで、外部から任意の Directory Server マスターに加えられた変更を検出および伝達しない

- Active Directory コネクタが通信できるのは 1 つの Active Directory ドメインコントローラに限定されるため、オンデマンドパスワード同期時にすべての Active Directory ドメインコントローラとの間で Directory Server プラグインが失敗する可能性がある。この点で、フェイルオーバーが最も重要となる —Directory Server が Active Directory ドメインコントローラにアクセスしてユーザーの新しいパスワードを検証できない場合、ユーザーは Directory Server にログインできない

2 マシン構成での配備例

ここでは、Identity Synchronization for Windows を使用して、Sun ディレクトリと Windows ディレクトリの間でユーザーオブジェクト作成の同期と、パスワード修正の双方向同期を行う配備例について説明します。

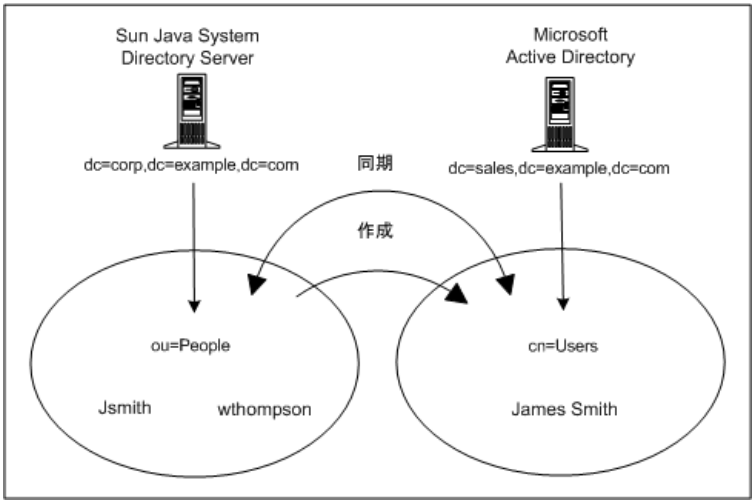
この配備例は、次の 2 つのシステムから構成されます。

- Sun Java System Directory Server が稼動するシステム (ホスト名は *corp.example.com*)
- Windows 2000 サーバー上で Active Directory が稼動するシステム (ホスト名は *sales.example.com*)

注	この例では NT は使用されませんが、Identity Synchronization for Windows は NT ドメインとの同期もサポートしています。

図 1-9 は、この配備例に適用される同期要件 (ノード構成と関連属性値) を示しています。

図 1-9　同期要件



この配備例には、次の 2 つの目的があります。

- ユーザーサブツリー (Directory Server の *ou=people* と Active Directory の *cn=users*) の間でユーザーパスワードを双方向に同期させる、つまり、いずれかのディレクトリでユーザーパスワードを変更するたびに、もう一方のディレクトリ内の関連ユーザーのパスワードが同期されるようにする

  たとえば、Directory Server の *ou=people* コンテナで uid=JSmith のパスワードを変更した場合、新しいパスワードは Active Directory サーバーの *cn=users* コンテナ内の cn=Joe Smith に自動的に同期される必要がある

- Directory Server の People サブツリーでのユーザーオブジェクトの作成を Active Directory の Users サブツリーに同期させる

  たとえば、特定の属性セットを持つ新規ユーザー (*ou=People* コンテナ内の uid=WThompson) を作成すると、Active Directory 上で同じ属性セットを持つ WThompson の新規アカウント (*cn=Users* コンテナ内の cn=William Thompson) が作成される

注

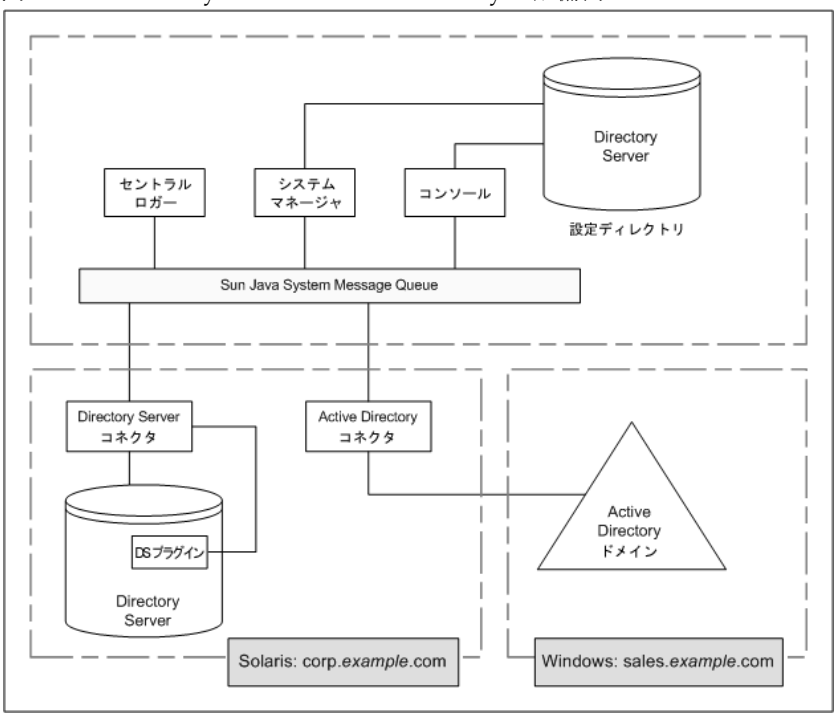
Identity Synchronization for Windows は、同一種類の複数の同期ソースをサポートします。たとえば、1 つの配備に複数の Directory Server や複数の Active Directory ドメインを持たせることができます。

同期設定の作成、修正、削除はディレクトリセット全体でグローバルに適用され、各ディレクトリソースに個別に指定することはできません。ユーザーオブジェクトの作成を Sun から Windows に同期させる場合、ユーザーオブジェクトの新規作成はすべての Sun Directory Server から、インストールに設定されているすべての Active Directory ドメインおよび Windows NT ドメインに伝達されます。

物理的な配備

図 1-10 は、製品のすべてのコンポーネントが 1 つの Solaris ボックスに物理的にどのように配備されるかを示しています。Active Directory ドメインは、異なる Active Directory ドメインコントローラ上に存在し、こちらにはコンポーネントはインストールされていません。

図 1-10 Directory Server と Active Directory の配備例



コンポーネントの分散

ホスト *corp.example.com* は、Solaris オペレーティングシステムにインストールされた Directory Server です。同期対象 Directory Server のルートサフィックスは *dc=corp,dc=example,dc=com* です。

このマシンには、次のコンポーネントが含まれます。

- Identity Synchronization for Windows コアコンポーネント
- Identity Synchronization for Windows Directory Server コネクタ
- Identity Synchronization for Windows Directory Server プラグイン
- Identity Synchronization for Windows 設定ディレクトリ (同期対象とは異なる Directory Server インスタンスに格納される)

ホスト *sales.example.com* は、同期対象 Active Directory ドメインです。

第 2 章

インストールの準備

Identity Synchronization for Windows 1 2004Q3 をインストールする、またはバージョン 1.0 からバージョン 1 2004Q3 に移行する前に、インストールと設定のプロセスについて理解する必要があります。

この章ではこれらのプロセスについて説明し、製品のインストールを準備する上で有用なその他の情報を提供します。この章で説明する内容は次のとおりです。

インストール要件

ここでは、Identity Synchronization for Windows のインストール要件について説明します。この要件には、オペレーティングシステムのバージョン、パッチ、各プラットフォームのユーティリティが含まれます。

オペレーティングシステムの要件

次の表は、このリリースの Identity Synchronization for Windows で必要とされるオペレーティングシステムを示しています。

表 2-1　Solaris 環境の要件

コンポーネント	Solaris 環境の要件
コアコンポーネント	コアコンポーネント Solaris 8™ for UltraSPARC® (32 ビット、および 64 ビット) Solaris 9™ SPARC® Platform Edition (32 ビット、および 64 ビット) Solaris 9™ オペレーティングシステム (x86 Platform Edition for Pentium II 以降) IA-32
Sun Java™ System Directory Server と Windows Active Directory のコネクタ	Solaris 8 for UltraSPARC (32 ビット、および 64 ビット) Solaris 9 for SPARC platforms (32 ビット、および 64 ビット) Solaris 9 オペレーティングシステム (x86 Platform Edition for Pentium II 以降) IA-32
Sun Java™ System Directory Server のプラグイン	Solaris 8 for UltraSPARC (32 ビット、および 64 ビット) Solaris 9 for SPARC platforms (32 ビット、および 64 ビット) Solaris 9 オペレーティングシステム (x86 Platform Edition for Pentium II 以降) IA-32

表 2-2　Windows 環境の要件

コンポーネント	Windows 環境の要件
コア	Windows 2000 Server SP4 Windows 2000 Advanced Server SP4
	Windows 2003 Server Standard Edition (および最新のセキュリティアップデート)
	Windows 2003 Server Enterprise Edition (および最新のセキュリティアップデート)
Sun Java™ System Directory Server と Windows Active Directory のコネクタ	Windows 2000 Server SP4 Windows 2000 Advanced Server SP 4
	Windows 2003 Server Standard Edition (および最新のセキュリティアップデート)
	Windows 2003 Server Enterprise Edition (および最新のセキュリティアップデート)

表 2-2　Windows 環境の要件 (続き)

コンポーネント	Windows 環境の要件
Sun Java™ System Directory Server のプラグイン	Windows 2000 Server SP4 Windows 2000 Advanced Server SP4
	Windows 2003 Server Standard Edition (および最新のセキュリティアップデート)
	Windows 2003 Server Enterprise Edition (および最新のセキュリティアップデート)
NT コネクタとサブコンポーネント	Windows Primary Domain Controller NT 4.0 Server SP 6A (x86 の場合のみ)

ハードウェアの要件

Identity Synchronization for Windows を実行するには、プラットフォームに関係なく、ハードウェアが次の最小要件を満たしている必要があります。

- 最小限のインストールに必要な、Directory Server 上の約 400M バイトのディスク容量
- Identity Synchronization for Windows コンポーネントを実行するすべてのサーバーで 512M バイト以上の RAM (これ以上の容量が望ましい)

Sun Java System ソフトウェアの要件

Identity Synchronization for Windows をインストールするには、事前に次の Sun Java System ソフトウェアコンポーネントをインストールしておく必要があります。

- Sun Java System Directory Server 5 2004Q2 パッチ 117907-02 以降

  次のパッチは、Directory Server 5 2005Q1 を使用する Identity Synchronization for Windows 1 2004Q3 の削除機能を有効化する

  - **Solaris SPARC パッケージ形式** : パッチ番号 117907-02 以降
  - **Solaris SPARC 圧縮アーカイブインストール** : パッチ 5077789
  - **Solaris x86 パッケージ形式** : パッチ番号 117908-02 以降
  - **Solaris x86 圧縮アーカイブインストール** : パッチ 5077789
  - **Windows 圧縮アーカイブインストール** : パッチ 5077789

  これらのパッチの詳細と、Directory Server 環境への適用方法については、Identity Synchronization for Windows ダウンロードの次の場所にある `README.patch` ファイルを参照

<*download_root*>/patches/directory/README.patch

Directory Server 5 2005Q1 を Solaris 環境にインストールする上で必要なパッチに関する最新の情報については、『Sun Java System Directory Server 5 2005Q1 Installation and Tuning Guide』および『Sun Java System Directory Server 5 2005Q1 リリースノート』を参照。これらのドキュメントは、次の Web サイトで入手できる

http://docs.sun.com/db/prod/entsys?l=ja

- Sun Java System Message Queue (従来の Sun ONE Message Queue) バージョン 3.5 Sp1 Enterprise Edition

注	Identity Synchronization for Windows バージョン 1.0 では、Message Queue が自動的にインストールされましたが、バージョン 1 2004Q3 ではインストールされません。 Sun Java System Message Queue の既存のインストールに Identity Synchronization for Windows コアをインストールするには、Message Queue バージョン 3.5 SP1 Enterprise Edition を使用している必要があります。不適切なバージョンの Message Queue にコアをインストールしようとすると、失敗します。

Identity Synchronization for Windows のダウンロードバンドルには Message Queue が含まれる。ソフトウェアは、各プラットフォームの次の /messagequeue ディレクトリにある

  - Solaris SPARC: /messagequeue/imq3_5-ent-solsparc.zip
  - Solaris x86: /messagequeue/imq3_5-ent-soli386.zip
  - Windows: /messagequeue/imq3_5-ent-win.exe

- Java 実行時環境

  この製品には Java 実行時環境 (JRE) が含まれない

  - Solaris または Windows で Identity Synchronization for Windows インストーラを実行するには、J2SE (または JRE) 1.4.2_04 以降をインストールする必要がある
  - Windows NT 環境では、JRE 1.4.1_03 以降をインストールする必要がある

インストールに必要なクレデンシャル

Identity Synchronization for Windows をインストールするには、次のディレクトリのクレデンシャルを指定する必要があります。

- 設定ディレクトリ
- 同期対象となる Directory Server
- Active Directory (「コアのインストール」を参照)

さらに、Identity Synchronization for Windows のインストールには次の権限が必要です。

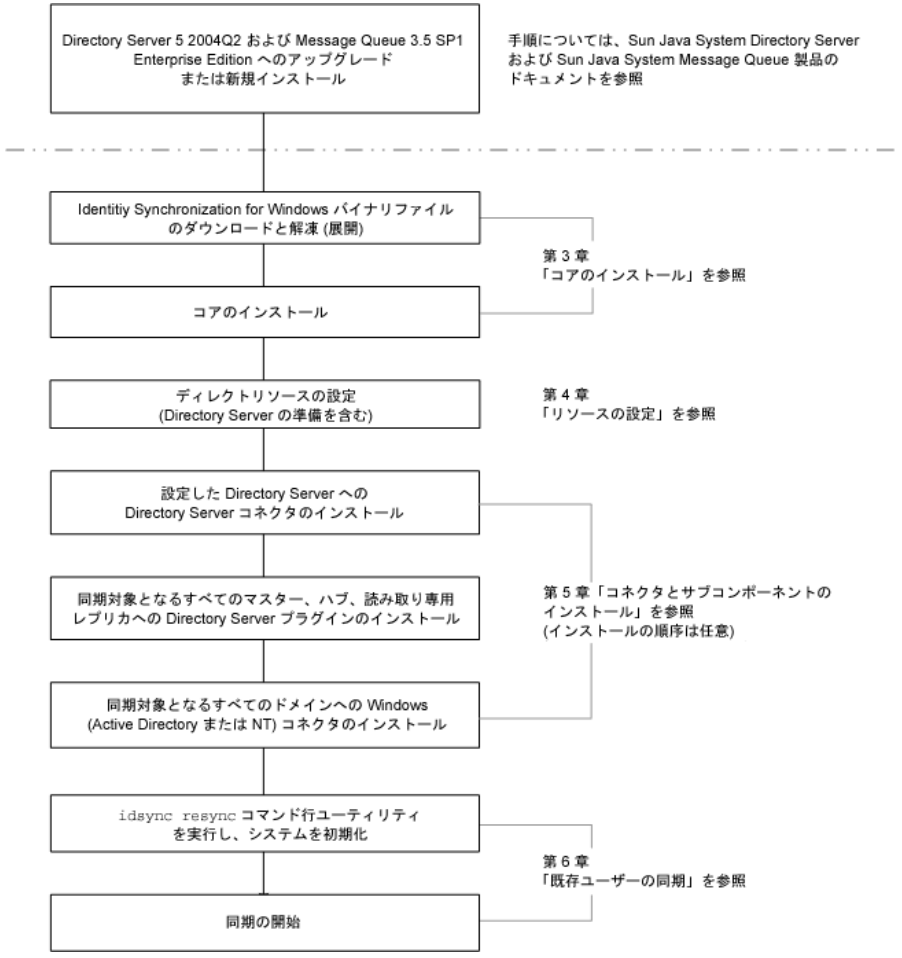
- **Solaris システム** : ルートとしてインストールする必要がある
- **Windows システム** : 管理者としてインストールする必要がある

注	テキストベースのインストーラを使用してパスワードを入力した場合、暗号化せずにエコーされることがないように、パスワードが自動的にマスキングされます。テキストベースのインストーラは Solaris システムだけでサポートされます。

インストールの概要

図 2-1 は、単一ホスト配備での製品のインストールプロセスを示しています。

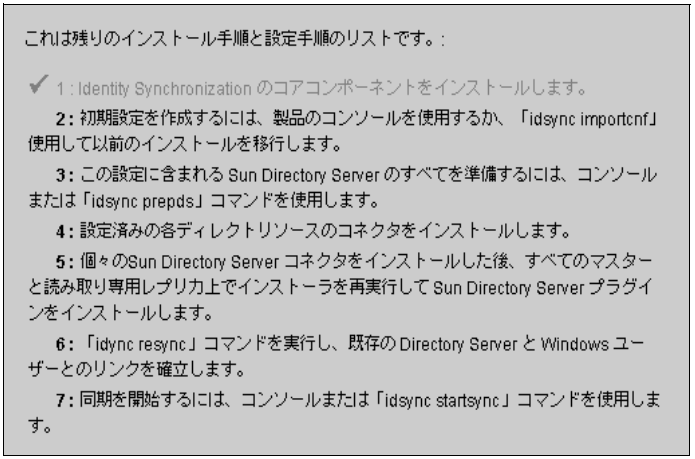
図 2-1 単一ホスト配備でのインストール



一部のコンポーネントは特定の順序でインストールする必要があるため、すべてのインストール手順をよく読んでください。

Identity Synchronization for Windows には、インストールと設定のプロセス全体で表示される、実行手順を示すリストが用意されています。この情報パネルには、製品のインストールと設定を正しく行うためのすべての手順が示されます。

図 2-2　Identity Synchronization for Windows の実行手順リスト



インストールと設定の手順を進めると、図 2-2 に示すように、すべての完了手順がリスト上でグレイ表示されます。

この節の残りの項では、インストールと設定のプロセスの概要を示します。説明する内容は次のとおりです。

- 60 ページの「コアのインストール」
- 60 ページの「製品の設定」
- 60 ページの「Directory Server の準備」
- 61 ページの「コネクタと Directory Server プラグイン」
- 62 ページの「既存ユーザーの同期」

注　インストールと設定の手順については、このマニュアルでさらに詳しく説明します。

コアのインストール

コアをインストールするときは、次のコンポーネントをインストールします。

- **コンソール** : 製品コンポーネントのすべての設定タスクと管理タスクを集中的に行う場所を提供する
- **セントラルロガー** : 監査とエラーのすべてのログ情報を一元的に管理する
- **システムマネージャ** : 設定の変更を動的にコネクタに伝達し、各コネクタの状態を維持する

注	コネクタのインストール方法については、第 3 章「コアのインストール」で説明します。

製品の設定

コアをインストールすると、コンソールを使用して、同期の対象となるディレクトリソースの初期設定、および配備のその他の特性を一元的に行えるようになります。

注	ディレクトリリソースの設定方法については、第 4 章「コアリソースの設定」で説明します。

Directory Server の準備

Directory Server コネクタは、Sun Java System Directory Server 5 2005Q1 をサポートします。

Directory Server コネクタをインストールするには、同期の対象となるすべての設定済み Directory Server マスター (優先マスターと二次マスターの両方) で Sun Java System Directory Server ソースを準備する必要があります。

このタスクは、コンソールから、または `idsync prepds` サブコマンドを使用してコマンド行から行うことができます。

注	Directory Server の準備手順については、111 ページの「Directory Server の準備」で説明します。

コネクタと Directory Server プラグイン

システムに設定されているディレクトリの数に応じて、任意の数のコネクタと Directory Server プラグインをインストールできます。

注 コンソールとインストールプログラムは、コネクタと同期対象ディレクトリの関連付けに、どちらもディレクトリのラベルを使用します。表 2-3 は、Identity Synchronization for Windows によるラベル名の指定に関する規則を示しています。

表 2-3 ラベル名の指定に関する規則

コネクタの種類	ディレクトリソースのラベル	サブコンポーネント
Directory Server コネクタ	ルートサフィックス、またはサフィックス / データベース	Directory Server プラグイン 同期対象ルートサフィックスのすべての Directory Server (マスターまたはコンシューマ) について、1 つずつプラグインをインストールする
AD コネクタ	ドメイン名	なし
NT コネクタ	ドメイン名	Windows NT コネクタと共に自動的にインストールされる、変更ディテクタおよびパスワードフィルタ DLL サブコンポーネントは、同じ場所にまとめてインストールされる Windows NT コネクタのインストールには、グラフィカルユーザーインタフェース (GUI) のインストーラを使用する必要がある

注 コネクタと Directory Server プラグインのインストールと設定については、第 5 章「コネクタと Directory Server プラグインのインストール」で説明します。

既存ユーザーの同期

コネクタ、プラグイン、サブコンポーネントのインストールが完了したら、コマンド行ユーティリティ idsync resync を実行して、配備に既存ユーザーを取り込む必要があります。このコマンドは、管理者が指定した一致規則を使用して次の処理を行います。

- 既存エントリのリンクを設定する (リンク設定の定義については、178 ページの「ユーザーのリンク」を参照)
- 空のディレクトリにリモートディレクトリの内容を取り込む
- Windows と Directory Server の両方のディレクトリ内で一意に識別され、相互にリンクされている既存ユーザーの間で、パスワードを含め、属性値を一括同期させる

注 配備での既存ユーザーの同期については、第 6 章「既存ユーザーの同期」で説明します。

設定の概要

製品のインストールが完了したら、製品の配備を設定します。これには次のタスクが含まれます。

- 同期させるディレクトリとグローバルカタログを設定する
- 属性変更とオブジェクトの有効化 / 無効化の同期設定を指定する
- 設定されたディレクトリ間でのユーザーエントリの作成と削除の同期設定を指定する (省略可能)

ここでは、次の設定要素について、その概要を説明します。

- 63 ページの「ディレクトリ」
- 63 ページの「設定ディレクトリとグローバルカタログ」
- 63 ページの「同期設定」
- 64 ページの「オブジェクトクラス」
- 65 ページの「属性と属性マッピング」
- 66 ページの「同期ユーザーリスト」

注 設定手順については、このマニュアルでさらに詳しく説明します。

ディレクトリ

ディレクトリが意味する内容は次のとおりです。

- 1 つまたは複数の Sun Java System Directory Server 内の 1 つのルートサフィックス (サフィックス / データベース)
- Windows 2000 または Windows 2003 Server Active Directory フォレスト内の 1 つの Active Directory ドメイン
- 1 つの Windows NT ドメイン

どの種類であっても、任意の数のディレクトリを設定できます。

設定ディレクトリとグローバルカタログ

Identity Synchronization for Windows は、フェッチした Directory Server または Active Directory のディレクトリトポロジと、ディレクトリのスキーマ情報のリポジトリとして、Sun Java System Directory Server 設定ディレクトリと、Active Directory グローバルカタログを使用します。

同期設定

Sun と Windows のディレクトリの間で、オブジェクトの作成、オブジェクトの削除、パスワードおよびその他の属性の変更を伝達する方向を制御するには、同期設定を使用します。同期フローには次のオプションがあります。

- Sun から Windows へ
- Windows から Sun へ
- 双方向

注 Active Directory と Windows NT が含まれる設定では、Active Directory と Sun の間の同期と Windows NT と Sun の間の同期に、異なる作成同期設定または変更同期設定を指定して設定を保存することはできません。

オブジェクトクラス

リソースを設定するときは、エントリのオブジェクトクラスに基づいて、どのエントリを同期対象とするかを指定します。オブジェクトクラスは、Directory Server と Active Directory の両方で同期させることができる属性を決定します。

注	オブジェクトクラスは Windows NT には適用されません。

Identity Synchronization for Windows は、次の 2 種類のオブジェクトクラスをサポートします。

- Structural オブジェクトクラス : 選択した Directory Server から作成された、または同期させられたすべてのエントリは、少なくとも 1 つの Structural オブジェクトクラスを持つ必要がある。Structural オブジェクトクラスは、ドロップダウンリストから選択する (デフォルトでは、Directory Server では *inetorgperson*、Active Directory では *User* が選択される)
- Auxiliary オブジェクトクラス :
  - Directory Server では、「利用可能 Auxiliary オブジェクトクラス」リストから 1 つまたは複数のオブジェクトクラスを選択することができる。指定した Structural クラスのほかにこれらのオブジェクトクラスを追加することで、他の属性を同期させることができる
  - Active Directory では、Auxiliary オブジェクトクラスによる指定はさらに限定的である。選択した Structural オブジェクトクラスのすべての有効 Auxiliary オブジェクトクラスの属性を同期対象として指定できる

注	オブジェクトクラスと属性の設定については、第 4 章「コアリソースの設定」を参照してください。

属性と属性マッピング

属性は、ユーザーエントリを説明する情報を保持しています。各属性にはラベルと 1 つまたは複数の値があります。属性値として格納できる情報の種類に応じて、標準の構文に従います。

注 属性は、コンソールで定義できます。属性を定義する方法については、第 4 章を参照してください。

属性の種類

Identity Synchronization for Windows は、有効ユーザー属性と作成ユーザー属性を次のように同期させます。

- **有効属性** : 属性が変更されるたびに、指定されている変更同期設定に基づいて、Sun と Windows のディレクトリ間を同期させる
- **作成属性** : 新規ユーザーが作成されるたびに、指定されているオブジェクト作成同期設定に基づいて、Sun と Windows のディレクトリ間を同期させる

  必須作成属性は、ターゲットディレクトリ内での作成動作の完了に「必須」とされる属性である。たとえば、Active Directory では、作成時に `cn` と `samaccountname` の両方に有効な値が必要となる。Sun 側で `user` オブジェクトクラスの `inetorgperson` を設定する場合、Identity Synchronization for Windows は `cn` と `sn` を新規作成の必須属性と見なす

  元ディレクトリから伝達された属性に値が含まれない場合、デフォルトの作成属性は、ターゲットディレクトリの作成属性をデフォルト値だけで更新する (作成属性のデフォルト値は、他の属性の値に基づくように設定できる。65 ページの「パラメータ化されたデフォルト属性値」を参照)

注 有効属性は、自動的に作成属性として同期されますが、その反対は行われません。作成属性は、ユーザー作成時にだけ同期されます。

パラメータ化されたデフォルト属性値

Identity Synchronization for Windows では、別の作成属性または有効属性の値を使用して、作成属性のパラメータ化されたデフォルト値を設定できます。

パラメータ化されたデフォルト属性値を指定するには、式文字列内の既存の作成属性または有効属性の名前の前後にパーセント記号を付けます (`%<attribute_name>%`)。たとえば、`homedir=/home/%uid%` や `cn=%givenName%. %sn%` のように指定します。

これらのデフォルト属性値は、次のように使用できます。

- 作成式には複数の属性を指定することができるが (cn=%givenName% %sn%)、%<*attribute_name*>% は 1 つの値をとる必要がある
- A=%B% の場合、B がとれるデフォルト値は 1 つだけである
- パーセント記号を通常の文字として使用する場合は、円記号を使用する (たとえば、diskUsage=0¥%)
- 循環代入条件を持つ式を使用しない (たとえば、sn=%uid% と uid= %sn%)

属性のマッピング

同期させる属性の定義が完了したら、Sun と Windows の間で属性名をマッピングする必要があります。たとえば、Sun の inetorgperson 属性を Active Directory の user にマッピングします。

注 有効属性と作成属性の両方の属性マップが使用されます。また、それぞれの種類のディレクトリで「必須作成属性」の属性マップを設定する必要があります。

同期ユーザーリスト

Sun と Windows の両方のディレクトリで同期させる特定のユーザーを定義するときは、同期ユーザーリスト (SUL) を作成します。これらの定義を利用することで、フラットなディレクトリ情報ツリー (DIT) と階層構造を持つディレクトリツリーの間を同期させることができます。

同期ユーザーリストの定義には、次の概念が使用されます。

- **ベース DN** (Windows NT には適用されない): 別の SUL によってより詳細に指定されていない、またはフィルタによって除外されていない場合に、その DN のすべてのユーザーを同期対象に含める
- **フィルタ** : ユーザーエントリの属性を使用して、ユーザーを同期対象から除外する、または、同一ベース DN に含まれるユーザーを複数の SUL に分割する。このフィルタには、LDAP フィルタ構文が適用される
- **作成式** (Windows NT には適用されない): 新規ユーザーの作成先となる DN を指定する。たとえば、cn=%cn%,ou=sales,dc=example,dc=com のように指定した場合、%cn% は既存ユーザーエントリの cn の値に置き換えられる。作成式の最後にはベース DN を指定する必要がある

SUL には 2 つの定義が含まれ、それぞれの定義は同期対象ユーザーグループをディレクトリの種類に応じたトポロジで識別します。

- 1 つの定義は、同期させる Directory Server ユーザーを識別する (例 : ou=people, dc=example, dc=com)

- もう 1 つの定義は、同期させる Windows ユーザーを識別する (例 : `cn=users, dc=example, dc=com`)

SUL の作成を準備するときは、次の質問に対する答えを用意します。

- どのユーザーを同期させるのか
- どのユーザーを同期対象から外すのか
- 新規ユーザーをどこに作成するのか

注 SUL の作成については、付録 D を参照してください。

バージョン 1 2004Q3 への移行

Identity Synchronization for Windows バージョン 1.0 (またはバージョン 1.0 SP1) からの移行手順は、少数の例外を除いて、1 2004Q3 の初回インストール手順と同じです。

注 移行手順については、第 7 章で説明します。

Identity Synchronization for Windows 1 2004Q3 への移行を行う前に、次の点に注意してください。

- コネクタのインストールが完了した後で、Directory Server のコネクタ状態ファイルと、Active Directory と NT のコネクタオブジェクトキャッシュファイルを手動で復元する必要がある。Active Directory と NT のコネクタのそれぞれのオブジェクトキャッシュのコピーを保存するために、十分なディスク容量 (`/isw-home/persist` ディレクトリおよびサブディレクトリのサイズによって決定される) が確保されていることを確認する
- 1.0 と 1.0 SP1 のすべてのコンポーネントをアンインストールする必要がある

  1 2004Q3 のインストーラがバージョン 1.0 システムの残存物を検出した場合、Directory Server にインストールされる Identity Synchronization for Windows スキーマと、マシンにインストールされる実際の Identity Synchronization for Windows バイナリに問題が生じる可能性がある

  注 詳細は、207 ページの「1.0 のアンインストールが失敗した場合の対応」を参照してください。

- Identity Synchronization for Windows 1 2004Q3 のコンポーネントは、インストールされていた 1.0 と同じプラットフォームおよびハードウェアアーキテクチャにインストールする必要がある

Active Directory とのパスワードの同期

Windows 2000 のデフォルトのパスワードポリシーは、パスワードの保護をデフォルトで強化するために Windows 2003 で変更されました。

たとえば、Directory Server から Active Directory に対する `resync -c` の実行時など、Identity Synchronization for Windows サービスは、パスワードを持たないエントリを作成しなければならないことがあります。このため、Windows 2000 または 2003 上の Active Directory、または Directory Server でパスワードポリシーを有効にしている場合、ユーザー作成時にエラーが発生する可能性があります。

Active Directory または Directory Server でパスワードポリシーを無効にする必要はありませんが、ほかのシステムに存在するパスワードポリシーの強化に関する問題について理解する必要があります。

Windows 2003 Server Standard Edition または Enterprise Edition 上の Active Directory との間でパスワードを同期させる場合は、次のインストール情報が重要となります。

- Windows 環境へのインストールでは、Solaris に Active Directory コネクタをインストールできる

注	Active Directory コネクタは、Windows 2000 と Windows 2003 Server のどちらの Active Directory とも相互動作する

- Windows 2003 環境でのディレクトリソース、グローバルカタログ、同期ユーザーリストの作成手順は、Windows 2000 上の Active Directory での作成手順と同じである
- Windows 2003 Server のデフォルトパスワードポリシーは厳密なパスワードを要求する。これは、Windows 2000 のデフォルトパスワードポリシーとは異なる

この節の残りの項で説明する内容は次のとおりです。

- 69 ページの「パスワードポリシーの適用」: Windows または Directory Server でパスワードポリシーを適用する場合は、この項に記載されている情報を読み、Active Directory と Directory Server の間の同期結果にパスワードポリシーがどのように影響するかを理解する

- 74 ページの「パスワードポリシーの例」: この項では、いくつかの異なる事例に適用されるパスワードポリシーの例を紹介する

パスワードポリシーの適用

ここでは、Windows 2003 Server および Windows 2000 上の Active Directory、および Sun Java System Directory Server 5 2005Q1 のパスワードポリシーが同期結果にどのように影響するかについて説明します。

ここで説明する内容は、次のとおりです。

- 69 ページの「概要」
- 69 ページの「重要な注意事項」
- 74 ページの「パスワードポリシーの例」
- 74 ページの「エラーメッセージ」

概要

Active Directory または Directory Server で、システムに適用されるパスワードポリシーを満たすユーザーを作成した場合は、ユーザーが正しく作成され、2 つのシステム間で同期されます。両方のシステムでパスワードポリシーを有効にした場合、パスワードは両システムのポリシーを満たす必要があり、満たせない場合はユーザー作成の同期は失敗します。

- Active Directory でパスワードポリシー機能を有効にした場合は、同様の設定、またはそれと一致するパスワードポリシーを Directory Server でも有効にする必要がある
- Active Directory と Directory Server の両方で整合性のあるパスワードポリシーを作成できない場合は、パスワードとユーザー作成のソースとして支配的と見なされるほうのパスワードポリシーを有効にする必要がある。ただし、パスワードポリシーの一部の設定により、ユーザー作成が想定どおりに機能しない場合もある

重要な注意事項

次に、パスワードポリシーに関する重要な情報を示します。

- 70 ページの「Directory Server のパスワードポリシー」
- 70 ページの「Active Directory のパスワードポリシー」
- 71 ページの「パスワードを持たないアカウントの作成」

Directory Server のパスワードポリシー

Directory Server のパスワードポリシーに違反するパスワードを持つユーザーを Active Directory に作成した場合、これらのユーザーは Directory Server 内に作成され、同期も行われますが、エントリはパスワードなしで作成されます。パスワードは、新しいユーザーが Directory Server にログインし、オンデマンドパスワード同期が行われるまで設定されません。このとき、パスワードが Directory Server のパスワードポリシーに違反するため、ログインは失敗します。

このような状況は、いくつかの方法で解決できます。

- ユーザーが次に Active Directory にログオンするときにパスワードの変更を強制する
- Active Directory 側のユーザーパスワードを変更し、新しいパスワードが Directory Server のパスワードポリシー要件を満たすようにする

Active Directory と Directory Server のパスワードポリシーを調べ、両者が可能な限り同等であることを確認してください。

Active Directory のパスワードポリシー

Active Directory のパスワードポリシーを満たさないユーザーを Active Directory に作成した場合、これらのユーザーは Directory Server に作成されます。

- Active Directory はユーザーを「一時的に」作成し、パスワードがパスワードポリシーの要件を満たさない場合にエントリを削除する。このとき、Active Directory コネクタはこの一時的な ADD 処理を認識し、Directory Server 側にユーザーを作成する。ユーザーはパスワードなしで Directory Server に作成されるため、どのユーザーもユーザーとしてログインすることができない。また、これらのエントリは Active Directory 上の有効なエントリにリンクされない。Active Directory から Directory Server に削除が同期される場合、一時的に作成されたユーザーは自動的に削除される
- ユーザーはパスワードなしで Directory Server に作成される。Directory Server は、エントリがパスワードを含んでいる場合以外はユーザー作成にパスワードポリシーを適用しない

このような状況は、いくつかの方法で解決できます。推奨される方法は、Active Directory から Directory Server への削除の同期を設定することです。また、Directory Server からユーザーを削除し、Active Directory のパスワードポリシーを満たす有効なパスワードを持つユーザーを Active Directory に追加することもできます。この方法では、ユーザーが確実に Directory Server に作成され、正しくリンクされます。Directory Server 側のユーザーのパスワードは、ユーザーがはじめて Active Directory にログインし、パスワードを変更した時点で無効化されます。

- Directory Server からユーザーを削除せずに、新しいパスワードを使用してユーザーを再び Active Directory に追加した場合、ユーザーがすでに Directory Server に存在するため、Directory Server への ADD 処理は失敗する。エントリは互いにリンクされないため、idsync resync を実行して 2 つの独立したアカウントをリンクさせる必要がある
- idsync resync コマンドを実行する場合は、Directory Server 上のエントリとリンクされている Active Directory 側のアカウントのパスワードをリセットする必要がある。パスワードをリセットすると、Directory Server 側のパスワードは無効化され、ユーザーが新しい Active Directory パスワードを使用して次に Directory Server へのユーザー認証を試みるときにオンデマンド同期が強制され、Directory Server 側のパスワードが更新される

パスワードを持たないアカウントの作成

再同期などを行う場合、Identity Synchronization for Windows はパスワードを持たないアカウントを作成する必要があります。

Directory Server: Identity Synchronization for Windows がパスワードなしで Directory Server にエントリを作成すると、userpassword 属性は {PSWSYNC}*INVALID*PASSWORD* に設定されます。ユーザーは、パスワードが再設定されるまで Directory Server にログインできません。ただし、-i NEW_USERS または NEW_LINKED_USERS オプションを指定して resync を実行した場合は例外です。この場合、resync によって新規ユーザーのパスワードは無効化され、次回のユーザーログイン時にオンデマンドパスワード同期が行われます。

Active Directory: Identity Synchronization for Windows がパスワードなしで Active Directory にエントリを作成すると、Active Directory のパスワードポリシー要件を満たす強力なパスワードがランダムに選択され、それがユーザーのパスワードとして設定されます。この場合、ログに警告メッセージが記録され、管理者がパスワードを再設定するまでユーザーは Active Directory にログインできません。

次の表は、Identity Synchronization for Windows の使用時に生じる可能性のある、いくつかの事例を示しています。

- 表 2-4 は、パスワードポリシーが同期にどのように影響するかを示す
- 表 2-5 は、パスワードポリシーが再同期にどのように影響するかを示す

パスワードが確実に同期されるように、この情報をガイドラインとして利用してください。システムの設定が異なるため、これらの表は生じる可能性のあるすべての事例について説明するものではありません。

表 2-4　パスワードポリシーが同期に与える影響

ケース			結果		
ユーザーの最初の作成場所	ユーザーが各ディレクトリでパスワードポリシーを満たすかどうか		ユーザーが各ディレクトリに作成されるかどうか		
	Directory Server	Active Directory	Directory Server	Active Directory	コメント
Active Directory	満たす	満たす	される	される	
	満たす	満たさない	**される (コメントを参照)**	されない	ユーザーは Directory Server に作成される。ただし、Active Directory から Directory Server への削除が同期される場合、このユーザーは直ちに削除される 詳しくは、70 ページの「Active Directory のパスワードポリシー」を参照
	満たさない	満たす	**される**	される	詳しくは、69 ページの「重要な注意事項」を参照
	満たさない	満たさない	**される (コメントを参照)**	されない	ユーザーは Directory Server に作成される ただし、Active Directory から Directory Server への削除が同期される場合、このユーザーは直ちに削除される 詳しくは、70 ページの「Active Directory のパスワードポリシー」を参照
Directory Server	満たす	満たす	される	される	
	満たす	満たさない	される	されない	
	満たさない	満たす	されない	されない	
	満たさない	満たさない	されない	されない	

表 2-5　パスワードポリシーが再同期に与える影響

ケース			
resync コマンド	ユーザーが各ディレクトリでパスワードポリシーを満たすかどうか		結果
	Directory Server	Active Directory	
`resync -c -o Sun`	適用外	満たす	ユーザーは Active Directory に作成されるが、ログインすることはできない 詳しくは、71 ページの「パスワードを持たないアカウントの作成」を参照
	適用外	満たさない	ユーザーは Active Directory に作成されるが、ログインすることはできない 詳しくは、71 ページの「パスワードを持たないアカウントの作成」を参照
`resync -c -i NEW_USERS | NEW_LINKED_USERS`	満たす	適用外	ユーザーは Directory Server に作成され、そのパスワードは初回のログイン時に設定される 詳しくは、71 ページの「パスワードを持たないアカウントの作成」を参照
	満たさない	適用外	ユーザーは Directory Server に作成される。ただし、パスワードが Directory Server のパスワードポリシーに違反するため、ログインすることはできない 詳細については、69 ページの「重要な注意事項」と 71 ページの「パスワードを持たないアカウントの作成」を参照
`resync -c`	満たす	適用外	ユーザーは Directory Server に作成される。ただし、Active Directory または Directory Server に新しいパスワードの値が設定されるまでログインすることはできない 詳しくは、71 ページの「パスワードを持たないアカウントの作成」を参照
	満たさない	適用外	ユーザーは Directory Server に作成される。ただし、新しいパスワードの値が Active Directory または Directory Server に設定されるまでログインすることはできない 詳しくは、71 ページの「パスワードを持たないアカウントの作成」を参照

パスワードポリシーの例

ここでは、次の仕様を使用する Active Directory と Directory Server のパスワードポリシーに関連する異なる事例について説明します。

- Active Directory 側の設定 :
  - パスワードの履歴を強制する : 20 日
  - パスワードの有効期間 : 30 日
  - パスワードの変更禁止期間 : 0 日
  - 最小パスワード長 : 7 文字
  - パスワードは要求する複雑さを満たす : 有効
- Directory Server 側の設定 :
  - リセット後、ユーザにパスワード変更を要求する
  - ユーザはパスワードを変更できる
  - 履歴に 20 のパスワードを維持する
  - パスワードの期限は 30 日で切れる
  - パスワードの期限が切れる 5 日前に警告を送信する
  - パスワード構文を検査 : パスワードの最小長は 7 文字とする

エラーメッセージ

コアシステムのセントラルロガー `audit.log` ファイルを調べ、次のエラーメッセージを探します。

Unable to update password on DS due to password policy during on-demand synchronization:

```
WARNING 125 CNN100 hostname "DS Plugin (SUBC100): unable to
update password of entry 'cn=John Doe,ou=people,o=sun', reason:
possible conflict with local password policy"
```

注

Windows 2003 のパスワードポリシーについては、http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dsscc_aut_xbby.asp を参照してください。

Directory Server 5 2005Q1 のパスワードポリシーについては、次の URL を参照してください。

http://docs.sun.com/db/coll/DirectoryServer_04q2

SSL 動作のための Windows の設定

パスワードの変更を Directory Server から Windows Active Directory に伝達する場合は、各 Active Directory サーバーが SSL を使用するように設定し、High Encryption Pack をインストールする必要があります。

次の URL で説明されているように、Microsoft Certificate Services Enterprise Root 認証局から自動的に証明書を取得し、SSL を介した LDAP を Active Directory で 有効にした場合、Identity Synchronization for Windows Active Directory コネクタインストーラは Active Directory コネクタに SSL を自動的に設定できます。

http://support.microsoft.com/default.aspx?scid=kb;en-us;q247078

ただし、次の Microsoft の知識ベース記事を参照することで、SSL を介した LDAP をより簡単に設定できます。

http://support.microsoft.com/default.aspx?scid=kb;en-us;321051

この場合、SSL 通信用の信頼された証明書を使用するときは、298 ページの「Active Directory コネクタでの SSL の有効化」で説明する方法に従って、コネクタの証明書データベースに証明書を手動でインストールする必要があります。

インストールと設定に必要な情報

ここでは、インストールと設定のまとめを示し、Identity Synchronization for Windows の配備に関する選択事項の詳細について説明します。インストールプロセスを開始する前に、これらの情報を準備してください。ここでは、次の内容について説明します。

コアのインストール

コアをインストールするときは、次の情報を指定する必要があります。

- **設定ディレクトリのホストとポート** : Identity Synchronization for Windows の設定情報が格納される設定 Directory Server インスタンスのホストとポートを指定する

  設定ディレクトリのポートとして SSL ポートを指定できる。この場合は、インストール時にポートが SSL ポートであることを指定する必要がある

注	Identity Synchronization for Windows は、ローカルホストとしてインストールされた設定ディレクトリをサポートしません。

- **ルートサフィックス** : 設定ディレクトリのルートサフィックスを指定する。すべての設定情報は、このサフィックスの下に格納される
- **管理者の名前とパスワード** : 設定 Directory Server のクレデンシャルを指定する
- **設定パスワード** : 機密性のある設定情報を保護するための、セキュリティ用パスワードを指定する
- **ファイルシステムディレクトリ** : Identity Synchronization for Windows のインストール先を指定する。コアは、Directory Server 管理サーバーと同じディレクトリにインストールする必要がある
- **未使用のポート番号** : Message Queue インスタンスが使用できるポート番号を指定する

コアの設定

コアを設定するときは、次の情報を指定する必要があります。

- **Sun Java System ディレクトリスキーマサーバー** : 設定ディレクトリから読み込む Directory Server データを指定する
- **user オブジェクトクラス (Directory Server のみ)**: ユーザーの種類を決定する user オブジェクトクラスを指定する。Identity Synchronization for Windows は、このオブジェクトクラスに基づいて属性 (パスワード属性を含む) のリストを生成する。このリストはスキーマから取り込まれる
- **同期させる属性** : Directory Server と Windows 環境の間で同期させるユーザーエントリ属性を指定する
- **変更、作成、削除のフロー** : Sun と Windows のシステムの間で、変更、作成、削除をどのように伝達させるかを指定する。次のオプションから選択できる
  - Sun から Windows へ
  - Windows から Sun へ
  - 双方向

  Sun と Windows のシステム間でオブジェクトの有効化と無効化を同期させるかどうか、およびこれらのオブジェクトを同期させる方法を指定する
- **グローバルカタログ** : Active Directory トポロジとスキーマ情報のリポジトリである、グローバルカタログを指定する
- **Active Directory スキーマコントローラ** : Windows グローバルカタログが取得される Active Directory スキーマソースの完全修飾ドメイン名 (FQDN) を指定する
- **設定ディレクトリ** : Identity Synchronization for Windows の設定情報が格納されている Directory Server を指定する
- **Active Directory ソース** : Active Directory ドメインの同期に使用されるソースを指定する
- **Windows NT 主ドメインコントローラ** : 同期対象となる Windows NT ドメイン、および各ドメインの主ドメインコントローラの名前を指定する
- **同期ユーザーリスト** : LDAP DIT とフィルタ情報を使用して、Directory Server、Active Directory、NT で同期させるユーザーを指定する
- **Sun Java System Directory Server** : 同期されるユーザーを格納する Directory Server インスタンスを指定する

コネクタと Directory Server プラグインのインストール

コネクタと Directory Server プラグインをインストールするときは、次の情報を指定する必要があります。

- **設定ディレクトリのホストとポート** : Identity Synchronization for Windows の設定情報が格納される設定 Directory Server インスタンスのホストとポートを指定する
- **ルートサフィックス** : 設定ディレクトリのルートサフィックスを指定する。コアのインストール時に指定したルートサフィックスを指定する
- **管理者の名前とパスワード** : 設定 Directory Server のクレデンシャルを指定する
- **設定パスワード** : 機密性のある設定情報を保護するための、セキュアなパスワードを指定する
- **ファイルシステムディレクトリ** : Identity Synchronization for Windows のインストール先を指定する。同じマシンにインストールされるすべてのコンポーネントは、同じインストールパスを持つ必要がある
- **ディレクトリソース** : インストールするコネクタまたはプラグインを使用するディレクトリソースを指定する

Directory Server コネクタと Windows NT コネクタをインストールする場合は、未使用のポートを指定する必要があります。

Directory Server コネクタとプラグインをインストールする場合は、コネクタまたはプラグインに対応する Directory Server のホスト、ポート、クレデンシャルを指定する必要があります。

コマンド行ユーティリティの使用

Identity Synchronization for Windows では、次のユーティリティを使用して、さまざまなタスクをコマンド行から実行できます。

- `idsync` スクリプトに次のサブコマンドを指定することで、Identity Synchronization for Windows のコマンド行ユーティリティを実行できる
  - `certinfo`: 設定と SSL 設定に基づく証明書情報を表示する
  - `changepw`: Identity Synchronization for Windows の設定パスワードを変更する
  - `prepds`: Identity Synchronization for Windows が使用できるように Sun Java System Directory Server ソースを準備する

- `printstat`: インストールされているコネクタ、システムマネージャ、Message Queue の状態を出力する

  `printstat` コマンドを使用して、インストールプロセスの完了に必要な、インストールと設定の残りの手順をリスト表示することもできる

- `resetconn`: 設定ディレクトリ内のコネクタの状態をアンインストール済みにリセットする (ハードウェアまたはアンインストーラに障害が発生した場合のみ)
- `resync`: 既存ユーザーの再同期とリンク設定を行い、インストールプロセスの一部としてディレクトリを事前に取り込む
- `startsync`: 同期を開始する
- `stopsync`: 同期を終了する

注 これらのユーティリティについては、付録 A を参照してください。

- Identity Synchronization for Windows 1.0 または 1.0 SP1 から Identity Synchronization for Windows 1 2004Q3 への移行には、次のユーティリティを使用する
  - `forcepwchg`: Identity Synchronization for Windows バージョン 1.0 からバージョン 1 2004Q3 への移行中にパスワードを変更したユーザーにパスワードの変更を要求する
  - `importcnf`: エクスポートされたバージョン 1.0 の設定 XML ドキュメントをインポートする

注 これらのユーティリティについては、第 7 章を参照してください。

インストールのチェックリスト

次のチェックリストは、インストールプロセスに役立ちます。Identity Synchronization for Windows のインストールを開始する前にこれを印刷し、次の情報を準備してください。

表 2-6 コアのインストール用チェックリスト

必要な情報	指定する内容
設定ディレクトリのホストとポート	
設定ディレクトリのルートサフィックス (dc=example,dc=com など)	
Identity Synchronization for Windows のインストール先ファイルシステムディレクトリ	
設定 Directory Server の管理者名とパスワード	
機密性のある設定情報を保護するためのセキュリティ用設定パスワード	
Message Queue インスタンスのポート番号	

表 2-7 コアの設定用チェックリスト

必要な情報	指定する内容
Active Directory グローバルカタログ (該当する場合)	
Directory Server スキーマサーバー	
Directory Server ユーザーの Structural および Auxiliary オブジェクトクラス	
同期させる属性	
ユーザーエントリ作成のフロー	
ユーザーエントリ変更のフロー	
ユーザーエントリの有効化と無効化のフロー	
ユーザーエントリ削除のフロー	
Sun Java System Directory Server ディレクトリソース	
Active Directory ディレクトリソース	
同期ユーザーリスト	

表 2-7　コアの設定用チェックリスト（続き）

必要な情報	指定する内容
Windows ソースフィルタ作成式	
Sun Java System ソースフィルタ作成式	

表 2-8　コネクタと Directory Server プラグインのインストール用チェックリスト

必要な情報	指定する内容
設定ディレクトリのホストとポート	
設定ディレクトリのルートサフィックス	
コネクタのインストール先ファイルシステムディレクトリ	
設定 Directory Server の管理者名とパスワード	
機密性のある設定情報を保護するためのセキュリティ用設定パスワード	
ディレクトリソース	
Directory Server と Windows NT 用の未使用のポート	
コネクタとプラグインに対応する Directory Server のホスト、ポート、クレデンシャル	

表 2-9　ユーザーのリンク用チェックリスト

必要な情報	指定する内容
リンクさせる同期ユーザーリスト	
一致によるユーザーの限定に使用される属性	
XML 設定ファイル	

表 2-10　再同期用チェックリスト

必要な情報	指定する内容
選択する同期ユーザーリスト	

表 2-10 再同期用チェックリスト (続き)

必要な情報	指定する内容
同期ソース	
対応するユーザーがターゲットディレクトリソースに見つからない場合、そのユーザーのエントリを自動的に作成するか ?	
Directory Server パスワードを無効化するか ?	
選択した SUL に存在し、指定した LDAP フィルタと一致するユーザーだけを同期させるか ?	

第 3 章

コアのインストール

この章では、Identity Synchronization for Windows のインストールプログラムの使用方法と、Identity Synchronization for Windows コアコンポーネントのインストール方法について説明します。

この章で説明する内容は次のとおりです。

はじめに

Identity Synchronization for Windows のインストールプロセスを開始する前に、次の事項を確認してください。

- 第 2 章「インストールの準備」を参照する。この章には、インストールの前提条件、チェックリスト、必要な管理権限などの重要情報が記載されている
- この製品には Java 実行時環境 (JRE) が含まれない。必要であれば、次のページで Java 開発キットをダウンロードできる

  `http://java.sun.com` または `http://www.java.com`

  Solaris または Windows 2000/2003 システムで Identity Synchronization for Windows インストールプログラムを実行するには、JRE 1.4.2_04 以降をインストールする必要がある
- **Windows システムだけに適用** : コアのインストール前に、開いているすべての「サービス」コントロールパネルウィンドウを閉じないと、インストールが失敗する

- マシンに Identity Synchronization for Windows バージョン 1.0 (または 1.0 SP1) がインストールされている場合は、第 7 章「Identity Synchronization for Windows 1 2004Q3 への移行」を参照する

注

Identity Synchronization for Windows 1.0 以外のアプリケーションが `SUNWjss` パッケージを使用するように登録されていない場合、Identity Synchronization for Windows 1.0 のアンインストールプログラムは、このパッケージを削除します。特に、Directory Server 5.2.2 の zip バージョンをインストールした Solaris 環境では、このような状況が生じる可能性があります。この場合、アンインストールプログラムは `/usr/share/lib/mps/secv1` から `jss3.jar` を削除します。

Identity Synchronization for Windows 1 2004Q3 への移行時にこのような状況が生じた場合、インストーラは必要ファイルが不足していることを示すメッセージを表示し、インストールログにファイル名を記録します。このエラーが発生したときは、必要なパッチ (55 ページの「Sun Java System ソフトウェアの要件」を参照) を再インストールしてからインストールプロセスをやり直してください。

- Identity Synchronization for Windows バージョン 1.0 では、Message Queue が自動的にインストールされたが、バージョン 1 2004Q3 ではインストールされない。事前に Message Queue 3.5 SP1 Enterprise Edition をインストールしておく必要がある

  Solaris システムだけに適用 : Message Queue と Identity Synchronization for Windows を同じディレクトリにインストールすることはできない

インストールプログラムの起動

ここでは、Identity Synchronization for Windows のインストールプログラムを次のプラットフォームでダウンロード、展開 (解凍)、実行する方法について説明します。

- 85 ページの「Solaris SPARC 環境」
- 85 ページの「Solaris x86 環境」
- 86 ページの「Windows 環境」

Solaris SPARC 環境

Solaris SPARC オペレーティングシステムで Identity Synchronization for Windows のインストールプログラムを準備および実行する手順は、次のとおりです。

1. ルートとしてログインします。
2. **# mkdir isw12004Q3** と入力して新しいディレクトリを作成し、そのディレクトリに移動します (**cd**)。
3. 製品のバイナリファイル (isw-12004Q3.sparc-sun-solaris.tar.gz) をインストールディレクトリにダウンロードしていない場合は、ダウンロードします。
4. 次のコマンドを使用して、製品のバイナリファイルを展開します。

   # gunzip -dc isw-12004Q3.sparc-sun-solaris.tar.gz | tar -xvof -

5. isw12004Q3 ディレクトリから installer ディレクトリに移動し、**./runInstaller.sh** と入力してインストールプログラムを実行します。

注 インストールプログラムをテキストベースモードで実行するには、次のように入力します。

./runInstaller.sh -nodisplay

runInstaller.sh プログラムを実行した場合、パスワードがクリアテキストとしてエコーされないように、Identity Synchronization for Windows はパスワードを自動的にマスクします。

Solaris x86 環境

Solaris x86 オペレーティングシステムで Identity Synchronization for Windows のインストールプログラムを準備および実行する手順は、次のとおりです。

1. ルートとしてログインします。
2. **# mkdir isw12004Q3** と入力して新しいディレクトリを作成し、そのディレクトリに移動します (**cd**)。
3. 製品のバイナリファイル (isw-12004Q3.x86-sun-solaris.tar.gz) をダウンロードしていない場合は、インストールディレクトリにダウンロードします。
4. 次のコマンドを使用して、製品のバイナリファイルを展開します。

   # gunzip -dc isw-12004Q3.x86-sun-solaris.tar.gz | tar -xvof -

5. isw12004Q3 ディレクトリから installer ディレクトリに移動し、**./runInstaller.sh** と入力してインストールプログラムを実行します。

注 インストールプログラムをテキストベースモードで実行するには、次のように入力します。

```
./runInstaller.sh -nodisplay
```

runInstaller.sh プログラムを実行した場合、パスワードがクリアテキストとしてエコーされないように、Identity Synchronization for Windows はパスワードを自動的にマスクします。

Windows 環境

Windows オペレーティングシステムで Identity Synchronization for Windows のインストールプログラムを準備および実行する手順は、次のとおりです。

1. 管理者としてログインします。
2. **# mkdir isw12004Q3** と入力し、新しいディレクトリを作成します。
3. isw12004Q3 ディレクトリに移動します (**cd**)。
4. 製品のバイナリファイル (isw-12004Q3-windows.zip) をダウンロードしていない場合は、インストールディレクトリにダウンロードします。
5. isw-12004Q3-windows.zip ファイルを空のディレクトリで解凍します。
6. isw12004Q3 ディレクトリから installer ディレクトリに移動し (**cd**)、**setup.exe** と入力してインストールプログラムを実行します。

   Identity Synchronization for Windows のインストールウィザードが表示されます。

注 コアは管理サーバーのルートにインストールされるため、ウィザードの一部のパネルでは、インストールに必要なほとんどの情報 (ディレクトリパスや名前など) が Identity Synchronization for Windows によって自動的に検出され、フィールドに入力されます。

情報が不足していたり、誤っていたりする場合は、必要な情報を手動で入力できます。

次の節では、コアのインストール方法について説明します。

コアのインストール

ここでは、Solaris と Windows の両方のオペレーティングシステムに Identity Synchronization for Windows コアをインストールする手順について説明します。

コアをインストールする前に、次の要件に注意してください。

- **Solaris システムだけに適用** : Solaris サービスをインストールおよび実行するには、ルート権限が必要である。

  注 プログラムのインストールはルートとして実行する必要がありますが、インストールの完了後は、ルート以外のユーザーとして Solaris サービスを実行できるようにソフトウェアを設定できます。付録 C「Solaris でのルート以外のユーザーによるサービスの実行」を参照してください。

- **Windows 2000/2003 システムだけに適用** : Identity Synchronization for Windows をインストールするには、管理者権限が必要である
- コアは、管理サーバー (バージョン 5 2004Q2 以降) によって管理される既存のサーバールートを持つディレクトリにインストールする必要がある。それ以外の場合、インストールプログラムは失敗する。管理サーバーは、Directory Server 5 2005Q1 のインストールプログラムを使用してインストールできる

インストールウィザードを使用して、Identity Synchronization for Windows コアコンポーネントを次のようにインストールします。

1. 「ようこそ」画面が表示されたら、そこに示される情報を読み、「次へ」をクリックして「ソフトウェアライセンス契約書」パネルに進みます。
2. ライセンス契約書を読み、次のいずれかを選択します。
   - **はい (ライセンス契約書に同意する)**: ライセンスの条項に同意し、次のパネルに移動する
   - **いいえ** : セットアッププロセスを中止し、インストールプログラムを終了する
3. 「設定ディレクトリの位置」パネル (図 3-1) が表示されるので、設定ディレクトリの位置を指定します。

図 3-1　　設定ディレクトリの位置の指定

次の情報を指定します。

- **設定ディレクトリホスト** : Identity Synchronization for Windows の設定情報が格納される Sun Java System Directory Server インスタンス (管理サーバーに属する) の完全修飾ドメイン名を入力する

  ローカルマシン上のインスタンス、または別のマシンで稼動するインスタンスを指定できる

注	無効なクレデンシャルやホスト名の警告を回避するために、インストールプログラムが稼動するマシンに DNS 解決できるホスト名を指定してください。

- **設定ディレクトリポート** : 設定ディレクトリがインストールされているポートを指定する。デフォルトポートは *389*

  セキュリティ保護された通信を有効にするには、「セキュアポート」オプションにチェックマークを付け、SSL ポートを指定する。デフォルトの SSL ポートは *636*

  設定ディレクトリで SSL が有効であることを一度プログラムが検出すると、Identity Synchronization for Windows のすべてのコンポーネントは設定ディレクトリとの通信に SSL を使用するようになる

注 設定 Directory Server に送信する前に、Identity Synchronization for Windows は、機密性のある設定情報を暗号化します。

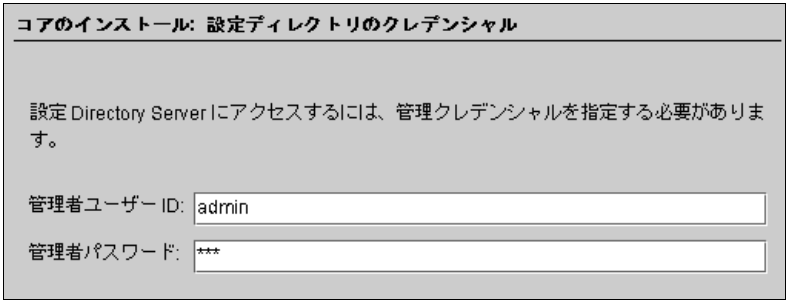
ただし、コンソールと設定ディレクトリの間に転送の暗号化を追加する場合は、管理サーバーと設定 Directory Server の両方で SSL を有効にします。次に、Directory Server コンソールを認証させる管理サーバーとの間に安全な接続を設定します。詳細については『Sun Java System Administration Server 5 2005Q1 Administration Guide』を参照してください。

- **設定ルートサフィックス** : Identity Synchronization for Windows の設定情報の格納先となるルートサフィックスをメニューから選択する

注 プログラムがルートサフィックスを検出できず、情報を手動で入力する必要がある場合、またはデフォルト値を変更する場合は、「更新」をクリックし、ルートサフィックスのリストを再生成する必要があります。設定 Directory Server 上に存在するルートサフィックスを指定してください。

4. 「次へ」をクリックし、「設定ディレクトリのクレデンシャル」パネルを開きます。

図 3-2 管理者のクレデンシャルを入力します。

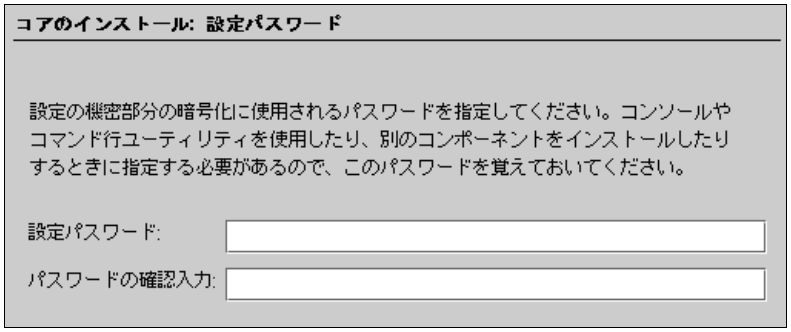


5. 設定ディレクトリの管理ユーザー ID とパスワードを入力します。
   - ユーザー ID として `admin` を指定した場合は、ユーザー ID を DN として指定する必要はない
   - それ以外のユーザー ID を指定した場合は、ID を完全 DN として指定する必要がある
     たとえば、*cn=Directory Manager* のように指定する

注 設定ディレクトリとの通信に SSL を使用しない場合 (88 ページの手順 3 を参照)、これらのクレデンシャルは暗号化されずに送信されます。

6. 操作が完了したら、「次へ」をクリックして「設定パスワード」パネルを開きます。

図 3-3 設定パスワードを入力します。



7. クレデンシャルのように機密性のある設定情報を暗号化するときに使用されるパスワードを入力し、同じ内容をもう一度入力することでそれを確認する必要があります。完了したら「次へ」をクリックします。

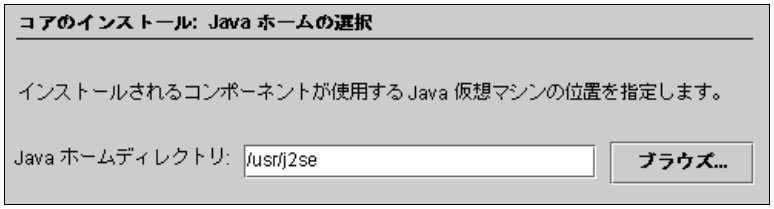
注 次の処理を行う場合に必要となるため、このパスワードを覚えておいてください。

- Identity Synchronization for Windows コンソールにアクセスする
- 設定を作成または編集する
- コンポーネントをインストールする
- コマンド行ユーティリティを実行する

設定パスワードの変更については、313 ページの「changepw の使用」を参照してください。

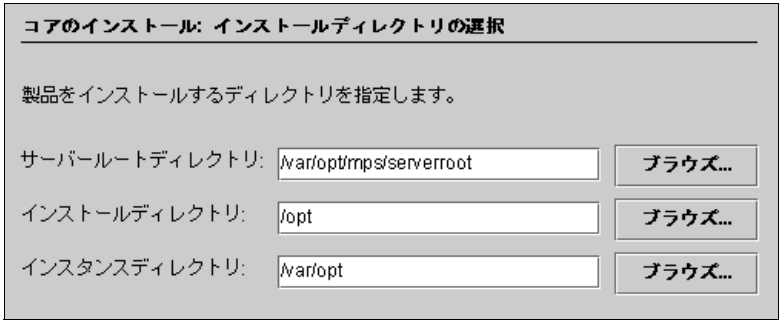
「Java ホームを選択します」パネル (図 3-4) が表示されます。インストールしたコンポーネントが使用する Java 仮想マシンのディレクトリ位置が自動的に挿入されます。

図 3-4　　Java ホームディレクトリの指定



8. Java ホームディレクトリが JDK/JRE 1.4.2_04 以降であることを確認します。
   - 指定した位置が正しければ、「次へ」をクリックして「インストールディレクトリの選択」パネル (91 ページの図 3-5) に進む
   - 指定された位置に誤りがある場合は、「ブラウズ」ボタンをクリックし、Java がインストールされているディレクトリを検索して選択する。たとえば、次のようなディレクトリを指定する
     - **Solaris 環境** : `/var/java`
     - **Windows 環境** : `C:¥Program Files¥j2sdk1.4.2_04`

