Sun Identity Manager 8.1 リソースリファレンス

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

Part No: 821–0779–10
2009 年 10 月

091118@22749

目次

はじめに

『Sun Identity Manager 8.1 リソースリファレンス』では、リソースに接続する場合、および接続したリソースのアカウントを管理する場合に役立つ参照情報と手順について説明します。

対象読者

『Sun™ Identity Manager リソースリファレンス』は、Identity Manager を設定および配備してリソースを管理するデプロイヤおよび管理者を対象としています。

デプロイヤは、プログラミングに関する予備知識があり、XML、Java、Emacs や IDE (Eclipse または NetBeans など) に精通していることが望まれます。

管理者にはプログラミングに関する予備知識は必ずしも必要ではありませんが、LDAP、Active Directory、SQL などのリソースドメインの 1 つ以上について、高度に熟練していることが望まれます。

お読みになる前に

本書を読む前に、『『Sun Identity Manager の概要』』の内容を理解しておいてください。

内容の紹介

『Identity Manager リソースリファレンス』は、次の章で構成されています。

- 第 1 章「リソースリファレンスの概要」。Identity Manager リソースアダプタベースのリソースでの、インストール、設定、および実装に関する情報を説明します。
- サポートされている各アダプタベースのリソースに関する章。これらの章はアルファベット順に示しています。
- 第 49 章「AttrParse オブジェクトの実装」。AttrParse 機能をカスタマイズするために必要な情報を説明しています。メインフレームベースのリソースアダプタは、この機能を使用してリソースから情報を抽出します。

- 第 50 章「リソースへのアクションの追加」。Identity Manager のさまざまなタイプのリソースに対して、アクションを作成および実装する方法について説明します。
- 第 51 章「LDAP パスワードの同期」。Sun Java™ System Directory Server から Identity Manager システムへのパスワード同期をサポートする、Identity Manager 製品の拡張機能を説明します。
- 第 52 章「Active Directory Synchronization Failover」。新しいドメインコントローラに切り替えたときに発生する、繰り返しイベントの数を制限する方法について説明します。
- 第 53 章「メインフレーム接続」。IBM の Host on Demand や Attachmate 3270 Mainframe Adapter for Sun Emulator Class Library を使用して、メインフレームリソースに接続する方法について説明します。
- 第 54 章「SNC (Secure Network Communications) 接続の有効化」。Access Enforcer、SAP、および SAP HR リソースアダプタで、SNC (Secure Network Communications) を使用して安全に SAP システムと通信する方法について説明します。
- 第 55 章「非推奨のリソースアダプタ」。サポートが終了したリソースアダプタの一覧を示します。
- 第 56 章「アイデンティティーコネクタの概要」。この章ではアイデンティティーコネクタを紹介します。これは、Identity Manager で新しくサポートされた機能です。コネクタは、リソースアダプタに代わって、ネイティブリソースのアイデンティティーとその他のオブジェクトタイプをマッピングします。
- サポートされている各コネクタベースのリソースに関する章。これらの章はアルファベット順に示しています。

関連マニュアル

Sun Identity Manager 8.1 のドキュメントセットには、次のマニュアルが含まれています。

主な対象読者	タイトル	説明
すべてのユーザー	『Sun Identity Manager の概要』	Identity Manager の機能についての概要を説明しています。製品のアーキテクチャー情報や、Identity Manager を Sun Open SSO Enterprise や Sun Role Manager などの他の Sun 製品と統合する方法について説明しています。
	『Sun Identity Manager 8.1 リリースノート』	既知の問題、修正された問題、および Identity Manager のドキュメントセットに記載されていない最新の情報を説明しています。
システム管理者	『Installation Guide』	Identity Manager と、Sun Identity Manager Gateway や PasswordSync などのオプションコンポーネントをインストールする方法を説明しています。
	『Upgrade Guide』	古いバージョンの Identity Manager を新しいバージョンにアップグレードする方法について説明しています。
	『System Administrator's Guide』	システム管理者が Identity Manager のインストールを管理、調整、およびトラブルシューティングする際に役立つ情報と操作方法を説明しています。
ビジネス管理者	『Business Administrator's Guide』	Identity Manager のプロビジョニングおよび監査機能の使用方法を説明しています。ユーザーインタフェース、ユーザーとアカウントの管理、レポート機能などの情報についても説明しています。

主な対象読者	タイトル	説明
システムインテグレータ	『Deployment Guide』	Identity Manager を複雑な IT 環境に配備する方法を説明しています。アイデンティティー属性、データの読み込みと同期、ユーザーアクションの設定、カスタムブランディングの適用などの話題も説明しています。
	『Deployment Reference』	ワークフロー、フォーム、ビュー、ルール、および XPRESS 言語について説明しています。
	『Resources Reference』	リソースアダプタのインストール、設定、および使用方法の情報を説明しています。
	『Service Provider 8.1 Deployment』	Identity Manager Service Provider の配備方法と、ビュー、フォーム、およびリソースの標準 Identity Manager 製品との違いを説明しています。
	『Web Services Guide』	SPML サポートの設定方法、サポートされる SPML 機能とサポートの理由、およびフィールドでサポートを拡張する方法について説明しています。

ドキュメントの更新

Sun Identity Manager のドキュメントに対する修正と更新は、Identity Manager Documentation Updates の Web サイトで公開されます。

`http://blogs.sun.com/idmdocupdates/`

RSS フィードリーダーを使用して Web サイトを定期的に確認し、更新を利用できる場合に通知を受けることができます。サイトを購読するには、フィードリーダーをダウンロードして、ページの右側の「Feeds」の下にあるリンクをクリックします。バージョン 8.0 から、メジャーリリースごとのフィードを利用できます。

関連するサードパーティー Web サイト

このドキュメントでは、サードパーティー URL を参照して、追加の関連情報を提供します。

注 – このドキュメントで取り上げる他社の Web サイトが使用可能かどうかについて、Sun は関知いたしません。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、または生じたと主張される、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、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。

ドキュメント、サポート、トレーニング

Sun の Web サイトでは、次の追加リソースに関する情報を入手できます。

- ドキュメント (http://www.sun.com/documentation/)
- サポート (http://www.sun.com/support/)
- トレーニング (http://www.sun.com/training/)

ご意見、ご要望の送付先

Sun ではドキュメントの品質向上のため、お客様のご意見、ご要望をお受けしております。ご意見をお寄せいただくには、http://docs.sun.com にアクセスして、「Feedback」をクリックしてください。

書体の表記規則

次の表は、本書で使用する表記上の規則について説明しています。

表 P–1　書体の表記規則

字体または記号	意味	例
AaBbCc123	コマンド名、ファイル名、ディレクトリ名、画面上のコンピュータ出力を示します。	.login ファイルを編集します。 すべてのファイルを一覧表示するには、ls -a を使用します。 machine_name% you have mail.

表 P–1 書体の表記規則 (続き)

字体または記号	意味	例
AaBbCc123	ユーザーが入力する文字を、画面上のコンピュータ出力とは区別して示します。	machine_name% **su** Password:
aabbcc123	変数を示します。実際の名前または値で置き換えます。	ファイルを削除するコマンドは、rm *filename* です。
AaBbCc123	書名、新しい用語、強調する語句を示します。	『ユーザーズガイド』の第 6 章を参照してください。 キャッシュは、ローカルに保存されたコピーです。 ファイルを保存しないでください。 注意: 一部の強調語句は、オンラインでは太字で示されます。

コマンドのシェルプロンプトの例

次の表は、C シェル、Bourne シェル、および Korn シェルの、デフォルトの UNIX® システムプロンプトとスーパーユーザーのプロンプトを示しています。

表 P–2 シェルプロンプト

シェル	プロンプト
C シェル	machine_name%
C シェル (スーパーユーザーの場合)	machine_name#
Bourne シェルおよび Korn シェル	$
Bourne シェルおよび Korn シェル (スーパーユーザーの場合)	#

注 – Windows のコマンド行プロンプトは C:\ です。

◆ ◆ ◆ 第 1 章

1 リソースリファレンスの概要

この章では、Identity Manager のインストールによって提供されるリソースアダプタとアイデンティティーコネクタについて説明します。

アダプタのタイプ

次の表に、提供されるアダプタをタイプ順に、サポートされるバージョン、Active Sync のサポート、接続方法、および通信プロトコルの概要とともに示します。サポートされる各リソースのバージョンを確認するには、リリースノートを参照してください。

リソースアダプタは、次のカテゴリに分類されます。

- CRM および ERP システム
- データベース
- ディレクトリ
- メッセージプラットフォーム
- その他
- オペレーティングシステム
- セキュリティーマネージャー
- Web シングルサインオン (SSO)

表 1–1 CRM および ERP システム

リソースアダプタ	サポートされるアプリケーション	Active Sync のサポート	ゲートウェイ	通信プロトコル
Oracle アプリケーション	Oracle Financials on Oracle Applications	なし	なし	JDBC

表 1–1 CRM および ERP システム (続き)

リソースアダプタ	サポートされるアプリケーション	Active Sync のサポート	ゲートウェイ	通信プロトコル
PeopleSoft コンポーネント	PeopleTools People Tools with HRMS	あり Smart ポーリング、リスナー	なし	Client Connection Toolkit (同期のみ)
PeopleSoft コンポーネントインタフェースアダプタ	PeopleTools	なし	なし	Client Connection Toolkit (読み取り/書き込み)
SAP	SAP R/3	なし	なし	SAP Java Connector 経由の BAPI
	SAP HR	あり Smart ポーリング、リスナー		ALE
	Governance, Risk, and Compliance (GRC) Access Enforcer	なし	なし	SAP Java Connector 経由の BAPI
	Enterprise Portal	なし	なし	Siebel Data API

表 1–2 データベース

リソースアダプタ	Active Sync のサポート	ゲートウェイ	通信プロトコル
DB2	なし	なし	JDBC、SSL
Microsoft SQL Server	なし	なし	JDBC、SSL
MySQL	なし	なし	JDBC、SSL
Oracle	なし	なし	JDBC、SSL
Sybase	なし	なし	JDBC、SSL

表 1–3 ディレクトリ

リソースアダプタ	サポートされるアプリケーション	Active Sync のサポート	ゲートウェイ	通信プロトコル
LDAP		あり Smart ポーリング、リスナー	なし	LDAP v3、JNDI、SSL
Microsoft Active Directory		あり Smart ポーリング	あり	ADSI
NetWare NDS	Netware eDirectoryNovell SecretStore	あり Smart ポーリング	あり	NDS クライアント、LDAP、SSL

表 1–4 メッセージプラットフォーム

リソースアダプタ	Active Sync のサポート	ゲートウェイ	通信プロトコル
Lotus Domino Gateway	あり Smart ポーリング	あり	RMI、IIOP (Toolkit for Java、CORBA を使用)
Novell GroupWise	なし	あり	NDS クライアント、LDAP、SSL

表 1–5 その他

リソースアダプタ	Active Sync のサポート	ゲートウェイ	通信プロトコル
データベーステーブル	あり Smart ポーリング	なし	JDBC
フラットファイル ActiveSync	あり Smart ポーリング (TSS 監査イベントをフィルタ)	なし	
INISafe Nexess		com.initech.eam.api クラス	
JMS リスナー	あり	なし	リソースごとに異なる
Microsoft Identity Integration Server	なし	なし	JDBC
Remedy Help Desk	あり Smart ポーリング	あり	Remedy API
Scripted Gateway		あり	リソースごとに異なる
スクリプトホスト		なし	TN3270
Sun Java™ System Communications Services	あり	なし	SSL または TCP/IP 経由の JNDI

表 1–6 オペレーティングシステム

リソースアダプタ	Active Sync のサポート	ゲートウェイ	通信プロトコル
AIX	なし	なし	Telnet、SSH、SSHPubKey
HP-UX	なし	なし	Telnet、SSH、SSHPubKey
OS/400	なし	なし	Java toolkit for AS400
Red Hat Linux	なし	なし	Telnet、SSH、SSHPubKey
Solaris	なし	なし	Telnet、SSH、SSHPubKey

表 1–6 オペレーティングシステム (続き)

リソースアダプタ	Active Sync のサポート	ゲートウェイ	通信プロトコル
SuSE Linux アダプタ	なし	なし	Telnet、SSH、SSHPubKey

表 1–7 セキュリティーマネージャー

リソースアダプタ	Active Sync のサポート	ゲートウェイ	通信プロトコル
ACF2	なし	なし	Secure TN3270
ClearTrust	なし	なし	Server Proxy API、JNDI、SSL
RACF	なし	なし	Secure TN3270
SecurID ACE/Server (Windows および UNIX)	なし	あり SecurID TCL インタフェース	SecurID Admin API、SSHPubKey (UNIX のみ)
Top Secret	あり Smart ポーリング (TSS 監査イベントをフィルタ)	なし	Secure TN3270

表 1–8 Web シングルサインオン (SSO)

リソースアダプタ	Active Sync のサポート	ゲートウェイ	通信プロトコル
IBM/Tivoli Access Manager	なし	なし	JNDI、SSL
Netegrity Siteminder	なし	なし	Netegrity SDK、JNDI、SSL
Sun Access Manager	なし	なし	JNDI、SSL

Identity Manager のアダプタは、多くの場合デフォルトの状態で使用できます。

▼ アダプタを有効にする

1 この章の「**Identity Manager** のインストールに関する注意事項」で説明されている、アダプタのインストールと設定の手順に従います。

2 『**Business Administrator's Guide**』の説明に従い、リソースウィザードを使用してリソースを **Identity Manager** に追加します。

カスタムアダプタの作成については、『[Title_Deploy_Tools テキストエンティティーを定義してください]』を参照してください。

アダプタに関する節の内容の紹介

この章のリソースアダプタに関する節は、次のように構成されています。

- 「はじめに」。サポートされるリソースのバージョンを一覧に示します。このリストに対する更新情報については、最新のサービスパックバージョンに付属している Readme ファイルを参照してください。
- 「リソースを設定する際の注意事項」。Identity Manager からリソースを管理できるようにするために、リソース上で実行する追加の手順を示します。
- 「Identity Manager のインストールに関する注意事項」。リソースを操作するために必要なインストールと設定の手順を説明します。
- 「使用上の注意」。リソースの使用に関する依存関係と制限を一覧に示します。
- 「セキュリティーに関する注意事項」。サポートされる接続のタイプと、基本的なタスクを実行するためにリソースで必要な認証について説明します。
- 「プロビジョニングに関する注意事項」。アダプタで、アカウントの有効化と無効化やアカウント名の変更などのタスクを実行できるかどうか、およびパススルー認証を許可するかどうかを一覧に示します。
- 「アカウント属性」。リソースでサポートされるデフォルトユーザー属性について説明します。
- 「リソースオブジェクトの管理」。アダプタで管理できるオブジェクトの一覧を示します。
- 「アイデンティティーテンプレート」。リソースアイデンティティーテンプレートの構築または操作に関する注意事項を説明します。
- 「サンプルフォーム」。カスタムのユーザー作成フォームおよびユーザー更新フォームの作成に使用できる、サンプルフォームの場所を説明します。特に指定がないかぎり、サンプルフォームは *InstallDir*`\idm\sample\forms\` ディレクトリに置かれています。
- 「トラブルシューティング」。トレースとデバッグに使用できるクラスの一覧を示します。

各トピックの詳細については、この節の残りの部分で説明します。

トピックの説明

ここでは、各アダプタに関する情報を提供します。 それぞれのトピックが次のように構成されています。

はじめに

この節では、アダプタでサポートされるリソースのバージョンを一覧に示します。これ以外にもサポートされているバージョンがあるかもしれませんが、それらはテストが完了していません。

ここでは、アダプタの Java クラス名の一覧も示します。クラス名はトレース時に常に使用されます。また、リソースがカスタムリソースである場合は、クラス名を「管理するリソースの設定」ページで指定する必要があります。カスタムリソースについては、39 ページの「Identity Manager のインストールに関する注意事項」を参照してください。

リソースの中には、複数のアダプタを備えているものもあります。たとえば、Identity Manager は Windows Active Directory と Windows Active Directory ActiveSync 用のアダプタを提供しています。このような場合、「概要」の節には次のような表が示されます。

GUI 名	Class Name
Windows 2000 / Active Directory	`com.waveset.adapter.ADSIResourceAdapter`
Windows 2000 / Active Directory ActiveSync	`com.waveset.adapter.ActiveDirectoryActiveSyncAdapter`

GUI 名は、「リソース」ページにドロップダウンメニューで表示されます。この名前は、リソースを Identity Manager に追加すると、リソースのブラウザに表示されます。

リソースを設定する際の注意事項

この節では、Identity Manager からリソースを管理するためにリソースで実行する必要がある追加手順を説明します。Identity Manager との接続を確立するには、リソースが完全に機能していることが前提です。

Identity Manager のインストールに関する注意事項

インストールの観点から、アダプタには 2 つのタイプがあります。

- Identity Manager アダプタ
- カスタムアダプタ

Identity Manager アダプタには、追加のインストール手順は必要ありません。次の手順を使用して、リソースを「リソース」ページのアクションメニューに表示します。

▼ リソースを「リソース」ページのアクションメニューに表示する

1. **Identity Manager** 管理インタフェースで、「リソース」をクリックし、次に「タイプの設定」をクリックします。
2. **Identity Manager** の「リソース」セクションで、適切なオプションを選択します。
3. ページの下部にある「保存」をクリックします。

   カスタムアダプタでは、追加のインストール手順が必要です。通常は、1 つ以上の JAR ファイルを *InstallDir*`\idm\WEB-INF\lib` ディレクトリにコピーし、アダプタの Java クラスをアダプタのリストに追加します。JAR ファイルは通常、インストールメディアから入手するか、インターネットからダウンロードすることができます。

   次の例は、DB2 対応のリソースアダプタについて、この手順を示したものです。
4. `db2java.jar` ファイルを *InstallDir*`\idm\WEB-INF\lib` ディレクトリにコピーします。
5. **Identity Manager** 管理者インタフェースで、「リソース」をクリックし、次に「タイプの設定」をクリックします。
6. ページの下部にある「カスタムリソースの追加」をクリックします。
7. 下部のテキストボックスに、アダプタの完全なクラス名 (たとえば、`com.waveset.adapter.DB2ResourceAdapter`) を入力します。
8. ページの下部にある「保存」をクリックします。

   次の表に、Identity Manager サーバーで JAR ファイルのインストールが必要なアダプタを示します。

アダプタ	必要なファイル
Access Enforcer	■ sapjco.jar ■ axis.jar ■ commons-discovery-0.2.jar ■ commons-logging-1.0.4.jar ■ jaxrpc.jar ■ log4j-1.2.8.jar ■ saaj.jar ■ wsdl4j-1.5.1.jar
Access Manager	pd.jar
ACF2	habeans.jar または ■ habase.jar ■ hacp.jar ■ ha3270.jar ■ hassl.jar ■ hodbase.jar または ■ RWebSDK.jar ■ wrqtls12.jar ■ profile.jaw
ClearTrust	ct_admin_api.jar
DB2	db2java.jar
INISafe Nexess	■ concurrent.jar ■ crimson.jar ■ external-debug.jar ■ INICrypto4Java.jar ■ jdom.jar ■ log4j-1.2.6.jar

アダプタ	必要なファイル
MS SQL Server	Microsoft SQL Server 2005 JDBC Driver と接続する場合 ■ `mssqlserver.jar` Microsoft SQL Server 2000 JDBC Driver と接続する場合 ■ `msbase.jar` ■ `mssqlserver.jar` ■ `msutil.jar`
MySQL	`mysqlconnector-java-`*Version* `-bin.jar`
Oracle および Oracle ERP	`oraclejdbc.jar`
PeopleSoft コンポーネントおよび PeopleSoft コンポーネントインタフェース	`psjoa.jar`
RACF	`habeans.jar` または ■ `habase.jar` ■ `hacp.jar` ■ `ha3270.jar` ■ `hassl.jar` ■ `hodbase.jar` または ■ `RWebSDK.jar` ■ `wrqtls12.jar` ■ `profile.jaw`
SAP	■ `sapjco.jar` ■ `sapidoc.jar`
SAP HR ActiveSync	■ `sapjco.jar` ■ `sapidoc.jar` ■ `sapidocjco.jar`

アダプタ	必要なファイル
Scripted Host	habeans.jar または ■ habase.jar ■ hacp.jar ■ ha3270.jar ■ hassl.jar ■ hodbase.jar または ■ RWebSDK.jar ■ wrqtls12.jar ■ profile.jaw
Siebel CRM	■ Siebel 7.0: ■ SiebelJI_Common.jar ■ SiebelJI_enu.jar ■ SiebelJI.jar Siebel 7.7、7.8 ■ Siebel.jar ■ SiebelJI_enu.jar
SiteMinder	■ smjavaagentapi.jar ■ smjavasdk2.jar
Sun Access Manager	7.0 より前のバージョン: ■ リリースによって異なる Version 7.0 以降 ■ am_sdk.jar ■ am_services.jar
Sun Java System Access Manager Realm	■ am_sdk.jar ■ am_services.jar
Sybase	jconn2.jar

アダプタ	必要なファイル
Top Secret	habeans.jar または ■ habase.jar ■ hacp.jar ■ ha3270.jar ■ hassl.jar ■ hodbase.jar または ■ RWebSDK.jar ■ wrqtls12.jar ■ profile.jaw

使用上の注意

ここでは、リソースの使用に関連する依存関係と制限について示します。この節で説明する内容は、アダプタによって異なります。

ActiveSync 設定

この節では、「Edit Synchronization Policy」ページで表示可能な、リソースに固有の設定情報を説明します。次の属性は、ほとんどの Active Sync アダプタに適用されます。

パラメータ	説明
処理規則	TaskDefinition の名前、またはフィード内のすべてのレコードに対して実行される TaskDefinition の名前を返す規則のいずれかです。この処理規則は、activeSync 名前空間内のリソースアカウント属性を、リソース ID およびリソース名とともに取得します。 このパラメータは、ほかのすべてのパラメータよりも優先されます。この属性を指定した場合、このアダプタに関するその他の設定に関係なく、すべての行に対して処理が実行されます。

パラメータ	説明
相関規則	リソースアカウントを所有する Identity Manager ユーザーのリソース情報が特定されない場合は、相関規則が呼び出され、(アカウントの名前空間内の) リソースアカウント属性に基づいて、ユーザーの照合に使用する、一致する可能性のあるユーザーまたはアカウント ID の候補のリスト、あるいは属性条件を特定します。 規則は、エントリを既存の Identity Manager アカウントに関連付けるために使用できる次のいずれかの情報を返します。 ■ Identity Manager ユーザー名 ■ WSAttributes オブジェクト (属性ベースの検索で使用) ■ AttributeCondition 型または WSAttribute 型の項目のリスト (AND 結合による属性ベースの検索) ■ String 型の項目のリスト (各項目は Identity Manager アカウントの Identity Manager ID またはユーザー名) 相関規則によって複数の Identity Manager アカウントが識別された場合は、複数の候補の中から一致させるべきアカウントを特定するために確認規則または解決プロセス規則が必要になります。 データベーステーブル、フラットファイル、および PeopleSoft コンポーネントの Active Sync アダプタの場合は、デフォルトの相関規則はリソース上の調整ポリシーから継承されます。
確認規則	相関規則によって返されるすべてのユーザーを対象にして評価される規則です。ユーザーごとに、Identity Manager の ID (account. 名前空間にある) リソースアカウント情報の相関を示す、完全なユーザービューが確認規則に渡されます。確認規則は、ブール値で表すことができる値を返すことが期待されます。たとえば、「true」、「1」、または「yes」や、「false」、「0」、または「null」です。 データベーステーブル、フラットファイル、および PeopleSoft コンポーネントの Active Sync アダプタの場合は、デフォルトの確認規則はリソース上の調整ポリシーから継承されます。
削除規則	`activeSync.` または `account.` という形式のキーを持つ値すべてのマップを期待できる規則です。プロキシ管理者のセッションに基づく LighthouseContext オブジェクト (`display.session`) は、この規則のコンテキストで利用できます。この規則は、ブール値で表すことができる値を返すことが期待されます。たとえば、「true」、「1」、または「yes」や、「false」、「0」、または「null」です。 あるエントリに関してこの規則によって true が返された場合、アダプタの設定方法に応じて、フォームとワークフローを介してアカウント削除リクエストが処理されます。

パラメータ	説明
解決プロセス規則	TaskDefinition の名前、またはフィード内のあるレコードに対して複数の一致がある場合に実行される TaskDefinition の名前を返す規則のいずれかです。解決プロセス規則は、リソースアカウント属性をリソース ID およびリソース名とともに取得します。 この規則は、一致がなく、「一致しないアカウントの作成」が選択されていない場合にも必要です。 このワークフローは、管理者による手動操作を求める処理にすることもできます。
一致しないアカウントの作成	true に設定すると、一致する Identity Manager ユーザーが見つからない場合に、リソース上にアカウントが作成されます。false に設定すると、処理規則が設定され、その規則が識別するワークフローによって新しいアカウントが保証されていることが確認されないかぎり、アカウントは作成されません。デフォルトは true です。
グローバルで利用	true に設定すると、activeSync 名前空間に加えてグローバル名前空間にも値が入力されます。デフォルト値は false です。

セキュリティーに関する注意事項

「セキュリティーに関する注意事項」では、接続と認証の情報を説明します。

「サポートされる接続」では、Identity Manager とリソース間の接続に使用する接続のタイプを一覧に示します。次の接続タイプが一般的に使用されます。

- Sun Identity Manager Gateway
- SSH (Secure Shell)
- SSL (Secure Sockets Layer) 経由の JDBC (Java Database Connectivity)
- SSL 経由の JNDI (Java Naming and Directory Interface)
- Telnet/TN3270

ほかの接続タイプである可能性もあります。

「必要な管理特権」では、Identity Manager からユーザーを作成したりタスクを実行する際に管理者アカウントで必要な特権の一覧を示します。管理者アカウントはリソース編集ページで指定します。

すべての Active Sync アダプタで、管理者アカウントには、「Active Sync の動作設定」の「ログファイルパス」フィールドで指定したディレクトリに対する読み取り、書き込み、および削除のアクセス権が必要です。

プロビジョニングに関する注意事項

この節では、次に示すアダプタのプロビジョニング機能の概要を示します。機能には次のようなものがあります。

- アカウントの有効化/無効化。ユーザーアカウントを有効化および無効化する機能は、リソースによって異なります。たとえば、一部の UNIX システムでは、パスワードをランダムな値に変更することでアカウントが無効化されます。
- アカウントの名前の変更。ユーザーアカウントの名前を変更する機能は、リソースによって異なります。
- パススルー認証。リソースユーザーが Identity Manager ユーザーインタフェースにログインできるようにする、Identity Manager の機能。
- 前アクションと後アクション。アクションとは、スクリプトアクションのネイティブサポートが存在する場合に、管理するリソースのコンテキスト内で実行するスクリプトです。

  たとえば、UNIX システムでは、アクションは UNIX シェルコマンドの処理になります。Microsoft Windows 環境では、アクションは CMD コンソール内で実行可能な DOS 形式のコンソールコマンドになります。
- データ読み込みメソッド。データを Identity Manager に読み込む方法を指定します。次の方法がサポートされています。
  - Active Sync。アイデンティティー情報の源泉として信頼性の高い外部リソース (アプリケーションやデータベースなど) に格納された情報を、Identity Manager のユーザーデータと同期させることができます。アダプタは、リソースアカウントの変更を Identity Manager に適用したり、読み込ませることができます。
  - 検出 (リソースから読み込み)。読み込みの前に表示確認を行わずに、最初からリソースアカウントを Identity Manager に読み込みます。リソースアカウント情報を、ファイルからインポート、またはファイルへエクスポートすることもできます。
  - 調整。定期的にリソースアカウントを Identity Manager に読み込み、設定されたポリシーに従って各アカウントを操作します。調整機能は、Identity Manager のリソースアカウントと実際にリソースに存在するアカウントの不整合をハイライト表示し、アカウントデータを定期的に相互に関連付けるために使用します。

アカウント属性

「アカウント属性」ページ (スキーママップ) は、Identity Manager アカウント属性をリソースアカウント属性にマップします。属性のリストはリソースごとに異なります。使用していない属性は、スキーママップページから削除するようにしてください。属性を追加すると、多くの場合、ユーザーフォームやその他のコードを編集する必要が生じます。

Identity Manager ユーザー属性は、規則、フォーム、およびその他の Identity Manager 固有の機能で使用できます。リソースユーザー属性は、アダプタがリソースと通信しているときにだけ使用されます。

Identity Manager がサポートするアカウント属性の種類を次に示します。

- string
- integer
- Boolean
- encrypted
- binary

注–バイナリ属性には、グラフィックスファイル、オーディオファイル、証明書などが含まれます。ほとんどのリソースはバイナリアカウント属性をサポートしません。現在、バイナリ属性を処理できるのは、特定のディレクトリアダプタ、フラットファイルアダプタ、データベースアダプタのみです。フォームやワークフローでは、そのバイナリ属性をサポートしていないリソースに、バイナリ属性を適用しないようにする必要があります。使用中のアダプタがバイナリ属性をサポートしているかどうかは、そのアダプタの説明の「アカウント属性」の節を参照してください。

また、バイナリ属性で参照するファイルのサイズは、できるだけ小さくしておきます。たとえば、非常に大きなサイズのグラフィックスファイルを読み込むと、Identity Manager のパフォーマンスが低下する可能性があります。

ほとんどのアダプタはバイナリアカウント属性をサポートしません。一部のアダプタは、グラフィックス、オーディオ、証明書などのバイナリ属性をサポートします。使用中のアダプタに対してサポートされているかどうかは、そのアダプタの説明の「アカウント属性」の節を参照してください。

`name` はビューの予約語であるため、リソーススキーママップのアイデンティティーシステムユーザー属性として使用しないようにしてください。

リソースオブジェクトの管理

Identity Manager で管理可能なリソース上のオブジェクトの一覧を示します。

アイデンティティーテンプレート

ユーザーのアカウント名の構文を定義します。ほとんどのリソースで、構文はアカウント ID と同じです。ただし、リソースが階層構造を持つ名前空間を使用する場合は、構文が異なります。

サンプルフォーム

フォームはページに関連付けられたオブジェクトであり、ブラウザでユーザー表示属性をそのページにどのように表示するかについての規則が含まれています。フォームにはビジネスロジックを組み込むことができ、通常はユーザーに表示する前に、表示データを処理するためにフォームが使用されます。

組み込みのフォーム

一部のフォームは、Identity Manager リポジトリにデフォルトで読み込まれます。リポジトリ内のフォームのリストを表示するには、次の手順を実行します。

▼ リポジトリ内のフォームのリストを表示する

1. **Web** ブラウザで、`http://`*IdentityManagerHost*`/idm/debug` にアクセスします。
   ブラウザに「System Settings」ページが表示されます。
2. オプションメニューから、「**List Objects**」の隣にある「**Type: ResourceForm**」を選択します。
3. 「**List Objects**」をクリックします。「**List Objects of Type: ResourceForm**」ページが表示されます。このページには、**Identity Manager** リポジトリに存在する編集可能なすべてのフォームが一覧表示されます。

その他の利用可能なフォーム

Identity Manager には、デフォルトでは読み込まれない多数のフォームが用意されています。これらのフォームは *InstallDir*`\idm\sample\forms\` ディレクトリに置かれています。

トラブルシューティング

トレース出力は、アダプタの問題を識別して解決する際に役立ちます。問題を特定して解決するためにトレースを使用する場合は、一般的に次のような手順を実行します。

▼ トレースを使用する

1. トレースをオンにします。
2. 問題を再現し、結果を評価します。
3. 必要に応じて、追加のパッケージやクラスのトレースをオンにしたり、トレースのレベルを上げたりして、手順 **2** と **3** を繰り返します。
4. トレースをオフにします。
   トレースをオンにするには、次の手順に従います。
5. **Configurator** アカウントで **Identity Manager** にログインします。
6. デバッグページ (`http://`*IdentityManagerHost*`:`*Port*`/idm/debug`) にアクセスします。

7 「**Show Trace**」をクリックします。

8 「**Trace Enabled**」にチェックマークが付いていることを確認します。

9 「**Method/Class**」テキストボックスに完全なクラス名を入力します。

10 トレースレベル **(1-4)** を入力します。各レベルで、異なるタイプの情報が取得されます。

- 1 は、public メソッドの入口と出口、および主要な例外を指定します。
- 2 は、すべてのメソッドの入口と出口を指定します。
- 3 は、メソッドの呼び出しごとに一度だけ発生する重要な情報表示 (フローを制御する変数の値など) を指定します。
- 4 は、メソッドの呼び出しごとに n 回発生する情報表示を指定します。

11 必要に応じて、ページのその他の項目を入力します。トレースの準備ができたら「**Save**」をクリックします。

トレース機能を無効にするには、「Show Trace」オプションを選択解除するか、「Method/Class」テキストボックスからクラス名を削除します。

◆ ◆ ◆ 第 2 章

2 Access Enforcer

SAP GRC (Governance, Risk, and Compliance) Access Enforcer リソースアダプタは、`com.waveset.adapter.AccessEnforcerResourceAdapter` クラスで定義されます。このクラスは、`SAPResourceAdapter` クラスを拡張します。

アダプタの詳細

リソースを設定する際の注意事項

アダプタが正常に動作するには、Access Enforcer の自動プロビジョニング設定を「true」に設定してください。

Identity Manager のインストールに関する注意事項

Access Enforcer リソースアダプタは、カスタムアダプタです。インストールプロセスを完了するには、次の手順を実行する必要があります。

▼ Access Enforcer リソースアダプタをインストールする

1 次の **URL** から **JCo (Java Connection)** ツールキットをダウンロードします。

http://service.sap.com/connectors

SAP JCo ダウンロードページにアクセスするには、ログインとパスワードが必要です。このツールキットには、`sapjco-ntintel-2.1.8.zip` のような名前が付けられます。この名前は、選択したプラットフォームやバージョンによって異なります。

注 – ダウンロードする JCo ツールキットが、アプリケーションサーバーが動作する Java のビットバージョンと一致していることを確認します。たとえば、JCo は Solaris x86 プラットフォーム上の 64 ビットバージョンでのみ使用できます。したがって、アプリケーションサーバーが Solaris x86 プラットフォーム上の 64 ビットバージョンで実行されている必要があります。

2 ツールキットを解凍し、インストール手順に従います。必ずライブラリファイルを正しい場所に配置し、環境変数を指示どおりに設定してください。

3 `sapjco.jar` ファイルを *InstallDir*`\WEB-INF\lib` ディレクトリにコピーします。

4 次の **URL** から **Apache Axis SOAP** ツールキットをダウンロードします。

http://www.apache.org/dyn/closer.cgi/ws/axis/1_4/

5 ツールキットを解凍し、インストール手順に従います。

6 次のファイルを *InstallDir* `\WEB-INF\lib` ディレクトリにコピーします。

- `axis.jar`
  - `commons-discovery-0.2.jar`
  - `commons-logging-1.0.4.jar`
  - `jaxrpc.jar`
  - `log4j-1.2.8.jar`
  - `saaj.jar`
  - `wsdl4j-1.5.1.jar`

`commons-discovery`、`commons-logging`、`log4j`、および `wsdl4j` の JAR ファイルは、これ以外のバージョンも使用できます。

7 **Access Enforcer** リソースを **Identity Manager** のリソースリストに追加するには、「管理するリソースの設定」ページの「カスタムリソース」セクションに次の値を追加する必要があります。

```
com.waveset.adapter.AccessEnforcerResourceAdapter
```

8 `$WSHOME/sample/accessenforcer.xml` をインポートして、**Access Enforcer** のサポートを有効にします。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Managerは、getUserメソッド、listObjectsメソッド、およびアカウント反復子について、SAP Java Connector (JCo) 経由のBAPIを使用してSAPシステムと通信します。

必要な管理特権

SAPに接続するユーザー名を、SAPユーザーにアクセスできるロールに割り当ててください。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	なし
パススルー認証	なし
前アクションと後アクション	なし
データ読み込みメソッド	■ リソースからのインポート (`SAPResourceAdapter` クラスを使用) ■ 調整 (`SAPResourceAdapter` クラスを使用)

アカウント属性

次の表に、Access Enforcerに固有のアカウント属性に関する情報を示します。一般的なSAP属性については、SAPアダプタのマニュアルを参照してください。特に明記されていないかぎり、すべての属性はString型であり、書き込み専用です。次に示すすべての属性の値は、大文字に変換されます。

アイデンティティーシステムユーザー属性	リソース属性名	説明
aeUserId	UserId	必須。Access Enforcerアカウントのユーザー ID
aeEmailAddress	EmailAddress	必須。ユーザーに割り当てられた電子メール。

アイデンティティーシステムユーザー属性	リソース属性名	説明
aeFirstName	FirstName	必須。ユーザーの名。
aeLastName	LastName	必須。ユーザーの姓。
aeRequestorId	RequestorId	必須。アカウントをリクエストしているユーザーのユーザー ID。
aeRequestorLastName	RequestorLastName	必須。要求者の姓。
aeRequestorFirstName	RequestorFirstName	必須。要求者の名。
aeRequestorEmailAddr	RequestorEmailAddr	必須。要求者の電子メールアドレス。
aePriority	Priority	必須。リクエストの優先順位。
aeApplication	Application	必須。アクセス権を付与するために追加するアプリケーション
aeLocation	場所	ユーザーの場所。
aeCompany	Company	ユーザーの会社。
aeDepartment	Department	ユーザーの部署。
aeEmployeeType	EmployeeType	ユーザーの在籍区分ステータス。
aeRequestReason	RequestReason	アクセスがリクエストされる理由。
aeRoles	ロール	Complex。ユーザーに割り当てられたロール。この属性には、ValidFrom、ValidTo、および Rolename の値が格納されます。
aeValidFrom	ValidFrom	リクエストの開始時刻。
aeValidTo	ValidTo	リクエストの終了時刻。
aeTelephone	Telephone	ユーザーの電話番号。
aeManagerId	ManagerId	必須。ユーザーのマネージャーのアカウント ID。この値は、Access Enforcer で有効な既存の値である必要があります。
aeManagerFirstName	ManagerFirstName	必須。マネージャーの名。この値は、Access Enforcer で有効な既存の値である必要があります。
aeManagerLastName	ManagerLastName	必須。マネージャーの姓。この値は、Access Enforcer で有効な既存の値である必要があります。

アイデンティティーシステムユーザー属性	リソース属性名	説明
aeManagerEmailAddr	ManagerEmailAddr	必須。マネージャーの電子メールアドレス。この値は、Access Enforcer で有効な既存の値である必要があります。

注 – 必須であると指定されている属性は、Submit Request サービス呼び出しで送信される必要があります。ただし、その他のリソースが割り当てられているユーザーを更新するときに競合が発生する可能性があるため、それらの属性はスキーママップで必須であるとマークされていません。

ほかの属性がスキーママップに追加されることがありますが、Access Enforcer ではカスタム属性であると見なされます。カスタム属性を識別するには、任意のリソースユーザー属性に `AE` を付加する必要があります。たとえば、`AEMyAttribute` とします。カスタム属性の値は、大文字に変換されません。

リソースオブジェクトの管理

適用不可

アイデンティティーテンプレート

```
$accountId$
```

サンプルフォーム

- Access Enforcer User Form
- Access Enforcer EnableDisableDelete Form

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

- `com.waveset.adapter.AccessEnforcerResourceAdapter`
- `com.waveset.adapter.SAPResourceAdapter`