図 3-5　　インストールディレクトリの指定



9. 表示されるテキストフィールドに次の情報を入力するか、「ブラウズ」をクリックして使用できるディレクトリを検索し、選択します。
   - **サーバールートディレクトリ** : Directory Server のインストールサーバールートのパスとディレクトリ名を指定する。コンソールはここにインストールされる

> **注**　　Windows オペレーティングシステムで使用できるサーバールートディレクトリは 1 つだけであるため、すべての製品はここにインストールされます。

- **インストールディレクトリ** (コアを Solaris 環境にインストールする場合にだけ適用): インストールディレクトリのパスとディレクトリ名を指定する。コアバイナリ、ライブラリ、実行可能ファイルは、このディレクトリにインストールされる
- **インスタンスディレクトリ** (コアを Solaris 環境にインストールする場合にだけ適用): インスタンスディレクトリのパスとディレクトリ名を指定する。ログファイルなど、変化する設定情報は、このディレクトリに格納される

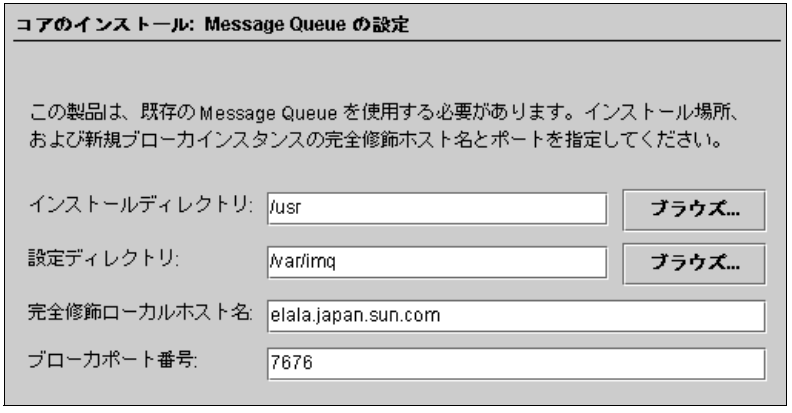
10. 「次へ」をクリックし、「Message Queue の設定」パネルに進みます。

注 Identity Synchronization for Windows のインストールを開始する前に、Message Queue 3.5 SP1 Enterprise Edition をインストールしておく必要があります。

Solaris システムだけに適用 : Message Queue と Identity Synchronization for Windows を同じディレクトリにインストールしないでください。

Windows システムだけに適用 : コアのインストールを継続する前に、開いているすべての「サービス」コントロールパネルウィンドウを閉じないと、コアのインストールは失敗します。

図 3-6 Message Queue の設定



11. 表示されるテキストフィールドに次の情報を入力するか、「ブラウズ」をクリックして使用できるディレクトリを検索し、選択します。
    - **インストールディレクトリ** : Message Queue インストールディレクトリのパスを指定する

- **設定ディレクトリ** : Message Queue インスタンスディレクトリのパスとディレクトリ名を指定する
- **完全修飾ローカルホスト名** : ローカルホストマシンの完全修飾ドメイン名 (FQDN) を指定する。1 つのホストで稼動できる Message Queue ブローカインスタンスは 1 つだけである
- **ブローカポート番号** : Message Queue ブローカが使用する未使用のポート番号を指定する。デフォルトポートは *7676*

12. 「次へ」をクリックし、「インストール準備完了」パネルを表示します。

    このパネルには、コアのインストール先ディレクトリや、コアのインストールに必要なディスク容量など、インストールに関する情報が表示されます。

    - 表示される情報が正しければ、「すぐにインストール」をクリックしてコアコンポーネントをインストールする。バイナリ、ファイル、パッケージはここにインストールされる
    - 情報に誤りがある場合は、「戻る」をクリックして変更を加える

    「インストールしています」というメッセージが表示され、すぐに「コンポーネントの設定」パネルが表示されます。インストールプログラムは、指定した設定 Directory Server に設定データを追加します。この動作には次の処理が含まれます。

    - Message Queue ブローカインスタンスの作成
    - 設定ディレクトリへのスキーマのアップロード
    - 設定ディレクトリへの配備固有の設定情報のアップロード

    この処理の完了には数分間かかり、断続的に中断されることもあります。10 分が経過しても処理が完了しないような場合を除き、特に気にする必要はありません。インストールプログラムの状況は、進捗状況バーで監視できます。

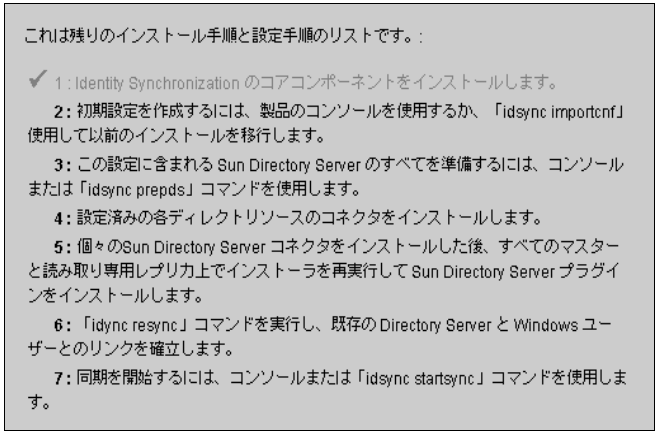
13. コンポーネントの設定が完了すると、Identity Synchronization for Windows が正しくインストールされたことを示す「インストール概要」パネルが表示されます。

    「詳細」ボタンをクリックすると、インストールされたファイルとその位置がリスト表示されます。

14. 「次へ」をクリックすると、Identity Synchronization for Windows のインストールと設定の完了に必要な残りの手順が、プログラムによって特定されます。

    「読み込んでいます」というメッセージが表示され、それに続いて「残りのインストール手順」パネルが次々と表示されます。すべての手順パネルが表示された後に、次に示すパネル (図 3-7) が表示されます。このパネルには、インストールと設定の残りの手順を示す実行手順リストが表示されます。コンソールの「状態」タブからこのパネルを表示することもできます。

図 3-7　Identity Synchronization for Windows の実行手順リスト

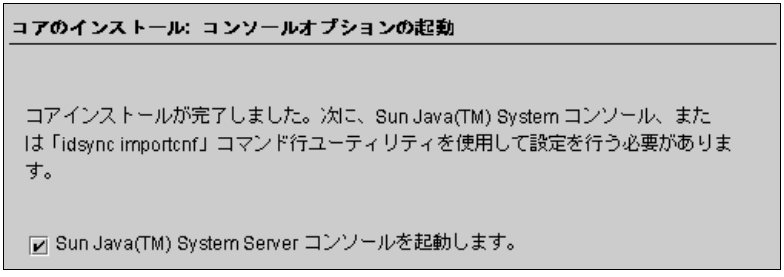


実行手順を示すパネルは、インストールと設定のプロセス全体で繰り返し表示されます。完了した手順は、リスト上でグレイ表示されます。

この時点では、実行手順リストには汎用の手順が表示されます。設定を保存すると、その配備に適した手順 (たとえば、適切なコネクタのインストールなど) が表示されます。

15. 手順のリストを確認したら、「次へ」をクリックします。コアのインストールが完了したことを示す「コンソールオプションの起動」パネルが表示されます。

図 3-8　コンソールの起動



16. 次に、Sun Java System コンソールからコアコンポーネントをインストールします。「Sun Java System コンソールを起動します」オプションには、デフォルトでチェックマークが付けられています。

Identity Synchronization for Windows 1.0 または SP1 から Identity Synchronization for Windows 1 2004Q3 への移行では、コマンド行ユーティリティ `idsync importcnf` を使用して 1.0 または SP1 の設定を XML ドキュメントとしてエクスポートし、それをインポートすることができます。手順については、第 7 章「Identity Synchronization for Windows 1 2004Q3 への移行」を参照してください。

17. 「終了」をクリックします。
18. コンソールの使用を選択した場合は、「Sun Java System コンソールログイン」ダイアログボックス (図 3-9) が表示されます。

図 3-9 コンソールへのログイン

コンソールにログインするには、次の情報を指定する必要があります。

- **ユーザー ID** : マシンに管理サーバーをインストールしたときに指定した管理者ユーザー ID を入力する
- **パスワード** : 管理サーバーのインストール時に指定した管理者パスワードを入力する
- **管理 URL** : 管理サーバーの現在の URL を次の形式で入力する

  http://<*hostname.your_domain.domain:port_number*>

  ここで

  - *hostname.your_domain.domain* は管理サーバーのインストール時に選択したコンピュータホスト名
  - *port_number* は管理サーバーに指定したポートの番号

19. クレデンシャルを指定したら、「了解」をクリックしてダイアログボックスを閉じます。
20. 設定パスワードの入力が求められます。パスワードを入力し、「了解」をクリックします。

Sun Java System サーバーコンソールウィンドウが表示され、コアを設定できるようになります。インストール方法については、次の第 4 章「コアリソースの設定」を参照してください。

第 4 章

コアリソースの設定

Identity Synchronization for Windows コアをインストールしたら (第 3 章を参照)、コアリソースの初期設定を直ちに行う必要があります。

この章では、コンソールを使用してこれらのリソースを追加、設定する方法について説明します。この章で説明する内容は次のとおりです。

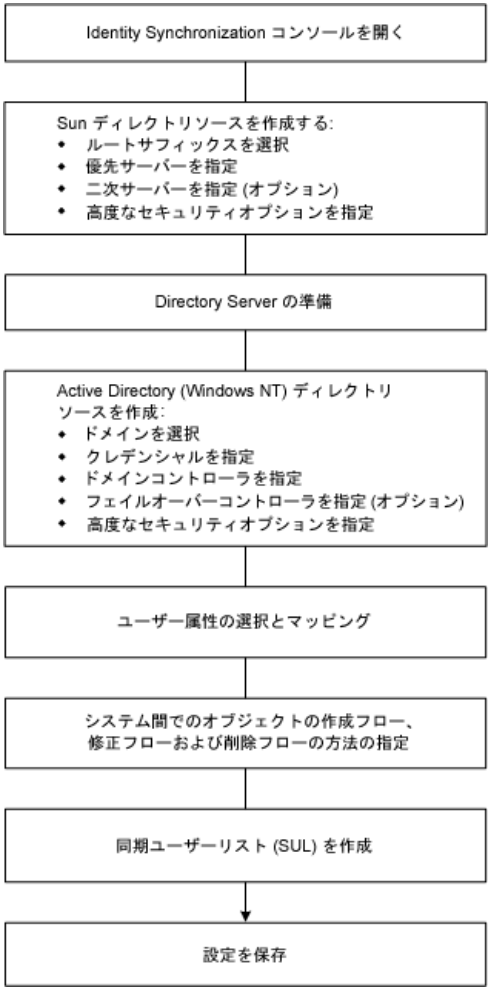
注 コアリソースを効率的に設定するには、Directory Server と Active Directory を設定、操作する方法を理解している必要があります。

これらのリソースは、特に指定されていない限り特定の順序で設定する必要はありません。しかし、製品に習熟するまでは、この章で説明する順序で設定を行うほうが時間の節約となり、エラーも防止できます。

設定の概要

図 4-1 は、配備に必要なコアリソースを設定する手順を示しています。

図 4-1 配備に必要なコアリソースの設定



Identity Synchronization for Windows コンソールの起動

注	Sun Java System サーバーコンソールにログインしていない場合は、95 ページを参照し、ログインしてください。

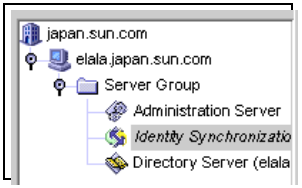
Sun Java System サーバーコンソールウィンドウ (図 4-2) には、管理の対象となるすべてのサーバーとリソースが表示され、システムに関する情報が示されます。

図 4-2　Sun Java System サーバーコンソール

Identity Synchronization for Windows コンソールを起動するには

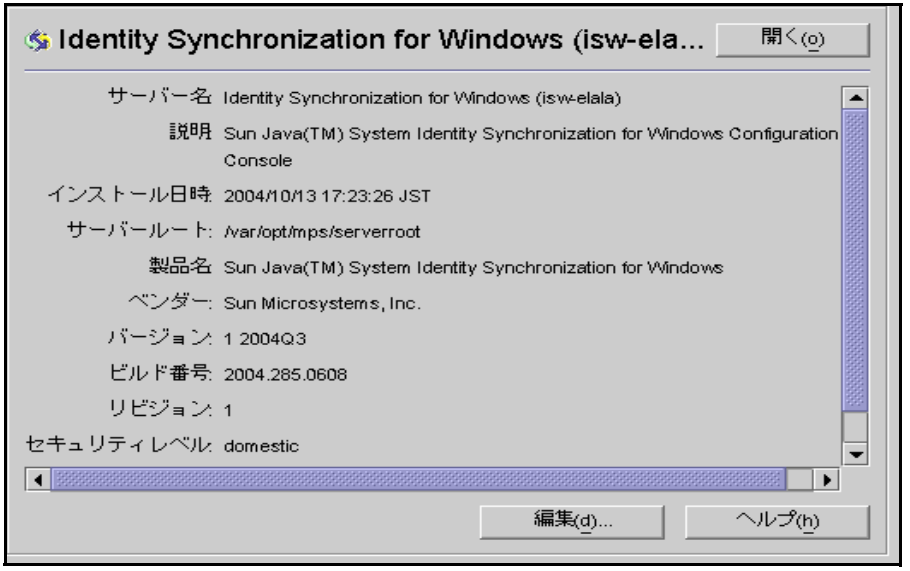
1. 「サーバーとアプリケーション」タブで、Identity Synchronization for Windows インスタンスが属するサーバーグループを含むナビゲーションツリーからホスト名のノードを選択します。
2. サーバーグループのノードを展開し、Identity Synchronization for Windows ノードを選択します (図 4-3 を参照)。

図 4-3　サーバーグループの展開



情報パネルの内容が、Identity Synchronization for Windows とシステムに関する情報に切り替わります (図 4-4 を参照)。

図 4-4　Identity Synchronization for Windows の情報パネル



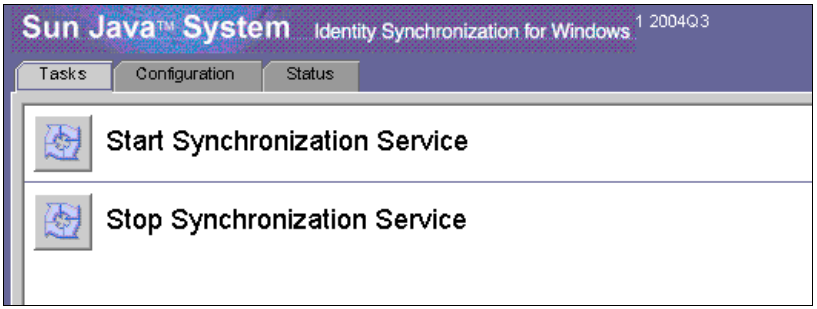
3. パネルの右上端にある「開く」ボタンをクリックします。

注	パネルの下部にある「編集」ボタンをクリックすると、サーバー名と説明を編集できます。

4. コアのインストール時に指定した設定パスワード (90 ページを参照) の入力が求められます。パスワードを入力し、「了解」をクリックします。

   次のような Identity Synchronization for Windows コンソールが表示されます。

図 4-5　Identity Synchronization for Windows コンソールの「タスク」タブ



このウィンドウには、3 つのタブとステータスバーが含まれます。

- **タスク** (デフォルト): Sun と Windows のシステム間で同期を開始および終了するときは、このタブを使用する。サービスの開始と停止については、第 6 章「既存ユーザーの同期」を参照

  注　同期サービスの開始と停止を Windows サービスの開始と停止と混同しないように注意してください。

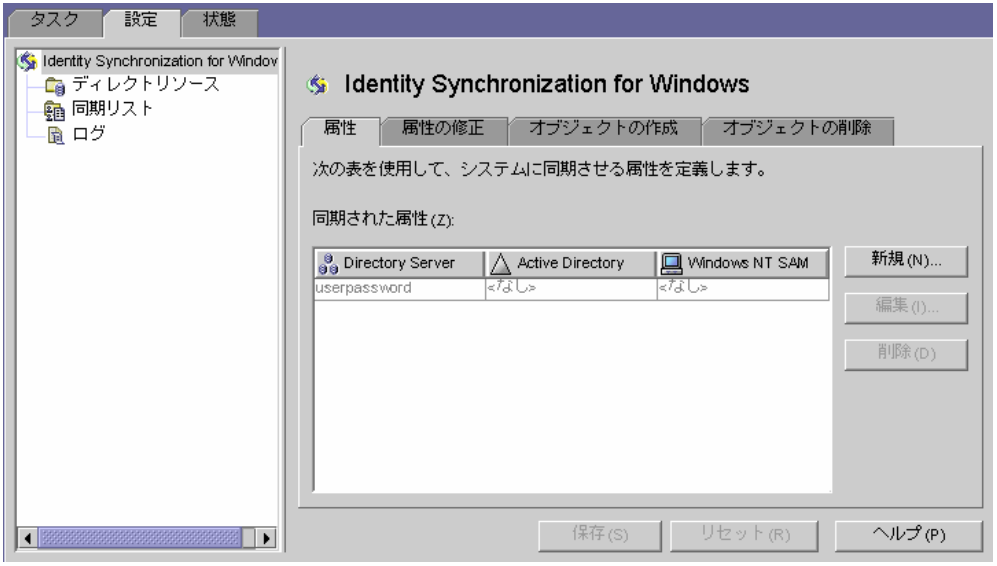
  Windows サービスを開始または停止するときは、Windows の「スタート」から「プログラム」>「管理ツール」>「コンピュータの管理」>「サービス」にアクセスする必要があります。

- **設定** : 同期をシステムに設定するときは、このタブを使用する
- **状態** : このタブは、次の操作に使用する
  - コネクタなどのシステムコンポーネントの状態を監視する
  - 設定時および同期時に Identity Synchronization for Windows が生成する監査ログとエラーログを表示する
  - インストールと設定の実行手順リストの更新とチェックを行う
  - **ステータスバー** : ここには、システムの状態が簡潔に示される

  注　「状態」タブについては、第 10 章を参照してください。

5. 「設定」タブ (図 4-6) を選択します。

図 4-6　Identity Synchronization for Windows コンソールの「設定」タブ



「設定」タブは、次のタブから構成されます。

- **属性** : システム間で同期させる属性を指定するときは、このタブを使用する
- **属性の修正** : パスワードと属性の変更、およびオブジェクトの無効化がシステム間でどのように伝達されるかを指定するときは、このタブを使用する
- **オブジェクトの作成** : 新規作成されたパスワードと属性がシステム間でどのように伝達されるかを指定するとき、および同期時に Identity Synchronization for Windows が生成するオブジェクトの初期値を指定するときは、このタブを使用する
- **オブジェクトの削除** : パスワードおよびその他の属性の削除がシステム間でどのように伝達されるかを指定するときは、このタブを使用する

少なくとも 1 つの Sun Java System Directory Server ディレクトリソース、および 1 つの Windows サーバーディレクトリソース (Active Directory または Windows NT) を設定する必要があります。方法については、次の節を参照してください。

ディレクトリソースの作成

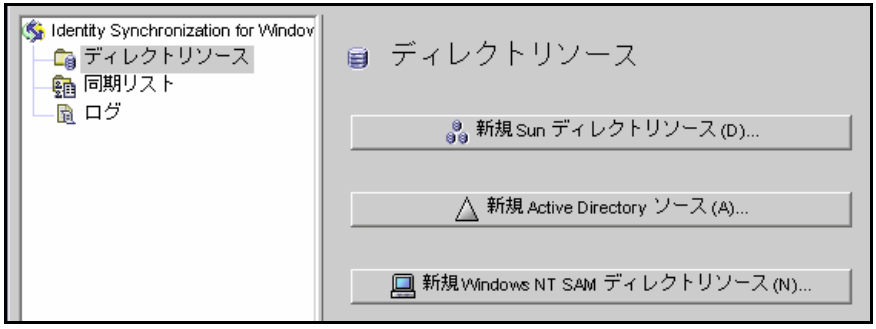
ディレクトリソースは、次の順序で作成する必要があります (どのソースを同期させるかによっても異なる)。

1. 104 ページの「Sun Java System ディレクトリソースの作成」
2. 111 ページの「Directory Server の準備」
3. 115 ページの「Active Directory ソースの作成」
4. 124 ページの「Windows NT SAM ディレクトリソースの作成」

注 少なくとも 1 つの Sun Java System ディレクトリソースと、1 つの Windows ディレクトリソース (Active Directory、NT SAM、または両方) を設定する必要があります。

ナビゲーションツリーでディレクトリソースのノードを選択して「ディレクトリソース」パネル (図 4-7) を表示します。

図 4-7 「ディレクトリソース」パネルの表示



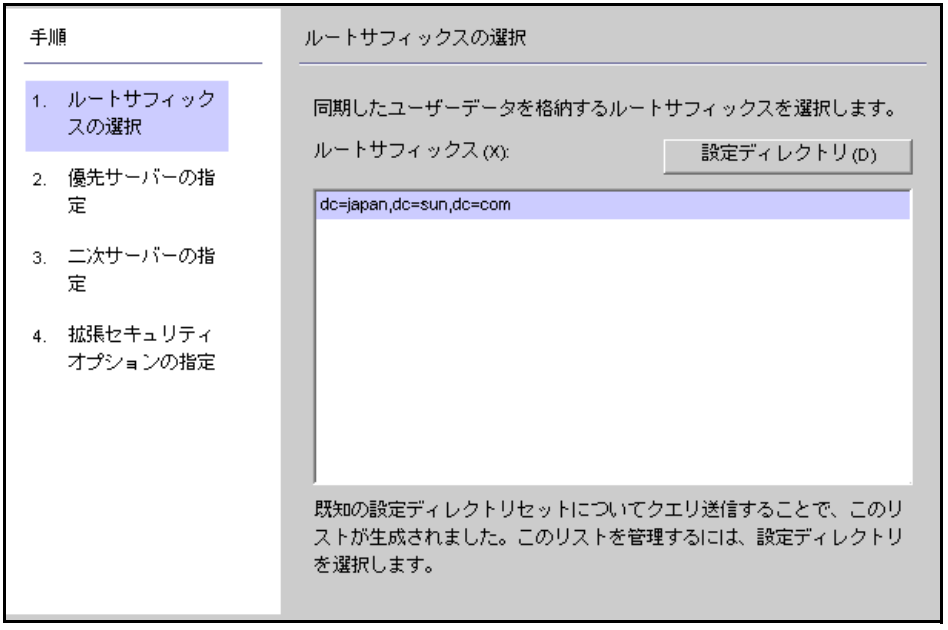
Sun Java System ディレクトリソースの作成

注 それぞれの Sun Java System ディレクトリソースは、コネクタ、および最大で 4 つのマスターから構成されるレプリケーション環境に配備できるプラグインセットと関連付けられています。どの Directory Server プラグインも、Windows ディレクトリソースからのパスワード妥当性チェックを処理することができ、ユーザーはどのマスターでもパスワードを変更できます。ただし、Directory Server コネクタが Windows ディレクトリソースからのデータ変更を同期させることができるマスターは、優先マスターと二次マスターの 2 つだけです。Directory Server レプリケーションは、これら 2 つのいずれかのマスターからの変更を、トポロジ内の他のサーバーにレプリケートします。

新しい Sun Java System ディレクトリソースを作成する手順は、次のとおりです。

1. 「新規 Sun ディレクトリソース」ボタンをクリックして、「Sun Java System ディレクトリソースの定義」ウィザードを起動します。

図 4-8 ルートサフィックスの選択



プログラムは既知の設定ディレクトリソースのセットを照会し、リストパネルに既存のルートサフィックス (ネーミングコンテキストとも呼ばれる) を表示します。

デフォルトでは、プログラムは製品がインストールされている設定ディレクトリを認識し、リストパネルにはその設定ディレクトリが認識するルートサフィックスが表示されます。

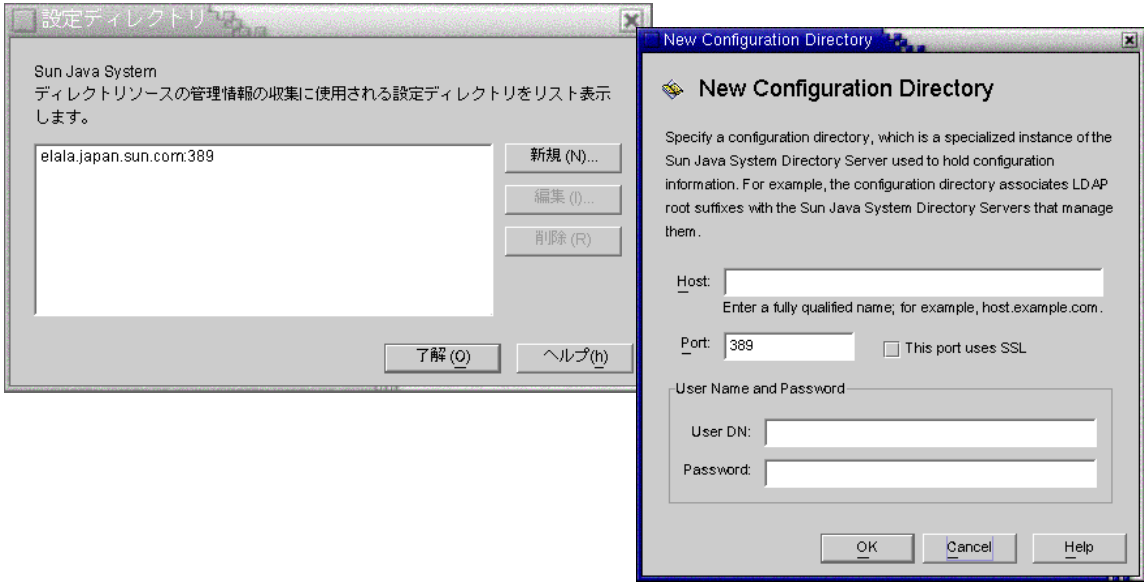
2. リストパネルで、管理するユーザーが属するルートサフィックスを選択します。複数のルートサフィックスが表示される場合は、ユーザーが属するルートサフィックスを 1 つ選択します。「次へ」をクリックし、手順 3 に進みます。

   同期させるルートサフィックスが、Identity Synchronization for Windows に登録されている設定ディレクトリによって認識されない場合は、次の方法で新しい設定ディレクトリを指定する必要があります。

   a. 「設定ディレクトリ」ボタンをクリックし、新しい設定ディレクトリを指定します。

   b. 「設定ディレクトリ」ダイアログボックス (図 4-9) が表示されるので、「新規」ボタンをクリックして「新規設定ディレクトリ」ダイアログボックスを開きます。

図 4-9　　新しい設定ディレクトリの選択



   c. 次の情報を入力し、「了解」をクリックします。変更内容が保存され、ダイアログボックスが閉じます。

- **ホスト** : 完全修飾ホスト名を入力する

  たとえば、**machine1.example.com** のように指定する

- **ポート** : 有効な未使用の LDAP ポート番号を入力する。デフォルトは 389

  Identity Synchronization for Windows が設定ディレクトリとの通信に SSL (Secure Socket Layer) を使用する場合は、「このポートに SSL を使用する」ボックスにチェックマークを付ける

- **ユーザー DN** : 管理者の (バインド) 識別名を入力する

  たとえば、次のように指定する

  uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot

- **パスワード** : 管理者のパスワードを入力する

ウィザードは指定された設定ディレクトリにクエリを送信し、そのディレクトリが管理するすべてのディレクトリサーバーを特定します。

注 1 つの Sun Java System Directory Server ソースについて Identity Synchronization for Windows がサポートするルートサフィックスは 1 つだけです。

注 **設定ディレクトリの編集と削除**

「設定ディレクトリ」ダイアログボックスを使用して、設定ディレクトリのリストを次のように管理することもできます。

- リストパネルから設定ディレクトリを選択し、「編集」ボタンをクリックする。「設定ディレクトリの編集」ダイアログが表示され、ホスト、ポート、セキュアポート、ユーザー名、パスワードの各パラメータを変更できる
- リストパネルから設定ディレクトリを選択して「消去」をクリックすると、そのディレクトリがリストから削除される

d. 「了解」をクリックして「設定ディレクトリ」ダイアログボックスを閉じます。リストパネルには、新たに選択した設定ディレクトリのルートサフィックスが表示されます。

Directory Server が作成するルートサフィックスのプレフィックスは、デフォルトではマシンの DNS ドメインエントリのコンポーネントと対応します。構文は次のとおりです。

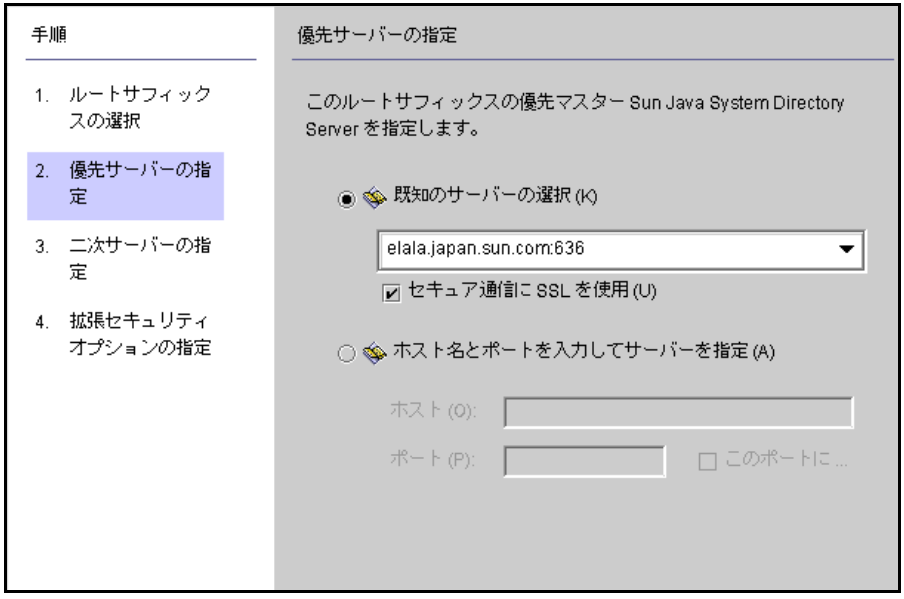
dc=< マシンの DNS ドメイン名 >

つまり、マシンのドメインが *example.com* であれば、サーバーのサフィックスを `dc=example, dc=com` のように設定します。選択したサフィックスによって命名されるエントリは、ディレクトリ内に事前に存在する必要があります。

e. ルートサフィックスを選択し、「次へ」をクリックします。

「優先サーバーの指定」パネル (図 4-10) が表示されます。

図 4-10　　優先サーバーの指定



Identity Synchronization for Windows は、Directory Server マスターに加えられた変更の検出に優先 Directory Server を使用します。優先サーバーは、Windows システムで加えられた変更が Sun Java System ディレクトリシステムに適用される際の一次場所としても機能します。

優先サーバーに障害が発生した場合は、優先サーバーがオンライン状態に復帰するまで二次サーバーに変更を格納できます。

3. 次のいずれかの方法で、優先サーバーを選択します。

   - 「既知のサーバーの選択」ボタンを有効にし、ドロップダウンリストからサーバー名を選択する

     注 リストに表示される Directory Server は、稼動している必要があります。
     サーバーが一時的にダウンしている場合は、「ホスト名とポートを入力してサーバーを指定」ボタンを有効にし、サーバー情報を手動で入力します。

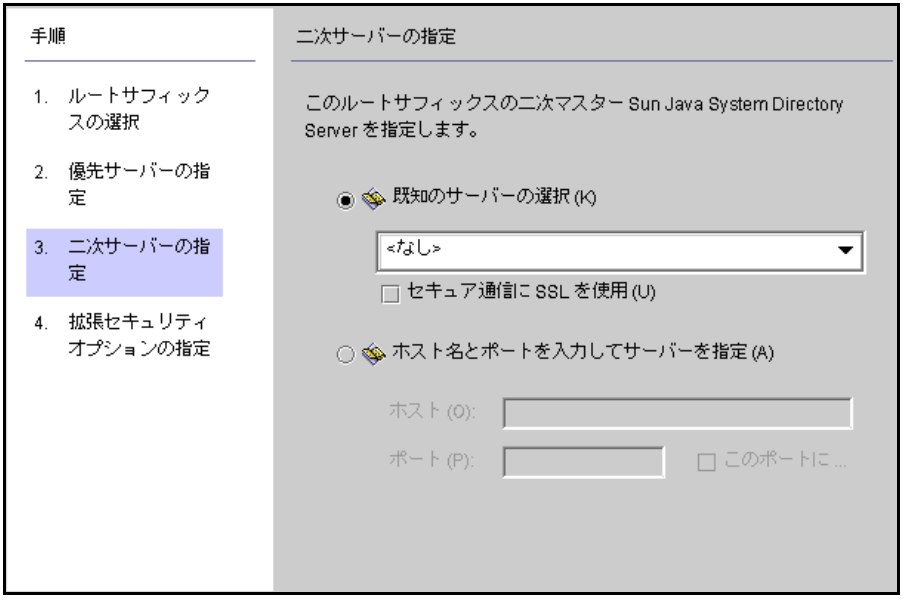
     Directory Server が通信に SSL を使用するように設定するときは、「セキュア通信に SSL を使用」ボックスを有効にする。ただし、この機能を有効にした場合は、インストールの完了後に追加の設定手順が必要となる。詳細については、294 ページの「Directory Server での SSL の有効化」を参照

   - 「ホスト名とポートを入力してサーバーを指定」ボタンを有効にし、対応するテキストフィールドにサーバーのホスト名とポート番号を入力する

     指定したポートが SSL を使用する場合は、「このポートに SSL を使用する」ボックスにチェックマークをつける

4. 「次へ」をクリックして「二次サーバーの指定」パネルを表示します。

図 4-11 二次サーバーの指定



- 優先サーバーの指定手順と同様に、ドロップダウンリストからサーバー名を選択するか、情報を手動で入力して二次 Directory Server を指定し、「次へ」をクリックする

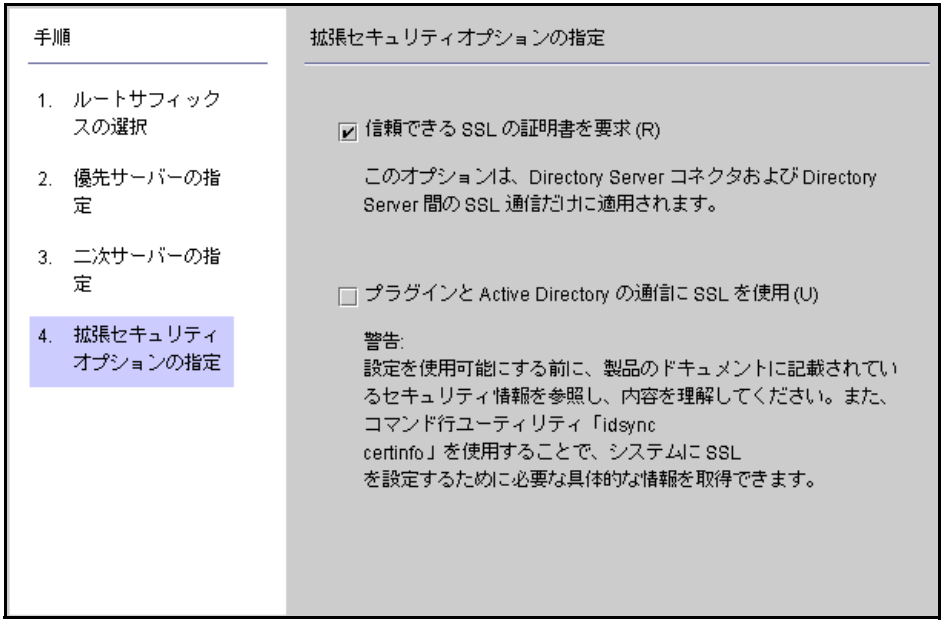
注	稼動していない Directory Server はドロップダウンリストに表示されません。サーバーが一時的にダウンしている場合は、サーバー情報を手動で入力してください。

- 二次サーバーを使用しない場合は、情報を指定せずに「次へ」ボタンをクリックする

注	• Sun ディレクトリソースの優先サーバーと二次サーバーには、同一ホスト名、同一ポートを使用しない • セキュアポート機能を有効にした場合は、インストールの完了後に追加の設定手順が必要となる。詳細については、294 ページの「Directory Server での SSL の有効化」を参照

次のような「拡張セキュリティオプションの指定」パネルが表示されます。

図 4-12　拡張セキュリティオプションの指定



インストールプロセスの一部として、ユーザーがバインドする、またはパスワードが変更される Directory Server ごとに Directory Server プラグインをインストールする必要があります。

Directory Server プラグインがパスワードと属性を Active Directory と同期させる場合、ユーザーとそのパスワードを検索するために、プラグインは Active Directory にバインドする必要があります。また、プラグインはセントラルログと Directory Server のログにログメッセージを書き込みます。デフォルトでは、これらの通信には SSL は使用されません。

5. SSL 通信を使用する場合は、表示される警告をよく読み、次のいずれか、または両方のオプションを有効にします。

   - チャネル通信だけを暗号化する場合、またはチャネル通信を暗号化し、証明書を使用して Directory Server と Directory Server コネクタの間で関係する各要素のアイデンティティを確実に検証するには、「SSL の証明書を要求」または「信頼できる SSL の証明書を要求」ボックスにチェックマークを付ける

     証明書を信頼しないときは、チェックマークを外す

   - Directory Server プラグインと Active Directory の間の通信に SSL を適用するには、「プラグインと Active Directory の通信に SSL を使用」ボックスにチェックマークを付ける

   注

   - これらの機能を有効にした場合は、インストール後に追加手順を実行する必要がある。詳細については、第 11 章「セキュリティの設定」を参照
   - 各 Directory Server プラグイン、コネクタ、または両方の証明書データベースに追加する必要のある証明書は、`idsync certinfo` コマンド行ユーティリティを使用して特定できる。313 ページの「certinfo の使用」を参照
   - 優先および二次 Directory Server がマルチマスターレプリケーション (MMR) 配備の一部である場合の追加設定については、付録 E「レプリケーション環境でのインストールに関する注意」を参照

6. 「拡張セキュリティオプションの指定」パネルの設定が完了したら、「終了」をクリックします。

   ナビゲーションツリーのディレクトリソースの下に選択したディレクトリソースが追加され、「Directory Server の準備を直ちに行いますか ?」ダイアログが表示されます。

Identity Synchronization for Windows が使用できるように、Directory Server を準備する必要があります。このタスクを直ちに実行するか、あとから実行するかを選択できますが、Directory Server の準備は、コネクタのインストール前に完了する必要があります。コネクタのインストール方法については、第 5 章で説明します。

- Directory Server の準備を直ちに行う場合は「はい」をクリックしてウィザードを表示し、111 ページの「Directory Server の準備」に進む
- この作業をあとから行う場合は「いいえ」をクリックし、115 ページの「Active Directory ソースの作成」に進む

Directory Server の準備

ここでは、Identity Synchronization for Windows が使用できるように Sun Java System Directory Server ソースを準備する方法について説明します。

Directory Server の準備には、次の作業が含まれます。

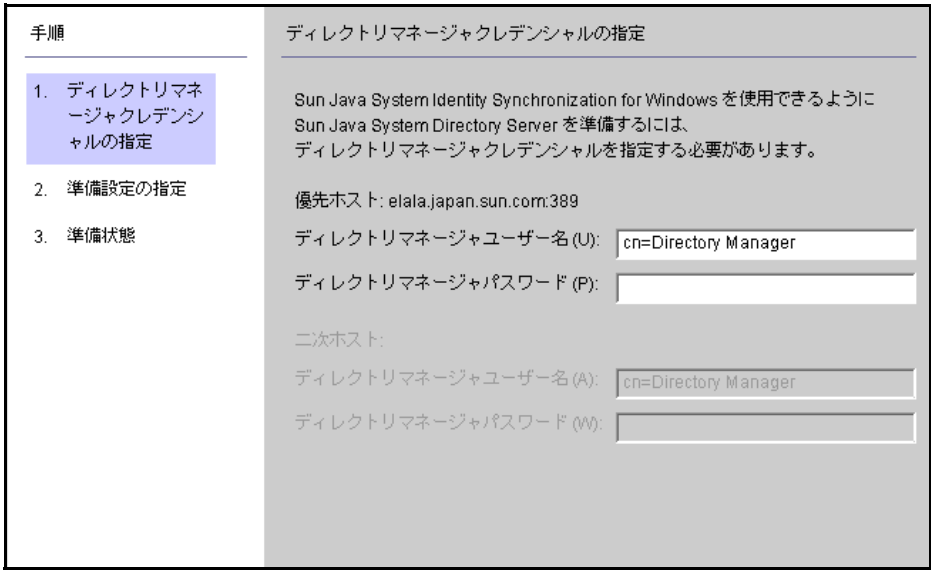
- 優先ホストで使用できる旧バージョン形式の更新履歴ログデータベースとアクセス制御インスタンスを作成する
- 優先ホストで使用できるコネクタユーザーとユーザーアクセス制御インスタンスを作成する
- 優先ホストと二次ホストで等価インデックスを作成する

注

- Directory Server の準備には、コンソールの代わりに `idsync prepds` コマンド行ユーティリティを使用できる。詳細については、316 ページの「prepds の使用」を参照
- `idsync prepds` コマンド行ユーティリティを使用して Directory Server を準備するときは、どのホストとサフィックスを使用するかを把握し、ディレクトリマネージャのクレデンシャルを準備しておく必要がある

Directory Server の準備には、「Directory Server の準備」ウィザード (図 4-13) を使用できます。

図 4-13　　ディレクトリマネージャクレデンシャルの入力



このウィザードには、次のいずれかの方法でアクセスします。

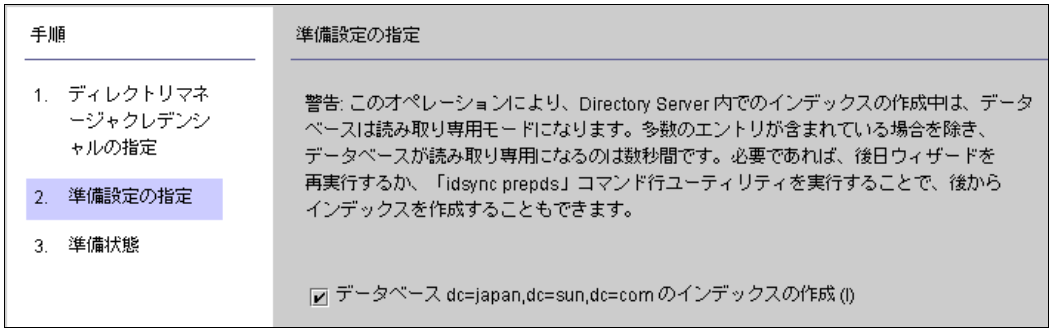
- 「Directory Server の準備を直ちに行いますか ?」ダイアログボックスが表示されたときに「はい」ボタンをクリックする
- 「設定」タブの「Sun ディレクトリソース」パネルで「Directory Server の準備」ボタンをクリックする

Directory Server ソースを準備するには

1. ディレクトリマネージャアカウントの次のクレデンシャルを入力します。
   - **ディレクトリマネージャユーザー名**
   - **ディレクトリマネージャパスワード**

   二次ホストを使用している場合は (MMR 構成)、「二次ホスト」オプションが設定可能になるので、これらのホストのクレデンシャルも指定する必要があります。
2. 情報の入力が完了したら、「次へ」をクリックして「準備設定の指定」パネル (図 4-14) を表示します。

図 4-14　「準備設定の指定」パネル



警告メッセージを読み、Directory Server インデックスを直ちに作成するか、あとから作成するかを指定します。

注

- データベースの規模に応じて、この処理には数秒から数分かかる
- データベースが読み取り専用モードの場合、データベース内の情報の更新は失敗する
- データベースをオフライン状態にすることで、インデックスをより高速に作成できる

- インデックスを直ちに作成するときは、「データベース (名前) のインデックスの作成」ボックスにチェックマークを付け、「次へ」をクリックする
- インデックスをあとから手動で、またはもう一度ウィザードを使用して作成するときは、「データベース (名前) のインデックスの作成」ボックスのチェックマークを外し、「次へ」をクリックする

3. Directory Server の準備の進捗状況に関する情報を示す「準備状態」パネルが表示されます。
   - メッセージ区画の下部に「成功」メッセージが表示されたら、「終了」をクリックする
   - エラーメッセージが表示されたときは、操作を続ける前に指摘された問題を解決する。詳細については、エラーログ (「状態」タブを参照) を確認する
4. コンソールの「設定」タブに戻ります。ナビゲーションツリーで Sun ディレクトリソースノードを選択し、「Sun ディレクトリソース」パネル (図 4-15) を開きます。

図 4-15　「Sun ディレクトリソース」パネル

このパネルでは、次のタスクを実行できます。

- **サーバーの編集** : サーバーの設定パラメータを変更するための「Sun Java System ディレクトリソースの定義」パネルを開くときは、このボタンをクリックする。操作方法については、「Sun Java System ディレクトリソースの作成」を参照
- **Directory Server の準備** : Directory Server を準備するときは、このボタンをクリックする。操作方法については、111 ページの「Directory Server の準備」を参照

  たとえば、インデックスが削除されたり、旧バージョン形式の更新履歴ログデータベースが喪失した場合など、サーバーの最初の準備の後で Directory Server に変更が生じたときは、サーバーの準備を再実行できる

  注　優先 Sun ディレクトリソースの旧バージョン形式の更新履歴ログデータベースを再作成する場合、デフォルトのアクセス制御設定が適用されると Directory Server コネクタはデータベースの内容を読み込めません。

  新しい旧バージョン形式の更新履歴ログデータベースのアクセス制御設定を復元するには、`idsync prepds` を実行するか、コンソールで適切な Sun ディレクトリソースを選択してから「Directory Server の準備」ボタンをクリックします。

- **再同期間隔** (の指定): Directory Server コネクタが変更を確認する頻度を指定する。デフォルトは *1000* ミリ秒

5. 同期させる Sun Java System Directory Server エンタープライズ内のユーザーグループごとに Directory Server ディレクトリソースを追加します。

Directory Server の準備が完了したら、少なくとも 1 つの Windows ディレクトリソースを作成する必要があります。

- Active Directory ディレクトリソースを作成するときは、115 ページの「Active Directory ソースの作成」に進む
- Windows NT ディレクトリソースを作成するときは、124 ページの「Windows NT SAM ディレクトリソースの作成」に進む

Active Directory ソースの作成

Active Directory ディレクトリソースは、ネットワーク上で同期させる Windows ドメインごとに追加する必要があります。

Active Directory の各配備には、すべての Active Directory ドメインに適用されるグローバル情報がすべて記録されたグローバルカタログが、少なくとも 1 つあります。

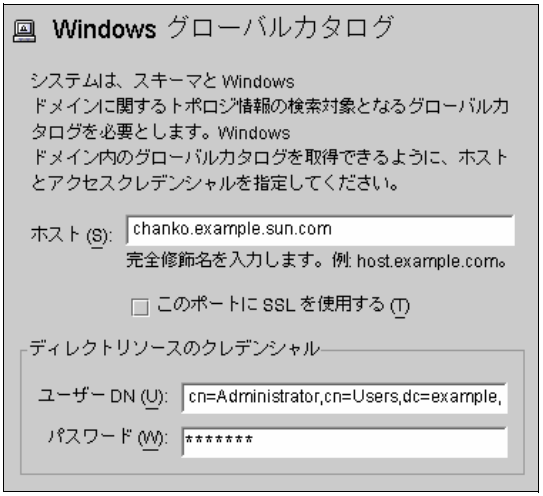
注 各 Active Directory サーバーをグローバルカタログとし、配備に複数のグローバルカタログを持たせることもできますが、指定が必要なグローバルカタログの数は 1 つだけです。

ネットワークに Windows Active Directory サーバーが存在する場合は、次の手順を実行します。

1. ナビゲーションツリーでディレクトリソースのノードを選択し、「ディレクトリソース」パネルの「新規 Active Directory ソース」ボタンをクリックします。

「Windows グローバルカタログ」ダイアログボックス (図 4-16) が表示されます。

図 4-16　「Windows グローバルカタログ」ダイアログボックス

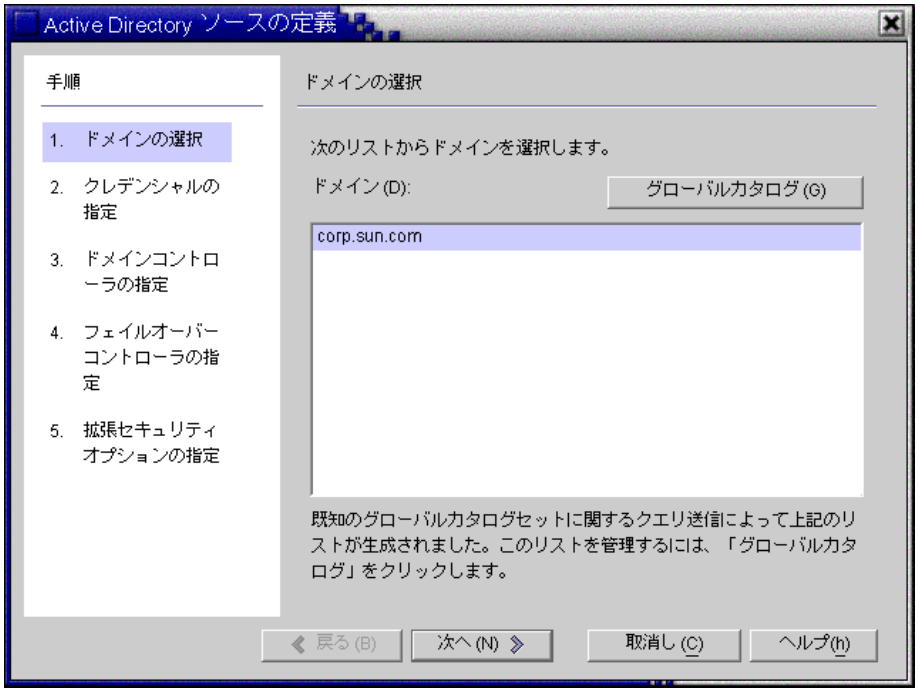


2. 次の情報を入力し、「了解」をクリックします。
   - **ホスト** : Active Directory フォレストのグローバルカタログを保持するマシンの完全修飾ホスト名を入力する

     たとえば、**`machine2.example.com`** のように指定する
   - **このポートに SSL を使用する** : Identity Synchronization for Windows がグローバルカタログとの通信に SSL ポートを使用する場合は、このオプションを有効にする
   - **ユーザー DN** : 管理者の (バインド) 完全修飾識別名を入力する。スキーマを検索し、システムで使用できる Active Directory ドメインを特定することができれば、どのようなクレデンシャルでも指定できる

     たとえば、**`cn=Administrator,cn=Users,dc=example,dc=com`** のように指定する
   - **パスワード** : 指定したユーザーのパスワードを入力する
3. 次のような「Active Directory ソースの定義」ウィザードが表示されます。

図 4-17　「Active Directory ソースの定義」ウィザード



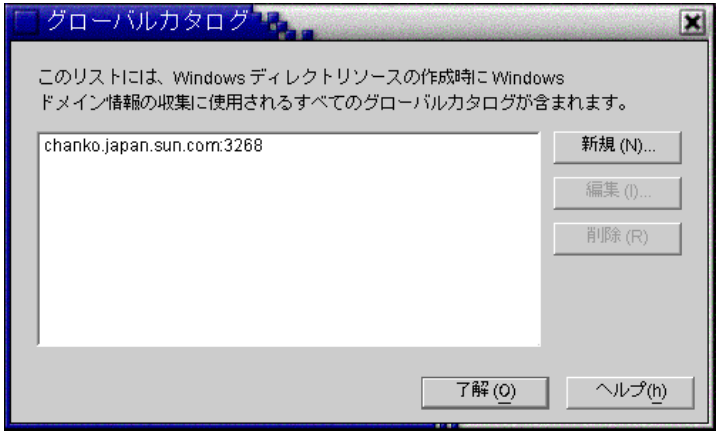
このウィザードは、Active Directory グローバルカタログにクエリ送信して存在するその他のドメインを特定し、「ドメイン」リストパネルにこれらのドメインを表示します。

4. リストパネルから名前を選択して Active Directory ドメインを指定し、「了解」をクリックして 118 ページの手順 5 に進みます。

   使用するドメインがリストに表示されないときは、次の手順を実行し、そのドメインを認識するグローバルカタログを追加する必要があります。

   a. 「グローバルカタログ」ボタンをクリックして「グローバルカタログ」ウィザード (図 4-18) を表示します。

図 4-18　新しいグローバルカタログの指定



b. 「新規」ボタンをクリックします。

c. 「Windows グローバルカタログ」ダイアログボックスが表示されるので、グローバルカタログのホスト名と、ディレクトリソースのクレデンシャル (116 ページを参照) を入力し、「了解」をクリックします。

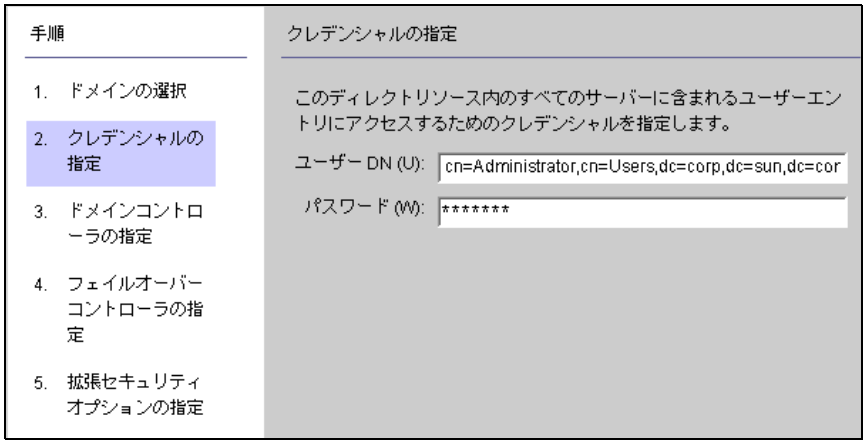
d. 「グローバルカタログ」リストパネルに新しいグローバルカタログとポートが表示されます。カタログ名を選択し、「了解」をクリックします。

e. これ以外のグローバルカタログ (ドメイン) をシステムに追加する場合は、以上の手順を繰り返します。

f. 操作が完了したら、「ドメインの選択」パネルの「次へ」ボタンをクリックします。

5. 「クレデンシャルの指定」パネルが表示されるので、「ユーザー DN」フィールドの値を確認します。

図 4-19　この Active Directory ソースのクレデンシャルの指定



管理者の識別名がプログラムによって「ユーザー DN」フィールドに自動的に入力されない場合、またはその管理者のクレデンシャルを使用したくない場合は、ユーザー DN とパスワードを手動で入力します。

Active Directory ソースを設定するときは、Active Directory コネクタが Active Directory への接続に使用できるユーザー名とパスワードを指定する必要があります。

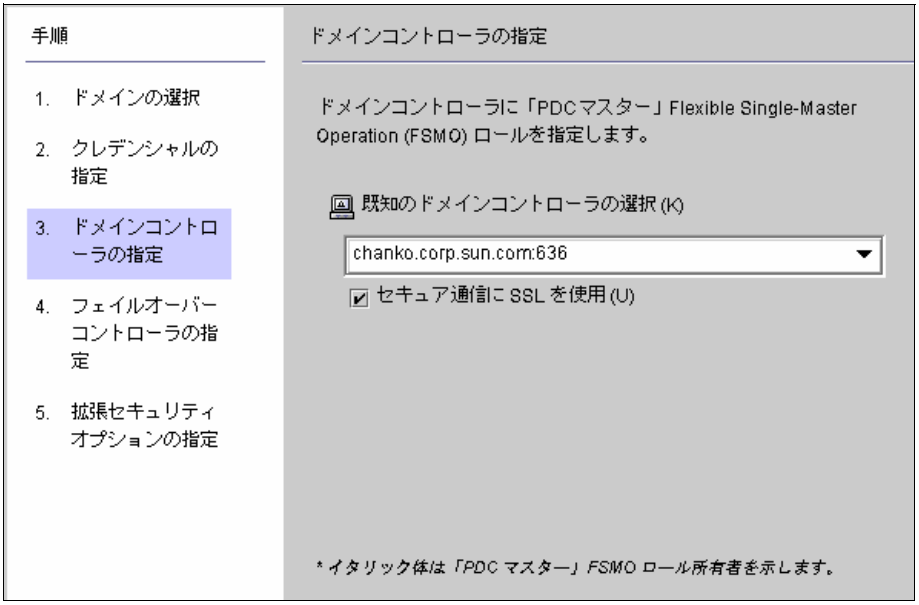
注　コネクタは、特定のアクセス権を必要とします。次に示すように、必要となる最低限の権限は、同期の方向によって異なります。

- Active Directory から Directory Server への同期フローだけを設定する場合は、Active Directory コネクタ用に指定するユーザーに特別な権限は必要ない。同期対象ドメインで「すべてのプロパティを読み取る」ための追加権限を持つ一般ユーザーで十分である
- Directory Server から Active Directory への同期フローを設定する場合は、同期によって Active Directory 内のエントリが変更されるため、コネクタユーザーにこれ以上の権限が必要となる。この設定では、コネクタユーザーは「完全管理」権限を持つか、管理者グループのメンバーである必要がある

---

6. 「次へ」をクリックし、「ドメインコントローラの指定」パネルを開きます。

図 4-20　　ドメインコントローラの指定



このパネルでは、指定ドメイン内で同期を行うコントローラを選択します。ドメインコントローラの概念は、Directory Server の優先サーバーに似ています。

選択している Active Directory ドメインに複数のドメインコントローラがあるときは、同期の主ドメインコントローラ FSMO ロールを持つドメインコントローラを選択します。

デフォルトでは、すべてのドメインコントローラで行われたパスワード変更は、直ちに主ドメインコントローラ FSMO ロール所有者にレプリケートされ、このドメインコントローラを選択した場合は、Identity Synchronization for Windows はパスワード変更を直ちに Directory Server と同期させます。

配備によっては、PDC との間に大きなネットワーク「距離」があり、それによって同期が大きく遅れるため、Windows レジストリに `AvoidPdcOnWan` 属性が設定されます。詳細については、Microsoft の知識ベース記事 232690 を参照してください。

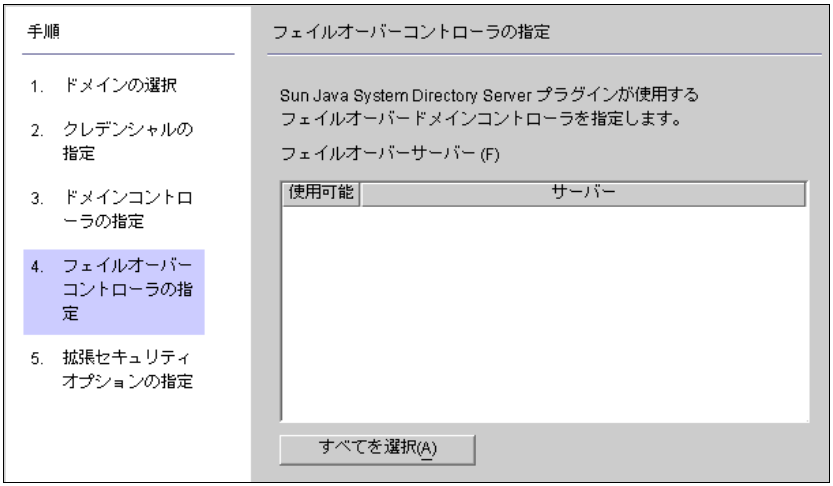
7. ドロップダウンリストからドメインコントローラを選択します。
8. Identity Synchronization for Windows がドメインコントローラとの通信にセキュリティ保護されたポートを使用するように設定するときは、「セキュアポートを使用します」ボックスにチェックマークを付けます。

注	マイクロソフト証明書サーバーを使用している場合は、Active Directory コネクタに CA 証明書が自動的にインストールされます。使用していない場合は、Active Directory コネクタに CA 証明書を手動で追加する必要があります。298 ページの「Active Directory コネクタでの SSL の有効化」を参照してください。また、初期設定後にフローの設定を変更した場合にも、この作業が必要です。

9. 完了したら「次へ」をクリックします。

「フェイルオーバーコントローラの指定」パネル (図 4-21) が表示されます。このパネルでは、任意の数のフェイルオーバードメインコントローラを指定できます。

図 4-21　フェイルオーバーコントローラの指定



Active Directory コネクタは、1 つの Active Directory ドメインコントローラだけと通信し、Identity Synchronization for Windows は、そのコネクタによって適用されるフェイルオーバー変更をサポートしません。ただし、Directory Server プラグインは Directory Server へのパスワード変更を検証するときに、任意の数のドメインコントローラと通信します。

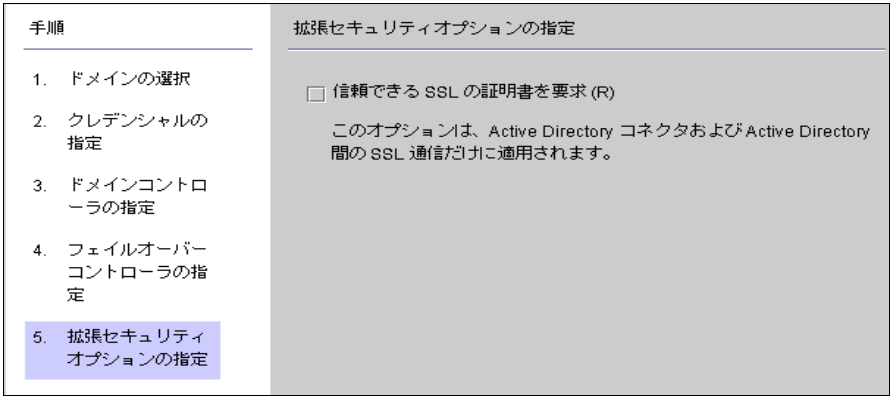
Directory Server が Active Directory ドメインコントローラへの接続を試み、そのドメインコントローラが見つからない場合は、Directory Server は指定されたフェイルオーバードメインコントローラへの接続試行を繰り返します。

10. 「フェイルオーバーサーバー」リストパネルに表示される 1 つまたは複数のサーバー名を選択するか、「すべてを選択」ボタンをクリックしてリスト内のすべてのサーバーを指定し、「次へ」をクリックします。

11. 次のような「拡張セキュリティオプションの指定」パネル (図 4-22) が表示されます。

    「信頼できる SSL の証明書を要求」オプションを有効にできるのは、「ドメインコントローラの指定」パネル (図 4-20 を参照) で「セキュア通信に SSL を使用」ボックスを有効にした場合だけです。

図 4-22 拡張セキュリティオプションの指定



- 「信頼できる SSL の証明書を要求」ボックスが無効化されている場合 (デフォルトの設定)、Active Directory コネクタは SSL 経由で Active Directory に接続し、Active Directory から渡された証明書が信頼されているかどうかを検証しない

  このオプションを無効にすることで、Active Directory 証明書データベースに Active Directory 証明書をインストールする必要がなくなるため、セットアップ手順が簡略化される

- 「信頼できる SSL の証明書を要求」ボックスを有効にした場合、Active Directory コネクタは SSL 経由で Active Directory に接続し、かつ Active Directory から渡された証明書が信頼されているかどうかを検証する

注 Active Directory コネクタの証明書データベースに Active Directory 証明書を追加する必要があります。手順については、301 ページの「コネクタの証明書データベースへの Active Directory 証明書の追加」を参照してください。

12. 「拡張セキュリティオプション」パネルの設定が完了したら、「終了」ボタンをクリックします。

ナビゲーションツリーのディレクトリソースの下に、新たに指定された Active Directory ディレクトリソースが追加されます。

13. Active Directory ディレクトリソースノードを選択し、「Active Directory ソース」パネル (図 4-23) を表示します。

図 4-23　「Active Directory ソース」パネル

このパネルでは、次のタスクを実行できます。

- **コントローラの編集** : ドメインコントローラの設定パラメータを変更するための「ドメインコントローラの指定」パネルを開くときは、このボタンをクリックする。操作方法については、「Active Directory ソースの作成」を参照
- **再同期間隔** (の設定): Active Directory コネクタが変更を確認する頻度を指定する。デフォルトは *1000* ミリ秒
- **ディレクトリソースのクレデンシャル** (の変更): 指定されているユーザー DN、パスワード、または両方を変更する

Active Directory ディレクトリソースの作成が完了したら、次の作業を行います。

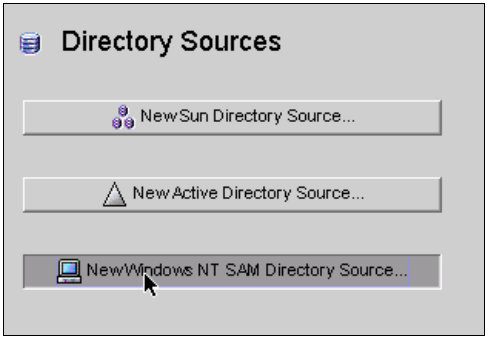
- Windows NT ディレクトリソースを作成するときは、「Windows NT SAM ディレクトリソースの作成」に進む
- 同期させる属性の選択とマッピングを行うときは、127 ページの「ユーザー属性の選択とマッピング」に進む

Windows NT SAM ディレクトリソースの作成

Windows NT プラットフォームに Identity Synchronization for Windows を配備するときは、NT SAM ディレクトリソースを次のように指定します。

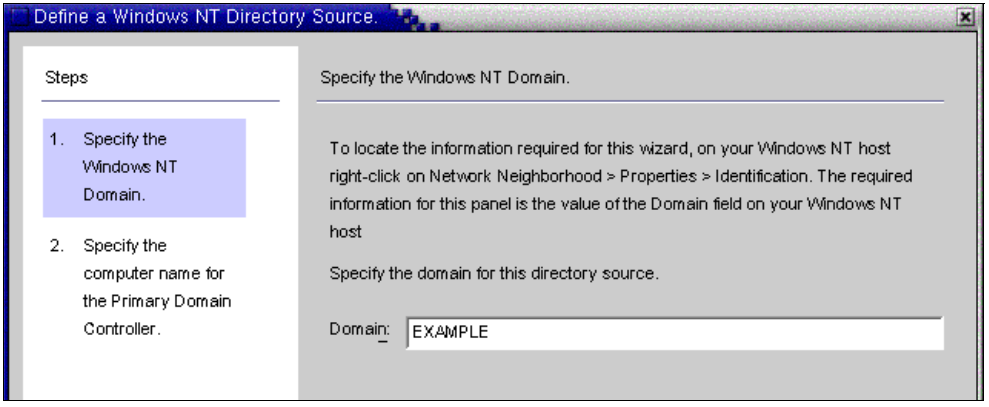
1. ナビゲーションツリーでディレクトリソースのノードを選択し、「新規 Windows NT SAM ディレクトリソース」ボタンをクリックします。

図 4-24　「ディレクトリソース」パネル



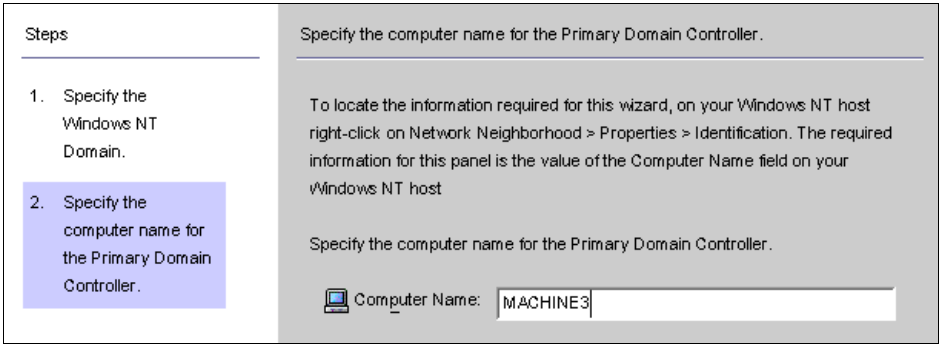
2. 「Windows NT SAM ディレクトリソースの定義」パネル (図 4-25) が表示されたら、指示に従って Windows NT ドメイン名を特定し、「ドメイン」フィールドに NT ディレクトリソースの一意の名前を入力します。完了したら「次へ」をクリックします。

図 4-25　Windows NT SAM ドメイン名の選択



3. 「主ドメインコントローラのコンピュータ名の指定」パネル (図 4-26) が表示されたら、指示に従って主ドメインコントローラコンピュータの名前を特定し、「コンピュータ名」に情報を入力します。

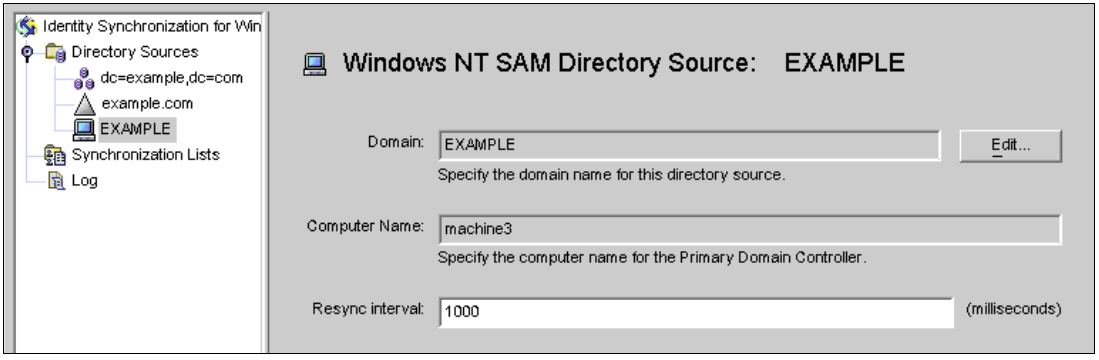
図 4-26　　主ドメインコントローラ名の指定



4. 「終了」をクリックします。

ナビゲーションツリーのディレクトリソースの下に、新たに指定された Windows NT SAM ディレクトリソースが追加されます。「Windows NT SAM ソース」パネル (図 4-27 を参照) を表示するには、新しいディレクトリソースのノードを選択します。

図 4-27　　「Windows NT SAM ディレクトリソース」パネル



このパネルでは、次のタスクを実行できます。

- **編集** : ドメインコントローラの設定パラメータを変更するための「ドメインコントローラの指定」パネルを開くときは、このボタンをクリックする。操作方法については、「Active Directory ソースの作成」を参照

- **再同期間隔** (の設定): Windows NT に加えられた変更を Identity Synchronization for Windows が調べる頻度を指定する。デフォルトは *1000* ミリ秒

5. ネットワーク上の Windows NT マシンごとに Windows NT ディレクトリソースを追加します。

Windows NT SAM ディレクトリソースの作成が完了すると、同期させる属性を選択およびマッピングする準備が整います。127 ページの「ユーザー属性の選択とマッピング」に進んでください。

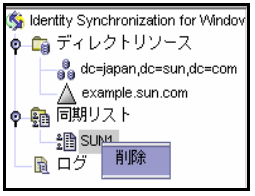
ディレクトリソースの削除

注	ディレクトリソースが関連付けられたコネクタがすでにインストールされている場合は、ディレクトリソースを削除する前にコネクタをアンインストールする必要があります。

ディレクトリソースの削除が必要な場合は、次の手順を実行します。

1. ディレクトリソースを削除する前に、そのソースと関連付けられているすべての SUL (同期ユーザーリスト) を削除する必要があります。
   a. ナビゲーションツリーの「同期リスト」ノードの下に表示されるリストの中から、該当する同期ユーザーリストを右クリックします。
   b. ポップアップメニューが表示されるので、「削除」を選択して SUL を削除します。

図 4-28 同期ユーザーリストの削除



2. ナビゲーションツリーのディレクトリソースのノードの下で、ディレクトリソースノードを右クリックします。
3. ポップアップメニューが表示されるので、「削除」を選択してそのディレクトリソースを削除します。

ユーザー属性の選択とマッピング

Directory Server と Windows のディレクトリソースの作成と設定が完了したら、同期させるユーザー属性を選択し、これらの属性をシステム間でマッピングする必要があります。

ここで説明する内容は次のとおりです。

属性の選択とマッピング

属性には、次の 2 種類があります。

- **有効** : ユーザーエントリの作成または変更時にシステム間で同期される属性
- **作成** : ユーザーエントリの作成時にだけシステム間で同期される属性

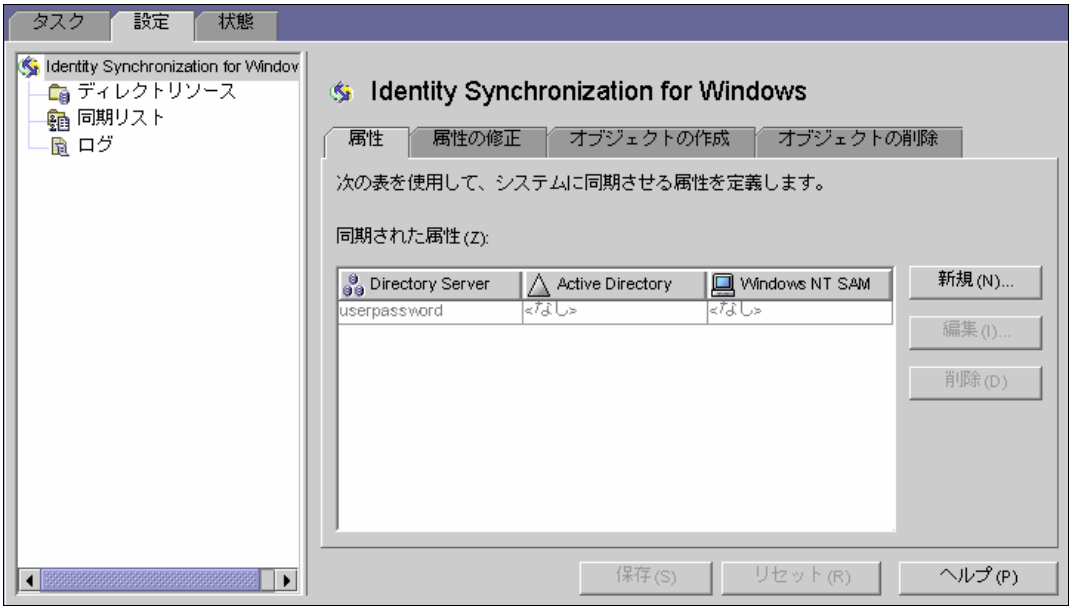
  各プラットフォームで使用されるスキーマによっては、一部の作成属性は必須属性となる。これらの属性はパスワードの同期に必要とされ、Active Directory サーバー上で `user` オブジェクトクラスエントリを正しく作成するために、Sun 属性とマッピングする必要がある

ここでは、同期させるユーザー属性を選択する方法と、属性をマッピングする方法について説明します。この属性マッピングにより、Directory Server 環境で属性を指定した場合に、対応する属性が Active Directory 環境や Windows NT 環境で特定され、対応する Windows 属性の値が同期されます。または、その逆方向で同期が行われます。

同期させる属性を選択し、マッピングするには

1. ナビゲーションツリーの最上位にある Identity Synchronization for Windows ノードを選択します (図 4-29 を参照)。

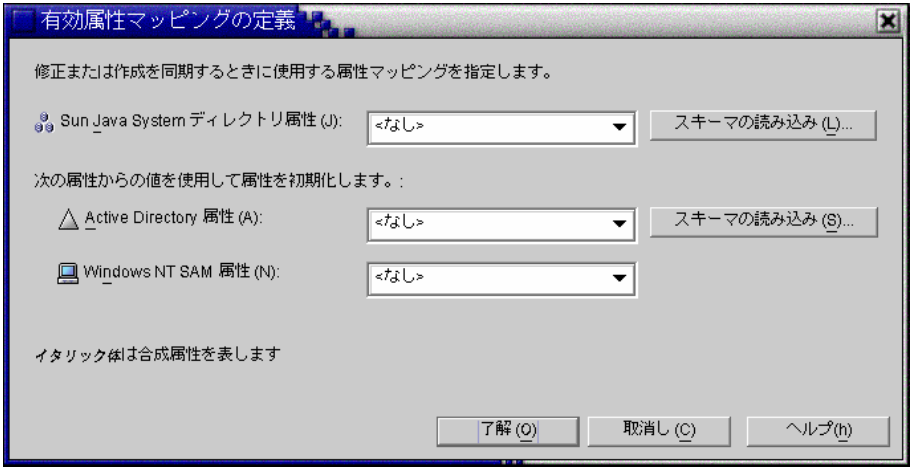
図 4-29　「属性」タブ



2. 「属性」タブを選択し、「新規」ボタンをクリックします。

   「有効属性マッピングの定義」ダイアログボックス (図 4-30) が表示されます。このダイアログボックスでは、Directory Server から Windows システム (Active Directory、Windows NT、または両方) への属性マッピングを行います。

図 4-30　有効属性マッピングの定義



注　どの作成属性が Directory Server (または Active Directory) の必須作成属性となるかは、Sun 側 (または Active Directory 側) のユーザーエントリに設定されているオブジェクトクラスによって異なります。

3. Sun Java System の属性ドロップダウンリストから属性を選択し (たとえば、*cn* など)、それに対応する属性を Active Directory、Windows NT SAM、または両方の属性ドロップダウンメニューから選択します。
4. 完了したら、「了解」をクリックします。
5. 別の属性を指定するときは、手順 2 から手順 4 を繰り返します。

完成した同期対象属性の表は、次の図に示す例のようになります。この例では、Directory Server の `userpassword`、`cn`、`telephonenumber` 属性が、それぞれ Active Directory の `unicodepwd`、`cn`、`telephonenumber` 属性にマッピングされます。

図 4-31　完成した同期対象属性の表

Directory Server	Active Directory	Windows NT SAM
userpassword	unicodepwd	<なし>
cn	cn	<なし>
telephonenumber	telephonenumber	<なし>

注　プログラムは、Sun Java System Directory Server のデフォルトオブジェクトクラスとして自動的に *inetOrgPerson* を使用し、Active Directory のスキーマは、グローバルカタログの指定時に読み込まれます。このため、デフォルトスキーマを変更する場合を除き、「スキーマの読み込み」ボタンを使用することはありません。

デフォルトのスキーマソースを変更する方法については、130 ページの「スキーマソースの変更」を参照してください。

パラメータ化されたデフォルト属性値の作成

Identity Synchronization for Windows では、別の作成属性または有効属性の値を使用して、属性のパラメータ化されたデフォルト値を設定できます。

パラメータ化されたデフォルト属性値を指定するには、式文字列内の既存の作成属性または有効属性の名前の前後にパーセント記号を付けます (`%<attribute_name>%`)。たとえば、`homedir=/home/%uid%` または `cn=%givenName% %sn%` のように指定します。

これらの属性値は、次のように使用できます。

- 作成式では、複数の属性を使用できる (`cn=%givenName% %sn%`)
- `A=%B%` の場合、`B` がとれるデフォルト値は 1 つだけである
- パーセント記号を通常の文字として使用する場合は、円記号 (¥) を使用する (たとえば、`diskUsage=0¥%`)
- 循環代入条件を持つ式を使用しない。たとえば、`description=%uid%` を指定した場合は、`uid=%description%` を使用できない

スキーマソースの変更

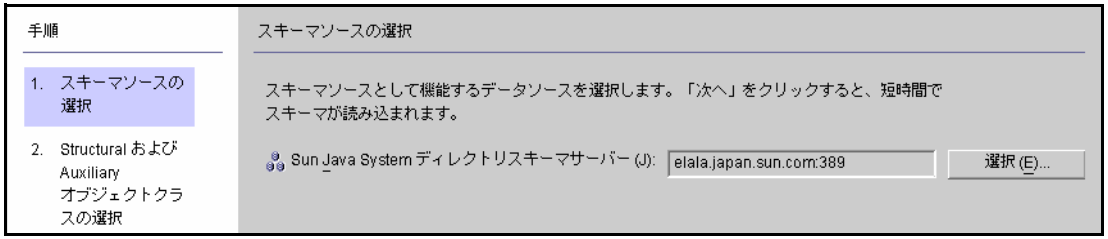
プログラムは自動的にスキーマソースを指定しますが、このデフォルトスキーマを変更することができます。

デフォルトのスキーマソースを変更する手順は、次のとおりです。

1. 「有効属性マッピングの定義」ダイアログボックスで「スキーマの読み込み」ボタンをクリックします。

   「スキーマソースの選択」パネル (図 4-32) が表示されます。

図 4-32　　スキーマソースの選択



このパネルでは、スキーマの読み込み元となる Sun Java System Directory Server スキーマサーバーを指定します。このスキーマには、システムで使用できるオブジェクトクラスが含まれます。ユーザーがシステムで使用できる属性は、これらのオブジェクトクラスによって決定されます。

「Sun Java System ディレクトリスキーマサーバー」フィールドには、デフォルトで設定ディレクトリが指定されます。

2. 別のサーバーを選択するときは、「選択」ボタンをクリックします。

   「Sun スキーマホストの選択」ダイアログボックスが表示されます。このダイアログボックスには、ディレクトリソースの管理情報を記録した設定ディレクトリがリスト表示されます。

   このダイアログボックスで行える操作は、次のとおりです。

   - 新しい設定ディレクトリを作成し、それをリストに追加する

     「新規」をクリックして「新規設定ディレクトリ」ダイアログボックスを表示し、ホスト、ポート、ユーザー DN、パスワードを指定する。終了したら、「了解」をクリックする

   - 既存のディレクトリを編集する

     「編集」をクリックして「設定ディレクトリの編集」ダイアログボックスを表示すると、ホスト、ポート、ユーザー DN、パスワードを編集できる。終了したら、「了解」をクリックする

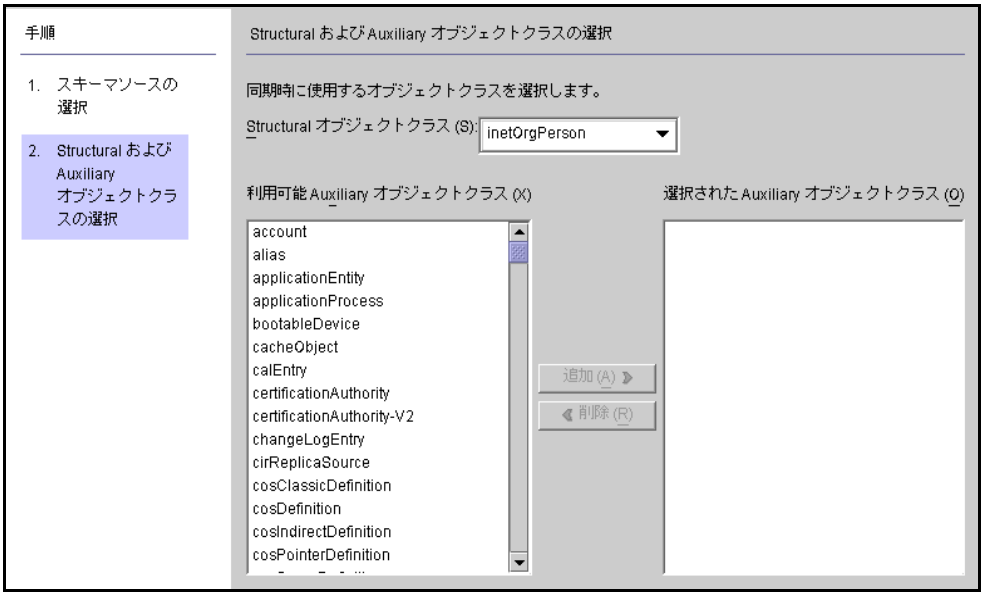
   - リストからディレクトリを削除する

     リスト上でディレクトリ名を選択し、「削除」ボタンをクリックする

3. リスト上でサーバーを選択し、「了解」をクリックします。通常は、いずれかの Sun 同期ホストがスキーマソースとして適しています。

4. 「次へ」ボタンをクリックして、「Structural および Auxiliary オブジェクトクラスの選択」パネル (図 4-33) を表示します。

図 4-33　Structural および Auxiliary オブジェクトクラスの選択



このパネルでは、同期させるオブジェクトクラスを次のように指定します。

- **Structural オブジェクトクラス** : 選択した Directory Server から作成された、または同期させられたすべてのエントリは、少なくとも 1 つの Structural オブジェクトクラスを持つ必要がある
- **Auxiliary オブジェクトクラス** : これらのオブジェクトクラスは、選択した Structural クラスを補完し、同期させる追加属性を指定する

Structural および Auxiliary オブジェクトクラスを指定するには

a. ドロップダウンリストから Structural オブジェクトクラスを選択します。デフォルトは *InetOrgPerson* です。

b. 「利用可能 Auxiliary オブジェクトクラス」リストパネルから 1 つまたは複数のオブジェクトクラスを選択し、「追加」をクリックして選択項目を「選択された Auxiliary オブジェクトクラス」リストパネルに移動します。

   選択されたオブジェクトクラスは、有効属性または作成属性として選択できる Directory Server ソース属性を決定します。また、必須作成属性もオブジェクトクラスによって決定されます。

   「選択された Auxiliary オブジェクトクラス」リストから選択項目を削除するには、オブジェクトクラス名を選択し、「削除」ボタンをクリックします。

c. 終了したら「終了」をクリックします。スキーマと、選択したオブジェクトクラスが読み込まれます。

システム間でのユーザー属性の伝達

同期させるユーザー属性を選択し、そのマッピングが完了したら、属性の作成、変更、削除を Sun と Windows のシステム間でどのように伝達させるか (伝達フロー) を Identity Synchronization for Windows に指定する必要があります。

Identity Synchronization for Windows のデフォルトの動作は次のとおりです。

- Windows から Sun Java System Directory Server への同期だけを行う
- パスワード属性だけを同期させる (前節で有効属性を指定していない場合)
- エントリの作成または削除を同期させない

ここでは、システム間での属性の同期を設定する方法について説明します。ここで説明する内容は、次のとおりです。

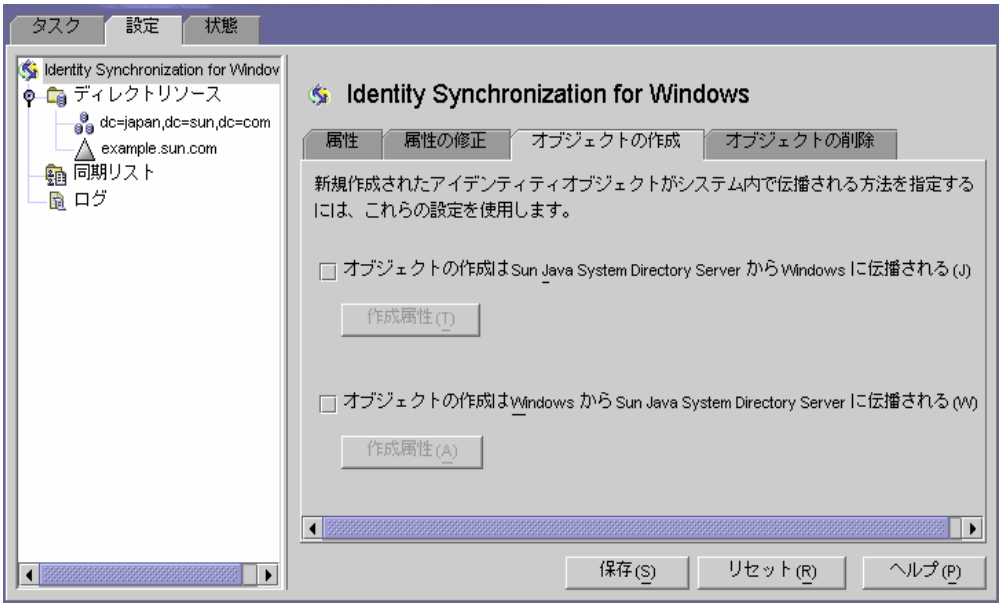
- 133 ページの「オブジェクト作成のフローの指定」
- 139 ページの「オブジェクト修正フローの方向の指定」
- 148 ページの「削除フローの方向の指定」

オブジェクト作成のフローの指定

Directory Server と Active Directory のシステム間でオブジェクト作成をどのように伝達させるかを指定する手順は、次のとおりです。

1. 「オブジェクトの作成」タブをクリックします。

図 4-34　作成の選択と伝達



2. 作成の伝達は、次のように有効化または無効化できます。
   - Directory Server 環境から Windows サーバーに作成を伝達するには、**「オブジェクトの作成は Sun Java System Directory Server から Windows に伝播される」**を有効にする
   - Windows 環境から Directory Server に作成を伝達するときは、**「オブジェクトの作成は Windows から Sun Java System Directory Server に伝播される」**にチェックマークを付ける
   - 双方向のフローを設定するときは、両方のオプションにチェックマークを付ける
   - システム間でユーザー作成を伝達しない場合は、どちらのオプションにもチェックマークを付けない (デフォルト)
3. 作成属性の追加、編集、削除をシステム間で同期させるときは、選択しているオプションの下にある「作成属性」をクリックします。

   「作成属性のマッピングと値」ダイアログボックス (図 4-35 および図 4-36) が表示されます。

図 4-35　作成属性のマッピングと値 : Directory Server から Windows への伝達

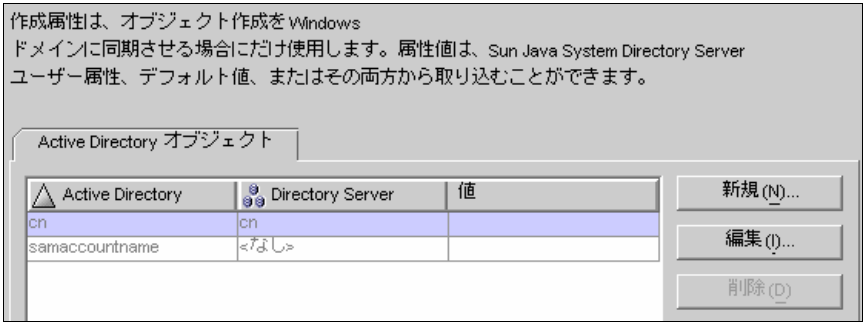
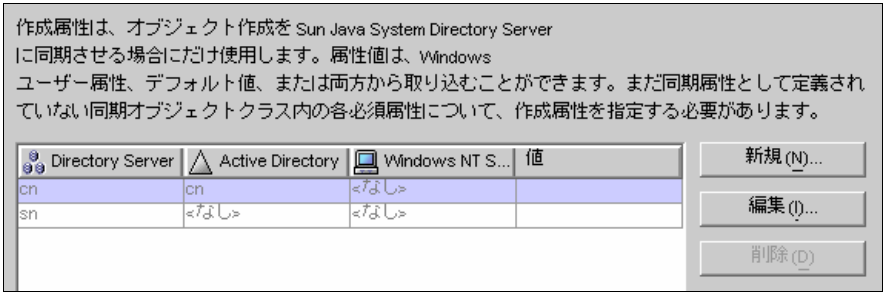


図 4-36　作成属性のマッピングと値 : Windows から Directory Server への伝達



いずれかのダイアログボックスを使用して、次の操作を行えます。

- 新規作成属性を指定する (136 ページを参照)

注　user オブジェクトクラスの必須属性に関するスキーマの制約を満たすために、ユーザー作成時にシステム間で受け渡される追加属性の指定が必要になる場合もあります。

127 ページの「ユーザー属性の選択とマッピング」で説明したように、必須属性を変更属性として指定した場合は、追加属性は必要ありません。

- 既存の属性を編集する (136 ページを参照)
- 既存の属性を削除する (136 ページを参照)

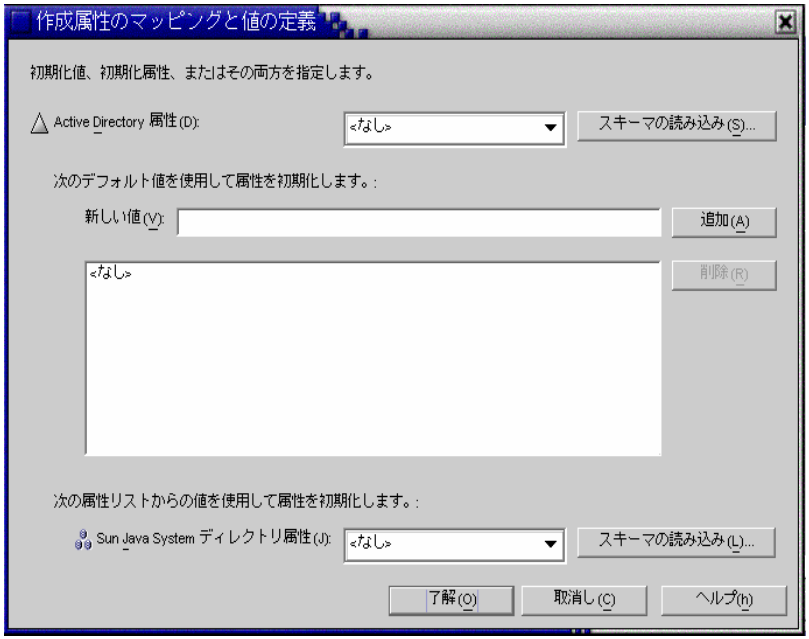
新規作成属性の指定

次に、作成属性を追加し、Active Directory から Directory Server にマッピングする方法について説明します。追加した属性を Directory Server から Windows、または Windows から Directory Server にマッピングする手順も、これに準じます。

1. 「作成属性のマッピングと値」ダイアログボックスの「新規」ボタンをクリックします。

   「作成属性のマッピングと値の定義」ダイアログボックス (図 4-37) が表示されます。

図 4-37　　作成属性のマッピングと値の定義



2. 「Active Directory 属性」ドロップダウンリストから属性値を選択します。

図 4-38　　新しい Active Directory 属性の選択

Identity Synchronization for Windows では、属性が複数の値を受け付ける場合に、複数の値を指定して属性を初期化することができます。

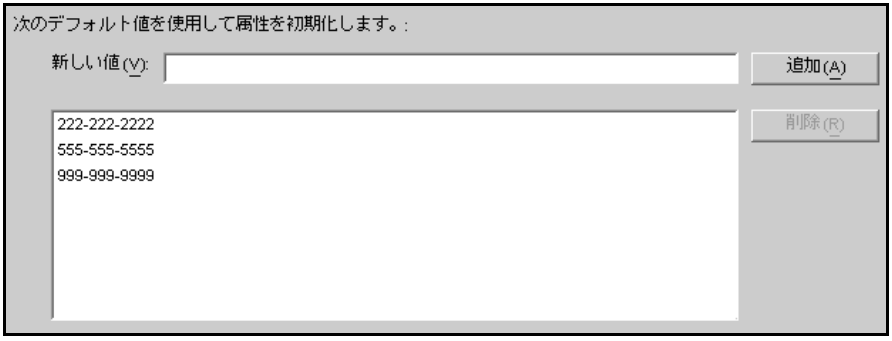
たとえば、会社に 3 つのファックス番号がある場合、Sun Java System Directory Server と Active Directory の両方に `facsilimiletelephonenumber` 属性を指定し、3 つの番号を設定できます。

どの属性が複数の値を受け付けるかは、管理者が把握している必要があります。複数の値を受け付けない属性に複数の値を追加しようとすると、プログラムがオブジェクト作成を試みる段階で実行時エラーが生じます。

3. 「新しい値」フィールドに値を入力し、「追加」をクリックします。

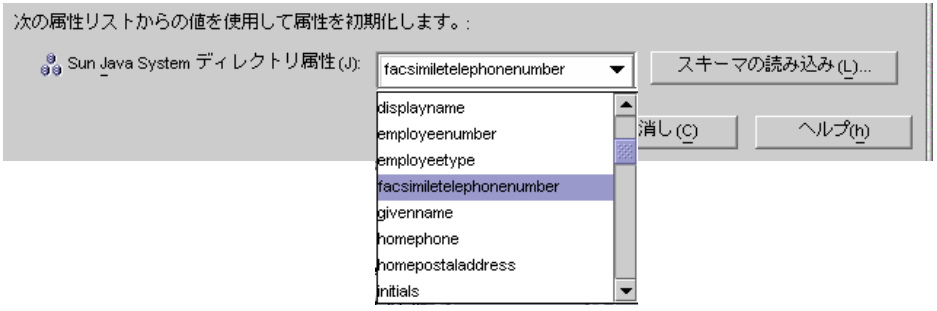
   リストパネルに属性値が追加されます。複数の属性値を追加するときは、必要な回数だけこの手順を繰り返します。

図 4-39　作成属性の複数の値の指定



4. 属性を Directory Server にマッピングするには、「Sun Java System ディレクトリ属性」ドロップダウンリストから属性名を選択します。

図 4-40　Directory Server 属性のマッピング



5. 完了したら、「了解」をクリックします。

   ここで説明した例では、作成属性とマッピングの表は次の図のようになります。

図 4-41　　完成した作成属性とマッピングの表

Active Directory	Directory Server	値
cn	cn	
samaccountname	<なし>	
facsimiletelephonenumber	facsimiletelephonenumber	[222-222-2222,555-555-5...

6. 別の属性を指定するときは、この手順を繰り返します。

既存属性の編集

作成属性のマッピングまたは値を編集するには

1. 「オブジェクトの作成」タブをクリックし、選択している作成オプションの下にある「属性の作成」ボタンをクリックします。
2. 「作成属性のマッピングと値」ダイアログボックスが表示されるので、表から属性を選択し、「編集」ボタンをクリックします。

   「作成属性のマッピングと値の定義」ダイアログボックスが表示されます。
3. Directory Server と Active Directory (または Windows NT) の間の既存のマッピングを変更するときは、ドロップダウンメニューを使用します。

   たとえば、Sun Java System Directory Server の `homephone` 属性が Active Directory の `othertelephone` 属性にマッピングされていると仮定します。「Active Directory の属性」ドロップダウンリストを使用して、マッピング先を `homephone` 属性に変更できます。
4. 属性値を追加または削除することもできます。
   - 属性値を追加するには、「新しい値」フィールドに情報を入力し、「追加」をクリックします。
   - 属性値を削除するには、リストパネルで値を選択し、「削除」をクリックします。
5. 終了したら、「了解」をクリックします。変更が適用され、「作成属性のマッピングと値の定義」ダイアログボックスが閉じられます。
6. もう一度「了解」をクリックして「作成属性のマッピングと値」ダイアログボックスを閉じます。

属性の削除

作成属性のマッピングまたは値を削除するには

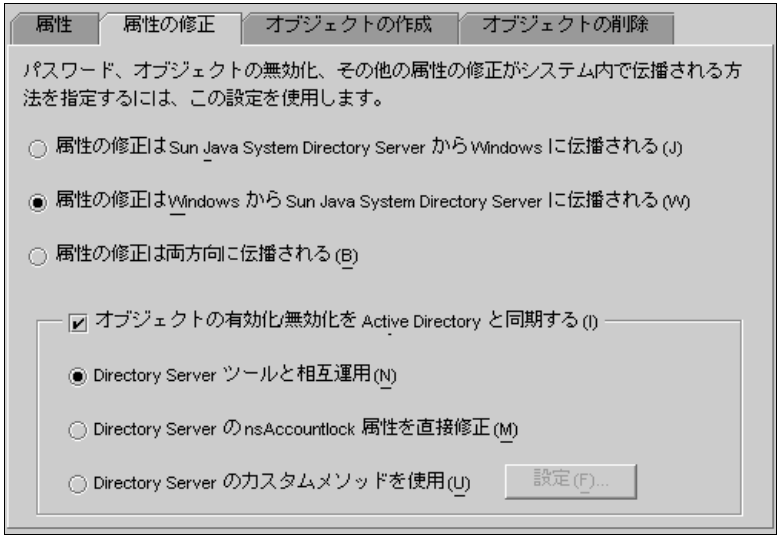
1. 「オブジェクトの作成」タブをクリックし、選択している作成オプションの下にある「属性の作成」ボタンをクリックします。
2. 「作成属性のマッピングと値」ダイアログボックスが表示されるので、表から属性を選択し、「削除」ボタンをクリックします。

   属性は、表から直ちに削除されます。
3. 終了したら、「了解」をクリックして「作成属性のマッピングと値」ダイアログボックスを閉じます。

オブジェクト修正フローの方向の指定

Sun と Windows のシステム間でユーザー属性とパスワードの変更がどのように伝達されるかを制御するときは、「属性の修正」タブ (図 4-42) を使用します。

図 4-42　「属性の修正」タブ



このタブでは、次の操作を行えます。

- Directory Server と Windows ディレクトリソースの間の修正フローの方向を指定する
- Directory Server と Active Directory のディレクトリソース間で、オブジェクトの有効化と無効化を同期させるかどうかを指定し、ユーザーアカウントを有効化および無効化する方法を指定する

注	アカウントの状態を Windows NT ディレクトリソースと同期させることはできません。

方向の指定

Directory Server および Windows 環境で加えられた変更がどのようにシステム間で伝達されるかを指定するときは、次のいずれかのボタンを選択します。

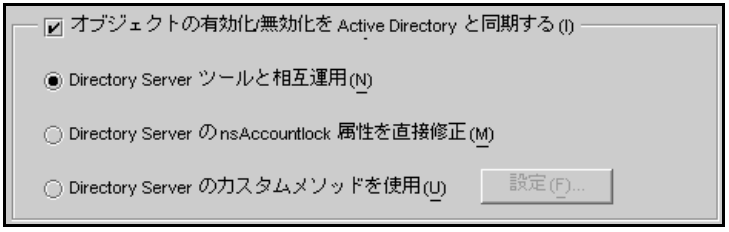
- **属性の修正は Sun Java System Directory Server から Windows に伝播される** : Directory Server 環境で加えられた変更が Windows サーバーに伝達される
- **属性の修正は Windows から Sun Java System Directory Server に伝播される** (デフォルト): Windows 環境で加えられた変更が Directory Server に伝達される
- **属性の修正は両方向に伝播される** : 変更は一方の環境からもう一方の環境に双方向に伝達される

オブジェクトの有効化と無効化の設定と同期

「オブジェクトの有効化 / 無効化を Active directory と同期する」ボックス (図 4-43 を参照) にチェックマークを付けることで、Directory Server と Active Directory のディレクトリソース間でオブジェクトの有効化と無効化を同期させることができます。

注	有効化と無効化を Windows NT ディレクトリソースと同期させることはできません。

図 4-43　オブジェクトの有効化と無効化の同期



オブジェクトの有効化と無効化を同期させるには

1. 「オブジェクトの有効化 / 無効化を Active directory と同期する」ボックスにチェックマークを付けます。
2. 次のいずれかのボタンを有効にして、オブジェクトの有効化と無効化を Identity Synchronization for Windows がどのように検出し、同期させるかを指定します。
    - **Directory Server ツールと相互運用** (141 ページを参照)

- Directory Server の nsAccountlock 属性を直接修正 (142 ページを参照)
- Use Directory Server のカスタムメソッドの設定 (143 ページを参照)

注 これらのオプションは、互いに排他的です。

- 「Directory Server ツールと相互運用」オプションを有効にした場合、Identity Synchronization for Windows は nsAccountLock 属性を直接設定または削除できなくなる。また、cn=nsdisabledrole, <*database suffix*> などの別のロールや、cn=nsdisabledrole, <*database suffix*> または cn=nsmanageddisabledrole, <*database suffix*> のように別のロール内に入れ子にされたロールを使用して無効化されたオブジェクトも検出できなくなる
- 「Directory Server の nsAccountlock 属性を直接修正」オプションを有効にした場合、Identity Synchronization for Windows は Directory Server のコンソールまたはコマンド行インタフェースを使用して有効化または無効化したオブジェクトを検出しなくなる
- 「Use Directory Server のカスタムメソッドの設定」オプションを有効にした場合、ディレクトリへのアクセスが Sun Java™ System Access Manager (従来の Sun JES Identity Server) などの外部アプリケーションによって制御されている場合を除き、Identity Synchronization for Windows はオブジェクトをディレクトリからロックアウトできなくなる

Directory Server ツールと相互運用

オブジェクトの有効化と無効化に Directory Server のコンソールまたはコマンド行ツールを使用する場合は、このオプションを選択します。

- オブジェクトを有効化する場合、Identity Synchronization for Windows は nsroledn 属性から cn=nsmanageddisabledrole,<*database suffix*> の値を削除する
- オブジェクトを無効化する場合、Identity Synchronization for Windows は nsroledn 属性に cn=nsmanageddisabledrole,<*database suffix*> の値を追加する

注 「Directory Server ツールと相互運用」オプションを有効にした場合、Identity Synchronization for Windows は nsAccountLock 属性を直接設定または削除できなくなります。また、その他のロールを使用して無効化されたオブジェクトも検出できなくなります。

たとえば、cn=nsdisabledrole, <*database suffix*> などのロールや、cn=nsdisabledrole, <*database suffix*> または cn=nsmanageddisabledrole, <*database suffix*> のように他のロール内にネスト化されたロールがこれに該当します。

表 4-1 は、「Directory Server ツールと相互運用」オプションを有効化した場合に、Identity Synchronization for Windows がオブジェクトの有効化と無効化をどのように検出し、同期させるかを示しています。

表 4-1　Directory Server ツールと相互運用

有効化 :	無効化
Identity Synchronization for Windows は、オブジェクトから cn=nsmanageddisabledrole,<*database suffix*> ロールが削除された場合にだけ有効化を検出する	Identity Synchronization for Windows は、エントリの nsroledn 属性に cn=nsmanageddisabledrole,<*database suffix*> ロールが含まれる場合にだけ無効化を検出する
Active Directory からのオブジェクト有効化を同期させる場合、Identity Synchronization for Windows は、オブジェクトから cn=nsmanageddisabledrole,<*database suffix*> ロールを削除することでオブジェクトを有効化する	Active Directory からのオブジェクト無効化を同期させる場合、Identity Synchronization for Windows は、オブジェクトに cn=nsmanageddisabledrole,<*database suffix*> ロールを追加することでオブジェクトを無効化する

Directory Server の nsAccountlock 属性を直接修正

Directory Server の有効化と無効化が Directory Server のオペレーション属性 nsAccountLock に基づく場合は、このオプションを使用します。この属性は、オブジェクトの状態を次のように制御します。

- nsAccountLock=true の場合、オブジェクトは無効化されており、ユーザーはログインできない
- nsAccountLock=false の場合 (または値を持たない場合)、オブジェクトは有効化されている

表 4-2 は、「Directory Server の nsAccountlock 属性を直接修正」オプションを有効にした場合に Identity Synchronization for Windows がオブジェクトの有効化と無効化をどのように検出し、同期させるかを示しています。

表 4-2　Directory Server の nsAccountlock 属性を直接修正

有効化	無効化
Identity Synchronization for Windows は、nsAccountLock 属性が **true** に設定されている場合にだけ、無効化されたオブジェクトを検出する	Identity Synchronization for Windows は、nsAccountLock 属性に値が設定されていない、または **false** に設定されている場合にだけ、有効化されたオブジェクトを検出する

表 4-2　Directory Server の nsAccountlock 属性を直接修正

Active Directory からオブジェクト無効化を同期させる場合、Identity Synchronization for Windows は nsAccountLock 属性を削除する	Active Directory からオブジェクト有効化を同期させる場合、Identity Synchronization for Windows は nsAccountLock 属性を **true** に設定する

Use Directory Server のカスタムメソッドの設定

Directory Server の有効化と無効化が Sun Java™ System Access Manager (従来の Sun JES Identity Server) などの外部アプリケーションによって完全に制御されている場合は、このオプションを使用します。

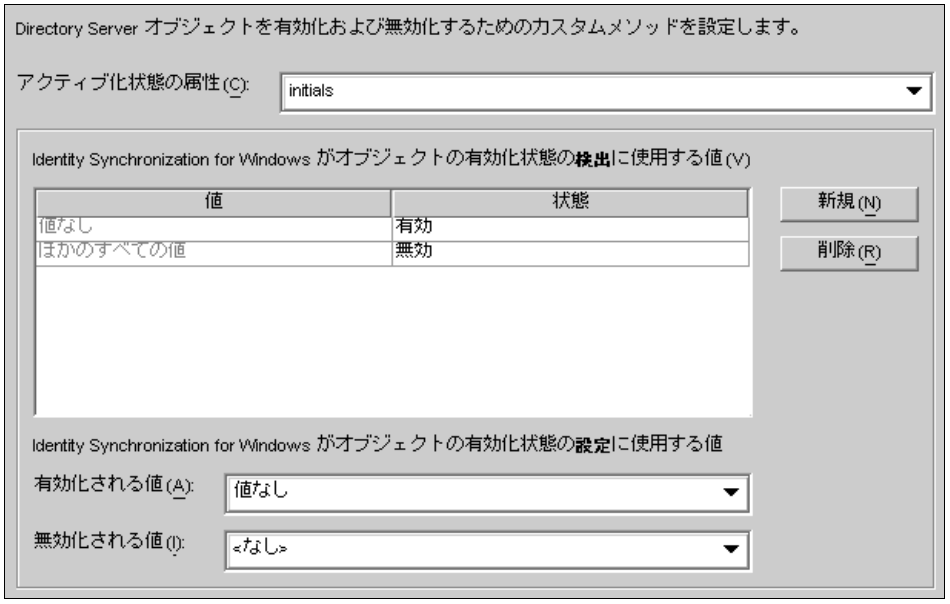
Directory Server 用のカスタムメソッドを設定するときは、次の条件を指定する必要があります。

- 外部アプリケーションが Directory Server 内のオブジェクトを有効化または無効化したことを、Identity Synchronization for Windows がどのように検出するか
- Active Directory から Directory Server への同期で、Identity Synchronization for Windows がオブジェクトをどのように有効化または無効化するか

注　「Use Directory Server のカスタムメソッドの設定」オプションを有効にした場合、ディレクトリへのアクセスが Access Manager などの外部アプリケーションによって制御されている場合を除き、Identity Synchronization for Windows はオブジェクトをディレクトリからロックアウトできなくなります。

有効化と無効化のカスタムメソッドを設定するときは、「設定」ボタンをクリックして「Directory Server のカスタムメソッドの設定」ダイアログボックス (図 4-44) を表示します。

図 4-44 有効化と無効化のカスタムメソッドの設定



このダイアログボックスには次の機能があります。

- **「アクティブ化状態の属性」ドロップダウンリスト** : Directory Server と Active Directory の間での有効化と無効化の同期に Identity Synchronization for Windows が使用する属性をこのリストから選択する

  このリストには、現在選択している Directory Server の Structural および Auxiliary オブジェクトクラスのスキーマに含まれる、すべての属性が表示される

- **「値」と「状態」の表** : 選択した属性と関連する値が、どのような場合に有効化または無効化されるかを指定する

  - **「値」列** : 有効または無効の状態を示すために使用される属性値を、この列と「新規」および「削除」ボタンを使用して指定する

    プログラムは、この列に自動的に 2 つの値を指定する

    - **値なし** : 有効時に属性は値を持たない
    - **ほかのすべての値** : 有効時に属性は値を持つが、「値」と「状態」の表に指定されている値ではない

  - **「状態」列** : 同じ行の「値」エントリに対応して有効化または無効化されるオブジェクトを、この列を使用して指定する

表 4-3　有効化状態と無効化状態の指定

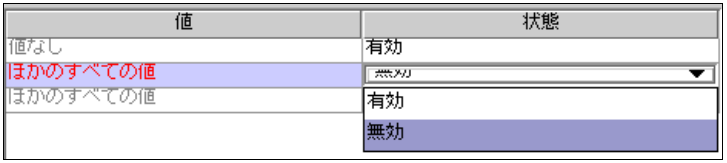
値	状態	結果
値なし	有効	属性が指定されていない、または値を持たない場合、Identity Synchronization for Windows はオブジェクトが有効であると見なす
	無効 :	属性が指定されていない、または値を持たない場合、Identity Synchronization for Windows はオブジェクトが無効であると見なす
<*user-defined*> の値	有効	属性が <*user-defined*> 属性を持つ場合、Identity Synchronization for Windows はオブジェクトが有効であると見なす
	無効 :	属性が <*user-defined*> 属性を持つ場合、Identity Synchronization for Windows はオブジェクトが無効であると見なす
ほかのすべての値	有効	属性が、表に指定されていない値を持つ場合、Identity Synchronization for Windows はオブジェクトが有効であると見なす
	無効 :	属性が、表に指定されていない値を持つ場合、Identity Synchronization for Windows はオブジェクトが無効であると見なす

- **「新規」ボタン** :「値」列に新しいエントリを追加するときは、このボタンをクリックする
- **「削除」ボタン** : エントリを削除するときは、「値」列でエントリを選択し、このボタンをクリックする
- **「有効化される値」および「無効化される値」ドロップダウンリスト** : Identity Synchronization for Windows がオブジェクトの状態の設定に使用する値を指定するときは、これらのリストを使用する

有効化と無効化の同期 : Directory Server と Active Directory の間でオブジェクトの状態を検出し、それを同期させるように Identity Synchronization for Windows を設定する手順は、次のとおりです。

1. 「アクティブ化状態の属性」ドロップダウンリストから属性を選択します。
2. 「新規」ボタンをクリックし、表の「値」列に属性値を追加します。
3. 各「値」エントリに対応する「状態」列の内側をクリックし、表示されるドロップダウンリストから「有効」または「無効」を選択します。

図 4-45　状態の選択



たとえば、Access Manager を使用している場合は、次のように指定します。

1. 「アクティブ化状態の属性」ドロップダウンリストから **inetuserstatus** を選択します。
2. 「新規」ボタンをクリックし、表の「値」列で **active**、**inactive**、**deleted** の各属性の値を入力します。
3. 各値に対応する「状態」列をクリックし、「有効」または「無効」を次のように選択します。
   - **値なし** : 有効
   - active: 有効
   - inactive: 無効
   - deleted: 無効
   - **ほかのすべての値** : 無効

表 4-4 は、この inetuserstatus の例に基づいて、「Use Directory Server のカスタムメソッドの設定」オプションを有効にした場合に Identity Synchronization for Windows がどのように有効化と無効化を検出し、それを同期させるかを示しています。

表 4-4　inetuserstatus の値を使用した例の結果

値	状態	結果
値なし	有効	inetuserstatus 属性が指定されていない、または値を持たない場合、Identity Synchronization for Windows はオブジェクトが有効であると見なす
active	有効	属性の値が **active** の場合、Identity Synchronization for Windows はオブジェクトが有効であると見なす
inactive	無効	属性の値が **inactive** の場合、Identity Synchronization for Windows はオブジェクトが無効であると見なす
deleted	無効	属性の値が **deleted** の場合、Identity Synchronization for Windows はオブジェクトが無効であると見なす

表 4-4　inetuserstatus の値を使用した例の結果 (続き)

値	状態	結果
ほかのすべての値	無効	属性が、表に指定されていない値を持つ場合、Identity Synchronization for Windows はオブジェクトが無効であると見なす

有効化と無効化の設定 : エントリと共に「値」と「状態」の表を取り込むと、Identity Synchronization for Windows は自動的に **「有効化される値」**および **「無効化される値」**ドロップダウンリストを次のように取り込みます。

- 「有効化される値」リストには、状態が「有効」のすべての値が含まれる
  たとえば、**`No Value`**、**`active`**
- 「無効化される値」リストには、状態が「無効」のすべての値が含まれる
  たとえば、**`inactive`**、**`deleted`**
- どちらのリストにも「ほかのすべての値」の値は含まれない

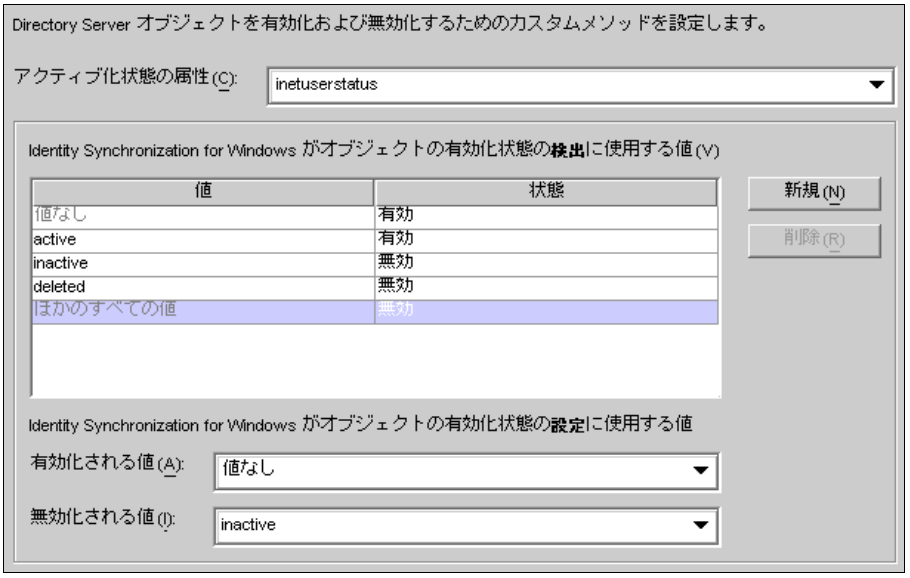
Active Directory から同期されるオブジェクトを Identity Synchronization for Windows がどのように有効化または無効化するかを指定するには、「有効化される値」、「無効化される値」、または両方のドロップダウンリストから値を選択します。

- **有効化される値** : オブジェクトの有効状態を制御する
  - **値なし** : オブジェクトに active という値が含まれている場合、Identity Synchronization for Windows は Directory Server 側の状態を有効に設定する
  - active: オブジェクトに active という値が含まれている場合、Identity Synchronization for Windows は Directory Server 側の状態を有効に設定する
- **無効化される値** : オブジェクトの有効状態を制御する
  - inactive または deleted: Identity Synchronization for Windows は Directory Server 側のオブジェクトの状態を無効に設定する
  - **< なし >**: 設定が無効である。値を選択しなければならない

注　無効化される値を指定する必要があります。指定しない場合、設定は無効となります。

図 4-46 は、設定が完了した「Directory Server のカスタムメソッドの設定」ダイアログボックスを示しています。

図 4-46　設定が完了したダイアログボックスの例



削除フローの方向の指定

Directory Server と Active Directory のシステム間でユーザーエントリの削除をどのように伝達させるかを指定するには、「オブジェクトの削除」タブを使用します。

注　Windows NT ではオブジェクト削除のフローを指定できません。

1. ナビゲーションパネルの最上位にある Identity Synchronization for Windows ノードを選択し、「オブジェクトの削除」タブをクリックします。

図 4-47　ユーザーエントリの削除の伝達

2. 削除のフローを次のように有効化、または無効化します。
   - Directory Server 環境から Active Directory サーバーに削除を伝達するときは、**「オブジェクトの削除は Sun Java System Directory Server から Active Directory に伝播される」**にチェックマークを付ける
   - Active Directory 環境から Directory Server に削除を伝達するときは、**「オブジェクトの削除は Active Directory から Sun Java System Directory Server に伝播される」**にチェックマークを付ける
   - 双方向のフローを設定するときは、両方のオプションにチェックマークを付ける
   - システム間でユーザー削除を伝達しない場合は、どちらのオプションにもチェックマークを付けない (デフォルト設定)

同期ユーザーリストの作成

同期ユーザーリスト (SUL) は、2 つのディレクトリソース内のどのユーザーを同期させるかを指定します。SUL に指定されたすべてのエントリはコネクタを通過し、その SUL に設定されている制約事項に対して評価されます。

各 SUL には 2 つの要素が含まれ、1 つは同期対象の Directory Server ユーザーを識別し、もう 1 つは同期対象の Windows ユーザーを識別します。

注

Directory Server のユーザーを複数の Active Directory ドメインと同期させるには、Active Directory ドメインごとに SUL を定義する必要があります。

定義のコンポーネント、複数 SUL の定義方法、複数 SUL の処理のしくみ、複数の Windows ドメインのサポートを設定する方法など、SUL の定義と設定については、335 ページの付録 D 「同期ユーザーリストの定義と設定」を参照してください。

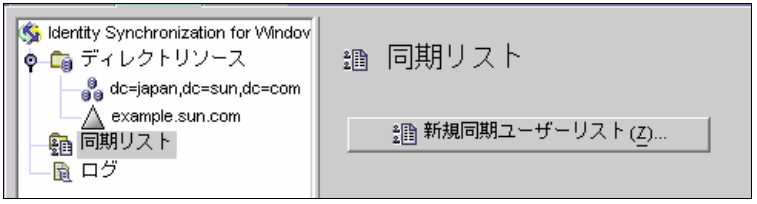
どちらの SUL 要素にも、同期させるユーザーを識別するための 3 つの定義が含まれます。

- **ベース DN** : 同期させるユーザーの位置 (NT には適用されない)
- **ネーミング属性** : 新規作成ユーザーに適用される属性 (作成式) (NT には適用されない)
- **フィルタ** : 特定のユーザーを同期対象から外す

サーバー間でユーザータイプを識別し、リンクさせるには

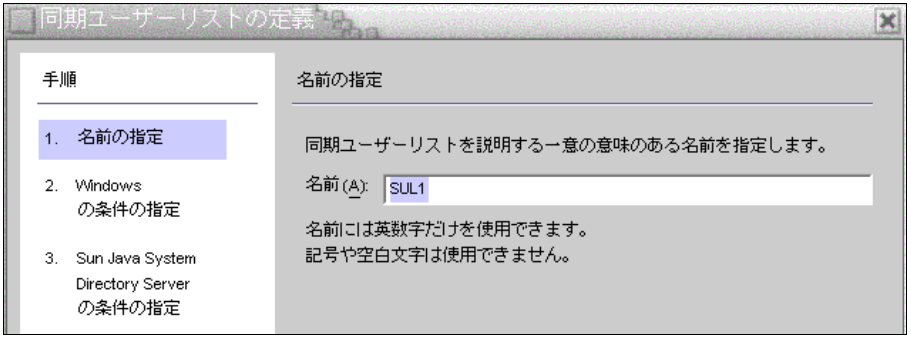
1. ナビゲーションツリーで同期ユーザーリストのノードを選択し、「新規同期ユーザーリスト」ボタンをクリックします。

図 4-48 同期ユーザーリストの新規作成



次のような「同期ユーザーリストの定義」ウィザードが表示されます。

図 4-49　　SUL 名の指定



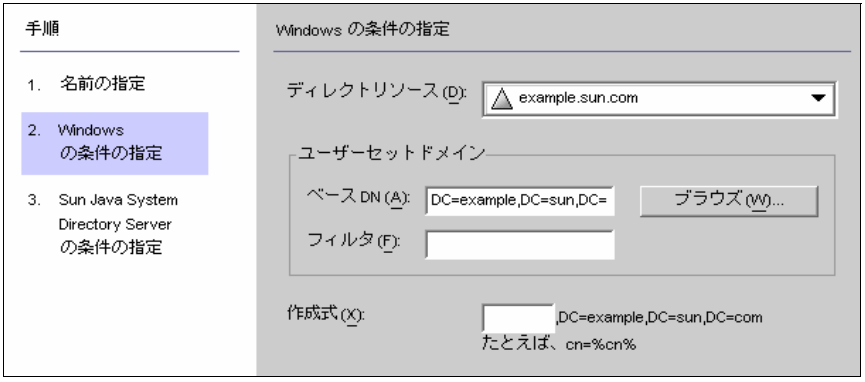
最初の同期ユーザーリストの名前は、デフォルトで *SUL1* となります。

- デフォルトの名前をそのまま使用するときは、「次へ」をクリックする
- 別の名前を指定するときは、「名前」フィールドに別の名前を入力してから「次へ」をクリックする

注
- SUL 名には空白文字や記号を含めることはできない
- システム内で一意の名前を指定する必要がある

図 4-50 のような「Windows の条件の指定」パネルが表示されます。

図 4-50　　Windows 条件の指定

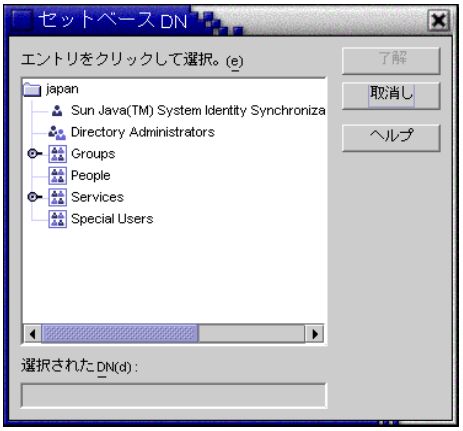


2. ドロップダウンメニューから Windows ディレクトリソースを選択します。

注	SUL の作成後にこのディレクトリソースを編集することはできません。

3. 「ユーザーセットドメイン」は、同期対象となるすべてのユーザーのセットです。次のいずれかの方法で、「ユーザーセットドメイン」の「ベース DN」を入力します。
   - テキストフィールドに名前を入力する (たとえば、**`DC=example,DC=com`**)
   - 「ブラウズ」ボタンをクリックして「セットベース DN」ダイアログボックスを開き、ベース DN を検索し、選択する

図 4-51　ベース DN の選択



フィルタを使用して明示的に除外しないかぎり、指定したベース DN の下のすべてのユーザーがこの SUL に含まれます。

注	Windows NT マシンでは、ベース DN と作成式は使用できません。

4. 等価、実在、または部分文字列フィルタを入力して、このベース DN のどのユーザーを同期させるかを指定することができます。たとえば、複数の同期ユーザーリストで同じベース DN を使用する場合は、フィルタを使用してリストを区別できます。

   等価フィルタの構文は、LDAP クエリの構文に似ています。ただし、等価部分文字列で使用できる文字は *、&、|、=、! だけです。たとえば、次のフィルタを使用して、SUL から管理者を除外することができます。

   `(!(cn=Administrator))`

「作成式」フィールドの内容は、プログラムによって自動的に挿入されます。

注 作成式は、新しいエントリが Active Directory から Directory Server に伝達されるときに使用される親 DN とネーミング属性を定義します。

ユーザー属性の作成が Active Directory から Directory Server に伝達されるように指定していない限り (133 ページの「オブジェクト作成のフローの指定」を参照)、Sun のディレクトリで作成式を使用することはできません。

5. 作成式が指定されていない、または既存のエントリを変更するときは、Windows Active Directory のすべての同期ユーザーリストに適用される作成式を、たとえば次のように入力できます。

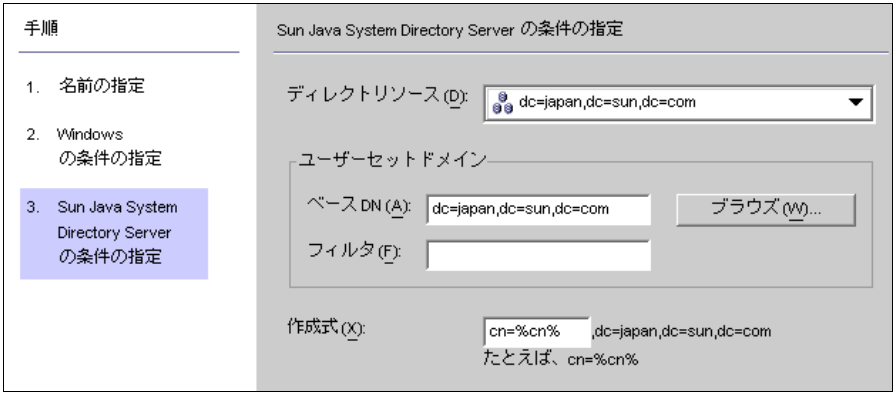
   `cn=`*%cn%*`,cl=`***users***`,dc=example,dc=com`**

   作成式を変更するときは、同期させる属性を選択する必要があります。必要に応じて「オブジェクトの作成」タブに戻り、「属性の作成」ボタンをクリックしてこの属性をマッピングしてください。

6. 「次へ」をクリックして、Sun Java System Directory Server の条件を指定します。

7. 「Sun Java System Directory Server の条件の指定」パネルが表示されたら、手順 2 から手順 5 を繰り返し、Directory Server の条件を指定します。

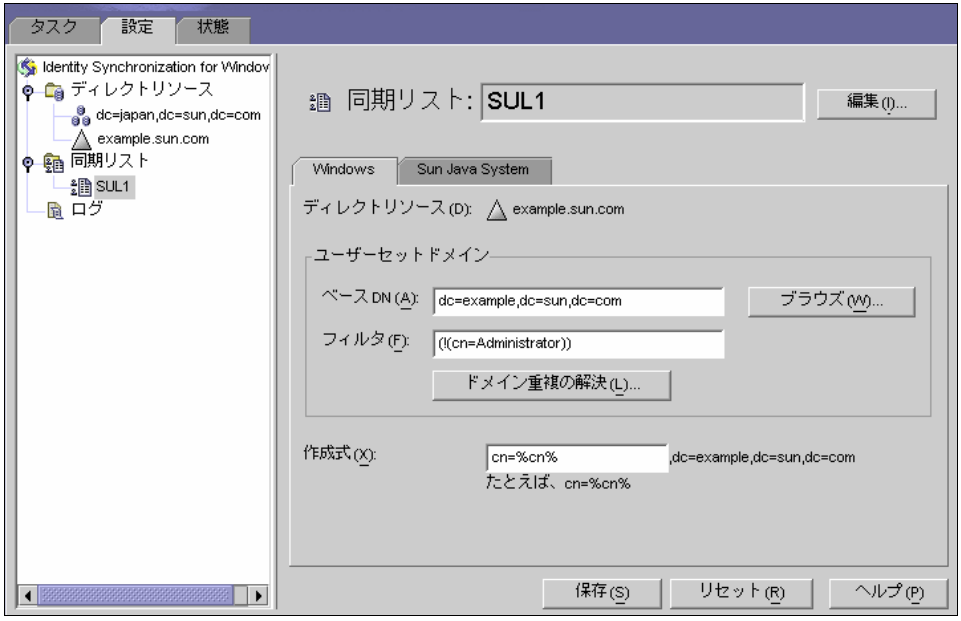
図 4-52 Directory Server の条件の指定



注 「終了」ボタンをクリックして SUL を作成した後に、この SUL に含まれる Active Directory または Directory Server ディレクトリソースを編集することはできません。

8. 終了したら、「終了」をクリックします。
9. ナビゲーションツリーに新しい SUL ノードが追加され、「設定」タブに「同期ユーザーリスト」パネルが表示されます。

図 4-53　「同期リスト」パネル



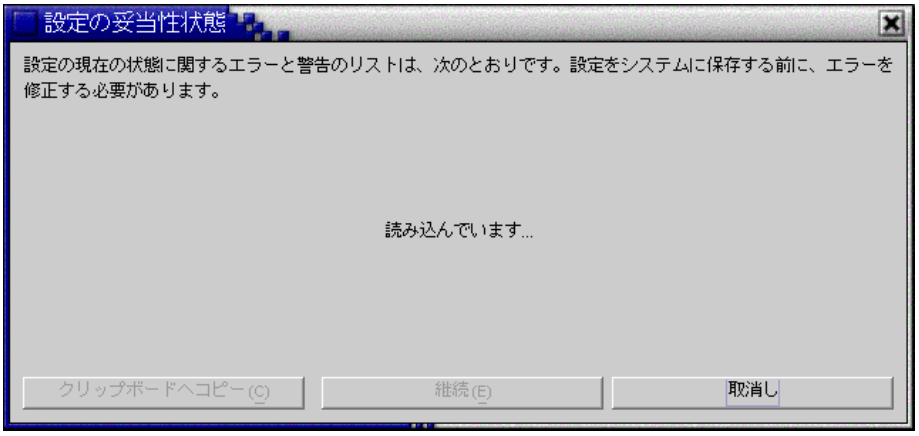
10. ユーザーが複数のリストと一致する場合は、「ドメイン重複の解決」ボタンをクリックして同期ユーザーリストの設定を定義します。詳細は、335 ページの「同期ユーザーリストの定義について」を参照してください。
11. Directory Server 以外のネットワーク上のすべてのディレクトリソースが含まれる同期ユーザーリストを作成します。