インストールされている SAP Java Connector (JCO) のバージョンを判定し、それが正しくインストールされているかどうかを判定するには、次のコマンドを実行します。

```
java -jar sapjco.jar
```

このコマンドは、JCO のバージョンとともに、SAP システムと通信する JNI プラットフォーム依存ライブラリおよび RFC ライブラリを返します。

プラットフォーム依存ライブラリが見つからない場合は、SAP のマニュアルを参照して、SAP Java Connector の正しいインストール方法を調べてください。

◆ ◆ ◆ 第 3 章

3 Sun Access Manager

Identity Manager では Sun Access Manager リソースアダプタが提供され、旧バージョンモードで動作している Sun Java™ System Access Manager をサポートします。

アダプタの詳細

このアダプタは、`com.waveset.adapter.SunAccessManagerResourceAdapter` クラスで定義されます。

注 –

- Sun Access Manager リソースアダプタは、旧バージョンモードで実行されているリソースに使用します。
- Sun Access Manager レルムリソースアダプタは、レルムモードで実行されているリソースに使用します。このアダプタの詳細は、「Sun Access Manager レルム」を参照してください。

リソースを設定する際の注意事項

注 – Access Manager 7 以降の場合、このアダプタでは旧バージョンモードのみがサポートされます。レルムモードはサポートされません。

設定できるのは (レルムモードまたは旧バージョンモードにかかわらず) 1 つの Access Manager サーバーだけです。

Policy Agent は、シングルサインオン (SSO) を有効にするために使用できるオプションモジュールです。使用している環境内でこの製品を使用していない場合は、Policy Agent の設定手順やインストール手順を実行しないでください。

Policy Agent の詳細は、http://docs.sun.com/app/docs/coll/1322.1 を参照してください。

Policy Agent をインストールするには、Policy Agent に付属するインストール手順書に従います。その後、次の作業を実行します。

▼ Policy Agent を設定する

1. AMAgent.properties ファイルを編集します。
2. **Sun Access Manager** でポリシーを作成します。

AMAgent.properties ファイルの編集

AMAgent.properties ファイルを変更して、Identity Manager を保護する必要があります。このファイルは AgentInstallDir/config ディレクトリにあります。

▼ AMAgent.properties ファイルを編集する

1. AMAgent.properties ファイル内で次の行を検索します。

```
com.sun.identity.agents.config.cookie.reset.enable = false
com.sun.identity.agents.config.cookie.reset.name[0] =
com.sun.identity.agents.config.cookie.reset.domain[] =
com.sun.identity.agents.config.cookie.reset.path[] =
```

   これらの行を次のように編集します。

```
com.sun.identity.agents.config.cookie.reset.enable = true
com.sun.identity.agents.config.cookie.reset.name[0] = AMAuthCookie
com.sun.identity.agents.config.cookie.reset.domain[0] = .example.com
com.sun.identity.agents.config.cookie.reset.path[0] = /
```

2. 次の行を追加します。

```
com.sun.identity.agents.config.cookie.reset.name[1] = iPlanetDirectoryPro
com.sun.identity.agents.config.cookie.reset.domain[1] = .example.com
com.sun.identity.agents.config.cookie.reset.path[1] = /
```

3. 次の行を検索します。

```
com.sun.identity.agents.config.profile.attribute.fetch.mode = NONE
com.sun.identity.agents.config.profile.attribute.mapping[] =
```

   これらの行を次のように編集します。

```
com.sun.identity.agents.config.profile.attribute.fetch.mode = HTTP_HEADER
com.sun.identity.agents.config.profile.attribute.mapping[uid] = sois_user
```

4 変更を有効にするために、**Web** サーバーを再起動します。

Sun Access Manager のポリシーの作成

▼ ポリシーを作成する

1 **Sun Access Manager** アプリケーションで、次の規則を設定した IDMGR という名前 (または類似の名前) の新しいポリシーを作成します。

サービスのタイプ	リソース名	アクション
URL ポリシーエージェント	http://*server:port*/idm	GET アクションと POST アクションを許可します
URL ポリシーエージェント	http://*server:port*/idm/*	GET アクションと POST アクションを許可します

2 1 つ以上の主体を IDMGR ポリシーに割り当てます。

Sun Access Manager (Access Manager 7.0 より前のバージョン) のインストールと設定

次に、Sun Access Manager および Policy Agent のインストールと設定の方法について説明します。Sun Access Manager を Identity Manager サーバーと同じシステムにインストールする場合は、Sun Access Manager リソースアダプタの設定に関する情報を参照してください。Policy Agent を使用している場合は、61 ページの「Policy Agent のインストールと設定」で追加情報を確認してください。

Access Manager を Identity Manager サーバーとは異なるシステムにインストールする場合は、Identity Manager システムで次の手順を実行します。

▼ Access Manager を別のシステムにインストールする場合

1 **Sun Access Manager** サーバーからコピーするファイルの配置先ディレクトリを作成します。この手順では、*CfgDir* という名前のディレクトリを使用します。**Access Manager** がインストールされている場所を *AccessMgrHome* とします。

2 次のファイルを *AccessMgrHome* から **CfgDir** にコピーします。ディレクトリ構造はコピーしないでください。

- `lib/*.*`
  - `locale/*.properties`
  - `config/serverconfig.xml`
  - `config/SSOConfig.properties` (Identity Server 2004Q2 以降)

- config/ums/ums.xml

3 **UNIX** では、全体的な読み取りアクセスを許可するために *CfgDir* 内の **JAR** ファイルのアクセス権を変更しなければならない場合があります。アクセス権を変更するには、次のコマンドを実行します。

```
chmod a+r CfgDir/*.jar
```

4 次のように **JAVA** クラスパスを付加します。

- **Windows**: *CfgDir* ;*CfgDir*/am_sdk.jar; *CfgDir*/am_services.jar;*CfgDir*/am_logging.jar
- **UNIX**: *CfgDir* :*CfgDir*/am_sdk.jar: *CfgDir*/am_services.jar:*CfgDir*/am_logging.jar

5 **Identity Server 6.0** を使用する場合は、*CfgDir* を指す **Java** システムプロパティーを設定します。次のようなコマンドを使用します。

```
java -Dcom.iplanet.coreservices.configpath=CfgDir
```

6 バージョン **6.1** 以降を使用する場合は、*CfgDir*/AMConfig.properties ファイルで、次の行を追加または編集します。

```
com.iplanet.services.configpath=CfgDir
com.iplanet.security.SecureRandomFactoryImpl=com.iplanet.am.util.
SecureRandomFactoryImpl
com.iplanet.security.SSLSocketFactoryImpl=netscape.ldap.factory.
JSSESocketFactory
com.iplanet.security.encryptor=com.iplanet.services.util.
JCEEncryption
```

最初の行では configpath を設定しています。最後の 3 行ではセキュリティー設定を変更しています。

7 *CfgDir*/am_*.jar ファイルを $WSHOME/WEB-INF/lib にコピーします。**Identity Server 6.0** を使用する場合は、jss311.jar ファイルも $WSHOME/WEB-INF/lib ディレクトリにコピーします。

8 **Identity Manager** が **Windows** 上で稼働している環境で **Identity Server 6.0** を使用する場合は、*IdServer*\lib\jss*.dll を *CfgDir* にコピーし、*CfgDir* をシステムパスに追加します。

注 – Identity Manager が Access Manager とは異なるシステムにインストールされている環境では、次のエラー条件を確認してください。Access Manager リソースへの接続時にエラー `java.lang.ExceptionInInitializerError` が返され、それに続く試行で `java.lang.NoClassDefFoundError` が返される場合は、設定データに誤りまたは欠落がないか確認します。

また、`java.lang.NoClassDefFoundError` で示されたクラスの JAR ファイルも確認します。そのクラスが含まれている JAR ファイルのクラスパスを、アプリケーションサーバーの JAVA クラスパスに付加します。

CfgDir に 59 ページの「Sun Access Manager (Access Manager 7.0 より前のバージョン) のインストールと設定」で説明したすべてのデータが含まれ、すべての設定プロパティーが正しく割り当てられていることを確認します。

Policy Agent のインストールと設定

適切な Access Manager Policy Agent を、Identity Manager サーバーにインストールする必要があります。Policy Agent は次の場所から入手できます。

```
http://wwws.sun.com/software/download/inter_ecom.html#dirserv
```

Policy Agent に付属するインストール手順書に従ってください。その後、次に示す作業を実行します。

AMAgent.properties ファイルの編集

`AMAgent.properties` ファイルを変更して、Identity Manager を保護する必要があります。このファイルは次のディレクトリにあります。

- **Windows**: \ *AgentInstallDir*`\es6\config\` *_PathInstanceName* \
- **UNIX**: `/etc/opt/SUNWam/agents/es6/config/` *_PathInstanceName/*

必ず、前述したディレクトリにあるファイルを使用してください。*AgentInstallDir*`\config` ディレクトリにあるファイルは使用しないでください。

▼ AMAgent.properties ファイルの編集

1 `AMAgent.properties` ファイル内で次の行を検索します。

```
com.sun.identity.agents.config.cookie.reset.enable = false
com.sun.identity.agents.config.cookie.reset.name[0] =
com.sun.identity.agents.config.cookie.reset.domain[] =
com.sun.identity.agents.config.cookie.reset.path[] =
```

これらの行を次のように編集します。

```
com.sun.identity.agents.config.cookie.reset.enable = true
com.sun.identity.agents.config.cookie.reset.name[0] = AMAuthCookie
com.sun.identity.agents.config.cookie.reset.domain[0] = .example.com
com.sun.identity.agents.config.cookie.reset.path[0] = /
```

2 次の行を追加します。

```
com.sun.identity.agents.config.cookie.reset.name[1] = iPlanetDirectoryPro
com.sun.identity.agents.config.cookie.reset.domain[1] = .example.com
com.sun.identity.agents.config.cookie.reset.path[1] = /
```

3 次の行を検索します。

```
com.sun.identity.agents.config.profile.attribute.fetch.mode = NONE
com.sun.identity.agents.config.profile.attribute.mapping[] =
```

これらの行を次のように編集します。

```
com.sun.identity.agents.config.profile.attribute.fetch.mode = HTTP_HEADER
com.sun.identity.agents.config.profile.attribute.mapping[uid] = sois_user
```

4 変更を有効にするために、**Web** サーバーを再起動します。

▼ Access Manager のポリシーの作成

1 **Access Manager** アプリケーションで、次の規則を設定した IDMGR という名前 (または類似の名前) の新しいポリシーを作成します。

サービスのタイプ	リソース名	アクション
URL ポリシーエージェント	http://*server*:*port*/idm	GET アクションと POST アクションを許可します
URL ポリシーエージェント	http://*server*:*port*/idm/*	GET アクションと POST アクションを許可します

2 1 つ以上の主体を IDMGR ポリシーに割り当てます。

Identity Manager のインストールに関する注意事項

ここでは、Sun Access Manager リソースアダプタおよび Policy Agent のインストールと設定に関する注意点を説明します。

Sun Access Manager リソースアダプタ

次の手順に従って、リソースアダプタのインストールと設定を行います。

▼ Access Manager リソースアダプタをインストールして設定する

1. 適切なバージョンの『Sun Java™ System Access Manager Developer's Guide』に記載された手順に従って、Sun Access Manager インストールからクライアント SDK を構築します。
2. 生成される war ファイルから AMConfig.properties ファイルと amclientsdk.jar ファイルを抽出します。
3. 次のディレクトリに AMConfig.properties をコピーします。

   ```
   $WSHOME/WEB-INF/classes
   ```

4. 次のディレクトリに amclientsdk.jar をコピーします。

   ```
   $WSHOME/WEB-INF/lib
   ```

5. サーバーのクラスパスに amclientsdk.jar ファイルを追加します。
6. Identity Manager アプリケーションサーバーを再起動します。
7. ファイルのコピーが終了したら、Sun Access Manager リソースを Identity Manager リソースリストに追加する必要があります。「管理するリソースの設定」ページの「カスタムリソース」セクションに次の値を追加します。

   ```
   com.waveset.adapter.SunAccessManagerRealmResourceAdapter
   ```

Policy Agent

Access Manager ログインモジュールが最初に表示されるように、管理者およびユーザーのログインモジュールを変更します。

注 – この手順を実行する前に、Access Manager リソースを設定する必要があります。

▼ 管理者とユーザーのログインモジュールを変更する

1. Identity Manager 管理者インタフェースのメニューバーで、「セキュリティー」を選択します。
2. 「ログイン」タブをクリックします。

3 ページの下部にある「ログインモジュールグループの管理」ボタンをクリックします。

4 変更するログインモジュールを選択します。たとえば、「アイデンティティーシステムのデフォルトの **ID/**パスワード ログインモジュールグループ」を選択します。

5 「ログインモジュールの割り当て」選択ボックスで、「**Sun Access Manager** ログインモジュール」を選択します。

6 「ログインモジュールの割り当て」オプションの横に新しく「選択」オプションが表示されたら、適切なリソースを選択します。

7 「ログインモジュールの修正」ページが表示されたら、表示されているフィールドを必要に応じて編集し、「保存」をクリックします。「ログインモジュールグループの修正」がもう一度表示されます。

8 モジュールグループの最初のリソースとして「**Sun Access Manager** ログインモジュール」を指定し、「保存」をクリックします。

使用上の注意

WebLogic で Identity Manager を実行している環境で、Access Manager に対するネイティブな変更が Identity Manager に表示されない場合は、クラスパスの `weblogic.jar` の前に `am_services.jar` を追加します。

複数のプロトコルハンドラがある場合は、次のようにプロトコルハンドラを設定します。

```
java.protocol.handler.pkgs=com.iplanet.services.comm|sun.net.www.protocol
```

セキュリティーに関する注意事項

ここでは、サポートされる接続と基本的なタスクの実行に必要な承認の要件について説明します。

サポートされる接続

Identity Manager は、SSL 経由の JNDI を使用してこのアダプタと通信します。

必要な管理特権

Access Manager に接続するユーザーに、ユーザーアカウントを追加または変更するためのアクセス権を付与してください。

プロビジョニングに関する注意事項

ここでは、アダプタのプロビジョニング機能の概要を表に示します。

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	なし
パススルー認証	はい。 シングルサインオンには Web Proxy Agent が必要です。
前アクションと後アクション	なし
データ読み込みメソッド	■ リソースから直接インポート ■ リソースの調整

アカウント属性

次の表に、デフォルトでサポートされる Access Manager ユーザーのアカウント属性を示します。特に記載されていないかぎり、属性はすべて省略可能です。

リソースユーザー属性	リソース属性タイプ	説明
cn	String	必須。ユーザーのフルネーム。
dynamicSubscriptionGroups	String	ユーザーが登録されている動的グループのリスト。
employeeNumber	Number	ユーザーの従業員番号。
givenname	String	ユーザーの名。
iplanet-am-user-account-life	Date	ユーザーアカウントが期限切れになる日時。この値が設定されていない場合、アカウントは期限切れになりません。
iplanet-am-user-alias-list	String	ユーザーに適用される可能性がある別名のリスト。
iplanet-am-user-failure-url	String	認証の失敗時にユーザーがリダイレクトされる URL。
iplanet-am-user-success-url	String	認証の成功時にユーザーがリダイレクトされる URL。

リソースユーザー属性	リソース属性タイプ	説明
mail	Email	ユーザーの電子メールアドレス。
postalAddress	String	ユーザーの自宅住所。
roles	String	ユーザーに割り当てられたロールのリスト。
sn	String	ユーザーの姓。
staticSubscriptionGroups	String	ユーザーが登録されている静的グループのリスト。
telephoneNumber	String	ユーザーの電話番号。
uid	String	必須。ユーザーの一意のユーザー ID。
userPassword	Password	必須。ユーザーのパスワード。

リソースオブジェクトの管理

Identity Manager は、次の Access Manager オブジェクトをサポートします。

リソースオブジェクト	サポートされる機能	管理される属性
ロール	表示、更新、削除	cn、iplanet-am-role-aci-description、iplanet-am-role-descri
Static subscription group	表示、作成、更新、削除、名前を付けて保存	cn、iplanet-am-group-subscribable、uniqueMember
Filtered group	表示、作成、更新、削除、名前を付けて保存	cn、accountMembers、membershipFilter
Dynamic subscription group	表示、作成、更新、削除、名前を付けて保存	cn、accountMembers、iplanet-am-group-subscribable
組織	表示、作成、削除、名前を付けて保存、検索	o

アイデンティティーテンプレート

デフォルトのアイデンティティーテンプレートは次のとおりです。

```
uid=$uid$,ou=People,dc=MYDOMAIN,dc=com
```

デフォルトのテンプレートを有効な値に置き換えてください。

サンプルフォーム

ここでは、組み込みのサンプルフォームと、Sun Access Manager リソースアダプタで利用できるその他のサンプルフォームの一覧を示します。

組み込みのフォーム

- Sun Access Manager Update Static Group Form
- Sun Access Manager Update Role Form
- Sun Access Manager Update Organization Form
- Sun Access Manager Update Filtered Group Form
- Sun Access Manager Update Dynamic Group Form
- Sun Access Manager Create Static Group Form
- Sun Access Manager Create Role Form
- Sun Access Manager Create Organization Form
- Sun Access Manager Create Filtered Group Form
- Sun Access Manager Create Dynamic Group Form

その他の利用可能なフォーム

`SunAMUserForm.xml`

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

```
com.waveset.adapter.SunAccessManagerResourceAdapter
```

◆ ◆ ◆ 第 4 章

Sun Access Manager レルム

Identity Manager では、Sun Access Manager レルムリソースアダプタレルムモードで動作している Sun™ Java System Access Manager のサポートが提供されます。

アダプタの詳細

このアダプタは、`com.waveset.adapter.SunAccessManagerRealmResourceAdapter` クラスで定義されます。

注 –

- Sun Access Manager レルムリソースアダプタは、レルムモードで実行されているリソースに使用します。
- Sun Access Manager リソースアダプタは、旧バージョンモードで実行されているリソースに使用します。このアダプタの詳細は、「Sun Access Manager」を参照してください。

リソースを設定する際の注意事項

レルムモードでも旧バージョンモードでも、設定できるのは、1 つの Access Manager サーバーだけです。異なるレルムのプロビジョニングを行う場合は、複数のリソースを定義できます。

Identity Server Policy Agent は、シングルサインオン (SSO) を有効にするために使用できるオプションモジュールです。この Policy Agent は次の場所から入手できます。

`http://wwws.sun.com/software/download/inter_ecom.html#dirserv`

注 – 使用している環境内でこの製品を使用していない場合は、Policy Agent のインストール手順や設定手順を実行しないでください。

Policy Agent の詳細については、次のマニュアルを参照してください。

`http://docs.sun.com/app/docs/coll/1322.1`

Identity Server Policy Agent は、Identity Manager がインストールされているサーバーと同じサーバーにインストールする必要があります。

Policy Agent をインストールするには、Policy Agent に付属するインストール手順書に従います。その後、次の作業を実行します。

▼ Policy Agent を設定する

1 `AMAgent.properties` ファイルを編集します。

2 **Sun Access Manager** でポリシーを作成します。

AMAgent.properties ファイルの編集

`AMAgent.properties` ファイルを変更して、Identity Manager を保護する必要があります。このファイルは `AgentInstallDir/config` ディレクトリにあります。

▼ AMAgent.properties ファイルを編集する

1 `AMAgent.properties` ファイル内で次の行を検索します。

```
com.sun.identity.agents.config.cookie.reset.enable = false
com.sun.identity.agents.config.cookie.reset.name[0] =
com.sun.identity.agents.config.cookie.reset.domain[] =
com.sun.identity.agents.config.cookie.reset.path[] =
```

これらの行を次のように編集します。

```
com.sun.identity.agents.config.cookie.reset.enable = true
com.sun.identity.agents.config.cookie.reset.name[0] = AMAuthCookie
com.sun.identity.agents.config.cookie.reset.domain[0] = .example.com
com.sun.identity.agents.config.cookie.reset.path[0] = /
```

2 次の行を追加します。

```
com.sun.identity.agents.config.cookie.reset.name[1] = iPlanetDirectoryPro
com.sun.identity.agents.config.cookie.reset.domain[1] = .example.com
com.sun.identity.agents.config.cookie.reset.path[1] = /
```

3 次の行を検索します。

```
com.sun.identity.agents.config.profile.attribute.fetch.mode = NONE
com.sun.identity.agents.config.profile.attribute.mapping[] =
```

これらの行を次のように編集します。

```
com.sun.identity.agents.config.profile.attribute.fetch.mode = HTTP_HEADER
com.sun.identity.agents.config.profile.attribute.mapping[uid] = sois_user
```

4 変更を有効にするために、**Web** サーバーを再起動します。

Sun Access Manager のポリシーの作成

▼ ポリシーを作成する

1 **Sun Access Manager** アプリケーションで、次の規則を設定した IDMGR という名前 (または類似の名前) の新しいポリシーを作成します。

サービスのタイプ	リソース名	アクション
URL ポリシーエージェント	http://*server*:*port*/idm	GET アクションと POST アクションを許可します
URL ポリシーエージェント	http://*server*:*port*/idm/*	GET アクションと POST アクションを許可します

2 1 つ以上の主体を IDMGR ポリシーに割り当てます。

Identity Manager のインストールに関する注意事項

ここでは、Sun Access Manager レルムリソースアダプタおよび Policy Agent のインストールと設定に関する注意点を説明します。

一般的な設定

次の手順に従って、リソースアダプタのインストールと設定を行います。

▼ Access Manager レルムリソースアダプタをインストールして設定する

1 適切なバージョンの『Sun Java™ System Access Manager Developer's Guide』に記載された手順に従って、Sun Access Manager インストールからクライアント SDK を構築します。

2 生成される war ファイルから AMConfig.properties ファイルと amclientsdk.jar ファイルを抽出します。

3 次のディレクトリに AMConfig.properties をコピーします。

```
$WSHOME/WEB-INF/classes
```

4 次のディレクトリに amclientsdk.jar をコピーします。

```
$WSHOME/WEB-INF/lib
```

5 サーバーのクラスパスに amclientsdk.jar ファイルを追加します。

6 Identity Manager アプリケーションサーバーを再起動します。

7 ファイルのコピーが終了したら、Sun Access Manager レルムリソースを Identity Manager リソースリストに追加する必要があります。「管理するリソースの設定」ページの「カスタムリソース」セクションに次の値を追加します。

```
com.waveset.adapter.SunAccessManagerRealmResourceAdapter
```

ログインモジュール

Sun Access Manager ログインモジュールが最初に表示されるように、管理者およびユーザーのログインモジュールを変更する必要があります。

注 – 次の手順を実行する前に、まず、Sun Access Manager レルムリソースを設定する必要があります。

▼ 管理者とユーザーのログインモジュールを変更する

1 Identity Manager 管理者インタフェースのメニューバーで、「セキュリティー」を選択します。

2 「ログイン」タブをクリックします。

3 ページの下部にある「ログインモジュールグループの管理」ボタンをクリックします。

4 変更するログインモジュールを選択します。たとえば、「アイデンティティーシステムのデフォルトの **ID/**パスワード ログインモジュールグループ」を選択します。

5 「ログインモジュールの割り当て」選択ボックスで、「**Sun Access Manager** レルムログインモジュール」を選択します。

6 「ログインモジュールの割り当て」オプションの横に新しく「選択」オプションが表示されたら、適切なリソースを選択します。

7 「ログインモジュールの修正」ページが表示されたら、表示されているフィールドを必要に応じて編集し、「保存」をクリックします。「ログインモジュールグループの修正」がもう一度表示されます。

8 モジュールグループの最初のリソースとして「**Sun Access Manager** レルムログインモジュール」を指定し、「保存」をクリックします。

9 **Identity Manager** からログアウトします。

セキュリティーに関する注意事項

ここでは、サポートされる接続と基本的なタスクの実行に必要な承認の要件について説明します。

サポートされる接続

Identity Manager は、SSL を使用してこのアダプタと通信します。

必要な管理特権

Sun Access Manager に接続するユーザーに、ユーザーアカウントを追加または変更するためのアクセス権を付与する必要があります。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	なし

機能	サポート状況
パススルー認証	はい。Policy Agent 経由。
前アクションと後アクション	なし
データ読み込みメソッド	■ リソースから直接インポート ■ リソースの調整

アカウント属性

次の表に、デフォルトでサポートされる Sun Access Manager ユーザーのアカウント属性を示します。特に記載されていないかぎり、属性はすべて省略可能です。

リソースユーザー属性	リソース属性タイプ	説明
uid	String	必須。ユーザーの一意のユーザー ID。
cn	String	必須。ユーザーのフルネーム
givenname	String	ユーザーの名
sn	String	ユーザーの姓
mail	Email	ユーザーの電子メールアドレス
employeeNumber	Number	ユーザーの従業員番号
telephoneNumber	String	ユーザーの電話番号
postalAddress	String	ユーザーの自宅住所
iplanet-am-user-account-life	Date	ユーザーのアカウントが期限切れになる日時
iplanet-am-user-alias-list	String	ユーザーの別名のリスト
iplanet-am-user-success-url	String	認証の成功時にユーザーがリダイレクトされる URL
iplanet-am-user-failure-url	String	認証の失敗時にユーザーがリダイレクトされる URL
roleMemberships	String	ユーザーが登録されているロールのリスト
groupMemberships	String	ユーザーが登録されているグループのリスト

リソースオブジェクトの管理

Identity Manager は、次の Sun Access Manager オブジェクトをサポートします。

リソースオブジェクト	サポートされる機能	管理される属性
グループ	表示、作成、更新、削除	name、user members
ロール	表示、作成、更新、削除	name、user members
Filtered Roles	表示、作成、更新、削除	name、nsrolefilter

アイデンティティーテンプレート

デフォルトのアイデンティティーテンプレートは `$accountId$` です。

サンプルフォーム

ここでは、組み込みのサンプルフォームと、Sun Access Manager レルムリソースアダプタで利用できるその他のサンプルフォームの一覧を示します。

組み込みのフォーム

- Sun Access Manager Realm Create Role Form
- Sun Access Manager Realm Update Role Form
- Sun Access Manager Realm Create Filtered Role Form
- Sun Access Manager Realm Update Filtered Role Form
- Sun Access Manager Realm Create Group Form
- Sun Access Manager Realm Update Group Form

その他の利用可能なフォーム

`SunAMRealmUserForm.xml`

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

```
com.waveset.adapter.SunAccessManagerRealmResourceAdapter
```

◆ ◆ ◆ 第 5 章

ACF2

ACF2 リソースアダプタは、OS/390 メインフレーム上のユーザーアカウントとメンバーシップの管理をサポートします。このアダプタは、TN3270 エミュレータセッションで ACF2 を管理します。

アダプタの詳細

ACF2 リソースアダプタは com.waveset.adapter.ACF2ResourceAdapter クラスで定義されます。

リソースを設定する際の注意事項

なし

Identity Manager のインストールに関する注意事項

ACF2 リソースアダプタは、カスタムアダプタです。インストールプロセスを完了するには、次の手順を実行してください。

▼ ACF2 リソースアダプタをインストールする

1 **ACF2** リソースを **Identity Manager** のリソースリストに追加するには、「管理するリソースの設定」ページの「カスタムリソース」セクションに次の値を追加する必要があります。

```
com.waveset.adapter.ACF2ResourceAdapter
```

2 適切な **JAR** ファイルを **Identity Manager** インストールの `WEB-INF/lib` ディレクトリにコピーします。

コネクションマネージャー	**JAR** ファイル
Host On Demand	IBM Host Access Class Library (HACL) は、メインフレームへの接続を管理します。HACL を含む推奨 JAR ファイルは `habeans.jar` です。これは、HOD に付属する HOD Toolkit (または Host Access Toolkit) とともにインストールされます。HACL のサポートされるバージョンは、HOD V7.0、V8.0、V9.0、および V10 に含まれるバージョンです。 habeans.jar ファイル ただし、このツールキットを利用できない場合は、HOD のインストールに含まれる次の JAR ファイルを `habeans.jar` の代わりに使用できます。 ■ `habase.jar` ■ `hacp.jar` ■ `ha3270.jar` ■ `hassl.jar` ■ `hodbase.jar` 詳細は、http://www.ibm.com/software/webservers/hostondemand/ を参照してください。
Attachmate WRQ	Sun 製品向け Attachmate 3270 メインフレームアダプタには、メインフレームへの接続の管理に必要なファイルが含まれます。 ■ `RWebSDK.jar` ■ `wrqtls12.jar` ■ `profile.jaw` この製品の入手については、Sun プロフェッショナルサービスにお問い合わせください。

3 `Waveset.properties` ファイルに次の定義を追加して、端末セッションを管理するサービスを定義します。

```
serverSettings.serverId.mainframeSessionType=Value
serverSettings.default.mainframeSessionType=Value
```

Value は、次のように設定できます。

- 1 は、IBM Host On-Demand (HOD) を表します。

- 3 は、Attachmate WRQ を表します。

  これらのプロパティーを明示的に設定しない場合、Identity Manager は WRQ、HOD の順に使用を試みます。

4 **Attachmate** ライブラリが **WebSphere** または **WebLogic** アプリケーションサーバーにインストールされている場合は、`com.wrq.profile.dir=`*LibraryDirectory* プロパティーを `WebSphere/AppServer/configuration/config.ini` または `startWeblogic.sh` ファイルに追加します。

これにより、Attachmate コードでライセンスファイルを検索できます。

5 `Waveset.properties` ファイルに加えた変更を有効にするために、アプリケーションサーバーを再起動します。

6 リソースへの **SSL** 接続の設定については、第 **53** 章「メインフレーム接続」を参照してください。

使用上の注意

ここでは、ACF2 リソースアダプタの使用に関連する依存関係と制限について示します。

管理者

TSO セッションでは、同時に複数の接続は許可されません。Identity Manager ACF 操作の同時実行を実現するには、複数の管理者を作成する必要があります。2 人の管理者を作成すれば、2 つの Identity Manager ACF 操作を同時に実行できます。少なくとも 2 人 (できれば 3 人) の管理者を作成するようにしてください。

クラスタ環境で運用している場合は、クラスタ内のサーバーごとに管理者を定義する必要があります。これは、各サーバーの管理者が同じ管理者である場合にも適用されます。TSO では、クラスタ内のサーバーごとに異なる管理者が必要です。

クラスタリングを使用していない場合は、すべての行でサーバー名は Identity Manager のホストマシンの名前となります。

注 – ホストリソースアダプタは、同じホストに接続している複数のホストリソースでの親和性管理者に対して最大接続数を強制しません。代わりに、各ホストリソース内部の親和性管理者に対して最大接続数が強制されます。

同じシステムを管理する複数のホストリソースがあり、現在それらが同じ管理者アカウントを使用するように設定されている場合は、同じ管理者がリソースに対して同時に複数のアクションを実行しようとしていないことを確認するために、それらのリソースを更新しなければならない可能性があります。

リソースアクション

ACF2 アダプタでは、login および logoff のリソースアクションが必要です。login アクションは、認証されたセッションに関してメインフレームとネゴシエーションを行います。logoff アクションは、そのセッションが不要になったときに接続を解除します。

login リソースアクションおよび logoff リソースアクションの作成については、565 ページの「メインフレームの例」を参照してください。

SSL 設定

Identity Manager は TN3270 接続を使用してリソースと通信します。

ACF2 リソースへの SSL 接続の設定については、第 53 章「メインフレーム接続」を参照してください。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は TN3270 接続を使用して ACF2 と通信します。

必要な管理特権

ACF2 と接続する管理者には、ACF2 ユーザーの作成と管理を行うための十分な特権が与えられている必要があります。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	あり
パススルー認証	なし
前アクションと後アクション	あり
データ読み込みメソッド	■ リソースから直接インポート ■ 調整

アカウント属性

次の表に、ACF2 アカウント属性に関する情報を示します。

リソースユーザー属性	データ型	説明
NAME	String	ロギングおよびセキュリティー違反レポートに表示されるユーザー名
PHONE	String	ユーザーの電話番号
ACCESS.ACC-CNT	String	このログイン ID の作成以降に、このログイン ID によってシステムにアクセスした回数
ACCESS.ACC-DATE	String	このユーザーが最後にシステムにアクセスした日付
ACCESS.ACC-SRCE	String	このログオン ID が最後にシステムにアクセスした論理的または物理的な入力ソース名またはソースグループ名
ACCESS.ACC-TIME	String	このユーザーが最後にシステムにアクセスした時刻
CANCEL/SUSPEND.CANCEL	Boolean	ログオン ID は、システムへのアクセスをキャンセルおよび拒否されます
CANCEL/SUSPEND.CSDATE	String	CANCEL フィールドまたは SUSPEND フィールドの設定された日付
CANCEL/SUSPEND.CSWHO	String	CANCEL、SUSPEND、または MONITOR フィールドを設定するログオン ID
CANCEL/SUSPEND.MON-LOG	Boolean	このユーザーがシステムに入るたびに、ACF2 は SMF レコードを書き込みます

リソースユーザー属性	データ型	説明
CANCEL/SUSPEND.MONITOR	Boolean	このユーザーがシステムに入るたびに、CA-ACF2 がセキュリティーコンソールと指定された ユーザー (CSWHO) にメッセージを送信します
CANCEL/SUSPEND.SUSPEND	Boolean	ログオン ID は、システムへのアクセスを中断および拒否されます
CANCEL/SUSPEND.TRACE	Boolean	このユーザーによるすべてのデータ参照は、トレースおよび記録されます
CICS.ACF2CICS	Boolean	このアドレス空間のログオン ID で実行されているすべての CICS/ESA 4.1 以降の領域で、CA-ACF2 CICS セキュリティーが初期化されることを示します
CICS.CICSCL	String	CICS オペレータクラス
CICS.CICSID	String	CICS オペレータ ID
CICS.CICSKEY	String	CICS リリース 1.6 以降をサポートするトランザクションセキュリティーキーの値の最初の 3 バイト
CICS.CICSKEYX	String	CICS リリース 1.6 以降をサポートするトランザクションセキュリティーキーの値の末尾の 5 バイト
CICS.CICSPRI	String	CICS オペレータの優先順位
CICS.CICSRSL	String	CICS リソースアクセスキー
CICS.IDLE	String	このユーザーの端末トランザクション間隔として許可された最大時間 (分)
IMS.MUSDLID	String	MUSASS アドレス空間のデフォルトのログオン ID
IDMS.IDMSPROF	String	ユーザーが CA-IDMS にサインオンするときに実行されるサインオンプロファイル CLIST の名前
IDMS.IDMSPRVS	String	ユーザーが CA-IDMS にサインオンするときに実行されるサインオンプロファイル CLIST の バージョン
MUSASS.MUSID	String	IMS レコードが適切な管理領域に確実に関連付けられるように、Infostorage データベース内の IMS レコードをグループ化します
MUSASS.MUSIDINF	Boolean	CA-ACF2 Info タイプのシステムエントリ呼び出しのために、MUSID フィールドを使用して MUSASS 領域へのアクセスを制限するようにしてください。
MUSASS.MUSOPT	String	CAIDMS アドレス空間を管理する CA-ACF2 CA-IDMS オプションモジュールの名前

リソースユーザー属性	データ型	説明
MUSASS.MUSPGM	String	CA-IDMS 起動プログラムの名前
MUSASS.MUSUPDT	Boolean	ユーザーが CA-ACF2 データベースを更新できるようにします
PRIVILEGES.ACCOUNT	Boolean	ユーザーは、範囲を制限されながらもログオン ID を挿入、削除、および変更できます
PRIVILEGES.ACTIVE	String	このフィールドに含まれる日付の午前 0 時 1 分に、ログオン ID が自動的にアクティブ化されます。
PRIVILEGES.AUDIT	Boolean	この特権を使用して、ユーザーは CAACF2 システムのパラメータを検査できますが、変更はできません。
PRIVILEGES.AUTODUMP	Boolean	データ設定やリソース違反が発生したときに作成されるダンプ
PRIVILEGES.AUTONOPW	Boolean	この仮想マシンには、パスワードを指定しなくても自動ログオンできます。
PRIVILEGES.BDT	Boolean	このログオン ID のアドレス空間は、Bulk Data Transfer (BDT) 製品に属しています。
PRIVILEGES.CICS	Boolean	ログオン ID には CICS にサインオンする権限があります。
PRIVILEGES.CMD-PROP	Boolean	これは、ユーザーが SET TARGET コマンドまたは TARGET パラメータを使用して、グローバル CPF ターゲットリストをオーバーライドできることを示しています。
PRIVILEGES.CONSULT	Boolean	ユーザーはほかのログオン ID を表示できます。
PRIVILEGES.DUMPAUTH	Boolean	このユーザーは、アドレス空間が実行専用環境またはパスコントロール環境にある場合でも、ダンプを生成できます。
PRIVILEGES.EXPIRE	String	一時的なログオン ID が期限切れになる日付。
PRIVILEGES.IDMS	Boolean	ログオン ID には CA-IDMS にサインオンする権限があります。
PRIVILEGES.JOB	Boolean	ユーザーは、バッチおよびバックグラウンドの端末監視プログラム (Terminal Monitor Program、TMP) ジョブを入力できます。
PRIVILEGES.JOBFROM	Boolean	ユーザーは //*JOBFROM 管理ステートメントを使用できます。

リソースユーザー属性	データ型	説明
PRIVILEGES.LEADER	Boolean	ユーザーは、ほかのユーザーのほかのログオン ID の特定のフィールドを表示して変更できます。
PRIVILEGES.LOGSHIFT	Boolean	ユーザーは、ログオン ID レコードの SHIFT フィールドで指定した期間外にシステムにアクセスできます。
PRIVILEGES.MAINT	Boolean	ユーザーは、指定のライブラリから実行される指定のプログラムを使用して、ロギングまたは検証なしでリソースにアクセスできます。
PRIVILEGES.MUSASS	Boolean	このログオン ID は、複数ユーザーのシングルアドレス空間システム (MUSASS) です。
PRIVILEGES.NO-INH	Boolean	ネットワークジョブは、送信者からこのログオン ID を継承できません。
PRIVILEGES.NO-SMC	Boolean	Step-must-complete (SMC) コントロールがバイパスされ、重要な VSAM 更新操作の実行中は、ジョブはキャンセル不可であるとみなされます。
PRIVILEGES.NO-STORE	Boolean	このユーザーは、規則セットの格納または削除を承認されていません。
PRIVILEGES.NON-CNCL	Boolean	規則によってこのアクセスが禁止されている場合でも、ユーザーはすべてのデータにアクセスできます。
PRIVILEGES.PGM	String	このログオン ID のジョブを送信するために指定された APF 承認のプログラム。
PRIVILEGES.PPGM	Boolean	ユーザーは、GSO PPGM レコードで指定されたこれらの保護されたプログラムを実行できます。
PRIVILEGES.PRIV-CTL	Boolean	ユーザーがシステムにアクセスして自分に付与された追加の特権や権限を確認したときに、特権管理リソース規則をチェックします。
PRIVILEGES.PROGRAM	String	このログオン ID のジョブを送信するために指定された APF 承認のプログラム。
PRIVILEGES.READALL	Boolean	ログオン ID には、そのサイトのすべてのデータに対する読み取りアクセス権のみがあります。
PRIVILEGES.REFRESH	Boolean	このユーザーは、オペレータのコンソールから F ACF2,REFRESH オペレータコマンドを発行することを承認されています。
PRIVILEGES.RESTRICT	Boolean	この限定されたログオン ID は本番稼働用で、ユーザー検証用のパスワードは必要ありません。