設定の保存

現在の設定をコンソールパネルから保存するには

1. 「保存」をクリックして、その時点での設定を設定ディレクトリに格納します。
2. 設定がプログラムによって評価され、「設定の妥当性状態」ウィンドウが表示されます。

図 4-54　「設定の妥当性状態」ウィンドウ



プログラムによる設定ディレクトリへの情報の再書き込みと、システムマネージャへの通知のため、設定の保存には数分かかります。

システムマネージャ (コアコンポーネント) は、情報を必要とするコンポーネントに設定情報を送ります。

注　設定の検証エラーは赤、警告は黄色で表示されます。

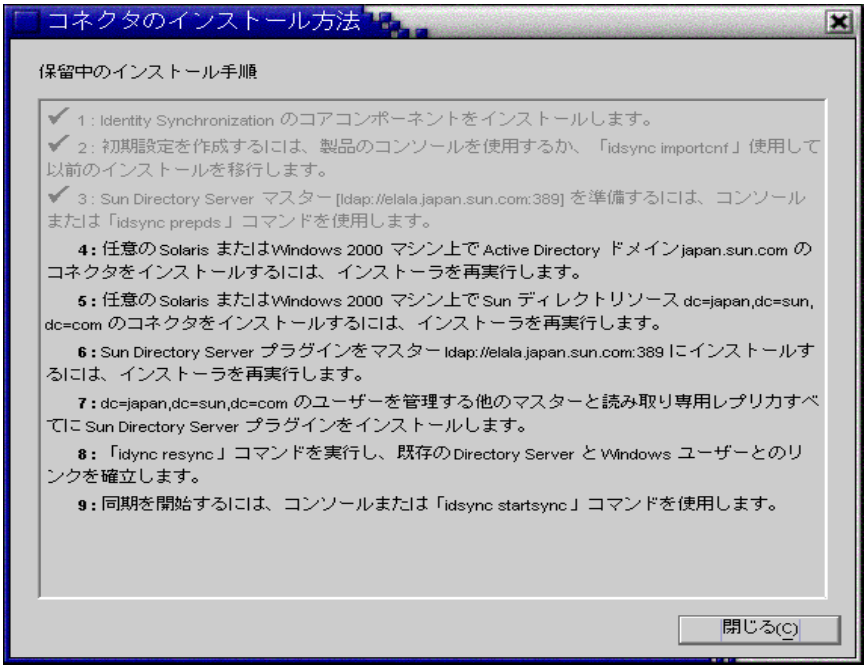
- エラーを残した状態で設定を保存することはできない
- 警告を残した状態でも設定を保存できるが、保存前に警告状態を解消しておくべきである

3. 設定が有効であれば、「継続」をクリックして設定を保存します。

Identity Synchronization for Windows のコネクタとサブコンポーネントをインストールする方法を示す「コネクタのインストール方法」ダイアログボックスが表示されます (図 4-55 のリストに類似する)。

このリストには汎用の手順が表示されていましたが、この時点で更新され、これ以後は配備に適した実行手順が表示されるようになります。実行手順リストへのアクセスと更新は、Identity Synchronization for Windows コンソールの「状態」タブでも行えます。

図 4-55　　コネクタのインストールに関する指示



4. 表示される情報をよく読み、「了解」をクリックします。

コアの初期設定が完了すると、Identity Synchronization for Windows のコネクタとサブコンポーネントをインストールする準備が整います。インストール方法については、次の第 5 章「コネクタと Directory Server プラグインのインストール」を参照してください。

第 5 章

コネクタと Directory Server プラグインのインストール

この章では、Identity Synchronization for Windows コネクタと Directory Server プラグインをインストールする方法について説明します。この章で説明する内容は、次とおりです。

Identity Synchronization for Windows は、ディレクトリソース間でのユーザーパスワードの同期にコネクタを使用し、コネクタによる変更検出の強化と双方向同期のサポートにサブコンポーネントを使用します。

はじめに

コネクタと Directory Server プラグインのインストールプロセスを開始する前に、次の事項に注意してください。

- インストールプロセスを開始する前にコンソールを閉じる。コネクタまたはプラグインのインストール時にコンソールが開いていると、コンポーネントがサーバーに設定データを追加している状態をプログラムが競合として認識し、エラーメッセージが出力される
- Directory Server プラグインは、マスター、レプリカ、ハブも含め、同期対象ユーザーが格納されている、配備内のすべての Directory Server マシンにインストールする必要がある
- Active Directory コネクタにはサブコンポーネントがない

- Windows NT のコネクタとサブコンポーネントは同時にインストールされる
- Directory Server または Active Directory のコネクタは、コアと同じマシンにインストールすることも、別のマシンにインストールすることもできる。Windows NT のコネクタは、同期対象ドメインの主ドメインコントローラ (PDC) にインストールする必要がある
  - コアと同じマシンにコネクタをインストールする場合、プログラムは自動的にコアと同じディレクトリにコネクタをインストールする
  - コネクタを別のマシンでインストールする場合、プログラムは次の情報の指定を要求する
    - コアのインストール時に提供される、設定ディレクトリに関する情報
    - インストールディレクトリ
- インストールプログラムは、コネクタまたは Directory Server プラグインをインストールするたびに実行する必要がある

  たとえば、Directory Server コネクタ、1 つの Directory Server プラグイン、Active Directory コネクタをインストールする場合は、コアのインストール後にインストールプログラムを合計 3 回実行する

インストールプログラムの実行

インストールプログラムを再起動して実行する手順は、次のとおりです。コネクタまたは Directory Server プラグインをインストールするたびに、この手順を繰り返します。

1. コネクタをインストールするマシンで、インストールプログラムを次のように再実行します。
   - Solaris 環境 : `installer` ディレクトリに移動し、**`./runInstaller.sh`** と入力してインストールプログラムを実行する

     注 インストールプログラムをテキストベースモードで実行するには、**`./runInstaller.sh -nodisplay`** と入力します。

     `runInstaller.sh` プログラムを実行した場合、パスワードがクリアテキストとしてエコーされないように、Identity Synchronization for Windows はパスワードを自動的にマスクします。

   - Windows 環境 : `installer` ディレクトリに移動し、**`setup.exe`** と入力してインストールプログラムを実行する

2. 「ようこそ」画面が表示されたら、そこに示される情報を読み、「次へ」をクリックして「ソフトウェアライセンス契約書」パネルに進みます。
3. ライセンス契約書を読み、次のいずれかを選択します。
   - **はい (ライセンス契約書に同意する)**: ライセンスの条項に同意し、次のパネルに移動する
   - **いいえ** : セットアッププロセスを中止し、インストールプログラムを終了する
4. 「Sun Java System Directory Server」パネルが表示されます。設定ディレクトリの位置を次のように指定します。
   - **設定ディレクトリホスト** : Identity Synchronization for Windows の設定情報が格納される Sun Java System Directory Server インスタンス (Administration Server と関連する) の完全修飾ドメイン名を入力する。コアのインストール時に指定したインスタンスと同じインスタンスを指定する必要がある
   - **設定ディレクトリポート** (デフォルトポートは *389*): 設定ディレクトリのポートを指定する。デフォルトのポート設定を受け入れるか、別の使用可能ポートに変更する

     コアと設定ディレクトリの間の SSL (Secure Socket Layer) 通信を有効にするには、「セキュアポート」オプションにチェックマークを付け、SSL ポートを指定する。デフォルトの SSL ポートは *636*。このオプションを有効にすることで、機密情報がクリアテキスト形式でネットワーク上を転送されることを防止できる
   - **設定ルートサフィックス** : コアのインストール時に指定したルートサフィックスをメニューから選択する。Identity Synchronization for Windows の設定は、このルートサフィックスに格納される

   注 プログラムがルートサフィックスを検出できず、サーバー情報を手動で入力する場合は、「更新」をクリックしてルートサフィックスのリストを取り込み直す必要があります。
5. 「次へ」をクリックし、「設定ディレクトリのクレデンシャル」パネルを開きます。
6. 設定ディレクトリの管理ユーザー ID とパスワードを入力します。
   - ユーザー ID として `admin` を指定した場合は、ユーザー ID を DN として指定する必要はない
   - それ以外のユーザー ID を指定した場合は、ID を完全 DN として指定する必要がある
     たとえば、*cn=Directory Manager* のように指定する

   注 手順 4 で SSL を有効にしなかった場合、これらのクレデンシャルは暗号化されずに送信されます。

7. 「次へ」をクリックして「設定パスワード」パネルを開きます。このパネルには、コアのインストール時に指定したパスワードを入力する必要があります。

   また、このマシンにコアがインストールされていない場合は、Java ホームディレクトリの位置 (91 ページ) を指定するように求められます。

8. 完了したら「次へ」をクリックします。

注 これ以後は、Directory Server プラグインをインストールするか、いずれかのコネクタをインストールするかによって操作方法が異なります。

- コネクタをインストールする場合は、160 ページの「コネクタのインストール」に進む
- Directory Server プラグインをインストールする場合は、171 ページの「Directory Server プラグインのインストール」に進む

コネクタのインストール

ここでは、3 種類の Identity Synchronization for Windows コネクタをインストールする方法について説明します。

- 161 ページの「Directory Server コネクタのインストール」
- 166 ページの「Active Directory コネクタのインストール」
- 170 ページの「Windows NT コネクタのインストール」

注 コネクタは特定の順序でインストールする必要はありませんが、複数のコネクタを並行してインストールしないようにしてください。

Directory Server コネクタのインストール

158 ページの「インストールプログラムの実行」で説明した手順が完了すると、「コネクタの設定」パネルが表示されます。

図 5-1　Directory Server コネクタの選択

「インストールするコンポーネントを選択します」リストには、まだインストールされていないコネクタコンポーネントだけが含まれます。たとえば、Directory Server コネクタ (図 5-1 の dc=example,dc=com) をインストールした後は、このエントリはリストから削除されます。

次の表は、ディレクトリソースエントリの例を示しています。

表 5-1　ディレクトリソースの例

ディレクトリソース	エントリの例
Sun Java System Directory Server	`dc=example,dc=com`
Windows Active Directory	`example.com`
Windows NT SAM	`EXAMPLE`

Directory Server コネクタをインストールするには

1. ディレクトリサーバーコネクタコンポーネントの隣のボタンを有効にし、「次へ」をクリックします。

   「Directory Server コネクタのクレデンシャル」パネル (図 5-2) が表示されます。

図 5-2　Directory Server コネクタのクレデンシャルの入力

注　ユーザー DN のフィールドには、ディレクトリマネージャの完全修飾識別名が自動的に指定されますが、必要に応じて変更できます。

次の情報を入力します。

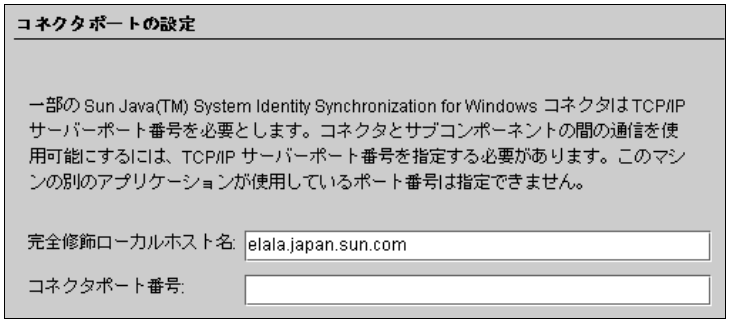
- **主 Directory Server ユーザー DN** : 必要に応じてディレクトリマネージャの完全修飾識別名を入力し、デフォルトのユーザー DN を変更する
- **主 Directory Server パスワード** : ディレクトリマネージャのパスワードを入力する

二次マスターを使用している環境では、二次 Directory Server のユーザー名とパスワードを指定するフィールドが設定可能になります。ディレクトリマネージャの DN フィールドには、主 Directory Server ユーザーの DN フィールドとパスワードフィールドと同じ内容が自動的に指定されます。この情報は、必要に応じて変更できます。

Directory Server でデータの同期準備が整っているかどうかが検証されます。Directory Server の準備が完了している場合は (111 ページを参照)、Directory Server への接続にコネクタが使用するアカウントが作成されます (たとえば、uid= `PSWConnectors`*suffix*)。

2. 「次へ」をクリックし、「コネクタポートの設定」パネルに進みます。

図 5-3　　コネクタのローカルホストとポートの指定

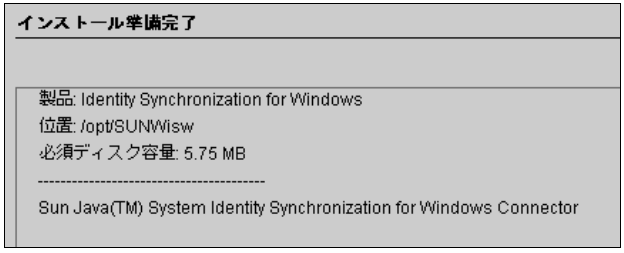


3. 完全修飾ローカルホスト名と、コネクタが待機する使用可能ポートの番号を入力します。すでに使用されているポートを指定すると、エラーメッセージが出力されます。

   Directory Server プラグインは、コンソールで保存した設定情報へのアクセスを必要とします。この情報を取得するために、プラグインはこのポートのサーバーソケットを通じて Directory Server コネクタと通信します。また、ログメッセージをセントラルログに記録するために、プラグインはこのチャネルを経由してメッセージを記録します。

4. 「次へ」をクリックして「インストール準備完了」パネルを表示します。このパネルには、コネクタのインストール先と、インストールに必要なディスク容量が表示されます。問題がなければ、「すぐにインストール」ボタンをクリックします。

図 5-4　　「インストール準備完了」パネル



注 コアをローカルマシンにインストールした場合、コネクタのインストールに必要な容量が「インストール準備完了」パネルにゼロと表示されます。これは、コアのインストールがコネクタバイナリをすでにインストールしているためです。追加インストールが必要なバイナリが存在しないため、追加容量も必要ありません。

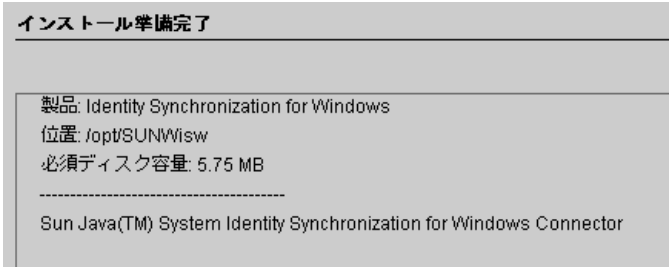
コアをインストールしたマシンとは異なるマシンにコネクタをインストールする場合は、ローカルマシンへのコネクタのインストールに必要な容量が「インストール準備完了」パネルに表示されます。

コネクタのインストールは、次の 2 段階で行われます。

- プログラムがバイナリのインストールを開始し、進捗状況バーを持つインストールパネルが表示される
- 次に、「コンポーネントの設定」パネルが表示される。この処理の完了には数分間かかるため、進捗状況バーが表示される

注 インストールを開始する前にコンソールを閉じなかった場合、警告が表示されます (図 5-5 を参照)。コンソールで「更新」をクリックし、コネクタの設定を読み込み直してください。

図 5-5 「設定に関する警告」ダイアログボックス



両方の段階が完了すると、「インストール概要」パネルが表示されます。

5. インストールログを表示するときは、「詳細」をクリックします。
   - Solaris 環境 : インストールログは `/var/sadm/install/logs/` に書き込まれる
   - Windows 環境 : インストールログは `%TEMP%` ディレクトリに書き込まれる。通常、これは次の場所の下にある `Local Settings` フォルダのサブディレクトリである
     `C:¥Documents and Settings¥Administrator`

注 Windows 2000 Advanced Server などの一部の Windows システムでは、`Local Settings` フォルダは隠しフォルダです。

このフォルダと `Temp` サブディレクトリを表示するには、Windows エクスプローラを開き、メニューバーから「ツール」>「フォルダ」を選択します。「フォルダオプション」ダイアログボックスが表示されるので、「表示」タブの「すべてのファイルとフォルダを表示する」を有効にします。

6. 「次へ」をクリックすると、正しく完了した手順と、未完了の手順を示す実行手順リスト (図 5-6) が表示されます。

図 5-6 実行手順リスト

7. 表示内容を確認したら、「終了」をクリックします。

Directory Server コネクタのインストールの後は、リソースの設定時に指定した (第 4 章を参照) その他のコネクタ、Directory Server プラグイン、または両方をインストールできます。

- その他の Directory Server コネクタのインストール : インストールプログラムを再起動し (158 ページの「インストールプログラムの実行」を参照)、手順 1 から手順 7 を繰り返す

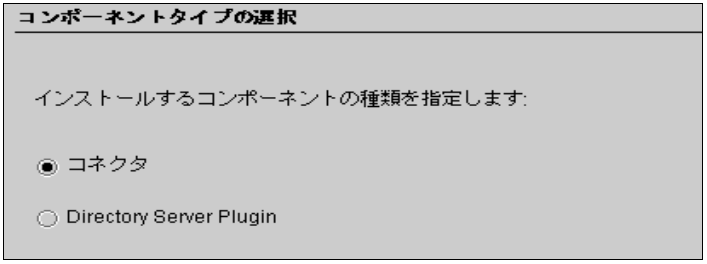
- Active Directory コネクタのインストール : 166 ページの「Active Directory コネクタのインストール」に進む
- Windows NT コネクタのインストール : 170 ページの「Windows NT コネクタのインストール」に進む
- Directory Server プラグインのインストール : 171 ページの「Directory Server プラグインのインストール」に進む

Active Directory コネクタのインストール

158 ページの「インストールプログラムの実行」で説明した手順が完了すると、「コンポーネントタイプの選択」パネルが表示されます。

注 インストールする別のコネクタが設定されている場合は、Directory Server コネクタのインストールが完了したあとに、「コネクタの設定」パネル (図 5-7 を参照) ではなく、それらのコネクタまたは Directory Server プラグインのインストールを促すオプションが表示されます。

図 5-7 コネクタの選択



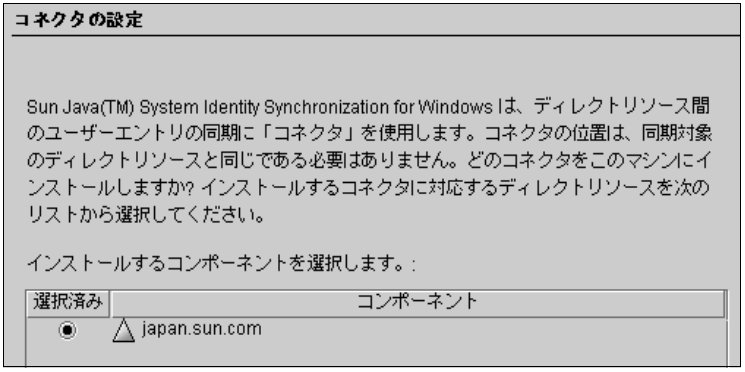
コンポーネントリストには、まだインストールされていないコネクタコンポーネントだけが含まれます。たとえば、Directory Server コネクタ (この例では dc=example,dc=com) がすでにインストールされている場合、このコンポーネントはリストに表示されません。

Active Directory コネクタをインストールするには

1. 「コネクタ」ボタンを有効にし、「次へ」をクリックします。

   「コネクタの設定」パネル (図 5-8) が表示されます。

図 5-8　　Active Directory コネクタの選択

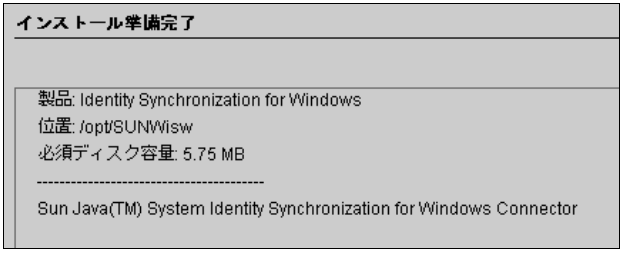


「インストールするコンポーネントを選択します」リストには、まだインストールされていないコネクタコンポーネントだけが含まれます。たとえば、Directory Server コネクタ (この例では dc=example,dc=com) のインストールが完了すると、このエントリはリストパネルに表示されなくなります。

2. Active Directory コンポーネントの隣のボタンを有効にし、「次へ」をクリックします。

「インストール準備完了」パネル (図 5-9) が表示されます。このパネルには、コネクタのインストール先と、インストールに必要なディスク容量が表示されます。

図 5-9　　「インストール準備完了」パネル



注 コアをローカルマシンにインストールした場合、コネクタのインストールに必要な容量が「インストール準備完了」パネルにゼロと表示されます。これは、コアのインストールがコネクタバイナリをすでにインストールしているためです。追加インストールが必要なバイナリが存在しないため、追加容量も必要ありません。

コアをインストールしたマシンとは異なるマシンにコネクタをインストールする場合は、ローカルマシンへのコネクタのインストールに必要な容量が「インストール準備完了」パネルに表示されます。

3. 問題がなければ、「すぐにインストール」ボタンをクリックします。

   進捗状況バーを持つ「インストールしています」パネルが表示され、プログラムがバイナリをインストールします。インストールが完了すると、それを確認する「インストール概要」パネルが表示されます。

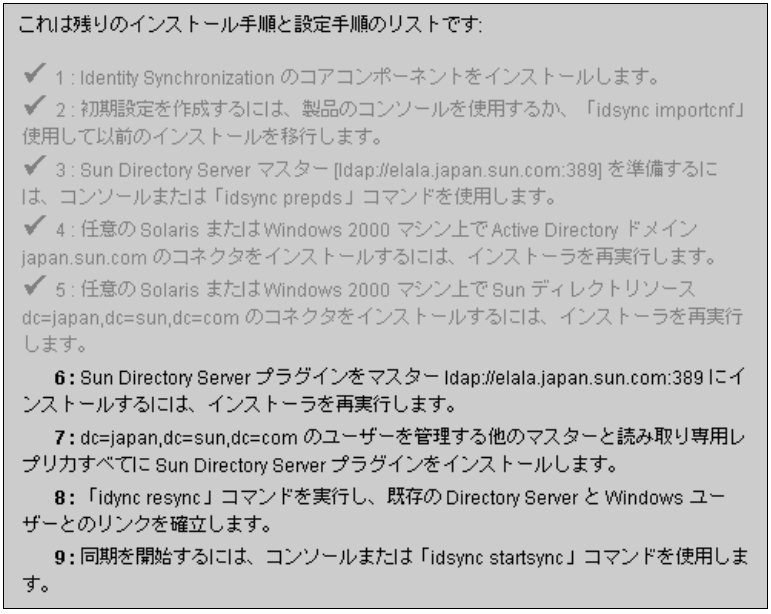
4. インストールログを表示するときは、「詳細」をクリックします。
   - **Solaris 環境** : インストールログは `/var/sadm/install/logs/` に書き込まれる
   - **Windows 環境** : インストールログは `%TEMP%` ディレクトリに書き込まれる。これは次の場所の下にある `Local Settings` フォルダのサブディレクトリである `C:¥Documents and Settings¥Administrator`

注 Windows 2000 Advanced Server などの一部の Windows システムでは、`Local Settings` フォルダは隠しフォルダです。

このフォルダと `Temp` サブディレクトリを表示するには、Windows エクスプローラを開き、メニューバーから「ツール」>「フォルダ」を選択します。「フォルダオプション」ダイアログボックスが表示されるので、「表示」タブの「すべてのファイルとフォルダを表示する」を有効にします。

5. 「次へ」をクリックすると、正しく完了した手順と、未完了の手順を示す実行手順リスト (図 5-10) が表示されます。

図 5-10　　実行手順リスト



6. 表示内容を確認したら、「終了」をクリックしてインストールプログラムを終了します。

Active Directory コネクタのインストールの後は、リソースの設定時に指定した (第 4 章を参照) その他のコネクタ、Directory Server プラグイン、または両方をインストールできます。

- その他の Active Directory コネクタのインストール : インストールプログラムを再起動し (158 ページの「インストールプログラムの実行」を参照)、手順 1 から手順 6 を繰り返す
- Windows NT コネクタのインストール : 170 ページの「Windows NT コネクタのインストール」に進む
- その他の Directory Server コネクタのインストール : インストールプログラムを再起動し (158 ページの「インストールプログラムの実行」を参照)、手順 1 から手順 7 を繰り返す
- Directory Server プラグインのインストール : 171 ページの「Directory Server プラグインのインストール」に進む

Windows NT コネクタのインストール

注	Windows NT コネクタは、設定したドメインの主ドメインコントローラ (PDC) にインストールする必要があります。

158 ページの「インストールプログラムの実行」で説明した手順が完了すると、「コネクタの設定」パネルが表示されます。

Windows NT コネクタと NT サブコンポーネントをインストールするには

1. Windows NT コネクタのボタンを有効化し、「次へ」をクリックします。
2. 「コネクタポートの設定」パネルが表示されるので、完全修飾ローカルホスト名と、コネクタが待機する使用可能ポート番号を入力します。すでに使用されているポートを指定すると、エラーメッセージが出力されます。

   Directory Server プラグインは、コンソールで保存した設定情報へのアクセスを必要とします。この情報を取得するために、プラグインはこのポートのサーバーソケットを通じて Windows NT コネクタと通信します。また、ログメッセージをセントラルログに記録するために、プラグインはこのチャネルを経由してメッセージを記録します。
3. 完了したら「次へ」をクリックします。

   「インストール準備完了」パネルが表示されます。このパネルには、コネクタのインストール先と、必要なディスク容量が表示されます。
4. 問題がなければ、「すぐにインストール」ボタンをクリックします。

   コネクタのインストールは、次の 2 段階で行われます。

   - プログラムがバイナリのインストールを開始し、進捗状況バーを持つインストールパネルが表示される
   - 次に、「コンポーネントの設定」パネルが表示される。この処理の完了には数分間かかるため、進捗状況バーが表示される

注	インストールを開始する前にコンソールを閉じなかった場合、警告が表示されます (図 5-5 を参照)。コンソールで「更新」をクリックし、コネクタの設定を読み込み直してください。

   両方の段階が完了すると、「インストール概要」パネルが表示されます。
5. インストールログを表示するときは、「詳細」をクリックします。

   インストールログは、`%TEMP%` ディレクトリに書き込まれます。ほとんどの Windows NT システムでは、このディレクトリは C:¥TEMP です。

6. 「閉じる」をクリックしてインストールプログラムを終了します。

Windows NT コネクタのインストールの後は、リソースの設定時に指定した (第 4 章を参照) その他のコネクタ、Directory Server プラグイン、または両方をインストールできます。

- その他の Windows NT コネクタのインストール : インストールプログラムを再起動し (158 ページの「インストールプログラムの実行」を参照)、手順 1 から手順 6 を繰り返す
- Directory Server コネクタのインストール : 161 ページの「Directory Server コネクタのインストール」に進む
- Active Directory コネクタのインストール : 166 ページの「Active Directory コネクタのインストール」に進む
- Directory Server プラグインのインストール : 171 ページの「Directory Server プラグインのインストール」に進む

Directory Server プラグインのインストール

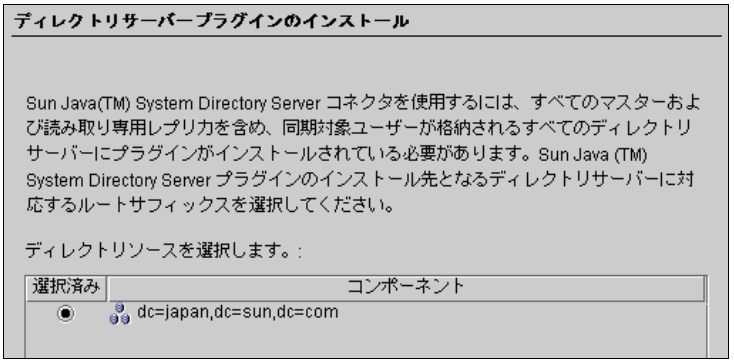
ここでは、Identity Synchronization for Windows の Directory Server プラグインをインストールする方法について説明します。

注 Directory Server プラグインは、Directory Server と同じマシンにインストールする必要があります。

コアまたはいずれかのコネクタと同じマシンにプラグインをインストールする場合、インストールプログラムはコアまたはコネクタがシステムにすでにインストールされているかどうかを検出します。すべての追加コンポーネントは、インストールディレクトリにインストールされます。

1. 158 ページの「インストールプログラムの実行」で説明した手順を完了します。

図 5-11　Directory Server プラグインの選択



2. 「コネクタの設定」パネルが表示されるので、Directory Server プラグイン (この例では dc=example,dc=com) のボタンを有効にし、「次へ」をクリックします。
3. 次のように、もう 1 つの「Directory Server プラグインのインストール」パネル (図 5-12) が表示されます。

図 5-12　Directory Server URL とクレデンシャルの指定

4. ドロップダウンリストから適切なホストタイプを選択します。
   - **優先** : 優先サーバーにプラグインをインストールする場合は、このオプションを選択する
   - **二次** : 二次サーバーにプラグインをインストールする場合は、このオプションを選択する

- **その他** : 優先または二次サーバー以外のマシンにプラグインをインストールする場合は、このオプションを選択する

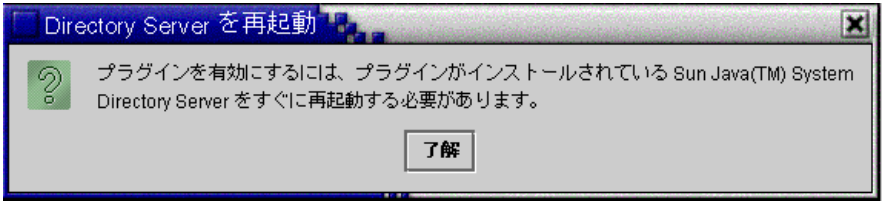
5. 優先または二次サーバー以外を指定した場合は、Directory Server の URL を入力します。
6. Directory Server の管理者名とパスワードを入力し、「次へ」をクリックします。

   「インストール準備完了」パネルが表示されます。このパネルには、プラグインのインストール先と、インストールに必要なディスク容量が表示されます。
7. 問題がなければ、「すぐにインストール」ボタンをクリックします。

   プラグインのインストールは、次の 2 段階で行われます。

   - プログラムがバイナリのインストールを開始し、進捗状況バーを持つインストールパネルが表示される
   - 次に、「コンポーネントの設定」パネルが表示される。この処理の完了には数分間かかるため、進捗状況バーが表示される
8. 両方の段階が完了すると、次のプロンプトが表示されます。表示内容を確認したら、「了解」をクリックしてダイアログボックスを閉じます。

図 5-13 Directory Server の再起動を促すプロンプト



9. インストールログを表示するときは、「詳細」をクリックします。
   - **Solaris 環境** : インストールログは `/var/sadm/install/logs/` に書き込まれる
   - **Windows 環境** : インストールログは `%TEMP%` ディレクトリに書き込まれる。これは次の場所の下にある `Local Settings` フォルダのサブディレクトリである `C:¥Documents and Settings¥Administrator`

注 Windows 2000 Advanced Server などの一部の Windows システムでは、`Local Settings` フォルダは隠しフォルダです。

このフォルダと `Temp` サブディレクトリを表示するには、Windows エクスプローラを開き、メニューバーから「ツール」>「フォルダ」を選択します。「フォルダオプション」ダイアログボックスが表示されるので、「表示」タブの「すべてのファイルとフォルダを表示する」を有効にします。

---

10. 「閉じる」をクリックしてインストールプログラムを終了します。

    Directory Server プラグインのインストールの後は、リソースの設定時に指定した (第 4 章を参照) その他のコネクタ、Directory Server プラグイン、または両方をインストールできます。

    - その他の Directory Server プラグインのインストール : インストールプログラムを再起動し (158 ページの「インストールプログラムの実行」を参照)、手順 2 から手順 9 を繰り返す

      Identity Synchronization for Windows では、配備に含まれるすべての Directory Server にプラグインをインストールする必要があるため、プラグインのインストールプログラムを何度でも続けて実行することができる

    - Directory Server コネクタのインストール : 161 ページの「Directory Server コネクタのインストール」に進む

    - Active Directory コネクタのインストール : 166 ページの「Active Directory コネクタのインストール」に進む

    - Windows NT コネクタのインストール : 170 ページの「Windows NT コネクタのインストール」に進む

11. Directory Server を再起動します。

第 6 章

既存ユーザーの同期

Identity Synchronization for Windows のコマンド行ユーティリティには、配備に既存のユーザーを取り込むための `idsync resync` サブコマンドが用意されています。このコマンドは、管理者が指定した一致規則を使用して既存エントリにリンクを設定し、空のディレクトリにリモートディレクトリの内容を取り込みます。また、既存の 2 つのユーザー集合間で、パスワードも含む属性値を一括同期させることもできます。

この章では、`idsync resync` サブコマンドを使用して、Identity Synchronization for Windows の新規インストール用に既存のユーザーにリンクを設定し、同期させる方法について説明します。また、同期とサービスを開始、終了する方法についても説明します。この章で説明する内容は、次のとおりです。

注 既存ユーザーをリンクおよび同期させるには、コアとコネクタのインストールが事前に完了している必要があります。

`idsync resync` サブコマンドについては、付録 A 「Identity Synchronization for Windows のコマンド行ユーティリティの使用」を参照してください。

表 6-1 は、インストール後の操作手順を既存ユーザーのタイプ別に示しています。

表 6-1　インストール後の手順 (既存ユーザーのタイプ別)

ユーザーが存在するディレクトリ		インストール後の手順	
Windows	Directory Server	既存ユーザーを同期させる	既存ユーザーを同期させない
存在しない	存在しない	なし	なし
存在しない	存在する	`idsync resync -o Sun -c` を実行し、既存の Directory Server ユーザーを Windows に作成する	なし
存在する	存在しない	`idsync resync -c` を実行し、既存の Windows ユーザーを Directory Server に作成する	`idsync resync -u` を実行し、コネクタのユーザーエントリローカルキャッシュを移植する
存在する	存在する	次のいずれかの方法を選択する • `idsync resync -f` <*filename*> を実行し、Active Directory から Directory Server にユーザーをリンクさせ、同期させる • `idsync resync -f` <*filename*> `-k` を実行し、ユーザーとのリンク設定だけを行う • `idsync resync -f` <*filename*> `-k` を実行して、ユーザーとのリンク設定を行い、`idsync resync -o Sun` を実行して、Directory Server からの既存ユーザーとの再同期を行う	`idsync resync -u` を実行し、コネクタのユーザーエントリローカルキャッシュを移植する

idsync resync の使用

次に、リンク設定と同期の手順について、idsync resync サブコマンドの正しい構文と、手順が正しく完了したことを検証する方法について説明します。ここで説明する内容は、次とおりです。

ユーザーの再同期

注 配備で同期を開始する前に、サーバー間ですべての既存ユーザーが同期されていることを確認してください。

`idsync resync` コマンドを使用して、既存エントリのリンク、ユーザーの作成、2 つのディレクトリソース間のユーザー属性の同期を行うことができます。具体的には、`idsync resync` コマンドを使用して次の操作を行えます。

- 空の Directory Server に Active Directory または Windows NT SAM ドメインの既存ユーザーを取り込む
- 既存の 2 つのディレクトリソースの間ですべてのユーザーをリンクさせ、次にパスワード以外のすべてのユーザーエントリ属性値を同期させる

注 Directory Server と Windows にユーザーが存在する場合に、これらのユーザーのリンクと同期を行うときは、`idsync resync -f` *<filename>* コマンドを実行する必要があります。

既存のユーザーを Directory Server と同期させないようにするには、引数 `-u` を指定して `idsync resync` を実行します。これにより、オブジェクトキャッシュの更新だけが行われ、Windows エントリから Directory Server への同期は行われません。

既存の Windows ユーザーが存在し、`idsync resync` を実行しなかった場合、これらのユーザーに対する変更は取り込まれたり、取り込まれなかったりします。また、フローの設定によっては、これらのユーザーは Directory Server 側に自動的に作成されます。すでに実行した場合でも、`idsync resync` を再実行する必要があります。

- 2 つのディレクトリソースの間で同期がずれた場合に、ユーザーエントリを同期させる
- Active Directory および Windows NT SAM コネクタのオブジェクトキャッシュデータベースを事前準備できる。このデータベースでは、Active Directory または Windows NT SAM ユーザーエントリのシャドウコピーが維持される

`idsync resync` コマンドを使用してパスワードを同期させることはできません。ただし、Directory Server パスワードを無効化し、Active Directory 環境でオンデマンドパスワード同期を強制する場合は例外です。

ユーザーのリンク

Active Directory と Directory Server にユーザーを取り込み、Active Directory と Directory Server のコネクタのインストールが完了したら (同期を開始する前)、`idsync resync` コマンドを使用して、2 つのディレクトリソース内のすべての既存ユーザーがリンクされていることを確認する必要があります。

リンク設定とは、次の一意で不変の識別子を格納することで、Identity Synchronization for Windows が Directory Server 側と Windows 側の同一ユーザーを関連付けることです。

- 各 Directory Server ユーザーエントリの `dspswuserlink` 属性
- 各 Active Directory ユーザーの `objectguid` 属性
- 各 Windows NT SAM ユーザーのドメイン名と `RID` の組み合わせ

この不変の識別子を格納することで、Identity Synchronization for Windows は `uid` や `cn` のような、その他の主要識別子も同期させることができます。`dspswuserlink` 属性は、次の場合に取り込まれます。

- Identity Synchronization for Windows が Directory Server に新規ユーザーを作成する (Windows からの新規ユーザーを同期させる、または `idsync resync -c` を実行する)
- Identity Synchronization for Windows が Windows に新規ユーザーを作成する (Directory Server からの新規ユーザーを同期させる、または `idsync resync -c -o Sun` を実行する)
- この章ですでに説明したように、`idsync resync -c -f` を実行して Directory Server と Windows の既存のエントリをリンクさせる

既存のユーザーをリンクさせるには、2 つのディレクトリの間でユーザーを一致させるための規則を指定する必要があります。たとえば、2 つのディレクトリのユーザーエントリをリンクさせるには、両方のディレクトリで姓と名が一致する必要がある、などの規則を指定します。

ユーザーエントリのリンクとデータ衝突の解決は、純粋に技術的な観点から説明できます。対応する 2 つのディレクトリソース間で idsync resync サブコマンドがユーザーのリンクに失敗する原因は数多くありますが、その多くはリンク対象ディレクトリ内のデータの不整合によるものです。

idsync resync を使用する際の戦略の 1 つとして、引数 -n の使用があげられます。この引数を指定した場合、コマンドの処理は「安全モード」で行われ、実際に変更を加えることなく実行結果を確認できます。安全モードで実行することで、最適なユーザー一致条件の組み合わせが見つかるまで、リンク条件を詳細に調整できます。

試行を繰り返すうちに、リンクの精度とリンク対象範囲のバランスが浮かび上がってきます。

たとえば、両方のディレクトリソースに従業員 ID 番号または社会保障番号の属性が含まれている場合は、まず、この番号だけを対象としたリンク条件を指定します。リンクの精度を向上させるには、条件に姓の属性も追加したほうがよいかもしれません。しかし、データに記録されている姓に不整合があれば、最初に番号だけで一致させた場合に特定できたエントリのリンクを失う可能性もあります。リンクに失敗するエントリについては、データクレンジングを行う必要があります。

idsync resync の引数

idsync resync コマンドは、次の引数を受け付けます。

表 6-2 idsync resync の使用方法

引数	意味
-f <*filename*>	Identity Synchronization for Windows に用意されているいずれかの XML 設定ファイルを使用して、リンクが設定されていないユーザーエントリの間にリンクを作成する (付録 B「LinkUsers XML ドキュメントのサンプル」を参照)
-k	ユーザーの作成、既存ユーザーの変更は行わずに、リンクが設定されていないユーザーの間だけにリンクを作成する。この引数は、引数 -f と組み合わせて使用する必要がある
-a <*ldap-filter*>	同期の対象となるエントリを制限する LDAP フィルタを指定する このフィルタは、同期処理のソース側に適用される たとえば、idsync resync -o Sun -a "usid=*" と指定した場合、uid 属性を持つすべての Directory Server ユーザーが Active Directory 側で同期される
-l <*sul-to-sync*>	再同期対象の同期ユーザーリスト (SUL) を個別に指定する **注意** : 複数の SUL ID を指定して複数の SUL を再同期させることも、SUL ID を指定せずにすべての SUL を再同期させることもできる

表 6-2　idsync resync の使用方法 (続き)

引数	意味
`-o (Sun | Windows)`	再同期処理のソースを指定する • Sun: Windows エントリの属性値を、Sun Java System Directory Server ディレクトリソースエントリ内の対応する属性値に設定する • Windows: Sun Java System Directory Server エントリの属性値を、Windows ディレクトリソースエントリ内の対応する属性値に設定する デフォルトは *Windows*
`-c`	ターゲット側に対応するユーザーが見つからなかった場合に自動的にユーザーエントリを作成する • Active Directory または Windows NT で作成されるユーザーには、暗号を使用してセキュリティ保護されたパスワードがランダムに生成される • Directory Server で作成されるユーザーには、特別なパスワード値 (`(PSWSYNC)` **`*INVALID PASSWORD*`**) が作成される (`-i` オプションを指定した場合を除く) **注意** : その方向の作成を設定していない場合でも、Identity Synchronization for Windows はユーザーの作成を試みる。たとえば、Windows から Sun (またはその反対) への同期を Identity Synchronization for Windows に設定しなかった場合でも、-c 引数を指定すると、Identity Synchronization for Windows は見つからなかったユーザーの作成を試みる
`-i (ALL_USERS | NEW_USERS | NEW_LINKED_USERS)`	Sun ディレクトリソースで同期されるユーザーエントリのパスワードをリセットし、次にユーザーパスワードの入力が求められるときに、これらのユーザーに現在のドメイン内でパスワードの同期を強制する • **`ALL_USERS`**: すべての同期対象ユーザーにオンデマンドパスワード同期を強制する • **`NEW_USERS`**: 新規作成ユーザーだけにオンデマンドパスワード同期を強制する • **`NEW_LINKED_USERS`**: すべての新規作成ユーザーとすべてのリンク設定済みユーザーにオンデマンドパスワード同期を強制する これらのオプションがパスワードの検証に与える影響については、表 6-3 を参照
`-u`	オブジェクトキャッシュを更新する この引数は、Windows ディレクトリソースのユーザーエントリのローカルキャッシュだけを更新する。これにより、Windows の既存ユーザーは Directory Server 側に作成されない。この引数を指定した場合、Windows ユーザーエントリは Directory Server ユーザーエントリと同期されない。この引数は、再同期のソースが Windows の場合にだけ有効である
`-x`	ソースエントリと一致しないターゲット側ユーザーエントリをすべて削除する

表 6-2　idsync resync の使用方法 (続き)

引数	意味
-n	実際の変更なしでコマンドの実行結果を確認できるように、安全モードで実行する

表 6-3　idsync resync による Directory Server 側ユーザーパスワードの無効化

	ユーザーは Active Directory と Directory Server にエントリを持ち、両者はリンクされている	ユーザーは Active Directory と Directory Server にエントリを持つが、両者はリンクされていない	ユーザーは Active Directory にエントリを持つが、Directory Server には持たない
-i ALL_USERS	無効にする	無効にする	無効にする
-i NEW_LINKED_USERS	無効にしない	無効にする	無効にする
-i NEW_USERS	無効にしない	無効にしない	無効にする
-i の指定なし	無効にしない	無効にしない	無効にしない

表 6-4 は、異なる引数を組み合わせた結果の例を示しています。表記を簡略化するため、-h、-p、-D、-w、-s の各引数にについてはデフォルトの動作を適用し、指定を省略しています。

表 6-4　idsync resync の使用例

引数	結果
idsync resync	resync の使用方法を表示する
idsync resync -i ALL_USERS	すべてのユーザーのパスワードを無効化し、オンデマンドパスワード同期を強制する (Active Directory 環境だけで有効) Active Directory と NT ドメインの両方が存在する複合環境では、Active Directory の SUL を明示的に指定する必要がある
idsync resync -c -i NEW_USERS	Directory Server 側にユーザーエントリが見つからない場合にユーザーを作成し、パスワードを無効化してオンデマンドパスワード同期を強制する。空の Directory Server インスタンスに既存の Windows ユーザーを取り込む場合に、このコマンドを使用する
idsync resync -c -l SUL_sales -l SUL_finance	SUL_sales および SUL_finance という SUL だけを対象に、Active Directory のすべての既存ユーザーを Directory Server 側に作成する。ただし、オンデマンドパスワード同期は強制されない

表 6-4　idsync resync の使用例 (続き)

引数	結果
`idsync resync`	`resync` の使用方法を表示する
`idsync resync -n`	実際の変更なしで `resync` コマンドの実行結果を確認できるように、安全モードで実行する
`idsync resync -o Sun -a "(sn=Smith)"`	Smith という姓 (sn) を持つすべての Directory Server ユーザーを Windows 側で同期させる
`idsync resync -u`	既存のユーザーが Directory Server に作成されないように、Windows コネクタのオブジェクトキャッシュだけを更新する。実際にはどのユーザーも同期されない
`idsync resync -f link.cfg -k -i NEW_LINKED_USERS`	`link.cfg` ファイルに指定されているリンク条件に基づいて、リンクが設定されていないユーザーをリンクさせる。Identity Synchronization for Windows はユーザーの作成または変更を行わないが、新たにリンクされたユーザーの Directory Server パスワードには、Active Directory ユーザーのパスワードが設定される

警告　`idsync resync` を使用してユーザーをリンクさせるときは、インデックスが付けられた属性を使用する必要があることに注意してください。インデックスが付けられていない属性は、パフォーマンスに影響する可能性があります。

ユーザー一致条件に複数の属性が指定されている場合、少なくとも 1 つにインデックスが付けられていれば、許容可能なパフォーマンスが得られる可能性が高くなります。しかし、インデックスが付けられた属性がユーザー一致条件 (`UserMatchingCriteria`) に 1 つも存在しない場合、大規模なディレクトリでのパフォーマンスは許容できないほど低下します。

セントラルログによる結果の確認

idsync resync のすべての動作の結果は resync.log という特別なセントラルログに記録されます。このログには、正しくリンクおよび同期されたユーザー、リンクできなかったユーザー、すでにリンクされているユーザーがすべて記録されます。

注	Administrator や Guest など、すでに存在する Active Directory の特別なユーザーは、このログではリンク失敗と表示されることがあります。

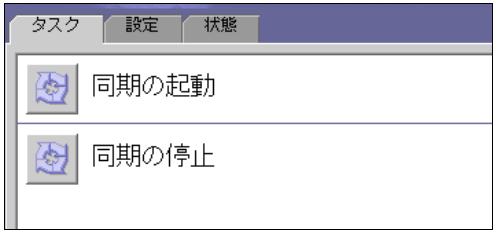
同期の開始と終了

同期を開始または終了しても、個々の Java プロセス、デーモン、サービスは開始または停止されません。同期の開始後、同期を終了しても処理が一時停止されるだけです。同期を再開すると、プログラムは直前の終了時から同期を再開するため、変更が失われることはありません。

同期を開始または終了するには、次の手順を実行します。

1. Sun Java System サーバーコンソールのナビゲーションパネルで Identity Synchronization for Windows インスタンスを選択します。
2. Identity Synchronization for Windows のパネルが表示されるので、右上端の「開く」ボタンをクリックします。
3. 入力が求められたら、設定パスワードを入力します。
4. 「タスク」タブ (図 6-1) を選択します。

図 6-1　同期の開始と終了



- 同期を開始するには、「同期を開始します」をクリックする
- 同期を終了するには、「同期を停止します」をクリックする

注 コマンド行ユーティリティ idsync startsync、idsync stopsync を使用して同期を開始、終了することもできます。詳細な方法については、325 ページの「startsync の使用」および 326 ページの「stopsync の使用」を参照してください。

サービスの開始と停止

Identity Synchronization for Windows と Message Queue は、Solaris 環境ではデーモンとして、Windows 環境ではサービスとしてインストールされます。これらのプロセスは、システムの起動時に自動的に開始されますが、次に示すように、これを手動で開始および停止することもできます。

- Solaris 環境 : コマンド行で次のように操作する
  - Identity Synchronization for Windows のすべてのプロセスを開始するには、/etc/init.d/isw start と入力する
  - Identity Synchronization for Windows のすべてのプロセスを停止するには、/etc/init.d/isw stop と入力する
  - Message Queue ブローカを開始するには、/etc/init.d/imq start と入力する
  - Message Queue ブローカを停止するには、/etc/init.d/imq stop と入力する
- Windows 環境 :
  - Windows の「スタート」メニューから次のように操作する
    I. 「スタート」>「設定」>「コントロールパネル」>「管理サービス」を選択する
    II. 「管理サービス」ダイアログボックスが表示されるので、「サービス」アイコンをダブルクリックして「サービス」ダイアログボックスを開く。
    III. 「Identity Synchronization for Windows」を選択し、メニューバーから「操作」>「開始」(または「停止」) を選択する。「iMQ Broker」についても同じ操作を繰り返す
  - コマンド行に net コマンドを入力し、サービスを制御する

注 停止した Identity Synchronization for Windows デーモンまたはサービスを再開するときは、30 秒以上が経過してから行ってください。コネクタは、すべての接続を終了してシャットダウンするまでに数秒を要することがあります。

第 7 章

Identity Synchronization for Windows 1 2004Q3 への移行

この章では、システムを Sun Java System Identity Synchronization for Windows バージョン 1.0 からバージョン 1 2004Q3 に移行する方法について説明します。

注 Identity Synchronization for Windows バージョン 1.0 では、Message Queue が自動的にインストールされましたが、Identity Synchronization for Windows 1 2004Q3 ではインストールされません。

Sun Java System Message Queue のインストール方法については、同製品のドキュメントを参照してください。

この章で説明する内容は次のとおりです。

概要

Identity Synchronization for Windows バージョン 1.0 または 1.0 SP1 から 1 2004Q3 への移行は、次の各段階に大別されます。

1. Identity Synchronization for Windows バージョン 1.0 または 1.0 SP1 のインストールで移行を準備します。
2. Identity Synchronization for Windows バージョン 1.0 または 1.0 SP1 をアンインストールします。
3. 依存関係のある製品をインストールまたはアップグレードします。
4. バックアップしておいた設定とコネクタの状態を使用して、Identity Synchronization for Windows 1 2004Q3 をインストールします。

注 Identity Synchronization for Windows 1 2004Q3 は、Identity Synchronization for Windows バージョン 1.0 または 1.0 SP1 と同じプラットフォームおよびアーキテクチャにインストールしてください。

移行の前に

移行プロセスを開始する前に、次の作業を行います。

- Sun Java System Identity Synchronization for Windows バージョン 1 2004Q3 の新しい機能について理解する
- 移行プロセスの計画時に利用できるインストールと設定の情報について、第 2 章「インストールの準備」を参照する
- バージョン 1.0 の配備と設定について書き出す
  行ったカスタマイズについて、その設定情報を必ず書き留める
- 移行の予定を立てる
  移行プロセスは最短でも 4 時間かかるため、通常の業務時間が終了してから移行を行うことが必要になることもある

  バージョン 1.0 から 1 2004Q3 へのシステム移行中にユーザーがパスワードや属性の変更を行った場合、Identity Synchronization for Windows はこれらの変更を次のように処理します。

  - **Active Directory での処理** : 移行プロセス中に Active Directory で変更されたパスワードは、移行プロセスの完了後に Directory Server プラグインによってオンデマンドで同期される

- **Directory Server での処理** : 移行中に Directory Server 上で行われたパスワードの変更は同期されない。ただし、移行プロセスの完了後に、Identity Synchronization for Windows 1 2004Q3 のログを調べることで、影響を受けるユーザーを特定できる。230 ページの「ログのチェック」を参照
- **Windows NT での処理** : 移行プロセス中に NT 上で行われたパスワードの変更は同期されない

  ただし、`forcepwchg` ユーティリティを使用した場合は、影響を受けるユーザーを特定し、パスワードの再変更を強制できる。詳細は、196 ページの「Windows NT でのパスワード変更の強制」および 230 ページの「ログのチェック」を参照
- ディレクトリソースを問わず、移行中に行われるその他すべての属性の変更は、移行プロセスの完了後に同期される

移行の準備

バージョン 1.0 からバージョン 1 2004Q3 への移行には、次のユーティリティを単独で、または組み合わせて使用します。

- **`export10cnf`**: Identity Synchronization for Windows 1.0 の設定からエクスポートした設定ファイルを作成するためのスタンドアロンユーティリティ。詳細については 188 ページの「バージョン 1.0 の設定のエクスポート」を参照

  エクスポートされる XML ドキュメントには、ディレクトリ配備のトポロジと、Identity Synchronization for Windows バージョン 1 2004Q3 のインストールの設定に必要な情報が含まれる
- **`checktopics`**: 1.0 インストールの Message Queue 同期トピックを調べ、未配信メッセージがキューに残されていないかどうかを確認するユーティリティ

  1.0 の同期を終了したあとに、Message Queue に更新が残される可能性がある。移行処理を進める前に、Message Queue に更新が残されていないことを確認する必要がある。詳細については 194 ページの「未配信メッセージのチェック」を参照
- **`forcepwchg`**: 移行プロセスでパスワードが変更されたユーザーを識別し、バージョン 1 2004Q3 システムの準備が整った段階でパスワードの再変更を強制する Windows NT ツール。Windows NT 上で変更されたパスワードは、移行プロセス中は検出されない。詳細については 196 ページの「Windows NT でのパスワード変更の強制」を参照

注 これらのユーティリティは、Identity Synchronization for Windows バージョン 1.0 から 1 2004Q3 への移行に使用されます。移行は、Identity Synchronization for Windows が配備されていた環境と同じ環境で行われます。このため、これらのユーティリティは Solaris/SPARC パッケージと Windows パッケージだけに用意されています。

移行ユーティリティは、インストールの `migration` ディレクトリに格納されています。追加のインストール手順は必要ありません。

バージョン 1.0 の設定のエクスポート

`export10cnf` ユーティリティを使用してバージョン 1.0 の既存の設定を XML ファイルとしてエクスポートし、コネクタのインストール前に `idsync importcnf` コマンドを使用して、そのファイルを迅速かつ正確にバージョン 1 2004Q3 システムにインポートすることができます。

ヒント Identity Synchronization for Windows コンソールを使用して 1.0 の設定を手動で再入力することもできますが、`export10cnf` ユーティリティを使用することを強くお勧めします。`export10cnf` を使用しない場合、コネクタの状態を保存することはできません。

バージョン 1.0 の設定をエクスポートすることには、次のような利点があります。

- 管理コンソールで行う初期設定プロセスのほとんどを省略できる
- バージョン 1 2004Q3 で割り当てられるコネクタ ID が、バージョン 1.0 で使用していたコネクタ ID と確実に一致する。これにより、既存のコネクタの状態を簡単に保存でき、バージョン 1 2004Q3 の配備で直接使用できる

  基本的には、`persist` ディレクトリと `etc` ディレクトリのバックアップを行い、基本となるディレクトリ構造に関係なく、それらのディレクトリを後から復元する

`export10cnf` ユーティリティは、インストールの `migration` ディレクトリに格納されています。追加のインストール手順は必要ありません。

export10cnf ユーティリティの使用

Identity Synchronization for Windows の設定を XML ファイルとしてエクスポートするには、次のように `migration` ディレクトリから `export10cnf` を実行します。

- 端末ウィンドウを開き、次のように入力します。

```
java -jar export10cnf.jar -h <hostname> -p <port> -D <bind DN>
-w <bind password> -s <rootsuffix> -q <configuration password> -Z
-P <cert-db-path> -m <secmod-db-path> -f <filename>
```

たとえば、次のようなメッセージが表示されます。

```
java -jar export10cnf.jar -D "cn=dirmanager" -w - -q - -s
"dc=example,dc=com" -f exported-configuration
```

export10cnf ユーティリティの引数は、Identity Synchronization for Windows のコマンド行ユーティリティの共通引数 (308 ページの「共通引数」を参照) と同じです。export10cnf に固有のオプションは、-f *<filename>* だけです。ユーティリティの実行が正常に完了すると、現在の設定がこの「-f」オプションの引数として指定されたファイルにエクスポートされます。

クリアテキストパスワードの挿入

export10cnf ユーティリティは、セキュリティ上の理由により、バージョン 1.0 の設定からクリアテキストのパスワードをエクスポートしません。cleartextPassword フィールドには、代わりに空の文字列が挿入されます。次に例を示します。

```
<Credentials
        userName="cn=iswservice,cn=users,dc=example,dc=com"
        cleartextPassword=""/>
        <!-- INSERT PASSWORD BETWEEN THE DOUBLE QUOTES IN THE ABOVE
FIELD -->
```

ファイルを Identity Synchronization for Windows 1 2004Q3 にインポートする前に、エクスポートされた設定ファイルのすべての cleartextPassword フィールドで、二重引用符の間に手動でパスワードを入力する必要があります。importcnf は、パスワードの値が空の設定ファイルがインポートされないように検証を行います。

次に例を示します。

```
<Credentials
        userName="cn=iswservice,cn=users,dc=example,dc=com"
        cleartextPassword="mySecretPassword"/>
        <!-- INSERT PASSWORD BETWEEN THE DOUBLE QUOTES IN THE
ABOVEFIELD -->
```

エクスポートされた設定ファイルの例

190 ページのコード例 7-1 は、エクスポートされた設定ファイルの例を示しています。

このファイルでは、

- `ad-host.example.com` は Active Directory ドメインコントローラを示す
- `ds-host.example.com` は Sun Java System Directory Server を実行するホストを示す

コード例 7-1 エクスポートされた設定ファイルの例

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

<ActiveConfiguration>
  <SunDirectorySource
    parent.attr="DirectorySource"
    onDemandSSLOption="true"
    maxConnections="5"
    displayName="dc=example,dc=com"
    resyncInterval="1000">
    <SynchronizationHost
      hostOrderOfSignificance="1"
      hostname="ds-host.example.com"
      port="389"
      portSSLOption="true"
      securePort="636">
      <Credentials
        userName="uid=PSWConnector,dc=example,dc=com"/>
    </SynchronizationHost>
<SyncScopeDefinitionSet
      index="0"
      location="ou=people,dc=example,dc=com"
      filter=""
      creationExpression="cn=%cn%,ou=people,dc=example,dc=com"
      sulid="SUL"/>
  </SunDirectorySource>
<ActiveDirectorySource
parent.attr="DirectorySource"
    displayName="example.com"
    resyncInterval="1000">
```

```
<SyncScopeDefinitionSet
      index="0"
      location="cn=users,dc=example,dc=com"
      filter=""
      creationExpression="cn=%cn%,cn=users,dc=example,dc=com"
      sulid="SUL"/>
</ActiveDirectorySource>
<ActiveDirectoryGlobals
    flowInboundCreates="true"
    flowInboundModifies="true"
    flowOutboundCreates="true"
flowOutboundModifies="true">
    <AttributeDescription
      parent.attr="CreationAttribute"
name="samaccountname"
syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
<AttributeMap>
      <AttributeDescription
        parent.attr="WindowsAttribute"
        name="samaccountname"
        syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
      <AttributeDescription
        parent.attr="SunAttribute"
        name="uid"
        syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
    </AttributeMap>
<AttributeDescription
      parent.attr="SignificantAttribute"
      name="description"
      syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
<AttributeMap>
      <AttributeDescription
        parent.attr="SunAttribute"
        name="sn"
        syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
<AttributeDescription
        parent.attr="WindowsAttribute"
        name="sn"
        syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
    </AttributeMap>
```

```
<SynchronizationHost
      hostOrderOfSignificance="1"
      hostname="ad-host.example.com"
      port="389"
      portSSLOption="true"
      securePort="636">
      <Credentials
        userName="cn=iswservice,cn=users,dc=example,dc=com"
        cleartextPassword=""/>
        <!-- INSERT PASSWORD BETWEEN THE DOUBLE QUOTES IN THE ABOVE FIELD -->
    </SynchronizationHost>
<AttributeDescription
      parent.attr="CreationAttribute"
      name="cn"
      syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
    <TopologyHost
      parent.attr="SchemaLocation"
hostname="ad-host.example.com"
      port="3268"
      portSSLOption="true"
      securePort="3269">
      <Credentials
        parent.attr="Credentials"
        userName="cn=iswservice,cn=users,dc=example,dc=com"
        cleartextPassword=""/>
        <!-- INSERT PASSWORD BETWEEN THE DOUBLE QUOTES IN THE ABOVE FIELD -->
    </TopologyHost>
    <TopologyHost
      parent.attr="HostsTopologyConfiguration"
      hostname="ad-host.example.com"
      port="3268"
      portSSLOption="true"
      securePort="3269">
<Credentials
        parent.attr="Credentials"
        userName="cn=iswservice,cn=users,dc=example,dc=com"
        cleartextPassword=""/>
        <!-- INSERT PASSWORD BETWEEN THE DOUBLE QUOTES IN THE ABOVE FIELD -->
    </TopologyHost>
<AttributeMap>
      <AttributeDescription
        parent.attr="SunAttribute"
        name="cn"
        syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
```

```
 <AttributeDescription
        parent.attr="WindowsAttribute"
        name="cn"
        syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
    </AttributeMap>
<AttributeMap>
      <AttributeDescription
        parent.attr="SunAttribute"
        name="description"
        syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
<AttributeDescription
        parent.attr="WindowsAttribute"
name="description"
        syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
    </AttributeMap>
</ActiveDirectoryGlobals>
<SunDirectoryGlobals
    userObjectClass="inetorgperson"
    flowInboundCreates="true"
    flowInboundModifies="true"
    flowOutboundCreates="true"
    flowOutboundModifies="true">
<TopologyHost
      parent.attr="SchemaLocation"
      hostname="ds-host.example.com"
      port="389"
      portSSLOption="false"
      securePort="636">
      <Credentials
        parent.attr="Credentials"
        userName="cn=directory manager"
        cleartextPassword=""/>
        <!-- INSERT PASSWORD BETWEEN THE DOUBLE QUOTES IN THE ABOVE FIELD -->
    </TopologyHost>
   <TopologyHost
      parent.attr="HostsTopologyConfiguration"
      hostname="ds-host.example.com"
      port="389"
      portSSLOption="false"
      securePort="636"><Credentials
        parent.attr="Credentials"
        userName="cn=directory manager"
        cleartextPassword=""/>
        <!-- INSERT PASSWORD BETWEEN THE DOUBLE QUOTES IN THE ABOVE FIELD -->
    </TopologyHost>
```

```
<AttributeDescription
      parent.attr="SignificantAttribute"
      name="description"
      syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
<AttributeDescription
      parent.attr="CreationAttribute"
      name="sn"
      syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
    <AttributeDescription
      parent.attr="CreationAttribute"
      name="cn"
      syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
  </SunDirectoryGlobals>
</ActiveConfiguration>
```

export10cnf による設定のエクスポートが完了すると、処理の結果が報告されます。処理が失敗した場合は、エラー ID を示すエラーメッセージが表示されるます。

未配信メッセージのチェック

Identity Synchronization for Windows 1.0 から 1 2004Q3 への移行プロセスでは、既存配備のコネクタの状態を保存することで、システムのダウン時間を最小化しています。しかし、これらの状態は Message Queue によって最後に受信、認識された変更までを反映しているため、メッセージが実際に配信され、送信先コネクタに適用されているかどうかはわかりません。

Message Queue の状態に変化がないかぎり、これによって問題が生じることはありませんが、移行プロセスで Message Queue 3.5 SP1 をインストールする際に Message Queue 上のメッセージは失われます。

移行処理を先に進める前に、既存の Message Queue の同期トピックに未配信のメッセージが残されていないことを確認する必要があります。Identity Synchronization for Windows の checktopics ユーティリティを使用することで、すべての同期トピックが確実に空であり、システムが休止していることを確認できます。

checktopics ユーティリティの使用

checktopics ユーティリティは、Solaris/SPARC および Windows の Identity Synchronization for Windows 1 2004Q3 パッケージの migration ディレクトリに格納されています。

注 checktopics を実行するための唯一の前提条件は、適切な Java 仮想マシン (バージョン 1.4.2_04 以降) です。

checktopics ユーティリティを実行すると、ユーティリティは、同期ユーザーリスト (SUL) に関する情報と、Message Queue で現在使用されている同期トピック名が保存されている設定ディレクトリに接続します。また、checktopics を実行すると、各アクティブ同期トピックに残されている未処理メッセージの数が Message Queue に照会され、この情報が表示されます。

checktopics コマンド行ユーティリティを実行する方法は、次のとおりです。

a. 端末ウィンドウを開き、migration ディレクトリに移動 (**cd**) します。

b. コマンドプロンプトに次のようにサブコマンドを入力します。

```
java -jar checktopics.jar -h <hostname> -p <port> -D <bind_DN>
-w <bind_password> -s <root_suffix> -q <configuration_password> -Z
```

次に例を示します。