リソースユーザー属性	データ型	説明
PRIVILEGES.RSRCVLD	Boolean	ユーザーの行うすべてのアクセスをリソース規則が承認する必要があることを指定します。
PRIVILEGES.RULEVLD	Boolean	このユーザーがアクセスするすべてのデータに対してアクセス規則が存在する必要があります。
PRIVILEGES.SCPLIST	String	この特権ユーザーのアクセスを制限する Infostorage 範囲のレコード。
PRIVILEGES.SECURITY	Boolean	このユーザーは、自分の制限範囲内で、アクセス規則、リソース規則、および Infostorage レコードを作成、維持、削除できるセキュリティー管理者です。
PRIVILEGES.STC	Boolean	開始済みタスクのみがこのログオン ID を使用します。
PRIVILEGES.SUBAUTH	Boolean	APF 承認のプログラムのみが、このログオン ID を指定するジョブを送信できます。
PRIVILEGES.SYNCNODE	String	Logonid データベース内で、このログオン ID と同期されるログオン ID の存在するノード
PRIVILEGES.TAPE-BLP	Boolean	このユーザーは、テープデータセットにアクセスしたときに、完全なラベルバイパス処理 (BLP) を使用できます。
PRIVILEGES.TAPE-LBL	Boolean	このユーザーは、テープデータセットにアクセスしたときに、制限された BLP を使用できます。
PRIVILEGES.TSO	Boolean	このユーザーは、TSO へのサインオンを承認されています。
PRIVILEGES.VAX	Boolean	このログオン ID は VAX (UAF) infostorage レコードと関連付けられています。
PRIVILEGES.VLDRSTCT	Boolean	RESTRICT ログオン ID に対してこのフィールドがオンになっていると、ログオン ID が継承される場合でも PROGRAM および SUBAUTH が検証されます。
PASSWORD.MAXDAYS	String	パスワードの期限が切れる前に、パスワードの変更間隔として許可される最大日数。値が 0 の場合、制限は何も適用されません。
PASSWORD.MINDAYS	String	ユーザーがパスワードを変更できるようになる前に経過する必要のある最小日数
PASSWORD.PSWD-DAT	String	最後の無効なパスワード試行のあった日付
PASSWORD.PSWD-EXP	Boolean	ユーザーのパスワードは、手動により強制的に期限切れにされました。

リソースユーザー属性	データ型	説明
PASSWORD.PSWD-INV	String	最後にログオンに成功して以来、パスワード違反の発生した回数
PASSWORD.PSWD-SRCE	String	このログオン ID の無効なパスワードを最後に受信した論理的または物理的な入力ソース名、またはソースグループ名
PASSWORD.PSWD-TIM	String	このログオン ID の無効なパスワードを最後に受信した時刻
PASSWORD.PSWD-TOD	String	パスワードの最終変更日時
PASSWORD.PSWD-VIO	String	PSWD-DAT で発生したパスワード違反の回数
PASSWORD.PSWD-XTR	Boolean	このログオン ID のパスワードは暗号化が不十分なので、APF 承認のプログラムによって抽出できます。
RESTRICTIONS.AUTHSUP1 〜 AUTHSUP8	Boolean	これらのフィールドによって、それぞれに指定されたシステムユーザーの拡張ユーザー認証 (EUA) をアクティブ化できます。
RESTRICTIONS.GROUP	String	このユーザーに関連付けられたグループ名またはプロジェクト名
RESTRICTIONS.PREFIX	String	このユーザーが所有してアクセスできるデータセットの高いレベルのインデックス
RESTRICTIONS.SHIFT	String	ユーザーがシステムへのログオンを許可されるタイミングを定義するシフトレコード
RESTRICTIONS.SOURCE	String	このログオン ID がシステムにアクセスする必要のある論理的または物理的な入力ソース名、またはソースグループ名
RESTRICTIONS.VMACCT	String	仮想マシンのデフォルトのアカウント番号を保持している loginID フィールド
RESTRICTIONS.VMIDLEMN	String	アイドル終了処理が開始される前に、このユーザーがシステム上でアイドル状態でいられる時間 (分)
RESTRICTIONS.VMIDLEOP	String	ユーザーがアイドル時間の制限を超えたときに実行されるアイドル終了処理のタイプ
RESTRICTIONS.ZONE	String	このログオン ID が通常システムにアクセスするタイムゾーン (つまり、ユーザーのローカルタイムゾーン) を定義する Infostorage Database ゾーンレコードの名前
STATISTICS.SEC-VIO	String	このユーザーのセキュリティー違反の総回数

リソースユーザー属性	データ型	説明
STATISTICS.UPD-TOD	String	このログオン ID の最終更新日時
TSO.ACCTPRIV	Boolean	ユーザーに TSO アカウンティング特権があるかどうかを示します
TSO.ALLCMDS	Boolean	ユーザーは特別なプレフィックス文字を入力することで、CA-ACF2 に制限されたコマンドリストをバイパスすることができます。
TSO.ATTR2	String	IBM プログラム管理機能 (PCF) が、コマンドの制限やデータセット保護のために PSCBATR2 フィールドを使用します。
TSO.CHAR	String	このユーザーの TSO 文字削除の文字
TSO.CMD-LONG	Boolean	TSO コマンドリストの使用時には、リストされたコマンドとエイリアスのみが受け入れられることを示します
TSO.DFT-DEST	String	TSO 回転 SYSOUT データセットのデフォルトのリモート宛先
TSO.DFT-PFX	String	ログオン時にユーザーのプロファイル内に設定されるデフォルトの TSO プレフィックス
TSO.DFT-SOUT	String	デフォルトの TSO SYSOUT クラス
TSO.DFT-SUBC	string	デフォルトの TSO 送信クラス
TSO.DFT-SUBH	string	デフォルトの TSO 送信保持クラス
TSO.DFT-SUBM	string	デフォルトの TSO 送信メッセージクラス
TSO.INTERCOM	Boolean	このユーザーは、TSO SEND コマンドを経由してほかのユーザーからのメッセージを受け入れます。
TSO.JCL	Boolean	このユーザーは、TSO からのバッチジョブの送信や、SUBMIT、STATUS、CANCEL、および OUTPUT コマンドの使用ができます。
TSO.LGN-ACCT	Boolean	このユーザーは、ログオン時にアカウント番号を指定できます。
TSO.LGN-DEST	Boolean	このユーザーは TSO ログイン時に DFT-DEST フィールドで指定された値をオーバーライドするリモートの出力先を指定できます。
TSO.LGN-MSG	Boolean	このユーザーはログオン時にメッセージクラスを指定できます。

リソースユーザー属性	データ型	説明
TSO.LGN-PERF	Boolean	このユーザーはログオン時にパフォーマンスグループを指定できます。
TSO.LGN-PROC	Boolean	このユーザーはログオン時に TSO プロシージャー名を指定できます。
TSO.LGN-RCVR	Boolean	このユーザーは、TSO または TSO/E コマンドパッケージの復元オプションを使用できます。
TSO.LGN-SIZE	Boolean	このユーザーは、ログオン時に任意の領域サイズを指定することを承認されています。
TSO.LGN-TIME	Boolean	このユーザーはログオン時に TSO セッション時間制限を指定できます。
TSO.LGN-UNIT	Boolean	このユーザーはログオン時に TSO ユニット名を指定できます。
TSO.LINE	String	TSO 行削除の文字
TSO.MAIL	Boolean	ログオン時に TSO からメールメッセージを受信します
TSO.MODE	Boolean	TSO からモーダルメッセージを受信します
TSO.MOUNT	Boolean	このユーザーはデバイスのマウントを発行できます。
TSO.MSGID	Boolean	プレフィックス TSO メッセージ ID
TSO.NOTICES	Boolean	ログオン時に TSO 通知を受信します
TSO.OPERATOR	Boolean	このユーザーは TSO オペレータ特権を持ちます
TSO.PAUSE	Boolean	CLIST 内で実行されたコマンドが多重メッセージを発行すると、プログラムを一時停止させます。
TSO.PMT-ACCT	Boolean	このユーザーがログオン時にアカウント番号を指定するように強制します。
TSO.PMT-PROC	Boolean	このユーザーがログオン時に TSO プロシージャー名を指定するように強制します。
TSO.PROMPT	Boolean	不足しているパラメータや不正なパラメータを指定し直すように求めます
TSO.RECOVER	Boolean	TSO または TSO/E コマンドパッケージの復元オプションを使用します
TSO.TSOACCT	String	ユーザーのデフォルトの TSO ログオンアカウント

リソースユーザー属性	データ型	説明
TSO.TSOCMDS	String	このユーザーが使用を承認されているコマンドのリストを含む TSO コマンドリストモジュールの名前。
TSO.TSOFSCRN	Boolean	このユーザーには全画面ログオンが表示されます。
TSO.TSOPERF	String	ユーザーのデフォルトの TSO パフォーマンスグループ
TSO.TSOPROC	String	ユーザーのデフォルトの TSO プロシージャー名
TSO.TSORBA	String	このユーザーのメールインデックスレポートポインタ (MIRP)
TSO.TSORGN	String	ユーザーがログオン時にサイズ指定しない場合の、ユーザーのデフォルトの TSO 領域サイズ (K バイト単位)
TSO.TSOSIZE	String	ユーザーが LGS-SZE フィールドを指定していない場合の、ユーザーの TSO 領域の最大サイズ (K バイト単位)
TSO.TSOTIME	String	ユーザーのデフォルトの TSO 時間パラメータ
TSO.TSOUNIT	String	ユーザーのデフォルトの TSO ユニット名
TSO.VLD-ACCT	Boolean	CA-ACF2 によって TSO アカウント番号が検証されることを示します
TSO.VLD-PROC	Boolean	CA-ACF2 によって TSO プロシージャー名が検証されることを示します
TSO.WTP	Boolean	Write-To-Programmer (WTP) メッセージを表示します

リソースオブジェクトの管理

なし

サンプルフォーム

`ACF2UserForm.xml`

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

- `com.waveset.adapter.HostAccess`
- `com.waveset.adapter.ACF2ResourceAdapter`

◆ ◆ ◆ 第 6 章

Active Directory

Windows 2000 / Active Directory リソースアダプタ
は、`com.waveset.adapter.ADSIResourceAdapter` クラスで定義されます。

アダプタの詳細

リソースを設定する際の注意事項

ここでは、Identity Manager で使用する次の Active Directory リソースの設定手順を説明します。

Sun Identity Manager Gateway の場所

「**LDAP** ホスト名」リソース属性が設定されていない場合、ゲートウェイはディレクトリに対してサーバーレスバインドを実行します。サーバーレスバインドが機能するためには、ドメイン内にあって、管理対象のドメインまたはディレクトリを「認識している」システム上に、ゲートウェイをインストールしてください。ゲートウェイが管理するすべての Windows ドメインは、同じフォレストに所属している必要があります。フォレスト境界を越えるドメインの管理はサポートされていません。複数のフォレストがある場合は、各フォレストに少なくとも 1 つのゲートウェイをインストールしてください。

「**LDAP** ホスト名」リソース属性は、ゲートウェイに特定の DNS ホスト名または IP アドレスとバインドするように指示します。これはサーバーレスバインドとは正反対です。ただし、LDAP ホスト名では、必ずしも特定のドメインコントローラを指定

する必要はありません。AD ドメインの DNS 名を使用できます。ゲートウェイシステムの DNS サーバーが、その DNS 名に対して複数の IP アドレスを返すように設定されている場合、そのうちの 1 つがディレクトリバインドに使用されます。これによって単一のドメインコントローラに依存する必要がなくなります。

パススルー認証や前アクションと後アクションを含む一部の操作では、ゲートウェイシステムがドメインのメンバーであることが求められます。

Sun Identity Manager Gateway のサービスアカウント

デフォルトでは、ゲートウェイサービスはローカルシステムアカウントとして実行されます。これは、「サービス」MMC スナップインで設定できます。

Exchange Server 2007 サポートが有効になっている Active Directory アダプタでゲートウェイが使用されている場合、ゲートウェイの実行に使用されるアカウントには特別な権限が必要です。

そのアカウントは、Exchange Server 2007 がインストールされているドメインにあるドメインアカウントである必要があります。使用されるアカウントは、標準 Exchange Server 2007 グループ Exchange Recipient Administrators のメンバーである必要もあります。このアカウントは、ゲートウェイによるすべての Exchange Server 2007 固有のアクションを実行します。リソースで指定された管理アカウントは使用されません。

許可されたゲートウェイアカウントでのこの制限は、Exchange Server 2007 API の制限に起因します。

これを正しく設定しないと、「PowerShell exception: Access to the address list service on all Exchange 2007 servers has been denied.」などの PowerShell エラーメッセージが表示されたあとに、スタックトレースが表示されます。

ゲートウェイをローカルシステム以外のアカウントとして実行する場合は、ゲートウェイサービスアカウントに「Act As Operating System」と「走査チェックのバイパス」のユーザー権限が必要です。ゲートウェイは、パススルー認証や、特定の状況でのパスワードの変更およびリセットに、これらの権限を使用します。

AD の管理の大部分は、リソース内で指定された管理アカウントを使用して行います。ただし、一部の操作はゲートウェイサービスアカウントで実行します。つまり、ゲートウェイサービスアカウントには、これらの操作を実行するための適切なアクセス権が必要です。現在、これに該当する操作は次のとおりです。

- ホームディレクトリの作成
- 実行中のアクション (前アクションと後アクションを含む)

Active Directory アダプタ 「認証のタイムアウト」リソース属性 (パススルー認証のみの場合) を使用すると、ゲートウェイ側で問題が発生してもアダプタが滞らずにすみます。

前アクションおよび後アクションのスクリプトを実行するときに、ゲートウェイに「プロセスレベルトークンの置き換え」の権限が必要な場合があります。この権限は、ゲートウェイが別のユーザー (リソース管理ユーザーなど) としてスクリプトのサブプロセスを実行しようとする場合に必要です。この場合、ゲートウェイプロセスには、そのサブプロセスに関連付けられたデフォルトのトークンを置き換える権限が必要です。

この権限がない場合は、サブプロセスの作成中に次のエラーが返されることがあります。

```
"Error creating process: A required privilege is not held by the client"
```

「プロセスレベルトークンの置き換え」権限は、デフォルトのドメインコントローラのグループポリシーオブジェクトと、ワークステーションおよびサーバーのローカルセキュリティーポリシーで定義されます。この権限をシステムに設定するには、「管理ツール」フォルダの「ローカルセキュリティーポリシー」アプリケーションを開き、「ローカルポリシー」>「ユーザー権利の割り当て」>「プロセスレベルトークンの置き換え」に移動します。

不在メッセージ

outOfOfficeEnabled および outofOfficeMessage のアカウント属性を使用すると、不在時の自動返信機能を有効にして、不在メッセージを設定できます。これらは Exchange 2000 または 2003 アカウントで使用できます。これらの属性が設定されるのはアカウントの更新時のみで、アカウントの作成時には設定されません。

このアダプタでは、ゲートウェイマシン上に Messaging Application Programming Interface (MAPI) をインストールする必要があります。MAPI サブシステムをインストールするには、少なくとも 2 とおりの方法があります。もっとも単純な方法は、ゲートウェイマシン上に Microsoft Outlook クライアントをインストールすることです。この場合、これ以外の設定は必要ありません。

Messaging Application Programming Interface (MAPI) もう 1 つの方法は、Exchange Server CD にある Exchange System Management Tools をインストールすることです。この管理ツールは、通常の Exchange Server のコンポーネントとしてインストールされます。ただし、このインストールによって MAPI サブシステムのファイルはインストールされますが、これで設定が完了するわけではありません。

`mapisvc.inf` ファイル (通常は `c:\winnt\system32` にある) には使用可能な MAPI サービスが格納されていますが、このファイルを更新して Exchange メッセージサービスのエントリを追加する必要があります。`msems.inf` ファイル (gateway zip ファイルに格納されている) に格納されているエントリは、Exchange メッセージサーバーを設定するために、`mapisvc.inf` ファイルにマージします。`msems.inf` ファイルは、メモ帳などのテキストエディタを使用して、手動で `mapisvc.inf` ファイルにマージできます。また、Microsoft Platform SDK には `MergeIni.exe` という名前のツールも用意されています。 これは `Microsoft SDK\Bin` ディレクトリの Windows Core SDK にあります。

MergeIni を実行するには、次のコマンドを使用します。

```
MergeIni msems.inf -m
```

Out of Office 属性は、msExchHideFromAddressLists 属性が有効になっている場合は取得できません。msExchHideFromAddressLists が true になっているときに、ユーザーフォームに Out of Office 属性を表示しようとしても、値は定義されません。サンプルの Active Directory ユーザーフォームには、msExchHideFromAddressLists が有効になっているときは Identity Manager に Out of Office 属性を表示させないロジックが組み込まれています。

Exchange Server 2007 では、ユーザーに対する Out Of Office メッセージの設定はサポートされていません。メッセージはユーザーエントリの一部として格納されなくなり、ユーザーのメールボックスの一部を形成します。Out of Office 返信を管理するには、エンドユーザーが Outlook または Outlook Web Access を使用することをお勧めします。

Exchange Server 2007 の要件

Exchange Server 2007 では、Exchange Management Shell を使用した API のプロビジョニングのみがサポートされています。このシェルでは、ユーザーとサーバーを管理およびプロビジョニングするコマンド行インタフェースが提供されます。このシェルは Microsoft Windows PowerShell 上でビルドされます。

ゲートウェイは、Microsoft Windows 32 ビット版オペレーティングシステムで実行する必要があります。さらに、ゲートウェイマシン上に次のアイテムをインストールする必要があります。

- 94 ページの「Microsoft Exchange Server 2007「管理ツール」、32 ビット」
- 95 ページの「Microsoft Windows PowerShell 1.0」
- 95 ページの「Microsoft .NET 2.0」

これらの要件については、次の節で詳細に説明します。

Microsoft Exchange Server 2007「管理ツール」、32 ビット

Exchange 管理シェルは、Exchange 用の管理ツールの一部です。Microsoft では、本稼働環境で 32 ビット版の Exchange Server 2007 を実行することはサポートされていません。管理ツールには、「Exchange Server 2007 システム要件」に記述したような例外があります。

ゲートウェイマシンには、32 ビット版の管理ツールのみをインストールします。64 ビット版のオペレーティングシステム上に 32 ビット版のツールをインストール、または両方の版のツールをインストールすると、予測不能な動作が発生する可能性があります。

32 ビット版の管理ツールは、次の Microsoft Web サイトからダウンロードできます。

```
http://go.microsoft.com/fwlink/?LinkID=82335
```

ダウンロードしてインストールするツールのバージョンは、残りの Exchange 環境にインストールされている Exchange Server 2007 バージョンと一致するようにしてください。

管理ツールのインストールを開始する前に、Microsoft Windows PowerShell 1.0 および Microsoft .NET 2.0 Framework がインストールされていることを確認してください。

インストールされている必要のあるパッケージは、次の 2 つです。

- Microsoft Windows PowerShell 1.0
- Microsoft .NET 2.0 Framework

Microsoft Windows PowerShell 1.0

Exchange 管理ツールは、Microsoft PowerShell の拡張 (またはスナップイン) として実装されます。現在は、PowerShell version 1.0 のみがサポートされ、サーバーにはこれをインストールする必要があります。

```
http://go.microsoft.com/fwlink/?LinkID=75790&clcid=0x09
```

PowerShell 環境では、メッセージのログがイベントビューアに記録されます。標準インストールされた PowerShell では、「PowerShell」と「Windows PowerShell」の 2 つのイベントログが作成されます。PowerShell イベントログは、ゲートウェイが PowerShell 実行時環境を作成するときに使用されます。書き込み操作がイベントログへの書き込みに失敗すると、PowerShell 環境は起動されず、ゲートウェイの PowerShell 関連のアクションは失敗します。この問題を防ぐには、イベントログを定期的に監視してクリーンアップするか、メッセージを上書きするように設定します。

Microsoft .NET 2.0

PowerShell を使用するには、Microsoft .NET 2.0 Framework をインストールする必要があります。この Framework はデフォルトでイントールされません。 次の場所にある Microsoft Download Center からインストールできます。

```
http://www.microsoft.com/downloads/details.aspx?familyid=0856EACB-4362-
4B0D-8EDD-AAB15C5E04F5
```

Identity Manager のインストールに関する注意事項

このリソースでは、追加のインストール手順は必要ありません。

使用上の注意

ここでは、Active Directory リソースアダプタの使用に関連する依存関係と制限について示します。 説明する内容は次のとおりです。

パスワード履歴の確認

エンドユーザーが自分のパスワードを変更するときに Active Directory アカウントのパスワード履歴を確認するには、AD パスワードを入力する必要があります。AD リソース上でこの機能を有効にするには、「変更時にユーザーがパスワードを入力」リソース属性を 1 に設定し、`WS_USER_PASSWORD` 属性のタイプを `encrypted` にしてアカウント属性に追加します。`WS_USER_PASSWORD` は、Identity Manager ユーザー属性およびリソースユーザー属性として追加する必要があります。

`waveset.properties` ファイル内の `sources.`*ResourceName*`.hosts` プロパティーを使用して、Active Sync を使用してリソースの同期を行うクラスタ内のホストを選択できます。*ResourceName* は、リソースオブジェクトの名前に置き換える必要があります。

Microsoft Exchange Server 2000 および 2003 のサポート

Microsoft Exchange Server 2000 および 2003 をサポートするには、次のアカウント属性を有効にします。

- `homeMDB`
- `homeMTA`
- `mailNickname`
- `msExchHomeServerName`

次のアカウント属性はデフォルトでスキーママップに表示され、Exchange アカウントの管理にも使用されます。

- `garbageCollPeriod`
- `mDBOverHardQuotaLimit`
- `mDBOverQuotaLimit`
- `mDBStorageQuota`
- `mDBUseDefaults`

Exchange Server の属性を管理するのに Active Directory リソースを使用していない場合、Identity Manager で Active Directory アカウントを正常にプロビジョニングするには、これらのアダプタのスキーママップからこれらの属性を削除する必要があります。

Exchange Server 2000/2003 と 2007 がインストールされた混合 Microsoft Exchange 環境は管理可能です。この Active Directory リソースが混合環境の管理に使用されず、Exchange Server 2007 のみが存在する場合は、前述の指示に従って、Exchange 属性をスキーマから削除します。

Active Directory アダプタは、プリンタ、コンピュータ、またはその他の Active Directory オブジェクトをサポートするように変更できます。次の例は、プリンタオブジェクトをサポートするように、該当する Java クラス内の XML コードを変更する方法を示しています。

```
<ObjectType name='Printer' icon='group'>
    <ObjectClasses operator='AND'>
       <ObjectClass name='printQueue'/>
    </ObjectClasses>
    <ObjectFeatures>
       <ObjectFeature name='create'/>
       <ObjectFeature name='update'/>
       <ObjectFeature name='delete'/>
    </ObjectFeatures>
    <ObjectAttributes idAttr='distinguishedName' displayNameAttr='cn'
        descriptionAttr='description'>
       <ObjectAttribute name='cn' type='string'/>
       <ObjectAttribute name='description' type='string'/>
       <ObjectAttribute name='managedby' type='string'/>
       <ObjectAttribute name='distinguishedName' type='string'/>
    </ObjectAttributes>
 </ObjectType>
```

プリンタオブジェクトをサポートするためには、少なくとも 1 つの新しいフォームを作成します。

Windows Active Directory リソースによって Exchange 2000 の連絡先を管理できるようにするには、オブジェクトクラスを `contact` に変更し、`password`、`accountId`、および `expirePassword` リソース属性を削除します。

Exchange 2007 のサポート

Microsoft Exchange Server 2007 は、Windows Server 2003 R2 または Windows Server 2003 Service Pack 1 以上でのみサポートされます。

Active Directory アダプタでは、デフォルトで Exchange 2007 電子メールアカウントは管理されません。これらのアカウントのサポートを有効にするには、次の操作を実行します。

- Exchange 2007 Support リソースパラメータを選択します。
- Exchange Recipient Administrators グループのメンバーであり、Windows ドメインにログインされているユーザーとして、ゲートウェイが動作していることを確認します。

- 次のアカウント属性をスキーママップに追加します。これらの属性の「必須」チェックボックスは選択しないでください。

属性名	説明
RecipientType (文字列)	リソースに対するユーザータイプ。Exchange 2007 対応のリソースでのアカウントの作成中に必要となります。指定可能な値は次のとおりです。 - User (Active Directory 専用ユーザー) - UserMailbox (ローカルメール記憶領域を持つ Active Directory および Exchange ユーザー) - MailUser (ローカルメール記憶領域を持たない Active Directory および Exchange ユーザー) Active Directory 専用ユーザー (RecipientType = User) から Exchange ユーザータイプ (RecipientType UserMailbox または MailUser) への変更時を除いて、この属性は読み取り専用です。RecipientType を User に戻したり、MailUser を UserMailbox (およびその逆) に変更したりすることはできません。
Database (文字列)	ユーザーのメールボックスを格納するデータベース。この値は、*Server\StorageGroup\MailboxDatabase* の形式で指定する必要があります。RecipientType が UserMailbox に設定されている場合は、この属性は値を持つ必要があります。RecipientType のほかの値がある場合は、この属性は無視されます。
ExternalEmailAddress (文字列)	Exchange 組織外部の電子メールアドレス。この属性は、RecipientType MailUser に対して Exchange 組織で一意の値に設定する必要があります。RecipientType のほかの値がある場合は、この属性は無視されます。

Active Sync の設定

Active Sync は常に同じドメインコントローラに接続する必要があるので、「子ドメインの検索」リソースパラメータが選択されていない場合は、特定のドメインコントローラのホスト名を指定するように LDAP ホスト名を設定します。「子ドメインの検索」オプションが選択されている場合は、グローバルカタログホスト名フィールドに、特定のグローバルカタログサーバーを設定します。

新しいドメインコントローラに切り替えたときに発生する繰り返しイベントの数を制限する方法については、第 52 章「Active Directory Synchronization Failover」 を参照してください。

パススルー認証用のドメインの指定

デフォルト設定では、ユーザー ID とパスワードのみを送信することによって、パススルー認証が実現されます。これらの 2 つの属性は、`w2k_user` および `w2k_password`

として、リソースオブジェクトの XML の AuthnProperties 要素で設定されます。ドメイン指定がない場合は、ゲートウェイで既知の全ドメインが検索され、ユーザーを含むドメイン内のユーザー認証が試みられます。

信頼されたマルチドメイン環境では、次の 2 つの状況が考えられます。

- すべてのドメインに同期されたユーザー/パスワードの組み合わせが含まれる。
- ユーザー/パスワードの組み合わせがドメインに依存する。

ユーザー/パスワードの組み合わせが同期される場合は、Active Directory リソースが共通リソースとなるように設定します。共通リソースの設定については、『Business Administrator's Guide』を参照してください。

ユーザー/パスワードの組み合わせがドメインに依存する場合、およびユーザーがドメイン情報を知るように要求される場合は、ログイン画面でドメイン情報を入力することをユーザーに許可できます。このオプションは、共通リソースを含む組み合わせで使用できます。

ログインページでドメインの入力をユーザーに許可するには、リソースオブジェクトの XML で <AuthnProperties> 要素に次のプロパティーを追加します。

```
<AuthnProperty name='w2k_domain' displayName='Domain:' formFieldType='text'
dataSource='user' doNotMap='true'/>
```

グローバルカタログにはフォレスト間の情報は含まれていないため、信頼される複数のドメインと Active Directory フォレストを含む環境では、これらの設定のいずれかを使用した認証に失敗する可能性があります。ドメイン数がロックアウトのしきい値よりも大きい場合は、ユーザーが不正なパスワードを入力すると、ユーザーのドメインでアカウントがロックアウトされる可能性もあります。

複数のゲートウェイ (フォレストごとに 1 つずつ) が配備されている場合にのみ、フォレスト間のユーザー管理が可能です。この場合、ユーザーがドメインを指定する必要がなく、アダプタごとに認証用に事前定義されたドメインを使用するようにアダプタを設定できます。これを実現するには、リソースオブジェクトの XML で <AuthnProperties> 要素に次の認証プロパティーを追加します。

```
<AuthnProperty name='w2k_domain' dataSource='resource attribute'
value='MyDomainName'/>
```

ユーザーを認証するドメインで *MyDomainName* を置き換えます。

ユーザーがドメインに存在し、パスワードが同期されない場合は、ドメインでログインに失敗します。

1 つの Login Module Group で、ドメイン情報用に複数のデータソースを使用することはできません。

ゲートウェイタイムアウト

Active Directory アダプタでは、RA_HANGTIMEOUT リソース属性を使用してタイムアウト値を秒単位で指定できます。この属性は、ゲートウェイに対する要求がタイムアウトしてハングしているとみなされるまでの時間を制御します。

次のように、この属性を Resource オブジェクトに手動で追加する必要があります。

```
<ResourceAttribute name='Hang Timeout' displayName='com.waveset.adapter.RAMessages:
   RESATTR_HANGTIMEOUT' type='int' description='com.waveset.adapter.RAMessages:
   RESATTR_HANGTIMEOUT_HELP' value='NewValue'>
 </ResourceAttribute>
```

この属性のデフォルト値は 0 です。これは Identity Manager がハングした接続を確認しないことを表します。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

「暗号化タイプ」リソースパラメータでは、Identity Manager ゲートウェイが Active Directory サーバーとの通信に使用する暗号化タイプを入力できます。このフィールドの有効な値は、None (デフォルト値)、Kerberos、および SSL です。

SSL を使用するには、ドメイン内に認証局が設定されている必要があります。また、Active Directory へのアクセスに使用するユーザー名は UPN 形式 (例: *DomainName**UserName*) で指定する必要があります。

必要な管理特権

ここでは、必要な Active Directory のアクセス許可とパスワードのリセット権の要件について説明します。

Active Directory アクセス権

Active Directory リソース内で設定する管理アカウントには、Active Directory における適切なアクセス権が必要です。

Identity Manager の機能	Active Directory アクセス権
Active Directory ユーザーアカウントの作成	ユーザーオブジェクトの作成 アカウントを有効な状態で作成するには、userAccountControl プロパティーの読み取り/書き込み権が必要です。パスワードの期限が切れた状態で作成するには、アカウント制限のプロパティーセット (userAccountControl プロパティーを含む) の読み取り/書き込みができるようにします。
Active Directory ユーザーアカウントの削除	ユーザーオブジェクトの削除
Active Directory ユーザーアカウントの更新	■ すべてのプロパティーの読み取り ■ すべてのプロパティーの書き込み 注意: プロパティーのサブセットのみが Identity Manager から管理されている場合は、これらのプロパティーのみに読み取りと書き込みのアクセスを許可できます。
AD ユーザーアカウントパスワードの変更/リセット AD ユーザーアカウントのロック解除 AD ユーザーアカウントの期限設定	ユーザーオブジェクトに関するアクセス許可: ■ 内容の一覧表示 ■ すべてのプロパティーの読み取り ■ 読み取りアクセス権 ■ パスワードの変更 ■ パスワードのリセット ユーザープロパティーに対するアクセス許可: ■ lockoutTime の読み取り/書き込み ■ アカウント制限の読み取り/書き込み ■ accountExpires の読み取り lockoutTime プロパティーに対するアクセス許可を設定するには、Windows 2000 Server リソースキットにある cacls.exe プログラムを使用してください。

パスワードのリセット

リソースオブジェクトの作成、削除、更新を実行する権限は期待するとおりのものです。アカウントには対応するオブジェクトタイプに対する作成権と削除権が必要で、ユーザーには、更新する必要のあるプロパティーに対する適切な読み取り/書き込み権が必要になります。

パススルー認証

Active Directory (AD) のパススルー認証をサポートするには、次の権限が必要となります。

- ゲートウェイをユーザーとして実行するように設定する場合、そのユーザーアカウントには「Act As Operating System」および「走査チェックのバイパス」のユーザー権限が必要です。デフォルトでは、ゲートウェイはローカルシステムアカウントとして実行され、このアカウントにはこれらの権限はすでに備わっています。また、「走査チェックのバイパス」ユーザー権限は、デフォルトですべてのユーザーに有効になっています。

注 – ユーザー権限を更新する必要のある場合、更新されたセキュリティーポリシーが伝播されるまでに遅延が生じる可能性があります。ポリシーが伝達されたら、ゲートウェイを再起動します。

- 認証されるアカウントには、ゲートウェイシステム上で「ネットワーク経由でコンピュータへアクセス」のユーザー権限が必要です。

ゲートウェイでは、`LogonUser` 関数に `LOGON32_LOGON_NETWORK` ログオンタイプおよび `LOGON32_PROVIDER_DEFAULT` ログオンプロバイダを設定して、パススルー認証を実行します。`LogonUser` 関数は、Microsoft Platform Software Development Kit で提供されています。

削除済みオブジェクトへのアクセス

管理アカウントには、Active Directory の削除済みオブジェクトコンテナへのアクセス権が必要です。デフォルトでは、管理者とシステムアカウントのみが、このコンテナにアクセスできます。その他のユーザーにこのコンテナへのアクセス権を許可することもできます。削除済みオブジェクトコンテナへのアクセス許可については、Microsoft ナレッジベースの記事 892806 を参照してください。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	あり

機能	サポート状況
パススルー認証	あり 「認証のタイムアウト」リソース属性 (パススルー認証のみの場合) を使用すると、ゲートウェイ側で問題が発生しても Active Direcotry アダプタが滞らずにすみます。
前アクションと後アクション	はい。 Active Directory リソースは、前アクションと後アクションをサポートしています。このアクションは、ユーザーが要求を作成、更新、および削除するときに、Active Directory ゲートウェイシステム上でバッチスクリプトを使用してアクティビティーを実行します。詳細は、第 50 章「リソースへのアクションの追加」を参照してください。
データ読み込みメソッド	■ リソースから直接インポート ■ リソースの調整 ■ Active Sync

アカウント属性

属性の構文 (または型) は、通常、属性がサポートされるかどうかを決定します。一般に、Identity Manager は boolean 型、文字列型、および整数型の構文をサポートします。バイナリ文字列と、それに類似した構文はサポートされていません。

属性構文のサポート

ここでは、サポートされるアカウント構文とサポートされないアカウント構文について説明します。

サポートされる構文

次の表に、Identity Manager でサポートされている Active Directory 構文を示します。

AD 構文	Identity Manager の構文	構文 ID	OM ID	ADS タイプ
Boolean	Boolean	2.5.5.8	1	ADSTYPE_BOOLEAN
Enumeration	String	2.5.5.9	10	ADSTYPE_INTEGER
Integer	Int	2.5.5.9	2	ADSTYPE_INTEGER
DN String	String	2.5.5.1	127	ADSTYPE_DN_STRING

AD 構文	Identity Manager の構文	構文 ID	OM ID	ADS タイプ
Presentation Address	String	2.5.5.13	127	ADSTYPE_CASE_IGNORE_STRING
IA5 String	String	2.5.5.5	22	ADSTYPE_PRINTABLE_STRING
Printable String	String	2.5.5.5	19	ADSTYPE_PRINTABLE_STRING
Numeric String	String	2.5.5.6	18	ADSTYPE_NUMERIC_STRING
OID String	String	2.5.5.2	6	ADSTYPE_CASE_IGNORE_STRING
Case Ignore String (teletex)	String	2.5.5.4	20 人	ADSTYPE_CASE_IGNORE_STRING
Unicode String	String	2.5.5.12	64	ADSTYPE_OCTET_STRING
Interval	String	2.5.5.16	65	ADSTYPE_LARGE_INTEGER
LargeInteger	String	2.5.5.16	65	ADSTYPE_LARGE_INTEGER

サポートされない構文

次の表に、Identity Manager でサポートされない Active Directory 構文を示します。

構文	構文 ID	OM ID	ADS タイプ
DN with Unicode string	2.5.5.14	127	ADSTYPE_DN_WITH_STRING
DN with binary	2.5.5.7	127	ADSTYPE_DN_WITH_BINARY
OR-Name	2.5.5.7	127	ADSTYPE_DN_WITH_BINARY
Replica Link	2.5.5.10	127	ADSTYPE_OCTET_STRING
NT Security Descriptor	2.5.5.15	66	ADSTYPE_NT_SECURITY_DESCRIPTOR
Octet String	2.5.5.10	4	ADSTYPE_OCTET_STRING
SID String	2.5.5.17	4	ADSTYPE_OCTET_STRING
UTC Time String	2.5.5.11	23	ADSTYPE_UTC_TIME
Object(Access-Point)	2.5.5.14	127	n/a

Identity Manager は、Replica Link 構文を使用する jpegPhoto および thumbnailPhoto アカウント属性をサポートしています。これ以外にもサポートされている Replica Link 属性があるかもしれませんが、それらはテストが完了していません。

Microsoft Exchange 2007 属性構文のサポート

このセクションでは、Microsoft Exchange 2007 専用のサポート済みおよび未サポートのアカウント構文に関する情報を提供します。

サポートされる構文

Identity Manager は、次の PowerShell 構文をサポートします。

構文	説明
String	Unicode 文字列。
Integer	Exchange 2007 では文字列として表現されます。
Nullable	値を含む必要のない属性。別のタイプなしで使用される場合、文字列が示されます。
Boolean	「True」または「False」の標準 boolean 値
Unlimited	特別に許可された値として文字列「Unlimited」を含む文字列として表現される整数。
ByteQuantifiedSize	サイズ修飾子あり、またはサイズ修飾子なしの文字列として表現される整数のサイズ。許可される修飾子は、なし、B (デフォルト)、KB、MB、または GB です。

Unlimited と ByteQuantifiedSize の組み合わせはサポートされています。

サポートされない構文

次の表に、Identity Manager でサポートされない PowerShell 構文を示します。

構文	説明
SwitchParameter	Boolean 値の特殊なコマンド行形式。
暗号化されています	パスワード属性

アカウント属性のサポート

ここでは、Identity Manager によってサポートされる Active Directory アカウント属性とサポートされない Active Directory アカウント属性を説明します。

サポートされるアカウント属性

次の表に、Identity Manager でサポートされるアカウント属性を示します。これ以外の属性 (Exchange の属性など) もサポートされる可能性があります。

スキーマ名	属性タイプ	説明
accountExpires	String	ユーザーのアカウントが期限切れになる日付。
AccountLocked	Boolean	アカウントがロックアウトされているかどうかを示します。true に設定することはできません (true に設定できるのは Windows システムのみ)。
accountNameHistory	String	アカウントがアクティブであった時間の長さ。読み取り専用。
aCSPolicyName	String	このユーザーに適用される ACS ポリシーの名前の文字列。
adminCount	String	指定されたオブジェクトが、管理グループの 1 つのメンバーであったために、その ACL がよりセキュリティーが高い値に (直接的または推移的に) 変更されたことを示します。システムによって設定されます。読み取り専用。
adminDescription	String	管理者の画面に表示される説明。
adminDisplayName	String	管理者画面に表示される名前。
altSecurityIdentities	String	認証に使用する、このユーザーに対する X.509 証明書または Kerberos ユーザーアカウントのマッピングを含みます。
assistant	String	ユーザーの管理補佐の識別名。
badPasswordTime	String	ユーザーが最後に不正なパスワードを使用してアカウントにログオンを試みた時刻。
badPwdCnt	String	読み取り専用。不正なパスワードによるログイン試行回数。この値は、問い合わせ先のドメインコントローラで失敗したログイン回数のみの場合があります。
businessCategory	String	組織で実施されているビジネスの種類を示します。
c	String	ユーザーの住所にある 2 文字の国番号。
cn	String	Common Name (共通名)。この属性は、DN 内の CN の値から設定されます。読み取り専用。
co	String	Text-Country (国名)
company	String	ユーザーの会社名。
codePage	Int	ユーザーの選択言語のコードページを指定します。

スキーマ名	属性タイプ	説明
countryCode	String	ユーザーの選択言語の国番号を指定します。
Database	String	この属性は、RecipientType の値が UserMailbox である場合に必要となります。デフォルトでは表示されません。Exchange 2007 アカウントを管理するには、これを追加する必要があります。 完全データベースパス (*Server\Storage\Database* の形式)。
defaultClassStore	String	指定されたユーザーのデフォルトの Class Store。
department	String	ユーザーが勤務する部署の名前を格納します。
description	String	オブジェクトの表示説明を格納します。この値はシステムによって単一値として処理されます。
desktopProfile	String	ユーザーまたはユーザーグループのデスクトッププロファイルの場所。
destinationIndicator	String	Active Directory では使用されません。
displayName	String	特定のユーザーのアドレス帳に表示される名前。通常は、名、ミドルネームのイニシャル、姓の組み合わせです。
displayNamePrintable	String	displayName のプリント可能なバージョン。
distinguishedName	String	直接設定することはできません。読み取り専用。DN テンプレートまたは accountId アカウント属性を使用して、作成時に DN を設定します。
division	String	ユーザーの部門。
dynamicLDAPServer	String	このアカウントの動的プロパティーを渡すサーバーの DNS 名。
employeeID	String	従業員の ID。
extensionName	String	ディレクトリオブジェクトの UI を拡張するために使用されるプロパティーページの名前。
ExternalEmailAddress	String	この属性は、RecipientType の値が MailUser である場合に必要となります。デフォルトでは表示されません。Exchange 2007 アカウントを管理するには、これを追加する必要があります。 Exchange サーバーで一意の電子メールアドレス (*User@Domain* の形式)。

スキーマ名	属性タイプ	説明
facsimileTelephoneNumber	String	ユーザーの勤務先の FAX 番号。
flags	Int	ビット情報を格納するためにオブジェクトによって使用されます。
garbageCollPeriod	Int	この属性は、CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,... オブジェクトに配置されています。DS ガベージコレクションの実行間隔 (時間単位) を表します。
generationQualifier	String	個人の世代を示します (たとえば、Jr. や II)。
givenName	String	ユーザーの名を格納します。
groupPriority	String	使用しません
groups	String	Windows のセキュリティーグループと配布グループ。
groupsToIgnore	String	使用しません
homeDirectory	String	ユーザーのホームディレクトリ。homeDrive が設定され、ドライブ文字が指定されている場合、homeDirectory は UNC パスにするようにしてください。このパスは \\server\share\directory という形式のネットワーク UNC パスにします。この値は NULL 文字列にすることもできます。 ユーザーのホームディレクトリは次の場合に作成されます。 ■ 値が、共有名ではない UNC パスである (share ディレクトリ上のディレクトリを指している) ■ すべての親ディレクトリが存在 ■ 「ホームディレクトリの作成」リソース属性が 1 に設定されている ■ ゲートウェイサービスの実行ユーザーには、ディレクトリの作成権が必要 ユーザーには、作成したディレクトリの完全な制御権が付与されます。
homeDrive	String	ホームディレクトリのマップ先になるコロンを含むドライブ文字 (「Z:」など)。homeDirectory が UNC パスの場合のみ指定するようにしてください。

スキーマ名	属性タイプ	説明
homeMDB	String	このメールボックスのメッセージデータベース (MDB) の識別名。次のような形式になります。CN=Mailbox Store (*SERVERNAME*),CN=First Storage Group, CN=InformationStore, CN=*SERVERNAME*,CN=Servers, CN=First Administrative Group, CN=Administrative Groups, CN=*EXCHANGE ORG*, CN=Microsoft Exchange, CN=Services, CN=Configuration,DC=*DOMAIN*, DC=*YOURCOMPANY*,DC=com'
homeMTA	String	このオブジェクトをサービスするメッセージ転送エージェント (MTA) を指します。次のような形式になります。CN=Microsoft MTA, CN=*SERVERNAME*, CN=Servers, CN=First Administrative Group, CN=Administrative Groups, CN=*EXCHANGE ORG*, CN=Microsoft Exchange, CN=Services, CN=Configuration,DC=*DOMAIN*, DC=*YOURCOMPANY*,DC=com
homePhone	String	ユーザーの自宅のメイン電話番号。
homePostalAddress	String	ユーザーの自宅の住所。
info	String	ユーザーのコメント。NULL 文字列にすることもできます。
initials	String	ユーザーのフルネームの一部を表すイニシャルを格納します。
internationalISDNNumber	String	オブジェクトに関連付けられた国際 ISDN 番号を指定します。
ipPhone	String	電話の TCP/IP アドレス。テレフォニーで使用します。
jpegPhoto	Binary	ユーザーの画像。(Windows 2003 Server 以上が必要)
l	String	ユーザーの住所の地域 (町村など)。
lastLogon	String	ユーザーが最後に DC にログオンした時刻。
lastLogonTimestamp	String	ユーザーが最後にドメインにログインした時刻。この値が更新されるのは、前回この値が更新されてから 1 週間以上が経過している状態で、ユーザーがログインしたときだけです。
lastLogoff	String	ユーザーが最後にログオフした時刻。
legacyExchangeDN	String	これまで Exchange によって使用されていた識別名。

スキーマ名	属性タイプ	説明
localeID	Int	この属性には、このアプリケーションによってサポートされるロケール ID の一覧が格納されます。ロケール ID は地理的な場所 (フランスなど) を表します。
lockoutTime	String	不正なログオンカウントがリセットされるまでの待機時間 (分)。
logonCount	Int	ユーザーがこのアカウントへのログオンを試みて成功した回数。このプロパティーは、ドメイン内でドメインコントローラ別に維持されます。
mail	String	1 つ以上の電子メールアドレス。
mailNickName	String	Exchange のニックネーム。
managedObjects	String	ユーザーによって管理されるオブジェクトの一覧を格納します。 システムによって設定されます。読み取り専用。
manager	String	ユーザーのマネージャーのディレクトリ名。
maxStorage	String	ユーザーの使用できる最大ディスク容量。
mDBOverHardQuotaLimit	String	メールボックスの最大サイズ (K バイト)。 これを超えるとメールを送受信できなくなります。
mDBOverQuotaLimit	String	メールボックスに割り当てられたオーバードラフト制限 (K バイト)。
mDBStorageQuota	String	メッセージデータベース割り当て (K バイト)。
mDBUseDefaults	String	メッセージを保存する際に、メールボックスごとの割り当て制限ではなく、デフォルトの割り当て制限を適用すべきかどうかを示します。
mhsORAddress	String	X.400 アドレス。
middleName	String	ユーザーのミドルネーム。
mobile	String	第一携帯電話番号。
msCOM-PartitionSetLink	String	COM+ パーティションを COM+ PartitionSet オブジェクトに関連付けるために使用するリンク。読み取り専用。
msCOM-UserLink	String	COM+ PartitionSet をユーザーオブジェクトに関連付けるために使用するリンク。読み取り専用。

スキーマ名	属性タイプ	説明
msCOM-UserPartitionSetLink	String	ユーザーを COM+ PartitionSet に関連付けるために使用するリンク。読み取り専用。
msDS-AllowedToDelegateTo	String	サービスプリンシパル名 (SPN) のリストを格納します。この属性は、Constrained Delegation (制限付き委任) に使用できるサービスチケットを取得できるようサービスを設定するために使用されます。
ms-DS-Approx-Immed-Subordinates	Int	このユーザーの部下のおよその数。読み取り専用。
msDS-Cached-Membership-Time-Stamp	String	セキュリティーアカウントマネージャーによって、トークン評価時にグループ拡張のために使用されます。読み取り専用。
mS-DS-ConsistencyChildCount	Int	この属性は、子オブジェクトの数を比較することで、ディレクトリとその他のオブジェクト、データベース、またはアプリケーションとの間の整合性をチェックするために使用されます。
msExchHomeServerName	String	Exchange Server の名前。次のような形式になります。/o=*EXCHANGEORG*/ou=First Administrative Group/cn=Configuration/cn=Servers/cn=*SERVERNAME*
ms-DS-KeyVersionNumber	Int	このアカウントの現在のキーの Kerberos バージョン番号。これは動的に構築される属性です。読み取り専用。
ms-DS-Mastered-By	String	msDS-hasMasterNC にバックリンクします。読み取り専用。
ms-DS-Members-For-Az-Role-BL	String	メンバーアプリケーショングループまたはユーザーから、そこにリンクしている Az-Role オブジェクトへバックリンクします。読み取り専用。
ms-DS-NC-Repl-Cursors	String	過去および現在のレプリケーションパートナーと、それぞれによる更新状況のリスト。読み取り専用。
ms-DS-NC-Repl-Inbound-Neighbors	String	このパーティションのレプリケーションパートナー。このサーバーは、ここに含まれる他のサーバー (ソースとして機能) からレプリケーションデータを取得します。読み取り専用。

スキーマ名	属性タイプ	説明
ms-DS-NC-Repl-Outbound-Neighbors	String	このパーティションのレプリケーションパートナー。このサーバーは、ここに含まれる他のサーバー (宛先として機能) にレプリケーションデータを送信します。このサーバーは、新しいデータが使用可能になると、これらの他のサーバーに通知します。読み取り専用。
ms-DS-Non-Members-BL	String	メンバーでないグループ/ユーザーから、そこにリンクしている Az グループへバックリンクします。読み取り専用。
ms-DS-Operations-For-Az-Role-BL	String	Az-Operation から、そこにリンクしている Az-Role オブジェクトへバックリンクします。読み取り専用。
ms-DS-Operations-For-Az-Task-BL	String	Az-Operation から、そこにリンクしている Az-Task オブジェクトへバックリンクします。読み取り専用。
ms-DS-Repl-Attribute-Meta-Data	String	レプリケートされた各属性のメタデータのリスト。読み取り専用。
ms-DS-Repl-Value-Meta-Data	String	属性の各値のメタデータのリスト。読み取り専用。
ms-DS-Tasks-For-Az-Role-BL	String	Az-Task から、そこにリンクしている Az-Role オブジェクトへバックリンクします。読み取り専用。
ms-DS-Tasks-For-Az-Task-BL	String	Az-Task から、そこにリンクしている Az-Task オブジェクトへバックリンクします。読み取り専用。
ms-DS-User-Account-Control-ComputedInt		期限切れのユーザーパスワードとロックアウトされたユーザーアカウントを求めるために使われる属性。
msExchMailboxSecurityDescriptor	String	この属性は、ユーザーの Exchange Mailbox 権限を決定します。 詳細は、123 ページの「ACL リストの管理」を参照してください。
ms-Exch-Owner-BL	String	所有者属性へのバックリンク。オブジェクトの所有者のリストを格納します。読み取り専用。
ms-IIS-FTP-Dir	String	ファイルサーバーの共有に関連するユーザーのホームディレクトリ。ms-IID-FTP-Root と組み合わせて使用することで、FTP ユーザーホームディレクトリを決定します。

スキーマ名	属性タイプ	説明
ms-IIS-FTP-Root	String	ファイルサーバーの共有を決定する属性。ms-IID-FTP-Dir と組み合わせて使用することで、FTP ユーザーホームディレクトリを決定します。
name	String	ユーザーの相対識別名 (RDN)。直接設定することはできません。読み取り専用。DN テンプレートまたは accountId アカウント属性を使用して、作成時に RDN を設定します。「name」は予約された属性名なので、スキーママップの左側には使用しないでください。
networkAddress	String	ネットワークセグメントの TCP/IP アドレス。
nTSecurityDescriptor	String	スキーマオブジェクトの NT セキュリティー記述子。 詳細は、123 ページの「ACL リストの管理」を参照してください。
o	String	会社または組織の名前。
objectCategory	なし	このクラスまたは派生したクラスのオブジェクトのグループ化に使用するオブジェクトクラス名。 システムによって設定されます。読み取り専用。
objectClass	なし	このクラスの派生元のクラスのリスト。 この属性の値は、「オブジェクトクラス」リソース属性を使用して設定するようにしてください。読み取り専用。
objectVersion	Int	オブジェクトのバージョン番号。
operatorCount	Int	コンピュータ上のオペレータの数。
otherFacsimileTelephoneNumber	String	代替の FAX 番号のリスト。
otherHomePhone	String	代替の自宅電話番号のリスト。
otherIpPhone	String	電話用の代替の TCP/IP アドレスのリスト。テレフォニーで使用します。
otherLoginWorkstations	String	ここに指定した 非 NT ワークステーションまたは LAN Manager ワークステーションからユーザーがログインできます。
otherMailbox	String	フォームにその他の追加メールアドレスを格納します (CCMAIL: JohnDoe など)。

スキーマ名	属性タイプ	説明
otherMobile	String	追加の携帯電話番号
otherPager	String	追加のポケットベル番号。
otherTelephone	String	追加の電話番号。
ou	String	組織単位
outOfOfficeEnabled	Boolean	不在時の自動返信機能を有効にします
outOfOfficeMessage	String	不在メッセージのテキスト。
pager	String	ポケットベル番号
personalTitle	String	ユーザーの役職
PasswordNeverExpires	Boolean	ユーザーのパスワードが期限切れになるかどうかを示します。
physicalDeliveryOfficeName	String	配達物の送付先となるオフィス。
postalAddress	String	ユーザーの勤務先オフィスの所在地。
postalCode	String	郵便配達用の郵便番号。
postOfficeBox	String	このオブジェクトの私書箱番号。
preferredDeliveryMethod	String	受取人への X.500 優先送付方式。
preferredOU	String	デフォルトでユーザーのデスクトップ上に表示される組織単位。
primaryGroupID	Int	ユーザーがまだグループのメンバーでない場合、primaryGroupID は 2 段階の手順で設定する必要があります。まずユーザーをグループに追加して、次に primaryGroupId を設定します。
primaryInternationalISDNNumber	String	第一 ISDN 番号。
primaryTelexNumber	String	第一テレックス番号。
profilePath	String	ユーザーのプロファイルへのパスを指定します。この値には、NULL 文字列、ローカル絶対パス、または UNC パスを設定できます。
proxyAddresses	String	プロキシアドレスは、Microsoft Exchange Server の受信者オブジェクトが外国のメールシステムで認識されるためのアドレスです。プロキシアドレスは、カスタム受信者や配信リストなど、すべての受信者オブジェクトに必要です。

スキーマ名	属性タイプ	説明
pwdLastSet	String	この属性は、ユーザーが最後にパスワードを変更した時刻を示します。この値は、1601 年 1 月 1 日 0 時 0 分 0 秒からの経過秒数を表す大きな整数として格納されます (FILETIME)。この値がゼロに設定され、ユーザーアカウントの「パスワードを無期限にする」プロパティーが false に設定されている場合、ユーザーは次のログオン時にパスワードを設定する必要があります。
RecipientType	String	すべての Exchange 2007 アカウントタイプで必要です。 指定可能な値は、User、UserMailbox、または MailUser です。 この属性はデフォルトでは表示されません。Exchange 2007 アカウントを管理するには、これを追加する必要があります。
revision	Int	セキュリティー記述子やその他の変更のバージョン。読み取り専用。
rid	Int	オブジェクトの相対識別子。読み取り専用。
sAMAccountName	String	ログイン名。
sAMAccountType	Int	この属性には、すべてのアカウントタイプのオブジェクトに関する情報が格納されます。システムによって設定されます。読み取り専用。
scriptPath	String	ユーザーのログオンスクリプトのパス。この文字列は null にできます。
seeAlso	String	関連するオブジェクトの DN。
serialNumber	String	ユーザーのシリアル番号。Active Directory では使用されません。
servicePrincipalName	String	オブジェクトに関連する識別名のリスト。
showInAddressBook	String	この属性は、オブジェクトが表示される MAPI アドレス帳を指定します。通常は、Exchange 受信者更新サービスによって保守されます。
showInAdvancedViewOnly	Boolean	この属性が UI の詳細モードに表示される場合は true になります。
sn	String	姓
st	String	州名または都道府県名
street	String	街路住所

スキーマ名	属性タイプ	説明
Structural-Object-Class	String	クラス階層に含まれるクラスのリストを格納します (abstract クラスを含む)。読み取り専用。
telephoneNumber	String	第一電話番号。
Terminal Services Initial Program	String	ユーザーのログオン時に実行される初期プログラムのパス。
Terminal Services Initial Program Directory	String	初期プログラムの作業用ディレクトリのパス
Terminal Services Inherit Initial Program	Boolean	クライアントが初期プログラムを指定できるかどうかを示します。 true - クライアントはプログラムを指定できます。 false - **Terminal Services Initial Program** の値が使用され、プログラムの終了時にクライアントはログオフされます。
Terminal Services Allow Logon	Boolean	false - ユーザーはログオンできません。 true - ユーザーはログオンできます。
Terminal Services Active Session Timeout	Integer	時間 (ミリ秒)。値が 0 の場合は、接続タイマーが無効であることを示しています。
Terminal Services Disconnected Session Timeout	Integer	端末サーバーが切断されたセッションを保持する最大時間 (ミリ秒)。 この時間を経過すると、ログオンは強制終了となります。値が 0 の場合は、切断タイマーが無効であることを示しています。
Terminal Services Idle Timeout	Integer	最大アイドル時間 (ミリ秒)。指定した間隔にキーボードやマウスの動きが何もなかった場合、ユーザーのセッションは、Terminal Services End Session On Timeout Or Broken Connection で指定されている値に基づいて、切断または終了します。値が 0 の場合は、アイドルタイマーが無効であることを示しています。
Terminal Services Connect Client Drives At Logon	Boolean	端末サーバーがログオン時にクライアントドライブのマッピングを自動的に再確立するかどうかを示します。 false - サーバーは以前にマップされたクライアントドライブに自動的に接続しません。 true - サーバーはログオン時に、以前にマップされたクライアントドライブに自動的に接続します。

スキーマ名	属性タイプ	説明
Terminal Services Connect Client Printers At Logon	Boolean	端末サーバーがログオン時にクライアントプリンタのマッピングを自動的に再確立するかどうかを示します。 false - サーバーは以前にマップされたクライアントプリンタに自動的に接続しません。 true - サーバーはログオン時に、以前にマップされたクライアントプリンタに自動的に接続します。
Terminal Services Default To Main Client Printer	Boolean	クライアントプリンタがデフォルトのプリンタかどうかを示します。 false - クライアントプリンタはデフォルトのプリンタではありません。 true - クライアントプリンタはデフォルトのプリンタです。
Terminal Services End Session On Timeout Or Broken Connection	Boolean	接続タイマーかアイドルタイマーの期限が切れたとき、または接続エラーによって接続が失われたときのアクションを指定します。 false - セッションが切断されます。 true - セッションが終了します。
Terminal Services Allow Reconnect From Originating Client Only	Boolean	このユーザーの切断されたセッションを再接続できるようにする方法を示します。 false - ユーザーは、任意のクライアントコンピュータにログオンして、切断されたセッションに再接続することができます。 true - ユーザーは、切断されたセッションの確立時に使用したクライアントコンピュータにログオンすることで、その切断されたセッションに再接続できます。
Terminal Services Callback Settings	Integer	端末サーバーのハングアップしたダイアルアップ接続の設定を示し、接続を確立するためにクライアントをコールバックします。 0 - コールバック接続が無効です。 1 - サーバーがユーザーに電話番号の入力を求め、その電話番号でユーザーをコールバックします。 2 - サーバーは、Terminal Services Callback Phone Number 属性によって指定された電話番号で、自動的にユーザーをコールバックします。

スキーマ名	属性タイプ	説明
Terminal Services Callback Phone Number	String	コールバック接続に使用する電話番号。
Terminal Services Remote Control Settings	Integer	ユーザーセッションを追跡できるかどうかを示します。追跡によって、ユーザーは別のユーザーの画面上の操作をリモートで監視できます。 0 - 無効 1 - 入力可能、通知あり 2 - 入力可能、通知なし 3 - 入力不可、通知あり 4 - 入力不可、通知なし
Terminal Services User Profile	String	端末サーバーにログオンするためのユーザーのプロファイルのパス。
Terminal Services Local Home Directory	String	端末サーバーにログオンするためのユーザーのホームディレクトリのパス。
Terminal Services Home Directory Drive	String	Terminal Services Local Home Directory 属性で指定された UNC パスのマップ先のドライブ名 (ドライブ文字とコロン)。
textEncodedORAddress	String	X.400 アドレスをテキスト形式でサポートします。
thumbnailPhoto	Binary	ユーザーの画像。
title	String	ユーザーの役職を格納します。このプロパティーは、一般に、プログラマーのような職種ではなく、「シニアプログラマー」のような正式な役職を示すために使用されます。通常、Esq. や DDS などの敬称には使用されません。
userAccountControl	Int	ユーザーのパスワード、ロックアウト、有効化/無効化、スクリプト、およびホームディレクトリの動作を制御するフラグを指定します。このプロパティーには、オブジェクトのアカウントタイプを示すフラグも格納されます。フラグは LMACCESS.H で定義されます。
userParameters	String	ユーザーのパラメータ。アプリケーションによる使用のために取り置かれるディレクトリの文字列を指します。この文字列は NULL 文字列にできます。 または、終わりを表す NULL 文字の前に任意の数の文字を設定できます。

スキーマ名	属性タイプ	説明
userPassword	暗号化されています	UTF-8 形式のユーザーのパスワード。これは書き込み専用属性です。
userPrincipalName	String	インターネット標準 RFC 822 に基づく、ユーザーのインターネット形式のログイン名。UPN は識別名よりも短く、覚えるのも簡単です。規約により、この名前は、ユーザーの電子メールの名前にマップするようにしてください。
userSharedFolder	String	ユーザーの共有ドキュメントフォルダへの UNC パスを指定します。このパスは \\server\share\directory という形式のネットワーク UNC パスにします。この値は NULL 文字列にすることもできます。
userSharedFolderOther	String	ユーザーの追加の共有ドキュメントフォルダへの UNC パスを指定します。このパスは \\server\share\directory という形式のネットワーク UNC パスにします。この値は NULL 文字列にすることもできます。
userWorkstations	String	コンマで区切られた、ユーザーがログインできるコンピュータの NetBIOS または DNS 名。
usnChanged	String	直前の変更 (作成を含む) に対してローカルディレクトリによって割り当てられた USN 値。読み取り専用。
usnCreated	String	オブジェクト作成時に割り当てられた USN 変更値。
USNIntersite	Int	サイト間のレプリケーションの USN。
uSNLastObjRem	String	サーバーから最後にオブジェクトが削除されたのがいつかを示します。読み取り専用。
uSNSource	String	ローカルサーバーに変更をレプリケートしたリモートディレクトリにあるオブジェクトの USN 変更属性の値。 読み取り専用。
WS_PasswordExpired	Boolean	ユーザーのパスワードを期限切れにするかどうかを示します。
WS_USER_PASSWORD	暗号化されています	ユーザーのパスワードを格納します。詳細については、「使用上の注意」を参照してください。
wbemPath	String	他の ADSI 名前空間にあるオブジェクトへの参照。

スキーマ名	属性タイプ	説明
whenChanged	String	このオブジェクトが最後に変更された日付。読み取り専用。
whenCreated	String	このオブジェクトが作成された日付。読み取り専用。
wWWHomePage	String	ユーザーの第一 Web ページ。
url	String	代替の Web ページのリスト。
x121Address	String	オブジェクトの X.121 アドレス。

Exchange Server 2007 でサポートされるアカウント属性

これらの属性は Exchange Server 2007 固有であり、RecipientType 属性が UserMailbox または MailUser 以外の場合は無視されます。

スキーマ名	属性タイプ	説明
AcceptMessagesOnlyFrom	String	このユーザーへのメール送信を許可されたユーザーのリスト。
AcceptMessagesOnly FromDLMembers	String	このユーザーへのメール送信を許可されたメンバーを含む配布グループのリスト。
Alias	String	ユーザーのエイリアス。
AntispamBypassEnabled	Boolean	このメールボックスでスパム対策処理をスキップするかどうかを指定します。(RecipientType UserMailbox のみ)
CustomAttribute1 through CustomAttribute15	String	追加情報を格納する属性。
DeliverToMailboxAnd Forward	Boolean	このメールボックスに送信されたメッセージを別のアドレスに転送するかどうかを指定します。(RecipientType UserMailbox のみ)
DisplayName	String	Microsoft Outlook で表示される名前。
DowngradeHighPriority MessagesEnabled	Boolean	メールボックスが優先度の高いメッセージを送信できないようにします。(RecipientType UserMailbox のみ)
EmailAddress	String	SMTP メールアドレスであり、PrimarySMTPAddress とは併用できません。

スキーマ名	属性タイプ	説明
EmailAddresses	String	電子メールアドレスのリスト。PrimarySmtpAddress または「True」に設定された EmailAddressPolicyEnabled とは併用できません。
EmailAddressPolicyEnabled	Boolean	デフォルトとして「True」に設定すると、プライマリ電子メールアドレスがユーザー用に生成され、次の属性の使用が禁止されます。 - PrimarySmtpAddress - WindowsEmailAddress
EndDateForRetentionHold	Nullable	メッセージレコード管理 (MRM) の保持期間の最終日 (RecipientType UserMailbox のみ)。
ExternalOofOptions	String	Out of Office メッセージを外部送信者に送信します。値は「InternalOnly」または「External」に限定されます (RecipientType UserMailbox のみ)。
ForwardingAddress	String	DeliverToMailboxAndForward が「True」に設定されている場合、メールの転送先アドレス (RecipientType UserMailbox のみ)。
GrantSendOnBehalfTo	String	このユーザーの代わりにメッセージを送信できるその他の受信者の識別名 (DN)。
HiddenFromAddressListsEnabled	Boolean	アドレスリストから電子メールアドレスを非表示にします。
IssueWarningQuota	Unlimited ByteQuantifiedSize	割り当て警告の発行先のメールボックスのサイズ。(RecipientType UserMailbox のみ)
Languages	String	表示用の言語の一覧。(RecipientType UserMailbox のみ)
MaxBlockedSenders	Nullable	ブロックされた送信者リストに追加できる送信者の最大数。
MaxReceiveSize	Unlimited ByteQantifiedSize	このユーザーが受信できるメッセージの最大サイズ。
MaxSafeSenders	Nullable	安全な送信者リストに追加できる送信者の最大数。(RecipientType UserMailbox のみ)
MaxSendSize	Unlimited ByteQantifiedSize	このユーザーが送信できるメッセージの最大サイズ。
OfflineAddressBook	String	関連付けられたアドレス帳。(RecipientType UserMailbox のみ)

スキーマ名	属性タイプ	説明
PrimarySmtpAddress	String	外部ユーザーがこのユーザーからメッセージを受信したときに、外部ユーザーに表示されるアドレス。EmailAddresses とは併用されません。EmailAddresses リストには PrimarySmtpAddress が含まれています。「True」に設定された EmailAddressPolicyEnabled とは併用できません。
ProhibitSendQuota	Unlimited ByteQantifiedSize	このメールボックスに関連付けられたユーザーがメッセージを送信できなくなる時点のメールボックスサイズ。(RecipientType UserMailbox のみ)
ProhibitSendReceiveQuota	Unlimited ByteQantifiedSize	このメールボックスに関連付けられたユーザーがメッセージを送信または受信できなくなる時点のメールボックスサイズ。(RecipientType UserMailbox のみ)
RecipientLimits	Unlimited	このメールボックスで送信できるメッセージ当たりの送信者の最大数。
RejectMessagesFrom	String	メッセージが拒否される受信者。
RejectMessagesFromDL Members	String	これらの配布リストの任意のメンバーからのメッセージが拒否されます。
RequireSenderAuthentication Enabled	Boolean	送信者は認証される必要があります。
RetainDeletedItemsFor	String	削除されたアイテムを保持する期間を指定する「dd.hh:mm:ss」の文字列形式で表現されるタイムスパン。(RecipientType UserMailbox のみ)
RetainDeletedItemsUntilBackup	Boolean	削除された項目を次回のバックアップまで保持します。(RecipientType UserMailbox のみ)
RetentionHoldEnabled	Boolean	保持をオンまたはオフに切り替えます (RecipientType UserMailbox のみ)。
RulesQuota	ByteQuantifiedSize	このメールボックスに対する規則のサイズ制限。最大値は 256K バイトです (RecipientType UserMailbox のみ)。
SCLDeleteEnabled	Nullable Boolean	SCL 削除のしきい値を満たしたメッセージを削除します (RecipientType UserMailbox のみ)。
SCLDeleteThreshold	Nullable	メールが削除される時点の Spam Confidence Level。指定できる値は 0 ～ 9 です。(RecipientType UserMailbox のみ)

スキーマ名	属性タイプ	説明
SCLJunkEnabled	Nullable Boolean	SCL ジャンクのしきい値を満たしたメッセージをジャンクとします (RecipientType UserMailbox のみ)。
SCLJunkThreshold	Nullable	メールがジャンクとしてマークされる時点の Spam Confidence Level。 許可される値は 0-9 です (RecipientType UserMailbox のみ)。
SCLQuarantineEnabled	Nullable Boolean	SCL 隔離のしきい値を満たしたメッセージを隔離します (RecipientType UserMailbox のみ)。
SCLQuarantineThreshold	Nullable	メールが隔離される時点の Spam Confidence Level。 許可される値は 0-9 です (RecipientType UserMailbox のみ)。
SCLRejectEnabled	Nullable Boolean	SCL 拒否のしきい値を満たしたメッセージを拒否します (RecipientType UserMailbox のみ)。
SCLRejectThreshold	Nullable	メールが拒否される時点の Spam Confidence Level。 許可される値は 0-9 です (RecipientType UserMailbox のみ)。
SimpleDisplayName	String	DisplayName の ASCII のみのバージョン。
StartDateForRetentionHold	Nullable	MRM の保持期間の開始日。(RecipientType UserMailbox のみ)
UseDatabaseQuotaDefaults	Boolean	このメールボックスが存在するメールボックスデータベースに指定された割り当て属性を、このメールボックスで使用するように指定します。(RecipientType UserMailbox のみ)
UseDatabaseRetentionDefaults	Boolean	このメールボックスが存在するメールボックスデータベースに指定された MailboxRetention 属性を、このメールボックスで使用するように指定します。(RecipientType UserMailbox のみ)
UserPrincipalName	String	これはユーザーのログオン名です。UPN はユーザー名とサフィックスで構成されます。

ACL リストの管理

`nTSecurityDescriptor` および `msExchMailboxSecurityDescriptor` 属性値には、特別な方法で指定する ACL リストが含まれています。

次に、企業がプロビジョニングする各ユーザーに対してデフォルトのアクセス権のセットを割り当てる場合に使用する可能性があるユーザーフォームの例を示します。

```
<Field name='attributes[AD].nTSecurityDescriptor' hidden='true'>
  <Expansion>
      <list>
        <s>Domain Admins|983551|0|0|NULL|NULL</s>
        <s>NT AUTHORITY\SYSTEM|983551|0|0|NULL|NULL</s>
         <s>Account Operators|983551|0|0|NULL|NULL</s>
         <s>NT AUTHORITY\Authenticated Users|131220|0|0|NULL|NULL</s>
        <s>NT AUTHORITY\Authenticated Users|256|5|0|
{AB721A55-1E2F-11D0-9819-00AA0040529B}|NULL</s>
         <s>NT AUTHORITY\SELF|131220|0|0|NULL|NULL</s>
      </list>
   </Expansion>
</Field>
```

nTSecurityDescriptor リスト内のエントリは、次の形式になります。

```
Trustee|Mask|aceType|aceFlags|objectType|InheritedObjectType
```

各表記の意味は次のとおりです。

- `Trustee` は、ユーザーの `DOMAIN\Account` です。
- `Mask` は、アクセス権 (読み取り、書き込みなど) を指定するフラグです。
- `aceType` は、アクセス制御エントリ (`ACE`) のタイプを示すフラグです。

  ```
  ADS_ACETYPE_ACCESS_ALLOWED = 0,
   ADS_ACETYPE_ACCESS_DENIED = 0x1,
  ADS_ACETYPE_SYSTEM_AUDIT = 0x2,
   ADS_ACETYPE_ACCESS_ALLOWED_OBJECT = 0x5,
   ADS_ACETYPE_ACCESS_DENIED_OBJECT = 0x6,
   ADS_ACETYPE_SYSTEM_AUDIT_OBJECT = 0x7,
   ADS_ACETYPE_SYSTEM_ALARM_OBJECT = 0x8 ADS_ACETYPE_ACCESS_ALLOWED
  ```

  各表記の意味は次のとおりです。

  - **ADS_ACETYPE_ACCESS_ALLOWED**: `ACE` は標準の `ACCESS ALLOWED` タイプになります。ここで、`ObjectType` および `InheritedObjectType` フィールドは `NULL` です。
  - **ADS_ACETYPE_ACCESS_DENIED**: `ACE` は標準のシステム監査タイプになります。ここで、`ObjectType` および `InheritedObjectType` フィールドは`NULL` です。
  - **ADS_ACETYPE_SYSTEM_AUDIT**: `ACE` は標準システムタイプになります。ここで、`ObjectType` および `InheritedObjectType` フィールドは `NULL` です。
  - **ADS_ACETYPE_ACCESS_ALLOWED_OBJECT**: Windows 2000 で、`ACE` は、オブジェクトまたはオブジェクトのサブオブジェクト (プロパティーやプロパティーのセットなど) へのアクセスを許可します。

ObjectType、InheritedObjectType、またはこれら両方に、プロパティーセット、プロパティー、拡張された権限、または子オブジェクトのタイプを特定する GUID が格納されます。

- **ADS_ACETYPE_ACCESS_DENIED_OBJECT**: Windows 2000 で、ACE オブジェクトまたはオブジェクトのサブオブジェクト (プロパティーやプロパティーのセットなど) へのアクセスを拒否します。

  ObjectType、InheritedObjectType、またはこれら両方に、プロパティーセット、プロパティー、拡張された権限、または子オブジェクトのタイプを特定する GUID が格納されます。

- **ADS_ACETYPE_SYSTEM_AUDIT_OBJECT**: Windows 2000 で、ACE オブジェクトまたはオブジェクトのサブオブジェクト (プロパティーやプロパティーのセットなど) へのアクセスを監査します。

  ObjectType、InheritedObjectType、またはこれら両方に、プロパティーセット、プロパティー、拡張された権限、または子オブジェクトのタイプを特定する GUID が格納されます。

- **ADS_ACETYPE_SYSTEM_ALARM_OBJECT**: 現時点で Windows 2000/XP では使用されません。

aceFlags は、ほかのコンテナやオブジェクトが ACL 所有者から ACE を継承できるかどうかを指定するフラグです。

```
ADS_ACEFLAG_INHERIT_ACE = 0x2,
 ADS_ACEFLAG_NO_PROPAGATE_INHERIT_ACE = 0x4,
 ADS_ACEFLAG_INHERIT_ONLY_ACE = 0x8,
 ADS_ACEFLAG_INHERITED_ACE = 0x10,
 ADS_ACEFLAG_VALID_INHERIT_FLAGS = 0x1f,
 ADS_ACEFLAG_SUCCESSFUL_ACCESS = 0x40,
```

各表記の意味は次のとおりです。

- **ADS_ACEFLAG_FAILED_ACCESS = 0x80 ADS_ACEFLAG_INHERIT_ACE**: このアクセス制御エントリ (ACE) を継承する子オブジェクトを示します。

  継承される ACE は、ADS_ACEFLAG_NO_PROPAGATE_INHERIT_ACE フラグを設定しない限り継承可能です。

- **ADS_ACEFLAG_NO_PROPAGATE_INHERIT_ACE**: 子オブジェクトの継承した ACE の ADS_ACEFLAG_INHERIT_ACE フラグが、システムによってクリアされます。これによって、ACE は、以降の世代のオブジェクトには継承されません。

- **ADS_ACEFLAG_INHERIT_ONLY_ACE**: 接続先のオブジェクト上でアクセス制御を実行しない継承専用の ACE を示します。

  このフラグを設定しない場合、ACE は、接続先のオブジェクト上でアクセス制御を実行する有効な ACE になります。

- **ADS_ACEFLAG_INHERITED_ACE**: ACE が継承されたかどうかを示します。このビットはシステムによって設定されます。

- **ADS_ACEFLAG_VALID_INHERIT_FLAGS**: 継承されたフラグが有効かどうかを示します。このビットはシステムによって設定されます。
- **ADS_ACEFLAG_SUCCESSFUL_ACCESS**: アクセスに成功した場合に、監査メッセージを生成し、システムアクセス制御リスト (SACL) でシステムを監査する ACE によって使用されます。
- **ADS_ACEFLAG_FAILED_ACCESS**: アクセスに失敗した場合に、監査メッセージを生成し、SACL でシステムを監査する ACE によって使用されます。

objectType は、ADSI オブジェクトタイプを示すフラグです。objectType の値は、文字列形式のプロパティーまたはオブジェクトの GUID です。

- この GUID は、ADS_RIGHT_DS_READ_PROP および ADS_RIGHT_DS_WRITE_PROP アクセスマスクの使用時に、プロパティーを参照します。
- この GUID は、ADS_RIGHT_DS_CREATE_CHILD および ADS_RIGHT_DS_DELETE_CHILD アクセスマスクの使用時に、オブジェクトを指定します。

InheritedObjectType は、ADSI オブジェクトの子オブジェクトのタイプを示すフラグです。InheritedObjectType の値は、オブジェクトに対する文字列形式の GUID です。このような GUID を設定する場合、ACE は、その GUID によって参照されるオブジェクトのみに適用されます。

objectType および InheritedObjectType フラグでは、ほかのオブジェクトの GUID を次の形式で指定します。

```
{BF9679C0-0DE6-11D0-A285-00AA003049E2}
```

オブジェクト/属性の GUID は、角括弧 { } で囲まれます。この形式は、取得したときに返されます。ADSI 内には、アクセスを許可する特定の属性や、継承関係の記述方法を表す GUID が存在しています。

渡していく正しい文字列を見つけるには、次の方法を実行します。

▼ 渡していく正しい文字列を見つける

1 スキーマに属性を追加し、次のフィールドをユーザーフォームに追加します。

```
<Field name='accounts[AD].nTSecurityDescriptor'>
  <Display class='TextArea'>
    <Property name='title' value='NT User Security Descriptor'/>
    <Property name='rows' value='20'/>
    <Property name='columns' value='100'/>
  </Display>
</Field>
```

または

```
<Field name='accounts[AD].msExchMailboxSecurityDescriptor'>
  <Display class='TextArea'>
    <Property name='title' value='Mailbox Security Descriptor'/>
    <Property name='rows' value='20'/>
    <Property name='columns' value='100'/>
  </Display>
</Field>
```

2 **Active Directory** でユーザーのオブジェクトを編集して、すべてのユーザーに対応する **ACL** リストを設定し、ベースラインを確立します。

3 **Edit User Form** を使って、**Identity Manager** で、ユーザーを編集します。

テキスト領域に、Active Directory のユーザーオブジェクトから取得された対応する値が入力されていることを確認します。

上記の方法は、必要な設定のために、フォームに追加する値を決定する場合に役立ちます。

サポートされない属性

次の表に、Identity Manager でサポートされないアカウント属性を示します。

スキーマ名	注意点
allowedAttributes	オペレーショナル属性
allowedAttributesEffective	オペレーショナル属性
allowedChildClasses	オペレーショナル属性
alowedChildClassesEffective	オペレーショナル属性
bridgeheadServerListBL	システムが使用します
canonicalName	オペレーショナル属性
controlAccessRights	String (Octet)
createTimeStamp	String (UTC-Time)
dBCSPwd	String (Octet)
directReports	システムが使用します。このユーザーによって管理されるユーザーのマネージャー属性を使用して設定します。
dSASignature	Object(Replica-Link)