```
java -jar checktopics.jar -D "cn=directory manager" -w - -s
"dc=example,dc=com" -q -
```

注

- checktopics ユーティリティの引数については、308 ページの「共通引数」を参照
- checktopics ユーティリティの使用については、194 ページの「未配信メッセージのチェック」を参照

checktopics を実行したら、端末でメッセージを確認します。

- 処理が正常に完了した場合、未配信メッセージがログに残されていないことを示すメッセージが端末に表示される
- 処理が失敗した場合は、エラー ID を示すエラーメッセージが表示される

メッセージのクリア

アクティブないずれかの同期トピックに未配信のメッセージが残されている場合は、次の手順を実行してメッセージをクリアできます。

1. 同期を再開します。

2. メッセージが送信先コネクタに適用されるのを待ちます。
3. 同期を終了します。
4. checktopics を再実行します。

Windows NT でのパスワード変更の強制

Windows NT ではパスワードの変更は監視されず、移行プロセス中に新しいパスワード値は取り込まれません。このため、移行完了後に新しいパスワード値を特定することができません。

1 2004Q3 への移行が完了したあとにすべてのユーザーにパスワードの変更を義務付ける代わりに、コマンド行ユーティリティ forcepwchg を使用して、移行プロセス中にパスワードを変更したユーザーを対象にパスワードの変更を強制することができます。

注 forcepwchg ユーティリティは、Windows パッケージだけで利用できます。

forcepwchg ユーティリティは、Windows の migration ディレクトリに格納されています。このディレクトリから forcepwchg を直接実行します。追加のインストール手順は必要ありません。

forcepwchg ユーティリティは、NT コンポーネント (コネクタ、変更ディテクタ DLL、パスワードフィルタ DLL) がインストールされている主ドメインコントローラ (PDC) ホスト上で実行する必要があります。forcepwchg をリモート実行することはできません。

また、forcepwchg ユーティリティは移行対象となるアカウント名を 1 行に 1 つずつ出力します。移行プロセス中にエラーが発生した場合は、最後に出力されたユーザーアカウントの移行でエラーが発生しています。

システムの移行

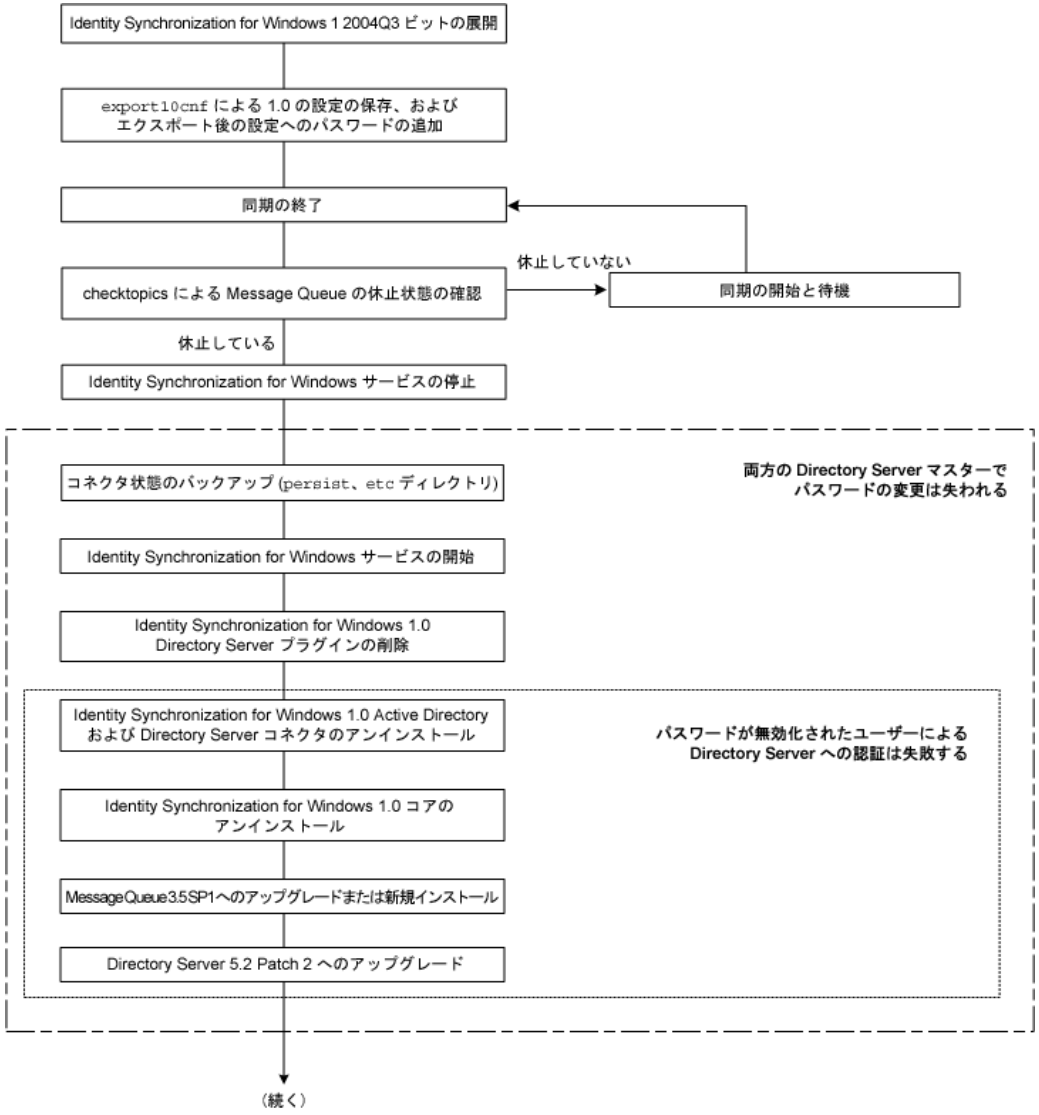
ここでは、単一ホストの配備をバージョン 1 2004Q3 に移行する手順について説明します。単一ホストの配備では、次に示す Identity Synchronization for Windows のすべてのコンポーネントが単一のホスト (Windows 2000 Server、Solaris バージョン 8 または 9、または SPARC) にインストールされます。

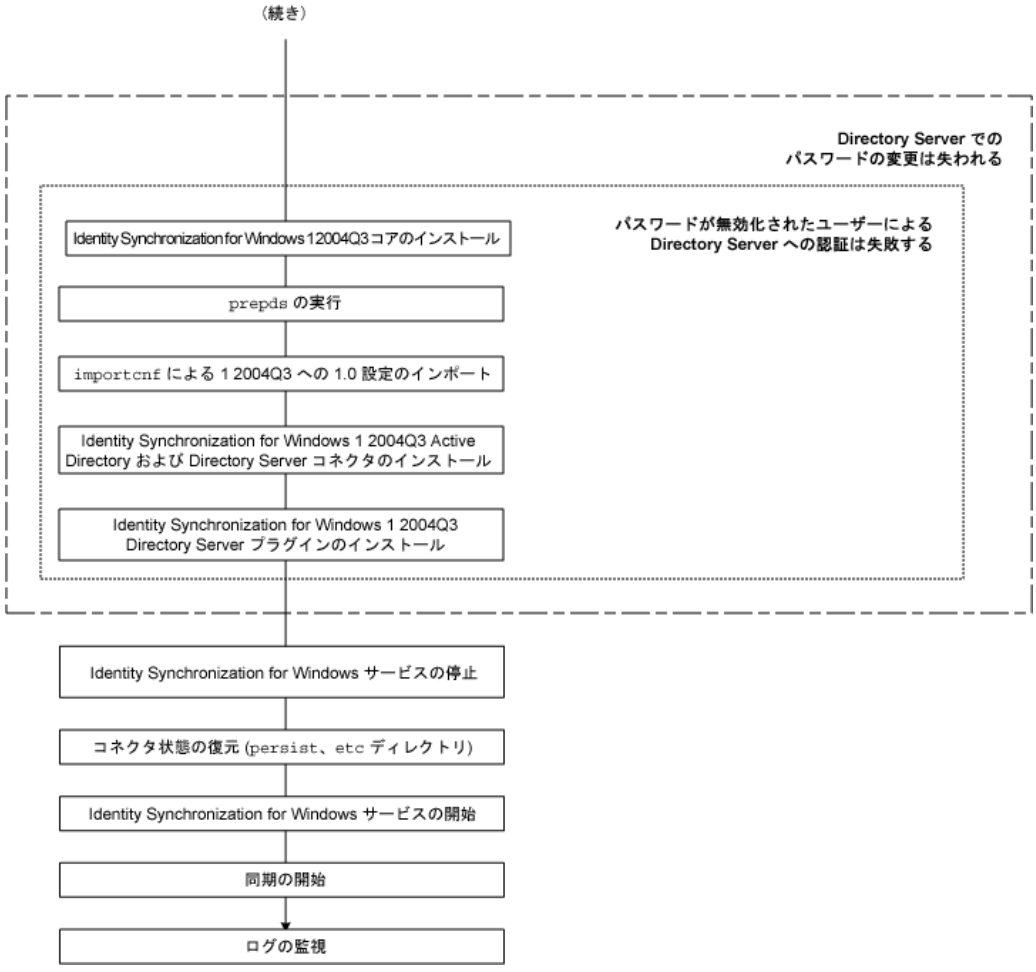
- Directory Server (1 インスタンス)
- コア (Message Queue、セントラルロガー、システムマネージャ、コンソール)
- Active Directory コネクタ
- Directory Server コネクタ
- Directory Server プラグイン

注 インストールホストに Solaris を使用している場合は、同期専用に Active Directory がインストールされた Windows 2000 マシンが必要となります。Windows 2000 マシンにはコンポーネントはインストールされません。

次の図は、移行プロセスを表しています。このあとに説明する同期手順を補足するチェックリストとしても使用できます。

図 7-1　単一ホスト配備の移行




（続き）
Directory Server での
パスワードの変更は失われる
パスワードが無効化されたユーザーによる
Directory Server への認証は失敗する
Identity Synchronization for Windows 1 2004Q3 コアのインストール
prepds の実行
importcnf による 1 2004Q3 への 1.0 設定のインポート
Identity Synchronization for Windows 1 2004Q3 Active Directory および Directory Server コネクタのインストール
Identity Synchronization for Windows 1 2004Q3 Directory Server プラグインのインストール
Identity Synchronization for Windows サービスの停止
コネクタ状態の復元 (persist、etc ディレクトリ)
Identity Synchronization for Windows サービスの開始
同期の開始
ログの監視

移行の準備

Identity Synchronization for Windows バージョン 1.0 からバージョン 1 2004Q3 への移行を準備する手順は、次のとおりです。

1. コマンドプロンプトに次のコマンドを入力します。

   - Solaris または SPARC 環境 : **`uncompress -c <`***filename***`> | tar xf -`** と入力する
   - Windows 環境 : **`%JAVA_HOME%\bin\jar -xf <`***filename***`>`** と入力する
     または、WinZip® などの任意の Windows 用 zip アーカイブプログラムを使用する

   バイナリの展開が完了すると、必要な移行ツールが格納された次のサブディレクトリが作成されます。

   - `installer/`
   - `lib/`
   - `migration/`

Solaris	Windows
export10cnf.jar	export10cnf.jar
—	forcepwchg.exe
checktopics.jar	checktopics.jar

2. バージョン 1.0 の設定を XML ファイルにエクスポートします。188 ページの「export10cnf ユーティリティの使用」で説明したように、`migration` ディレクトリから `export10cnf` を実行します。次に例を示します。

   ```
   java -jar export10cnf.jar -D "cn=directory manager" -w - -s
   "dc=example,dc=com" -q - -f export.cfg
   ```

3. エクスポートされた XML ファイルにパスワードを入力します。

   エクスポートした設定ファイルのすべての `cleartextPassword` フィールドで、二重引用符の間にパスワードを入力します (189 ページの「クリアテキストパスワードの挿入」を参照)。

4. 183 ページの「同期の開始と終了」で説明した方法で同期を終了します。

5. システムが静止状態にあることを確認します。194 ページの「checktopics ユーティリティの使用」で説明したように、`migration` ディレクトリから `checktopics` を実行します。

   次に例を示します。

```
java -jar checktopics.jar -D "cn=directory manager" -w - -s
"dc=example,dc=com" -q -
```

6. 184 ページの「サービスの開始と停止」で説明した方法で Identity Synchronization for Windows サービス (デーモン) を停止します。

注	この時点では Sun Java System Message Queue サービスを停止しないでください。

7. *Windows NT* のみに適用 : Sun Java System NT Change Detector サービスを停止します。サービスは、コマンド行に次のように入力することで停止できます。

```
net stop "Sun Java(TM) System NT Change Detector"
```

8. *Windows NT* のみに適用 : 次の手順を実行し、NT ChangeDetector サービスのカウンタを保存します。
   a. `regedt32.exe` を実行してレジストリエディタを開きます。
   b. `HKEY_LOCAL_MACHINE` ウィンドウを選択します。
   c. `SOFTWARE¥Sun Microsystems¥PSW¥1.0` ノードを探します。
   d. 次のレジストリ値を保存します。
      - `HighestChangeNumber`
      - `LastProcessedSecLogRecordNumber`
      - `LastProcessedSecLogTimeStamp`
      - `QueueSize`
9. 既存の 1.0 インストールの `persist` ディレクトリと `etc` ディレクトリをバックアップし、コネクタの状態を保存します。
   - Solaris 環境 : **`cd <`*serverroot*`>/isw-<`*hostname*`> tar cf /var/tmp/connector-state.tar persist etc`** と入力する
   - Windows 環境 : **`cd <`*serverroot*`>¥isw-<`*hostname*`>`**
     `zip -r C:¥WINNT¥Temp¥connector-state.zip persist etc`
     `%JAVA_HOME%¥bin¥jar -cfM %TEMP%¥connector-state.jar persist etc` と入力する
     または、WinZip などの任意の Windows 用 zip アーカイブプログラムを使用する
10. Identity Synchronization for Windows サービスを開始します (184 ページを参照)。

注	Sun Java Message Queue サービスは停止されていないため、開始の必要はありません。

Identity Synchronization for Windows のアンインストール

注

Identity Synchronization for Windows 1.0 以外のアプリケーションが `SUNWjss` パッケージを使用するように登録されていない場合、Identity Synchronization for Windows 1.0 のアンインストールプログラムは、このパッケージを削除します。特に、Directory Server 5.2.2 の zip バージョンをインストールした Solaris 環境では、このような状況が生じる可能性があります。この場合、アンインストールプログラムは `/usr/share/lib/mps/secv1` から `jss3.jar` を削除します。

Identity Synchronization for Windows 1 2004Q3 への移行時にこのような状況が生じた場合、インストーラは必要ファイルが不足していることを示すメッセージを表示し、インストールログにファイル名を記録します。このエラーが発生したときは、必要なパッチ (55 ページの「Sun Java System ソフトウェアの要件」を参照) を再インストールしてからインストールプロセスをやり直してください。

準備手順を完了すると、次の方法で Identity Synchronization for Windows バージョン 1.0 または 1.0 SP1 をアンインストールする準備が整います。

1. Directory Server プラグインを手動でアンインストールし、プラグインがインストールされていた Directory Server をそれぞれ再起動します。
2. プラグインがインストールされていた各 Directory Server で、次の手順を実行します。
   a. Directory Server から次のエントリを削除します。

      ```
      cn=config,cn=pswsync,cn=plugins,cn=config
      cn=pswsync,cn=plugins,cn=config
      ```

      次に例を示します。

      `ldapdelete -D "cn=directory manager" -w - -p <`*`port`*`> -c cn=config, cn=pswsync,cn=plugins,cn=config cn=pswsync,cn=plugins,cn=config`

   b. Directory Server を再起動します。
      - Solaris 環境 : **`<`*`serverroot`*`>/slapd-<`*`hostname`*`>/restart-slapd`** と入力する
      - Windows 環境 : **`<`*`serverroot`*`>¥slapd-<`*`hostname`*`>¥restart-slapd.bat`** と入力する

   c. システムからプラグインバイナリを削除します。

- Solaris 環境 : **rm <*serverroot*>/lib/psw-plugin.so**
  rm <*serverroot*>/lib/64/psw-plugin.so と入力する
- Windows 環境 : **del <*serverroot*>¥lib¥psw-plugin.dll** と入力する

3. ディレクトリを **<*server_root*>¥isw-<*hostname*>** に変更し (**cd**)、Identity Synchronization for Windows 1.0 のアンインストールプログラムを使用してバージョン 1.0 または 1.0 SP1 のコネクタとコンポーネントをアンインストールします。

注	コネクタは、常にコアコンポーネントのアンインストール前にアンインストールしてください。

   - Solaris または SPARC 環境 : **./runUninstaller.sh** と入力する
   - Windows 環境 : **¥runUninstaller.bat** と入力する

4. 次の手順を実行し、製品レジストリファイルから Identity Synchronization for Windows に関するエントリを削除します。
   a. 次の位置にあるファイルのバックアップを作成します。
      - Solaris 環境 : `/var/sadm/install/productregistry`
      - Windows 環境 : `C:¥WINNT¥System32¥productregistry`
   b. 「Solaris からの 1.0 コアとインスタンスの手動アンインストール」の手順 6 に示される方法で、レジストリファイルから Identity Synchronization for Windows に関連するエントリを削除します。
5. *Windows* 環境のみに適用 : コアのアンインストールが完了したら、マシンを再起動します。

注	何らかの理由でアンインストールが失敗したときは、Identity Synchronization for Windows コンポーネントの手動アンインストールが必要になることがあります。実行方法については、207 ページの「1.0 のアンインストールが失敗した場合の対応」を参照してください。

6. *Windows* 環境のみに適用 : Identity Synchronization for Windows が稼動していないことを確認します。必要に応じてコマンド行に次のように入力し、サービスを停止してください。

   ```
   net stop "Sun Java(TM) System Identity Synchronization for Windows"
   ```

   アンインストールの完了後にこのサービスが稼動していると、共有違反が発生し、インスタンスディレクトリを削除できなくなります。

7. Identity Synchronization for Windows インスタンスのディレクトリ (`isw-<hostname>`) を削除します。

依存関係を持つ製品のインストールまたはアップグレード

次に、JRE (Java 実行時環境) のアップグレード、Message Queue のインストール、Directory Server のアップグレードを行う方法について説明します。

1. Identity Synchronization for Windows コンポーネントがインストールされている Windows NT 以外の各ホストで、Java 2 SDK (Java 2 実行時環境) をアップグレードします。1.4.2_04 以降のバージョンである必要があります。
   - Java 2 SDK: `http://java.sun.com/j2se/1.4.2/install.html`
   - Java 2 実行時環境 : `http://java.sun.com/j2se/1.4.2/jre/install.html`
2. 『Sun Java System Message Queue 3.5 SP1 Installation Guide』に記載されている手順に従って、Message Queue 3.5 SP1 をインストールします。
3. 次のサイトで入手できる『Sun Java System Directory Server 5 2004Q2 Installation and Migration Guide』に記載されている手順に従って、Directory Server のバージョンを 5.2 SP2 にアップグレードします。

   `http://docs.sun.com/db/coll/DirectoryServer_04q2`

   Directory Server をアップグレードしても、Directory Server の現在の設定とデータベースは維持されます。

Identity Synchronization for Windows 1 2004Q3 のインストール

Identity Synchronization for Windows 1 2004Q3 コンポーネントをインストールする手順は、次のとおりです。

1. Identity Synchronization for Windows 1 2004Q3 コアをインストールします。87 ページの「コアのインストール」を参照してください。
2. 次のように、Directory Server に対して `idsync prepds` を実行し、スキーマを更新します。
   - Solaris 環境 : **`cd /opt/SUNWisw/bin`** と入力する
     次に、**`idsync prepds`** *<arguments>* と入力する
   - Windows 環境 : **`cd ¥`***<serverroot>***`¥isw-`***<hostname>***`¥bin`** と入力する
     次に、**`idsync prepds`** *<arguments>* と入力する

idsync prepds については、付録 A 「Identity Synchronization for Windows のコマンド行ユーティリティの使用」を参照してください。

3. 次のように入力し、バージョン 1.0 の設定が記録された XML ファイルをインポートします。

   idsync importcnf <*arguments*>

   注 プログラムが入力設定ファイル内のエラーを検出した場合はエラーとなります。Identity Synchronization for Windows は importcnf プロセスを中止し、問題の解決に必要な情報を出力します。

   idsync importcnf の使用については、付録 A の「importcnf の使用」を参照してください。

4. Identity Synchronization for Windows 1 2004Q3 コネクタをインストールします (160 ページの「コネクタのインストール」を参照)。
5. Identity Synchronization for Windows 1 2004Q3 Directory Server プラグインをインストールします (171 ページの「Directory Server プラグインのインストール」を参照)
6. 184 ページの「サービスの開始と停止」で説明した方法で Identity Synchronization for Windows サービス (デーモン) を停止します。
7. *Windows NT* のみに適用 : Sun Java™ System NT ChangeDetector サービスを停止します。サービスは、コマンド行に次のように入力することで停止できます。

   net stop "Sun Java(TM) System NT Change Detector"

8. *Windows NT* のみに適用 : 次の手順を実行し、NT ChangeDetector サービスのカウンタを復元します。
   a. regedt32.exe を実行してレジストリエディタを開きます。
   b. HKEY_LOCAL_MACHINE ウィンドウを選択します。
   c. SOFTWARE¥Sun Microsystems¥Sun Java(TM) System Identity Synchronization for Windows¥1.1 ノードを探します。
   d. 次の各エントリをダブルクリックし、バージョン 1.0 のアンインストール前に保存した値を復元します。
      - HighestChangeNumber
      - LastProcessedSecLogRecordNumber
      - LastProcessedSecLogTimeStamp
      - QueueSize

9. *Windows NT* のみに適用 : Sun Java™ System NT ChangeDetector サービスを開始します。サービスは、コマンド行に次のように入力することで開始できます。

   ```
   net start "Sun Java(TM) System NT Change Detector"
   ```

10. インスタンスのディレクトリから 1 2004Q3 の `persist` ディレクトリと `etc` ディレクトリ (およびすべての内容) を削除し、200 ページの「移行の準備」でバックアップしたバージョン 1.0 または 1.0 SP1 の `persist` ディレクトリと `etc` ディレクトリを復元します。

    - Solaris 環境 : 次のように入力する

      ```
      cd /var/opt/SUNWisw
      rm -rf etc persist
      tar xf /var/tmp/connector-state.tar
      ```

    - Windows 環境 : 次のように入力する

      ```
      cd <serverroot>¥isw-<hostname>
      rd /s etc persist
      %JAVA_HOME%¥bin¥jar -xf %TEMP%¥connector-state.jar
      ```

      または、WinZip などの任意の Windows 用 zip アーカイブプログラムを使用する

11. Identity Synchronization for Windows サービスを開始します (184 ページを参照)。

12. 183 ページの「同期の開始と終了」で説明した方法で同期を開始します。

13. セントラル監査ログを調べ、警告メッセージが出力されていないことを確認します。

注 バージョン 1.0 のログ設定をカスタマイズしていた場合は、バージョン 1 2004Q3 のインストールにそのカスタマイズ設定を手動で適用する必要があります。バージョン 1 2004Q3 のログの設定は、Identity Synchronization for Windows コンソールを使用して行います。

1.0 のアンインストールが失敗した場合の対応

バージョン 1 2004Q3 のインストールプログラムがバージョン 1.0 システムの残存物を検出すると、1 2004Q3 のインストールは失敗します。このため、バージョン 1 2004Q3 をインストールする前に、1.0 のすべてのコンポーネントをシステムから完全に削除する必要があります。

アンインストールプログラムがバージョン 1.0/1.0 SP1 のコンポーネントをすべて削除できなかった場合は、Identity Synchronization for Windows の製品レジストリと Solaris パッケージを手動でクリーンアップする必要があります。

次の 3 つの項では、Identity Synchronization for Windows バージョン 1.0 を手動でアンインストールする詳細な手順について説明します。

- 208 ページの「Solaris からの 1.0 コアとインスタンスの手動アンインストール」
- 214 ページの「Windows 2000 からの 1.0 コアとインスタンスの手動アンインストール」
- 219 ページの「Windows NT からの 1.0 インスタンスの手動アンインストール」

注 ここに示すアンインストール手順は、Identity Synchronization for Windows バージョン 1.0 のアンインストールだけに適用されます。

Identity Synchronization for Windows のアンインストールプログラムが失敗した場合以外は、次に示す手動アンインストール手順を使用しないでください。

Solaris からの 1.0 コアとインスタンスの手動アンインストール

Solaris マシンからコアを手動でアンインストールするには、ここで説明する手順を実行します。

注 ここでは、Identity Synchronization for Windows の位置を次のように示します。

<*serverroot*>/isw-<*hostname*>

この <*serverroot*> は、Identity Synchronization for Windows のインストール先の親ディレクトリを示します。

たとえば、Identity Synchronization for Windows を /var/Sun/mps/isw-<*example*> にインストールした場合、<*serverroot*> は /var/Sun/mps となります。

---

1. 端末ウィンドウに **/etc/init.d/isw stop** と入力し、Identity Synchronization for Windows のすべての Java プロセスを停止します。

   上のコマンドを実行してもすべての Java プロセスが停止されない場合は、次のように入力します。

   /usr/ucb/ps -gauxwww | grep java

   kill -s SIGTERM < 上のコマンドで得られるプロセス ID**>**

2. 次の方法で Message Queue を停止します。

   a. プロンプトに次のコマンドを入力し、Message Queue ブローカを停止します。

      /etc/init.d/imq stop

   b. 次のように入力し、残りの imq プロセスを停止します。

      *** ps -ef | grep imqbroker**

      *** kill -s SIGTERM <** 上のコマンドで得られるプロセス ID**>**

   c. 次のいずれかの方法で、ブローカのパッケージとディレクトリをアンインストールします。

      - コアがインストールされているホストの Identity Synchronization for Windows インスタンスのディレクトリに格納されている Message Queue ブローカアンインストールスクリプトを使用して、ブローカをアンインストールする。次のように入力する

        /<*serverroot*>/isw-<*hostname*>/imq_uninstall

      - パッケージとディレクトリを次のように手動アンインストールする

pkgrm: コマンドを使用して、これらのパッケージを削除する

SUNWaclg	SUNWiqum	SUNWiqjx
SUNWiqlen	SUNWxsrt	SUNWiqu
SUNWjaf	SUNWiqfs	SUNWjhrt
SUNWiqdoc	SUNWiquc	SUNWiqsup
SUNWiqr	SUNWjmail	

rm -rf コマンドを使用して、これらのディレクトリを削除する

```
rm -rf /etc/imq
rm -rf /var/imq
rm -rf /usr/bin/imq*
```

3. Identity Synchronization for Windows 1.0 Solaris パッケージを削除するには、表 7-1 に示されるパッケージごとに pkgrm <*packageName*> を実行します。
たとえば、**pkgrm SUNWidscm SUNWidscn SUNWidscr SUNWidsct SUNWidsoc** のように実行します。

表 7-1 削除する Solaris パッケージ

パッケージ名	説明
SUNWidscm	Sun Java System Directory Server Identity Synchronization のコアコンポーネントとコネクタのパッケージ
SUNWidscn	Sun Java System Directory Server Identity Synchronization のコンソールヘルプファイルのパッケージ
SUNWidscr	Sun Java System Directory Server Identity Synchronization のコアコンポーネントのパッケージ
SUNWidsct	Sun Java System Directory Server Identity Synchronization のコネクタのパッケージ
SUNWidsoc	Sun Java System Directory Server Identity Synchronization のオブジェクトキャッシュのパッケージ

すべてのパッケージが削除されたことを確認するには、次のように入力します。

```
pkginfo | grep -i "Identity Synchronization"
```

注	依存関係により、既存のパッケージがまだ残っている場合は、pkgrm <*packageName*> コマンドを再実行します。

4. 次の方法で Directory Server プラグインを削除します。
   a. Directory Server コンソールで、「設定」タブを選択します。
   b. 左のパネルでプラグインのノードを展開し、「pswsync」ノードを選択します。
   c. 右のパネルで、「プラグインを有効に」ボックスのチェックマークを外します。
   d. 「保存」をクリックして変更を保存します。
   e. Directory Server コンソールで、設定ディレクトリ内の次のエントリを検索し、それを削除します。

      ```
      cn=pswsync,cn=plugins,cn=config
      ```

   f. Directory Server を停止します。
   g. 次のように入力して、プラグインのバイナリを削除します。

      rm -f /<*serverroot*>/lib/psw-plugin.so

   h. Directory Server を再起動します。
5. /var/sadm/install/productregistry にある現在の productregistry ファイルのバックアップを作成 (コピーして名前を変更) します。
6. /var/sadm/install/ にある productregistry ファイルを手動で編集し、次のエントリを削除します (存在する場合)。

注	• 最適な結果を得るには、XML エディタを使用する。標準的なテキストエディタを使用することもできる • 次のコンポーネントの一部は、ファイルに含まれていないこともある • 開始タグ (<compid>)、終了タグ (<¥compid>)、および 2 つのタグの間に含まれるすべての内容を削除する必要がある。次のリストでは、これらのタグの一部として含まれる追加テキストやタグは、連続するピリオドで表されている。211 ページの例を参照

   - `<compid>Identity Synchronization for Windows .. . </compid>`
   - `<compid>Core .. . </compid>`

- <compid>unistaller .. . </compid>
- <compid>wpsyncwatchdog .. . </compid>
- <compid>setenv .. . </compid>
- <compid>Create DIT .. . </compid>
- <compid>Extend Schema .. . </compid>
- <compid>resources .. . </compid>
- <compid>CoreComponents .. . </compid>
- <compid>Connector .. . </compid>
- <compid>DSConnector .. . </compid>
- <compid>Directory Server Plugin .. . </compid>
- <compid>DSSubcomponents .. . </compid>
- <compid>ObjectCache .. . </compid>
- <compid>ObjectCacheDLLs .. . </compid>
- <compid>SUNWidscr .. . </compid>
- <compid>SUNWidscm .. . </compid>
- <compid>SUNWidsct .. . </compid>
- <compid>SUNWidscn .. . </compid>
- <compid>SUNWidsoc .. . </compid>
- <compid>ADConnector .. . </compid>

次に、<compid> タグの例を示します。<compid> と </compid>、およびその間にあるすべてのテキストとタグを削除します。

```
<compid>Identity Synchronization for Windows
    <compversion>1.0
          <uniquename>Identity Synchronization for
Windows</uniquename>
           <compinstance>1
                    <children>
                        <compref>ADConnector
                            <instance>1
                                <version>1.0</version>
                            </instance>
                        </compref>
                        <compref>DSSubcomponents
                        . . .

        </compinstance>
    </compversion>
</compid>
```

7. Identity Synchronization for Windows の次のディレクトリとファイルを削除します。

   a. インストール位置で、次のように入力します。

      rm -rf /<*serverroot*>/isw-<*hostname*>

   b. 次のように入力し、ブートストラップファイルを削除します。

      rm -rf /etc/init.d/isw

8. 次の方法で設定ディレクトリをクリーンアップします。

   a. Identity Synchronization for Windows コアがインストールされている設定ディレクトリに対して次の `ldapsearch` コマンドを実行し、Identity Synchronization for Windows コンソールのサブツリーを識別します。

      ```
      ldapsearch -D "cn=directory manager" -w <my_password> -b
      o=netscaperoot "(nsnickname=isw)" dn
      ```

注	ldapsearch は、Directory Server の *<serverroot>*/shared/bin/ldapsearch ディレクトリに格納されています。 たとえば、/var/Sun/mps/shared/bin/ldapsearch にあります。

実行結果として、次のようなエントリが取得されます。エントリは、常に *o=NetscapeRoot* で終わります。

```
"cn=Sun Java System Identity Synchronization for
Windows,cn=server group,
cn=myhost.mydomain.com,ou=mydomain.com,o=NetscapeRoot"
```

b. Directory Server コンソールを使用して、Identity Synchronization for Windows コンソールのサブツリーと、その下のすべてのサブツリーを削除します。

9. 次の方法で Identity Synchronization for Windows 設定レジストリをクリーンアップします。

   a. 次の ldapsearch コマンドを実行し、Directory Server 内の Identity Synchronization for Windows 設定レジストリを識別します。

   ```
   ldapsearch -D "cn=directory manager" -w <my_password> -b
   "dc=my,dc=domain"
   "(&(objectclass=iplanetservice)(ou=IdentitySynchronization))" dn
   ```

   実行結果として、次のようなエントリが取得されます。

   ```
   "ou=IdentitySynchronization,ou=Services,dc=my,dc=domain"
   ```

   b. Directory Server コンソールを使用して、Identity Synchronization for Windows 設定レジストリと、その下のすべてのサブツリーを削除します。

10. 次の方法で、コンソールに関連するその他すべてのファイルをクリーンアップします。

    a. 次のように入力し、コンソールのすべての jar ファイルを削除します。

    rm -rf <*serverroot*>/java/jars/isw*
    たとえば、/var/Sun/mps/java/jars/isw* のように実行します。

    b. 次のように入力し、コンソールサーブレットのすべての jar ファイルを削除します。

    rm -rf <*serverroot*>/bin/isw/
    たとえば、/var/Sun/mps/bin/isw/ のように実行します。

Windows 2000 からの 1.0 コアとインスタンスの手動アンインストール

Windows 2000 マシンからコアを手動でアンインストールするには、ここで説明する手順を実行します。

注 ここでは、Identity Synchronization for Windows の位置を次のように示します。

<*serverroot*>¥isw-<*hostname*>

この <*serverroot*> は、Identity Synchronization for Windows のインストール先の親ディレクトリを示します。

たとえば、Identity Synchronization for Windows を `C:¥Program Files¥Sun¥mps¥isw-`*example* にインストールした場合、<*serverroot*> は `C:¥Program Files¥Sun¥mps` となります。

1. 次のいずれかの方法で、Identity Synchronization for Windows のすべての Java プロセスを停止します。
   - 「スタート」>「設定」>「コントロールパネル」>「管理ツール」>「サービス」を選択し、「サービス」ウィンドウを開きます。右のパネルで「Sun Java System Identity Synchronization for Windows」を右クリックし、「停止」を選択する
   - コマンドプロンプトウィンドウを開き、次のコマンドを入力する

     `net stop "Sun Java(TM) System Identity Synchronization for Windows"`
   - 上の方法が機能しない場合は、次の手順を実行して Java プロセスを手動で停止する
     I. 「サービス」ウィンドウで「Sun Java System Identity Synchronization for Windows」を右クリックし、「プロパティ」を選択します。
     II. 「プロパティ」ウィンドウの「全般」タブで、「スタートアップの種類」ドロップダウンリストから「手動」を選択します。

     注 Windows のタスクマネージャで Java プロセス (`pswwatchdog.exe` など) を表示することができますが、どのプロセスが Identity Synchronization for Windows と関連するかは示されません。このため、Windows のタスクマネージャからプロセスを停止しないでください。

2. 次のいずれかの方法で、Message Queue を停止します (コアをアンインストールするだけのため)。
   - 「サービス」ウィンドウの右パネルで「iMQ Broker」を右クリックし、「停止」を選択する
   - コマンドプロンプトウィンドウを開き、次のコマンドを入力する

     net stop "iMQ Broker"
   - 上の方法が機能しない場合は、次の手順を実行して Message Queue を手動で停止する

     I. 「サービス」ウィンドウで「iMQ Broker」を右クリックし、「プロパティ」を選択します。

     II. 「プロパティ」ウィンドウの「全般」タブで、「スタートアップの種類」ドロップダウンリストから「手動」を選択します。
3. 次の方法で Directory Server プラグインを削除します。
   a. Directory Server コンソールで、「設定」タブを選択します。
   b. 左のパネルでプラグインのノードを展開し、「pswsync」ノードを選択します。
   c. 右のパネルで、「プラグインを有効に」ボックスのチェックマークを外します。
   d. 「保存」をクリックして変更を保存します。
   e. コンソールで、設定ディレクトリ内の次のエントリを検索し、それを削除します。

      `cn=pswsync,cn=plugins,cn=config`
   f. 次のいずれかの方法で、Directory Server を停止します。
      - 「サービス」ウィンドウの右パネルで「Sun Java System Directory Server 5.2」を右クリックし、「停止」を選択する
      - コマンドプロンプトウィンドウを開き、次のコマンドを入力する

        net stop slapd-<*myhostname*>
   g. Windows エクスプローラを開き、プラグインのバイナリを検索して削除します。

      <*serverroot*>¥lib¥psw-plugin.so
   h. Directory Server を再起動します。
4. コマンドプロンプトウィンドウを開き、**regedit** と入力して「レジストリエディタ」ウィンドウを開きます。

重要 : 手順 5 に進む前に、現在のレジストリファイルのバックアップを行ってください。

a. 「レジストリエディタ」の左パネルで、最上位のノード (「マイコンピュータ」) を選択します。

b. メニューバーから「レジストリ」> 「レジストリファイルの書き出し」を選択します。

c. 「レジストリファイルの書き出し」ダイアログボックスが表示されるので、ファイル名を指定し、バックアップレジストリの保存場所を選択します。

5. 「レジストリエディタ」のメニューバーから「編集」> 「削除」を選択し、Windows レジストリから次の Identity Synchronization for Windows キーを削除します。

   - `HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Uninstall¥Identity Synchronization for Windows` の下のすべてのエントリ
   - `HKEY_LOCAL_MACHINE¥SYSTEM¥*` の下のすべての `CurrentControlSet` と `ControlSet` (`ControlSet001`、`ControlSet002` など)。存在する場合は、次のエントリが削除の対象となる
     - `...¥Control¥Session Manager¥Environment¥<`*isw-installation directory*`>`
     - `...¥Services¥Eventlog¥Application¥Sun Java System Identity Synchronization for Windows`
     - `...¥Services¥Sun Java System Identity Synchronization for Windows`
     - `...¥Services¥iMQBroker`

6. `C:¥WINNT¥system32` にある現在の `productregistry` ファイルのバックアップを作成 (コピーして名前を変更) します。

7. `C:¥WINNT¥system32 ¥productregistry` ファイルを編集し、次のタグを削除します。

注

- 最適な結果を得るには、XML エディタを使用する。標準的なテキストエディタを使用することもできる
- 次のコンポーネントの一部は、ファイルに含まれていないこともある
- 開始タグ (`<compid>`)、終了タグ (`<¥compid>`)、および 2 つのタグの間に含まれるすべての内容を削除する必要がある。次のリストでは、これらのタグの一部として含まれる追加テキストやタグは、連続するピリオドで表されている。217 ページの例を参照

- <compid>Identity Synchronization for Windows .. . </compid>
- <compid>Core .. . </compid>
- <compid>unistaller .. . </compid>
- <compid>wpsyncwatchdog .. . </compid>
- <compid>setenv .. . </compid>
- <compid>Create DIT .. . </compid>
- <compid>Extend Schema .. . </compid>
- <compid>resources .. . </compid>
- <compid>CoreComponents .. . </compid>
- <compid>Connector .. . </compid>
- <compid>DSConnector .. . </compid>
- <compid>Directory Server Plugin .. . </compid>
- <compid>DSSubcomponents .. . </compid>
- <compid>ObjectCache .. . </compid>
- <compid>ObjectCacheDLLs .. . </compid>
- <compid>ADConnector .. . </compid>

次に、<compid> タグの例を示します。<compid> と </compid>、およびその間にあるすべてのテキストとタグを削除します。

```
<compid>Identity Synchronization for Windows
    <compversion>1.0
          <uniquename>Identity Synchronization for Windows</uniquename>
          <compinstance>1
                    <children>
                        <compref>ADConnector
                            <instance>1
                                <version>1.0</version>
                            </instance>
                        </compref>
                        <compref>DSSubcomponents
                        . . .

        </compinstance>
    </compversion>
</compid>
```

8. <*serverroot*>¥isw-<*hostname*> にある Identity Synchronization for Windows のインストールフォルダを削除します。

   たとえば、C:¥Program Files¥Sun¥mps¥isw-example のようなフォルダです。

9. 次の方法で設定ディレクトリをクリーンアップします。

   a. コマンドプロンプトウィンドウから、Identity Synchronization for Windows コアがインストールされている設定ディレクトリに対して ldapsearch コマンドを実行し、Identity Synchronization for Windows コンソールのサブツリーを識別します。

   注 ldapsearch は、<*serverroot*>¥shared¥bin¥ldapsearch にあります。

   次に例を示します。
   C:¥Program Files¥Sun¥mps¥shared¥bin¥ldapsearch

   ```
   ldapsearch -D "cn=directory manager" -w <my_password> -b
   o=netscaperoot "(nsnickname=isw)" dn
   ```

   実行結果として、次のようなエントリが取得されます。エントリは、常に *o=NetscapeRoot* で終わります。

   ```
   "cn=Sun Java System Identity Synchronization for
   Windows,cn=server group,
   cn=myhost.mydomain.com,ou=mydomain.com,o=NetscapeRoot"
   ```

   b. Directory Server コンソールを使用して、検索した Identity Synchronization for Windows コンソールのサブツリーと、その下のすべてのサブツリーを削除します。

10. 次のように、Identity Synchronization for Windows の設定ディレクトリ (設定レジストリとも呼ばれる) をクリーンアップします。

    a. コマンドプロンプトウィンドウから次の ldapsearch コマンドを実行し、Directory Server 内の Identity Synchronization for Windows 設定ディレクトリを識別します。

    ```
    ldapsearch -D "cn=directory manager" -w <my_password> -b
    "dc=my,dc=domain"
    "(&(objectclass=iplanetservice)(ou=IdentitySynchronization))"
    dn
    ```

    実行結果として、次のようなエントリが取得されます。

    ```
    "ou=IdentitySynchronization,ou=Services,dc=my,dc=domain"
    ```

    b. Directory Server コンソールを使用して、検索した設定ディレクトリのサブツリーと、その下のすべてのサブツリーを削除します。

11. 次の方法で、コンソールに関連するその他すべてのファイルをクリーンアップします。

    a. <*serverroot*>¥java¥jars¥isw* にある、コンソールのすべての jar ファイルを削除します。
    たとえば、C:¥Program Files¥Sun¥mps¥java¥jars¥isw* を削除します。

    b. ¥<*directory_server_install_root*>¥bin¥isw¥ にある、コンソールサーブレットのすべての jar ファイルを削除します。
    たとえば、C:¥SunJavaSystem¥Servers¥bin¥isw¥ 内の jar ファイルを削除します。

12. マシンを再起動し、すべての変更を適用します。

Windows NT からの 1.0 インスタンスの手動アンインストール

Windows NT マシンからインスタンスを手動でアンインストールするには、ここで説明する手順を実行します。

注

ここでは、Identity Synchronization for Windows の位置を次のように示します。

<*serverroot*>¥isw-<*hostname*>

この <*serverroot*> は、Identity Synchronization for Windows のインストール先の親ディレクトリを示します。たとえば、Identity Synchronization for Windows を C:¥Program Files¥Sun¥mps¥isw-*example* にインストールした場合、<*serverroot*> は C:¥Program Files¥Sun¥mps となります。

1. 次のいずれかの方法で、Identity Synchronization for Windows のすべての Java プロセス (コアとインスタンスのインストール) を停止します。

    - 「スタート」>「設定」>「コントロールパネル」>「管理ツール」>「サービス」を選択し、「サービス」ウィンドウを開きます。右のパネルで「Sun Java System Identity Synchronization for Windows」を右クリックし、「停止」を選択する
    - コマンドプロンプトウィンドウを開き、次のコマンドを入力する

      net stop "Sun Java(TM) System Identity Synchronization for Windows"

    - 上の方法が機能しない場合は、次の手順を実行して Java プロセスを手動で停止する

I. 「サービス」ウィンドウで「Sun Java System Identity Synchronization for Windows」を右クリックし、「プロパティ」を選択します。

II. 「プロパティ」ウィンドウの「全般」タブで、「スタートアップの種類」ドロップダウンリストから「手動」を選択します。

注 Windows のタスクマネージャで Java プロセス (`pswwatchdog.exe` など) を表示することができますが、どのプロセスが Identity Synchronization for Windows と関連するかは示されません。このため、Windows のタスクマネージャからプロセスを停止しないでください。

2. 次のいずれかの方法で、変更ディテクタサービスを停止します。
   - 「サービス」ウィンドウの右パネルで「Sun Java System NT Change Detector」サービスを右クリックし、「停止」を選択する
   - コマンドプロンプトウィンドウを開き、次のコマンドを入力する

     ```
     net stop "Sun Java(TM) System NT Change Detector"
     ```

   - 上の方法が機能しない場合は、次の手順を実行して変更ディテクタサービスを手動で停止する

     I. 「サービス」ウィンドウで「Change Detector Service」を右クリックし、「プロパティ」を選択します。

     II. 「プロパティ」ウィンドウの「全般」タブで、「スタートアップの種類」ドロップダウンリストから「手動」を選択します。
3. Windows NT コンピュータを再起動します。
4. Identity Synchronization for Windows のレジストリキーを削除する必要があります。コマンドプロンプトウィンドウを開き、**`regedt32`** と入力して「レジストリエディタ」ウィンドウを開きます。

警告 プログラムが複数値文字列の編集を許可しないため、`regedit` は使用しないでください。

手順 5 に進む前に、必ず現在の Windows レジストリファイルをバックアップしてください。

a. 「レジストリエディタ」の左パネルで、最上位のノード (「マイコンピュータ」) を選択します。

b. メニューバーから「レジストリ」>「レジストリファイルの書き出し」を選択します。

c. 「レジストリファイルの書き出し」ダイアログボックスが表示されるので、ファイル名を指定し、バックアップレジストリの保存場所を選択します。

5. 「レジストリエディタ」のメニューバーから「編集」>「削除」を選択し、レジストリから次の Identity Synchronization for Windows キーを削除します。

   - HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Uninstall¥Identity Synchronization for Windows の下のすべてのエントリ
   - HKEY_LOCAL_MACHINE¥SYSTEM¥* の下のすべての CurrentControlSet と ControlSet (ControlSet001、ControlSet002 など)。存在する場合は、次のエントリが削除の対象となる
     - ...¥Control¥Session Manager¥Environment¥<*isw-installation directory*>
     - ...¥Services¥Eventlog¥Application¥Sun Java System Identity Synchronization for Windows
     - ...¥Services¥Sun Java System Identity Synchronization for Windows
     - ...¥Services¥iMQBroker
   - HKEY_LOCAL_MACHINE¥SOFTWARE¥Sun Microsystems¥PSW

6. **regedt32** を使用して (regedit は使用しない)、次のレジストリキーを修正します (削除しない)。

   a. 左パネルでレジストリキーエントリを選択します。

      HKEY_LOCAL_MACHINE¥SYSTEM¥¥CurrentControlSet¥¥CONTROL¥¥LSA

      レジストリ値の型は REG_MULTI_SZ である必要があります。

   b. 右パネルで「Notification Packages」を右クリックし、「変更」を選択します。

   c. PASSFLT の値を FPNWCLNT に変更します。

7. C:¥WINNT¥system32 にある現在の productregistry ファイルのバックアップを作成 (コピーして名前を変更) します。

8. C:¥WINNT¥system32 productregistry ファイルを編集し、次のタグを削除します。

注

- 最適な結果を得るには、XML エディタを使用する。標準的なテキストエディタを使用することもできる
- 次のコンポーネントの一部は、ファイルに含まれていないこともある
- 開始タグ (<compid>)、終了タグ (<¥compid>)、および 2 つのタグの間に含まれるすべての内容を削除する必要がある。次のリストでは、これらのタグの一部として含まれる追加テキストやタグは、連続するピリオドで表されている。217 ページの例を参照

- <compid>Identity Synchronization for Windows .. . </compid>
- <compid>Core .. . </compid>
- <compid>uninstaller .. . </compid>
- <compid>wpsyncwatchdog .. . </compid>
- <compid>setenv .. . </compid>
- <compid>Create DIT .. . </compid>
- <compid>Extend Schema .. . </compid>
- <compid>resources .. . </compid>
- <compid>CoreComponents .. . </compid>
- <compid>Connector .. . </compid>
- <compid>DSConnector .. . </compid>
- <compid>Directory Server Plugin .. . </compid>
- <compid>DSSubcomponents .. . </compid>
- <compid>ObjectCache .. . </compid>
- <compid>ObjectCacheDLLs .. . </compid>
- <compid>ADConnector .. . </compid>

次に、<compid> タグの例を示します。<compid> と </compid>、およびその間にあるすべてのテキストとタグを削除します。

```
<compid>Identity Synchronization for Windows
    <compversion>1.0
       <uniquename>Identity Synchronization for Windows</uniquename>
          <compinstance>1
                    <children>
                        <compref>ADConnector
                            <instance>1
                                <version>1.0</version>
                            </instance>
                        </compref>
                        <compref>DSSubcomponents
                        . . .

         </compinstance>
    </compversion>
</compid>
```

9. *<serverroot>*¥isw-*<hostname>* にある Identity Synchronization for Windows のインストールフォルダを削除します。

   たとえば、C:¥Program Files¥Sun¥mps¥isw-example のようなフォルダです。

   注 手順 10 に進む前に、手順 8 で説明した方法で Windows レジストリを編集する必要があります。

10. パスワードフィルタ DLL を削除します。

    C:¥winnt¥system32 フォルダから passflt.dll ファイルを検索し、ファイル名を **passflt.dll.old** に変更します。

11. マシンを再起動し、すべての変更を適用します。

その他の移行例

配備によっては別のトポロジが採用されるため、単一ホストの配備を例に説明した移行プロセスとは若干異なるプロセスが必要になることもあります。

ここでは、その他の 2 つの配備例を紹介し、それぞれの移行方法について説明します。ここで説明する配備例は、次のとおりです。

- 「マルチマスターレプリケーション配備」
- 227 ページの「Windows NT を使用したマルチホスト配備」

マルチマスターレプリケーション配備

マルチマスターレプリケーション (MMR) 配備では、異なるホストに 2 つの Directory Server インスタンスがインストールされます。ホストを異なるオペレーティングシステムで実行することも可能ですが、ここでは、両方のホストが同じオペレーティングシステムで稼動している例について説明します。

表 7-2 は、2 つのホストの間で Identity Synchronization for Windows コンポーネントがどのように分散されているかを示しています。

表 7-2 マルチマスターレプリケーション配備でのコンポーネントの分散

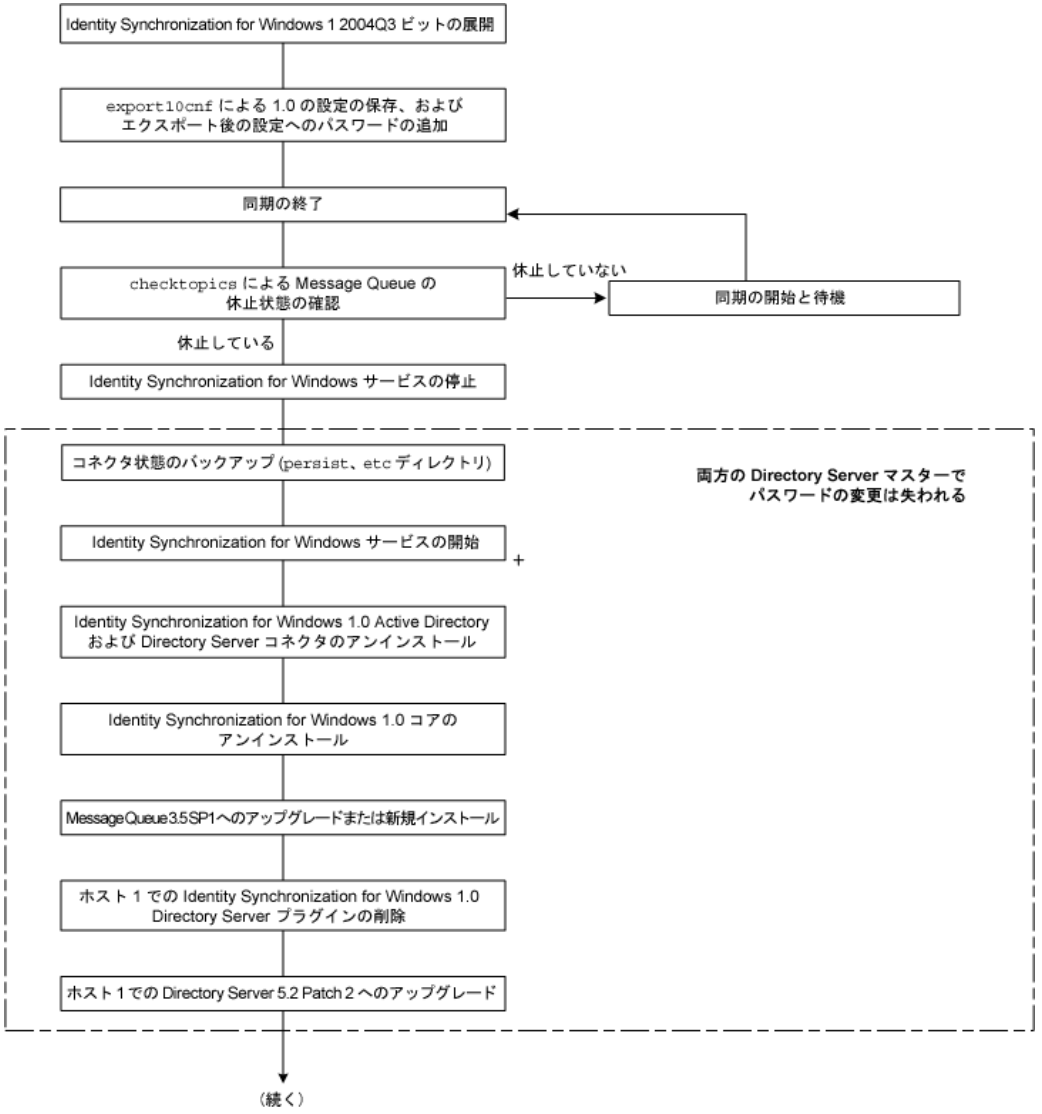
ホスト 1	ホスト 2
同期対象ユーザーの二次マスターとしての Directory Server (1 インスタンス)	同期対象ユーザーの優先マスターとしての Directory Server (1 インスタンス)
コア (Message Queue、セントラルロガー、システムマネージャ、コンソール)	Directory Server プラグイン
Active Directory コネクタ	
Directory Server コネクタ	
Directory Server プラグイン	

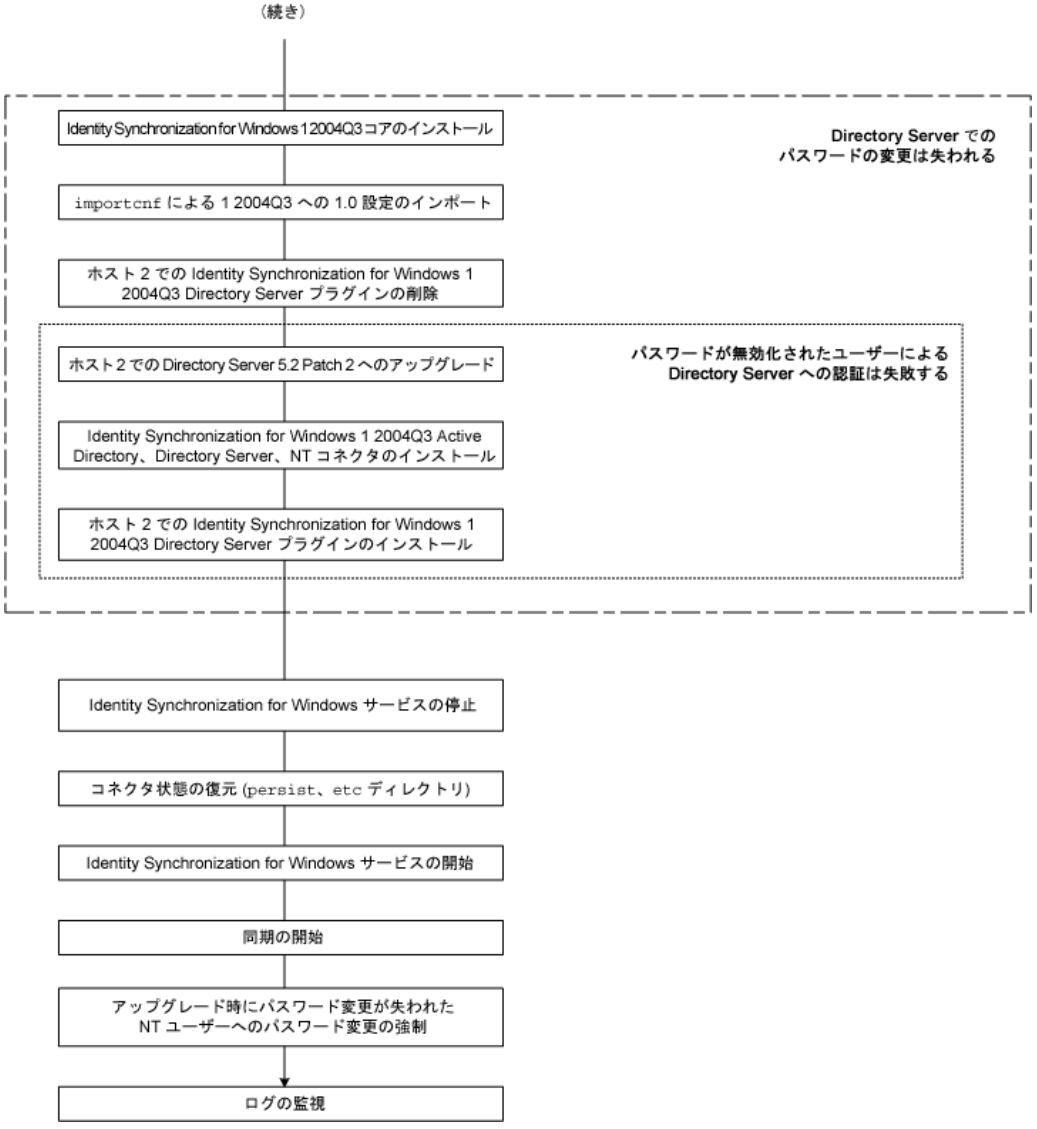
移行プロセスでは、優先マスターまたは二次マスターで継続して実行されるオンデマンドパスワード同期が維持されます。

注 両方のホストを Solaris オペレーティングシステムで実行している場合、Active Directory がインストールされた Windows 2000 を実行する第 3 のホストが同期専用に必要となります。第 3 のホストにはコンポーネントはインストールされません。

次の図は、MMR 配備での Identity Synchronization for Windows の移行プロセスを示しています。

図 7-2　マルチマスターレプリケーション配備での移行




（続き）
Identity Synchronization for Windows 1 2004Q3 コアのインストール
importcnf による 1 2004Q3 への 1.0 設定のインポート
ホスト 2 での Identity Synchronization for Windows 1 2004Q3 Directory Server プラグインの削除
ホスト 2 での Directory Server 5.2 Patch 2 へのアップグレード
Identity Synchronization for Windows 1 2004Q3 Active Directory、Directory Server、NT コネクタのインストール
ホスト 2 での Identity Synchronization for Windows 1 2004Q3 Directory Server プラグインのインストール
Directory Server での パスワードの変更は失われる
パスワードが無効化されたユーザーによる Directory Server への認証は失敗する
Identity Synchronization for Windows サービスの停止
コネクタ状態の復元 (persist、etc ディレクトリ)
Identity Synchronization for Windows サービスの開始
同期の開始
アップグレード時にパスワード変更が失われた NT ユーザーへのパスワード変更の強制
ログの監視

Windows NT を使用したマルチホスト配備

この配備例では、次の 3 つのホストが使用されます。

- Windows NT システム
- 同期対象ユーザーを格納する Directory Server と Directory Server コネクタ用のホスト
- その他すべてのコンポーネント用のホスト

表 7-3 は、3 つのホストの間で Identity Synchronization for Windows コンポーネントがどのように分散されているかを示しています。

表 7-3 マルチホスト配備

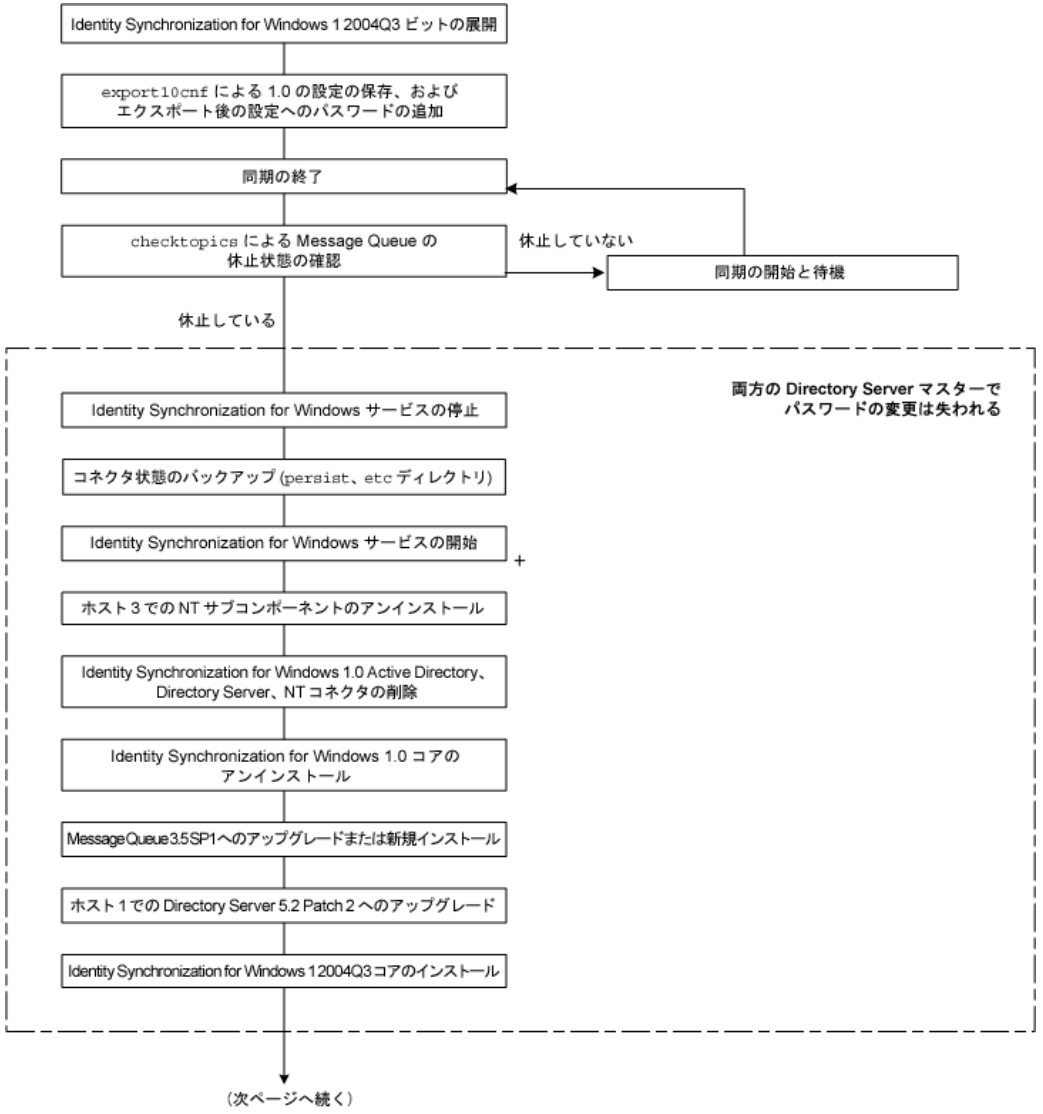
ホスト 1	ホスト 2	ホスト 3
設定リポジトリが格納された Directory Server	同期対象ユーザー用の Directory Server	Windows NT コネクタ
コア (Message Queue、セントラルロガー、システムマネージャ、コンソール)	Directory Server コネクタ	Windows NT サブコンポーネント (パスワードフィルタ DLL と変更ディテクタサービス)
Active Directory コネクタ	Directory Server プラグイン	

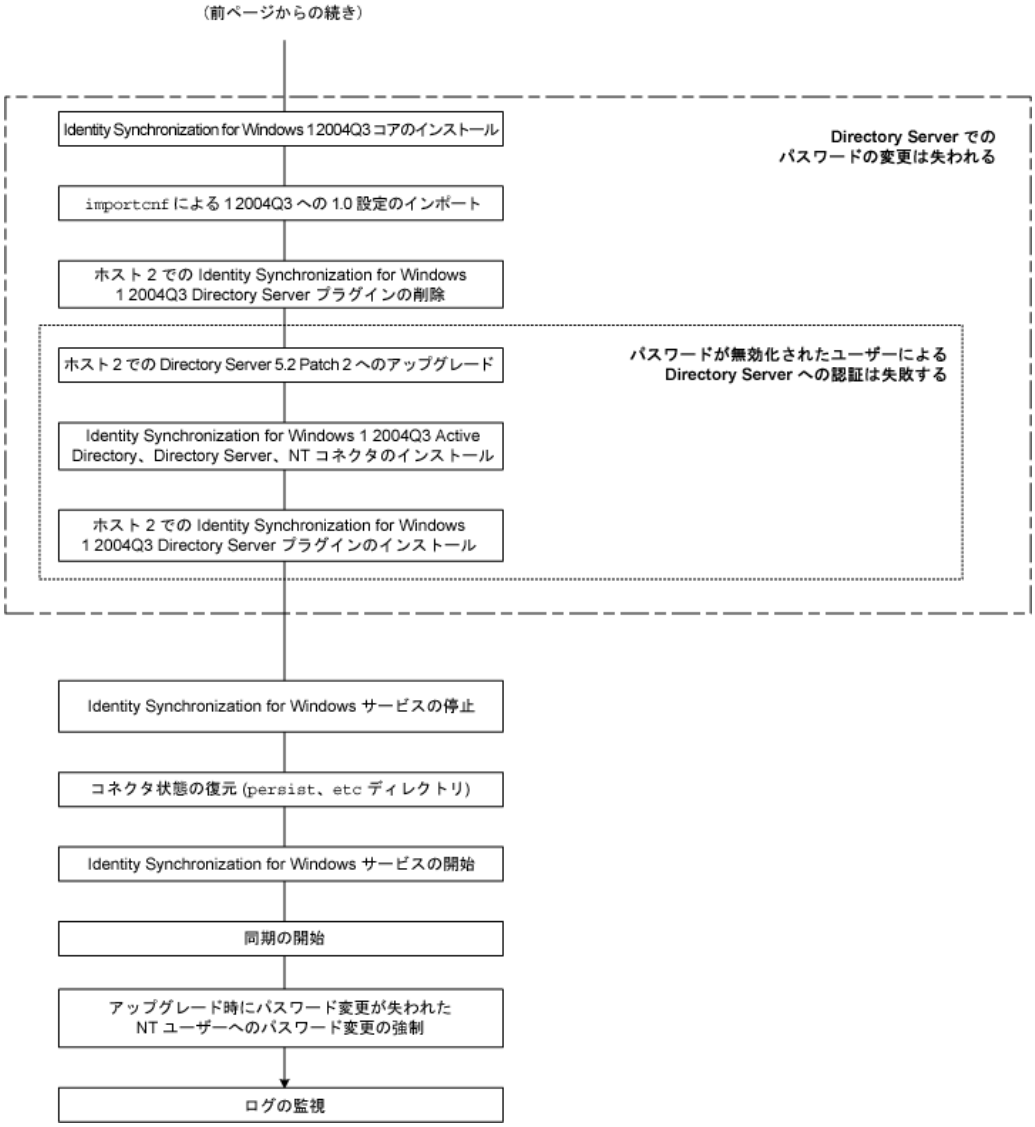
前述の例と同様に、ホスト 1、ホスト 2 は同一オペレーティングシステムで稼動しています。

注 両方のホストを Solaris オペレーティングシステムで実行している場合、Active Directory がインストールされた Windows 2000 を実行する第 4 のホストが同期専用に必要となります。第 4 のホストにはコンポーネントはインストールされません。

図 7-3 は、マルチホスト配備での Identity Synchronization for Windows の移行プロセスを示しています。

図 7-3　Windows NT を使用したマルチホスト配備での移行




（前ページからの続き）
Identity Synchronization for Windows 1 2004Q3 コアのインストール
Directory Server での
パスワードの変更は失われる
importcnf による 1 2004Q3 への 1.0 設定のインポート
ホスト 2 での Identity Synchronization for Windows
1 2004Q3 Directory Server プラグインの削除
パスワードが無効化されたユーザーによる
Directory Server への認証は失敗する
ホスト 2 での Directory Server 5.2 Patch 2 へのアップグレード
Identity Synchronization for Windows 1 2004Q3 Active
Directory、Directory Server、NT コネクタのインストール
ホスト 2 での Identity Synchronization for Windows
1 2004Q3 Directory Server プラグインのインストール
Identity Synchronization for Windows サービスの停止
コネクタ状態の復元 (persist、etc ディレクトリ)
Identity Synchronization for Windows サービスの開始
同期の開始
アップグレード時にパスワード変更が失われた
NT ユーザーへのパスワード変更の強制
ログの監視

ログのチェック

バージョン 1 2004Q3 への移行が完了したら、問題を示すメッセージが記録されていないかどうか、セントラル監査ログを調べます。特に、移行プロセス中に Directory Server ユーザーがパスワードの変更に失敗した場合、次のようなメッセージがログに記録されます。