スキーマ名	注意点
dSCorePropagationData	String (UTC-Time)
fromEntry	オペレーショナル属性
frsComputerReferenceBL	システムが使用します
fRSMemberReferenceBL	システムが使用します
fSMORoleOwner	システムが使用します
groupMembershipSAM	String (Octet)
instanceType	システムが使用します
isCriticalSystemObject	システムが使用します
isDeleted	システムが使用します
isPrivilegeHolder	システムが使用します
lastKnownParent	システムが使用します
lmPwdHistory	String (Octet)
logonHours	String (Octet)
logonWorkstations	String (Octet)
masteredBy	システムが使用します。
memberOf	システムが使用します。groups 属性を使用します。
modifyTimeStamp	String (UTC-Time)
MS-DRM-Identity-Certificate	String (Octet)
ms-DS-Cached-Membership	String (Octet)
mS-DS-ConsistencyGuid	String (Octet)
mS-DS-CreatorSID	String (Sid)
ms-DS-Site-Affinity	String (Octet)
mSMQDigests	String (Octet)
mSMQDigestsMig	String (Octet)
mSMQSignCertificates	String (Octet)
mSMQSignCertificatesMig	String (Octet)
msNPAllowDialin	RAS MPR API を使用して、値の読み取りと更新を行います。
msNPCallingStation	RAS MPR API を使用して、値の読み取りと更新を行います。

スキーマ名	注意点
msNPSavedCallingStationID	RAS MPR API を使用して、値の読み取りと更新を行います。
msRADIUSCallbackNumber	RAS MPR API を使用して、値の読み取りと更新を行います。
msRADIUSFramedIPAddress	RAS MPR API を使用して、値の読み取りと更新を行います。
msRADIUSFramedRoute	RAS MPR API を使用して、値の読み取りと更新を行います。
msRADIUSServiceType	RAS MPR API を使用して、値の読み取りと更新を行います。
msRASSavedCallbackNumber	RAS MPR API を使用して、値の読み取りと更新を行います。
msRASSavedFramedIPAddress	RAS MPR API を使用して、値の読み取りと更新を行います。
msRASSavedFramedRoute	RAS MPR API を使用して、値の読み取りと更新を行います。
netbootSCPBL	システムが使用します
nonSecurityMemberBL	システムが使用します
ntPwdHistory	システムが使用します
objectGUID	String (Octet)。この GUID は、アカウントの Identity Manager ユーザーオブジェクトの ResourceInfo に格納されます。
objectSid	String (Sid)
otherWellKnownObjects	Object (DN-Binary)
partialAttributeDeletionList	システムが使用します
partialAttributeSet	システムが使用します
possibleInferiors	システムが使用します
proxiedObjectName	Object (DN-Binary)
queryPolicyBL	システムが使用します
registeredAddress	String (Octet)
replPropertyMetaData	システムが使用します
replUpToDateVector	システムが使用します
repsFrom	システムが使用します
repsTo	システムが使用します
sDRightsEffective	オペレーショナル属性
securityIdentifier	String (Sid)
serverReferenceBL	システムが使用します

スキーマ名	注意点
sIDHistory	String (Sid)
siteObjectBL	システムが使用します
subRefs	システムが使用します
subSchemaSubEntry	システムが使用します
supplementalCredentials	システムが使用します
systemFlags	システムが使用します
telexNumber	String (Octet)
teletexTerminalIdentifier	String (Octet)
terminalServer	String (Octet)
thumbnailLogo	String (Octet)
tokenGroups	String (Sid) / オペレーショナル属性
tokenGroupsGlobalAndUniversal	String (Sid)
tokenGroupsNoGCAcceptable	String (Sid) / オペレーショナル属性
unicodePwd	String (Octet)。userPassword を使用して、ユーザーのパスワードを設定します。
userCert	String (Octet)
userCertificate	String (Octet)
userSMIMECertificate	String (Octet)
wellKnownObjects	Object (DN-String)
x500uniqueIdentifier	String (Octet)

リソースオブジェクトの管理

Identity Manager は、次の Active Directory オブジェクトをサポートします。

リソースオブジェクト	サポートされる機能	管理される属性
Group	作成、更新、削除	cn、samAccountName、description、managedby、member、r
DNS Domain	Find	dc
Organizational Unit	作成、削除、検索	ou

リソースオブジェクト	サポートされる機能	管理される属性
Container	作成、削除、検索	cn、description

リソースオブジェクト上で管理できる属性は、一般に、属性構文によって指示することもできます。これらのオブジェクトタイプの属性は、ユーザーアカウントの属性と類似しているので、同じようにサポートされています。

アイデンティティーテンプレート

Windows Active Directory は、階層ベースのリソースです。アイデンティティーテンプレートによって、ユーザーが作成するディレクトリツリー内のデフォルトの場所が指定されます。デフォルトのアイデンティティーテンプレートは次のとおりです。

```
CN=$fullname$,CN=Users,DC=mydomain,DC=com
```

デフォルトのテンプレートを有効な値に置き換えてください。

サンプルフォーム

ここでは、Active Directory リソースアダプタに用意されているサンプルフォームの一覧を示します。

組み込みのフォーム

- ActiveDirectory ActiveSync Form
- Windows Active Directory コンテナ作成フォーム
- Windows Active Directory グループ作成フォーム
- Windows Active Directory 組織単位作成フォーム
- Windows Active Directory Create Person Form
- Windows Active Directory ユーザー作成フォーム
- Windows Active Directory コンテナ更新フォーム
- Windows Active Directory グループ更新フォーム
- Windows Active Directory 組織単位更新フォーム
- Windows Active Directory Update Person Form
- Windows Active Directory ユーザー更新フォーム

その他の利用可能なフォーム

`ADUserForm.xml`

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

```
com.waveset.adapter.ADSIResourceAdapter
```

また、Identity Manager のデバッグページを使用して、ゲートウェイサービス上でトレースを有効にすることもできます (*InstallDir*/idm/debug/Gateway.jsp)。このページでは、トレースのレベル、トレースファイルの場所、およびトレースファイルの最大サイズを指定できます。また、ゲートウェイのトレースファイルをリモートで取得して、ゲートウェイのバージョン情報を表示することもできます。

さまざまなコマンド行スイッチによって、デバッグトレースをしているコンソールから、ゲートウェイサービスを起動することもできます。-h を使用して、ゲートウェイサービスの使用方法を確認してください。

接続の問題を診断するために、次のメソッドでトレースを有効にすることもできます。

- com.waveset.adapter.AgentResourceAdapter#sendRequest
- com.waveset.adapter.AgentResourceAdapter#getResponse

◆ ◆ ◆ 第 7 章

7 AIX

AIX リソースアダプタは、com.waveset.adapter.AIXResourceAdapter クラスで定義されます。

アダプタの詳細

リソースを設定する際の注意事項

リソースと Identity Manager 間の通信に SSH (Secure Shell) を使用する場合は、アダプタを設定する前に、リソースで SSH を設定します。

Identity Manager のインストールに関する注意事項

このリソースでは、追加のインストール手順は必要ありません。

使用上の注意

AIX リソースアダプタは、主に次の AIX コマンドのサポートを提供します。

- mkuser、chuser、rmuser
- mkgroup、chgroup、rmgroup
- passwd、pwdadm

注 – サポートされる属性およびファイルの詳細については、これらのコマンドに関する AIX マニュアルページを参照してください。

UNIX リソース (AIX、HP-UX、Solaris、または Linux) に接続するときは、root シェルとして Bourne 互換シェル (sh、ksh) を使用してください。

AIX アカウントを管理する管理アカウントには、英語 (en) または C ロケールを使用してください。これは、ユーザーの `.profile` ファイルで設定できます。

NIS が実装されている環境では、次の機能を実装することにより、一括プロビジョニング中のパフォーマンスを向上させることができます。

- `user_make_nis` という名前のアカウント属性をスキーママップに追加し、この属性を調整やその他の一括プロビジョニングワークフローで使用します。この属性を追加した場合、リソース上の各ユーザーが更新された後は、システムで NIS データベースへの接続手順がバイパスされます。
- すべてのプロビジョニングが完了した後で NIS データベースに変更を書き込むには、ワークフローで `NIS_password_make` という名前の ResourceAction を作成します。

ユーザーパスワードに制御文字 (0x00、0x7f など) を使用しないでください。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は、次の接続を使用して AIX アダプタと通信します。

- Telnet
- SSH (SSH はリソース上に個別にインストールする)
- SSHPubKey

SSHPubKey 接続の場合、「リソースパラメータ」ページで非公開鍵を指定する必要があります。この鍵には `--- BEGIN PRIVATE KEY ---` および `--- END PRIVATE KEY --` のような注釈行を含める必要があります。公開鍵は、サーバー上の `/.ssh/authorized_keys` ファイルに配置する必要があります。

必要な管理特権

ユーザーやグループを管理するには、管理者が root ユーザーであるか、セキュリティーグループのメンバーである必要があります。

このアダプタでは、一般ユーザーとしてログインしてから su コマンドを実行し、root ユーザー (または root ユーザーと同等のアカウント) に切り替えて管理アクティビティーを実行できます。 また、root ユーザーとして直接ログインすることもできます。また、root ユーザーとして直接ログインすることもできます。

さらに、sudo 機能 (バージョン 1.6.6 以降) もサポートしており、これは AIX Toolbox から AIX にインストールできます。sudo 機能を使用すると、システム管理者は特定のユーザー (またはユーザーのグループ) に、root ユーザーまたは別のユーザーとして一部 (またはすべて) のコマンドを実行する機能を提供することができます。

さらに、sudo がリソースで有効になっている場合は、その設定が、root ユーザーおよび管理者ユーザーのリソース定義ページでの設定よりも優先されます。

sudo を使用する場合は、Identity Manager 管理者に対して有効にされたコマンドの `tty_tickets` パラメータを true に設定する必要があります。詳細については、sudoers ファイルのマニュアルページを参照してください。

管理者は、sudo で次のコマンドを実行する特権が付与されている必要があります。

ユーザー、グループ、およびセキュリティーコマンド		NIS コマンド	その他のコマンド	
■ `chgroup`	■ `rmgroup`	■ `make`	■ `awk`	■ `grep`
■ `chgrpmem`	■ `rmuser`	■ `ypcat`	■ `cat`	■ `ls`
■ `chsec`	■ `passwd`	■ `ypmatch`	■ `cd`	■ `mv`
■ `chuser`	■ `pwdadm`	■ `yppasswd`	■ `chmod`	■ `rm`
■ `lsgroup`			■ `chown`	■ `sed`
■ `lssec`			■ `cp`	■ `sleep`
■ `lsuser`			■ `cut`	■ `sort`
■ `mkgroup`			■ `diff`	■ `tail`
■ `mkuser`			■ `echo`	■ `touch`

テスト接続を使用して次のテストができます。

- 各コマンドが管理ユーザーのパスに存在するかどうか
- 管理ユーザーが /tmp に書き込めるかどうか
- 管理ユーザーに、特定のコマンドを実行する権限があるかどうか

注 – テスト接続では、通常のプロビジョニングの実行とは異なるコマンドオプションを使用できます。

このアダプタには、基本的な sudo 初期化機能とリセット機能が用意されています。ただし、リソースアクションが定義されていて、そこに sudo 認証を必要とするコマンドが含まれている場合は、UNIX コマンドとともに sudo コマンドを指定して

ください。たとえば、単に useradd と指定する代わりに sudo useradd を指定してください。sudo を必要とするコマンドは、ネイティブリソースに登録されている必要があります。それらのコマンドを登録するには、visudo を使用します。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	なし
パススルー認証	あり
前アクションと後アクション	あり
データ読み込みメソッド	■ リソースから直接インポート ■ リソースの調整

このリソース上のすべてのユーザーに対して、次のタスクを制御するリソース属性を定義できます。

- ユーザーの作成時にホームディレクトリを作成する
- ユーザーの作成時にユーザーのホームディレクトリにファイルをコピーする
- ユーザーの削除時にホームディレクトリを削除する

アカウント属性

次の表に、AIX ユーザーのアカウント属性を示します。属性の型はすべて String です。特に記載されていないかぎり、属性は省略可能です。

リソースユーザー属性	**mkuser** での指定方法	説明
accountId	login_name	必須。ユーザーのログイン名。
account_locked	account_locked=[true | false]	ユーザーアカウントがロックされているかどうかを示します。
admin	admin=[true|false]	ユーザーの管理ステータスを定義します。

リソースユーザー属性	**mkuser**での指定方法	説明
daemon	daemon=[true|false]	ユーザーが cron または SRC デーモンを使用してプログラムを実行できるかどうかを示します。
expires	expires=MMDDhhmmyy	アカウントの有効期限。
gecos	gecos=String	ユーザーに関する全般的な情報。
groups	groups=GroupNames	ユーザーの属しているグループ名のコンマ区切りリスト。
home	home=PathName	ユーザーのホームディレクトリへのフルパス。このアカウント属性で指定された値はすべて、「ホームベースディレクトリ」リソース属性で指定された値よりも優先されます。
id	id=Integer	ユーザー ID を表す一意の整数文字列。
login	login=[true | false]	ユーザーがログインコマンドを使用してシステムにログインできるかどうかを示しています。
loginretries	loginretries=attempts	最後に正常にログインしてからシステムがそのアカウントをロックするまでに許可されるログイン試行の失敗回数。
maxage	maxage=weeks	パスワードの最大有効期間 (週)。
maxexpired	maxexpired=weeks	maxage で定義されている期間を過ぎたあとも、ユーザーが期限切れパスワードを変更できる期間の最大値 (週)。
pgrp	pgrp=GroupName	ユーザーの一次グループ。
rlogin	rlogin=[true | false]	telnet または rlogin コマンドを使用した、リモートの場所からアカウントへのアクセスを許可します。
shell	shell=PathName	セッションの開始時にユーザーに対して実行されるプログラム。 NIS マスターにプロビジョニングしている場合は、ユーザーシェルの値は NIS マスターに対してのみチェックされます。ユーザーがログオンする可能性のあるその他のマシンに対してチェックは実行されません。
su	su=[true | false]	別のユーザーが su コマンドで指定のユーザーアカウントに切り替えることができるかどうかを示します。

リソースユーザー属性	**mkuser** での指定方法	説明
umask	umask=Value	ファイルのアクセス権を設定します。

リソースオブジェクトの管理

Identity Manager は、次のネイティブ AIX オブジェクトをサポートします。

リソースオブジェクト	サポートされる機能	管理される属性
Group	作成、更新、削除、名前を付けて保存	`groupName、admin、users`

アイデンティティーテンプレート

$accountId$

サンプルフォーム

組み込みのフォーム

- AIX Group Create Form
- AIX Group Update Form

その他の利用可能なフォーム

`AIXUserForm.xml`

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

- `com.waveset.adapter.AIXResourceAdapter`
- `com.waveset.adapter.ScriptedConnection`

◆ ◆ ◆ 第 8 章

BridgeStream SmartRoles

BridgeStream SmartRoles アダプタは、ユーザーを SmartRoles にプロビジョニングします。このアダプタは、これらのユーザーを SmartRoles 内で適切な組織に配置することで、これらのユーザーが持つべきビジネスロールを SmartRoles によって決定できるようにします。

アダプタの詳細

SmartRoles からユーザーを検出するときに、アダプタはユーザーのビジネスロールを検出します。これらのビジネスロールは、ユーザーに割り当てる必要のある Identity Manager のロール、リソース、属性、およびアクセスを決定するために、Identity Manager 内で使用できます。

さらに、SmartRoles を、Active Sync を使用するユーザー変更のソースにすることもできます。SmartRoles ユーザーを Identity Manager にロードして、それらを調整できます。

BridgeStream SmartRoles リソースアダプタ
は、`com.waveset.adapter.SmartRolesResourceAdapter` クラスで定義されます。

リソースを設定する際の注意事項

なし

Identity Manager のインストールに関する注意事項

SmartRoles アダプタは、カスタムアダプタです。インストールプロセスを完了するには、次の手順を実行してください。

▼ SmartRules アダプタをインストールする

1 **SmartRoles** リソースを **Identity Manager** のリソースリストに追加するには、「管理するリソースの設定」ページの「カスタムリソース」セクションに次の値を追加する必要があります。

```
com.waveset.adapter.SmartRolesResourceAdapter
```

2 次の **JAR** ファイルを、**SmartRoles** インストールディレクトリ (*SR_install_dir*/Foundation/lib) から $WSHOME/WEB-INF/lib にコピーします。

- bridgestream-common.jar
  - jgroups-all.jar
  - log4j-1.2.8.jar
  - rowset.jar
  - fxrm.jar
  - jmxri.jar
  - ojdbc14.jar
  - jcert.jar
  - jmxtools.jar
  - ojdbc14_g.jar

3 次のファイルを、*SR_install_dir* /Foundation/config ディレクトリから $WSHOME/WEB-INF/classes ディレクトリにコピーします。

- bridgestream_jaas.config
  - log4j.properties
  - foundation_config.xml
  - foundation_config.dtd

4 log4j.properties ファイルを編集して、log4j.appender.debuglog.File および log4j.appender.logfile.File プロパティーファイル内のログファイルへのパスを指定します。これらのプロパティーは両方とも同じファイルを指定できます。

5 **Identity Manager** を実行している **JVM** に、次の **Java** システムプロパティーを設定します。

システムプロパティー	値
java.security.auth.login.config	bridgestream_jaas.config ファイルへのパス
brLoggingConfig	log4j.properties ファイルへのパス
brfConfig	foundation_config.xml および foundation_config.dtd ファイルへのパス

注 – これらのプロパティーを JVM のコマンド行に指定する必要がある場合は、 -D オプションを使用して、次のようにプロパティーを設定します。

```
-Djava.security.auth.login.config=PathToBridgestream_jaas.config
-DbrLoggingConfig=PathTolog4j.properties
-DbrfConfig=PathTofoundation_config.xml and  foundation_config.dtd files
```

使用上の注意

ここでは、SmartRoles リソースアダプタの使用に関連する情報を提供します。説明する内容は次のとおりです。

- 全般的な注意事項
- Complex 属性のサポート
- 制限事項

全般的な注意事項

このリソースに関する全般的な注意事項は次のとおりです。

- SmartRoles アダプタは SmartRoles リポジトリと直接通信するため、このアダプタを動作させるために Relationship Manager アプリケーションを実行する必要はありません。
- このアダプタは汎用 ID を生成し、設定ファイル内に接続情報を格納できます。

  SmartRoles アダプタを設定するときに、SmartRoles で新しいアカウントの汎用 ID を生成するか、アダプタで汎用 ID を提供するかを選択できます。アダプタで ID を提供する場合は、アイデンティティーテンプレートで生成された値が使用されます。

Complex 属性のサポート

Identity Manager では新しい *complex* 属性タイプが導入され、これによって SmartRoles アダプタが複雑な属性をサポートできるようになりました。この complex 属性タイプは、属性値が単一の値や値のリストよりも複雑な場合に使用されます。この新しい complex タイプは、次の属性とともに使用されます。

- `sr_positions`
- `sr_grantedRolesSphere`
- `sr_organizations`

Complex 属性の属性値は、新しい `com.waveset.object.GenericAttribute` クラスのインスタンスです。`GenericAttribute` インスタンスは、実際の属性値情報を格納している `GenericObject` インスタンスをラップします。`GenericObject` は、パス表現を使用して設定および取得できる階層内に、属性と値を格納します。

ResourceAction のサポート

このアダプタは before および after アクションをサポートしていませんが、runResourceAction プロビジョニングワークフローサービスを使用して、実行中のアクションをサポートしています。SmartRoles アクションは JavaScript または BeanShell で作成でき、作成されたアクションは SmartRoles API を呼び出してワークフローの一部としてカスタム動作を実行できます。アクションスクリプトへの入力は、actionContext という名前のマップオブジェクトに格納されます。actionContext マップに格納される内容は次のとおりです。

キー	値
action	実行しているアクションのタイプを説明する文字列。現在、このアクションを run 以外にすることはできません。
adapter	com.waveset.adapter.SmartRolesResourceAdapter インスタンスへの参照を格納します。
additionalArgs	runResourceAction プロビジョニングワークフローサービスの呼び出しに渡される追加の引数を格納するマップです。
result	runResourceAction プロビジョニングワークフローサービスの呼び出しから返される WavesetResult への参照。
session	SmartRoles の IOMSession インスタンスへの参照。セッションは、SmartRoles リソースで定義される管理者とパスワードを使用して作成されます。
trace	com.waveset.adapter.SmartRolesResourceAdapter クラスに関連付けられた com.sun.idm.logging.trace.Trace インスタンスへの参照。これを使用して、アクションスクリプトのデバッグに使用するためのトレースメッセージを出力できます。

次に示す ResourceAction XML は、BeanShell アクションの例です。JavaScript アクションの場合は actionType を JAVASCRIPT に設定します。このアクションは、additionalArgs マップから取得された user という名前の引数を使用し、SmartRoles リポジトリを検索して、user 引数の値と一致する LOGON_ID を持つ 1 つ以上の Person オブジェクトを見つけます。すると、一致したそれぞれの Person の文字列表現は、ACTION_RC ResultItem 内の WavesetResult に返されます。

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE ResourceAction PUBLIC 'waveset.dtd' 'waveset.dtd'>
<!--  MemberObjectGroups="#ID#Top"-->
<ResourceAction createDate='1148443502593'>
   <ResTypeAction restype='SmartRoles' timeout='0' actionType='BEANSHELL'>
      <act>
         import bridgestream.core.*;
         import bridgestream.util.*;
         import bridgestream.temporal.person.*;
```

```
            import java.util.*;
            import com.waveset.object.*;
            IOMSession session = actionContext.get("session");
            OMEngine engine = OMEngine.getInstance(session);
            String user = actionContext.get("additionalArgs").get("user");
            UTNameValuePair[] criteria = new UTNameValuePair[] { new UTNameValuePair
               ("LOGON_ID", user) };
            UTTimestamp time = UTTimestamp.getSystemTimestamp();
            List list = session.search("PERSON", criteria, time, null, null);
            Iterator iter = list.iterator();
            StringBuffer buf = new StringBuffer();
            while (iter.hasNext()) {
               ENPerson person = (ENPerson)iter.next();
               buf.append(person.toString());
               buf.append("\n\n");
            }
            WavesetResult result = actionContext.get("result");
            result.addResult("ACTION_RC", buf.toString());
         </act>
      </ResTypeAction>
      <MemberObjectGroups>
         <ObjectRef type='ObjectGroup' id='#ID#Top' name='Top'/>
      </MemberObjectGroups>
   </ResourceAction>
```

制限事項

現在、このアダプタには次のような制限があります。

- ロールは、SmartRoles の person オブジェクトにのみ許可されます。position オブジェクトにロールを許可することはできません。
- Identity Manager では、1 つの SmartRoles インストールとの通信のみ設定できます。
- 許可されたロール範囲の制御を割り当てる場合、その範囲の制御内の組織には、直接割り当てられた組織だけでなく、それらの組織のすべての子孫も含まれます。割り当て済みの組織の子孫を割り当てようとすると、エラーが発生します。
- アダプタは SmartRoles の組織を名前で参照するため、SmartRoles 内の組織名は一意にしてください。
- SmartRoles の person オブジェクトを position に割り当てるときに、アダプタは使用可能な position を見つけようとはしません。代わりに、アダプタは常に新しい position オブジェクトを作成し、person オブジェクトをその新しい position に割り当てます。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

SmartRoles アダプタは、SmartRoles インストールからコピーされた設定ファイルの指定どおりに、SmartRoles リポジトリと通信します。この接続設定の詳細については、SmartRoles 製品のマニュアルを参照してください。

必要な管理特権

アダプタが SmartRoles に接続するために使用するユーザーには、SmartRoles ユーザーを管理できるロール (SmartRoles 管理者ロールなど) を割り当ててください。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	あり アカウントを無効にすると、アカウントは SmartRoles にログインできなくなります。
アカウントの名前の変更	あり
パススルー認証	なし
前アクションと後アクション	なし `runResourceAction` プロビジョニングワークフローサービスを使用して、ワークフローからアクションを実行できます。詳細については、「ResourceAction のサポート」の節を参照してください。
データ読み込みメソッド	■ リソースからインポート ■ Active Sync ■ 調整

アカウント属性

SmartRoles アダプタでは、次のアイデンティティーシステムユーザー属性を使用できます。

ユーザー属性	データ型	説明
sr_allRoles	String	許可されて派生したロールのリスト (読み取り専用)
sr_departments	String	ユーザーがメンバーになっている部署のリスト (読み取り専用)
sr_derivedRoles	String	規則またはポリシーに基づいて割り当てられたロール (読み取り専用)
sr_financialGroups	String	ユーザーがメンバーになっている FinancialGroup のリスト (読み取り専用)
sr_financialTeams	String	ユーザーがメンバーになっている FinancialTeam のリスト (読み取り専用)
sr_grantedRoles	String	Person に直接許可されたロール (読み取り専用)
sr_grantedRolesSphere	complex	許可されたロールと各ロールの制御範囲を規定する complex 属性。制御範囲によって、アカウントのロールの対象となる組織を指定します。 GenericAttribute 内の GenericObject のスキーマは次のとおりです。 ■ **roles**[*] - アカウントに許可されたロールのリスト。 ■ **roles**[*index*]**.roleName** - 許可されたロールの名前。 ■ **roles**[*index*]**.organizations** - アカウントがロールを持つ組織のリスト。 注: このリストで組織を指定すると、子の組織もすべて指定されます。このリスト内で明示的に子の組織も指定すると、エラーが発生します。
sr_groups	String	ユーザーがメンバーになっているグループのリスト (読み取り専用)

ユーザー属性	データ型	説明
sr_organizations	complex	直接または従業員を経由して組織のメンバーシップを規定する complex 属性。組織のメンバーシップは、部署、グループ、チームを含むすべての組織タイプに適用されます。(読み取り/書き込み) GenericAttribute 内の GenericObject のスキーマは次のとおりです。 ■ **organizations**[*] - アカウントがメンバーになっている組織のリスト。 ■ **organizations**[*index*]**.orgName** - 組織名 (必須)。 ■ **organizations**[*index*]**.duties** - 組織内のアカウントの責任を記述した文字列 (省略可能)。 ■ **organizations**[*index*]**.memberRoles** - アカウントと組織との関係を説明するメンバーシップロールのリスト。有効な値は、HEAD、PRIMARY、SECONDARY、LIAISON、CONTRIBUTOR、TEAM ADMINISTRATOR、および TEAM MEMBER です (省略可能ですが指定してください)。 **organizations**[*index*]**.viaWorker** - 組織のメンバーシップを、そのアカウントに関連付けられた従業員 (*Person*) に割り当てられたアカウントに直接割り当てるかどうかを示すブール値。
sr_positions	complex	position を使用して役職名や組織のメンバーシップを規定する complex 属性。組織のメンバーシップは、部署、グループ、チームを含むすべての組織タイプに適用されます。(読み取り/書き込み) GenericAttribute 内の GenericObject のスキーマは次のとおりです。 ■ **positions**[*] - アカウントが割り当てられている役職名のリスト。 ■ **positions**[*index*]**.title** - 役職名 (必須)。 ■ **positions**[*index*]**.jobCode** - 役職名に関連付けられたジョブコード (省略可能)。 ■ **positions**[*index*]**.duties** - 役職の責任を記述した文字列 (省略可能)。 ■ **positions**[*index*]**.organizations**[*] - その役職名がメンバーになっている組織のリスト。各組織の属性は、sr_organizations 属性に記述されます。ただし、viaWorker 属性のみは例外で、このコンテキストでは無効です。

ユーザー属性	データ型	説明
sr_teams	String	ユーザーがメンバーになっているチームのリスト (読み取り専用)

属性の名前空間を使用して、関連するオブジェクトや配下のオブジェクトの属性を総称的に指定します。次のように「ドットの付いた」構文を使用します。

```
namespace.attribute_name
```

- Worker 属性には、WORKER を使用します (例: WORKER.WORKER_TYPE)
- Person オブジェクトに対する追加の属性を含む情報オブジェクトには、X500_PERSON および AUTHENTICATION_INFO 名前空間を使用します。
- X500_PERSON には、POSTAL_ADDRESS、SECRETARY などの属性が含まれます
- AUTHENTICATION_INFO には、LOGON_ATTEMPTS、PASSWORD_CHANGED (日付) などの属性が含まれます

リソースオブジェクトの管理

SmartRoles アダプタは、オブジェクトの表示のみをサポートしており、次のオブジェクトタイプをサポートします。

- 組織
- ロール

オブジェクトを表示するときには、option マップに次のオプションを指定できます。

オプション名	説明
searchContext (ResourceAdapter.RA_SEARCH_CONTEXT)	どのコンテキストで検索を実行するかを決定します。subTree 以外の searchScope を使用して組織を表示する場合のみ、このオプションを使用します。 このオプションを指定しない場合、最上位レベルの組織が表示されます。それ以外の場合は、検索を開始する組織の名前を使用してください。

オプション名	説明
searchScope (ResourceAdapter.RA_SEARCH_SCOPE)	現在のオブジェクトを、指定した searchContext のコンテキスト内のみから検索するのか、指定した searchContext 内のすべてのサブコンテキストから検索するのかを指定します。 有効な値は次のとおりです。 ■ object ■ oneLevel ■ subTree (デフォルト) このオプションは、organization 以外のすべてのオブジェクトタイプで無視されます。
searchFilter (ResourceAdapter.RA_SEARCH_FILTER)	返されるオブジェクトのリストをフィルタするために使用するキーと値のペアのセットを含むマップを指定します。これらのオブジェクトは、マップ内の対応する値と一致する値の属性を持つようになります。 このオプションを指定しない場合、指定したタイプのすべてのオブジェクトがアダプタによって返されます。
searchAttrsToGet (ResourceAdapter.RA_SEARCH_ATTRS_TO_GET)	オブジェクトごとに取得する objectType 固有の属性名のリストを指定します。

アイデンティティーテンプレート

```
$Logon ID$
```

サンプルフォーム

SmartRoles リソースアダプタには、次のサンプルフォームが用意されています。

組み込みのフォーム

なし

その他の利用可能なフォーム

SmartRolesUserForm.xml

トラブルシューティング

Identity Manager のデバッグページを使用して、`com.waveset.adapter.SmartRolesResourceAdapter` クラスでトレースオプションを設定します。

JVM のシステムプロパティー内で設定した `log4j.properties` ファイルを編集することで、SmartRoles API の DEBUG ロギングを有効にすることもできます。

▼ SmartRoles API の DEBUG ロギングを有効にする

1. `log4j.appender.debuglog.File` および `log4j.appender.logfile.File` properties が有効なファイルパスに設定されていることを確認します。
2. 次のように、`log4j.logger.bridgestream` プロパティーを **`DEBUG`** に設定します。

   ```
   log4j.logger.bridgestream=DEBUG
   ```

3. これらのログ設定を有効にするために、サーバーを再起動します。

◆ ◆ ◆ 第 9 章

9 ClearTrust

ClearTrust リソースアダプタは com.waveset.adapter.ClearTrustResourceAdapter クラスで定義されます。

アダプタの詳細

リソースを設定する際の注意事項

ClearTrust の eserver.conf ファイルを編集して SSL モードを設定します。cleartrust.eserver.api_port.use_ssl 設定を変更します。

詳細については、ClearTrust のマニュアルを参照してください。

Identity Manager のインストールに関する注意事項

ClearTrust リソースアダプタは、カスタムアダプタです。インストールプロセスを完了するには、次の手順を実行してください。

▼ ClearTrust リソースアダプタをインストールする

1. このリソースを Identity Manager のリソースリストに追加するには、「管理するリソースの設定」ページの「カスタムリソース」セクションに次の値を追加する必要があります。

   ```
   com.waveset.adapter.ClearTrustResourceAdapter
   ```

2. ClearTrust のインストール CD から ct_admin_api.jar ファイルを WEB-INF\lib ディレクトリにコピーします。

使用上の注意

ClearTrust API は、ユーザー用と管理者用に分かれています。ユーザーはサーバーへのアクセスを許可されていません。管理者は ClearTrust サーバーの管理特権を持つユーザーです。Identity Manager では、ClearTrust 管理ユーザーを作成または管理しません。

ClearTrust には、Application、Application Function、および URL の 3 種類のエンタイトルメントがあります。Identity Manager は Application Function のみをサポートし、ほかのエンタイトルメントは無視されます。エンタイトルメントをグループに割り当て、グループを (アダプタによってサポートされている) ユーザーに割り当てるようにしてください。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は、JNDI over SSL を使用して ClearTrust アダプタと通信します。

必要な管理特権

なし

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	なし
パススルー認証	あり
前アクションと後アクション	なし
データ読み込みメソッド	■ 調整 ■ リソースからインポート

アカウント属性

次の表に、ClearTrust のアカウント属性に関する情報を示します。

Identity Manager ユーザー属性	リソースユーザー属性	説明
accountId	accountName	必須。このユーザーの一意のアカウント ID。
isAdminLockout	isAdminLockout	ブール型。
externalDN	externalDN	このユーザーの外部ドメイン名。
email	emailAddress	ユーザーの電子メールアドレス。
endDate	endDate	このユーザーの終了日。
startDate	startDate	ユーザーの開始日。
firstname	firstName	ユーザーの名。
lastname	lastName	ユーザーの姓。
userGroup	userGroup	ユーザーに割り当てられたグループ。

リソースオブジェクトの管理

なし

アイデンティティーテンプレート

```
$accountId$
```

サンプルフォーム

```
ClearTrustUserForm.xml
```

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

```
com.waveset.adapter.ClearTrustResourceAdapter
```

◆ ◆ ◆ 第 10 章

10 データベーステーブル

データベーステーブルは、`com.waveset.adapter.DatabaseTableResourceAdapter` クラスで定義されます。

アダプタの詳細

このアダプタは、JDBC ドライバを備えたリレーショナルデータベースをすべてサポートします。

データベーステーブルリソースアダプタは、単一のカスタムデータベーステーブルに配置されたユーザーに接続して管理するための一連の手順を実行できるように設計されています。このアダプタは、アカウント変更をポーリングする Active Sync もサポートします。

注 – このリソースは、一般的に複数のテーブルで使用されている、DBMS システムアカウントを管理するように設計されていません。アダプタは結合の操作をサポートしません。DBMS システムアカウントを管理したい場合には、Oracle、SQL Server、DB2、Sybase、および MySQL リソースを引き続き使用してください。

リソースを設定する際の注意事項

なし

Identity Manager のインストールに関する注意事項

SQL Server へのすべての接続は、同じバージョンの Microsoft SQL Server JDBC ドライバを使用して実行してください。使用可能なバージョンは 2005 または 2000 です。こ

れには、リポジトリだけではなく、SQL Server のアカウントまたはテーブルを管理または要求するすべてのリソースアダプタ (Microsoft SQL アダプタ、Microsoft Identity Integration Server アダプタ、データベーステーブルアダプタ、スクリプト JDBC アダプタ、これらのアダプタをベースとするすべてのカスタムアダプタなど) が含まれます。異なるバージョンのドライバを使用しようとすると、競合エラーが発生します。

使用上の注意

ここでは、データベースリソースアダプタの使用に関連する次のような設定の注意点について説明します。

- 一般的な設定の注意点
- Active Sync 設定の注意点

一般的な設定

新しくデータベーステーブルリソースを設定するには、次の手順に従います。

▼ 新しいデータベーステーブルアダプタを設定する:一般的な手順

1. データベースアクセスパラメータを指定します。データベースタイプ、接続情報、管理対象のテーブルが配置されているデータベース名などがあります。
2. そのデータベースで使用可能なすべてのテーブルが、「データベーステーブル」ページに表示されます。このリソースのリソースアカウントを格納するテーブルを選択します。
3. **Identity Manager** で管理する列をテーブルから選択します。ウィザードページで表示されている列のうちの **1** つをキー列として指定し、ユーザーのアカウント名属性用に使用します。 さらに、別の **1** 列をパスワード列として指定し、アカウントパスワード用に使用します。その他の列は、管理対象の属性として選択できます。
4. リソーススキーママップページには、管理対象として選択されたこれらの属性が表示されます。このページにはキー属性やパスワード属性は表示されません。これらの属性は暗黙的に管理されます。
5. **Active Sync** 設定ページでは、**Active Sync** に関連するデータベーステーブル属性を任意で指定できます。アダプタを **Active Sync** として使用しない場合は、これらの値をスキップできます。詳細は、**157** ページの「**ActiveSync** 設定」を参照してください。
6. このリソースに使用するアイデンティティーテンプレートを指定します。これは、キー属性に使用する **Identity Manager** の属性名です。

7 このリソース用の **Identity Manager** リソースパラメータを指定します。ここには、リソース名、**Active Sync** のスケジューリングとロギング、リソースの承認者などの情報が含まれます。

ActiveSync 設定

注 – Active Sync アダプタは、アカウントの削除を検出しません。このため、アカウントの削除を検出するように調整してください。

データベーステーブルアダプタは、Active Sync ポーリングの実行中に、ユーザーフォーム (指定されている場合はワークフロー) に渡すためのリソースアカウントを、指定したデータベーステーブルから選択します。

「静的検索述語」パラメータによって、データベースから返されるアカウントを限定するために使用される任意の静的な述語を指定します。述語は SQL 式として評価されます。このパラメータは、ネイティブな SQL 構文で表してください。

次の例は、このパラメータの使用方法を示したものです。

```
syncState = ”P’
```

この例では、`syncState` という名前の列が存在することと、`P` が取り得る値であることが必要です。この値を「最後にフェッチされた述語」パラメータと結合させることで、完全な修飾子が形成されます。

「付加する結合子」パラメータの値は、AND または OR です。これは、最後にフェッチされた述語の前に付加される結合を指定します。

「最後にフェッチされた述語」パラメータでは、述語をもう 1 つ任意で指定しますが、この述語には Identity Manager で定義された 1 つ以上のユーザー属性を含めることができます。この機能によって、前回のポーリングで返された値を現在のポーリングで返された値と比較する述語を、ネイティブ SQL 構文で構築することができます。たとえば、`lastMod` 列にタイムスタンプが格納されていれば、その値を各ポーリングで比較することができます。次に、現在のポーリングの値が前のポーリングの値より大きい場合は、データベースエントリに関する情報を返します。次の式は、この機能を示しています。

```
lastMod > ’$(lastmod)’
```

括弧内には、スキーママップページで定義された Identity Manager ユーザー属性を指定する必要があります。`$(lastmod)` トークンは、前のポーリングで返された値に置き換えられます。たとえば、`2004-06-20 6:23:00` などの値になります。

注 – アダプタが最初にポーリングを行なったときは、前に取得された値が存在しないため、「**LAST FETCHED** フィルタ」は適用されません。このフィルタは、その後のすべてのポーリングで実行されます。

データベーステーブルアダプタは、「静的検索述語」、「付加する結合子」、および「最後にフェッチされた述語」リソースパラメータを連結して、次のような検索式を送信します。

```
syncState = 'P' AND lastMod > '2004-06-20 6:23:00'
```

ORDER BY パラメータを使用すると、指定した順序で行を処理するためのポーリングを強制する、ネイティブの SQL ORDER BY 節を指定できます。値の中には `ORDER BY` という単語を含めないでください。たとえば、`lastMod` の値を指定する場合、行は `lastMod` 列に基づいて、昇順に並べ替えられます。

オプションで、「変更時に実行するプロセス」パラメータを指定した場合、データベースから返されるそれぞれの修飾アカウントで起動する Identity Manager ワークフローが特定されます。このワークフローに渡される値のマップは、スキーママップの左側の属性によってキー設定されます。この値が指定されていない場合は、標準の Active Sync ユーザーフォーム処理によって更新が実行されます。

セキュリティーに関する注意事項

データベーステーブルに接続するプロキシユーザーには、次の特性が必要です。

- ユーザーは、アクセスされるデータベーステーブルまたはビューを所有している必要があります。修飾子を使用して所有者を指定せずに、接続ユーザー名によってテーブルまたはビューを参照できる必要があります。
- ユーザーには、アダプタがサポートするように設定されている任意のアクションを実行するための権限を与えてください。最低限、ユーザーにはデータベーステーブルまたはビュー (配下のテーブルを含む可能性がある) に対する SELECT 特権が必要です。たとえば、アダプタがユーザーを作成、更新、削除するように設定されている場合、ユーザーには SELECT、INSERT、UPDATE、および DELETE 特権が必要です。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	なし
アカウントの名前の変更	あり
パススルー認証	なし
前アクションと後アクション	なし
データ読み込みメソッド	■ リソースからインポート ■ Active Sync ■ 調整

アカウント属性

リソースユーザー属性は、リソースの作成または編集中にウィザードによって設定されます。次に、選択したユーザーのこれらの列の値が、Identity Manager ユーザー属性で見つかった対応する属性名でマップされます。

このアダプタでは、Oracle の BLOBなどのバイナリデータ型がサポートされます。対応する属性は、スキーママップでバイナリとしてマークされている必要があります。バイナリ属性の例には、グラフィックスファイル、オーディオファイル、証明書などがあります。

`waveset.properties` ファイル内の `sources.`*ResourceName*`.hosts` プロパティーを使用して、Active Sync アダプタの同期部分の実行にクラスタ内のどのホストを使用するかを制御できます。*ResourceName* は、リソースオブジェクトの名前に置き換える必要があります。

リソースオブジェクトの管理

なし

アイデンティティーテンプレート

```
$accountId$
```

サンプルフォーム

なし

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

```
com.waveset.adapter.DatabaseTableResourceAdapter
```

さらに、リソースインスタンスに対して次の Identity Manager Active Sync ロギングパラメータを設定できます。

- ログアーカイブの最大数
- アクティブログの最大有効期間
- ログファイルの最大サイズ
- ログファイルパス
- ログレベル

◆ ◆ ◆ 第 11 章

11 DB2

DB2 リソースアダプタは、com.waveset.adapter.DB2ResourceAdapter クラスで定義されます。

アダプタの詳細

このアダプタを使用して、DB2 にログインするためのユーザーアカウントをサポートします。カスタム DB2 テーブルがある場合、リソースアダプタウィザードを使用してカスタム DB2 テーブルリソースを作成する方法については、第 10 章「データベーステーブル」を参照してください。

リソースを設定する際の注意事項

DB2 では 2 種類の JDBC アクセスが提供され、それぞれで異なるドライバが必要となります。

- アプリケーションドライバ (COM.ibm.db2.jdbc.app.DB2Driver) には、ローカルクライアントソフトウェアとローカルデータベースインスタンスが必要です。

  大部分の本稼働環境において、DB2 は単独の (多くの場合、専用の) ホスト上で実行されるため、通常、ローカルデータベースインスタンスには、リモートデータベースインスタンスに対する別名が含まれています。この設定では、ローカルデータベースインスタンスは、DB2 固有のプロトコルを使用してリモートデータベースインスタンスと通信します。「DB2 リソースパラメータ」ページでは、このタイプのドライバがデフォルト値です。

- ネットワークドライバ (COM.ibm.db2.jdbc.net.DB2Driver) には、ローカルクライアントソフトウェアやローカルデータベースは必要ありません。

  このドライバでは、ターゲットサーバー上で DB2 Java Daemon (db2jd) が実行されている必要があります。大部分の本稼動環境において、ターゲットサーバーは単独のホストですが、ネットワークドライバはローカルデータベースインスタンスで同様に操作できます。

このデーモンはデフォルトでは起動されませんが、データベース管理者は、手動で起動、またはデータベースインスタンスの起動時に自動的に起動するように設定できます。

Identity Manager のインストールに関する注意事項

DB2 リソースアダプタは、カスタムアダプタです。インストールプロセスを完了するには、次の手順を実行してください。

▼ DB2 リソースアダプタをインストールする

1. このリソースを **Identity Manager** のリソースリストに追加するには、「管理するリソースの設定」ページの「カスタムリソース」セクションに次の値を追加する必要があります。

   ```
   com.waveset.adapter.DB2ResourceAdapter
   ```

2. `Db2\java\db2java.zip` ファイルを解凍します。

3. `db2java.jar` ファイルを *InstallDir*`\idm\WEB-INF\lib` ディレクトリにコピーします。

使用上の注意

DB2 では、外部認証と内部承認が実行されます。認証は、外部の認証者に accountID とパスワードを渡すことによって実行されます。デフォルトでは、オペレーティングシステムが認証を実行しますが、ほかのプログラムを認証目的に使用することもできます。

承認は、データベース、インデックス、パッケージ、スキーマ、サーバー、テーブル、またはテーブル空間 (あるいはその組み合わせ) のレベルで、さまざまなアクセス権に対して accountID を内部的にマッピングすることによって実行されます。承認を与えても自動的に accountID が認証されるわけではありません。したがって、実在しないアカウントを承認することができます。承認を取り消しても、公開されている権限は accountID から削除されません。

通常は、DB2 アプリケーションを、インストール先のマシンと同じリソースグループ内に配置するようにしてください。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は、SSL 経由の JDBC を使用して DB2 アダプタと通信します。

必要な管理特権

管理者には、DBADM 権限を許可する SYSADM 権限が必要です。その他の権限を許可するには、DBADM 権限か SYSADM 権限のいずれかが必要です。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	なし
アカウントの名前の変更	なし
パススルー認証	なし
前アクションと後アクション	なし
データ読み込みメソッド	リソースからインポート

アカウント属性

次の表に、DB2 ユーザーのアカウント属性を示します。属性の型はすべて String です。

リソースユーザー属性	説明
accountId	必須。
grants	必須。 有効な許可のコンマ区切りリスト。たとえば、次のようにします。 CONNECT ON MySchema.MyTable,DELETE ON MySchema.MyTable,INSERT ON MySchema.MyTable,SELECT ON MySchema.MyTable,UPDATE ON MySchema.MyTable

リソースオブジェクトの管理

なし

アイデンティティーテンプレート

```
$accountId$
```

サンプルフォーム

なし

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

```
com.waveset.adapter.DB2ResourceAdapter
```

◆ ◆ ◆ 第 12 章

12 Domino

Domino リソースアダプタは、com.waveset.adapter.DominoResourceAdapter クラスで定義されます。

アダプタの詳細

リソースを設定する際の注意事項

ここでは、Identity Manager で使用する Domino リソースの設定手順を説明します。次のような手順があります。

- Domino リソースを Identity Manager で使用するための一般的な設定手順
- Domino をサポートするようにゲートウェイをインストールする手順

一般的な設定手順

Domino アダプタ Domino リソースアダプタを設定するには、次の手順を使用します。

▼ Domino リソースアダプタを設定する

1. **Domino** で **Identity Manager** 管理者を作成します。ユーザーの管理に必要とされるすべての組織へのアクセス権を持つ認証者 **ID** を使用します。
2. サーバーのアドレス帳 **(names.nsf)** のアクセス制御リスト **(ACL)** に、ユーザーを追加します。
   a. ユーザーには、編集者のアクセス権を付与します。
   b. ユーザーに次のロールを割り当てます。

- GroupModifier
  - UserCreator
    - UserModifier

3 認証ログデータベース (**certlog.nsf**) の **ACL** に、投稿者のアクセス権を付与したユーザーを追加します。

4 管理要求 (**admin4.nsf**) の **ACL** に、投稿者のアクセス権を付与したユーザーを追加します。

5 新しく作成されたユーザーをサーバーのセキュリティーに追加します。

a. 「セキュリティー」パネルを開いて、サーバー設定を編集します。

b. **Domino** サーバーへのアクセスが制限されている場合、**Identity Manager** のプロキシアカウントにサーバーへのアクセス権があるかどうかを確認します。確認を行うには、アカウント名か、プロキシアカウントの属しているグループを、「アクセスサーバー」フィールドに指定します。

c. **Domino** エージェントを呼び出す前アクションと後アクションが存在する場合、呼び出されるエージェントの設定方法によって、「制限されていない **LotusScript/Java** エージェントを実行」または「制限されている **LotusScript/Java** エージェントを実行」のいずれかのフィールドに、ユーザーの追加が必要となる場合もあります。

Domino をサポートするようにゲートウェイをインストールする

ゲートウェイを Dimino に接続するには、あらかじめインストールされた Notes クライアントを、ゲートウェイマシン上に用意する必要があります。

Domino が正しく動作するように、Windows レジストリの `HKEY_LOCAL_MACHINE\SOFTWARE\Waveset\Lighthouse\Gateway` に次の文字列値を追加します。

- `notesInstallDir`。クライアントがインストールされる場所で、notes.dll ファイルの場所です。通常、この場所は `C:\Lotu\Notes\` などになります。
- `notesIniFile`。Lotus Notes の初期化ファイルへの、ファイル名を含むフルパス。このファイルは、デフォルトの場所 (`C:\Lotus\Notes\notes.ini` など) から、Identity Manager ゲートウェイが格納されているディレクトリにコピーするようにしてください。したがって、このレジストリキーの値は `C:\`*GatewayDir*`\notes.ini` のような値に設定してください。

注 – Notes クライアントがネットワーク対応のプロファイルとともに実行中であることを確認します。ini ファイルのコピー後にネットワーク接続を変更する場合、再度コピーを行うか、次のようなコマンド行によってクライアントを実行します。

```
C:\Lotus\Notes\notes.exe=PathToIniFile
```

Identity Manager のインストールに関する注意事項

このリソースでは、追加のインストール手順は必要ありません。

使用上の注意

ここでは、Domino リソースアダプタの使用に関する情報を示します。 次のトピックで構成されています。

Identity Manager を使用して Domino グループを作成するときに、グループの別名を使用できます。グループの別名は、「Group1;alias1;alias2」という構文で表します。リストにグループ名が表示されるときには、基本名のみが表示されます。

再認証処理

再認証処理は、recertify という名前の Boolean ユーザー属性を使用して実行されます。更新操作中に属性がチェックされ、有効な場合は、ユーザー ID が再認証されます。

再認証処理は adminp 処理によって行われます。つまり、adminp 要求を生成すると、それ以降のいずれかの時点で、その ID の再認証が行われます。再認証のタイミングは、Dimino サーバーの設定に基づいて決まります。

パスワードの変更

Lotus ユーザーには、2 つの異なるパスワードがあります。

- HttpPassword。Web ブラウザまたはその他の HTTP クライアントから Notes サーバーにアクセスするときに使用するパスワード。
- ID ファイル。ユーザーの Notes ID ファイルを暗号化するパスワード。このパスワードは、現在のパスワードを指定しない限り変更できません。結果として、Identity Manager 管理者はこのパスワードを変更できません。

  詳細は、172 ページの「ID ファイル」を参照してください。

アダプタは、これらのパスワードの一方または両方を管理するように構成できます。

HttpPasswords のみの管理

ID ファイルパスワードではなく HttpPasswords を管理するには、Domino Gateway アダプタを次のように構成します。

- 「変更時にユーザーがパスワードを入力」リソースパラメータを 0 に設定します。
- スキーママップで password リソースユーザー属性を HTTPPassword に変更します。
- HTTPPassword アイデンティティーシステムユーザー属性をスキーママップから削除します。

HttpPasswords と ID ファイルパスワードの管理

ユーザーインタフェースから ID ファイルパスワードを管理したり、管理者インタフェースやユーザーインタフェースから HttpPasswords を管理したりするには、Domino Gateway アダプタを次のように構成します。

- 「変更時にユーザーがパスワードを入力」リソースパラメータを 0 に設定します。
- ID ファイルパスワードは、ユーザーが現在のパスワードを指定しない限り変更できません。現在のパスワードは、スキーママップ内で WS_USER_PASSWORD という名前のアカウント属性として定義される必要があります。この属性が存在し、そのデータ型が暗号化されていることを確認します。
- スキーママップで HTTPPassword リソースユーザー属性を password に変更します。この変更により、password リソースユーザー属性が HTTPPassword とともに、password にマッピングされます。
- Password および LoginChange のビューを WS_USER_PASSWORD アカウント属性に追加します。[IDMIDELong テキストエンティティーを定義してください] またはデバッグページを使用して、リソース定義を次のように編集します。

```
<AccountAttributeType id='66' name='WS_USER_PASSWORD' syntax='encrypted'
  mapName='WS_USER_PASSWORD' mapType='string'>
   <Views>
      <String>Password</String>
```

```
      <String>LoginChange</String>
    </Views>
</AccountAttributeType>
```

- WS_USER_PASSWORD フィールドおよび idFile フィールドを次のフォームに追加します。
  - マイパスワード変更フォーム
  - パスワード変更フォーム
  - 有効期限切れログインフォーム

    これらのフィールドは、resourceAccounts ビューを指すように定義してください。

```
<Field name='resourceAccounts.currentResourceAccounts[ResourceName].
attributes.idFile'>
   <Display class='Text'>
      <Property name='title' value='idfile'/>
   </Display>
</Field>
<Field name='resourceAccounts.currentResourceAccounts[ResourceName].
attributes.WS_USER_PASSWORD'>
   <Display class='Text'>
      <Property name='title' value='WS_USER_PASSWORD'/>
   </Display>
</Field>
```

ID ファイルパスワードのみの管理

HttpPasswords は管理せずに、ユーザーインタフェースから ID ファイルパスワードを管理するには、Domino Gateway アダプタを次のように構成します。

- 「変更時にユーザーがパスワードを入力」リソースパラメータを 1 に設定します。
- ID ファイルパスワードは、ユーザーが現在のパスワードを指定しない限り変更できません。現在のパスワードは、スキーママップ内で WS_USER_PASSWORD という名前のアカウント属性として定義される必要があります。この属性が存在し、そのデータ型が暗号化されていることを確認します。
- idFile フィールドを次のフォームに追加します。
  - マイパスワード変更フォーム
  - パスワード変更フォーム
  - 有効期限切れログインフォーム

    このフィールドは、resourceAccounts ビューを指すように定義してください。

```
<Field name='resourceAccounts.currentResourceAccounts[ResourceName].
attributes.idFile'>
```

```
          <Display class='Text'>
             <Property name='title' value='idfile'/>
          </Display>
       </Field>
```

有効化と無効化

Domino 6.0 以降では、ユーザーを無効にする方法として、CheckPassword アカウント属性を 2 に設定する方法が使用されています。ただし、ユーザーを DNY GROUP に追加する 5.x の方法も使用できます。

Domino の初期のバージョンでは、ユーザーごとのネイティブな無効化フラグが実装されていないため、無効化された各ユーザーは DENY GROUP 内に配置されます。有効化すると、これらは定義済みグループのいずれかのメンバーとして削除されます。DENY GROUP にはメンバーの最大数のしきい値が設定されているので、グループをリソースに対するアカウント属性として指定してください。このためには、追加の DenyGroups アカウント属性をリソースに渡す必要があります。DenyGroups は、無効化、有効化、またはプロビジョニング解除の実行時に設定できますが、取得するには追加のコーディングが必要です。

プロビジョニング解除または無効化の実行中に、ユーザーを追加する先の DenyGroups のリストを送信します。有効化の実行中には、ユーザーが削除される DenyGroups のリストを送信します。

次のコードによって、使用可能な DenyGroups をリソースから取得できます。

```
<invoke name='listResourceObjects' class='com.waveset.ui.FormUtil'>
    <ref>:display.session</ref>
    <s>DenyLists</s>
    <s>YourResourceName</s>
    <null/>
    <s>false</s>
 </invoke>
```

次のコードによって、現在割り当てられている DenyGroups を、無効化、有効化、またはプロビジョニング解除フォームに取得できます。

```
<invoke name='getList'>
    <invoke name='getView'>
       <ref>display.session</ref>
       <concat>
          <s>UserViewer:</s>
          <ref>resourceAccounts.id</ref>
       </concat>
       <map>
          <s>TargetResources</s>
          <list>
```

```
            <s>YourResourceName</s>
          </list>
        </map>
    </invoke>
    <s>accounts[YourResourceName].DenyGroups</s>
 </invoke>
```

無効化、有効化、またはプロビジョニング解除フォームでは、DenyGroups 属性を次のようにアドレス指定します。

```
resourceAccounts.currentResourceAccounts [YourResourceName].attributes.DenyGroups
```

次の例では、複数選択ボックスの左側にある使用可能な DenyGroups を一覧表示する無効化フォームのフィールドを定義しています。

```
<Field name='resourceAccounts.currentResourceAccounts [
  YourResourceName].attributes.DenyGroups'>
    <Display class='MultiSelect'>
       <Property name='title' value='Deny Groups'/>
       <Property name='required'>
          <Boolean>false</Boolean>
       </Property>
       <Property name='allowedValues'>
          <invoke name='listResourceObjects' class='com.waveset.ui.FormUtil'>
             <ref>:display.session</ref>
             <s>DenyLists</s>
             <s>YourResourceName</s>
             <null/>
             <s>false</s>
          </invoke>
       </Property>
       <Property name='availableTitle' value='Available Deny Groups'/>
       <Property name='selectedTitle' value='Assigned Deny Groups'/>
    </Display>
 </Field>
```

次の例では、非表示フィールドの取得規則内の割り当てられた DenyGroups を一覧表示する有効化フォームのフィールドを定義しています。

```
<Field name='resourceAccounts.currentResourceAccounts
  [YourResourceName].attributes.DenyGroups'>
   <Derivation>
       <invoke name='getList'>
          <invoke name='getView'>
             <ref>display.session</ref>
             <concat>
                <s>UserViewer:</s>
                <ref>resourceAccounts.id</ref>
```

```
            </concat>
            <map>
               <s>TargetResources</s>
               <list>
                  <s>YourResourceName</s>
               </list>
            </map>
         </invoke>
         <s>accounts[YourResourceName].DenyGroups</s>
      </invoke>
   </Derivation>
</Field>
```

ID ファイル

ゲートウェイマシンでは、新しく登録されたユーザーに対して新規 ID が生成されます。これらは、ゲートウェイの処理やサービスにアクセス可能な UNC パス上に配置されます。したがって、`\\machine\ids\myidfile.id` と指定すると、ネットワーク共有に配置されます。

ユーザーの作成時に指定される共有部分にアクセスするためのサービスとしてゲートウェイを設定した場合、このゲートウェイに対してユーザーとして実行する必要がある可能性があります。共有部分にアクセスできるように SYSTEM を割り当てることもできますが、これはゲートウェイネットワーク環境がどのように見えるかに依存します。

「アドレス帳に ID を保存」リソース属性を TRUE または FALSE に設定することで、ID ファイルをアドレス帳に格納するかどうかを指定することもできます。

Rename/Move

move/rename アクションは、`adminp` プロセスでも実行されます。move は、`certifierOrgHierarchy` 属性を変更して元の `certifierId` ファイルとその `id` ファイルのパスワードを入力することによって、名前変更フォームから開始できます。move 要求によって要求データベース内に「名前移動要求」が作成されます。また、move 要求は、ユーザーの新しい組織を代表する新しい認証者が完了する必要があります。move は、ユーザーの姓または名を変更することで開始できます。

注 – rename と move を同時に実行することはできません。 `adminp` 処理で rename と move の同時実行ができないのは、要求が、どちらの場合にも変更される標準的な名前を参照するためです。

リソース名

ゲートウェイでは、すべての Domino リソースに一意の名前を付ける必要があります。複数の Identity Manager の配備があり、それらが同じゲートウェイを指している場合は、それらの配備に存在するすべての Domino リソースに一意のリソース名を付ける必要があります。

ローミングのサポート

リソースが Domino 7.0 以降のサーバーの場合、Identity Manager でローミングユーザーを作成できます。Identity Manager は、ユーザーのローミング状態を変更できません。そのため、RoamingUser アカウント属性を既存のユーザーに設定することはできません。

ゲートウェイタイムアウト

Domino アダプタでは、`RA_HANGTIMEOUT` リソース属性を使用してタイムアウト値を秒単位で指定できます。この属性は、ゲートウェイに対する要求がタイムアウトしてハングしているとみなされるまでの時間を制御します。

次のように、この属性を Resource オブジェクトに手動で追加する必要があります。

```
<ResourceAttribute name='Hang Timeout' displayName='com.waveset.adapter.RAMessages:
  RESATTR_HANGTIMEOUT' type='int' description='com.waveset.adapter.RAMessages:
  RESATTR_HANGTIMEOUT_HELP' value='NewValue'>
 </ResourceAttribute>
```

この属性のデフォルト値は 0 です。これは Identity Manager がハングした接続を確認しないことを表します。

追加情報

ここでは、このアダプタに関して、次のようないくつかの追加情報を提供します。

ListAllObjects

Domino で指定したすべてのオブジェクトを一覧表示できます。`listAllObjects` 呼び出しへの「タイプ」として表示名に渡します。

フォームの更新

これらの操作の一部には追加の属性が必要であるため、それらの属性を含むように、デフォルトのフォームを更新してください。

さまざまなビューに渡される属性は、リソース定義によってあらかじめ定義されています。

- 有効化フォーム、無効化フォーム: DenyGroups
- プロビジョニング解除フォーム: DenyGroups (オプション)
- 有効期限切れログインフォーム、パスワード変更フォーム、マイパスワード変更フォーム: HTTPPassword (秘密にする必要あり)、ID ファイル
- 名前変更フォーム: certifierIDFile、credentials (秘密にする必要あり)

searchFilter

次のサンプル UserForm では、getResourceObjects メソッドの searchFilter オプションを Domino 用に実装する方法を示します。このフォームでは、リソース MyResource 上で姓が Smith であるすべてのユーザーを検索しています。ユーザーはアカウント ID 順ではなく、com.waveset.object.GenericObject%4014a614a6 などの内部識別子の順に表示されます。

```
<DOCTYPE Configuration PUBLIC 'waveset.dtd' 'waveset.dtd'>
<Configuration name='Domino searchFilter Form' wstype=UserForm'"
 <Extension>
  <Form>
   <Display class='EditForm'/>
   <Field name='rcwfield'>
      <Display class='MultiSelect'>
         <Property name='title' value='My Lister'/>
         <Property name='availableTitle' value='Listing available items'/>
         <Property name='selectedTitle' value='Selected Item(s)'/>
         <Property name='allowedValues'>
         <block trace='true'>
               <invoke name='getResourceObjects' class='com.waveset.ui.FormUtil'>
                  <ref>:display.session</ref>
                  <s>People</s>
                  <s>MyResource</s>
                  <Map>
                     <MapEntry key='searchAttrsToGet'>
                        <List>
                           <String>LastName</String>
                           <String>ShortName</String>
                           <String>MailFile</String>
                        </List>
                     </MapEntry>
                     <MapEntry key='searchFilter' value='@IsAvailable(LastName) &amp;
```

```
@Contains(@LowerCase(LastName);"smith")'/>
                  </Map>
                </invoke>
         </block>
         </Property>
        </Display>
        <Disable>
         <i>0</i>
        </Disable>
     </Field>
  </Form>
 </Extension>
</Configuration>
```

その他のフォームに関する問題点

- 管理者が変更またはリセットできるのは、HTTPPassword のみです。HTTPPassword のみを変更したくない場合には、デフォルトテーブルによって Domino アダプタをフィルタします。
- マイパスワード変更フォーム、パスワード変更フォーム、および有効期限切れログインフォームは、「Forgot Old Password?」という名前の列を生成します。Domino リソースでは、この列を削除する必要があります。Identity Manager は管理者パスワードの更新をサポートしていません。

ビューに渡されるように設定する属性

- idFile。Password、LoginChange
- DenyGroups。Enable、Disable、Delete
- certifierIdFile、credentials。名前の変更
- HTTPPassword。Password、LoginChange

アクション

前アクションと後アクションで、次の変数を使用できます。

- WSUSER_accountId
- WSUSER_UNID

WSUSER_UNID 変数は、Lotus Notes の汎用 ID を表します。この変数は、アカウントが作成されるまで参照することができません。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は、Sun Identity Manager Gateway を使用して Domino と通信します。

必要な管理特権

なし

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	あり
パススルー認証	なし
前アクションと後アクション	あり
データ読み込みメソッド	■ リソースからインポート ■ 調整 ■ Active Sync

アカウント属性

次の表に、Domino アカウント属性の情報を示します。特に記載されていないかぎり、デフォルトのデータ型は文字列です。

リソースユーザー属性	説明
`alternateOrgUnit`	代替言語での、ユーザーの組織単位。
`AltFullName`	ユーザーの母国語での、ユーザーのフルネーム。
`AltFullNameLanguage`	代替のフルネームに使用される言語。
`Assistant`	補佐の名前。
`CalendarDomain`	カレンダのドメイン名。
`CellPhoneNumber`	ユーザーの携帯電話番号。

リソースユーザー属性	説明
certifierIDFile	ゲートウェイマシンを基準とした認証者 ID ファイルへのパス (リソースの値をオーバーライドする)
CertifierOrgHierarchy	/US1 など、認証者の組織階層のパス (リソースの値をオーバーライドする)。
CheckPassword	整数値。 0 = チェックしません 1 = チェックします 2 = ユーザーを無効にします
Children	従業員の子の名前 (複数可)。
City	ユーザーの自宅住所の市。
Comment	ユーザーに関するコメント。
CompanyName	ユーザーが勤務する会社。
Country	ユーザーの自宅住所の国。
credentials	認証者 ID ファイルのパスワード (リソースの値をオーバーライドする)
dbQuotaSizeLimit	ユーザーのメールデータベースの最大サイズを指定します。1000 未満の値を指定した場合、最大サイズの単位はメガバイト (M バイト) になります。1000 以上の値を指定した場合、最大サイズはバイト単位で表されます。1001 ～ 1023 の値は、1024 バイトに切り上げられます。 この属性を設定するには、プロキシ管理者がサーバードキュメント内で管理者として一覧表示される必要があります。
dbQuotaWarningThreshold	データベースのサイズについての警告が生成される基準となる、ユーザーのメールデータベースのサイズを指定します。1000 未満の値を指定した場合、しきい値の単位はメガバイト (M バイト) になります。1000 以上の値を指定した場合、しきい値はバイト単位で表されます。1001 ～ 1023 の値は、1024 バイトに切り上げられます。 この属性を設定するには、プロキシ管理者がサーバードキュメント内で管理者として一覧表示される必要があります。
defaultPasswordExp	新しい証明書が発行されるまでの日数 (作成操作、再認証操作)。

リソースユーザー属性	説明
deleteMailFileOption	リソースの属性を次のようにオーバーライドします。 ■ **0**: メールファイルを削除しません。 ■ **1**: 人物レコードに指定されたメールファイルのみを削除します。 ■ **2**: 人物レコードに指定されたメールファイルとすべての複製を削除します。 注意: mailfile を削除するように設定した場合、adminp 要求はキューに入れられます。削除する前に、ネイティブで承認する必要があります。
DenyGroups	リソースへのアクセスを拒否されるユーザーのリスト。
Department	ユーザーの部署名または部署番号。
DisplayName	ユーザーの表示名。
EmployeeID	ユーザーの一意の従業員 ID。
firstname	ユーザーの名。
HomeFAXPhoneNumber	ユーザーの自宅の FAX 番号と電話番号。
HTTPPassword	Web ブラウザまたはその他の HTTP クライアントから Notes サーバーにアクセスするときに使用するパスワード。
idFile	ゲートウェイマシンを基準とした ID ファイルへの完全修飾パス。
gateway machine	
InternetAddress	
JobTitle	ユーザーの役職。
lastModified	ユーザーを最後に変更した日時の文字列表現。
lastname	ユーザーの姓。
Location	オフィスの場所またはメールの到着場所
MailAddress	ユーザーの電子メールアドレス。
MailDomain	ユーザーのメールサーバーのドメイン名。
MailFile	メールファイルの名前 (MAIL\JSMITH など)
mailOwnerAccess	メールボックスの所有者のアクセス制御レベルを示します。指定できる値は、0 (マネージャー)、1 (設計者)、および 2 (エディター) です。 この属性は、デフォルトではスキーママップ内に存在しません。ユーザーの作成時のみに適用できる属性です。

リソースユーザー属性	説明
MailServer	ユーザーのメールサーバー名。
MailTemplate	メールテンプレートの名前。作成時のみ有効。
Manager	ユーザーのマネージャー。
MiddleInitial	最後にピリオドの付いたミドルネームのイニシャル。
NetUserName	ユーザーのネットワークアカウント名。
NotesGroups	
objectGUID	ユーザーの NotesID。
OfficeCity	ユーザーの勤務先住所の市。
OfficeCountry	ユーザーの勤務先住所の国。
OfficeFAXPhoneNumber	ユーザーの勤務先住所の FAX 番号。
OfficeNumber	ユーザーの勤務先住所の局番号。
OfficePhoneNumber	ユーザーの勤務先住所の電話番号。
OfficeState	ユーザーの勤務先住所の州または都道府県。
OfficeStreetAddress	ユーザーの勤務先住所の街路住所。
OfficeZIP	ユーザーの勤務先住所の郵便番号。
orgUnit	
password	ユーザーのパスワード。
PasswordChangeInterval	整数値。ユーザーが新しいパスワードを設定する必要が生じるまでの日数。
PasswordGracePeriod	パスワードの期限切れ後にユーザーがロックアウトされるまでの日数。
PhoneNumber	ユーザーの自宅電話番号。
PhoneNumber_6	
Policy	ユーザーの明示的ポリシー。「明示的ポリシー名」リソースパラメータの値によって、この属性が上書きされます。このパラメータは、Domino 7.0 以降のみに適用されます。
Profiles	ユーザーに割り当てられたプロファイル。この値によって、リソースパラメータとして指定されたプロファイルが上書きされます。この属性は、Domino 7.0 以上のみに適用されます。
Recertify	ブール型。ユーザーを再認証することを示すフラグ。
RoamCleanPer	RoamCleanSetting が 1 の場合は、クリーニング間隔の日数。

リソースユーザー属性	説明
RoamCleanSetting	Domino がユーザーのローミングファイルをクリーンアップするタイミングを指定します。有効な値は次のとおりです。 0 (削除しない) 1 (定期的) 2 (Domino サーバーのシャットダウン時) 3 (ユーザーに確認)
RoamingUser	1 に設定すると、ユーザーがローミングユーザーであることを指定します。
RoamRplSrvrs	ユーザーのローミングファイルがレプリケートされるサーバーの一覧。
RoamSrvr	ユーザーのローミングファイルが置かれるサーバーを指定します。
RoamSubdir	ユーザーのローミングファイルが含まれるディレクトリを指定します。
SametimeServer	ユーザーの Sametime サーバーの階層名。
ShortName	一般に外国のメールシステムによって使用される短いユーザー名。
Spouse	ユーザーの配偶者の名前。
State	ユーザーの自宅住所中の州または都道府県。
StreetAddress	ユーザーの自宅住所。
Suffix	ユーザーの世代を表す修飾子。
Title	ユーザーの役職。
WebSite	ユーザーの Web サイト。
WS_USER_PASSWORD	ユーザーのパスワード変更要求時に、ユーザーの現在のパスワードを送信するために使用する属性。
x400Address	
Zip	ユーザーの自宅住所の郵便番号。

リソースオブジェクトの管理

Identity Manager は、次のネイティブ Domino オブジェクトを管理します。

表 12–1 ネイティブ Domino オブジェクト

リソースオブジェクト	サポートされる機能	管理される属性
Group	作成、削除、一覧表示、名前の変更、名前を付けて保存、更新	ConflictAction、Group_Main、AvailableFo

アイデンティティーテンプレート

Domino では、各ユーザーのアイデンティティーは `userid` ファイルに格納されます。ただし、それと同じユーザー名が `FullName` 属性内のユーザーレコードに格納されます。この属性は複数値を取り、リスト内の最初の属性は一意です。リスト内の最初の名前は、標準的な形式で格納され、次のようになります。

```
CN=Joe T Smith/O=MyCompany
```

この名前を使用して、名前とアドレス帳のレコードにアクセスできます。Identity Manager は、この文字列を適切なフォームの `resourceInfo` に、次のように格納します。

```
Joe T Smith/MyCompany
```

Domino には、API レベルで名前を変換する組み込み機能があります。Identity Manager は、`NOTEID` も `GUID` 属性として格納し、可能な場合は、このグローバル識別子を使用して Domino のユーザーを検索します。

デフォルトのアイデンティティーテンプレートは次のとおりです。

```
$firstname$ $MiddleInitial$ $lastname$$CertifierOrgHierarchy$
```

環境によっては、ミドルネームのイニシャルが含まれない場合もあります。

サンプルフォーム

`DominoActiveSyncForm.xml`

`Dominogroupcreate.xml`

`Dominogroupupdate.xml`

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

```
com.waveset.adapter.DominoResourceAdapter
```

ゲートウェイへの接続の問題を診断するために、次のメソッドでトレースを有効にすることもできます。

- `com.waveset.adapter.AgentResourceAdapter#sendRequest`
- `com.waveset.adapter.AgentResourceAdapter#getResponse`

◆ ◆ ◆ 第 13 章

13 外部リソース

外部リソースアダプタは、com.waveset.adapter.ExternalResourceAdapter クラスで定義されます。

アダプタの詳細

リソースを設定する際の注意事項

このアダプタを設定するには、「設定」、「外部リソース」の順に選択します。リソース情報の格納と、リソースのプロビジョニングツールへの通知方法について、タスクを設定する必要があります。

- データストア - すべての外部リソースに対して、1 つの外部データストアが必要です。データストアには、ディレクトリまたはデータベースのいずれかを使用できます。データストアがデータベースの場合の設定については、ScriptedJDBC リソースアダプタの説明を参照してください。データベースがディレクトリの場合は、LDAP アダプタの説明を参照してください。
- プロビジョニングツールの通知 - 通知設定は、「設定」、「外部リソース」の順に選択して設定するか、リソースごとに設定できます。

Identity Manager のインストールに関する注意事項

データストアがデータベースの場合は、ScriptedJDBC アダプタのインストール手順に従います。データストアがディレクトリの場合は、LDAP アダプタのインストール手順に従います。

使用上の注意

外部リソースアダプタは、外部リソース設定からデータストア情報を取得します。設定中にデータストア情報が変更されると、外部リソースの設定も同様に更新されます。

外部リソースのデータストア設定を変更するには、外部リソース設定を変更する必要があります。システム全体の設定を変更すると、すべての外部リソースが新しいデータストア設定で更新されます。

ActiveSync 設定

なし

セキュリティーに関する注意事項

データストアがデータベースの場合は、ScriptedJDBC アダプタを参照してください。データストアがディレクトリの場合は、LDAP アダプタを参照してください。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	あり
パススルー認証	なし
前アクションと後アクション	なし
データ読み込みメソッド	なし

アカウント属性

なし。

リソースオブジェクトの管理

データストアがデータベースの場合は、ScriptedJDBC アダプタを参照してください。データストアがディレクトリの場合は、LDAP アダプタを参照してください。

アイデンティティーテンプレート

データストアがデータベースの場合は、ScriptedJDBC アダプタを参照してください。データストアがディレクトリの場合は、LDAP アダプタを参照してください。

サンプルフォーム

なし。

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

```
com.waveset.adapter.ExternalResourcesAdapter
```

その他のトラブルシューティングに関する説明については、データストアがデータベースの場合は ScriptedJDBC の説明を、データストアがディレクトリの場合は LDAP アダプタの説明を、それぞれ参照してください。

◆ ◆ ◆ 第 14 章

14 フラットファイル Active Sync

フラットファイル Active Sync アダプタ
は、`com.waveset.adapter.FlatFileActiveSyncAdapter` クラスで定義されます。

アダプタの詳細

フラットファイル Active Sync アダプタでは、次のタイプのファイルを読み取ることができます。

- 区切りファイル。コンマ区切り (CSV) ファイル、パイプ (|) 区切りファイルなど。
- LDAP データ交換形式 (LDIF)。Netscape の `ldapjdk.jar` がクラスパスに指定されている必要があります。

パーサークラスが `com.waveset.util.FlatFileIterator` インタフェースを実装する場合は、カスタムパーサーも使用できます。

このアダプタはソース専用アダプタです。ファイルへの書き戻しは行いません。

次に、フラットファイル Active Sync アダプタを使用するのが適していると思われる事例をいくつか挙げます。

- 直接的な API やその他のプログラムによるインタフェースが存在しない。
- そのリソース用のリソースアダプタが存在しない。
- 1 つ以上のリソースに格納されているデータを、Identity Manager に読み取る前に事前処理する必要がある。
- リソースの所有者が、リソースへの直接的な接続を許可していない。
- リソースに対して直接接続する方法が提供されていない。

リソースを設定する際の注意事項

アダプタによって読み取られるフラットファイルは、プラットフォームに応じて、ローカルハードドライブ、ネットワーク共有、またはマウント済みドライブのいずれかにあるアプリケーションサーバー (クラスタが実行されている場合は、すべてのアプリケーションサーバー) で利用できるようにしてください。同期ロギングが設定されている場合は、ログディレクトリも、アプリケーションサーバーから見えるようにし、アプリケーションサーバーの処理を実行するアカウントによって書き込めるようにしてください。

もっとも信頼できる設定 (推奨される方法) は、アプリケーションサーバーに対してローカルなドライブにフラットファイルを格納することです。ログファイルも、ローカルディレクトリに書き込まれるようにしてください。異なるサーバー上で複数の Identity Manager インスタンスを使用している場合は、1 つのサーバーをフラットファイル Active Sync アダプタの実行用に選択し、管理インタフェースの「同期ポリシーの編集」ページでそのサーバーを指定します。これにより、アダプタ上のポーリング操作が sources.hosts プロパティーで指定したサーバー (複数可) 上で常に実行されることが保証されます。

Identity Manager のインストールに関する注意事項

このリソースでは、追加のインストール手順は必要ありません。

使用上の注意

ここでは、フラットファイル Active Sync リソースアダプタの使用に関連する設定の注意点について説明します。 次のトピックで構成されています。

- 188 ページの「全般的な注意事項」
- 189 ページの「ActiveSync 設定」
- 190 ページの「サポートされているファイルの例」

全般的な注意事項

LDIF ファイルをポーリングしている場合は、LDAP API によって属性名が小文字に変換されます。したがって、大文字を含む属性名 (`accountId` など) がある場合、LDAP API によって `accountid` のように変換されます。Active Sync の起動時に、次のエラーのログがとられます。

```
com.waveset.util.WavesetException: No name attribute found for user based
on Resolve Identity Rule or schema map.
```

この状況を解決するには、スキーママップで、リソースユーザー属性を accountid に設定します。

ファイル内の列を使用して accountId を直接設定していないファイルをインポートしたときに、同じエラーが再度発生する可能性があります。このエラーメッセージを回避するには、Active Sync フォームに global.accountId のフィールドを追加し、そのフィールドに accountId を構築するロジックを追加して、ユーザーフォームを変更します。次に示すフィールド例では、accountId を firstname.lastname に設定しています。 ただし、create 操作に対してのみです。