```
[16/Apr/2004:14:23:41.029 -0500] WARNING    14  CNN101

ds-connector-host.example.com  "Unable to obtain password of user
cn=JohnSmith,ou=people,dc=example,dc=com, because the password was
encoded by a previous installation of Identity Synchronization for
Windows Directory Server Plugin. The password of this user cannot be
synchronized at this time.Update the password of this user again in
the Directory Server."
```

このログメッセージは、Identity Synchronization for Windows 1 2004Q3 で同期を開始するまで確認できません。このため、移行プロセスの最後の手順は、ログの確認となります。

第 8 章

ソフトウェアの削除

この章では、Identity Synchronization for Windows 1 2004Q3 を削除する手順について説明します。この章で説明する内容は次のとおりです。

アンインストールの計画

ソフトウェアを削除する前に、次の点に注意してください。

注	製品のコンポーネントとサブコンポーネントのアンインストールは、指示に明記されているとおりに行い、すべてのコンポーネントが正しくアンインストールされたことを確認してください。

- サブコンポーネントと Directory Server プラグインは、関連するコネクタの前にアンインストールし、すべてのコネクタは、コアの前にアンインストールする必要がある。Active Directory コネクタは、アンインストールすべきサブコンポーネントを持たない

  いずれかのコンポーネントを正しい順序でアンインストールしない場合、アンインストールすべきその他のコンポーネントを選択できなくなる。たとえば、コネクタを最初にアンインストールしなかった場合、アンインストールのためにコアを選択できなくなる
- Directory Server プラグインのアンインストールは、コアをアンインストールする前に行う必要がある

最初にコアをアンインストールすると、Directory Server から登録を解除する前にプラグインのビットが削除され、cn=pswsync,cn=plugins,cn=config を手動で削除しないかぎり、Directory Server を起動できなくなる

- 主サーバーと二次サーバーのほかにレプリカを使用するレプリケート環境では、Directory Server プラグインをアンインストールしたあとにサーバーを再起動する必要がある
- コネクタは、任意の順序でアンインストールできる
- Sun Java System Directory Server または Windows NT コネクタをアンインストールしたあとに、別のマシンにコネクタを再インストールしたり、別のサーバーポートを使用するように設定する場合は、追加手順を実行する必要がある

  この場合、関連するすべてのサブコンポーネントもアンインストールおよび再インストールし、コアがインストールされている Identity Synchronization for Windows デーモン / サービスを再起動する必要がある (184 ページの「サービスの開始と停止」を参照)
- すべてのシステムでコネクタとサブコンポーネントのアンインストールが完了するまでコアをアンインストールしてはならない
- Windows 2000 および NT プラットフォームでは、isw-*<hostname>* ディレクトリに格納されている uninstall.cmd スクリプトを実行する必要がある。また、このバッチファイルは、管理者として実行する必要がある
- Solaris オペレーティングシステムでは、デフォルトでインストールディレクトリ /opt/SUNWisw に格納されている Uninstall.sh スクリプトを実行する。このスクリプトはルートとして実行する必要がある

ソフトウェアのアンインストール

システムには、次の Identity Synchronization for Windows コンポーネントの一部またはすべてがインストールされています。

- Active Directory コネクタ
- Directory Server コネクタおよびプラグイン
- コア

Windows NT システムには、Windows NT コネクタとサブコンポーネントがインストールされている可能性があります。

すべてのコネクタとサブコンポーネントを削除し、コア (インストールされている場合) を削除するには、runUninstaller.sh (Solaris) または uninstall.cmd (Windows) を使用します。

ここでは、次の手順について説明します。

Directory Server プラグインのアンインストール

注

- アンインストーラは、Identity Synchronization for Windows の Directory Server プラグインだけを削除します。このアンインストーラを使用して、その他の Directory Server プラグインを削除することはできません。
  このマニュアルでは、特に指定がないかぎり、Directory Server プラグインという表現は、Identity Synchronization for Windows の Directory Server プラグインを意味します。
- アンインストールプログラムをテキストベースモードで実行するには、次のように入力します (Solaris 環境のみ)。

  ```
  ./runUninstaller.sh -nodisplay
  ```

  このプログラムを実行すると、パスワードがクリアテキストとしてエコーされないように、Identity Synchronization for Windows はパスワードを自動的にマスクします。

Identity Synchronization for Windows Directory Server プラグインをアンインストールする手順は、次のとおりです。

1. アンインストールプログラム (Solaris の場合は `runUninstaller.sh`、Windows の場合は `uninstall.cmd`) を起動します。

   これらのアンインストールプログラムは、インストールディレクトリ (デフォルトでは `/opt/SUNWisw`) に格納されています。
2. 「ようこそ」画面が表示されるので、「次へ」をクリックします。
3. 設定ディレクトリのホスト名とポート番号を入力します。
   - 設定ディレクトリのルートサフィックスを選択する。必要に応じて「更新」をクリックし、サフィックスのリストを表示する
   - アンインストールプログラムと設定ディレクトリサーバーの間の通信をセキュリティ保護する場合は、「セキュアポート」ボックスにチェックマークを付け、Directory Server の SSL ポート番号を指定する
4. 設定ディレクトリの管理者の名前とパスワードを入力します。

5. 「ディレクトリサーバープラグインをアンインストールします」オプションを選択します。
6. Directory Server のホスト名とポート番号、管理者のクレデンシャル (名前とパスワード) を入力します。
7. 「次へ」をクリックし、アンインストールに必要な関連タスクを実行します。
8. プラグインがインストールされていた Directory Server の再起動が要求されるので、Directory Server を再起動します。
9. サマリーウィンドウが表示されます。このウィンドウに表示される指示に従って操作します。
   - **Solaris システム** : アンインストールログは `/var/sadm/install/logs/` に書き込まれる
   - **Windows システム** : アンインストールログは `%TEMP%` ディレクトリに書き込まれる。これは次の場所の下にある `Local Settings` フォルダのサブディレクトリである

     `C:¥Documents and Settings¥Administrator`

     注 Windows 2000 Advanced Server などの一部の Windows システムでは、`Local Settings` フォルダは隠しフォルダです。

     このフォルダと `Temp` サブディレクトリの内容を表示するには、次のように操作します。

     Windows エクスプローラを開き、メニューバーから「ツール」>「フォルダオプション」を選択します。「フォルダオプション」ダイアログボックスが表示されるので、「表示」タブの「すべてのファイルとフォルダを表示する」を有効にします。

   「閉じる」をクリックしてプログラムを終了します。
10. ターゲットホストにインストールされている Identity Synchronization for Windows コンポーネントが Directory Server プラグインだけである場合は、isw-*hostname* フォルダを削除できます。
11. ネットワーク上の Windows 2000 サーバーにインストールされている Directory Server プラグインごとに、手順 1 から手順 9 を繰り返します。

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手順は、次のとおりです。

1. アンインストールプログラム (Solaris の場合は `runUninstaller.sh`、Windows の場合は `uninstall.cmd`) を起動します。

   これらのプログラムは、インストールディレクトリ (デフォルトでは `/opt/SUNWisw`) に格納されています。

2. 「ようこそ」画面が表示されるので、「次へ」をクリックします。
3. 設定ディレクトリのホスト名とポート番号を入力します。
   - 設定ディレクトリのルートサフィックスを選択する。必要に応じて「更新」をクリックし、サフィックスのリストを表示する
   - アンインストールプログラムと設定ディレクトリサーバーの間の通信をセキュリティ保護する場合は、「セキュアポート」ボックスにチェックマークを付け、Directory Server の SSL ポート番号を指定する
4. 設定ディレクトリの管理者の名前とパスワードを入力します。
5. アンインストールするコネクタを選択します。

   注 選択したコネクタは、ターゲットホストに存在する必要があります。

6. 「次へ」をクリックし、アンインストールに必要な関連タスクを実行します。
7. サマリーウィンドウが表示されます。このウィンドウに表示される指示に従って操作します。
   - **Solaris システム** : アンインストールログは `/var/sadm/install/logs/` に書き込まれる
   - **Windows システム** : アンインストールログは `%TEMP%` ディレクトリに書き込まれる。これは次の場所の下にある `Local Settings` フォルダのサブディレクトリである

     `C:¥Documents and Settings¥Administrator`

注 Windows 2000 Advanced Server などの一部の Windows システムでは、`Local Settings` フォルダは隠しフォルダです。このフォルダと `Temp` サブディレクトリの内容を表示するには、次のように操作します。

Windows エクスプローラを開き、メニューバーから「ツール」> 「フォルダオプション」を選択します。「フォルダオプション」ダイアログボックスが表示されるので、「表示」タブの「すべてのファイルとフォルダを表示する」を有効にします。

8. 「閉じる」をクリックしてプログラムを終了します。
9. ターゲットホストのすべてのインストールコネクタがアンインストールされた場合は、`isw-`*<hostname>* フォルダを安全に削除できます。
10. コネクタがインストールされているすべてのホストで、手順 1 から手順 7 を繰り返します。

コアのアンインストール

注 Directory Server プラグインのアンインストールは、コアをアンインストールする前に行う必要があります。

プラグインを削除する前にコアをアンインストールすると、Directory Server から登録を解除する前にプラグインのビットが削除され、`cn=pswsync,cn=plugins,cn=config` を手動で削除しないかぎり、Directory Server を起動できなくなります。

コアをアンインストールする手順は、次のとおりです。

1. アンインストールプログラムを起動します。
   - Windows 環境 :
     I. 「スタート」> 「設定」> 「コントロールパネル」を選択します。
     II. 「アプリケーションの追加と削除」をダブルクリックします。
     III. 「アプリケーションの追加と削除」ダイアログボックスで「Identity Synchronization for Windows」を選択し、「変更と削除」をクリックします。

- **Solaris または Windows 環境** : Solaris では `runUninstaller.sh`、Windows では `uninstall.cmd` を実行する

  これらのプログラムは、インストールディレクトリ (デフォルトでは `/opt/SUNWisw` ディレクトリ) に格納されている

2. 「ようこそ」画面が表示されるので、「次へ」をクリックします。
3. 設定ディレクトリのホスト名とポート番号を入力します。
   - 設定ディレクトリのルートサフィックスを選択する。必要に応じて「更新」をクリックし、サフィックスのリストを表示する
   - アンインストールプログラムと設定ディレクトリサーバーの間の通信をセキュリティ保護する場合は、「セキュアポート」ボックスにチェックマークを付け、Directory Server の SSL ポート番号を指定する
4. 設定ディレクトリの管理者の名前とパスワードを入力します。
5. アンインストールするコアを選択し、「次へ」をクリックします。
6. 設定ディレクトリの URL を入力して「更新」をクリックし、ドロップダウンメリストから適切なルートサフィックスを選択します。
7. 「次へ」をクリックし、アンインストールに必要な関連タスクを実行します。
8. サマリーウィンドウが表示されます。このウィンドウに表示される指示に従って操作します。
   - **Solaris システム** : アンインストールログは `/var/sadm/install/logs/` に書き込まれる
   - **Windows システム** : アンインストールログは `%TEMP%` ディレクトリに書き込まれる。これは次の場所の下にある `Local Settings` フォルダのサブディレクトリである

     `C:¥Documents and Settings¥Administrator`

   注 Windows 2000 Advanced Server などの一部の Windows システムでは、`Local Settings` フォルダは隠しフォルダです。

   このフォルダと `Temp` サブディレクトリの内容を表示するには、次のように操作します。

   Windows エクスプローラを開き、メニューバーから「ツール」>「フォルダオプション」を選択します。「フォルダオプション」ダイアログボックスが表示されるので、「表示」タブの「すべてのファイルとフォルダを表示する」を有効にします。
9. 「閉じる」をクリックしてプログラムを終了します。

注

ハードディスクの障害によってコネクタファイルを喪失した場合など、何らかの理由によって特定コネクタのアンインストーラを実行できない場合は、idsync resetconn サブコマンドを使用します (321 ページの「resetconn の使用」を参照)。

このコマンドは、コネクタを任意の場所に再インストールできるように、設定ディレクトリ内のコネクタの状態を「アンインストール済み」にリセットします。resetconn サブコマンドは、設定ディレクトリにアクセスするその他のコマンドに似ており、次の 2 つのオプションを指定できます。

- **-e <***dir-source***>**: リセットするディレクトリソースの名前を指定する。インストーラは、コネクタをディレクトリソース名で識別する
- **-n** (安全モード): 実際の処理を行わずに、指定された引数が正しいかどうかを示す

次に、コマンドの実行例を示します。

```
idsync resetconn -D "cn=Directory Manager" -w [-h CR-hostname]
[-p 389] [-s dc=example,dc=sun,dc=com] -q [-Z] [-P "cert8.db"]
[-m "secmod.db"] -e "dc=central,dc=example,dc=com" [-n]
```

resetconn の出力 :

注意 : このプログラムは、指定されたディレクトリソース「dc=central,dc=example,dc=com」に関連するコネクタのインストール状態を UNINSTALLED にリセットします。

コネクタの状態を UNINSTALLED に変更するのは最後の手段です。これは、コネクタをアンインストールすることが目的ではありません。通常は、そのコネクタを使用するマシンを失い、アンインストーラを実行できない場合に使用されます。また、このプログラムは既存の設定を書き替えます。これは少し手間のかかるプロセスです。処理を進める前に、コンソール、実行中のインストーラ、およびその他すべてのシステムプロセスを停止します。また、設定ディレクトリ内の ou=Services ツリーをバックアップのために ldif ファイルにエクスポートします。

コネクタのインストーラ設定をリセットしてよろしいですか (y/n)?

コンソールの手動アンインストール

その他すべての Identity Synchronization for Windows コンポーネントを削除したあとに、コンソールを手動でアンインストールする必要があります。

Solaris システムでの操作

Solaris システムからコンソールをアンインストールする手順は、次のとおりです。

1. 設定ディレクトリから次のサブツリーを削除します。

   ```
   cn=Sun Java (TM) System Identity Synchronization for
   Windows,cn=<server_group>,cn=<hostname>, ou=<domain_ name>,
   o=netscaperoot
   ```

2. コンソールのすべてのインストールで、*isw* というプレフィックスを持つ .jar ファイルを次のディレクトリから削除します。

   ```
   <serverroot></server>/java/jars
   ```

Windows システムでの操作

Windows Active Directory または NT システムからコンソールをアンインストールする手順は、次のとおりです。

1. 設定ディレクトリから次のサブツリーを削除します。

   ```
   cn=Sun Java (TM) System Identity Synchronization for
   Windows,cn=<server_group>,cn=<hostname>, ou=<domain_name>, o=netscaperoot
   ```

2. コンソールのすべてのインストールで、*isw* というプレフィックスを持つ .jar ファイルを次のディレクトリから削除します。

   ```
   <serverroot>/<server>/java/jars
   ```

第 9 章

トラブルシューティング

この章では、Identity Synchronization for Windows の使用時に発生する可能性のある問題の解決に役立つ情報を提供します。この章で説明する内容は、次とおりです。

トラブルシューティングチェックリスト

注

管理者 : 問題のデバッグを行うときは、ログレベル (271 ページの「ログファイルの設定」を参照) を調整し、問題の原因として考えられるすべてのイベントがログに記録されるようにします。

ユーザーが SUL に指定されていないために、プログラムがユーザー変更の同期に失敗する場合など、一部のイベントはログレベルを FINE 以上に設定するまでログに記録されません。`idsync resync` を利用したすべての操作では、ログレベルを INFO の状態に保ちます。

Identity Synchronization for Windows をインストール、設定するときは、`idsync printstat` コマンドが便利です。`printstat` を実行すると (320 ページの「printstat の使用」を参照)、インストールと設定の完了までに残されている手順がリスト表示されます。

1. セントラルエラーログファイル (error.log) に記録されている問題はありますか？

   `isw-<hostname>/logs/central/error.log`

   ほとんどのエラーはセントラルエラーログファイルに記録されます。また、通常はエラーに関する追加情報が `audit.log` ファイルに記録されます。関連するログエントリの追跡を容易にするために、エラーログのすべてのエントリは `audit.log` ファイルにも記録されます。

2. 「リリースノート」には既知の問題点が数多く記載されています。発生した問題は、そこで説明されていますか？

3. インストールは新規インストールとして行われましたか？以前の設定が完全にアンインストールされていない場合、この製品の再インストール時に問題が発生する可能性があります。過去のインストールをクリーンアップする方法については、第 8 章「ソフトウェアの削除」を参照してください。

4. コアは正しくインストールされていますか？コアが正しく完全にインストールされていれば、`isw-<hostname>/logs/central/` ディレクトリにログファイルが存在します。

5. リソースの設定時に Directory Server は稼動していましたか？

6. Message Queue とシステムマネージャを含め、コアは現在稼動していますか ?Windows 環境では、適切なサービス名を確認します。Solaris 環境では、適切なデーモン名を確認します。Message Queue とシステムマネージャがアクティブであるかどうかを確認するには、`idsync printstat` コマンドを使用します。

7. 設定は正しく保存されていますか ?`idsync printstat` コマンドを実行してコネクタのリストが出力されれば、設定は正しく保存されています。

8. コネクタはすべてインストールされていますか？同期対象のディレクトリソースごとに 1 つのコネクタをインストールする必要があります。

9. サブコンポーネントはすべてインストールされていますか？Directory Server と Windows NT のコネクタは、サブコンポーネントを必要とします。サブコンポーネントは、コネクタのインストール後にインストールします。Directory Server のそれぞれのレプリカには、Directory Server プラグインをインストールする必要があります。

10. インストール後の手順は実行しましたか？Directory Server プラグインのインストール後は、Directory Server を再起動する必要があります。また、Windows NT サブコンポーネントのインストール後は、Windows NT 主ドメインコントローラを再起動する必要があります。

11. コンソールとコマンド行のいずれかから同期を開始しましたか？

12. すべてのコネクタが現在稼動していますか？

13. コンソールまたは `idsync printstat` コマンド行ユーティリティを使用して、すべてのコネクタの状態が SYNCING であることを確認します。

14. 同期対象のディレクトリソースは現在稼動していますか?

15. コンソールを使用して、修正、作成、またはその両方が指定どおりの同期方向で同期されていることを確認します。

16. いずれか一方のディレクトリソースに存在するユーザーを同期させる場合、`idsync resync` コマンドを使用してこれらのユーザーをもう一方のディレクトリソースに作成しましたか?

    注 既存ユーザーが存在する場合は、常に `idsync resync` を実行する必要があります。既存ユーザーを再同期させない場合、再同期の動作は未定義のまま残ります。

17. 同期対象ユーザーが両方のディレクトリソースに存在する場合、`idsync resync` コマンドを使用してこれらのユーザーをリンクさせましたか?

18. Active Directory または Windows NT から Sun Java System Directory Server へのユーザー作成が失敗した場合は、Directory Server オブジェクトクラス内のすべての必須属性が作成属性として指定され、対応する属性の値がソース側ユーザーエントリに用意されていることを確認します。

19. Directory Server から Windows NT に作成を同期させる場合に、ユーザー作成には成功しても、アカウントが使用不可能となるときは、ユーザー名が Windows NT の要件に違反していないことを確認します。

    たとえば、指定した名前が Windows NT で許容される最大長を超える場合、NT 上にユーザーは作成されますが、ユーザー名を変更 (「ユーザー」>「名前の変更」) するまで使用、編集できません。

20. Windows NT SAM 変更ディテクタサブコンポーネントを有効にするには、NT 監査ログを有効にする必要があります。「スタート」>「プログラム」>「管理ツール」>「ユーザーマネージャ」を選択し、「原則」>「監査の原則」を選択します。「監査するイベント」を選択し、「ユーザーとグループの管理」で「成功」と「失敗」の両方を選択します。

    「イベントビューア」で「イベントログの設定」を選択し、「ログサイズが最大値に達したときの操作」の「必要に応じてイベントを上書きする」を選択します。

21. 同期に失敗するユーザーは、同期ユーザーリストに指定されていますか?たとえば、それらのユーザーは、同期ユーザーリストに指定されているベース DN およびフィルタと一致しますか?Active Directory が含まれる配備では、Sun Java System Directory Server エントリが同期ユーザーリストに指定されていない場合、オンデマンドのパスワード同期は警告なしで失敗します。多くの場合、この問題は同期ユーザーリストのフィルタが正しくないために発生します。

22. 同期設定は変更されていませんか?Active Directory から Sun Java System Directory Server へのユーザーの同期を、Directory Server から Active Directory へのユーザーの同期に変更した場合は、コネクタの証明書データベースに Active Directory SSL CA 証明書を追加する必要があります。`idsync certinfo` コマンドを実行すると、現在の SSL 設定でインストールが必要な SSL 証明書が示されます。

23. すべてのホスト名は正しく指定され、DNS 解決されていますか? Active Directory ドメインコントローラは、Active Directory コネクタが稼動するマシン、および Sun Java System Directory Server プラグインが稼動しているマシンから DNS 解決できる必要があります。

24. Active Directory ドメインコントローラの IP アドレスは、コネクタがコントローラの接続に使用する名前に解決されますか?

25. ソースコネクタは、ユーザーに加えられた変更を検出していますか?ユーザーが追加または修正されたディレクトリソースのコネクタが変更を検出するかどうかを確認するときは、セントラル監査ログ (`audit.log`) を調べます。

26. ターゲットコネクタは、この変更を処理していますか?

27. 複数の同期ユーザーリストが設定されていませんか?設定されている場合、それらは競合していませんか?コンソールを使用して、詳細度がより高い同期ユーザーリストの順序を、詳細度が低い同期ユーザーリストより先にします。

28. 同期フローを双方向、または Sun から Windows に設定し、配備に Active Directory データソースが含まれる場合、コネクタは SSL 通信を使用するように設定されていますか?

29. Solaris 環境でメモリの問題が発生したと考えられる場合は、プロセスを調べます。どのコンポーネントが別プロセスとして実行されているかを確認するときは、次のように入力します。

    `/usr/ucb/ps -gauxwww | grep com.sun.directory.wps`

    コネクタの ID、システムマネージャ、セントラルロガーなど、すべての詳細情報が出力されます。これは、いずれかのプロセスがメモリを過度に消費していないかどうかを調べる場合に便利です。

30. Sun Java System Directory Server ソースを作成または編集する場合に、Directory Server の「既知のサーバーを選択します」ドロップダウンリストに Directory Server が表示されない場合は、その Directory Server が稼動していることを確認します。使用可能ホストのドロップダウンリストに表示される Directory Server は、稼動している必要があります。

    該当するサーバーが一時的にダウンしている場合は、「ホスト名とポートを入力してサーバーを指定」フィールドにホスト名とポート番号を入力します。

注	Identity Synchronization for Windows は、デフォルトでは短いホスト名を使用しますが、デフォルトのホスト名が実際の配備では正しく機能しない場合もあります。ホスト名を指定するときは、常に完全修飾名を使用することをお勧めします。

31. アンインストールプログラムの実行時に次のエラーメッセージが出力されますか？

```
./runInstaller.sh
IOException while making /tmp/SolarisNativeToolkit_5.5.1_1
executable:java.io.IOException: Not enough space
java.io.IOException: Not enough space
```

/tmp にマウントされるスワップファイルのサイズを大きくします。

コネクタのトラブルシューティング

ここでは、コネクタに関連する問題のトラブルシューティングについて説明します。ここで説明する内容は次のとおりです。

- 245 ページの「ディレクトリソースを管理するコネクタの ID を特定する方法」
- 247 ページの「コネクタの現在の状態を確認する方法」

ディレクトリソースを管理するコネクタの ID を特定する方法

コネクタ ID は、次のいずれかの方法で特定することができます。

- 「セントラルログの使用」
- 「idsync printstat の使用」

セントラルログの使用

セントラル監査ログ (audit.log) を調べ、同期させるディレクトリソースのコネクタ ID を特定します。起動時に、セントラルロガーは各コネクタと、それが管理するディレクトリソースの ID をログに記録します。最新の情報を確認するには、起動バナーの最後のインスタンスについて調べます。

たとえば、次のログメッセージでは 2 つのコネクタを確認できます。

- CNN101 は、dc=airius,dc=com を管理する Sun Directory Server コネクタ
- CNN100 は、airius.com ドメインを管理する Active Directory コネクタ

```
[2003/03/19 00:00:00.722 -0600] INFO    16     "System Component
Information:    SysMgr_100 is the system manager (CORE);  console
is the Product Console User Interface;  CNN101 is the connector
that manages [dc=airius,dc=com (ldap://host1.airius.com:389)];
CNN100 is the connector that manages [airius.com
(ldaps://host2.airius.com:636)];"
```

idsync printstat の使用

コネクタの ID と状態は、idsync printstat コマンドを使用して確認することもできます (320 ページの「printstat の使用」を参照)。

次に、このコマンドの出力例を示します。

```
Connector ID: CNN100
   Type:Active Directory
   Manages: airius.com (ldaps://host2.airius.com:636)
   State:READY

Connector ID: CNN101
   Type:     Sun Java System Directory
   Manages: dc=airius,dc=com (ldap://host1.airius.com:389)
   State:READY

Sun Java System Message Queue Status: Started

Checking the System Manager status over the Sun Java System
Message Queue.

System Manager Status: Started

SUCCESS
```

コネクタの現在の状態を確認する方法

同期に関与するコネクタの現在の状態を調べるときは、コンソールの「状態」パネル、または前述の idsync printstat コマンドを使用するか、セントラル監査ログ (audit.log) を調べます。

コネクタの状態を示す最後のメッセージを audit.log ファイルで検索します。たとえば、次のメッセージでは、コネクタ CNN101 の状態が READY であることがわかります。

```
[2003/03/19 10:20:16.889 -0600] INFO    13  SysMgr_100 host1
"Connector [CNN101] is now in state "READY"."
```

表 9-1 は、コネクタの各種状態を説明しています。

表 9-1 コネクタの状態の意味

状態	意味
UNINSTALLED	コネクタはインストールされていない
INSTALLED	コネクタはインストールされているが、設定を受信していない
READY	コネクタはインストールされ、設定も受信しているが、同期のために起動されていない
SYNCING	コネクタはインストールされ、設定も受信し、同期のための起動も試みられている

コネクタの状態が UNINSTALLED である場合の対応

コネクタをインストールします。

コネクタのインストールに失敗したが、再インストールできない場合の対応

コネクタのインストールに失敗したが、Identity Synchronization for Windows のインストールプログラムでコネクタがインストールされているものと見なされる場合、インストールプログラムを使用してコネクタを再インストールすることはできません。

idsync resetconn を実行してコネクタの状態を UNINSTALLED (アンインストール済み) にリセット (321 ページの「resetconn の使用」を参照) してからコネクタを再インストールします。

コネクタの状態が INSTALLED である場合の対応

コネクタの状態が長期間インストール済みとされるときは、ほとんどの場合は稼動していないか、Message Queue と通信できない状態にあります。

コネクタがインストールされているマシンで、発生した可能性のあるエラーについて、コネクタのログ (`audit.log` と `error.log`) を調べます。コネクタが Message Queue に接続できない場合は、エラーメッセージがここに記録されます。この場合は、考えられる原因について 255 ページの「Message Queue のトラブルシューティング」を参照してください。

監査ログの最後のメッセージの日時が古い場合は、おそらくそのコネクタは稼動していません。249 ページの「コンポーネントのトラブルシューティング」を参照してください。

コネクタの状態が READY である場合の対応

同期が開始され、すべてのサブコンポーネントがインストールされてコネクタに接続するまで、コネクタは READY 状態のまま残されます。同期が開始されていない場合は、コンソールまたはコマンド行ユーティリティを使用して開始します。

同期が開始されてもコネクタの状態が SYNCING に変わらないときは、多くの場合サブコンポーネントに問題があります。253 ページの「サブコンポーネントのトラブルシューティング」を参照してください。

コネクタの状態が SYNCING である場合の対応

すべてのコネクタの状態が SYNCING であっても、変更が同期されない場合は、同期が正しく設定されていることを確認します。

- コンソールを使用して、修正、作成、または両方が指定どおりの同期方向 (たとえば、Windows から Sun Java System Directory Server など) で同期されていることを確認する
- コンソールを使用して、変更される属性が同期対象属性であることを確認する。ただし、パスワードは常に同期される。作成したユーザーエントリが同期されない場合は、ユーザー作成フローが有効化されていることをコンソールで確認する
- ソースコネクタは、ユーザーに加えられた変更を検出しているか？ユーザーが追加または修正されたディレクトリソースのコネクタが変更を検出するかどうかを確認するときは、セントラル監査ログ (`audit.log`) を調べる。ターゲットコネクタは、この変更を処理しているか？

Active Directory コネクタが SSL 経由で Active Directory に接続できない場合の対応

Active Directory コネクタが SSL 経由での Active Directory への接続に失敗し、次のエラーメッセージが表示される場合は、Active Directory ドメインコントローラを再起動します。

```
Failed to open connection to ldaps://server.example.com:636,
error(91): Cannot connect to the LDAP server, reason:
SSL_ForceHandshake failed: (-5938) Encountered end of file.
```

コンポーネントのトラブルシューティング

コンポーネントのトラブルシューティングには、ここに示す情報を使用します。ここで説明する内容は次のとおりです。

- 249 ページの「Solaris 環境」
- 251 ページの「Windows 環境」
- 251 ページの「WatchList.properties の調査」

Solaris 環境

`/usr/ucb/ps -auxww | grep com.sun.directory.wps` コマンドを実行すると、実行されているすべての Identity Synchronization for Windows プロセスがリスト表示されます。次の表は、稼動している必要のあるプロセスを示しています。

表 9-2　Identity Synchronization for Windows のプロセス

Java プロセスクラス名	コンポーネント	条件
`com.sun.directory.wps.watchdog.server.WatchDog`	システムウォッチドッグ	常に稼動している必要がある
`com.sun.directory.wps.centrallogger.CentralLoggerManager`	セントラルロガー	コアがインストールされている場合のみ
`com.sun.directory.wps.manager.SystemManager`	システムマネージャ	コアがインストールされている場合のみ

表 9-2　Identity Synchronization for Windows のプロセス (続き)

Java プロセスクラス名	コンポーネント	条件
com.sun.directory.wps.controller.AgentHarness	コネクタ	インストールされているコネクタごとに必要

想定される数のプロセスが実行されていない場合は、次のコマンドを実行し、Identity Synchronization for Windows のすべてのプロセスを開始し直します。

```
# /etc/init.d/isw stop
# /etc/init.d/isw start
```

WatchDog プロセスが稼動していても、想定される数の java.exe プロセスが実行されていない場合は、「WatchList.properties の調査」を参照し、すべてのコンポーネントが正しくインストールされていることを確認します。

その他のシステムコンポーネントと同様に、Sun Java System Directory Server プラグインも、ユーザーが表示できるようにセントラルロガーが管理するバスを経由してログレコードを送信します。ただし、サブコンポーネントがコネクタに接続できない場合など、プラグインはこのバスを経由せずに一部のメッセージをログに記録します。この場合、ログメッセージは次のような形式で、ファイルシステム内のプラグインの logs ディレクトリだけに記録されます。

<*serverroot*>/isw-<*hostname*>/logs/SUBC<*id*>

プラグインは Directory Server プロセスと共に実行されるため、プラグインが logs ディレクトリへの書き込みを試みるときに問題が発生する可能性があります。この問題は、logs ディレクトリの所有者以外のユーザーとして Directory Server が実行される場合に生じます。この場合、そのディレクトリのアクセス権、またはネイティブオペレーティングシステムコマンドを使用する所有者を変更し、プラグインにアクセス権を明示的に与えることが必要となる可能性があります。

Windows 環境

「サービス」コントロールパネルを使用して、「Sun Java System Identity Synchronization for Windows」サービスが開始されていることを確認します。開始されていない場合、そのマシンでは Identity Synchronization for Windows は稼動していないので、開始する必要があります。サービスが開始されている場合は、タスクマネージャを使用して、`pswwatchdog.exe` (Watchdog プロセス) が実行されていることと、想定される数の次の `java.exe` プロセスが実行されていることを確認します。

- コアがインストールされている場合は、Message Queue ブローカ用の 1 プロセス
- コアがインストールされている場合は、システムマネージャ用の 1 プロセス
- コアがインストールされている場合は、セントラルロガー用の 1 プロセス
- そのマシンにインストールされているコネクタごとに 1 プロセス

注 Directory Server コンソール用など、その他の java プロセスが稼動していることも考えられます。`pswwatchdog.exe` が稼動していない場合は、「Sun Java System Identity Synchronization for Windows」サービスを開始し直します。稼動していても、想定される数の `java.exe` が実行されていない場合は、251 ページの「WatchList.properties の調査」を参照し、すべてのコンポーネントが正しくインストールされていることを確認します。

WatchList.properties の調査

Identity Synchronization for Windows コンポーネントがインストールされている各マシンでは、そのマシンで実行する必要のあるコンポーネントが `isw-<`*machine_name*`>/resources/WatchList.properties` ファイルに列挙されます。`process.name[n]` プロパティは、実行が必要なコンポーネントの名前を示します。

コアがインストールされているマシンでは、`WatchList.properties` にセントラルロガーとシステムマネージャのエントリが含まれます。

```
process.name[1]=Central Logger
...
process.name[2]=System Manager
...
```

コネクタがインストールされているマシンでは、WatchList.properties にコネクタごとのエントリが含まれます。process.name プロパティは、コネクタ ID を示します。

```
process.name[3]=CNN100
...
process.name[4]=CNN101
...
```

WatchList.properties 内のエントリと、実際に稼動しているプロセスの間に不一致がある場合は、Identity Synchronization for Windows デーモンまたはサービスを開始し直します。

2 つのコネクタがインストールされているのに 1 つのエントリしか表示されない場合など、WatchList.properties に含まれるエントリの数が想定される数より少ない場合は、インストールの失敗についてインストールログを調べます。

- **Solaris システム** : インストールログは /var/sadm/install/logs/ に書き込まれる
- **Windows システム** : インストールログは %TEMP% ディレクトリに書き込まれる。これは次の場所の下にある Local Settings フォルダのサブディレクトリである

  C:¥Documents and Settings¥Administrator

注 Windows 2000 Advanced Server などの一部の Windows システムでは、Local Settings フォルダは隠しフォルダです。

このフォルダと Temp サブディレクトリの内容を表示するには、次のように操作します。

1. Windows エクスプローラを開き、メニューバーから「ツール」>「フォルダオプション」を選択します。
2. 「フォルダオプション」ダイアログボックスが表示されるので、「表示」タブの「すべてのファイルとフォルダを表示する」を有効にします。

サブコンポーネントのトラブルシューティング

配備に含まれるサブコンポーネントのトラブルシューティングには、次のチェックリストを使用します。

1. すべてのサブコンポーネントがインストールされていますか？

   サブコンポーネントのインストールは、コネクタのインストール後に行う必要があります。

   - Active Directory コネクタでは、サブコンポーネントはインストールされない
   - Sun Java System Directory Server コネクタでは、同期対象の Sun Java System Directory Server にプラグインをインストールする必要がある
   - Windows NT コネクタでは、同期対象の Windows NT ドメインごとに変更ディテクタとパスワードフィルタのサブコンポーネントを主ドメインコントローラにインストールする必要がある。これら 2 つのサブコンポーネントは、Windows NT コネクタのインストール後にまとめてインストールされる

注 Windows NT SAM 変更ディテクタサブコンポーネントを有効にするには、NT 監査ログを有効にする必要があります。「スタート」> 「プログラム」> 「管理ツール」> 「ユーザーマネージャ」を選択し、「原則」> 「監査の原則」を選択します。「監査するイベント」を選択し、「ユーザーとグループの管理」で「成功」と「失敗」の両方を選択します。

「イベントビューア」で「イベントログの設定」を選択し、「ログサイズが最大値に達したときの操作」の「必要に応じてイベントを上書きする」を選択します。

---

2. サブコンポーネントのインストール後の操作手順は完了していますか？

   Directory Server プラグインを Sun Java System Directory Server にインストールした後は、サーバーを再起動する必要があります。また、NT 変更ディテクタとパスワードフィルタを主ドメインコントローラにインストールした後はサーバーを再起動する必要があります。

3. サブコンポーネントは稼動していますか？

   プラグインがインストールされている Directory Server は稼動していますか？変更ディテクタとパスワードフィルタがインストールされた主ドメインコントローラは稼動していますか？

4. サブコンポーネントはコネクタとのネットワーク接続を確立していますか？

コネクタが実行されているマシンで netstat -n -a を実行し、コネクタがサブコンポーネントの接続を待機していることを確認します。次の例は、異なる 3 つの配備でのこのコマンドの実行例を示しています。コネクタは、ポート 9999 で待機するように設定されています。

a. 想定どおりにコネクタは接続を待機し、サブコンポーネントは正常に接続している

```
netstat -n -a | grep 9999
      *.9999               *.*    0   0 65536    0 LISTEN
12.13.1.2.44397 12.13.1.2.9999  73620 0 73620    0
ESTABLISHED
12.13.1.2.9999  12.13.1.2.44397 73620 0 73620    0
ESTABLISHED
```

b. コネクタは接続を待機しているが、サブコンポーネントは接続していない

```
# netstat -n -a | grep 9999
     *.9999               *.*    0   0 65536    0 LISTEN
```

サブコンポーネントが稼動していることを確認し、問題についてサブコンポーネントのローカルログを調べます。

c. コネクタが接続を待機していない

```
# netstat -n -a | grep 9999
<no output>
```

正しいポート番号が指定されていることを確認します。コネクタが稼動し、状態が READY であることを確認します。問題についてコネクタのローカルログを調べます。

Message Queue のトラブルシューティング

Sun Java System Message Queue ブローカが実行されていることを確認します。Message Queue ブローカが稼動しているマシンとポートに対して telnet コマンドを実行すると、アクティブな Message Queue サービスのリストが返されます。

```
# telnet localhost 7676
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
101 psw-broker 3.0.1
cluster tcp CLUSTER 32914
admin tcp ADMIN 32912
portmapper tcp PORTMAPPER 7676
ssljms tls NORMAL 32913
jms tcp NORMAL 32911
.
Connection closed by foreign host.
```

- 出力に「ssljms tcp NORMAL」サービスが含まれない場合は、問題について Message Queue ログを調べる。コアが Solaris にインストールされている場合、Message Queue ブローカのログは次の場所にある

  /var/imq/instances/psw-broker/log/log.txt

- コアが Windows にインストールされている場合、ブローカのログは次の場所にある

  <*installation_root*>¥isw-<*machine_name*>¥imq¥var¥instances¥isw-broker¥log¥log.txt

telnet コマンドの実行が失敗した場合は、ブローカが実行されていない、または指定したポートが誤っています。ブローカのログでポート番号を確認してください。ブローカのポートは、次の行に指定されます。

```
[13/Mar/2003:18:17:09 CST] [B1004]: "Starting the portmapper
service using tcp [ 7676, 50 ] with min threads 1 and max threads
of 1"
```

ブローカが実行されていない場合、Solaris 環境では /etc/init.d/imq start を実行することで稼動を開始できます。Windows 環境では iMQ Broker Windows サービスを開始します。

Message Queue を Solaris 8 にインストールするときに、mquinstall を実行してすべてのパッケージをインストールする場合は、ソフトウェアが正しいバージョンの Java を認識するように、mqinstall を実行する前に IMQ_JAVAHOME を設定する必要があります。

まだコアをインストールしていない場合は、使用する JVM が Identity Synchronization for Windows のインストールプログラムによって Message Queue に指定されるため、IMQ_JAVAHOME を設定する必要はありません。

ブローカと設定ディレクトリの通信に関するトラブルシューティング

Message Queue ブローカは、Identity Synchronization for Windows の設定が格納されている Directory Server に対してクライアントの認証を行います。ブローカがこの Directory Server に接続できない場合、どのクライアントも Message Queue に接続できず、「javax.naming.CommunicationException」や「javax.naming.NameNotFoundException」のような javax.naming 例外がブローカログに記録されます。

javax.naming 例外が発生した場合は、次のように対応します。

- /var/imq/instances/isw-broker/props/config.properties 内のすべての imq.user_repository.ldap properties に正しい値が指定されていることを確認する。いずれかに誤りがある場合は、Message Queue ブローカを停止し、ファイルを修正、保存してからブローカを開始し直す。Directory Server のホスト名は、ブローカのマシンから解決可能である必要がある
- /etc/imq/passfile 内の imq.user_repository.ldap.password プロパティが正しいことを確認する
- ルートサフィックスに空白文字が含まれる場合、ブローカがエントリを検索できない可能性がある

ブローカのメモリ設定に関するトラブルシューティング

通常の動作中に Message Queue ブローカが過度のメモリを消費することはありません。しかし、idsync resync の実行時は、ブローカのメモリ消費量は大きくなります。ブローカの使用メモリ量が制限に達すると、未配信のメッセージが蓄積され、idsync resync の動作速度が著しく低下する、または完全に停止します。これ以後、Identity Synchronization for Windows が応答しなくなることもあります。

ブローカの使用可能メモリ容量が低下すると、ログに次のようなメッセージが記録されます。

```
[03/Nov/2003:14:07:51 CST] [B1089]: In low memory condition,
Broker is attempting to free up resources

[03/Nov/2003:14:07:51 CST] [B1088]: Entering Memory State
[B0024]: RED  from previous state [B0023]: ORANGE - current
memory is 1829876K, 90% of total memory
```

このような状況の発生を回避するには、次のように対応します。

- 『Sun Java System 1 2004Q3 Identity Synchronization for Windows リリースノート』で説明されているように、ブローカのメモリ制限を 1 または 2G バイトに増やす
- idsync resync の実行中は、ログレベルを INFO で維持する。ログレベルを FINE 以上に変更した場合、セントラルロガーに送信されるログメッセージが増えるため、ブローカでの負荷が大きくなる
- 1 同期ユーザーリストごとに idsync resync を実行する

ブローカの使用可能メモリがなくなった場合に復元するには、次の手順を実行します。

1. 適切なディレクトリで持続的なメッセージストアを調べ、ブローカに未配信メッセージのバックログがあることを確認します。
   - Solaris 環境 : /var/imq/instances/psw-broker/filestore/message/
   - Windows 環境 : <*installation_root*>¥isw-<*machine_name*>¥imq¥var¥instances¥isw-broker¥filestore¥message¥
2. このディレクトリ内の各ファイルには、1 つの未配信メッセージが含まれます。このディレクトリ内のファイル数が 10000 を超える場合、ブローカはメッセージのバックログを持ちます。[1] バックログが存在しない場合は、ブローカに別の問題があります。

3. メッセージのバックログは、idsync resync の動作に関連するログファイルの中で、おそらく安全に削除できる唯一のログファイルです。
4. 184 ページの「サービスの開始と停止」で説明した方法で Message Queue ブローカを停止します。
5. 持続的メッセージストア内のすべてのファイルを削除します。これらのファイルを削除する最も簡単な方法は、message/ ディレクトリを一度削除し、作成し直すことです。
6. Message Queue ブローカを開始し直します。

ブローカの使用可能メモリがなくならないように、ここで説明した操作方法を実行します。

SSL の問題に関するトラブルシューティング

SSL に関する問題を診断するときは、Identity Synchronization for Windows のコンポーネント間で SSL を設定する方法について説明している第 11 章「セキュリティの設定」も参照してください。ここで説明する内容は次のとおりです。

- コアコンポーネント間の SSL
- コネクタと Directory Server または Active Directory の間の SSL
- Directory Server プラグインと Active Directory の間の SSL

コアコンポーネント間の SSL

Identity Synchronization for Windows のインストールプログラムは、コアのインストール時に指定された SSL ポートが正しいかどうかを検証できません。コアのインストール時に誤った SSL ポート番号を指定した場合、コアコンポーネントは正しく通信できません。設定を最初に保存するときまで、この問題に気がつかない可能性があります。コンソールには、次の警告が表示されます。

```
The configuration was successfully saved, however, the System
Manager could not be notified of the new configuration.
```

1. すべてのメッセージが配信された場合でも、ファイルの作成と削除がパフォーマンスを犠牲にしないように、ブローカは最大で 10000 のメッセージファイルを維持できます。

システムマネージャログには次のようなエントリが記録されます。

```
[10/Nov/2003:10:24:35.137 -0600] WARNING 14   example  "Failed to
connect
to the configuration directory because "Unable to connect:
(-5981)
Connection refused by peer.".  Will retry shortly."
```

このような場合は、コアをアンインストールし、正しい SSL ポート番号を指定してインストールし直します。

コネクタと Directory Server または Active Directory の間の SSL

コネクタが SSL 経由で Directory Server または Active Directory に接続できない場合は、セントラルエラーログに次のようなメッセージが記録されます。

```
[06/Oct/2003:14:02:48.911 -0600] WARNING 14  CNN100 host1
"failed to open connection to ldaps://host2.airius.com:636."
```

コンソールを開き、「拡張セキュリティオプションの指定」パネルを調べます (122 ページを参照)。

信頼されない証明書

セントラル監査ログでは、これ以上の情報を確認できます。たとえば、LDAP サーバーの SSL 証明書が信頼されていない場合は、次のようなメッセージが記録されます。

```
[06/Oct/2003:14:02:480.951 -0600] INFO    14  CNN100 host1
"failed to open connection to ldaps://host2.airius.com:636,
error(91): Cannot connect to the LDAP server, reason:
SSL_ForceHandshake failed: (-8179) Peer's Certificate issuer is
not recognized."
```

ほとんどの場合は、コネクタの証明書データベースに CA 証明書が追加されていないことが原因です。これは、Directory Server に付属する certutil プログラムを実行することで確認できます。[1]

注 SUNWtlsu パッケージには、Directory Server にバンドルされていない certutil などの証明書管理ユーティリティが含まれます。このパッケージは、Sun Microsystems のサイトから無償でダウンロードできます。

このパッケージをダウンロードすると、次の場所に certutil が保存されます。

/usr/sfw/bin/certutil

次に、証明書データベースに証明書がひとつも含まれていない場合の例を示します。[2]

```
# /usr/sunone/servers/shared/bin/certutil -L -d
/usr/sunone/servers/ isw-host1/etc/CNN100
Certificate Name                                  Trust Attributes
p    Valid peer
P    Trusted peer (implies p)
c    Valid CA
T    Trusted CA to issue client certs (implies c)
C    Trusted CA to certs(only server certs for ssl) (implies c)
u    User cert
w    Send warning
```

次に、証明書データベースに Active Directory CA 証明書だけが含まれる場合の例を示します。

1. Solaris 環境では、このコマンドを実行する前に環境変数 LD_LIBRARY_PATH に <*installation_root*>/lib ディレクトリを追加する必要があります。
2. Sun Java System Directory Server と Windows NT のコネクタのデフォルト証明書データベースには、saint-cert100 と saintRootCA という 2 つの証明書が含まれます。これらの証明書はこのリリースでは使用されません。

```
# /usr/sunone/servers/shared/bin/certutil -L -d
/usr/sunone/servers/ isw-host1/etc/CNN100
Certificate Name                                    Trust Attributes
airius.com CA                                        C,c,
p    Valid peer
P    Trusted peer (implies p)
c    Valid CA
T    Trusted CA to issue client certs (implies c)
C    Trusted CA to certs(only server certs for ssl) (implies c)
u    User cert
w    Send warning
```

ここに示されるように、CA 証明書の信頼性フラグは「C,,」である必要があります。証明書が存在し、信頼性フラグが正しく設定されていても、コネクタが接続できない場合は、まず、証明書の追加後にコネクタを再起動したことを確認し、問題の診断のために Sun Java System Directory Server に付属する ldapsearch コマンドを使用します。ldapsearch が証明書を受け付けない場合、コネクタもその証明書を受け付けません。たとえば、証明書が信頼されていない場合、ldapsearch はその証明書を拒否できます。

```
# /usr/sunone/servers/shared/bin/ldapsearch -Z -P /usr/sunone/
servers/isw-host1/etc/CNN100 -h host2 -b "" -s base
"(objectclass=*)"
ldap_search: Can't contact LDAP server
    SSL error -8179 (Peer's Certificate issuer is not
recognized.)
```

ldapsearch の -P オプションは、SSL 証明書の検証にコネクタ CNN100 の証明書データベースを使用することを指定しています。コネクタの証明書データベースに正しい証明書を追加したら、ldapsearch がその証明書を受け付けることを確認し、コネクタを再起動します。

ホスト名のミスマッチ

すべての証明書を信頼する設定を無効にした状態で Identity Synchronization for Windows が SSL 接続を確立しようとすると、Identity Synchronization for Windows のコネクタは、SSL ネゴシエーション段階でサーバーに提示される証明書に記録されたホスト名とサーバーのホスト名が一致するかどうかを検証します。ホスト名が一致しない場合、コネクタは接続の確立を拒否します。

Identity Synchronization for Windows に設定するディレクトリソースのホスト名は、そのディレクトリソースが使用する証明書に埋め込まれたホスト名と常に一致する必要があります。

ホスト名の一致の確認には、次のように ldapsearch を使用できます。

```
/var/mps/serverroot/shared/bin/ldapsearch.exe -Z -P
/var/opt/SUNWisw/etc/CNN100 -3
-h host2.example.com -p 636 -s base -b "" "(objectclass=*)"
```

コマンド行に指定したホスト名 (host2.example.com) と、証明書に埋め込まれたホスト名が一致しない場合は、次のエラーメッセージが出力されます。

```
ldap_search: Can't contact LDAP server
SSL error -12276 (Unable to communicate securely with peer:
requested do main name does not match the server's certificate.)
```

ホスト名が一致した場合は、ldapsearch コマンドは正常に完了し、ルート DSE の内容が出力されます。

期限切れの証明書

サーバーの証明書の期限が切れている場合、次のようなメッセージがログに記録されます。

```
[06/Oct/2003:14:06:47.130 -0600] INFO    20  CNN100 host1
 "failed to open connection to ldaps://host2.airius.com:636,
error(91): Cannot connect to the LDAP server, reason:
SSL_ForceHandshake failed: (-8181) Peer's Certificate has
expired."
```

この場合は、サーバーは新しい証明書の発行を受ける必要があります。

Directory Server プラグインと Active Directory の間の SSL

デフォルトでは、オンデマンドパスワード同期の実行時に Directory Server は Active Directory と SSL 経由で通信しません。この通信を SSL で保護するためにデフォルトの設定を変更したときは、第 11 章「セキュリティの設定」で説明するように、各マスターレプリカの Directory Server 証明書データベースに Active Directory CA 証明書を追加する必要があります。この証明書が追加されていない場合、「DSA is unwilling to perform.」というエラーが出力され、ユーザーは Directory Server へのバインドに失敗します。プラグインのログ (たとえば `isw-<hostname>/logs/SUBC100/pluginwps_log_0.txt`) には、次のようなエントリが記録されます。

```
[06/Nov/2003:15:56:16.310 -0600]  INFO    td=0x0376DD74
logCode=81             ADRepository.cpp:310    "unable to open
connection to Active Directory server at
ldaps://host2.airius.com:636, reason: "
```

このような場合は、Directory Server の証明書データベースに Active Directory CA 証明書を追加し、Directory Server を再起動します。

コントローラの問題に関するトラブルシューティング

Active Directory ドメインコントローラをバックアップファイルから復元した場合、一部のカウンタはリセットされません。

すべてのカウンタを正しくリセットするには、Active Directory ドメインコントローラの復元後にすべてのユーザーを再同期させます。

第 10 章

監査とエラーのログファイルについて

Identity Synchronization for Windows は、インストールと設定の状態、日々のシステム動作、配備に関連するエラー状態に関する情報を記録します。

この章では、この情報にアクセスし、それを解釈する方法について説明します。ここで説明する内容は次のとおりです。

ログについて

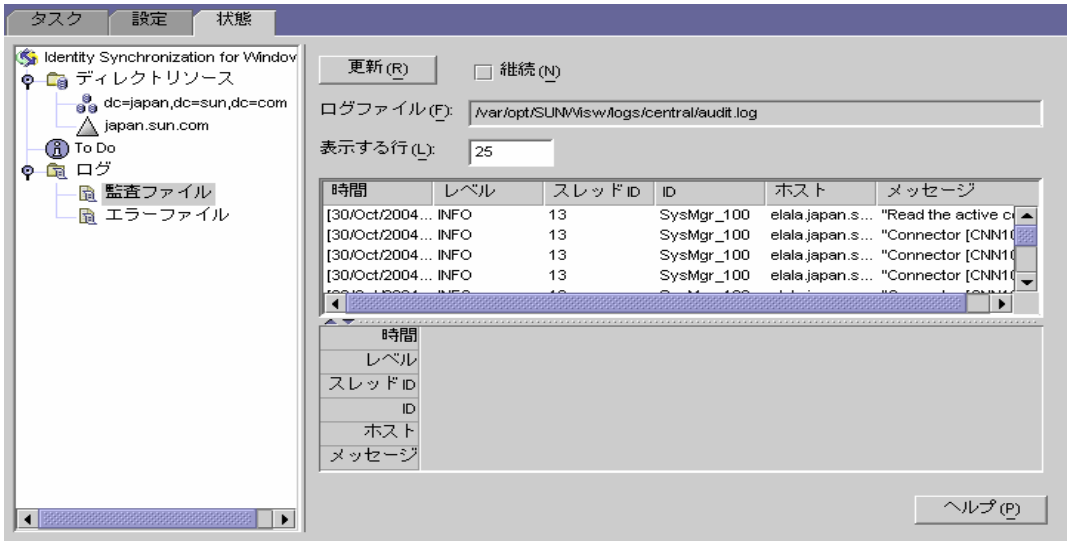
Identity Synchronization for Windows コンソールの「状態」タブには、さまざまな情報を表示できます。

左側のナビゲーションツリーパネルで次のいずれかのノードを選択すると、「状態」タブの内容が更新され、選択した項目に関する情報が表示されます。

- **ディレクトリソース** : ディレクトリソースノード (dc=example,dc=com など) を選択すると、そのディレクトリソースの状態に関する情報が表示される
- To Do : このノードを選択すると、Identity Synchronization for Windows のインストールと設定を正しく完了するために必要な手順がリスト表示される (すでに完了している手順は、すべてグレイ表示される)
- **監査ファイル** : このノードを選択すると、システムの日々の動作に関する情報 (エラー状態も含まれる) が表示される

- **エラーファイル** : このノードを選択すると、システムのエラー状態に関する情報が表示される。エラーログは、基本的にはエラーに関するエントリだけを表示するためのフィルタのように機能する

図 10-1 「状態」タブ



ログの種類

ここでは、Identity Synchronization for Windows で利用できる各種のログについて説明します。

- 266 ページの「セントラルログ」
- 267 ページの「ローカルコンポーネントログ」
- 268 ページの「Windows NT サブコンポーネントのローカルログ」
- 268 ページの「Directory Server プラグインのログ」

セントラルログ

Identity Synchronization for Windows が Message Queue にアクセスできるかぎり、監査とエラーのメッセージは Identity Synchronization for Windows セントラルロガーに記録されます。このため、これらのセントラルログ (すべてのコンポーネントからのメッセージが記録される) が主な監視対象となります。

セントラルログは、コアがインストールされているマシンの次のディレクトリに格納されます。

- Solaris 環境 : /var/opt/SUNWisw/logs
- Windows 環境 : <*installation_root*>/isw-<*machine_name*>/logs/central/

表 10-1 は、それぞれのログについて説明しています。

表 10-1 Identity Synchronization for Windows ログの種類

ログ名	説明
error.log	警告と重大なメッセージが記録される
audit.log	各同期イベントに関するメッセージを記録した、error.log のスーパーセット
resync.log	resync コマンドによって生成されるメッセージが記録される

次のように、各セントラルログには各コンポーネント ID に関する情報も含まれます。

```
[2003/03/14 14:48:23.296 -0600] INFO 13 "System Component
Information:    SysMgr_100 is the system manager (CORE);  console
is the Product Console User Interface;  CNN100 is the connector
that manages [airius.com (ldaps:// server1.airius.com:636)];
CNN101 is the connector that manages [dc=airius,dc=com (ldap://
server2.airius.com:389)];"
```

セントラルロガーのほかに、各コンポーネントには専用のローカルログがあります。セントラルロガーにログを記録できない場合は、これらのローカルログを使用して、コネクタとの問題を診断できます。

ローカルコンポーネントログ

各コネクタ、システムマネージャ、セントラルロガーには、次のローカルログがあります。

表 10-2 ローカルログ

ログ名	説明
audit.log	各同期イベントに関するメッセージを記録した、error.log のスーパーセット。これらのメッセージは、セントラルログの audit.log にも記録される

表 10-2　ローカルログ (続き)

ログ名	説明
error.log	警告と重大なメッセージが記録される。これらのメッセージは、セントラルログの error.log にも記録される

ローカルログは、次のサブディレクトリに格納されます。

- Solaris 環境 : /var/opt/SUNWisw/logs
- Windows 環境 : <*installation_root*>/isw-<*machine_name*>/logs/central/

sysmgr ディレクトリと clogger100 (セントラルロガー) ディレクトリは、コアがインストールされているマシンにあります。

Identity Synchronization for Windows は、現在のログファイルの内容を、次のようにファイル名に日付を追加したログファイルに移動し、ローカルコンポーネントログを毎日ローテーションさせます。

audit_2004_08_06.log

注　デフォルトでは、Identity Synchronization for Windows のコネクタログは 10 日後に削除されます。この期間は、Log.properties ファイルで com.sun.directory.wps.logging.maxmiumDaysToKeepOldLogs の値を編集し、サービスまたはデーモンを開始し直すことで調整できます。

Windows NT サブコンポーネントのローカルログ

次の Windows NT サブコンポーネントにもローカルログがあります。

- Windows NT 変更ディテクタ DLL
- パスワードフィルタ DLL

これらのサブコンポーネントのログは、次のディレクトリの SUBC1XX (たとえば SUBC100 など) サブディレクトリに格納されます。

<*installation_root*>/isw-<*machine_name*>/logs/

これらのファイルのサイズは 1M バイトに制限され、最新のログファイル 10 本だけが維持されます。

Directory Server プラグインのログ

Directory Server プラグインは、Directory Server コネクタを通じてセントラルログに情報を記録し、また、Directory Server のログ機能も使用します。このため、Directory Server のエラーログには、Directory Server プラグインのローカルログメッセージも保存されます。

Directory Server は、その他の Directory Server プラグインおよびコンポーネントからの情報をエラーログに保存します。Identity Synchronization for Windows Directory Server プラグインからのメッセージを識別するには、isw という文字列を含む行をフィルタリングして取り除きます。

デフォルトでは、エラーログには最小限のプラグインログメッセージが記録されます。次に例を示します。

```
[14/Jun/2004:17:08:36 -0500] - ERROR<38747> - isw - conn=-1 op=-1
msgId=-1 - Plugins unable to establish connection to DS Connector at
attila:1388, will retry later
```

次のように、Directory Server エラーログのデフォルトの詳細度は、Directory Server の管理コンソールで変更できます。

1. Directory Server コンソールを開きます。
2. 「設定」タブを選択します。
3. ナビゲーションパネルでログのノードをクリックします。
4. 「エラー」タブを選択します。
5. 「ログレベル」ボタンをクリックします。
6. 「プラグイン」ボックスを有効にします。詳細度を上げるには、「詳細モード」を有効にします。
7. 「了解」をクリックし、「保存」をクリックします。

Directory Server のログの詳細については、『Sun Java System Directory Server 5 2005Q1 管理ガイド』(http://docs.sun.com/db/prod/entsys?l=ja) を参照してください。

ログの解釈

すべてのログメッセージには、次の情報が含まれます。

- **時刻** : ログのエントリが生成された日時を示す。たとえば、次のように表記される

  `[13/Aug/2004:06:14:36:753 -0500]`

- **レベル** : ログメッセージの重要度と詳細度を示す
  Identity Synchronization for Windows には、次のログレベルがある

表 10-3　ログレベル

ログレベル	説明
INFO	これらのメッセージには、それぞれのアクションに関する最少量の情報が含まれ、システムが正常に稼動していることを確認できる。たとえば、変更がいつ検出されたか、同期がいつ行われたかを確認できる。これらのメッセージは、常に監査ログに記録される
FINE	これらのメッセージには、システム内で行われるアクションに関するより詳細な情報が含まれる
FINER	これらのメッセージには、システム内で行われるアクションに関する、さらに詳細な情報が含まれる。ログレベルを FINER に設定すると、すべてのコンポーネントのパフォーマンスに影響が生じることがある
FINEST	これらのメッセージには、システム内で行われるアクションに関するもっとも詳細な情報が含まれる。ログレベルを FINEST に設定すると、すべてのコンポーネントのパフォーマンスに著しい影響が生じることがある

- **スレッド ID** : イベントが生じた機能の Java スレッド ID を示す
- **ID** : イベントが生じたコンポーネント (コンソール、システムマネージャなど) を識別する
- **ホスト** : イベントが生じたホストの名前を示す
- **メッセージ** : イベントに関する監査またはエラー情報を示す
  たとえば、次のような情報が記録される

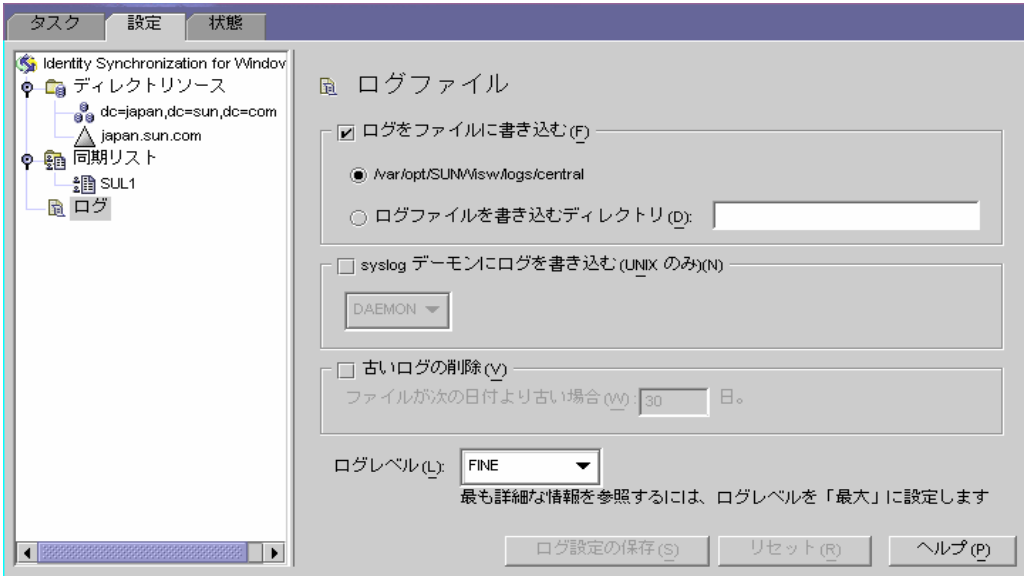
```
"Resetting Central Logger configuration ..."
"System manager is shutting down."
"Processing request (ID=<ID_number> from the console to stop
synchronization."
```

ログファイルの設定

配備のログの設定は、次のように Identity Synchronization for Windows コンソールで行います。

1. コンソールを開き、「設定」タブを選択します。
2. ナビゲーションツリーパネルでノードを展開し、「ログ」ノードを表示します。
3. 「ログ」ノードを選択すると、「設定」タブに「ログファイル」パネルが表示されます (図 10-2 を参照)。

図 10-2　　ログファイルの設定



4. 「ログファイル」パネルを使用して、ログファイルを次のように設定します。
   - **ログをファイルに書き込みます** : コアホスト上のファイルにログを書き込むときは、このオプションを有効にする

     このオプションを有効にすると、次の設定を行えるようになる

     - デフォルトのログディレクトリとログファイル (たとえば `/var/opt/SUNWisw/logs/central`) を有効にする
     - 「ログファイルをディレクトリに書き込みます」オプションを有効にし、ログファイルのパスとファイル名を指定する

注 コンソールは、指定されたログファイルの場所が実際に存在するかどうかを確認しません。指定されたログディレクトリが存在しない場合、セントラルロガーはこのディレクトリの作成を試みます。このため、存在しないログの場所を指定および保存してしまったかどうかは、ログを表示してみるまでわかりません。ログの表示を何度か試みると、指定された場所でコンソールがログを見つけられないことを示すメッセージが表示されます。

- **Solaris のみに適用 : syslog デーモンにログを書き込みます** : Identity Synchronization for Windows が Solaris プラットフォーム上に存在する場合は、このオプションを有効にする。ログの書き込みのカテゴリをドロップダウンリストから選択する。デフォルトはデーモン

注 このオプションを選択すると、Identity Synchronization for Windows はすべての情報を syslog に書き込みます。しかし、syslog は、デフォルトでは WARNING と SEVERE のメッセージだけを記録するように設定されています。

INFO メッセージも記録されるように syslog を設定するには、/etc/syslog.conf の次の行を編集します。

```
*.err;kern.debug;daemon.notice;mail.crit
/var/adm/messages
```

これを次のように変更します。

```
*.err;kern.debug;daemon.notice;daemon.info;mail.c
rit /var/adm/messages
```

この変更が完了したら、次の方法で syslog デーモンを開始し直す必要があります。

```
/etc/init.d/syslog stop ; /etc/init.d/syslog
start
```

FINE、FINER、FINEST の記録を有効にするには、セミコロン区切りのリストに deamon.debug を追加します。

- **古いログの削除** : ログファイルの数は、永続的に毎日増えつづける。このオプションを有効にすると、ディスクスペースが不足しないように、どの程度の時間が経過したら、プログラムが古いログをセントラルログファイルから削除できるかを指定できる

  たとえば、30 日と指定した場合、Identity Synchronization for Windows は作成から 31 日目に達しているすべてのファイルを削除できる

- **ログレベル** : システムログへの記録の詳細度をドロップダウンリストから選択する。270 ページの「ログレベル」を参照

5. 「ログ設定の保存」をクリックすると、選択したオプションに基づいてログファイルが作成されます。

ディレクトリソースの状態の表示

ディレクトリソースの状態を表示する手順は、次のとおりです。

1. Identity Synchronization for Windows コンソールで「状態」タブを選択します。
2. ナビゲーションツリーパネルでディレクトリソースの親ノードを展開し、ディレクトリソースのノード (dc=example,dc=com など) を選択します。

   「状態」タブの表示が更新され、選択したディレクトリソースに関する情報が表示されます (図 10-3 の例を参照)。

図 10-3　　ディレクトリソースの状態の表示

注　　ディレクトリソースの状態を表示した場合、主にそのディレクトリソースに関連するコネクタの状態が表示されます。

「状態」タブには、次の情報が表示されます。

- **更新** :「更新」をクリックすると、このタブに表示される情報が更新される
- **状態** : ディレクトリソースの現在の状態を示す有効な状態には、次の種類がある
  - UNINSTALLED: コネクタはインストールされていない

- INSTALLED: コネクタはインストールされているが、まだ実行時設定を受信していないため、同期の準備が整っていない。コネクタがこの状態で 1 分以上が経過した場合、何らかの異常が考えられる
- READY : コネクタは同期の準備が整っているが、現時点ではどのオブジェクトも同期させていない。同期が開始されていない、または同期が開始されていても一部のサブコンポーネントでコネクタとの接続が確立していない場合、コネクタの状態は READY のまま維持される
- SYNCING: コネクタはオブジェクトを同期させている。この状態になってもエラーが発生している可能性があるため、変更が同期されない場合はエラーログを確認する

- **アクティブ** : ディレクトリソースがアクティブであるか、ダウンしているかを示す
- **前回の通信** : ディレクトリソースのコネクタからの最後の応答時刻が示される

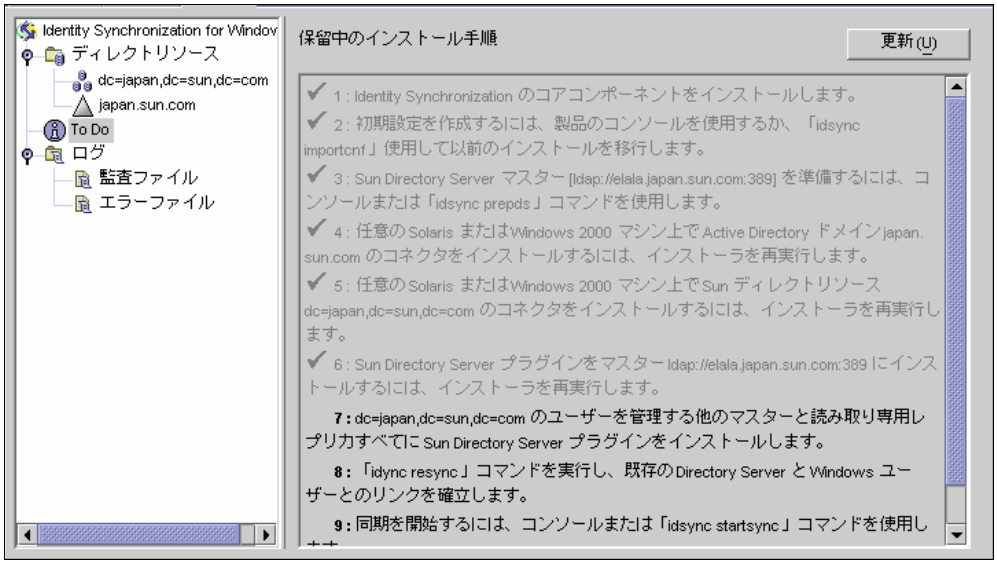
インストールと設定の状態の確認

Identity Synchronization for Windows のインストールと設定のプロセスで、実行が必要な手順を確認する方法は、次のとおりです。

1. Identity Synchronization for Windows コンソールで、「状態」タブを選択します。
2. ナビゲーションツリーパネルで「To Do」ノードを展開します。

   「状態」タブの表示が更新され、インストールと設定の手順チェックリストが表示されます (図 10-3 の例を参照)。

図 10-4　　表示、実行手順リスト



3. 右上の「更新」ボタンをクリックし、リストを更新します。

   完了した手順にはチェックマークが付けられ、グレイ表示されます。インストールと設定を完了するには、残りの手順を実行する必要があります。

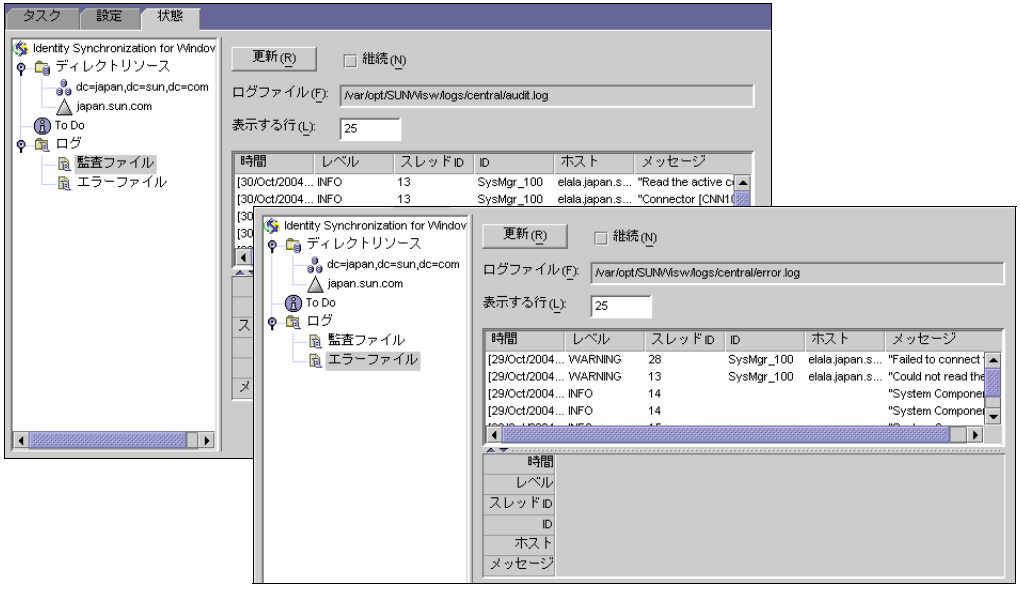
監査ログとエラーログの表示

エラーログを表示する手順は、次のとおりです。

1. Identity Synchronization for Windows コンソールで、「状態」タブを選択します。
2. ナビゲーションツリーパネルで、監査ファイルまたはエラーファイルのノードを展開します。

   「状態」タブの表示が更新され、現在のログの内容が表示されます (図 10-5 を参照)。

図 10-5　　ログの表示



「状態」タブには、次の情報が表示されます。

- **更新** : 監査またはエラーの最新情報を読み込む
- **継続** : 監査またはエラーの最新情報を継続的に更新、表示する
- **ログファイル** : 次のように、現在読み込んでいる監査またはエラーログの完全パス名を表示する

  `C:¥Program Files¥Sun¥MPS¥isw-`*<hostname>*`¥logs¥central¥audit.log`

- **表示する行** : 監査またはエラーの表示エントリ数を指定する。デフォルトは *25*

Windows NT マシンでの監査の有効化

配備に Windows NT マシンが含まれる場合、監査を有効にしない限り、Identity Synchronization for Windows はそのマシンからのメッセージをログに記録できません。

Windows NT マシンで監査ログの記録を有効にする手順は、次のとおりです。

1. Windows NT の「スタート」メニューから「プログラム」>「管理ツール」>「ドメインのユーザーマネージャ」を選択します。
2. 「ユーザーマネージャ」ダイアログボックスが表示されるので、メニューバーから「原則」>「監査」を選択します。

   「監査の原則」ダイアログボックスが表示されます。
3. 「監査するイベント」ボタンを有効にし、「成功」と「失敗」のボックスを有効にします。
4. 「OK」をクリックしてダイアログボックスを閉じます。

この設定は、設定し直すまで有効です。

第 11 章

セキュリティの設定

この章は、配備のセキュリティ設定に関する重要な情報を提供します。ここで説明する内容は、次のとおりです。

注 この章は、公開鍵暗号方式と SSL (Secure Sockets Layer) プロトコルの基本概念に習熟し、イントラネット、エクストラネット、インターネットのセキュリティの概念と、企業での電子証明書の役割を理解していることを前提に記述されています。これらの概念に初めて接する方は、『Managing Servers with iPlanet Console 5.0』でセキュリティに関連する付録を参照してください。

セキュリティの概要

パスワードは機密性のある情報です。Identity Synchronization for Windows は、同期させるディレクトリへのアクセスに使用する、ユーザーと管理者のパスワードクレデンシャルの安全性を確保するために、セキュリティ対策を講じています。

ここでは、セキュリティを保護するための次の方法について説明します。

- 281 ページの「設定パスワードの指定」
- 281 ページの「SSL の使用」
- 282 ページの「生成された 3DES キー」
- 282 ページの「SSL と 3DES キーによる保護の概要」
- 284 ページの「Message Queue のアクセス制御」
- 285 ページの「ディレクトリのクレデンシャル」
- 285 ページの「持続ストレージの保護の概要」

このセキュリティ保護は、次のような事態が生じることを回避することを目的としています。

- 盗聴者がネットワーク経由でクリアテキスト形式のパスワードを傍受する
- アタッカーがコネクタを操作してユーザーのパスワードを任意の値に変更し、クリアテキスト形式のユーザーパスワードが傍受された場合と同様の結果を招く
- アタッカーが、特別な権限を持つ Identity Synchronization for Windows コンポーネントへのアクセス権を得る
- 特別な権限を持たないユーザーが、ディスクに格納されているファイルからパスワードを復元する
- 侵入者が、システム内のいずれかのコンポーネントから削除されたハードディスクからパスワードを復元する。これは、同期対象のパスワードである場合も、ディレクトリへのアクセスに使用されるシステムパスワードである場合もある

設定パスワードの指定

製品の設定ディレクトリに格納され、ネットワークを介して転送される機密情報を保護するために、Identity Synchronization for Windows は設定パスワードを使用します。管理者はコアのインストール時に設定パスワードを指定します。コンソールを開いたり、Identity Synchronization for Windows のインストールプログラムを実行したりするときは、そのたびにこのパスワードを指定する必要があります。

注

システムマネージャは、コネクタに渡す前に設定パスワードにアクセスする必要があります。このため、システムマネージャはその初期化ファイルにこのパスワードを記録します。

ファイルシステムのアクセス制御により、権限を持たないユーザーはシステムマネージャの初期化ファイルにアクセスできません。Identity Synchronization for Windows のインストールプログラムは、このパスワードにパスワードポリシーを適用しません。

設定パスワードを選ぶときに、パスワードのセキュリティを向上させる方法については、287 ページの「セキュリティの強化」を参照してください。

SSL の使用

コンポーネントが LDAP を使用するすべての機会で SSL を介した LDAP を使用するように Identity Synchronization for Windows を設定することができます。Message Queue へのすべてのアクセスは、SSL で保護されます。

Directory Server から Active Directory への同期では、Active Directory コネクタと Active Directory の間で SSL を使用する必要があります。

信頼された SSL 証明書の要求

デフォルトでは、SSL を使用するように設定されたコネクタは、サーバー (Directory Server または Active Directory) から返されるすべての SSL 証明書を受け付けます。しかし、これには信頼されない証明書や、有効期限切れ、または無効な証明書も含まれます。コネクタとサーバーの間のすべてのネットワークトラフィックは暗号化されますが、あるサーバーが本物の Active Directory や Directory Server に成りすましている場合、コネクタはその成りすましを検出できません。

コネクタが信頼された証明書だけを受け付けるように強制するには、コンソールで「Directory Server の設定」ウィザードを開き、「拡張セキュリティオプションの指定」パネルで「信頼できる SSL の証明書を要求」オプションを有効にする必要があります (122 ページを参照)。このオプションを有効にしたら、`idsync certinfo` によって表示される適切な CA 証明書をコネクタの証明書データベースに追加する必要があります。

生成された 3DES キー

製品の設定ディレクトリ内のすべての機密情報の保護には、設定パスワードから生成される 3DES キーが使用されます。ログメッセージを除き、Message Queue に送信されるすべてのメッセージは、トピックごとに切り替わる 3DES キーで暗号化されます。コネクタとサブコンポーネントの間で送信されるメッセージは、セッションごとに切り替わる 3DES キーによって暗号化されます。Directory Server プラグインは、ユーザーパスワードのすべての変更を 3DES キーで暗号化します。

SSL と 3DES キーによる保護の概要

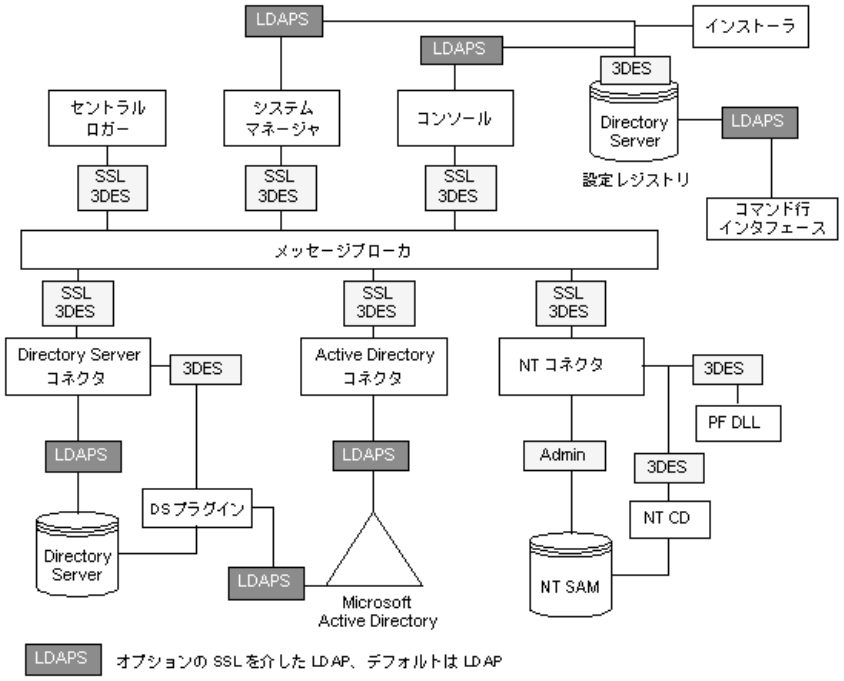
表 11-1 は、ネットワーク上で送信される機密情報を Identity Synchronization for Windows がどのように保護するかを示しています。

表 11-1 ネットワークセキュリティによる機密情報の保護

保護の方法	保護の対象となる通信経路
SSL を介した LDAP (オプション)	• Directory Server コネクタと、Directory Server、Active Directory コネクタ、Active Directory の間 • Directory Server プラグインと Active Directory の間 • コマンド行インタフェースと製品の設定ディレクトリの間 • コンソールと製品の設定ディレクトリの間 • コンソールと Active Directory のグローバルカタログの間 • コンソールと、同期対象の Active Directory ドメインまたは Directory Server の間 • Message Queue ブローカと製品の設定ディレクトリの間 • コネクタ、システムマネージャ、セントラルロガー、コマンド行インタフェース、コンソールは、LDAPS を介して Message Queue を認証できる • インストーラと設定 Directory Server の間 • インストーラと Active Directory の間 • インストーラと同期対象 Directory Server の間
3DES キーによる暗号化 (デフォルト)	• Directory Server コネクタと Directory Server プラグイン (全データ) • Windows NT コネクタ、Windows NT パスワードフィルタ DLL、Windows NT 変更ディテクタ (全データ) • 製品の設定ディレクトリ内のすべての機密情報 • コネクタとサブコンポーネントの間で送信されるすべてのメッセージ (セッションごとに切り替わる 3DES キーによって暗号化される) • Message Queue を介して送信されるログ以外のすべてのメッセージ

図 11-1 は、ここで説明したセキュリティ機能の概要を示しています。

図 11-1 Identity Synchronization for Windows のセキュリティの概要



Message Queue のアクセス制御

Identity Synchronization for Windows は、各コネクタが受信メッセージを信頼できるように、Message Queue のアクセス制御を使用して、メッセージの登録と公開に対する未認証アクセスを防止しています。

Message Queue ブローカへのアクセス時は、Message Queue とコネクタだけが認識している一意のユーザー名とパスワードが指定されます。Message Queue に送信される各メッセージは、トピックごとに切り替わる 3DES キーで暗号化されるため、メッセージの内容は保護され、トピックキーを知らない部外者が意味のあるメッセージを送信することを防止できます。これらの対策により、アタッカーが偽のパスワード同期メッセージをコネクタに送ったり、コネクタに成りすまして実際のパスワード更新を受信したりすることが防止されます。

注 デフォルトでは、コネクタやシステムマネージャなど、Message Queue のクライアントは、Message Queue ブローカから返されるすべての SSL 証明書を受け付けます。Message Queue 証明書の検証と、Message Queue に関連するセキュリティ上の問題については、287 ページの「セキュリティの強化」を参照してください。

ディレクトリのクレデンシャル

同期対象の Active Directory と Directory Server でパスワードを変更する場合、コネクタは、特別な権限を持つクレデンシャルを要求します。特別な権限を持つこれらのクレデンシャルは、製品の設定ディレクトリへの格納前に暗号化されます。

持続ストレージの保護の概要

表 11-2 は、ディスクに格納される機密情報を Identity Synchronization for Windows がどのように保護するかを示しています。

表 11-2 持続ストレージの保護

持続ストレージ	機密情報	保護
設定 Directory Server に格納される製品の設定情報	製品の設定ディレクトリには、ディレクトリにアクセスするためのクレデンシャルと、Message Queue トピックごとの 3 DES キーが格納される	製品の設定ディレクトリに格納されるすべての機密情報は、設定パスワードから生成される 3DES キーを使用して暗号化される。製品の設定ディレクトリをさらに保護するための推奨事項については、「セキュリティの強化」を参照
Directory Server の旧バージョン形式の更新履歴ログ	Directory Server プラグインは、パスワードの変更を取り込み、Directory Server の旧バージョン形式の更新履歴ログに書き込む前にそれを暗号化する	Directory Server プラグインは、各配備で一意の 3DES キーを使用して、変更されたすべてのユーザーパスワードを暗号化する
Message Queue ブローカの持続ストレージ	Message Queue ブローカは、すべてのコネクタ間で送受信されるパスワード同期メッセージを格納する	ログメッセージを除き、すべての持続メッセージは、トピックごとの 3DES キーで暗号化される
Message Queue ブローカのディレクトリクレデンシャル	Message Queue ブローカは製品の設定ディレクトリに対してユーザーを認証する。設定ディレクトリへの接続には、コアのインストール時に設定されたディレクトリ管理ユーザーの名前とパスワードが使用される	ディレクトリパスワードは、ファイルシステムのアクセス制御によって保護されたパスファイルに格納される

表 11-2　持続ストレージの保護 (続き)

持続ストレージ	機密情報	保護
システムマネージャの起動ファイル	システムマネージャの起動ファイルには、設定情報へのアクセスに必要な情報が記録されている。これには、設定パスワードと、コアのインストール時に設定されたディレクトリ管理ユーザーの名前とパスワードが含まれる	このファイルは、ファイルシステムのアクセス制御によって保護される
コネクタとセントラルロガーの起動ファイル	各コネクタとセントラルロガーには、Message Queue へのアクセスに必要なクレデンシャルを記録した初期設定ファイルがある	これらのファイルは、ファイルシステムのアクセス制御によって保護される
Directory Server プラグインの起動設定	cn=config に格納されるプラグインの設定には、コネクタへの接続に必要なクレデンシャルが記録されている	cn=config サブツリーは、ACI によって保護され、このツリーのミラーである `dse.ldif` ファイルは、ファイルシステムのアクセス制御によって保護される
NT パスワードフィルタ DLL と NT 変更ディテクタの起動設定	Windows レジストリに格納される NT サブコンポーネントの設定には、コネクタへの接続に必要なクレデンシャルが記録されている	PDC レジストリへのアクセスがセキュリティ保護されていない場合は、アクセス制御によってこれらのレジストリキーを保護できる
Windows コネクタのオブジェクトキャッシュ	Windows コネクタは、ハッシュ化されたユーザーパスワードをコネクタのオブジェクトキャッシュに格納する	パスワードはクリアテキスト形式ではなく、MD5 ハッシュで暗号化された形式で格納される。これらのデータベースファイルは、ファイルシステムのアクセス制御によって保護される (「セキュリティの強化」を参照)

セキュリティの強化

ここでは、製品の現行リリースに潜在的に存在するセキュリティ上の弱点について説明し、製品のデフォルト設定以外でセキュリティを拡張、強化する方法について推奨事項を示します。ここで説明する内容は、次のとおりです。

設定パスワード

機密性のある設定情報の保護には設定パスワードが使用されますが、インストールプログラムはこのパスワードにパスワードポリシーを適用しません。このパスワードを設定するときは、厳密なガイドラインに従って容易に想像できない複雑なパスワードを選択し、強力なパスワードを作成するための標準的なポリシーガイドラインに準拠していることを確認してください。

たとえば、大文字、小文字、英数字以外の文字を含む、8 文字以上の長さのパスワードを作成します。名前、イニシャル、日付などを含めないようにしてください。

設定ディレクトリのクレデンシャルの作成

製品の設定ディレクトリが存在する Directory Server にアクセスするには、その管理者のクレデンシャルが設定管理者グループに含まれている必要があります。しかし、何らかの理由で *admin* 以外のクレデンシャルを作成する必要がある場合は、次の方法で対応してください。

インストールプログラムは、コンソールの管理サブツリーに格納されているユーザーのクレデンシャルを要求します。しかし、コアのインストールプログラムは、*admin* 以外のユーザーを `uid=admin,ou=Administrators, ou=TopologyManagement, o=NetscapeRoot` に拡張しません。このため、コアのインストール時は、DN 全体を指定する必要があります。

admin 以外の新規ユーザーを作成する手順は、次のとおりです。

1. 次の DN でユーザーを作成します。

   ```
   ou=Administrators, ou=TopologyManagement, o=NetscapeRoot
   ```

2. 設定管理者のグループに新しいクレデンシャルを追加します。
3. このユーザーと、設定管理者グループのすべてのユーザーだけが、製品の設定ディレクトリが格納された Directory Server にアクセスできるように、ACI を設定します。
4. コアのインストール時は、DN 全体を指定します。

   Directory Server でのアクセス制御の管理については、『Sun Java System Directory Server 5 2005Q1 管理ガイド』の第 6 章「アクセス制御の管理」を参照してください。

Message Queue クライアントによる証明書の検証

デフォルトでは、コネクタやシステムマネージャなど、Message Queue のクライアントは、Message Queue ブローカから返されるすべての SSL 証明書を受け付けます。

1. この設定を無効にし、Messege Queue クライアントが Message Queue ブローカの証明書を検証するように設定するには、次のファイルを編集します。

   <*installation_root*>/resources/WatchList.properties

2. `Watchlist.properties` ファイルの各プロセスの JVM 引数に次の設定を追加します。

   ```
   -Djavax.net.ssl.trustStore=<keystore_path>
   -DimqSSLIsHostTrusted=false
   ```

3. Identity Synchronization for Windows デーモンまたはサービスを開始し直します。

`javax.net.ssl.trustStore` プロパティは、ブローカ証明書を信頼する JSEE キーストアをポイントする必要があります。たとえば、コアがインストールされているマシンでは、ブローカも `/etc/imq/keystore` を使用しているので、このキーストアを使用できます。

Message Queue の自己署名 SSL 証明書

デフォルトでは、Message Queue ブローカは自己署名 SSL 証明書を使用します。別の証明書をインストールするには、Java に付属する `keytool` ユーティリティを使用して、ブローカのキーストア (Solaris 環境では `/var/imq/instances/isw-broker/etc/keystore`、Windows 2000 環境では `<`*mq_installation_root*`>/var/instances/isw-broker/etc/keystore`) を修正します。証明書のエイリアスは、`imq` である必要があります。

Message Queue ブローカへのアクセス

デフォルトでは、Message Queue はポートマッパ以外のすべてのサービスに動的なポートを使用します。ファイアウォールを通過してブローカにアクセスしたり、ブローカに接続できるホストを制限したりする場合は、ブローカがすべてのサービスに固定ポートを使用するように設定する必要があります。

このように設定するには、ブローカ設定プロパティの `imq.<`*service_name*`>.<`*protocol_type*`>.port` を設定します。詳細については、『Sun Java System Message Queue 3.5 SP1 管理ガイド』を参照してください。

ディレクトリ証明書の検証の設定

製品の設定ディレクトリに SSL 経由でアクセスする場合、システムマネージャはすべての証明書を受け付け、Message Queue ブローカもすべての証明書を受け付けます。現時点では、製品の設定ディレクトリの SSL 証明書をシステムマネージャまたは Message Queue ブローカに検証させる方法はありません。

設定ディレクトリへのアクセスの制限

コアのインストール時に、製品の設定ディレクトリが格納される Directory Server に追加される情報には、アクセス制御に関する情報が含まれません。次の ACI を使用することで、アクセス可能なユーザーを設定管理者だけに制限できます。

```
(targetattr = "*") (target =
"ldap:///ou=IdentitySynchronization,ou=Services,dc=example,dc=com")
(version 3.0;acl "Test";deny (all)(groupdn !=
"ldap:///cn=Configuration Administrators, ou=Groups,
ou=TopologyManagement, o=NetscapeRoot");)
```

Directory Server でのアクセス制御の管理については、『Sun Java System Directory Server 5 2005Q1 管理ガイド』の第 6 章「アクセス制御の管理」を参照してください。

レプリケートされた構成のセキュリティ保護

レプリケーションを使用する Directory Server に接続する配備には、「セキュリティの概要」で説明した規則がそのまま適用されます。ここでは、レプリケートされた構成の例を示し、その構成で SSL の使用を有効化する方法について説明します。

注	レプリケートされた設定の計画、配備、セキュリティ保護の概要については、付録 E 「レプリケーション環境でのインストールに関する注意」を参照してください。

表 11-3 は、CA 証明書を必要とする構成コンポーネントと、必要となる証明書の種類を示しています。

表 11-3　CA 証明書を必要とする MMR 構成コンポーネント

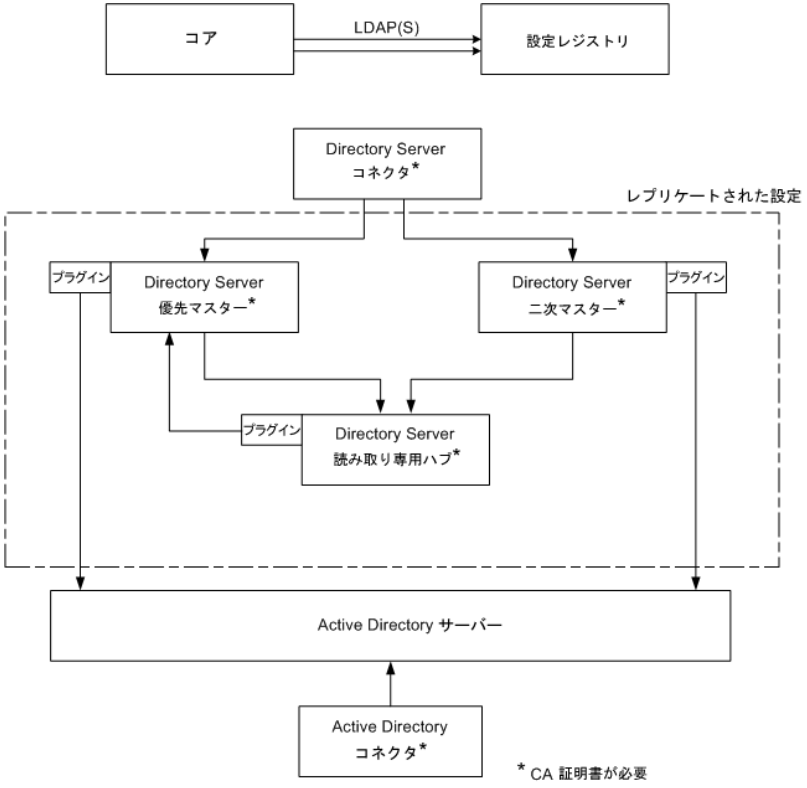
コンポーネント	必要な CA 証明書
優先 Directory Server のレプリケートされたマスター	Active Directory システム
二次 Directory Server のレプリケートされたマスター	Active Directory システム
読み取り専用の Directory Server ハブ	優先 Directory Server のレプリケートされたマスター 二次 Directory Server のレプリケートされたマスター

表 11-3　CA 証明書を必要とする MMR 構成コンポーネント (続き)

コンポーネント	必要な CA 証明書
Directory Server コネクタ	優先 Directory Server のレプリケートされたマスター 二次 Directory Server のレプリケートされたマスター
Active Directory コネクタ	Active Directory システム

図 11-2 は、MMR 構成の配備にインストールされた Identity Synchronization for Windows を示しています。この配備には、レプリケートされた 2 つの Directory Server マスターと、読み取り専用ハブまたはコンシューマの複数の Directory Server が含まれます。各 Directory Server にはプラグインがあり、Directory Server コネクタ、Active Directory システム、Active Directory コネクタは、それぞれ 1 つだけです。

図 11-2　レプリケートされた構成



注 Directory Server ソースに SSL を設定するときは、レプリカ Directory Server が、優先、二次の両方の Directory Server 証明書を信頼するように設定する必要があります。これは、システムにインストールされている、ハブまたは読み取り専用レプリカ以外の Directory Server のすべてのプラグインにも該当します。

Directory Server プラグインは、関連する Directory Server と同じ CA 証明書にアクセスできます。

idsync certinfo の使用

Identity Synchronization for Windows の現在の SSL 設定で必要となる証明書を調べるには、`idsync certinfo` ユーティリティを使用します。`idsync certinfo` を実行することで、各証明書データベースで必要とされる証明書に関する情報を取得できます。

注 SSL を使用するように Directory Server ソースを設定するときは、すべての Directory Server サブコンポーネントまたはプラグインのレプリカ Directory Server が、優先および二次 Directory Server ソース証明書を信頼することを確認する必要があります。

すべての証明書を信頼する設定を有効にした状態で、Identity Synchronization for Windows が SSL 接続の確立を試みたときに、サーバーのホスト名と、SSL ネゴシエーションの段階でサーバーから提示される証明書に記録されているホスト名が一致しない場合、Identity Synchronization for Windows コネクタは接続の確立を拒否します。

Identity Synchronization for Windows に設定するディレクトリソースのホスト名は、そのディレクトリソースが使用する証明書に埋め込まれたホスト名と常に一致する必要があります。

引数

表 11-4 は、`idsync certinfo` サブコマンドに指定できる引数を説明しています。

表 11-4 certinfo の引数

引数	説明
`-h` <*CR-hostname*>	設定ディレクトリのホスト名を指定する。この引数のデフォルト値は、コアのインストール時に指定された値である
`-p` <*CR-port-no*>	設定ディレクトリの LDAP ポート番号を指定する。デフォルトは *389*

表 11-4 certinfo の引数 (続き)

引数	説明
-D <*bind-DN*>	設定ディレクトリのバインド識別名 (DN) を指定する。この引数のデフォルト値は、コアのインストール時に指定された値である
-w <*bind-password* | ->	設定ディレクトリのバインドパスワードを指定する 値として - を指定した場合、パスワードは標準入力 (STDIN) から読み取られる
-s <*rootsuffix*>	設定ディレクトリのルートサフィックスを指定する。ルートサフィックスは、dc=example,dc=com などの識別名である この引数のデフォルト値は、コアのインストール時に指定された値である
-q <*configuration_password*>	設定パスワードを指定する。値として - を指定した場合、パスワードは標準入力 (STDIN) から読み取られる

使用方法

次に、idsync certinfo を使用して、SSL 通信を行うように指定されているシステムコンポーネントを検索する例を示します。この実行例の結果では、2 つのコネクタ (CNN101 と CNN100) が識別され、適切な CA 証明書をどこにインポートするべきかが示されます。

```
:¥Program Files¥Sun¥MPS¥isw-hostname¥bin> idsync certinfo -h
CR-hostname
-p 389 -D "cn=Directory Manager" -w dirmanager -s
dc=example,dc=com
-q <password>
Connector: CNN101
Certificate Database Location: C:¥Program
Files¥Sun¥MPS¥isw-hostname¥etc¥CNN101
Get 'Active Directory CA' certificate from Active Directory and
import into Active Directory Connector certificate db for server
ldaps::/hostname.example.com:636
Connector: CNN100
Certificate Database Location:   C:¥Program
Files¥Sun¥MPS¥isw-hostname¥etc¥CNN100
Export 'Directory Server CA' certificate from Directory Server
certificate db and import into Directory Server Connector
certificate db ldaps://hostname.example.com:636
Export 'Active Directory CA' certificate from Active Directory
Server hostname.example.sun.com:389 and import into Directory
Server Server certificate db for server
ldaps://hostname.example.com:638
SUCCESS
```

Directory Server での SSL の有効化

Directory Server で自己署名証明書を使用して SSL を有効にする手順は、次のとおりです。

注 ここでは、手順の概略を示します。詳細については、『Sun Java System Directory Server 5 2005Q1 管理ガイド』を参照してください。

注

- Windows 環境では、Directory Server 5 2004Q2 以降に付属するバージョンの `certutil` を使用する
  5 2004Q2 より前のバージョンの Directory Server に付属する `certutil` は使用できない。これより前のバージョンの `certutil` には、Identity Synchronization for Windows との互換性がない
- Solaris 環境では、`certutil` はデフォルトで `/usr/sfw/bin` にインストールされている

1. 次のように入力し、Directory Server のキー証明書データベースを新規作成します。

```
C:¥Program Files¥Sun¥MPS¥shared¥bin¥certutil.exe -d . -P
slapd-hostname-

In order to finish creating your database, you
must enter a password which will be used to
encrypt this key and any future keys.
The password must be at least 8 characters long,
and must contain at least one non-alphabetic character.
Enter new password:
Re-enter password:
```

注 これらの例は、サーバールートの直下にある alias ディレクトリで実行されます。他のディレクトリで実行した場合、Directory Server は証明書データベースを見つけることができません。

2. Directory Server が使用するサーバー証明書となる自己署名証明書を生成します。Directory Server が稼動しているサーバーのホスト名に従って DN を決定してください。

注 自己署名証明書のデフォルトの有効期限は 3 か月です。この期間を調整するには、`-v <months-valid>` オプションを使用します。たとえば、期間を 24 か月に延長するときは **`-v 21`** と指定し、1 か月に短縮するときは **`-v -2`** と指定します。

```
C:¥Program Files¥Sun¥MPS¥shared¥bin¥certutil.exe -d . -P
slapd-hostname- -S -n server-cert -s
"cn=hostname.example.com,c=us" -x -t CTu,,
A random seed must be generated that will be used in the
creation of your key.  One of the easiest ways to create a
random seed is to use the timing of keystrokes on a keyboard.
To begin, type keys on the keyboard until this progress meter
is full.  DO NOT USE THE AUTOREPEAT FUNCTION ON YOUR KEYBOARD!
Continue typing until the progress meter is full:
|************************************************************|
Finished.  Press enter to continue:
Enter Password or Pin for "NSS Certificate DB":
Generating key.  This may take a few moments...
```

3. 確認のために証明書を表示します。

```
C:¥Program Files¥Sun¥MPS¥shared¥bin¥certutil.exe -L -d . -P
slapd-hostname-
Certificate Name           Trust Attributes
server-cert                CTu,,
p    Valid peer
P    Trusted peer (implies p)
c    Valid CA
T    Trusted CA to issue client certs (implies c)
C    Trusted CA to certs(only server certs for ssl) (implies c)
u    User cert
w    Send warning
```

4. Directory Server の再起動のたびに証明書データベースパスワードを指定する必要がなくなるように、PIN ファイルを作成します。

   ```
   C:¥Program Files¥Sun¥MPS¥alias > echo Internal (Software)
   Token:<secret12> slapd-hostname-pin.txt
   ```

5. 次のように、Directory Server で SSL を有効化します。

   a. コンソールを開きます。

   b. 「設定」タブを選択します。

   c. 右側のパネルで「暗号化」タブを選択します。

d. 「このサーバーの SSL を有効にする」にチェックマークを付けます。

e. 「この暗号化方式ファミリを使用 : RSA」にチェックマークを付けます。

f. 「保存」をクリックし、「了解」を 2 回クリックします。

g. 「ネットワーク」タブを選択します。

h. 「セキュアポート」フィールドを更新します。Active Directory と同じマシンで実行している場合、ポートを 636 から未使用ポートに変更しないかぎり、Directory Server を起動できません。

i. 「保存」、「はい」、「了解」を順にクリックします。

j. 上部にある「タスク」タブを選択します。

k. 「Directory Server を再起動します」をクリックし、「はい」をクリックします。

Directory Server 証明書データベースからの CA 証明書の取得

Directory Server で SSL が有効化されていることを確認します。Directory Server コネクタの証明書データベースにインポートできるように、Directory Server 証明書を一時ファイルとしてエクスポートするには、次のコマンドを実行します。

```
C:¥Program Files¥Sun¥MPS¥shared¥bin¥certutil.exe -L -d . -P
slapd-hostname- -n server-cert -a > C:¥s-cert.txt
```

これらの例は、サーバールートの直下にある `alias` ディレクトリで実行されます。他のディレクトリで実行した場合、Directory Server は証明書データベースを見つけることができません。

Active Directory コネクタでの SSL の有効化

Identity Synchronization for Windows は Active Directory の SSL 証明書を SSL 通信経由で自動的に取得し、コネクタに指定したクレデンシャルと同じ情報を使用して、それをコネクタの証明書データベースにインポートします。

しかし、クレデンシャルが無効であったり、SSL 証明書が見つからなかったなどの理由でエラーが発生することもあります。このような場合は、Active Directory の CA 証明書を取得し、それをコネクタの証明書データベースに追加します。次に、この方法について説明します。

- 298 ページの「Active Directory 証明書の取得」
- 301 ページの「コネクタの証明書データベースへの Active Directory 証明書の追加」

Active Directory 証明書の取得

エラーが発生したときは、Windows 2000/2003 に付属する `certutil` プログラム、または LDAP を使用して Active Directory の証明書を取得します。次の各項では、その手順について説明します。

注	ここで説明する `certutil` ユーティリティは、このマニュアルですでに説明された Directory Server に付属する `certutil` ユーティリティとは異なります。

Windows の certutil の使用

`certutil` プログラムを使用して Active Directory 証明書を取得する手順は、次のとおりです。

1. Active Directory が稼動するマシンで次のコマンドを実行し、証明書をエクスポートします。

   ```
   C:¥>certutil -ca.cert cacert.bin
   ```

2. 生成される `cacert.bin` ファイルは、証明書データベースにインポートできます。

LDAP の使用

LDAP を使用して Active Directory 証明書を取得する手順は、次のとおりです。

1. Active Directory に対して次の検索を実行します。

```
ldapsearch -h <CR-hostname> -D <administrator_DN> -w
<administrator_password> -b
"cn=configuration,dc=put,dc=your,dc=domain,dc=here"
"cacertificate=*"
```

この *<administrator_DN>* には、次のような DN が指定されます。

```
cn=administrator,cn=users,dc=put,dc=your,dc=domain,dc=here
```

この例では、ドメイン名は *<put.your.domain.name.here>* です。

いくつかのエントリが検索フィルタと一致します。通常は、DN に `cn=Certification Authorities, cn=Public Key Services` が含まれるエントリが必要となります。

2. テキストエディタを開き、最初の CA 証明書属性の最初の値を切り取ります。これは、base64 でエンコードされたテキストブロックです。切り取ったテキストブロックをテキストエディタに貼り付けます (値のみ)。どの行の先頭も空白文字とならないように、内容を編集します。
3. 最初の行の前に `-----BEGIN CERTIFICATE-----`、最後の行の後に `-----END CERTIFICATE-----` を追加します。次の例を参照してください。

```
-----BEGIN CERTIFICATE-----

MIIDvjCCA2igAwIBAgIQDgoyk+Tu14NGoQnxhmNHLjANBgkqhkiG9w0BAQUFA
DCBjjEeMBwGCSqGSIb3DQEJARYPYmVydG9sZEBzdW4uY29tMQswCQYDVQQGEw
JVUzELMAkGA1UECBMCVFgxDzANBgNVBAcTBkF1c3RpbjEZMBcGA1UEChMQU3V
uIE1pY3Jvc3lzdGVtczEQMA4GA1UECxMHaVBsYW5ldDEUMBIGA1UEAxMLUmVz
dGF1cmFudHMwHhcNMDIwMTExMDA1NDA5WhcNMTIwMTExMDA1OTQ2WjCBjjEeM
BwGCSqGSIb3DQEJARYPYmVydG9sZEBzdW4uY29tMQswCQYDVQQGEwJVUELMAk
GA1UECBMCVFgxDzANBgNVBAcTBkF1c3RpbjEZMBcGA1UEChMQU3VuIE1pY3Jv
c3lzdGVtczEQMA4GA1UECxMHaVBsYW5ldDEUMBIGA1UEAxMLUmVzdGF1cmFud
HMwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAyekZa8gwwhw3rLK3eV/12St1DV
Usg31LOu3CnB8cMHQZXlgiUgtQ0hm2kpZ4nEhwCAHhFLD3iIhIP4BGWQFjcwI
DAQABo4IBnjCCAZowEwYJKwYBBAGCNxQCBAYeBABDAEEwCwYDVR0PBAQDAgFG
MA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFJ5Bgt6Oypq7T8Oykw4LH6ws2
d/IMIIBMgYDVR0fBIIBKTCCASUwgdOggdCggc2GgcpsZGFwOi8vL0NOPVJlc3
RhdXJhbnRzLENOPWRvd2l0Y2hlcixDTj1DRFAsQ049UHVibGljJTIwS2V5JTI
wU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlvbixEQz1yZXN0
YXVyYW50cyxEQz1jZW50cmFsLERDPXN1bixEQz1jb20/Y2VydGlmaWNhdGVSZ
XZvY2F0aW9uTGlzdD9iYXNlP29iamVjdGNsYXNzPWNSTERpc3RyaWJ1dGlvbl
BvaW50ME2gS6BJhkdodHRwOi8vZG93aXRjaGVyLnJlc3RhdXJhbnRzLmNlbnR
yYWwuc3VuLmNvbS9DZXJ0RW5yb2xsL1Jlc3RhdXJhbnRzLmNybDAQBgkrBgEE
AYI3FQEEAwIBADANBgkqhkiG9w0BAQUFAANBAL5R9R+ONDdVHWu/5Sd9Tn9dp
xN8oegjS88ztv1HD6XSTDzGTuaaVebSZV3I+ghSInsgQbH0gW4fGRwaI
BvePI4=

-----END CERTIFICATE-----
```

4. 証明書をファイルとして (たとえば `ad-cert.txt` など) 保存します。
5. このファイル (この例では `ad-cert.txt`) を証明書データベースにインポートできます。方法については、次の節「コネクタの証明書データベースへの Active Directory 証明書の追加」を参照してください。

コネクタの証明書データベースへの Active Directory 証明書の追加

この手順は、Active Directory コネクタのインストール後にコネクタによる SSL の使用を有効にした、またはインストール時に無効なクレデンシャルを指定した場合にだけ実行してください。

1. Active Directory コネクタがインストールされているマシンで、Identity Synchronization for Windows サービス / デーモンを停止します。
2. 次のいずれかの方法で Active Directory の CA 証明書を取得します。
   - 298 ページの「Windows の certutil の使用」
   - 298 ページの「LDAP の使用」
3. ここでは、Active Directory コネクタのコネクタ ID が CNN101 であると仮定します (コネクタ ID と管理対象ディレクトリソースのマッピングについては、`logs/central/error.log` ファイルを参照)。証明書データベースがインストールされているマシンで証明書データベースのディレクトリに移動し、証明書ファイルをインポートします。
   - `certutil` を使用して証明書を取得した場合は、次のように入力する

     ```
     C:¥¥Program Files¥Sun¥MPS¥shared¥bin¥certutil.exe -A -d . -n
     ad-ca-cert -t C,, -i ¥cacert.bin
     ```

   - LDAP を使用して証明書を取得した場合は、次のように入力する

     ```
     C:¥¥Program Files¥Sun¥MPS¥shared¥bin¥certutil.exe -A -d . -n
     ad-ca-cert -t C,, -a -i ¥ad-cert.txt
     ```
4. Identity Synchronization for Windows サービス / デーモンを開始し直します。

注

Directory Server の `certutil.exe` は、Directory Server 5 2005Q1 のインストール時に自動的にインストールされます。このため、Directory Server がインストールされていないマシンにインストールされたコネクタに CA 証明書を追加することはできません。

少なくとも、Active Directory コネクタがインストールされているサーバーに、Directory Server 5 2005Q1 パッケージから Sun Java System Server Basic Libraries と Sun Java System Server Basic System Libraries をインストールする必要があります。ただし、管理サーバーや Directory Server のコンポーネントをインストールする必要はありません。

また、アンインストール可能になるように、コンソールで JRE サブコンポーネントを選択します。

Directory Server への Active Directory 証明書の追加

Directory Server 証明書データベースに Active Directory CA 証明書を追加する手順は、次のとおりです。

注	Directory Server で SSL が有効化されていることを確認します。

1. 次のいずれかの方法で Active Directory の CA 証明書を取得します。
   - 298 ページの「Windows の certutil の使用」
   - 298 ページの「LDAP の使用」
2. Directory Server を停止します。
3. Directory Server がインストールされているマシンで、次のように Active Directory CA 証明書をインポートします。
   - `certutil` を使用して証明書を取得した場合は、次のように入力する

     ```
     C:¥¥Program Files¥Sun¥MPS¥shared¥bin¥certutil.exe -A -d . -P
     slapd-hostname- -n ad-ca-cert -t C,, -i ¥cacert.bin
     ```

   - LDAP を使用して証明書を取得した場合は、次のように入力する

     ```
     C:¥¥Program Files¥Sun¥MPS¥shared¥bin¥certutil.exe -A -d . -P
     slapd-hostname- -n ad-ca-cert -t C,, -a -i ¥ad-cert.txt
     ```

4. Directory Server を起動します。

Directory Server コネクタへの Directory Server 証明書の追加

Directory Server プラグインと Active Directory の間で SSL 通信を有効にした場合は、各 Directory Server マスターの証明書データベースに Active Directory の CA 証明書を追加する必要があります。手順は次のとおりです。

1. Directory Server コネクタがインストールされているマシンで、Identity Synchronization for Windows サービス / デーモンを停止します。
2. Directory Server CA 証明書を取得します。
3. ここでは、Directory Server コネクタのコネクタ ID が CNN100 であると仮定します (コネクタ ID と管理対象ディレクトリソースのマッピングについては、`logs/example/error.log` ファイルを参照)。証明書データベースがインストールされているマシンで証明書データベースのディレクトリに移動し、`cacert.bin` ファイルをインポートします。

```
C:¥Program Files¥Sun¥MPS¥shared¥bin¥certutil.exe -A -d . -n
ds-cert -t C,, -i C:¥s-cert.txt
```

注 ASCII 形式の証明書を取得した場合は、`certutil` コマンドに引数「`-a`」を指定し、ファイルがバイナリ形式ではなく、ASCII 形式であることを示します。

4. Identity Synchronization for Windows サービス / デーモンを開始し直します。

第 2 部

付録

Identity Synchronization for Windows のコマンド行ユーティリティの使用

Identity Synchronization for Windows では、さまざまなタスクをコマンド行から実行できます。この付録では、Identity Synchronization for Windows のコマンド行ユーティリティを使用して各種タスクを実行する方法について説明します。この章で説明する内容は次のとおりです。

共通機能

Identity Synchronization for Windows の各コマンド行ユーティリティは、次の機能を共有しています。

共通引数

ここでは、ほとんどのコマンド行ユーティリティに共通する引数 (オプション) について説明します。次の表に、引数の情報をまとめて示します。

- 表 A-1 「すべてのサブコマンドに共通する引数」は、*prepds* を除く idsync のすべてのサブコマンドと移行ツールに共通する、次の引数について説明している

```
-D <bind-DN> -w <bind-password | -> [-h <Configuration Directory-hostname>]
[-p <Configuration Directory-port-no>] [-s <rootsuffix>] [-Z] [-P
<cert-db-path>]
[-m <secmod-db-path>]
```

注

角括弧 ([ ]) は、省略可能な引数を示します。

Identity Synchronization for Windows のインストールプログラムは、インストール時に指定された情報に基づいて、-h、-p、-D、-s の各引数に自動的にデフォルト値を書き込みます。ただし、コマンド行で別の値を指定した場合は、デフォルト値に優先して適用されます。

マルチバイト文字をサポートするために、Identity Synchronization for Windows は -s <*rootsuffix*> と -D <*bind-DN*> のデフォルト値を base64 形式で符号化し、コマンド行インタフェース (CLI) の環境ファイルに書き込みます。ルートサフィックスのデフォルトは変更できません。バインド DN のデフォルトは、コマンド行でオーバーライドしたり、CLI 環境ファイル内の base64 形式で符号化された適切な値で更新したりすることが可能です。

- 表 A-2 「すべてのサブコマンドに共通する SSL 関連引数」は、SSL (Secure Socket Layer) の使用による設定ディレクトリへの安全なアクセスに関する情報を指定するオプション引数について説明している。これらの引数は、idsync のすべてのサブコマンドと移行ツールにも共通する
- 表 A-3 「設定ディレクトリの引数」は、設定ディレクトリに関連する引数について説明している。これらの引数は、idsync の複数のサブコマンドと移行ツールにも共通する

注

特定のサブコマンドだけで使用される引数については、該当するサブコマンドの項で説明します。

表 A-1 すべてのサブコマンドに共通する引数

引数	説明
`-h` <*Configuration Directory-hostname*>	設定ディレクトリのホスト名を指定する。この引数のデフォルト値は、コアのインストール時に指定された値である
`-p` <*Configuration Directory-port-no*>	設定ディレクトリの LDAP ポート番号を指定する
`-D` <*bind-DN*>	設定ディレクトリのバインド識別名 (DN) を指定する。この引数のデフォルト値は、コアのインストール時に指定された値である
`-w` <*bind-password* | `->`	設定ディレクトリのバインドパスワードを指定する 値として - を指定した場合、パスワードは標準入力 (`STDIN`) から読み取られる
`-s` <*rootsuffix*>	設定ディレクトリのルートサフィックスを指定する。このルートサフィックスは、`dc=example,dc=com` などの識別名である この引数のデフォルト値は、コアのインストール時に指定された値である
`-q` <*configuration_password* | `->`	設定パスワードを指定する。値として - を指定した場合、パスワードは標準入力 (`STDIN`) から読み取られる この引数は、`prepds` を除くすべてのサブコマンドで必須である

表 A-2 すべてのサブコマンドに共通する SSL 関連引数

引数	説明
`-Z`	セキュリティ保護された通信のために SSL の使用を指定する。設定ディレクトリへの接続時、コマンド行インタフェースまたは優先 / 二次 Directory Server へのアクセス時に、証明書ベースのクライアント認証が行われる
`-P` <*cert-db-path*>	クライアントの証明書データベースのパスとファイル名を指定する この証明書データベースは、Directory Server の証明書データベースへの署名に使用する CA 証明書が含まれている必要がある `-Z` を指定し、`-P` を指定しない場合、<*cert-db-path*> はデフォルトでは <*current-working-directory*>`/cert8.db` となる **注意** : 指定されたディレクトリから Identity Synchronization for Windows が証明書データベースファイルを見つけることができない場合、`cert8.db`、`key3.db`、`secmod.db` の 3 ファイルから構成される *empty* というデータベースがそのディレクトリに作成される

表 A-2　すべてのサブコマンドに共通する SSL 関連引数 (続き)

引数	説明
-m <*secmod-db-path*>	セキュリティモジュールデータベースへのパスを指定する。たとえば、次のように指定する /var/Sun/MPS/slapd-<*serverID*>/secmod.db この引数は、証明書データベースとは異なるディレクトリにセキュリティモジュールデータベースがある場合にだけ指定する

表 A-3　設定ディレクトリの引数

引数	説明
-a <*ldap_filter*> forcepwchg および resync サブコマンドで使用	ソース SUL からユーザーを取得するときに、指定した SUL にユーザーが該当するかどうかを確認する前に、ディレクトリソースから特定のユーザーサブセットを取得するための LDAP フィルタを指定する
-f <*filename*> export10cnf、importcnf、resync サブコマンドで使用	設定情報を記録した XML ドキュメントファイルの名前を指定する
-n forcepwchg、importcnf、resetconn サブコマンドで使用	実際の変更なしでコマンドの実行結果を確認できるように、安全モードで実行する

パスワードの入力

-w <*bind-password*> や -q <*configuration_password*> のようにパスワードの指定が必要な引数では、引数の値として「-」を指定することで、パスワードプログラムにパスワードを STDIN から読み取らせることができます。

複数のパスワードの指定が可能なオプションの値として「-」を指定した場合、idsync は引数の順序に基づいてパスワードを要求します。

このとき、プログラムはまず <*bind-password*> を想定し、次に <*configuration-password*> を想定します。

ヘルプの参照

次のいずれかのコマンドを使用して、コマンドコンソールから idsync またはそのサブコマンドの使用方法に関する情報を表示できます。

- **-help**
- **--help**
- **-?**

使用方法に関する情報を表示するには

- idsync に関する情報 (有効なサブコマンドのリストを含む) を表示するには、コマンドプロンプトにいずれかの上記ヘルプオプションを入力し、Return をクリックする
- サブコマンドに関する情報を表示するには、コマンドプロンプトにサブコマンドとヘルプオプションを入力し、Return をクリックする

idsync コマンドの使用

idsync コマンドとサブコマンドを使用して、Identity Synchronization for Windows のコマンド行ユーティリティを実行することができます。

注 idsync コマンドを実行すると、引数に指定されたすべての DN (バインド DN やサフィックス名など) は、Directory Server への送信前に、そのウィンドウに指定されている文字セットから UTF-8 に変換されます。

サフィックス名では、エスケープ文字としてバックスラッシュを使用しないください。

Solaris 環境で UTF-8 文字を指定するには、端末ウィンドウに UTF-8 に基づくロケールが必要です。環境変数の LC_CTYPE と LANG.are が正しく設定されていることを確認してください。

特に明記されていないかぎり、idsync コマンドとサブコマンドは、次のいずれかの方法で実行できます。

- Solaris 環境 :
  a. 端末ウィンドウを開き、/opt/SUNWisw/bin ディレクトリに移動 (**cd**) します。
  b. 次のように、1 つのサブコマンドを指定して idsync コマンドを実行します。

     idsync <*subcommand***>**

- Windows 環境 :

  a. コマンドウィンドウを開き、<*install_path*>¥isw-<*hostname*>¥bin ディレクトリに移動 (**cd**) します。

  b. 次のように、1 つのサブコマンドを指定して idsync コマンドを実行します。

  idsync <*subcommand***>**

表 A-4 は、idsync ユーティリティのすべてのサブコマンドとその目的を示しています。

表 A-4 idsync ユーティリティのサブコマンドのクイックリファレンス

サブコマンド	機能
certinfo	設定と SSL 設定に基づく証明書情報を表示する 313 ページの「certinfo の使用」を参照
changepw	Identity Synchronization for Windows の設定パスワードを変更する 313 ページの「changepw の使用」を参照
importcnf	エクスポートされた Identity Synchronization for Windows バージョン 1.0 の設定 XML ドキュメントをインポートする。315 ページの「importcnf の使用」を参照
prepds	Identity Synchronization for Windows が使用できるように Sun Java System Directory Server ソースを準備する。316 ページの「prepds の使用」を参照
printstat	インストールと設定のプロセスで完了が必要な手順をリスト表示する。また、インストールされているコネクタ、システムマネージャ、Message Queue の状態を出力する。320 ページの「printstat の使用」を参照
resetconn	設定ディレクトリ内のコネクタの状態を *UNINSTALLED* (アンインストール済み) にリセットする 321 ページの「resetconn の使用」を参照
resync	既存のユーザーのリンク設定と再同期を行い、インストールプロセスの一部としてディレクトリを事前に取り込む。322 ページの「resync の使用」を参照
startsync	同期を開始する。325 ページの「startsync の使用」を参照
stopsync	同期を終了する。326 ページの「stopsync の使用」を参照

certinfo の使用

certinfo サブコマンドを使用することで、設定と SSL 設定に基づいて証明書情報を表示できます。この情報は、各コネクタ、Directory Server プラグイン、または両方の証明書データベースに追加する必要のある証明書を特定するときに役立ちます。

証明書情報を表示するには、端末ウィンドウ (またはコマンドウィンドウ) を開き、**idsync certinfo** コマンドを次のように入力します。

```
idsync certinfo [<bind-DN>] -w <bind-password | -> [-h <Configuration
Directory-hostname>] [-p <Configuration Directory-port-no>] [-s <rootsuffix>] -q
<configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>]
```

注 certinfo サブコマンドは、コネクタと Directory Server のどちらの証明書データベースに対してもアクセス権を持たないため、表示される一部の手順はすでに実行されている可能性があります。

たとえば、次のように実行します。

```
idsync certinfo -w <admin-password> -q <configuration-password>
```

注 certinfo 引数の詳細については、308 ページの「共通引数」を参照してください。

changepw の使用

changepw サブコマンドを使用することで、Identity Synchronization for Windows の設定パスワードを変更できます。

Identity Synchronization for Windows の設定パスワードを変更する手順は、次のとおりです。

1. Identity Synchronization for Windows のすべてのプロセス (たとえば、システムマネージャ、セントラルロガー、コネクタ、コンソール、インストーラ、アンインストーラなど) を停止します。
2. すべてのプロセスを停止したら、設定ディレクトリを ldif にエクスポートして ou=Services のバックアップを行います。
3. **idsync changepw** コマンドを次のように入力します。

```
idsync changepw [-D <bind-DN>] -w <bind-password | -> [-h
<Configuration Directory-hostname>] [-p <Configuration Directory-port-no>] [-s
<rootsuffix>]
-q <configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>]
-b <new password | - > [-y]
```

たとえば、次のように実行します。

idsync changepw -w <*admin password*> -q <*old config password*> -b -q <*new config password*>

次の引数は、changepw だけで使用されます。

表 A-5 idsync changepw の引数

引数	説明
-b <*password*>	新しい設定パスワードを指定する。値として - を指定した場合、パスワードは標準入力 (STDIN) から読み取られる
[-y]	プロンプトにコマンドの確認を表示しない

注 changepw のその他の引数については、308 ページの「共通引数」を参照してください。

4. 端末ウィンドウに表示されるメッセージに応答します。たとえば、次のようなメッセージが表示されます。

```
本当に設定パスワードの変更を行いますか (y/n)? yes
システムを再起動する前に -
$PSWHOME/resources/SystemManagerBootParams.cfg ファイルを編集し、
「deploymentPassword」の値を変更します。

成功
```

5. システムを再起動する前に、SystemManagerBootParams.cfg ファイルを修正する必要があります。

   $PSWHOME¥resources (この $PSWHOME は <*isw-installation directory*>) 内の SystemManagerBootParams.cfg ファイルには、システムマネージャが設定ディレクトリへの接続に使用する設定パスワードが含まれます。

   たとえば、パスワードの値を次のように変更します。

   変更前 : <*Parameter name="manager.configReg.deploymentPassword" value="***oldpassword***"*/>

   変更後 : <*Parameter name="manager.configReg.deploymentPassword" value="***newpassword***"*/>

6. プログラムがエラーを報告する場合は、手順 2 でエクスポートした ldif を使用して設定ディレクトリを復元し、処理をやり直します。多くの場合は、設定ディレクトリをホストする Directory Server がパスワード変更時に使用不可能であったことがエラーの原因です。

importcnf の使用

警告 idsync importcnf は、Identity Synchronization for Windows バージョン 1.0 または 1.0 SP1 から 1 2004Q3 に移行する場合にだけ使用します。

コアをインストールしたら (第 3 章「コアのインストール」を参照)、Identity Synchronization for Windows バージョン 1.0 または 1.0 SP1 からエクスポートした、コアの設定情報が記録された設定 XML ファイルを idsync importcnf サブコマンドを使用してインポートします。

バージョン 1.0 または 1.0 SP1 の設定 XML ファイルをインポートするには、端末ウィンドウ (またはコマンドウィンドウ) を開き、**idsync importcnf** コマンドを次のように入力します。

```
idsync importcnf [-D <bind-DN>] -w <bind-password | -> [-h
<Configuration Directory-hostname>] [-p <Configuration Directory-port-no>] [-s
<rootsuffix>] -q <configuration_password> [-Z] [-P <cert-db-path>] [-m
<secmod-db-path>] -f <filename> [-n]
```

たとえば、次のように実行します。

```
idsync importcnf -w <admin_password> -q <configuration_password> -f
"MyConfig.cfg"
```

次の引数は、importcnf だけで使用されます。

表 A-6　idsync importcnf の引数

引数	説明
-f <*filename*>	設定情報を記録した XML ドキュメントの名前を指定する
-n	実際の変更なしでコマンドの実行結果を確認できるように、安全モードで実行する

注　importcnf のその他の引数については、308 ページの「共通引数」を参照してください。

バージョン 1.0 または 1.0 SP1 の設定 XML ファイルをインポートしたら、Identity Synchronization for Windows のコネクタとサブコンポーネントをインストールできるように、同期対象の Directory Server ソースに対して prepds を実行する必要があります (316 ページの「prepds の使用」を参照)。

prepds の使用

Identity Synchronization for Windows が使用できるように Sun Java System Directory Server ソースを準備するときは、コンソール、または prepds サブコマンドを使用します。prepds は、Directory Server コネクタのインストール前に実行する必要があります。

idsync prepds サブコマンドを実行すると、旧バージョン形式の更新履歴ログデータベースのルートノードである cn=changelog エントリに適切な ACI が適用されます。

- Identity Synchronization for Windows が使用できるように優先マスター Directory Server を準備するときは、ディレクトリマネージャのクレデンシャルを指定する必要がある

  ディレクトリマネージャユーザーは Directory Server の特別なユーザーで、Directory Server インスタンス内のあらゆる場所に対して完全な権限を持つ。ACI はディレクトリマネージャユーザーには適用されない

  たとえば、旧バージョン形式の更新履歴ログデータベースのアクセス制御は、ディレクトリマネージャだけが設定できる。これは、優先マスターサーバーの準備で Identity Synchronization for Windows がディレクトリマネージャのクレデンシャルを必要とする理由の 1 つである

注 何らかの理由で優先 Sun ディレクトリソースの旧バージョン形式の更新履歴ログデータベースを再作成する場合、デフォルトのアクセス制御設定が適用されると Directory Server コネクタはデータベースの内容を読み込めません。

旧バージョン形式の更新履歴ログデータベースのアクセス制御設定を復元するには、`idsync prepds` を実行するか、コンソールで適切な Sun ディレクトリソースを選択してから「Directory Server の準備」ボタンをクリックします。

注 指定した期間の経過後に更新履歴ログのエントリを自動的に削除する (または切り取る) ようにシステムを設定することができます。コマンド行から `cn=Retro Changelog Plugin, cn=plugins, cn=config` の `nsslapd-changelogmaxage` の設定を次のように変更します。

`nsslapd-changelogmaxage:` *IntegerTimeunit*

ここで

- Integer は数値である
- Timeunit は単位で、s は秒、m は分、h は時、d は日、w は週をそれぞれ意味する。Integer 変数と timeUnit 変数の間には空白を挿入しない

たとえば、`nsslapd-changelogmaxage: 2d` のように指定します。

詳細については、『Sun Java™ System Directory Server 5 2005Q1 管理ガイド』の「レプリケーションの管理」の章を参照してください。

- 二次サーバーの準備には、管理者ユーザーのクレデンシャルを使用できる

注 使用するホストとサフィックスを指定する必要があるので、`idsync prepds` を実行する前に Identity Synchronization for Windows の設定を計画しておいてください。

Directory Server コネクタとプラグインがすでにインストールされ、設定されている Directory Server サフィックスで `idsync prepds` を実行すると、同期時に Directory Server コネクタのインストールを促すメッセージが出力されます。このメッセージは無視してください。

Sun Java System Directory Server ソースを準備するには、端末ウィンドウ (またはコマンドウィンドウ) を開き、**`idsync prepds`** コマンドを次のように入力します。

```
idsync prepds [-D <bind-DN>] -w <bind-password | -> [-h <preferred host>]
[-p <preferred-port>] [-s <database-suffix>] [-Z] [-P <cert-db-path>]
[-m <secmod-db-path>] [-j <secondary_host>] [-r <secondary-port>] [-E <admin
DN of secondary host>] [-u <password for secondary host | ->] [-x]
```

たとえば、次のように実行します。