```
<Field name='waveset.accountId'>
   <Expansion>
      <concat>
         <ref>activeSync.firstname</ref>
         <s>.</s>
         <ref>activeSync.lastname</ref>
      </concat>
   </Expansion>
   <Disable>
      <neq>
         <ref>feedOp</ref>
         <s>create</s>
      </neq>
   </Disable>
</Field>
```

ActiveSync 設定

フラットファイル Active Sync アダプタは、フラットファイルのタイムスタンプを追跡できます。また、アダプタは最後に処理されたファイルをアーカイブして、これを最新のバージョンと比較します。Identity Manager は、2 つのファイルが異なっているアカウントで処理を実行します。

これらの機能が有効になっている場合、Identity Manager がソースのフラットファイルを最初にポーリングするときに、そのファイルがコピーされ、同じディレクトリ内に配置されます。コピーされた (保存された) ファイルには、FFAS_ *timestamp*.FFAS という名前が付けられます。timestamp は、元のファイルが最後に変更された時刻を示します。タイムスタンプの形式は、ソースファイルのあるオペレーティングシステムによって決まります。

その後のポーリングごとに、Identity Manager は元のファイルのタイムスタンプと最新のタイムスタンプを比較します。新しいタイムスタンプの値が直前の値と同じ場合、ファイルは変更されていないので、次のポーリングが行われるまでそれ以上の処理は実行されません。タイムスタンプの値が異なる場合、Identity Manager は FFAS ファイルの存在をチェックします。このファイルが存在していなければ、Identity Manager は更新されたソースファイルを新しいファイルとして処理します。

タイムスタンプが異なっており、保存されている FFAS ファイルが存在する場合、Identity Manager はソースファイルと保存されているファイルを比較します。この比較によって、変更されていないユーザーを処理の対象から除外します。変更されたユーザーは、アダプタを通して通常の方法で送信され、設定された処理、相関規則および削除規則によって、このユーザーに対する処理が決まります。

これらの規則を利用しやすくするために、差分メカニズムで検出された状況を示すための属性がアダプタによって追加されます。新しく更新されたソースファイルのみに存在しているユーザーに対して、ユーザーレコードに値が `create` の `diffAction` という属性が追加されます。ソースファイル内のいずれかのエントリが更新された場合、そのエントリに対して属性 `diffAction` が追加され、値には `update` が設定されます。いずれかのユーザーが削除された場合、そのユーザーレコードに対して、`diffAction` 属性の値は `delete` になります。

2 つのファイルの比較が完了し、すべてのアカウント処理が行われたあと、Identity Manager によって元の FFAS ファイルが削除され、現在のソースファイルが新しい FFAS ファイルにコピーされます。このファイルのタイムスタンプは、直前の FFAS ファイルとは異なるものになります。

サポートされているファイルの例

次に、このアダプタによってサポートされているファイルの例を示します。

区切り文字およびテキスト修飾子は、任意の 1 文字に設定できます。どちらかで Unicode 文字を使用する場合は、/u#### という形式で入力できます。区切り文字およびテキスト修飾子は、LDAP データ交換形式には適用されません。

コンマ区切り

次の例では、引用符 (" ") がテキスト修飾子として使用されます。文字列 `1234 Pecan Ave., Ste 30` にはコンマが含まれています。そのためシステムがこの文字列内の `Ste 30` を一つの属性として解釈しないように、引用符で修飾させる必要があります。

```
accountId,firstname,lastname,email,street address
kb323441,Kevin,Brown,Kevin.Brown@example.com,”1234 Pecan Ave., Ste 30”
pc432343,Penelope,Carter,Penelope.Carter@example.com,4234 Main St.
```

パイプ区切り

```
accountId|firstname|lastname|email|street address
kb323441|Kevin|Brown|Kevin.Brown@example.com|1234 Pecan Ave., Ste 30
pc432343|Penelope|Carter|Penelope.Carter@example.com|4234 Main St.
```

LDAP データ交換形式

```
dn: cn=Kevin Brown,ou=People,dc=example,dc=com
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalperson
objectClass: inetorgperson
employeeNumber: kb323441
cn: Kevin Brown
sn: Brown
departmentNumber: 7013
description: Production
displayName: Kevin
givenName: Kevin
mail: Kevin.Brown@example.com
o: Acme
ou: Production
postalAddress: 1234 Pecan Ave., Ste 30
postalCode: 43231
st: CA
street: 1234 Pecan Ave, Ste 30
title: Production Assistant
jpegphoto: file:///c:/photos/Kevin.Brown.jpg
```

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

188 ページの「リソースを設定する際の注意事項」を参照してください。

必要な管理特権

管理ユーザーに、フラットファイルを含むディレクトリに対する読み取りと書き込みのアクセス権を与えてください。「違いのみを処理」の Active Sync パラメータが有効になっている場合は、管理ユーザーに削除のアクセス権も与える必要があります。

さらに、管理者アカウントには、Active Sync の「ログファイルパス」フィールドに指定したディレクトリに対する読み取り、書き込み、および削除の権限が必要です。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	なし
アカウントの名前の変更	なし
パススルー認証	なし
前アクションと後アクション	なし
データ読み込みメソッド	Active Sync 調整はサポートされません。

アカウント属性

リソースアダプタのスキーマ定義は、フラットファイルの内容に依存します。属性が何も指定されていない場合、アダプタはフラットファイルから取得した属性名を使用します。区切りファイルの場合、これらの値は列見出しに対応しています。1 つ以上の Identity Manager の属性名をフラットファイルで定義している列の名前にマップするには、スキーママップのページで、各々のマッピングを設定します。

フラットファイルの形式が LDIF である場合は、バイナリ属性 (グラフィックスファイル、オーディオファイル、証明書など) を指定できます。バイナリ属性は、区切りファイルに対してはサポートされていません。

リソースオブジェクトの管理

適用不可

アイデンティティーテンプレート

このアダプタでは、アイデンティティーテンプレートは無視されます。

サンプルフォーム

なし

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

```
com.waveset.adapter.FlatFileActiveSyncAdapter
```

◆ ◆ ◆ 第 15 章

15 HP OpenVMS

HP OpenVMS リソースアダプタは、com.waveset.adapter.VMSResourceAdapter クラスで定義されます。

アダプタの詳細

リソースを設定する際の注意事項

なし。

Identity Manager のインストールに関する注意事項

このリソースを Identity Manager のリソースリストに追加するには、「管理するリソースの設定」ページの「カスタムリソース」セクションに次の値を追加する必要があります。

```
com.waveset.adapter.VMSResourceAdapter
```

使用上の注意

HP OpenVMS ユーザー属性の情報については、使用している VMS の製品マニュアルを参照してください。

セキュリティーに関する注意事項

必要な管理特権

HP Open VMS リソースに接続するユーザーアカウントは、SYSPRV、SNETMBX、およびTMPMBX の権限を持っている必要があります。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	なし
パススルー認証	あり
前アクションと後アクション	あり
データ読み込みメソッド	■ リソースから直接インポート ■ 調整

アカウント属性

次の表に、HP OpenVMS リソースアダプタに付属して提供されるアカウント属性を示します。

リソースユーザー属性	種類	説明
`device`	String	新しいユーザーのデフォルトのデバイスを特定します
`directory`	String	新しいユーザーのデフォルトのディレクトリを特定します
`create default directory`	Boolean	デフォルトのディレクトリが作成されるかどうかを示します
`copy login script`	Boolean	既存のログインスクリプトがコピーされるかどうかを示します
`login script source`	String	新しいユーザーにコピーされる既存のログインスクリプトを示します
`owner`	String	VMS のマニュアルを参照してください。

リソースユーザー属性	種類	説明
account	String	VMS のマニュアルを参照してください。
UIC	String	VMS のマニュアルを参照してください。
CLI	String	VMS のマニュアルを参照してください。
clitables	String	VMS のマニュアルを参照してください。
lgicmd	String	VMS のマニュアルを参照してください。
expiration	String	VMS のマニュアルを参照してください。
pwdminimum	String	VMS のマニュアルを参照してください。
loginfails	String	VMS のマニュアルを参照してください。
pwdlifetime	String	VMS のマニュアルを参照してください。
pwdchange	String	VMS のマニュアルを参照してください。
lastlogin	String	VMS のマニュアルを参照してください。
maxjobs	String	VMS のマニュアルを参照してください。
fillm	String	VMS のマニュアルを参照してください。
bytlm	String	VMS のマニュアルを参照してください。
maxacctjobs	String	VMS のマニュアルを参照してください。
shrfillm	String	VMS のマニュアルを参照してください。
pbytlm	String	VMS のマニュアルを参照してください。
maxdetach	String	VMS のマニュアルを参照してください。
biolm	String	VMS のマニュアルを参照してください。
jtquota	String	VMS のマニュアルを参照してください。
prclm	String	VMS のマニュアルを参照してください。
diolm	String	VMS のマニュアルを参照してください。
prio	String	VMS のマニュアルを参照してください。
astlm	String	VMS のマニュアルを参照してください。
wsquo	String	VMS のマニュアルを参照してください。
queprio	String	VMS のマニュアルを参照してください。
tqelm	String	VMS のマニュアルを参照してください。
wsextent	String	VMS のマニュアルを参照してください。

リソースユーザー属性	種類	説明
cpu	String	VMS のマニュアルを参照してください。
enqlm	String	VMS のマニュアルを参照してください。
pgflquo	String	VMS のマニュアルを参照してください。
GRANT.IDS	CSV String	使用を許可する ID のリストを提供します。 grant/identifier grantId accountId
REVOKE.IDS	CSV String	使用許可を取り消す ID のリストを提供します。 revoke/identifier grantId accountId
FlagList	ArrayList	リスト内で有効なエントリは次のとおりです。 DisCtlY、DefCLI、LockPwd、Restricted、DisUser、DisWelcome、DisNewMail
PrivilegesList	ArrayList	リスト内で有効なエントリは次のとおりです。 ACNT、ALLSPOOL、ALTPRI、AUDIT、BUGCHK、BYPASS、CMEXEC、CM
DefPrivilegesList	ArrayList	リスト内で有効なエントリは次のとおりです。 ACNT、ALLSPOOL、LTPRI、AUDIT、BUGCHK、BYPASS、CMEXEC、CMK
PrimaryDaysList	ArrayList	リスト内で有効なエントリは次のとおりです。 Mon、Tue、Wed、Thu、Fri、Sat、Sun

サンプルフォーム

VMSUserForm.xml

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

- com.waveset.adapter.VMSResourceAdapter
- com.waveset.adapter.ScriptedConnection

◆ ◆ ◆ 第 16 章

16 HP-UX

HP-UX リソースアダプタは、com.waveset.adapter.HPUXResourceAdapter クラスで定義されます。

アダプタの詳細

リソースを設定する際の注意事項

リソースと Identity Manager 間の通信に SSH (Secure Shell) を使用する場合は、アダプタを設定する前に、リソースで SSH を設定します。

Identity Manager のインストールに関する注意事項

このリソースでは、追加のインストール手順は必要ありません。

使用上の注意

HP-UX リソースアダプタは、主に次の HP-UX コマンドに対するサポートを提供します。

- useradd、usermod、userdel
- groupadd、groupmod、groupdel
- passwd

サポートされる属性およびファイルの詳細については、これらのコマンドに関する HP-UX マニュアルページを参照してください。

HP-UX リソースでユーザーアカウントの名前の変更を実行すると、グループメンバーシップは新しいユーザー名に移動されます。次の条件に該当する場合は、ユーザーのホームディレクトリの名前も変更されます。

- 元のホームディレクトリの名前がユーザー名と一致していた。
- 新しいユーザー名と一致するディレクトリがまだ存在していない。

UNIX リソース (AIX、HP-UX、Solaris、または Linux) に接続するときは、root シェルとして Bourne 互換シェル (sh、ksh) を使用してください。

HP-UX アカウントを管理する管理アカウントには、英語 (en) または C ロケールを使用してください。これは、ユーザーの `.profile` ファイルで設定できます。

NIS が実装されている環境では、次の機能を実装することにより、一括プロビジョニング中のパフォーマンスを向上させることができます。

- `user_make_nis` という名前のアカウント属性をスキーママップに追加し、この属性を調整やその他の一括プロビジョニングワークフローで使用します。この属性を追加した場合、リソース上の各ユーザーが更新された後は、システムで NIS データベースへの接続手順がバイパスされます。
- すべてのプロビジョニングが完了した後で NIS データベースに変更を書き込むには、ワークフローで `NIS_password_make` という名前の ResourceAction を作成します。
- このアダプタでは、HP-UX Trusted Mode はサポートされません。

ユーザーパスワードに制御文字 (0x00、0x7f など) を使用しないでください。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は、次の接続を使用して HP-UX アダプタと通信します。

- Telnet
- SSH (SSH はリソース上に個別にインストールする)
- SSHPubKey

SSHPubKey 接続の場合、「リソースパラメータ」ページで非公開鍵を指定する必要があります。この鍵には `--- BEGIN PRIVATE KEY ---` および `--- END PRIVATE KEY --` のような注釈行を含める必要があります。公開鍵は、サーバー上の `/.ssh/authorized_keys` ファイルに配置する必要があります。

必要な管理特権

このアダプタでは、一般ユーザーとしてログインしてから su コマンドを実行し、root ユーザー (または root ユーザーと同等のアカウント) に切り替えて管理アクティビティーを実行できます。 また、root ユーザーとして直接ログインすることもできます。また、root ユーザーとして直接ログインすることもできます。

アダプタは、sudo 機能 (バージョン 1.6.6 以降) もサポートします。この機能は、HP-UX 11i に HP-UX Internet Express CD からインストールできます。sudo 機能を使用すると、システム管理者は特定のユーザー (またはユーザーのグループ) に、root ユーザーまたは別のユーザーとして一部 (またはすべて) のコマンドを実行する能力を与えることができます。

さらに、sudo がリソースで有効になっている場合は、その設定が、root ユーザーのリソース定義ページでの設定よりも優先されます。

sudo を使用する場合は、Identity Manager 管理者に対して有効にされたコマンドの `tty_tickets` パラメータを true に設定する必要があります。詳細については、sudoers ファイルのマニュアルページを参照してください。

管理者は、sudo で次のコマンドを実行する特権が付与されている必要があります。

ユーザーとグループのコマンド	NIS コマンド	その他のコマンド	
■ `groupadd`	■ `make`	■ `awk`	■ `ls`
■ `groupdel`	■ `ypcat`	■ `cat`	■ `mv`
■ `groupmod`	■ `ypmatch`	■ `chmod`	■ `rm`
■ `last`	■ `yppasswd`	■ `chown`	■ `sed`
■ `listusers`		■ `cp`	■ `sleep`
■ `logins`		■ `cut`	■ `sort`
■ `passwd`		■ `diff`	■ `tail`
■ `useradd`		■ `echo`	■ `touch`
■ `userdel`		■ `grep`	■ `which`
■ `usermod`			

テスト接続を使用して次のテストができます。

- 各コマンドが管理ユーザーのパスに存在するかどうか
- 管理ユーザーが /tmp に書き込めるかどうか
- 管理ユーザーに、特定のコマンドを実行する権限があるかどうか

注 – テスト接続では、通常のプロビジョニングの実行とは異なるコマンドオプションを使用できます。

このアダプタには、基本的な sudo 初期化機能とリセット機能が用意されています。ただし、リソースアクションが定義されていて、そこに sudo 認証を必要とするコマンドが含まれている場合は、UNIX コマンドとともに sudo コマンドを指定してください。たとえば、単に `useradd` と指定する代わりに `sudo useradd` を指定してください。sudo を必要とするコマンドは、ネイティブリソースに登録されている必要があります。それらのコマンドを登録するには、`visudo` を使用します。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	HP-UX は、Identity Manager の enable アクションと disable アクションをネイティブではサポートしません。Identity Manager は、ユーザーのパスワードを変更することによって、アカウントの有効化と無効化をシミュレートします。enable アクションでは変更されたパスワードが公開されますが、disable アクションでは公開されません。 その結果、enable アクションと disable アクションは update アクションとして処理されます。update で動作するように設定されている前アクションと後アクションすべてが実行されます。
アカウントの名前の変更	あり
パススルー認証	あり
前アクションと後アクション	あり
データ読み込みメソッド	■ リソースから直接インポート ■ リソースの調整

このリソース上のすべてのユーザーに対して、次のタスクを制御するリソース属性を定義できます。

- ユーザーの作成時にホームディレクトリを作成する
- ユーザーの作成時にユーザーのホームディレクトリにファイルをコピーする
- ユーザーの削除時にホームディレクトリを削除する

アカウント属性

次の表に、HP-UX ユーザーのアカウント属性を示します。特に記載されていないかぎり、これらの属性は省略可能です。属性の型はすべて String です。

リソースユーザー属性	**useradd** での指定方法	説明
accountId	login	必須。ユーザーのログイン名。
comment	-c comment	ユーザーのフルネーム。
dir	-d directory	ユーザーのホームディレクトリ。このアカウント属性で指定された値はすべて、「ホームベースディレクトリ」リソース属性で指定された値よりも優先されます。
expire	-e expiration date	アカウントにアクセスできる最終日付。
group	-g group	ユーザーの一次グループ。
inactive	-f days	アカウントが非アクティブになってからロックされるまでの日数。
secondary_group	-G group	ユーザーの二次グループのコンマ区切りリスト。 ロールを有効にしてこの属性をプロビジョニングするには、'csv=true' を Role オブジェクト XML の RoleAttribute 要素に追加する必要があります。
shell	-s /Path	ユーザーのログインシェル。 NIS マスターにプロビジョニングしている場合は、ユーザーシェルの値は NIS マスターに対してのみチェックされます。ユーザーがログオンする可能性のあるその他のマシンに対してチェックは実行されません。
time_last_login	最終コマンドから取得されます。	最終ログインの日時。この値は読み取り専用です。
uid	-u User ID	数字形式でのユーザー ID。

リソースオブジェクトの管理

Identity Manager は、次のネイティブ HP-UX オブジェクトを管理します。

リソースオブジェクト	サポートされる機能	管理される属性
Group	作成、更新、削除、名前の変更、名前を付けて保存	groupName、gid、users

アイデンティティーテンプレート

```
$accountId$
```

サンプルフォーム

組み込みのフォーム

- HP-UX Group Create Form
- HP-UX Group Update Form

その他の利用可能なフォーム

`HP-UXUserForm.xml`

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

- `com.waveset.adapter.HPUXResourceAdapter`
- `com.waveset.adapter.SVIDResourceAdapter`
- `com.waveset.adapter.ScriptedConnection`

◆ ◆ ◆ 第 17 章

17 INISafe Nexess

INISafe Nexess リソースアダプタ
は、com.waveset.adapter.INISafeNexessResourceAdapter クラスで定義されます。

アダプタの詳細

リソースを設定する際の注意事項

なし

Identity Manager のインストールに関する注意事項

INISafe Nexess リソースアダプタは、カスタムアダプタです。インストールプロセスを完了するには、次の手順を実行してください。

▼ INISafe Nexess リソースアダプタをインストールする

1 「管理するリソースの設定」ページの「カスタムリソース」セクションに次の値を追加します。

```
com.waveset.adapter.INISafeNexessResourceAdapter
```

2 次の JAR ファイルを *$WSHOME$* /WEB-INF/lib ディレクトリにコピーします。

JAR ファイルの名前	取得方法
concurrent.jar	http://www.jboss.org/products/jbosscache
crimson.jar	http://ant.apache.org/bindownload.cgi
external-debug.jar	INITECH のサポートに問い合わせてください。
INICrypto4Java.jar	INISafe Nexess と一緒にインストールされなければ INITECH のサポートに問い合わせてください。
jdom.jar	http://jdom.org/downloads/index.html
log4j-1.2.6.jar	http://logging.apache.org/log4j/docs/download.html

使用上の注意

このアダプタは、ユーザーの作成、更新、削除のみをサポートしています。調整やリソースからのデータのロードは実行できません。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

INISafe Nexess との通信は、com.initech.eam.api クラスを使用して実行されます。

必要な管理特権

管理者に Nexess Daemon とログインサーバーへのアクセス権を与えてください。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	なし
パススルー認証	なし

機能	サポート状況
前アクションと後アクション	なし
データ読み込みメソッド	該当なし。 このアダプタでは、ユーザーを個別に作成、削除、更新することのみができます。

アカウント属性

次の表に、INISafe Nexess アカウント属性を示します。

リソースユーザー属性	データ型	説明
`accountId`	string	必須。ユーザーのアカウント ID。
`password`	暗号化されています	必須。ユーザーのパスワード。
`fullname`	string	必須。ユーザーのフルネーム。
`email`	string	必須。ユーザーの電子メールアドレス。
`enable`	string	ユーザーが有効であるかどうかを示します。この属性はデフォルトでは表示されません。

その他のアカウント属性を追加する場合は、リソースのユーザー属性名を次のいずれかの形式にしてください。

- `Account.`*name*
- `Attribute.`*name*
- `Field.`*name*

たとえば、`sn` という名前のフィールドは、`Field.sn` というリソースユーザー属性名を持ちます。

リソースにアカウントがある場合は、`Account.accounts` という名前のリソースユーザー属性を追加する必要があることもあります。アカウント名は、次の 3 つのフィールドによるコンマ区切り値 (CSV) 文字列として並べられます。

```
ServiceName, accountId, password
```

ユーザーフォームによってこれらの文字列を構築および分解する必要があります。

リソースオブジェクトの管理

なし

アイデンティティーテンプレート

```
$accountId$
```

サンプルフォーム

なし

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

```
com.waveset.adapter.INISafeNexessResourceAdapter
```

◆ ◆ ◆ 第 18 章

18 JMS リスナー

JMS リスナーは、JMS 準拠のメッセージングシステムのキューまたはトピックから送信されたメッセージに対して Active Sync 処理を実行する機能を備えた、JMS (Java Message Service) クライアントです。

このアダプタはソース専用アダプタで、メッセージをキューやトピックに書き戻しすることはできません。

JMS リスナーリソースアダプタは、`com.waveset.adapter.JmsListenerResourceAdapter` クラスで定義されます。

アダプタの詳細

リソースを設定する際の注意事項

JMS リスナーアダプタは、JMS (Java Message Service) オープン標準のバージョン 1.1 以降をサポートするメッセージングシステムのみと対話できます。

アダプタは、指定した接続ファクトリおよび宛先の標準の JNDI 検索を通して、ソース JMS メッセージングシステムのトピックまたはキューと対話します。したがって、メッセージングシステムの管理者は、接続ファクトリと宛先があらかじめ作成済みで、標準の JNDI 検索によって使用可能であることを確認する必要があります。

Identity Manager のインストールに関する注意事項

JMS リスナーリソースアダプタは、次のものをサポートするアプリケーションサーバー環境でのみ使用されます。

- Client API for JMS、バージョン 1.1 以降
- JNDI (Java Naming and Directory Interface) API 1.1 以降

アプリケーションサーバーの管理者は、Identity Manager の Web アプリケーションが、ソース JMS メッセージングシステムに適した JMS 接続ファクトリと宛先オブジェクトに対して、JNDI 経由で正常にバインドできることを確認する必要があります。

使用上の注意

ここでは、JMS リスナーリソースアダプタの使用に関する情報を示します。 次のトピックで構成されています。

接続

Active Sync 処理が開始されると、まず、「接続ファクトリの **JNDI** 名」リソースパラメータフィールドで指定された接続ファクトリを使用して、ソースメッセージングシステムへの接続が作成されます。「ユーザー」および「パスワード」フィールドが指定されている場合は、接続を確立するときに、これらが認証に使用されます。これらのフィールドが指定されていない場合は、デフォルトの認証を使用して接続が確立されます。

JMS リスナーアダプタは、同期モードで操作します。「宛先の **JNDI** 名」フィールドによって指定されたキューまたはトピックの宛先で、同期メッセージコンシューマが確立されます。各ポーリング間隔で、アダプタは提供されるすべてのメッセージを受信および処理します。「メッセージセレクタ」フィールドの有効な JMS メッセージセレクタ文字列を定義することで、メッセージを必要に応じて追加修飾することもできます。

接続ファクトリと宛先の属性によって、指定した宛先タイプに対応するオブジェクトを指定します。宛先タイプに「永続性トピック」を指定した場合、「永続性トピック **ClientID**」および「永続性トピック登録ラベル」という追加フィールドを使用して、永続性登録を設定します。

メッセージマッピング

修飾されたメッセージをアダプタが処理する場合、まず、「メッセージマッピング」フィールドによって指定されたメカニズムを使用して、受信した JMS メッセージを名前付きの値のマップに変換します。変換されたマップは、メッセージ値マップと呼ばれます。

次に、メッセージ値マップは、アカウント属性のスキーママップを使用して、Active Sync マップに変換されます。アダプタにアカウント属性が指定されている場合、アダプタは、スキーママップにリソースユーザー属性としても表示されているキー名で、メッセージ値マップを検索します。値が存在すれば Active Sync マップにコピーされますが、Active Sync マップ内のエントリ名は、スキーママップ内のアイデンティティーシステムのユーザー属性の列で指定された名前に変換されます。

メッセージ値マップにアカウント属性のスキーママップを使用して変換できないエントリが存在する場合は、メッセージ値マップのエントリは、変更されずに Active Sync マップにコピーされます。

保証される配信/信頼される処理

配信の保証は、メッセージの送信者側に責任があります。メッセージシステムによって配信されるまで、持続的に送信されたメッセージのみが保存されます。これにより、メッセージシステムのクラッシュまたはシャットダウンのためにメッセージが失われることを確実に防止できます。この仕組みは once-and-only-once 配信と呼ばれます。

「Reliable Messaging サポート」フィールドは、アダプタが処理する信頼性の高いメッセージ処理の書式を示します。

- LOCAL に設定すると、アダプタに対して JMS セッションが実行されます。処理段階でエラーが発生したかどうかに関係なく、このセッションはメッセージが処理されたあとに常にコミットされます。これにより、メッセージが確実に 1 回だけ処理されます。
- AUTO に設定すると、セッションは処理されませんが、メッセージは AUTO_ACK の JMS 定義に従って即座に自動認識されます。
- DUPS_OK に設定すると、セッションは処理されませんが、メッセージは DUPS_OK_ACK の JMS 定義に従って即座に自動認識されます。
- CLIENT に設定すると、セッションは処理されず、メッセージはアダプタに認識されません。その代わりに、「メッセージライフサイクルリスナー」フィールドに指定されたライフサイクルリスナーが、必要に応じてメッセージを認識します。ライフサイクルリスナーは、AWAITING_CLIENT_ACK ライフサイクルイベントとともに、受信確認が行われる典型的なポイントで呼び出されます。このモードが必要になることはほとんどありません。

ライフサイクルリスナー

「メッセージライフサイクルリスナー」フィールドでは、任意のライフサイクルリスナークラスをアダプタに登録できます。ライフサイクルリスナーを使用すると、次のものを実行できます。

- アダプタの処理段階のカスタムログ
- アダプタの処理段階におけるデータのカスタム操作
- CLIENT_ACK モードで受信したメッセージのカスタム認識

再接続

メッセージングシステムに対する接続を失った場合 (メッセージングシステムサーバーがシャットダウンされた場合など)、リスナーを再度確立するために、メッセージングシステムに対して定期的に再接続を試みるように、アダプタを設定できます。

「例外発生時に再初期化」チェックボックスをオンにすると、再接続動作が使用可能になります。「接続再試行間隔 (秒)」フィールドを使用して、再接続の試行間隔が設定できます。

JMX 監視

JMS リスナーアダプタは、Java Management Extensions (JMX) で監視できる複数の属性および操作を提供します。Identity Manager サーバーでの JMX の設定については、『Business Administrator's Guide』の設定に関する章を参照してください。

Active Sync プロセスが実行されている (かつ信頼できる MBean を含む) サーバーでは、指定されたウィンドウの時間に基づいて統計値が計算されます。setWindowMillis 操作は、期間の長さを設定します。統計値が計算されるたびに、統計ウィンドウの実際の期間が ActualWindowTime 属性として記録されます。

たとえば setWindowMillis 操作が 10000 (10 秒) に設定できても、ActualWindowTime には実際のウィンドウが 10.005 秒であったことを示す値 10005 が含まれる可能性があります。MsgCountInWindow などその他の属性は、実際のウィンドウを使用して統計値を計測またはカウントします。MsgCountInWindow に値 63 が含まれる場合、10.005 秒間に 63 個のメッセージが JMS から取得されたことになります。

次の表に、アダプタが JMX で使用できるようにする属性および操作を示します。属性および操作は、JMX コンソールから IDM/Cluster/ Synchronization/Active Sync/JMS Listener/SyncStats:*DestinationName* で確認できます。*DestinationName* の値は、「宛先タイプ」および「宛先の **JNDI** 名」リソースパラメータの値を結合して生成されます。

JMX の属性

属性	説明
ActualWindowTime	最新のウィンドウの実際の時間 (ミリ秒) を示します。
Attributes	アダプタのリソースパラメータの値を一覧表示します。
Authoritative	サーバーが Active Sync プロセスを実行しているサーバーであるかどうかを示します。
AvgMsgWaitTime	メッセージの待機に費やされた平均の時間 (ミリ秒) を示します。
AvgProcessTime	メッセージの処理に費やされた平均の時間 (ミリ秒) を示します。
CurrentMsgWaitStart	現在のメッセージ待機の待機が開始した日付と時刻を示します。保留中の待機がない場合は NULL です。
CurrentMsgWaitTime	メッセージの待機に費やされたミリ秒を示します。
CurrentPollStart	Active Sync が現在実行中の場合に、Active Sync が最後に開始した日付と時刻を示します。
CurrentProcessStart	現在処理中のメッセージの処理が開始した日付と時刻を示します。
CurrentProcessTime	現在のメッセージの処理に費やされたミリ秒の合計を示します。値が 0 の場合は、メッセージが処理されていないことを示しています。
LastCalculatedPollTime	現在のポーリングが含まれるポーリングループにおけるミリ秒について、最後に計算された時点での合計を示します。
MaxMsgWaitTime	1 メッセージの待機に費やされる最大ミリ秒を示します。
MaxPollTime	1 ポーリングサイクルの最大ミリ秒を示します。
MaxProcessTime	1 メッセージの処理に費やされる最大ミリ秒を示します。
MsgCountInWindow	最後のウィンドウの時間中に受信したメッセージ数を示します。
MsgPerUnittime	指定されたウィンドウ中に処理されたメッセージ数を示します。
PollMsgWaitPercent	メッセージの待機に費やされた時間の割合を示します。
PollOtherPercent	オーバーヘッドとして費やされた時間の割合を示します。
PollProcessPercent	メッセージの処理に費やされた時間の割合を示します。
PollStatistics	最新のウィンドウの実際の時間を示します。
TotMsgCount	受信したメッセージの合計数を示します。
TotMsgWaitTime	メッセージの待機に費やされたミリ秒の合計を示します。
TotProcessTime	メッセージの処理に費やされたミリ秒の合計を示します。

JMX の操作

操作	説明
getWindowMillis	統計ウィンドウの期間 (ミリ秒) を取得します。この操作は、Authoritative 属性が true の場合のみ使用できます。
refreshAttributes	リソース属性の最新の値を返します。
resetStatistics	アダプタの統計値をリセットします。この操作は、Authoritative 属性が true の場合のみ使用できます。
setWindowMillis	統計ウィンドウの期間 (ミリ秒) を設定します。この操作は、Authoritative 属性が true の場合のみ使用できます。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

多くのメッセージングシステムが、クライアントとブローカ間のメッセージの暗号化機能をサポートしています。設定方法は、メッセージングシステムによって異なります。ただし、通常、暗号は抽象化されるので、JMS リスナーアダプタとメッセージングシステムのブローカ間の暗号を有効にするには、特別に設定された接続ファクトリを選択するだけで十分です。

必要な管理特権

JMS リスナーアダプタに対して設定するユーザーおよびパスワードは、JMS メッセージングシステムで認証されたユーザーでなくてはなりません。 また、そのユーザーには、JMS 宛先からのメッセージを読み取るために十分な特権を許可してください。

メッセージングシステム管理者は、デフォルト認証を無効にすることで、JMS 接続を保護するようにしてください。それ以上の保護については、メッセージングシステム管理者が、承認 (アクセス制御) を設定してセキュリティーを最適化します。

プロビジョニングに関する注意事項

次の表に、JMS リスナーアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの作成	なし
アカウントの更新	なし
アカウントの削除	なし
アカウントの有効化/無効化	なし
アカウントの名前の変更	なし
パススルー認証	なし
前アクションと後アクション	なし
データ読み込みメソッド	なし

アカウント属性

アカウント属性はトピックまたはキューから読み取られるメッセージによってかなり異なるため、JMS リスナーアダプタにはデフォルトのアカウント属性が用意されていません。

アイデンティティーシステムユーザー属性の名前が `accountId` であるアカウント属性を定義する必要があります。

リソースオブジェクトの管理

サポートされていません。

アイデンティティーテンプレート

なし。有効な値を持つアイデンティティーテンプレートを設定する必要があります。

サンプルフォーム

`JmsListenerActiveSync.xml`

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

```
com.waveset.adapter.JmsListenerResourceAdapter
```

リソースインスタンスに対して、次の Active Sync ログパラメータを設定することもできます。

- ログアーカイブの最大数
- アクティブログの最大有効期間
- ログファイルの最大サイズ
- ログファイルパス
- ログレベル

タイプ JMS リスナーのリソースを作成時または編集時に、リソースウィザードの「設定のテスト」ボタンを使用すると、広範囲に及ぶチェックが実行されます。これは、設定上の問題のトラブルシューティングに非常に役立ちます。

また、Send JMS Message という名前のレポートでは、キューやトピックにメッセージを送信または発行するための単純なツールも使用できます。このレポートを使用するには、最初に交換ファイル `$WSHOME/sample/SendJMSMessageReport.xml` をインポートします。すると、Send JMS Message レポートのインスタンスを作成できます。このレポートのインスタンスが実行されているときには、指定したキューまたはトピックに、指定したメッセージが書き込まれます。

◆ ◆ ◆ 第 19 章

19 LDAP

Identity Manager では、Lightweight Directory Access Protocol (LDAP) バージョン 3 をサポートするリソースアダプタが提供されます。このアダプタのクラス名は、`com.waveset.adapter.LDAPResourceAdapter` です。

アダプタの詳細

LDAPアダプタは、標準 LDAP インストールのプロビジョニングサービスを提供します。LDAP サーバーのレプリケーションの更新履歴ログを読み取り、それらの変更を Identity Manager ユーザーまたはカスタムワークフローに適用することもできます。

注 – LDAP ChangeLog Active Sync アダプタおよび LDAP リスナー Active Sync は非推奨になりました。これらのアダプタのすべての機能は、LDAP リソースアダプタに統合されました。

リソースを設定する際の注意事項

LDAP アダプタは、旧バージョン形式のログを使用する Sun Java™ System Directory Server リソース用の Active Sync をサポートします。Identity Manager 側では、LDAPActiveSyncForm.xml または LDAPPasswordActiveSyncForm.xml のいずれかを、同期の入力フォームとして使用します。Identity Manager の設定については、『Sun Identity Manager Deployment Guide』の第 3 章「Data Loading and Synchronization」および第 51 章「LDAP パスワードの同期」を参照してください。

Sun Java System Directory Server を設定して、更新履歴ログと修飾子情報の追跡を有効にするには、次の手順を参考にしてください (実際の手順は、Directory Server のバージョンによって異なります)。

▼ LDAP アダプタを使用するように Directory Server を設定する

1 ディレクトリサーバーの設定タブで、「レプリケーション」フォルダをクリックし、「**Enable change log**」ボックスを選択します。**5.0** 以降のサーバーでは、**RetroChangelog** スナップインも有効にします。設定タブで、プラグインオブジェクトに移動し、旧バージョン形式の更新履歴ログプラグインを選択して有効にします。

2 新規作成または変更されたエントリの特殊な属性を維持するようにサーバーが設定されていることを確認するには、**Directory Server** コンソールの「設定」タブをクリックし、左側の区画でナビゲーションツリーのルートエントリを選択します。

3 「設定」サブタブをクリックし、「エントリの変更時間を記録」ボックスにチェックマークが付いていることを確認します。

サーバーは、イベントが Identity Manager から起動されたかどうかを判断するために、新しく作成または変更したエントリに次の属性を追加します。

- **creatorsName**: そのエントリを最初に作成したユーザーの DN。
- **modifiersName**: そのエントリを最後に変更したユーザーの DN。

4 次の手順を実行して、自己署名付き証明書が実装されたディレクトリサーバーに **SSL** 経由で接続します。

- CA 証明書をディレクトリサーバーから一時ファイルにエクスポートします。たとえば、Sun Java System Directory Server で次のコマンドを入力します。

```
certutil -L -d DB_Directory -P slapd-HostName- -n Nickname -a > ds-cert.txt
```

- この証明書をキーストアにインポートします。
-

```
cd $JAVA_HOME/jre/lib/security
keytool -import -file PathTo/ds-cert.txt -keystore ./cacerts
 -storepass changeit -trustcacerts
```

Identity Manager のインストールに関する注意事項

このリソースでは、追加のインストール手順は必要ありません。

使用上の注意

ここでは、LDAP リソースアダプタの使用に関する情報を示します。 次のトピックで構成されています。

LDAP リソースでのパスワード同期の有効化については、第 51 章「LDAP パスワードの同期」を参照してください。

全般的な注意事項

- LDAP に接続するときは、管理者アカウント CN=Directory Manager を使用するのではなく、Identity Manager サービスアカウントを作成するようにしてください。LDAP Directory Server 管理ツールを使用して、各ベースコンテキストで ACI (アクセス制御命令) によってアクセス権を設定します。

  ACI でのアクセス権をソースに基づいて設定します。アダプタからアイデンティティー情報の源泉となるソースに接続する場合は、読み取り、検索、および (場合によっては) 比較のアクセス権のみを設定します。アダプタを書き戻し用に使用する場合は、書き込みと (場合によっては) 削除のアクセス権を設定します。

注 – 更新履歴ログの監視にアカウントを使用する場合は、`cn=changelog` で ACI も作成するようにしてください。更新履歴ログのエントリに対しては書き込みも削除もできないため、アクセス権は読み取りと検索のみに設定するとよいでしょう。

- LDAP アダプタは、別名を管理できます。ただし、`getUser` の呼び出しが実行される場合、別名が逆参照されて、アダプタは参照先オブジェクトを返します。結果として、アダプタは別名オブジェクト自体の属性を検索しません。

  これは、JNDI のデフォルトが次の設定になっているために発生します。

  ```
  java.naming.ldap.derefAliases=always
  ```

  このプロパティーは、次の行が含まれる `jndi.properties` ファイルを作成することでグローバルに変更できます。