```
idsync prepds -D "cn=Directory Manager" -w <preferred master password> -h
<preferred-host> -p 389 -s dc=example,dc=com -j "secondary host" -r 389
-E "cn=Administrator" -u <secondary master password> -s dc=example,dc=com
```

注 -h、-p、-D、-w、-s の各引数は、prepds サブコマンド専用に再定義されています。これらの引数については、次の表で説明します。また、-q 引数は適用されません。

表 A-7 は、idsync prepds だけで使用される引数を説明しています。

表 A-7 prepds の引数

引数	説明
-h <*name*>	優先ホストとして機能する Directory Server インスタンスの DNS 名を指定する
-p <*port*>	優先ホストとして機能する Directory Server インスタンスのポート番号を指定する デフォルトは *389*
-j <*name*> (省略可能)	二次ホストとして機能する Directory Server インスタンスの DNS 名を指定する。Sun Java System Directory Server 5 2005Q1 のマルチマスターレプリケーション (MMR) 環境に適用される
-r <*port*> (省略可能)	二次ホストとして機能する Directory Server インスタンスのポート番号を指定する。Sun Java System Directory Server 5 2005Q1 のマルチマスターレプリケーション (MMR) 環境に適用される。デフォルトは *389*
-D <*dn*>	優先ホストのディレクトリマネージャユーザーの識別名を指定する
-w <*password*>	優先ホストのディレクトリマネージャユーザーのパスワードを指定する 値として - を指定した場合、パスワードは標準入力 (STDIN) から読み取られる
-E <*admin-DN*>	二次ホストのディレクトリマネージャユーザーの識別名を指定する
-u <*password*>	二次ホストのディレクトリマネージャユーザーのパスワードを指定する 値として - を指定した場合、パスワードは標準入力 (STDIN) から読み取られる

表 A-7　prepds の引数 (続き)

引数	説明
-s <*rootsuffix*>	インデックスの追加に使用されるルートサフィックスを指定する (同期対象ユーザーが存在するルートサフィックスを指定する) **注意** : 優先ホストと二次ホストのデータベース名は異なる場合がありますが、サフィックスが異なることはありません。このため、プログラムは各ホストのデータベース名を検出し、それを使用してインデックスを追加できます。
-x	dspswuserlink 属性の等価インデックスと実在インデックスをデータベースに追加しない

レプリケートされた環境 (たとえば、優先マスター、二次マスター、2 つのコンシューマが含まれる環境など) で idsync prepds を実行するときは、優先マスターと二次マスターで idsync prepds を 1 回だけ実行します。

idsync prepds を実行する手順は、次のとおりです。

1. Directory Server のレプリケーションが稼動していることを確認します (該当する場合)。
2. コンソールから、またはコマンド行から次のように idsync prepds を実行します。

   ```
   idsync prepds -h M1.example.com -p 389 -j M2.example.com -r 389 . . .
   ```

idsync prepds コマンドを実行することで、次の処理が行われます。

- M1 では、次の処理が行われる
  - RCL を有効化および拡張し、より多くの属性 (dspswuserlink など) を取り込む

    RCL は M1 だけで必要とされる
  - スキーマを拡張する
  - ACI に uid=pswconnector,<*suffix*> user を追加する
  - dspswuserlink 属性にインデックスを追加する。これにより、インデックス作成が完了するまで Directory Server は一時的に読み取り専用になる

    ダウン時間を避けるために、インデックスを後から追加することもできるが、インデックスの追加は Directory Server コネクタのインストール前に完了させる必要がある
- M2 では、インデックスを追加する

注

- レプリケーションにより、Identity Synchronization for Windows はスキーマ情報と `uid=pswconnector` を優先マスターから二次マスターと両方のコンシューマにコピーする
- Directory Server コネクタは 1 回だけインストールする。Directory Server プラグインは、すべてのディレクトリにインストールする必要がある
- インデックス作成は、優先マスターと二次マスターだけで必要とされる。インデックスの設定は、レプリケーションによって優先マスターから二次マスターに伝達されない

printstat の使用

`printstat` サブコマンドを使用することで、次の操作を行えます。

- インストールと設定を完了するために実行が必要な残りの手順をリスト表示する
- インストールされているコネクタ、システムマネージャ、Message Queue の状態を出力する

  状態の種類は、次のとおりです。

  - UNINSTALLED : コネクタはインストールされていない
  - INSTALLED : コネクタはインストールされているが、実行時設定を受信していないため、同期の準備は整っていない
  - READY : コネクタは同期の準備が整っているが、どのオブジェクトも同期させていない
  - SYNCING : コネクタはオブジェクトを同期させている

インストールされているコネクタ、システムマネージャ、Message Queue の状態を出力するには、端末ウィンドウ (またはコマンドウィンドウ) を開き、**`idsync printstat`** コマンドを次のように入力します。

```
idsync printstat [-D <bind-DN>] -w <bind-password | -> [-h <Configuration
Directory-hostname>] [-p <Configuration Directory-port-no>] [-s <rootsuffix>]
-q <configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>]
```

たとえば、次のように実行します。

```
idsync printstat -w <admin password> -q <configuration password>
```

注 printstat の引数については、308 ページの「共通引数」を参照してください。

resetconn の使用

resetconn サブコマンドを使用することで、設定ディレクトリ内のコネクタの状態を *UNINSTALLED* にリセットできます。たとえば、ハードウェアの障害によってコネクタをアンインストールできなくなった場合は、コネクタを再インストールできるように、resetconn を使用してコネクタの状態を UNINSTALLED (アンインストール済み) に変更します。

警告 resetconn サブコマンドは、ハードウェアまたはアンインストーラに障害が発生した場合の使用だけが想定されています。

コネクタの状態をコマンド行からリセットするには、端末ウィンドウ (またはコマンドウィンドウ) を開き、**idsync resetconn** コマンドを次のように入力します。

```
idsync resetconn [-D <bind-DN>] -w <bind-password> | -> [-h
<Configuration Directory-hostname>] [-p <Configuration Directory-port-no>] [-s
<rootsuffix>] -q <configuration_password> [-Z] [-P <cert-db-path>] [-m
<secmod-db-path>] -e <directory-source-name> [-n]
```

たとえば、次のように実行します。

```
idsync resetconn -w <admin password> -q <configuration_password> -e
"dc=example,dc=com"
```

表 A-7 は、resetconn だけで使用される引数を説明しています。

表 A-8 idsync resetconn の引数

引数	説明
-e <*dir-source*>	リセットするディレクトリソースの名前を指定する

表 A-8　idsync resetconn の引数 (続き)

引数	説明
-n	実際の変更なしでコマンドの実行結果を確認できるように、安全モードで実行する

注　idsync printstat を使用して、ディレクトリソースの名前を調べることができます。

resetconn のその他の引数については、308 ページの「共通引数」を参照してください。

resync の使用

resync サブコマンドを使用して、配備に既存ユーザーを取り込む (ブートストラップ) ことができます。このコマンドは、管理者が指定した一致規則を使用して次の処理を行います。

- 既存のエントリにリンクを設定する
- 空のディレクトリにリモートディレクトリの内容を取り込む
- 2 つの既存のユーザー集合の間で属性値を一括同期させる

注　ユーザーのリンク設定と同期については、175 ページの「既存ユーザーの同期」を参照してください。

既存のユーザーを再同期させ、ディレクトリを事前に取り込むには、端末ウィンドウ (またはコマンドウィンドウ) を開き、**idsync resync** コマンドを次のように入力します。

```
idsync resync [-D <bind-DN>] -w <bind-password> | -> [-h <Configuration
Directory-hostname>] [-p <Configuration Directory-port-no>] [-s <rootsuffix>] -q
<configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>] [-n]
[-f <xml filename for linking>] [-k] [-a <ldap-filter>] [-l <sul-to-sync>] [-o
Sun | Windows] [-c] [-x] [-u] [-i ALL_USERS | NEW_USERS |
NEW_LINKED_USERS]
```

たとえば、次のように実行します。

```
idsync resync -w <admin password> -q <configuration_password>
```

表 A-9 は、resync だけで使用される引数を説明しています。

表 A-9 idsync resync の使用方法

引数	意味
`-f <filename>`	Identity Synchronization for Windows に用意されているいずれかの XML 設定ファイルを使用して、リンクが設定されていないユーザーエントリの間にリンクを作成する 付録 B「LinkUsers XML ドキュメントのサンプル」を参照
`-k`	ユーザーの作成、既存ユーザーの変更は行わずに、リンクが設定されていないユーザーの間だけにリンクを作成する
`-a <ldap-filter>`	同期の対象となるエントリを制限する LDAP フィルタを指定する このフィルタは、同期処理のソース側に適用される たとえば、`idsync resync -o Sun -a "uid=*"` と指定した場合、uid 属性を持つすべての Directory Server ユーザーが Active Directory 側で同期される
`-l <sul-to-sync>`	再同期対象の同期ユーザーリスト (SUL) を個別に指定する **注意** : 複数の SUL ID を指定して複数の SUL を再同期させることも、SUL ID を指定せずにすべての SUL を再同期させることもできる
`-o (Sun | Windows)`	再同期処理のソースを指定する • Sun: Windows エントリの属性値を、Sun Java System Directory Server ディレクトリソースエントリ内の対応する属性値に設定する • Windows: Sun Java System Directory Server エントリの属性値を、Windows ディレクトリソースエントリ内の対応する属性値に設定する (デフォルトは Windows)
`-c`	ターゲット側に対応するユーザーが存在しない場合は、ユーザーエントリを自動的に作成する • Active Directory または Windows NT で作成されるユーザーには、ランダムに生成パスワードが割り当てられる • Directory Server で作成されるユーザーには、`-i` オプションを指定しない場合、特別なパスワード値 (`(PSWSYNC)`**`*INVALID PASSWORD*`**) が自動的に作成される

表 A-9　idsync resync の使用方法 (続き)

引数	意味
-i (ALL_USERS | NEW_USERS | NEW_LINKED_USERS)	Sun ディレクトリソース内で同期されるユーザーエントリのパスワードをリセットし、これらのユーザーが次にユーザーパスワードを求められる機会に、現在のドメイン内でパスワードの同期を強制する • **ALL_USERS**: すべての同期対象ユーザーにオンデマンドパスワード同期を強制する • **NEW_USERS**: 新たに作成されたユーザーだけにオンデマンドパスワード同期を強制する • **NEW_LINKED_USERS**: すべての新規作成ユーザーと、新たにリンクが設定されたユーザーにオンデマンドパスワード同期を強制する
-u	オブジェクトキャッシュだけを更新する。エントリは変更されない この引数は、Windows ディレクトリソースのユーザーエントリのローカルキャッシュだけを更新するため、既存の Windows ユーザーは Directory Server に作成されない。この引数を指定した場合、Windows ユーザーエントリと Directory Server ユーザーエントリは同期されない。この引数は、resync のソースが Windows である場合にだけ適用される
-x	ソースエントリと一致しないターゲット側ユーザーエントリをすべて削除する
-n	実際の変更なしでコマンドの実行結果を確認できるように、安全モードで実行する

注
- 使用方法を表示するときは、引数を指定せずに idsync resync を実行する
- resync のその他の引数については、308 ページの「共通引数」を参照
- 既存ユーザーの再同期については、175 ページの「既存ユーザーの同期」を参照

resync を実行したら、セントラル監査ログ (audit.log) の resync.log ファイルを調べてください。エラーが記録されている場合は、第 9 章「トラブルシューティング」を参照してください。

startsync の使用

startsync サブコマンドを使用することで、コマンド行から同期を開始できます。

同期を開始するには、端末ウィンドウ (またはコマンドウィンドウ) を開き、**idsync startsync** コマンドを次のように入力します。

```
idsync startsync [-D <bind-DN>] -w <bind-password | -> [-h <Configuration
Directory-hostname>] [-p <Configuration Directory-port-no>] [-s <rootsuffix>] -q
<configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>]
```

たとえば、次のように実行します。

```
idsync startsync -w <admin password> -q <configuration_password>
```

表 A-10 は、startsync だけで使用される引数を説明しています。

表 A-10 idsync startsync の引数

引数	説明
[-y]	プロンプトにコマンドの確認を表示しない

注 startsync のその他の引数については、308 ページの「共通引数」を参照してください。

stopsync の使用

stopsync サブコマンドを使用することで、コマンド行から同期を終了できます。

同期を終了するには、端末ウィンドウ (またはコマンドウィンドウ) を開き、**idsync stopsync** コマンドを次のように入力します。

```
idsync stopsync [-D <bind-DN>] -w <bind-password | -> [-h <Configuration
Directory-hostname>] [-p <Configuration Directory-port-no>] [-s <rootsuffix>] -q
<configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>]
```

たとえば、次のように実行します。

```
idsync stopsync -w <admin password> -q <configuration_password>
```

注 stopsync の引数については、308 ページの「共通引数」を参照してください。

移行ユーティリティ forcepwchg の使用

移行中にパスワードを変更したユーザーは、Windows NT と Directory Server のそれぞれに異なるパスワードを持つことになります。forcepwchg ユーティリティを使用することで、Identity Synchronization for Windows のバージョン 1.0 または 1.0 SP1 からバージョン 1 2004Q3 へのアップグレード中にパスワードを変更したユーザーに、パスワードの変更を強制できます。

注 forcepwchg ユーティリティは、Windows パッケージだけに付属します。

forcepwchg を使用する前に、次の事項を確認してください。

- userpassword 属性の値に 7 ビット値を強制する 7 ビットチェックプラグインが Directory Server に設定されていないことを確認する。この確認は、Directory Server コンソールで行う
- 認証に使用するクライアントが、使用環境のロケールを UTF-8 に正しく変換することを確認する。たとえば、Directory Server に付属する ldapsearch の -i オプションを使用する

forcepwchg コマンド行ユーティリティを実行する方法は、次のとおりです。

1. 「コマンドプロンプト」ウィンドウを開き、移行を行うホストの `migration` ディレクトリに移動 (cd) します。PDC ホストには、Identity Synchronization for Windows 1.0 NT コンポーネント (コネクタ、変更ディテクタ DLL、パスワードフィルタ DLL) がインストールされている必要があります。
2. `migration` ディレクトリで、次のように入力します。

```
java -jar forcepwchg.jar [-n] [-a] [-t <time_specification>]
```

たとえば、次のように実行します。

```
forcepwchg.jar -n -a
forcepwchg.jar -t 33m
```

表 A-11 は、`forcepwchg` だけで使用される引数を説明しています。

表 A-11 forcepwchg の引数

オプション	説明
-n	プレビューモードを指定する プレビューモードでは、このユーティリティは次のユーザーを除くすべての通常ユーザーの名前を出力する • -a 引数を指定した場合は、内蔵アカウント (Administrator および Guest) • -t 引数によって指定された期間中にパスワードを変更したユーザー プレビューモードでは、すべてのユーザーが `forcepwchg` を実行できる プレビューモード以外のモードで `forcepwchg` を実行できるのは管理者だけである
-a	パスワードの変更をすべてのユーザー (Administrator と Guest を除く) に強制する -t 引数を使用する場合は、この引数を使用できない
-t <*time_specification*>	<*time_specification*> で指定した時間だけさかのぼった時刻から現在までの間にパスワードを変更したユーザーにパスワードの変更を強制する <*time_specification*> には、次の形式で時間を指定できる • < 数値 >: 秒数 (`-t 30` など) • < 数値 >m: 分数 (`-t 25m` など) • < 数値 >h: 時間数 (`-t 6h` など) たとえば、`forcepwchg -t 6h` と指定した場合、過去 6 時間にパスワードを変更したすべてのユーザーに、パスワードの再変更が強制される
-?	使用方法に関する情報を出力する

注 `forcepwchg` の使用方法については、196 ページの「Windows NT でのパスワード変更の強制」を参照してください。

LinkUsers XML ドキュメントのサンプル

この付録では、idsync resync サブコマンドで配備に含まれる既存ユーザーにリンクを設定するときに使用される XML 設定ドキュメントの 2 つの例を示します。

コアのインストール先にある samples1 サブディレクトリには、次のファイルが両方とも用意されています。

- 329 ページの「サンプル 1: linkusers-simple.cfg」(一般的で単純な設定の例)
- 330 ページの「サンプル 2: linkusers.cfg」(リンク条件のすべての指定方法を示す、より複雑な設定の例)

これらのサンプルを環境に合わせて変更できます。どちらのファイルにも、サンプルを変更してユーザーにリンクを設定する方法がコメントとして含まれています (複数の SUL に含まれるユーザーの指定も含む)。

サンプル 1: linkusers-simple.cfg

```
<!--

    Copyright 2004 Sun Microsystems, Inc. All rights reserved

    使用はライセンス条項の対象となります。

-->

<!--

    この XML ファイルは、Windows と Sun Directory Server のユーザーをコマンド行からリンクさせるときに使用します。これは「idsync resync」の -f オプションによってスクリプトに渡されます。

    これは、Directory Server の uid 属性が Active Directory の samaccountname 属性と一致する、つまり同一のログイン名を持つ SUL 1 同期ユーザーリストのユーザーにリンクを設定する、単純なファイルです。

    より複雑な一致規則については、linkusers.cfg sample を参照してください。
```

```
-->
<UserLinkingOperationList>
    <UserLinkingOperation parent.attr="UserLinkingOperation" sulid="SUL1">
        <UserMatchingCriteria parent.attr="UserMatchingCriteria">
            <AttributeMap parent.attr="AttributeMap">
                <AttributeDescription parent.attr="SunAttribute" name="uid"/>
                <AttributeDescription parent.attr="WindowsAttribute" name="samaccountname"/>
            </AttributeMap>
        </UserMatchingCriteria>
    </UserLinkingOperation>
</UserLinkingOperationList>
```

サンプル 2: linkusers.cfg

```
<?xml version ="1.0" encoding="UTF-8"?>
<!--
    Copyright 2004 Sun Microsystems, Inc. All rights reserved
    使用はライセンス条項の対象となります。
-->
<!--
    この XML ファイルは、Windows と Sun Directory Server のユーザーをコマンド行からリンク
    させるときに使用されます。これは「idsync resync」の -f オプションによってスクリプトに渡
    されます。
-->
<!--
    次のパラメータ allowLinkingOutOfScope が true の場合、Windows ユーザーを、ユーザーの
    同期ユーザーリストに含まれない Sun Directory Server ユーザーにリンクさせることができます。
    デフォルトは false です。
-->
<UserLinkingOperationList allowLinkingOutOfScope="false">
```

```
<!--
    UserLinkingOperation は、1 つの SUL の設定をリンクにカプセル化します。
    これには、SUL ID と、一致させる属性のリストが含まれます。
    リンクさせる SUL ごとに、独立した UserLinkingOperation を指定する必要があります。
-->
<UserLinkingOperation parent.attr="UserLinkingOperation" sulid="SUL1">

<!--
    UserMatchingCriteria は、リンク対象ユーザーと一致する必要のある属性のリストを
    カプセル化します。-->

<!--
    この UserMatchingCriteria を使用して 2 ユーザーと一致させるには、どちらのユーザーも
    givenName、および同一の sn を持つ必要があります。-->

<UserMatchingCriteria parent.attr="UserMatchingCriteria">
    <AttributeMap parent.attr="AttributeMap">
        <AttributeDescription parent.attr="SunAttribute" name="sn"/>
        <AttributeDescription parent.attr="WindowsAttribute" name="sn"/>
    </AttributeMap>
    <AttributeMap parent.attr="AttributeMap">
        <AttributeDescription parent.attr="SunAttribute" name="givenName"/>
        <AttributeDescription parent.attr="WindowsAttribute"
        name="givenName"/>
    </AttributeMap>
</UserMatchingCriteria>

<!--
    1 つの SUL に複数の UserMatchingCriteria を指定できます。これらは、論理 OR として
    扱われます。この例では、リンク対象ユーザーの (givenName と sn が一致する必要がある ) OR
    (employee(Number|ID) が一致する必要がある ) と解釈されます。指定された属性
    employeeNumber が DS 属性の名前であることに注意してください。-->

<!--
    employeeNumber は DS 内でインデックス付けされていない属性であるため、
    この UserMatchingCriteria はコメントアウトされます。UserMatchingCriteria で
    使用されるすべての属性にはインデックスが付けられている必要があります。

    <UserMatchingCriteria parent.attr="UserMatchingCriteria">
        <AttributeMap parent.attr="AttributeMap">
            <AttributeDescription parent.attr="SunAttribute" name="employeeNumber"/>
            <AttributeDescription parent.attr="WindowsAttribute" name="employeeID"/>
        </AttributeMap>
    </UserMatchingCriteria>

-->

</UserLinkingOperation>
```

```
<!--
    複数の SUL をリンクさせる場合、それぞれに異なる UserLinkingOperation が指定されます。
    ここに示されるように、各 UserLinkingOperation は異なる UserMatchingCriteria を
    使用できます。この例では、SUL2 のユーザーは、sn と employeeNumber が一致する場合にだけ
    リンクされます。

    注 : 設定例に含まれる SUL は 1 つだけであるため、この UserLinkingOperation は
    コメントアウトされています。

<UserLinkingOperation parent.attr="UserLinkingOperation" sulid="SUL2">
    <UserMatchingCriteria parent.attr="UserMatchingCriteria">
        <AttributeMap parent.attr="AttributeMap">
            <AttributeDescription parent.attr="SunAttribute" name="sn"/>
            <AttributeDescription parent.attr="WindowsAttribute" name="sn"/>
        </AttributeMap>
            <AttributeMap parent.attr="AttributeMap">
                <AttributeDescription parent.attr="SunAttribute" name="employeeNumber"/>
                <AttributeDescription parent.attr="WindowsAttribute" name="employeeID"/>
        </AttributeMap>
    </UserMatchingCriteria>
</UserLinkingOperation>
-->

</UserLinkingOperationList>
```

Solaris でのルート以外のユーザーによるサービスの実行

Identity Synchronization for Windows サービスをインストールおよび実行するには、ルート権限が必要です。しかし、製品のインストール後であれば、プログラムのサービスをルート以外のユーザーとして実行できるように、ソフトウェアを設定することができます。

注 ルート以外のユーザーとしてサービスを実行するには、Identity Synchronization for Windows インスタンスのディレクトリの下にあるすべてのディレクトリのアクセス権限を変更する必要があります。デフォルトディレクトリは `/var/opt/SUNWisw` です。

Solaris でルート以外のユーザーとしてサービスを実行できるようにする手順は、次のとおりです。

1. UNIX の `useradd` コマンドを使用し、Identity Synchronization for Windows 用のユーザーアカウントを作成します (この手順は省略可能)。

   `nobody` ユーザーを使用してサービスを実行することもできます。
   以後の手順に示す例は、*iswuser* というユーザーを作成したことを前提とします。

2. Solaris に Sun Java System Directory Server コネクタをインストールするには、インストール時に、特別な権限を持たないポートをコネクタ用に選択する必要があります。
   たとえば、1024 より大きい番号のポートが受け付けられます。

   注 以後の手順では、すべてのコマンドを `root` として実行する必要があります。

3. すべてのコンポーネントをインストールしたら、次のコマンドを実行して Identity Synchronization for Windows を停止します。

```
/etc/init.d/isw stop
```

4. インスタンスディレクトリの所有権を変更する必要があります。たとえば、製品を /var/opt/SUNWisw にインストールした場合は、次のように変更します。

```
chown -R iswuser /var/opt/SUNWisw
chown -R iswuser /opt/SUNWisw
```

5. テキストエディタで /etc/init.d/isw ファイルを開き、次の行を編集します。

```
"$EXEC_START_WATCHDOG" "$JAVA_PATH" "$INSTALL_DIR" "CONFIG_DIR"
```

これを、次のように変更します。

```
su iswuser -c "$EXEC_START_WATCHDOG '$JAVA_PATH' '$INSTALL_DIR'
'CONFIG_DIR'"
```

6. 次のコマンドを実行して、サービスを開始し直します。

```
/etc/init.d/isw start
```

7. 次のコマンドを実行し、割り当てたユーザーのユーザー ID でコンポーネントが実行されていることを確認します。

```
ps -ef | grep iswuser
```

同期ユーザーリストの定義と設定

この付録では、SUL (同期ユーザーリスト) の定義について補足情報を示し、複数ドメインを設定する方法について説明します。ここで説明する内容は次のとおりです。

同期ユーザーリストの定義について

すべての SUL (同期ユーザーリスト) には、同期対象となる Directory Server ユーザーを識別するための定義と、同期対象となる Windows ユーザーを識別するための定義の 2 つが含まれます。

それぞれの定義は、ディレクトリ内のどのユーザーを同期させるか、どのユーザーを同期対象から外すか、新規ユーザーをどこに作成するかを指定します。

注

同期対象ユーザーは、Identity Synchronization for Windows コンソールで選択したオブジェクトクラスによっても決定されます。プログラムは、選択したオブジェクトクラスを持つユーザーだけを同期させます。これには、選択したオブジェクトクラスのサブクラスを持つユーザーも含まれます。

たとえば、`organizationalPerson` オブジェクトクラスを選択すると、このオブジェクトクラスのサブクラスである `inetorgperson` を持つユーザーも同期の対象となります。

表 D-1 は、SUL 定義の要素を説明しています。

表 D-1　SUL 定義の要素

要素	定義	適用対象		
		Sun	AD	NT
ベース DN	同期対象のすべてのユーザーの親 LDAP ノードを定義する 同期ユーザーリストのフィルタによってユーザーが除外されるか、またはユーザーの DN がより詳細な同期ユーザーリストと一致する場合を除き、同期ユーザーリストのベース DN には、その DN のすべてのユーザーが含まれる たとえば、`ou=sales,dc=example,dc=com`			×
フィルタ	同期ユーザーリストにユーザーを含めたり、ユーザーを除外したりするための LDAP に似たフィルタを定義する フィルタでは、`&`、`|`、`!`、`=`、`*` の各演算子を使用できる。演算子 `>=` および `<=` はサポートされない。すべての比較は、大文字と小文字を区別しない文字列の比較として行われる たとえば、`(& (employeeType=manager)(st=CA))` はカリフォルニアのマネージャだけを範囲に含める			
作成式	新規作成ユーザーの親 DN とネーミング属性を定義する。これは、作成を有効にした場合にだけ適用される 作成式には、同期ユーザーリストのベース DN を含める必要がある。たとえば、`cn=%cn%,ou=sales,dc=example,dc=com`。この `%cn%` トークンは、作成されるユーザーエントリからの値に置き換えられる			×

注　Sun Java System Directory Server のユーザーを複数の Active Directory ドメインと同期させるには、Active Directory ドメインごとに少なくとも 1 つの SUL を定義する必要があります。

複数の SUL を定義すると、Identity Synchronization for Windows は各 SUL 定義を繰り返し一致させることで、SUL のメンバーを特定します。プログラムは、より詳細なベース DN が指定されている SUL 定義から順に調べます。
たとえば、プログラムは `dc=example,dc=com` を調べる前に `ou=sales,dc=example,dc=com` との一致を調べます。

2 つの SUL 定義が同じベース DN と別のフィルタを持つ場合、Identity Synchronization for Windows はどちらのフィルタを最初に調べるかを自動的に決定することができません。このため、管理者は「ドメイン重複の解決」機能を使用して、2 つの SUL 定義の順序を決定する必要があります。ユーザーが SUL 定義のベース DN と一致するが、そのベース DN のどのフィルタとも一致しない場合、そのユーザーが詳細度の低いベース DN のフィルタと一致したとしても、このユーザーは同期対象から除外されます。

複数の Windows ドメインの設定

複数の Windows ドメインを同じ Directory Server コンテナ (`ou=people,dc=example,dc=com` など) に同期させるために、Identity Synchronization for Windows はドメイン情報の格納に合成 Windows 属性を使用します。

- Active Directory ドメインでは、エントリを Directory Server に同期させる前に、Identity Synchronization for Windows は `activedirectorydomainname` 属性を Active Directory ドメイン名 (*east.example.com* など) に設定する
- Windows NT ドメインでは、エントリを Directory Server に同期させる前に、Identity Synchronization for Windows は `user_nt_domain_name` 属性を Windows NT ドメイン名 (*NTEXAMPLE* など) に設定する

これらの属性は実際には Windows ユーザーエントリには表示されませんが、同期のために Identity Synchronization for Windows コンソールで使用され、Directory Server 側のユーザー属性にマッピングできます。Identity Synchronization for Windows がドメイン属性をマッピングすると、同期時に Directory Server エントリ内の属性として設定され、SUL (同期ユーザーリスト) フィルタでも使用できるようになります。

次の例は、Identity Synchronization for Windows がこれらの属性をどのように使用するかを示しています。この例は、3 つの Windows ドメイン (2 つの Active Directory ドメインと 1 つの Windows NT ドメイン) を 1 つの Directory Server インスタンスに同期させることを前提としています。

1. Active Directory east.example.com ドメインのユーザーは、`ou=people,dc=example,dc=com` 内の Directory Server に同期される
2. Active Directory west.example.com ドメインのユーザーは、`ou=people,dc=example,dc=com` 内の Directory Server に同期される
3. Windows NT NT NTEXAMPLE ドメインのユーザーは、`ou=people,dc=example,dc=com` 内の Directory Server に同期される

Directory Server ユーザーを作成または修正すると、プログラムは SUL フィルタを使用して、どの Windows ドメインでユーザーを同期させるかを決定します (各 Directory Server SUL に同じベース DN ou=people,dc=example,dc=com が指定されているため)。activedirectorydomainname 属性と user_nt_domain_name 属性を使用することで、これらのフィルタを簡単に作成できます。

コンソールの「属性」タブでフィルタを作成する手順は、次のとおりです。

1. Directory Server の destinationindicator 属性を、Active Directory の activedirectorydomainname 属性および Windows NT の user_nt_domain_name 属性にマッピングします。
2. 各 Windows ドメインの SUL を次のように設定します。

```
EAST_SUL
  Sun Java System Directory Server definition
    Base DN:  ou=people,dc=example,dc=com
    Filter:  destinationindicator=east.example.com
    Creation Expression:  cn=%cn%,ou=people,dc=example,dc=com
Active Directory definition (east.example.com)
    Base DN:  cn=users,dc=east,dc=example,dc=com
    Filter:  <none>
    Creation Expression:
cn=%cn%,cn=users,dc=east,dc=example,dc=com
WEST_SUL
  Sun Java System Directory Server definition
    Base DN:  ou=people,dc=example,dc=com
    Filter:  destinationindicator=west.example.com
    Creation Expression:  cn=%cn%,ou=people,dc=example,dc=com
Active Directory definition (west.example.com)
    Base DN:  cn=users,dc=west,dc=example,dc=com
    Filter:  <none>
    Creation Expression:
cn=%cn%,cn=users,dc=west,dc=example,dc=com
NT_SUL
  Sun Java System Directory Server definition
    Base DN:  ou=people,dc=example,dc=com
    Filter:  destinationindicator=NTEXAMPLE
    Creation Expression:  cn=%cn%,ou=people,dc=example,dc=com
Windows NT definition (NTEXAMPLE)
    Base DN:  NA
    Filter:  <none>
    Creation Expression:  NA
```

各 Directory Server SUL 定義に指定されているベース DN と作成式は同じですが、対応する Windows ユーザーエントリのドメインがフィルタによって特定されることに注意してください。

これらの設定が、Directory Server ユーザーエントリをどのように各 Windows ドメインに同期させているかを示すために、次の事例を考えます。

1. Active Directory ドメイン east.example.com に `cn=Jane Test,cn=users,dc=east,dc=example,dc=com` というエントリを作成します。
2. Identity Synchronization for Windows は、`destinationindicator=east.example.com` という属性を持つユーザーエントリ `cn=Jane Test,ou=people,dc=example,dc=com` を Directory Server に作成します。
3. Directory Server で `cn=Jane Test,ou=people,dc=example,dc=com` エントリに修正を加えます。
4. Jane Test の `destinationindicator` 属性の値は east.example.com であるため、このエントリは同期ユーザーリストフィルタ `EAST_SUL` と一致し、修正は Active Directory ドメイン east.example.com に同期されます。

この例は、Identity Synchronization for Windows が Windows から Directory Server への方向でユーザー作成を同期させることを前提としています。これ以外の場合は、`idsync resync` を実行して `destinationindicator` 属性を設定できます。

注 複数の SUL を使用する配備で `idsync resync -f` を使用する場合、通常はリンク設定ファイルの `allowLinkingOutOfScope` オプションを `true` に設定する必要があります。詳細については、付録 B「LinkUsers XML ドキュメントのサンプル」を参照してください。

この例では、`inetorgperson` オブジェクトクラスの既存の属性 `destinationIndicator` を使用しましたが、この属性が別の目的で使用されている可能性もあります。この属性がすでに使用されている、または別のオブジェクトクラスを選択した場合は、ユーザーの Directory Server エントリで使用できるその他の属性を `user_nt_domain_name`、`activedirectorydomainname`、または両方の属性にマッピングする必要があります。この値を保持するように指定した Directory Server 属性は、その他の属性マッピング設定で使用しているオブジェクトクラスの属性である必要があります。

このドメイン情報を保持できる未使用属性が残されていない場合は、新しいドメイン属性と、Identity Synchronization for Windows で使用されるその他すべての属性を包括した新しいオブジェクトクラスを作成します。

付録 E

レプリケーション環境でのインストールに関する注意

Identity Synchronization for Windows 1 2004Q3 は、レプリケートされた単一サフィックスでのユーザーの同期をサポートしています。

注

この付録では、マルチマスターレプリケーション (MMR) 配備を設定およびセキュリティ保護する方法について説明します。この情報は『Sun Java System Directory Server 5 2005Q1 管理ガイド』から抜き出されたものであり、Identity Synchronization for Windows 専用に用意されたものではありません。

ここに示される情報は概要に過ぎません。
配備の計画については『Sun Java System Directory Server 5 2005Q1 配備計画ガイド』、配備の実装については『Sun Java System Directory Server 5 2005Q1 管理ガイド』を参照してください。

この付録で説明する内容は、次のとおりです。

レプリケーションの設定

注 マルチマスターレプリケーション (MMR) 環境の Identity Synchronization for Windows では、1 つの Sun ディレクトリソースに対して優先マスターサーバーと二次マスターサーバーを指定できます。

新しい Directory Server バージョン 5 2005Q1 は 4 方向の MMR をサポートし、4 つのマスターにレプリケートされたいずれかのデータベースに変更を加えることができます。第 3、第 4 のマスターにプラグインをインストールするときは、プラグインのインストール時にホストの種類として「その他」を選択し、Directory Server インスタンスのパラメータを手動で入力する必要があります。

次の手順は、単一サフィックスのレプリケーションを前提としています。複数のサフィックスをレプリケートする場合は、各サーバーでサフィックスを並行に設定します。言い換えれば、各手順を繰り返すことで、複数サフィックスのレプリケーションを設定できます。

レプリケーショントポロジの設定は、次の順序で行います。

1. 単一マスター以外のすべてのサーバーでレプリケーションマネージャを定義します。または、すべてのサーバーでデフォルトのレプリケーションマネージャを使用します。
2. 専用のコンシューマレプリカを持つすべてのサーバーで次の操作を行います。
   a. コンシューマレプリカ用の空のサフィックスを作成します。
   b. レプリケーションウィザードを使用して、サフィックス上でコンシューマレプリカを有効にします。
   c. オプションとして、高度なレプリカ設定を行います。
3. ハブレプリカを使用する場合、ハブレプリカを持つすべてのサーバーで次の操作を行います。
   a. コンシューマレプリカ用の空のサフィックスを作成します。
   b. レプリケーションウィザードを使用して、サフィックス上でハブレプリカを有効にします。
   c. オプションとして、高度なレプリカ設定を行います。
4. マスターレプリカを持つすべてのサーバーで次の操作を行います。
   a. マスターレプリカとなるいずれかのマスターでサフィックスを選択または作成します。
   b. レプリケーションウィザードを使用して、サフィックス上でマスターレプリカを有効にします。

c. オプションとして、高度なレプリカ設定を行います。

5. すべてのサプライヤレプリカで、レプリケーションアグリーメントを次の順序で設定します。

   a. マルチマスターセットのマスター間

   b. マスターとその専用コンシューマの間

   c. マスターとハブレプリカの間

      オプションとして、部分レプリケーションをこの段階で設定できます。

6. ハブレプリカとそのコンシューマの間のレプリケーションアグリーメントを設定します。

7. マルチマスターレプリケーションでは、オリジナルデータを含む 1 つのマスターレプリカからすべてのマスターを初期化します。ハブとコンシューマレプリカを初期化します。

SSL を介したレプリケーションの設定

注 この手順では、すべての参照先は『Sun Java System Directory Server 5 2005Q1 管理ガイド』内の情報です。

すべてのレプリケーション操作が SSL 接続を経由するように、レプリケーションに関連する Directory Server を設定する手順は、次のとおりです。

1. サプライヤサーバーとコンシューマサーバーの両方を、SSL を使用するように設定します。

   詳細については、第 11 章「認証と暗号化の管理」を参照してください。

   注
   - サプライヤサーバー証明書が、SSL ハンドシェイク時にクライアントとして機能できない SSL サーバー専用の証明書である場合、SSL を介したレプリケーションは失敗する
   - SSL を介したレプリケーションでは、現時点では自己署名証明書だけがサポートされる

2. コンシューマサーバー上のサフィックスにレプリケーションが設定されていない場合は、第 8 章の「コンシューマレプリカの有効化」で説明されている方法で有効化します。

3. 第 8 章の「コンシューマの詳細設定」で説明されている方法で、コンシューマ上の証明書エントリの DN を他のレプリケーションマネージャと同様に定義します。
4. サプライヤサーバー上のサフィックスにレプリケーションが設定されていない場合は、第 8 章の「ハブレプリカの有効化」または「マスターレプリカの有効化」で説明されている方法で有効化します。
5. サプライヤサーバーで、レプリケーションアグリーメントを新規作成し、安全な SSL ポート上のコンシューマに更新を送信します。詳細な方法については、第 8 章の「レプリケーションアグリーメントの作成」で説明されている手順を参照してください。コンシューマサーバーでセキュアポートを指定し、パスワードまたは証明書の使用を指定する SSL オプションを選択します。選択した SSL オプション (レプリケーションマネージャまたは証明書) の DN を入力します。

レプリケーションアグリーメントの設定が完了すると、サプライヤはすべてのレプリケーション更新メッセージを SSL 経由でコンシューマに送信します。証明書を使用するオプションを選択した場合は、証明書が使用されます。SSL が設定されたアグリーメントを使用してコンソールから実行する場合、顧客の初期化にも安全な接続が使用されます。

MMR 環境での Identity Synchronization for Windows の設定

次に、MMR 環境で Identity Synchronization for Windows を設定する手順について、その概要を示します。詳細な手順については、このマニュアルの各該当箇所を参照してください。

1. Identity Synchronization for Windows のコンソールで、同期対象サフィックスの優先および二次 Directory Server マスターを指定します。
104 ページの「Sun Java System ディレクトリソースの作成」を参照してください。

   トポロジに含まれるその他の Directory Server に関する情報を指定する必要はありません。
2. コンソールまたはコマンド行ユーティリティ `idsync prepds` を使用して、優先および二次サーバーを準備します。111 ページの「Directory Server の準備」または 316 ページの「prepds の使用」を参照してください。

   コマンド行ユーティリティを使用する場合は、優先サーバーと二次サーバーの両方の引数を指定し、1 回の実行で両方のサーバーを準備する必要があります。
3. これらのディレクトリの間でレプリケートされるサフィックス用に Directory Server コネクタをインストールします。161 ページの「Directory Server コネクタのインストール」を参照してください。

4. 優先マスター、二次マスター、およびレプリケートされるサフィックスでユーザーを管理するその他すべての Directory Server インスタンスに Directory Server プラグインをインストールします。171 ページの「Directory Server プラグインのインストール」を参照してください。

用語集

次の用語は、Identity Synchronization for Windows 製品と、このドキュメントセット全体で使用されています。

Auxiliary オブジェクトクラス (Auxiliary object class)　選択した Structural クラスを補完し、同期させる追加属性を指定するオブジェクトクラス。「Structural オブジェクトクラス (Structural object class)」を参照。

CA　「認証局 (certificate authority)」を参照。

CLI　「コマンド行インタフェース (command line interface)」を参照。

DIT　「ディレクトリ情報ツリー (directory information tree)」を参照。

DM　「ディレクトリマネージャ (Directory Manager)」を参照。

DNS　ドメインネームシステム。標準の IP アドレス (198.93.93.10 など) をホスト名 (`www.example.com` など) と関連付けるためにネットワーク上のマシンが使用するシステム。通常、マシンはホスト名の IP アドレスを DNS サーバーから取得するか、システムで維持されているテーブルでアドレスを検索する。

FSMO ロール (FSMO Role)　Flexible Single-Master Operation ロールの略称。マルチマスター配備で更新の競合を防止するために Active Directory で使用されるメカニズム。マルチマスターの配備であっても、一部のオブジェクトはシングルマスターモードで更新される。これは、Windows NT ドメインの古い概念である PDC (Primary Domain Controller) に類似する。Active Directory の配備には 5 つの FSMO ロールがあるが、PDC エミュレータロールだけが Identity Synchronization for Windows に影響する。パスワードの更新は PDC エミュレータロールが割り当てられた Active Directory ドメインコントローラだけに迅速にレプリケートされるため、Identity Synchronization for Windows は同期にこのドメインコントローラを使用する。Sun Java System Directory Server とのその他の同期は、数分間の遅延を伴う場合がある。

Identity Synchronization for Windows コンソール　Identity Synchronization for Windows の設定と監視に使用されるグラフィカルユーザーインタフェース。

IP アドレス (IP address)　インターネットプロトコルアドレス。ドットで区切られた一組の数字で、インターネット上にあるマシンの実際の位置を指定する (たとえば、192.168.2.1 など)。

ISO　International Standards Organization (国際標準化機構) の略称。

Java Message Service　Java 2 Platform, Enterprise Edition (J2EE) に準拠するアプリケーションコンポーネントがメッセージを作成、送信、受信、表示するための、メッセージング用の標準 API。これにより、緩やかに結合された、信頼性の高い、非同期の分散通信を行うことができる。

JMS　「Java Message Service」を参照。

LDAP　Lightweight Directory Access Protocol の略称。TCP/IP を介して複数のプラットフォーム間で動作するように設計されたディレクトリサービスプロトコル。Identity Synchronization for Windows は、Active Directory ドメインコントローラと Sun Java System Directory Server との間の通信に LDAP を使用する。

LDAP URL　DNS を使用してディレクトリサーバーを検出し、LDAP を介して照会を完了する方法を提供する。たとえば、`ldap://ldap.example.com` など。

LDAP クライアント (LDAP client)　LDAP Directory Server からの LDAP エントリを要求および表示するために使用されるソフトウェア。LDAP サーバーへの接続時に LDAP クライアントとして機能する Identity Synchronization for Windows コネクタ。

Lightweight Directory Access Protocol　「LDAP」を参照。

Message Queue　「Sun Java System Message Queue」を参照。

MMR　「マルチマスターレプリケーション」を参照。

MQ　「Sun Java System Message Queue」を参照。

RCL　「旧バージョン形式の更新履歴ログ (retro changelog)」を参照。

Secure Sockets Layer　「SSL」を参照。

SSL　Secure Sockets Layer の略称。二者 (クライアントとサーバー) 間でセキュリティ保護された通信を確立するために使用されるソフトウェアライブラリ。HTTP の安全なバージョンである HTTPS と、LDAP の安全なバージョンである LDAPS の実装に使用される。

Structural オブジェクトクラス (Structural object class)　Identity Synchronization for Windows による同期の対象となる、ユーザーエントリの有効属性と必須属性のセットを定義するエントリの主オブジェクトクラス。たとえば、Active Directory のデフォルトのオブジェクトクラスは `user` で、Directory Server のデフォルトのオブジェクトクラスは `inetorgperson` である。「Auxiliary オブジェクトクラス (Auxiliary object class)」を参照。

SUL 「同期ユーザーリスト (Synchronization User List)」を参照。

Sun Java System Message Queue オープン標準である JMS (Java Message Service) を実装するエンタープライズメッセージングシステム。Message Queue の基本アーキテクチャは、共通のサービスを使用してメッセージを交換するパブリッシャとサブスクライバから構成される。Sun Java System Message Queue は、Message Queue へのアクセスの制御、アクティブなパブリッシャとサブスクライバに関する情報の維持、メッセージ配信の確認を行う専用のメッセージブローカによって管理される。Identity Synchronization for Windows は Message Queue を使用して、ユーザー変更イベントの同期、設定情報のやり取り、リモートコンポーネントの状態の監視を安全に行う。

Sun Java System Message Queue ブローカ (Sun Java System Message Queue Broker)

Sun Java System Message Queue にクライアントアクセスを提供するためのスタンドアロン Java サーバー。Solaris 環境では、ブローカの制御に `/etc/init.d/imq daemon` スクリプトが使用され、Windows 環境では「iMQ Broker」サービスが使用される。Identity Synchronization for Windows は、コアのインストール時にブローカの設定と起動を行う。

uid UNIX システム上で、各ユーザーと関連付けられた一意の番号。

URL Uniform Resource Locator の略称。サーバーおよびクライアントが文書の要求に使用するアドレス指定システム。ロケーションとも呼ばれる。URL の形式は、`[protocol]://[machine:port]/[document]`。ポート番号は一部のサーバーだけで必要とされ、多くの場合はサーバーによって割り当てられるため、その場合ユーザーは URL でポート番号を指定する必要はない。

Watchdog コアまたはコネクタがインストールされるすべてのマシンにインストールされる、スタンドアロン Java プロセス。システムマネージャ、セントラルロガー、コネクタなど、Identity Synchronization for Windows のすべての Java プロセスは Watchdog によって起動される。いずれかのコンポーネントが停止した場合、Watchdog はそれを再起動させる。Solaris 環境では、Watchdog の制御に `/etc/init.d/isw` デーモンスクリプトが使用され、Windows 環境では「Sun Java™ System Identity Synchronization for Windows」サービスが使用される。

アウトバウンド (outbound) Message Queue からディレクトリソースへ向かう、コネクタ内でのアクションの方向。コネクタが適用する変更は、同期対象のディレクトリソースに向かって (アウトバウンドに) 送られる。コネクタのアウトバウンド側で発生したイベントは、アクションについてログメッセージを調べる場合によく参照される。

アクション (action) カプセル化された 1 つの同期イベント。Identity Synchronization for Windows コネクタは、アクションを使用してユーザーによる変更イベントをやり取りする。アクションには、タイプ (`CREATE`、`MODIFY`、`DELETE` など) と、送信先のコネクタが変更を同期させるために必要な、ユーザーエントリから取得される属性が含まれる。すべてのアクションはアトミックに処理されます。

アクセサ (accessor)　LDAP などのプロトコルを介してディレクトリソースとのインタフェースを直接提供するコネクタ層。Identity Synchronization for Windows には、Directory Server、Active Directory、Windows NT のそれぞれに専用のアクセサ実装が用意されている。アクセサは、アクションについてログメッセージを調べる場合によく参照される。

インバウンド (inboud)　ディレクトリソースから Message Queue へ向かう、コネクタ内でのアクションの方向。コネクタが検出した変更は、システムに向かって (インバウンドに) 送られる。コネクタのインバウンド側で発生したイベントは、アクションについてログメッセージを調べる場合によく参照される。

エージェント (agent)　Message Queue とのインタフェースを提供し、Directory Server 側の属性名と Windows 側の属性名を相互に変換するコネクタコンポーネント。エージェントは、アクションについてログメッセージを調べる場合によく参照される。

オブジェクトキャッシュ (object cache)　ユーザーエントリへの変更を検出するために Windows コネクタが使用する、プロセス内のデータベース。オブジェクトキャッシュには、各ユーザーエントリのハッシュ化されたサマリーが格納されているため、Windows コネクタは、ユーザーエントリ内のどの属性が変更されたのかを特定できる。

オブジェクトクラス (object class)　あるエントリが意味するオブジェクトの種類、およびそのエントリに含まれる有効属性と必須属性のセットを指定するためのテンプレート。たとえば、Directory Server は `cn`、`userpassword` などの属性を持つ `inetorgperson` オブジェクトクラスを指定します。

オンデマンドパスワード同期　ユーザーが Directory Server に対して認証を試みるまで Directory Server 内のユーザーパスワードを更新しないようにするメカニズム。ユーザーのパスワードは、指定したパスワードが Active Directory に記録されているパスワードと一致した場合にだけ同期される。これにより、Active Directory 環境でのパスワードの同期が簡略化される。

カスケード型レプリケーション (cascading replication)　カスケード型レプリケーションでは、特定のレプリカで 1 つのサーバー (ハブサプライヤとも呼ばれる) がコンシューマとサプライヤの両方として動作する。このサーバーは読み取り専用のレプリカを保持し、更新履歴ログを管理する。また、データのマスターコピーを保持するサプライヤサーバーから更新を受け取り、コンシューマにこの更新を供給する。

監査ログ (audit log)　ユーザーパスワードの同期など、日常的なイベントのエントリが記録されるセントラルログファイル。管理者は、このログに記録されるエントリの数と詳細度を Identity Synchronization for Windows コンソールから制御できる。
各コネクタは、そのコネクタが処理するユーザーの監査ログを生成し、配備に含まれるすべてのコネクタが生成する監査ログの内容はセントラル監査ログに一元的に記録される。

旧バージョン形式の更新履歴ログ (retro changelog)　Directory Server に加えられたすべての変更の記録を格納する Directory Server データベース (cn=changelog)。Identity Synchronization for Windows は、Directory Server に加えられた変更の検出に旧バージョン形式の更新履歴ログを使用する。MMR 環境では、旧バージョン形式の更新履歴ログを優先 Directory Server 上で有効化する必要がある。

クライアント (client)　「LDAP クライアント (LDAP client)」を参照。

グローバルカタログ (global catalog)　Active Directory のディレクトリトポロジと Active Directory ディレクトリのスキーマ情報を記録した Windows リポジトリ。

権限 (permission)　アクセス制御のコンテキスト内で、ディレクトリ情報へのアクセスの許可と拒否、および許可または拒否されるアクセスのレベルを規定する。

コア (Core)　最初にインストールされる Identity Synchronization for Windows コンポーネント。コアは、設定ディレクトリに格納される初期設定、システムマネージャ、セントラルロガー、コンソール、コマンド行インタフェースから構成される。

コネクタ (connector)　Identity Synchronization for Windows と単一データソース (Directory Server、Active Directory ドメイン、Windows NT ドメインなど) の間のやり取りを管理する Java プロセス。コネクタは、ユーザーがデータソースに加えた変更を検出し、これらの変更を Message Queue 経由でリモートコネクタに公開する。また、ユーザー変更トピックに加入し、これらのトピックから取得した更新をデータソースに適用する。

コマンド行インタフェース (command line interface)　プログラムとユーザーの間で、テキストの入出力だけを使用して通信を行う方法。コマンドの入力にはキーボードなどの装置が使用され、プログラムはコマンドを解釈し、それを実行する。Identity Synchronization for Windows のコマンド行インタフェースは `idsync` と呼ばれ、コアのインストールディレクトリ内の `bin/` ディレクトリに格納される。

コンソール (console)　サーバーアプリケーションの設定と監視に使用されるグラフィカルユーザーインタフェース。Sun Java System Directory Server と Identity Synchronization for Windows はそれぞれ異なるコンソールを持つ。

コントローラ (controller)　エージェントコンポーネントとアクセサコンポーネントの間のインタフェースを提供するコネクタコンポーネント。コントローラは、同期ユーザーリストにユーザーが含まれているかどうかの確認、該当ユーザーエントリの検索とリンク設定、現行ユーザーエントリとオブジェクトキャッシュ内の過去のバージョンとの比較による変更の検出など、同期に関連する重要なタスクを実行する。コントローラは、アクションについてログメッセージを調べる場合によく参照される。

サーバーコンソール (Server Console)　GUI を利用して Directory Server を管理するための Java ベースのアプリケーション。

サーバールート (server root)　サーバープログラムの設定、管理、情報が記録されたファイルを格納する、サーバーマシン上の専用ディレクトリ。

サービス (service)　特定のシステムタスクを受け持つ、Windows マシン上のバックグラウンドプロセス。サービスプロセスは、動作を続けるためにユーザーの介入を必要としない。Windows 環境では、コネクタ、システムマネージャ、およびセントラルロガーは Identity Synchronization for Windows Watchdog サービスによって起動、監視されるプロセスとして実行される。

再同期間隔 (resync interval)　コネクタがディレクトリソース内の変更を確認する頻度。前回の確認後に変更されたユーザーのエントリだけを読み込むことになるため、この定期的な確認は効率的である。コンソールでは、この値はミリ秒単位で表示される。デフォルトは 1000 (1 秒)。

作成属性 (creation attributes)　オブジェクトの作成時にだけ同期される属性。重要な属性は、オブジェクトの作成時にすべて自動的に同期される。リモートディレクトリに対応する属性値が存在しない場合に備え、作成属性にデフォルト値を設定しておくことができる。

サフィックス (suffix)　ディレクトリツリーの頂点にあるエントリの名前で、この下にデータが格納される。同じディレクトリ内に複数のサフィックスが存在できる。各データベースはサフィックスを 1 つだけ持つ。

サブコンポーネント (subcomponent)　コネクタから独立して実行される軽量のプロセスまたはライブラリ。サブコンポーネントは、コネクタが管理するディレクトリソースの近くで実行され、リモートマシンや別のプロセスでは利用できないコネクタの機能を利用できるようにする。設定情報の取得、変更イベントのレポート、セントラルロガーへの記録を行うときに、サブコンポーネントは暗号化されたカスタムチャネルを通じてコネクタと通信する。Identity Synchronization for Windows には、Directory Server プラグイン、Windows NT パスワードフィルタ DLL、Windows NT 変更ディテクタの 3 種類のサブコンポーネントがある。

識別名 (distinguished name)　エントリの名前と LDAP ディレクトリ内での位置を文字列で表したもの。

システムマネージャ (System Manager)　コアがインストールされているマシンの Watchdog デーモンまたはサービスによって起動される、スタンドアロン Java プロセス。システムマネージャは、コネクタとセントラルロガーへの設定情報の伝達、システムの状態監視、`idsync resync` 処理の調整を行う。

受信通知 (acknowledgement)　別のコンポーネントからのメッセージの受信を確認するための特別なメッセージ。Identity Synchronization for Windows では、すべての変更が確実に同期されていることを確認するために、コネクタと Message Queue の間、およびコネクタコンポーネント (エージェント、コントローラ、アクセサ) 間で受信通知が使用される。

証明書 (certificate)　公開鍵とネットワークのアイデンティティを関連付けるデータの集合。この情報により、電子メッセージの受信者はメッセージとメッセージの送信者の信頼性を検証できる。SSL 通信を使用するように Identity Synchronization for Windows コネクタを設定する場合、信頼される SSL 通信を行うには、事前に証明書をコネクタの証明書データベースに追加する必要がある。「認証局 (certificate authority)」も参照。

証明書データベース (certificate database)　セキュリティ保護された証明書リポジトリで、`cert8.db`、`key3.db`、`secmod.db` の 3 ファイルから構成される。Identity Synchronization for Windows では、各コネクタに専用の証明書データベースディレクトリがある (たとえば *<install-root>*`/etc/CNN100` など) 「証明書 (certificate)」も参照。

スーパーユーザー (superuser)　「ルート」を参照。

スキーマ (schema)　ディレクトリにどのようなタイプの情報をエントリとして格納できるかについての定義。スキーマと一致しない情報がディレクトリに格納されている場合、そのディレクトリにアクセスを試みているクライアントが正しい結果を表示できないことがある。

スキーマ検査 (schema checking)　ディレクトリ内で追加または変更されたエントリが、定義したスキーマに確実に従うことを確認する。スキーマ検査はデフォルトで有効化されており、スキーマに従わないエントリを格納しようとした場合、エラーメッセージが表示される。

設定ディレクトリ (configuration directory)　設定情報と状態情報のリポジトリとして機能する Directory Server の特殊なインストール。Identity Synchronization for Windows は、コアのインストール時に指定された設定ディレクトリ内にすべての設定情報を記録する。

設定パスワード (configuration password)　Identity Synchronization for Windows の設定ディレクトリに記録されるすべての機密情報を保護するために、コアのインストール時に指定するパスワード。インストーラ、コンソール、コマンド行インタフェースを使用するときは、常に設定パスワードを入力する必要がある。

設定レジストリ (configuration registry)　Identity Synchronization for Windows の設定ディレクトリと同義。

セントラルロガー (sentral logger)　すべてのコネクタの監査ログとエラーログの集合であるセントラルログをすべて管理するコアコンポーネント。管理者はこれらのログを監視することで Identity Synchronization for Windows のインストール全体の状態を監視できる。セントラルログは、直接参照することも、Identity Synchronization for Windows コンソールから参照することもできる。デフォルトでは、セントラルログはコアがインストールされているマシンの *<install-root>*`/logs/central/` サブディレクトリに保存される。

属性 (attribute)　エントリを説明する情報を保持する。属性にはラベルと値がある。また、各属性は、属性値として格納される情報のタイプに応じた標準の構文に従う。

属性リスト (attribute list)　特定のエントリタイプまたはオブジェクトクラスに対応する、必須の属性と省略可能な属性のリスト。

デーモン (daemon)　特定のシステムタスクを担当する、UNIX マシン上のバックグラウンドプロセス。デーモンプロセスは、動作の継続に人の介入を必要としない。コネクタ、システムマネージャ、およびセントラルロガーはデーモンプロセスとして実行され、Identity Synchronization for Windows Watchdog によって起動、監視される。

ディレクトリ情報ツリー (directory information tree)　ディレクトリに格納された情報の論理表現。ほとんどのファイルシステムで使用されているツリーモデルと同様に、階層の最上位がツリーのルートとして表示される。

ディレクトリソース (directory source)　Sun Java System Directory Server、Windows Active Directory ドメイン、または Windows NT ドメイン。ディレクトリソースには、同期対象のユーザーが含まれる。

ディレクトリマネージャ (Directory Manager)　UNIX のルートユーザーに相当する、特権を持ったディレクトリサーバー管理者。Identity Synchronization for Windows で特定の設定操作を行うには、ディレクトリマネージャのクレデンシャルが必要となる。ただし、コネクタが同期を行う場合にディレクトリマネージャのクレデンシャルが要求されることはない。

同期させる属性 (synchronized attributes)　「有効属性」を参照。

同期ホスト (synchronization host)　同期ユーザーリスト (SUL) に定義されたルールに従って同期データが格納されるサーバー。

同期ユーザーリスト (Synchronization User List)　Sun と Windows のディレクトリに含まれるユーザーの中で、どのユーザーを同期対象とするかを定義する。同期ユーザーリストを使用して、同期対象ユーザーの範囲を LDAP ベース DN またはフィルタに基づいて制限することができる。

トポロジ (topology)　ディレクトリツリーが複数の物理的なサーバーにまたがって、どのように分割されているか、およびこれらのサーバーが相互にどのようにリンクをしているかを示す。

ドメイン (domain)　(1) (n.) ドメイン名を所有する企業または組織を識別するための完全修飾ドメイン名の最後の部分 (たとえば、example.com、host.example.com など)。

(2) (n.) 1 つのコンピュータシステムによって制御されるリソース。

ドメインコントローラ (domain controller)　Windows ドメインでユーザーアカウント情報の格納、ユーザーの認証、セキュリティポリシーの適用を行う Windows サーバー。Identity Synchronization for Windows コネクタは、ドメインコントローラと直接通信し、ユーザーアカウントへの変更の検出、および Directory Server ユーザーエントリに加えられた変更の同期を行う。

二次ディレクトリサーバー　MMR 環境で、優先ディレクトリサーバーが使用不可能な場合に Identity Synchronization for Windows が使用するディレクトリサーバーマスターインスタンス。優先ディレクトリサーバーが使用不可能な状態にあっても、Identity Synchronization for Windows は Active Directory または Windows NT で加えられた変更であれば、二次ディレクトリサーバー上で同期させることができる。ただし、二次サーバーまたは他のディレクトリサーバーマスターで加えた変更は、優先ディレクトリサーバーが使用可能な状態に戻るまで同期されない。

認証 (authentication)　クライアントユーザーの ID を Directory Server に対して示すプロセス。ユーザーがディレクトリへのアクセスを許可されるには、バインド DN および対応するパスワードを提示する必要がある。ディレクトリ管理者がユーザーに許可したアクセス権に基づき、Directory Server はユーザーに機能の実行やファイルおよびディレクトリへのアクセスを許可する。

認証局 (certificate authority)　認証証明書を販売および発行する企業または組織。認証証明書は、信頼する認証局 (CA とも呼ばれる) から購入できる。別の証明書への署名には、ルート認証局証明書が使用される。SSL を使用するように Identity Synchronization for Windows コネクタを設定するときは、適切なルート認証局証明書をコネクタの証明書データベースに追加する必要がある。

認証証明書 (authentication certificate)　譲渡または偽造することのできない、第三者が発行する電子ファイル。認証証明書は、他方を検証し認証するために、サーバーからクライアントへ、あるいはクライアントからサーバーへ送信される。

ネーミングコンテキスト (naming context)　識別名 (DN) によって特定される、ディレクトリ情報ツリー (DIT) の特殊なサフィックス (たとえば、dc=example,dc=com など)。ルートサフィックスとも呼ばれる。Identity Synchronization for Windows では、Sun Java System Directory Server のディレクトリソースは同期対象データを含むサフィックスによって定義される。

バインド DN (bind DN)　操作を実行するときに LDAP ディレクトリ (Active Directory または Directory Server) に対する認証に使用される識別名。

バインド識別名 (bind distinguished name)　「バインド DN (bind DN)」を参照。

パスワードファイル (password file)　UNIX ユーザーのログイン名、パスワード、およびユーザー ID 番号が格納されている UNIX マシン上のファイル。格納場所に由来して、`/etc/passwd` とも呼ばれる。

パスワードポリシー (password policy)　ディレクトリ内でのパスワードの使い方の基準となる規則のセット。

ファイル拡張子 (file extension)　一般にファイルの種類を定義する、ファイル名のピリオドまたはドット (.) より後ろの部分 (たとえば、.GIF、.HTML など)。たとえば、ファイル名が `index.html` であれば、ファイル拡張子は *html* である。

ファイルタイプ (file type)　特定のファイルの形式。たとえば、グラフィックファイルは `GIF` 形式で保存される場合が多く、テキストファイルは通常 `ASCII` テキスト形式で保存される。通常、ファイルタイプは「ファイル拡張子 (file extension)」で識別される (たとえば、.GIF、.HTML など)。

プラグイン (plug-in)　読み込み後、システムの一部として使用できるアクセサリプログラム。

たとえば、Identity Synchronization for Windows は Directory Server プラグインを使用して Directory Server コネクタの変更検出機能を拡張することで、Active Directory と Directory Server の間で双方向のパスワード同期をサポートする。

ブローカ (Broker) 「Sun Java System Message Queue ブローカ (Sun Java System Message Queue Broker)」を参照。

プロトコル (protocol) ネットワーク上のデバイスが情報を交換する方法を記述した規則のセット。

ベース DN (base DN) ベース識別名。検索処理はベース DN に対して行われる。ベース DN とは、ディレクトリツリー内でエントリおよびその下にあるすべてのエントリの DN のこと。Active Directory と Directory Server では、同期ユーザーリストは特定のベース DN をルートとする。フィルタによって明示的に対象から外される場合を除き、このベース DN の下のすべてのユーザーが同期される。

ベース識別名 (base distinguished name) 「ベース DN (base DN)」を参照。

ホスト名 (hostname) machine.domain.com のような書式のマシン名で、IP アドレスに変換される。たとえば、`www.example.com` は、*com* ドメインの *example* サブドメインにある *www* マシンである。

マルチマスターレプリケーション ディレクトリサーバーのレプリケーションモデル。マスターレプリカの複数のコピーのどれを使用しても、エントリの書き込みと更新を行える。書き込みまたは更新の前に、他のマスターレプリカと通信を行う必要はない。1 つのサーバーに対する変更は、自動的にほかのサーバーにもレプリケートされる。Identity Synchronization for Windows は、複数のディレクトリサーバーマスターを持つ配備にもインストールできる。ただし、変更を Windows と同期させる場合は、優先ディレクトリサーバーが使用可能な状態にある必要がある。また、Windows からの変更を同期させる場合は、優先または二次ディレクトリサーバーが使用可能な状態でなければならない。

メインオブジェクトクラス (main object class) 「Structural オブジェクトクラス (Structural object class)」を参照。

有効属性 エントリの作成時または変更時に同期される属性。

優先ディレクトリサーバー (preferred directory server) Identity Synchronization for Windows がユーザーエントリの変更の検出と適用に使用する、ディレクトリサーバーのマスターインスタンス。このサーバーが使用可能な状態にある場合、Identity Synchronization for Windows は他のディレクトリサーバーマスターと通信を行わない。

ルート UNIX マシン上でもっとも高いレベルの特権を持つユーザー。スーパーユーザーとも呼ばれる。ルートユーザーは、マシン上のすべてのファイルに対して完全なアクセス権限を持つ。Solaris システムでは、Identity Synchronization for Windows のインストールは、ルートとしてログインしたユーザーが行う必要がある。

ルートサフィックス (root suffix)　1 つまたは複数の LDAP サブサフィックスの親。ディレクトリツリーは複数のルートサフィックスを含むことができる。

ロケール (locale)　住む地域や、文化、習慣の異なるユーザーが、データを表すために使用するもので、照合順序、文字タイプ、通貨形式、時刻 / 日付の形式を識別する。ロケールには、特定言語のデータの解釈方法、格納方法、または照合方法に関する情報が含まれる。また、特定言語を表現するために使用するコードページを提供する。

文字タイプ (character type)　英字を、数字またはほかの文字と識別し、また大文字から小文字へのマッピングを識別する。

索引

B

C

D

E

F

I

J

K

L

M

N

O

P

R

S

T

U

W

X

あ

い

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

つ

て

と

な

に

ね

は

ひ

ふ

へ

ほ

ま

む

め

ゆ