  ```
  java.naming.ldap.derefAliases=never
  ```

  `jndi.properties` ファイルは、Java ライブラリパス (`$WSHOME/WEB-INF/classes` など) に配置する必要があります。変更を有効にするために、アプリケーションサーバーを再起動します。

- 同期ポリシーを編集するときは、「変更者フィルタ」フィールドの値を指定してください。標準の値は、このアダプタで使用される管理者の名前です。管理者の名前を入力すると、無限ループが発生することを防ぐことができます。エントリの形式は、`cn=Directory Manager` です。

Directory Server 向けの仮想リスト表示のサポート

注 – ここでは、Identity Manager が RootDN 以外のユーザーとして LDAP リソースに接続することを前提としています。RootDN ユーザーとして接続する場合は、ここで説明する手順を適用できますが、ほかの LDAP 属性値でも可能な場合があります。詳細は、Directory Server のマニュアルを参照してください。

Microsoft ADAM でこの機能を有効にする方法については、223 ページの「ADAM スキーマの修正」を参照してください。

Directory Server では、検索できる LDAP エントリの数と取得できる LDAP エントリの数を、それぞれ `nsLookThroughLimit` 属性と `nsslapd-sizelimit` 属性によって定義します。`nsLookThroughLimit` のデフォルト値は 5,000 で、`nsslapd-sizelimit` のデフォルト値は 2,000 です。どちらの属性も、-1 に設定すると制限が無効になります。これらの属性の値を変更した場合は、Directory Server を再起動してください。

必ずしもデフォルト値を変更した方がよいとは限りません。LDAP 検索のパフォーマンスを向上させるために、LDAP 仮想リスト表示 (VLV) コントロールを有効にできます。VLV は、一度にすべての検索結果を返さず、検索結果の一部を返します。

「ブロックを使用」リソース属性を使用すると、VLV コントロールの使用によって Identity Manager のクエリー結果を常にサイズ制限の範囲内を収めることができます。「ブロック数」リソース属性は、取得するユーザーの数を指定しますが、この値は `nsslapd-sizelimit` 属性に設定された値以下にする必要があります。

VLV インデックス (参照インデックスとも呼ばれる) を作成してください。 作成しないと、`nsslapd-sizelimit` によるサイズ制限が有効なままになります。VLV インデックスによってアカウントの反復処理のパフォーマンスが大幅に向上するため、調整、リソースからの読み込み、またはファイルへのエクスポートを頻繁に行う予定である場合は、インデックスを設定するようにしてください。

VLV インデックスの作成の詳細な手順については、Directory Server のマニュアルを参照してください。基本的なプロセスは次のとおりです。

▼ VLV インデックスを作成する

1 次のプロパティーを持つ vlvsearch オブジェクトを作成します。

```
vlvbase: YourBaseContext
vlvfilter: (&(objectclass=top)(objectclass=person)
(objectclass=organizationalPerson) (objectclass=inetorgperson))
vlvscope: 2
```

vlvbase 属性は、「ベースコンテキスト」リソース属性に指定した値に一致させる必要があります。vlvfilter 属性には、「オブジェクトクラス」リソース属性に指定したクラスを、ここに示した形式で含める必要があります。vlvscope の値 2 は、サブツリー検索を示します。

2 vlvindex コンポーネントを vlvsearch のサブオブジェクトとして作成します。vlvsort 属性を uid に設定してください。

3 vlvindex コマンドまたはほかのメカニズムを使用して、**VLV** インデックスを構築します。

4 **ACI (**アクセス制御命令**)** により次の項目のアクセス権を設定します。

- vlvsearch オブジェクト
  - vlvindex
  - インデックスが作成されたディレクトリ

    更新履歴ログの VLV を設定するには、次の一般的な手順に従います。詳細な手順については、Directory Server のマニュアルを参照してください。

5 更新履歴ログの参照インデックスをまだ作成していない場合は、作成します。**Directory Server** のユーザーインタフェースを使用すると、デフォルトで "MCC cn=changelog" という名前の vlvsearch オブジェクトと、"SN MCC cn=changelog" という名前の vlvindex オブジェクトが作成されます。

6 アクセス制御命令 **(ACI)** によりアクセス権を設定し、**Identity Manager** アカウントが次の項目の読み取り、比較、および検索の権限を持つようにします。

- 更新履歴ログ (cn=changelog)
  - vlvsearch オブジェクト (cn="MCC cn=changelog",cn=config,cn=ldbm)
  - vlvindex オブジェクト ("SN MCC cn=changelog",cn=config,cn=ldbm)

Directory Server の一部のバージョンでは、更新履歴ログの nsLookThroughLimit 属性に 5,000 の値がハードコードされています。更新履歴ログの nsLookThroughLimit 制限にかかるのを避けるには、サーバーで保持する更新履歴ログエントリの最大数を 5,000 未満に制限します。更新履歴ログのエントリが失われるのを避けるには、アダプタのポーリング間隔を短くします。

アカウントの無効化と有効化

LDAP アダプタには、LDAP リソース上のアカウントを無効にするための方法が複数用意されています。アカウントを無効にするには、次のいずれかの手法を使用します。

パスワードを不明な値に変更する

アカウントのパスワードを不明な値に変更することによってアカウントを無効にするには、「LDAP アクティブ化メソッド」フィールドと「LDAP アクティブ化パラメータ」フィールドを空白のままにします。これは、アカウントを無効にするときのデフォルトの方法です。無効になったアカウントは、新しいパスワードを割り当てることによって再度有効にできます。

nsmanageddisabledrole ロールを割り当てる

`nsmanageddisabledrole` LDAP ロールを使用してアカウントの無効化と有効化を行うには、LDAP リソースを次のように設定します。

▼ **nsmanageddisabledrole LDAP ロールを使用するように LDAP リソースを設定する**

1. 「リソースパラメータ」ページで、「**LDAP** アクティブ化メソッド」フィールドを `nsmanageddisabledrole` に設定します。
2. 「**LDAP** アクティブ化パラメータ」フィールドを *IDMAttribute*`=CN=nsmanageddisabledrole,` *baseContext* に設定します。*IDMAttribute* は、次の手順でスキーマに指定します。
3. 「アカウント属性」ページで、*IDMAttribute* をアイデンティティーシステムユーザー属性として追加します。リソースユーザー属性を `nsroledn` に設定します。この属性のタイプは文字列にしてください。
4. **LDAP** リソース上に `nsAccountInactivationTmp` という名前のグループを作成し、`CN=nsdisabledrole,`*baseContext* をメンバーとして割り当てます。

   これで、LDAP アカウントを無効にできます。LDAP コンソールを使用して検証するには、`nsaccountlock` 属性の値を確認します。値が `true` であれば、アカウントはロックされています。

   あとでアカウントが再度有効にされると、ロールからアカウントが削除されます。

nsAccountLock 属性を設定する

`nsAccountLock` 属性を使用してアカウントの無効化と有効化を行うには、LDAP リソースを次のように設定します。

▼ nsAccountLock 属性を使用するように LDAP リソースを設定する

1 「リソースパラメータ」ページで、「**LDAP** アクティブ化メソッド」フィールドを `nsaccountlock` に設定します。

2 「**LDAP** アクティブ化パラメータ」フィールドを *IDMAttribute*=`true` に設定します。*IDMAttribute* は、次の手順でスキーマに指定します。たとえば、`accountLockAttr=true` とします。

3 「アカウント属性」ページで、「**LDAP** アクティブ化パラメータ」フィールドに指定した属性 (たとえば、**accountLockAttr**) をアイデンティティーシステム ユーザー属性として追加します。リソースユーザー属性を `nsaccountlock` に設定します。この属性のタイプは文字列にしてください。

4 リソース上で、`nsAccountLock` **LDAP** 属性を `true` に設定します。

アカウントを無効化すると、Identity Manager は、`nsaccountlock` を `true` に設定します。また、すでに `nsaccountlock` が `true` に設定されていた LDAP ユーザーについても、無効と見なします。`nsaccountlock` の値が `true` 以外の値 (NULL を含む) に設定されている場合、そのユーザーは有効であるとみなします。

nsmanageddisabledrole 属性や nsAccountLock 属性を使用せずにアカウントを無効にする

「使用中のディレクトリサーバーでは `nsmanageddisabledrole` 属性や `nsAccountLock` 属性を使用できないが、アカウントを無効にする同様の方法がある場合は、「LDAP アクティブ化メソッド」フィールドに次のいずれかのクラス名を入力します。「LDAP アクティブ化パラメータ」フィールドに入力する値は、クラスによって異なります。

Class Name	使用する状況
`com.waveset.adapter.util.ActivationByAttributeEnableFalse`	ディレクトリサーバーは、属性を false に設定することによってアカウントを有効にし、属性を true に設定することによってアカウントを無効にします。 この属性をスキーママップに追加します。次に、「LDAP アクティブ化パラメータ」フィールドに、(スキーママップの左側に定義された) この属性の Identity Manager 名を入力します。

Class Name	使用する状況
com.waveset.adapter.util.ActivationByAttributeEnableTrue	ディレクトリサーバーは、属性を true に設定することによってアカウントを有効にし、属性を false に設定することによってアカウントを無効にします。 この属性をスキーママップに追加します。次に、「LDAP アクティブ化パラメータ」フィールドに、(スキーママップの左側に定義された) この属性の Identity Manager 名を入力します。
com.waveset.adapter.util.ActivationByAttributePullDisablePushEnable	Identity Manager は、LDAP から属性と値のペアを引き出すことによってアカウントを無効にし、LDAP に属性と値のペアをプッシュすることによってアカウントを有効にします。 この属性をスキーママップに追加します。次に、「LDAP アクティブ化パラメータ」フィールドに属性と値のペアを入力します。スキーママップの左側に定義されている、属性の Identity Manager 名を使用します。
com.waveset.adapter.util.ActivationByAttributePushDisablePullEnable	Identity Manager は、LDAP に属性と値のペアをプッシュすることによってアカウントを無効にし、LDAP から属性と値のペアを引き出すことによってアカウントを有効にします。 この属性をスキーママップに追加します。次に、「LDAP アクティブ化パラメータ」フィールドに属性と値のペアを入力します。スキーママップの左側に定義されている、属性の Identity Manager 名を使用します。
com.waveset.adapter.util.ActivationNsManagedDisabledRole	ディレクトリは、特定のロールを使用してアカウントステータスを決定します。このロールにアカウントが割り当てられている場合、そのアカウントは無効になります。 このロール名をスキーママップに追加します。次に、「LDAP アクティブ化パラメータ」フィールドに次の形式で値を入力します。 *IDMAttribute*=CN=*roleName*, *baseContext* *IDMAttribute* は、スキーママップの左側に定義されている、ロールの Identity Manager 名です。

ADAM のサポート

LDAP アダプタは、Microsoft の Application Directory Application Mode (ADAM) にプロビジョニングするように設定できます。次のそれぞれの節では、ADAM のサポートを有効にする方法について説明します。

ADAM スキーマの修正

Identity Manager で使用するために ADAM スキーマの調整が必要なことがあります。リソーススキーマおよび LDAP リソースのアイデンティティーテンプレートには、一意の識別子 (またはアカウント ID) の参照が含まれることがあります。ADAM は、次の点がその他の LDAP 実装と異なります。

- ADAM では、オブジェクトクラス定義は、単一の命名属性だけを許容します。命名属性は、DN の一番左にある RDN コンポーネントに現れる属性です。
- `uid` 属性は、複数値として定義されます。
- `cn` 属性は、単一値として定義され、64 文字以下にする必要があります。

ADAM スキーマは、属性インデックス設定を定義します。スキーマの各属性定義エントリには `searchFlags` 属性があります。たとえば `Uid` は、スキーマコンテキストの cn=Uid,cn=Schema に位置します。`searchFlags` 属性は、ビットマスクであり、1 (インデックス作成)、2 (コンテナごとのインデックス作成)、および 64 (効率的な VLV クエリをサポートするインデックス) の値はインデックス作成に関連します。

ADAM インスタンスでスキーマを更新する詳細は、Microsoft のマニュアルを参照してください。

ADAM でのアカウントの有効化と無効化

ADAM での調整では、ページング結果コントロールまたは仮想リスト表示コントロールのいずれかを使用できます。ページング結果コントロールを使用するには、リソースのリソースパラメータ設定ページで、「Use Paged Results Control」チェックボックスにチェックマークを付けます。仮想リスト表示コントロールを使用するには、リソースのリソースパラメータ設定ページの「VLV Sort Attribute」で名前を付けた属性が、有効な VLV クエリーをサポートするオプションを設定して、ADAM でインデックス化されている必要があります。詳細は、「ADAM スキーマの修正」を参照してください。

Active Sync は ADAM でサポートされていません。

次の手順に従って、Identity Manager が ADAM のアカウントを有効および無効にできるようにします。

▼ ADAM でのアカウントの有効化と無効化

1 「**LDAP** リソースパラメータ」ページで、「**LDAP** アクティブ化メソッド」パラメータを `com.waveset.adapter.util.ActivationByAttributePushDisablePullEnable` に設定します。

2 「**LDAP** アクティブ化パラメータ」を *Identity_System_Attribute*=`true` に設定します。アイデンティティーシステム属性は、次の手順で「アカウント属性」ページで指定します。たとえば `MyUserAccountDisabled=true` とします。

3 「アカウント属性」ページで、「**LDAP** アクティブ化パラメータ」フィールドに指定したアイデンティティーシステム属性をアイデンティティーシステムユーザー属性として追加します。リソースユーザー属性を `msDS-UserAccountDisabled` に設定します。この属性のタイプは文字列にしてください。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は、TCP/IP または SSL 経由の Java Naming and Directory Interface (JNDI) を使用して LDAP アダプタと通信します。

- TCP/IP を使用する場合は、「リソースパラメータ」ページでポート 389 を指定します。
- SSL を使用する場合は、ポート 636 を指定します。

必要な管理特権

「ユーザー DN」リソースパラメータに値 `cn=Directory Manager` を指定すると、Identity Manager 管理者には、LDAP アカウント管理に必要なアクセス権が付与されます。別の識別名を指定する場合は、そのユーザーに、ユーザーの読み取り、書き込み、削除、および追加のアクセス権を付与してください。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	あり
パススルー認証	あり
前アクションと後アクション	なし

機能	サポート状況
データ読み込みメソッド	■ リソースから直接インポート ■ リソースの調整

アカウント属性

属性の構文 (または型) は、通常、属性がサポートされるかどうかを決定します。一般に、Identity Manager は Boolean 型、文字列型、整数型、およびバイナリ型の構文をサポートします。バイナリ属性は、バイト配列としてのみ安全に表現できる属性です。

次の表に、サポートされている LDAP 構文の一覧を示します。ほかの LDAP 構文でも、事実上 Boolean 型、文字列型、または整数型であれば、サポートされる可能性があります。オクテット文字列はサポートされません。

LDAP 構文	属性タイプ	オブジェクト ID
Audio	Binary	1.3.6.1.4.1.1466.115.121.1.4
Binary	Binary	1.3.6.1.4.1.1466.115.121.1.5
Boolean	Boolean	1.3.6.1.4.1.1466.115.121.1.7
Country String	String	1.3.6.1.4.1.1466.115.121.1.11
DN	String	1.3.6.1.4.1.1466.115.121.1.12
Directory String	String	1.3.6.1.4.1.1466.115.121.1.15
Generalized Time	String	1.3.6.1.4.1.1466.115.121.1.24
IA5 String	String	1.3.6.1.4.1.1466.115.121.1.26
Integer	Int	1.3.6.1.4.1.1466.115.121.1.27
Postal Address	String	1.3.6.1.4.1.1466.115.121.1.41
Printable String	String	1.3.6.1.4.1.1466.115.121.1.44
Telephone Number	String	1.3.6.1.4.1.1466.115.121.1.50

デフォルトのアカウント属性

次の属性は、LDAP リソースアダプタの「アカウント属性」ページに表示されます。特に記載されていないかぎり、属性の型はすべて String です。

アイデンティティーシステム属性	リソースユーザー属性	LDAP 構文	説明
accountId	uid	Directory string	User ID
accountId	cn	Directory string	必須。ユーザーのフルネーム。
firstname	givenname	Directory string	ユーザーの名。
lastname	sn	Directory string	必須。ユーザーの姓。
modifyTimeStamp	modifyTimeStamp	Generalized time	ユーザーエントリが変更された日時を示します。
password	userPassword	Octet string	暗号化された値。ユーザーのパスワード。

グループ管理属性

次の表に示すアカウント属性は、デフォルトではスキーマに表示されません。グループを管理するには、これらの属性をスキーママップに追加してください。

アイデンティティーシステム属性	リソースユーザー属性	LDAP 構文	説明
user defined	ldapGroups	ldapGroups	LDAP ユーザーがメンバーになっているグループの識別名のリスト。 リソース属性である「グループメンバー属性」では、ユーザーの識別名を含むように更新される LDAP グループエントリの属性を指定します。「グループメンバー属性」のデフォルト値は、uniquemember です。
user defined	posixGroups	なし	LDAP ユーザーがメンバーになっている posixGroups エントリの識別名のリスト。 アカウントに Posix グループのメンバーシップを割り当てるには、そのアカウントが uid LDAP 属性の値を持っている必要があります。posixGroup エントリの memberUid 属性は、ユーザーの uid を含むように更新されます。

スキーママップに posixGroups または ldapGroups が定義されている場合は、次の動作に注意してください。

- LDAP アカウントが削除されると、Identity Manager はすべての LDAP グループからそのアカウントの DN を削除し、すべての posixGroups からそのアカウントの uid を削除します。

- アカウントの uid が変更されると、Identity Manager は、該当する posixGroups 内で、古い uid を新しい uid で置き換えます。
- アカウントの名前が変更されると、Identity Manager は、該当する LDAP グループ内で、古い DN を新しい DN で置き換えます。

Person オブジェクトクラス

次の表に、LDAP Person オブジェクトクラスで定義されている、サポートされている属性を示します。Person オブジェクトクラスに定義されている属性の一部は、デフォルトで表示されます。

アイデンティティーシステム属性	リソースユーザー属性	LDAP 構文	説明
description	Directory string	String	ユーザーの特定の関心事についての簡潔でわかりやすい説明
seeAlso	DN	String	ほかのユーザーへの参照
telephoneNumber	Telephone number	String	第一電話番号

Organizationalperson オブジェクトクラス

次の表に、LDAP organizationalPerson オブジェクトクラスで定義される追加のサポート対象属性の一覧を示します。このオブジェクトクラスは、Person オブジェクトクラスから属性を継承することもできます。

リソースユーザー属性	LDAP 構文	属性タイプ	説明
destinationIndicator	Printable string	String	この属性は、電報サービスに使用されます。
facsimileTelephoneNumber	Facsimile telephone number	String	第一 FAX 番号。
internationaliSDNNumber	Numeric string	String	オブジェクトに関連付けられた国際 ISDN 番号を指定します。
l	Directory string	String	都市、国、その他の地理的領域などの地域の名前
ou	Directory string	String	組織単位の名前
physicalDeliveryOfficeName	Directory string	String	配達物の送付先となるオフィス。
postalAddress	Postal address	String	ユーザーの勤務先オフィスの所在地。

リソースユーザー属性	LDAP 構文	属性タイプ	説明
postalCode	Directory string	String	郵便配達用の郵便番号。
postOfficeBox	Directory string	String	このオブジェクトの私書箱番号。
preferredDeliveryMethod	Delivery method	String	受取人への優先される送付方法
registeredAddress	Postal Address	String	受信者に配達を受け入れてもらう必要がある電報や速達文書の受け取りに適した郵便の宛先。
st	Directory string	String	州名または都道府県名。
street	Directory string	String	郵便の宛先の番地部分。
teletexTerminalIdentifier	Teletex Terminal Identifier	String	オブジェクトに関連付けられたテレテックス端末の識別子
telexNumber	Telex Number	String	国際表記法によるテレックス番号
title	Directory string	String	ユーザーの役職を格納します。このプロパティーは、一般に、プログラマーのような職種ではなく、「シニアプログラマー」のような正式な役職を示すために使用されます。通常、Esq. や DDS などの敬称には使用されません。
x121Address	Numeric string	String	オブジェクトの X.121 アドレス。

inetOrgPerson オブジェクトクラス

次の表に、LDAP inetOrgPerson オブジェクトクラスで定義される追加のサポート対象属性の一覧を示します。このオブジェクトクラスは、organizationalPerson オブジェクトクラスから属性を継承することもできます。

アイデンティティーシステム属性	リソースユーザー属性	LDAP 構文	説明
audio	Audio	Binary	オーディオファイル。
businessCategory	Directory string	String	組織で実施されているビジネスの種類。
carLicense	Directory string	String	自動車の登録番号 (ナンバープレート)
departmentNumber	Directory string	String	組織内の部署を特定します
displayName	Directory string	String	エントリを表示するときに優先的に使用されるユーザーの名前
employeeNumber	Directory string	String	組織内の従業員を数値で示します

アイデンティティーシステム属性	リソースユーザー属性	LDAP 構文	説明
employeeType	Directory string	String	従業員、契約社員などの雇用形態
homePhone	Telephone number	String	ユーザーの自宅電話番号。
homePostalAddress	Postal address	String	ユーザーの自宅住所。
initials	Directory string	String	ユーザーのフルネームの各部のイニシャル。
jpegPhoto	JPEG	Binary	JPEG 形式のイメージ。
labeledURI	Directory string	String	ユーザーに関連付けられた URI (Universal Resource Indicator) とオプションのラベル。
mail	IA5 string	String	1 つ以上の電子メールアドレス。
manager	DN	String	ユーザーのマネージャーのディレクトリ名。
mobile	Telephone number	String	ユーザーの携帯電話番号。
o	Directory string	String	組織の名前。
pager	Telephone number	String	ユーザーのポケットベル番号。
preferredLanguage	Directory string	String	優先される、ユーザーの書き言葉または話し言葉の言語。
roomNumber	Directory string	String	ユーザーのオフィスまたは部屋の番号。
secretary	DN	String	ユーザーの管理補佐のディレクトリ名。
userCertificate	certificate	Binary	バイナリ形式の証明書。

リソースオブジェクトの管理

Identity Manager は、デフォルトで次の LDAP オブジェクトをサポートします。文字列ベース、整数ベース、またはブールベースの属性も管理できます。

リソースオブジェクト	サポートされる機能	管理される属性
Group	作成、更新、削除、名前の変更、名前を付けて保存	cn、description、owner、uniqueMember

リソースオブジェクト	サポートされる機能	管理される属性
Posix Group	作成、更新、削除、名前の変更、名前を付けて保存	cn、description、gid、memberUid
Domain	Find	dc
Organizational Unit	作成、削除、名前の変更、名前を付けて保存、検索	ou
組織	作成、削除、名前の変更、名前を付けて保存、検索	o

LDAP リソースアダプタは、posixGroup エントリの管理機能を提供します。デフォルトでは、posixGroup に割り当てることができるアカウントのリストに posixAccount オブジェクトクラスが含まれています。LDAP Create Posix Group Form と LDAP Update Posix Group Form をカスタマイズして、posixAccount 以外のアカウントを一覧表示できます。ただし、これらのアカウントに対して、posixGroup のメンバーになるための uid 属性を定義する必要があります。

アイデンティティーテンプレート

このリソースのアイデンティティーテンプレートを指定する必要があります。

サンプルフォーム

組み込みのフォーム

- LDAP グループ作成フォーム
- LDAP 組織作成フォーム
- LDAP 組織単位作成フォーム
- LDAP 人物作成フォーム
- LDAP Create Posix Group Form
- LDAP グループ更新フォーム
- LDAP 組織更新フォーム
- LDAP 組織単位更新フォーム
- LDAP 人物更新フォーム
- LDAP Update Posix Group Form

その他の利用可能なフォーム

- LDAPActiveSyncForm.xml
- LDAPGroupCreateExt.xml
- LDAPGroupUpdateExt.xml

- LDAPgroupScalable.xml
- LDAPPasswordActiveSyncForm.xml

LDAPGroupCreateExt.xml フォームと LDAPGroupUpdateExt.xml フォームには、一意でないメンバー名を入力できます。

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスの 1 つ以上でトレースオプションを設定します。

- com.waveset.adapter.LDAPResourceAdapterBase
- com.waveset.adapter.LDAPResourceAdapter

◆ ◆ ◆ 第 20 章

20 Microsoft Identity Integration Server

Microsoft Identity Integration Server (MIIS) リソースアダプタは、`com.waveset.adapter.MIISResourceAdapter` クラスで定義されます。

アダプタの詳細

MIIS アダプタは、データベーステーブルリソースアダプタとして実装されます。このため、MIIS アダプタには同様のインストール要件があり、配下のデータベースと同じ管理特権が必要です。

MIIS アダプタは、次のデータベースシステムと組み合わせて使用できます。

- SQL Server
- DB2
- MySQL
- Oracle

リソースを設定する際の注意事項

なし

Identity Manager のインストールに関する注意事項

ここに示すインストールの注意点では、SQL Server のデータベーステーブルを管理することを想定します。SQL Server 以外のデータベースを使用している場合は、そのデータベースに必要な JAR ファイルをコピーします。詳細は、該当するデータベースリソースアダプタの、「Identity Manager のインストールに関する注意事項」の節を参照してください。

MIIS リソースアダプタは、カスタムアダプタです。インストールプロセスを完了するには、次の手順を実行してください。

▼ MIIS リソースアダプタをインストールする

1 「管理するリソースの設定」ページの「リソース」セクションから「**Microsoft Identity Integration Server**」オプションを選択します。

2 **Microsoft SQL Server 2005 Driver for JDBC** を使用してリソースに接続する場合は、`mssqlserver.jar` ファイルを *InstallDir*`\idm\WEB-INF\lib` ディレクトリにコピーします。

Microsoft SQL Server 2000 Driver for JDBC を使用してリソースに接続する場合は、次の JAR ファイルを `Program Files\2000 Microsoft SQL Server 2000 Driver for JDBC\lib` ディレクトリから *InstallDir*`\idm\WEB-INF\lib` ディレクトリにコピーします。

- `msbase.jar`
  - `mssqlserver.jar`
  - `msutil.jar`

注 – SQL Server への接続は、すべて同じバージョンの JDBC ドライバを使用して実行してください。これには、リポジトリだけではなく、SQL Server のアカウントまたはテーブルを管理または要求するすべてのリソースアダプタ (Microsoft SQL アダプタ、Microsoft Identity Integration Server アダプタ、データベーステーブルアダプタ、スクリプト JDBC アダプタ、これらのアダプタをベースとするすべてのカスタムアダプタなど) が含まれます。異なるバージョンのドライバを使用しようとすると、競合エラーが発生します。

使用上の注意

なし

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は、JDBC を使用して MIIS アダプタと通信します。

必要な管理特権

ユーザーは、データベース内のフィールドの読み取り、書き込み、削除、および変更ができる必要があります。詳細は、データベースアダプタのマニュアルを参照してください。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	なし
パススルー認証	あり
前アクションと後アクション	なし
データ読み込みメソッド	■ リソースからのデータのインポート ■ 調整

アカウント属性

アカウント属性のリストは、MIIS リソースの設定中に「Managed Columns」として選択したデータベース列によって決まります。選択できるアカウント属性は、インストールごとに異なります。

リソースオブジェクトの管理

なし

アイデンティティーテンプレート

$accountId$

サンプルフォーム

なし

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

- `com.waveset.adapter.MIISResourceAdapter`
- `com.waveset.adapter.JdbcResourceAdapter`

◆ ◆ ◆ 第 21 章

21 Microsoft SQL Server

Microsoft SQL Server リソースアダプタ
は、`com.waveset.adapter.MSSQLServerResourceAdapter` クラスで定義されます。

アダプタの詳細

このアダプタを使用して、SQL Server 上の複数のデータベースを管理しま
す。サーバー自体へのログインだけでなく、管理対象のデータベースへのログイン
も管理できます。

カスタム SQL テーブルがある場合、リソースアダプタウィザードを使用してカスタム Microsoft SQL テーブルリソースを作成する方法については、第 10 章「データベーステーブル」を参照してください。

リソースを設定する際の注意事項

なし

Identity Manager のインストールに関する注意事項

Microsoft SQL Server リソースアダプタは、カスタムアダプタです。インストールプロセスを完了するには、次の手順を実行する必要があります。

▼ Microsoft SQL Server リソースアダプタをインストールする

1 このリソースを **Identity Manager** のリソースリストに追加するには、「管理するリソースの設定」ページの「カスタムリソース」セクションに次の値を追加する必要があります。

```
com.waveset.adapter.MSSQLServerResourceAdapter
```

2 **Microsoft SQL Server 2005 Driver for JDBC** を使用してリソースに接続する場合は、`mssqlserver.jar` ファイルを *InstallDir*`\idm\WEB-INF\lib` ディレクトリにコピーします。

Microsoft SQL Server 2000 Driver for JDBC を使用してリソースに接続する場合は、次の JAR ファイルを `Program Files\2000 Microsoft SQL Server 2000 Driver for JDBC\lib` ディレクトリから *InstallDir*`\idm\WEB-INF\lib` ディレクトリにコピーします。

- `msbase.jar`
  - `mssqlserver.jar`
  - `msutil.jar`

注 – SQL Server への接続は、すべて同じバージョンの JDBC ドライバを使用して実行してください。これには、リポジトリだけではなく、SQL Server のアカウントまたはテーブルを管理または要求するすべてのリソースアダプタ (Microsoft SQL アダプタ、Microsoft Identity Integration Server アダプタ、データベーステーブルアダプタ、スクリプト JDBC アダプタ、これらのアダプタをベースとするすべてのカスタムアダプタなど) が含まれます。異なるバージョンのドライバを使用しようとすると、競合エラーが発生します。

使用上の注意

SQL Server では、2 種類の認証を使用できます。

- Windows 認証。この場合、SQL Server はすべての認証とセキュリティーに関して Windows のメカニズムを信頼します。ユーザーが SQL Server にアクセスすると、SQL Server はユーザーのネットワークセキュリティー属性からユーザーとパスワードの情報を取得します。ユーザーに Windows 内部から SQL Server へのアクセス権が許可されている場合、そのユーザーは SQL Server に自動的にログインします。アダプタに渡されるアカウント ID は、*Domain* *accountID* の形式にする必要があります。Windows 認証では、パススルー認証はサポートされていません。
- 混合モード認証。このシナリオでは、Windows 認証と SQL Server 認証の両方が有効になります。ユーザーが信頼できない接続から指定されたログイン名とパスワードを使用して接続すると、SQL Server ログインアカウントが設定されているかどうか、および指定されたパスワードが以前に記録されたものと一致するかど

うかを確認することにより、SQL Server はそれ自体で認証を行います。SQL Server にログインアカウントが設定されていない場合、認証は失敗し、ユーザーはエラーメッセージを受信します。

SQL Server リソースアダプタの Windows 認証モードを Microsoft SQL Server アダプタで設定できるのは、SQL Server サーバーインスタンスと同じ Windows セキュリティーおよび認証フレームワークに含まれる Windows マシンで Identity Manager サーバーが実行されている場合のみです。

JDBC ドライバでは、integratedSecurity 接続文字列プロパティーを使用して、Windows オペレーティングシステムにおけるタイプ 2 の統合認証の使用をサポートします。統合認証を使用するには、`sqljdbc_auth.dll` ファイルを JDBC ドライバがインストールされているコンピュータの Windows システムパス上のディレクトリにコピーします。

`sqljdbc_auth.dll` ファイルは、次の場所にインストールされます。

`InstallationDirectory``\sqljdbc_`**`Version\Language`**`\auth\`

32 ビットプロセッサでは、x86 フォルダの `sqljdbc_auth.dll` ファイルを使用します。64 ビットプロセッサでは、x64 フォルダの `sqljdbc_auth.dll` ファイルを使用します。

詳細については、次の記事を参照してください。

`http://msdn2.microsoft.com/en-us/library/ms378428.aspx`

SQL Server リソースアダプタは、次のシステムプロジージャーを使用してユーザーアカウントを管理します。

- sp_addlogin、sp_droplogin
- sp_addrole
- sp_addrolemember、sp_droprolemember
- sp_addsrvrolemember、sp_dropsrvrolemember
- sp_grantdbaccess
- sp_helplogins
- sp_helprole
- sp_helpuser
- sp_helpsrvrolemember
- sp_password
- sp_revokedbaccess

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は、SSL 経由の JDBC を使用して SQL Server と通信します。

必要な管理特権

次の表に、システムプロジージャーを実行できるユーザーを示します。

システムプロジージャー	必要なアクセス権
sp_addlogin	**sysadmin** および **securityadmin** 固定サーバーロールのメンバー。
sp_addrole	**sysadmin** 固定サーバーロール、および **db_securityadmin** 固定データベースロールと **db_owner** 固定データベースロールのメンバー。
sp_addrolemember	**sysadmin** 固定サーバーロールと d**b_owner** 固定データベースロールのメンバーは、sp_addrolemember を実行して固定データベースロールにメンバーを追加できます。ロールの所有者は、sp_addrolemember を実行して自分が所有する任意の SQL Server ロールにメンバーを追加できます。**db_securityadmin** 固定データベースロールのメンバーは、任意のユーザー定義のロールにユーザーを追加できます。
sp_addsvrrolemember	**sysadmin** 固定サーバーロールのメンバー。
sp_droplogin	**sysadmin** および **securityadmin** 固定サーバーロールのメンバー。
sp_droprolemember	**sysadmin** 固定サーバーロール、**db_owner** 固定データベースロール、および **db_securityadmin** 固定データベースロールのメンバーのみが、sp_droprolemember を実行できます。**db_owner** 固定データベースロールのメンバーのみが固定データベースロールからユーザーを削除できます。
sp_dropsvrrolemember	**sysadmin** 固定サーバーロールのメンバー。
sp_grantdbaccess	**sysadmin** 固定サーバーロール、**db_accessadmin** 固定データベースロール、および **db_owner** 固定データベースロールのメンバー。
sp_helplogins	**sysadmin** および **securityadmin** 固定サーバーロールのメンバー。
sp_helprole	デフォルトでは、**public** ロールに実行権が設定されます。
sp_helpsrvrolemember	デフォルトでは、**public** ロールに実行権が設定されます。
sp_helpuser	デフォルトでは、**public** ロールに実行権が設定されます。
sp_password	自分のログイン用のパスワードを変更するユーザーのために、デフォルトで **public** ロールに実行権が設定されます。**sysadmin** ロールのメンバーのみがほかのユーザーのログイン用のパスワードを変更できます。
sp_revokedbaccess	**sysadmin** 固定サーバーロール、**db_accessadmin** 固定データベースロール、および **db_owner** 固定データベースロールのメンバー。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	なし
パススルー認証	■ 混合モード認証: 使用可 ■ Windows 認証: 使用不可
前アクションと後アクション	なし
データ読み込みメソッド	■ リソースから直接インポート ■ リソースの調整

アカウント属性

次の表に、デフォルトのアカウント属性 (すべて文字列) を示します。

Identity Manager ユーザー属性	リソースユーザー属性	説明
domain	IGNORE_ATTR	ユーザーが属するドメイン。
defaultDB	defaultDB	ユーザーがデフォルトで使用するデータベース。
serverRoles	serverRoles	ユーザーがメンバーになっているデータベースロール。

複数のデータベースを管理する可能性があるため、Identity Manager の管理者は、各データベースを管理するためのアカウント属性を追加する必要があります。ほかの管理対象データベースの属性と区別するため、これらの属性には属性名の一部としてデータベース名を含めてください。

Identity Manager ユーザー属性	データ型	説明
userName*DBName*	String	データベース上のアカウントのユーザー名。データベースの userName を設定することによってアカウントにデータベースへのアクセス権が与えられ、データベースの userName を消去することによってアクセス権が削除されます。

Identity Manager ユーザー属性	データ型	説明
roles*DBName*	String	データベース上のアカウントのロール。

リソースオブジェクトの管理

なし

アイデンティティーテンプレート

```
$domain$ $accountId$
```

サンプルフォーム

```
MSSQLServerUserForm.xml
```

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

- `com.waveset.adapter.MSSQLServerResourceAdapter`
- `com.waveset.adapter.JdbcResourceAdapter`

◆ ◆ ◆ 第 22 章

22 MySQL

MySQL リソースアダプタは、com.waveset.adapter.MySQLResourceAdapter クラスで定義されます。

アダプタの詳細

このアダプタを使用して、MySQL にログインするためのユーザーアカウントをサポートします。カスタムテーブルがある場合、リソースアダプタウィザードを使用してカスタム MySQL テーブルリソースを作成する方法については、第 10 章「データベーステーブル」を参照してください。

リソースを設定する際の注意事項

なし

Identity Manager のインストールに関する注意事項

MySQL リソースアダプタは、カスタムアダプタです。インストールプロセスを完了するには、次の手順を実行する必要があります。

▼ MySQL リソースアダプタをインストールする

1 このリソースを **Identity Manager** のリソースリストに追加するには、「管理するリソースの設定」ページの「カスタムリソース」セクションに次の値を追加してください。

```
com.waveset.adapter.MySQLResourceAdapter
```

2 **http://dev.mysql.com/downloads/#connector-j** にアクセスして、**Connector/J JDBC** ドライバの最新バージョンへのリンクを使用します。

3 ダウンロードしたファイルを解凍します。

4 `mysqlconnector-java-`*Version* `-bin.jar` ファイルを、*InstallDir*`\idm\WEB-INF\lib` ディレクトリにコピーします。

使用上の注意

Identity Manager は、「User Model」リソースパラメータに指定したユーザーのアカウントプロパティーに基づいて、新しいユーザーを作成します。ユーザーを作成するには、有効な値を指定する必要があります。

MySQL リソースアダプタは、MySQL のユーザーパスワードのみを更新できます。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は、SSL 経由の JDBC を使用して MySQL と通信します。

必要な管理特権

ユーザーを作成するためには、MySQL の root ユーザーであるか、GRANT 特権を持つ必要があります。ユーザーを削除するには、REVOKE 特権が必要です。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	なし
アカウントの名前の変更	なし
パススルー認証	なし
前アクションと後アクション	なし

機能	サポート状況
データ読み込みメソッド	■ リソースからインポート ■ 調整

アカウント属性

なし

リソースオブジェクトの管理

なし

アイデンティティーテンプレート

```
$accountId$
```

サンプルフォーム

なし

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

```
com.waveset.adapter.MySQLResourceAdapter
```

◆ ◆ ◆ 第 23 章

23 NetWare NDS

Identity Manager では、次の Novell 製品をサポートするアダプタを提供します。

- eDirectory を含む NetWare
- Novell SecretStore

NetWare NDS アダプタは、GroupWise アカウントもサポートします。

アダプタの詳細

次の表に、Novell アダプタの属性の概要を示します。

GUI 名	クラス名
NetWare NDS	`com.waveset.adapter.NDSResourceAdapter`
NetWare NDS with SecretStore	`com.waveset.adapter.NDSSecretStoreResourceAdapter`

リソースを設定する際の注意事項

ここでは、Identity Manager で使用する NetWare NDS リソースの次の設定手順を説明します。

- ゲートウェイロケーションのインストール手順
- ゲートウェイサービスアカウントの設定手順
- SecretStore 証明書の設定手順

ゲートウェイの場所

管理するドメインに接続できる任意の NDS クライアントに、Sun Identity Manager Gateway をインストールします。パススルー認証が有効である場合は、複数のゲートウェイをインストールするようにしてください。

ゲートウェイサービスアカウント

デフォルトでは、ゲートウェイサービスはローカルシステムアカウントとして実行されます。これは、「サービス」MMC スナップインで設定できます。

ゲートウェイをローカルシステム以外のアカウントとして実行する場合は、ゲートウェイサービスアカウントに「Act As Operating System」ユーザー権限と「走査チェックのバイパス」のユーザー権限が必要です。ゲートウェイは、パススルー認証や、特定の状況でのパスワードの変更およびリセットに、これらの権限を使用します。

前アクションおよび後アクションのスクリプトを実行するときに、ゲートウェイに「プロセスレベルトークンの置き換え」の権限が必要な場合があります。この権限は、ゲートウェイが別のユーザー (リソース管理ユーザーなど) としてスクリプトのサブプロセスを実行しようとする場合に必要です。この場合、ゲートウェイプロセスには、そのサブプロセスに関連付けられたデフォルトのトークンを置き換える権限が必要です。

この権限がない場合は、サブプロセスの作成中に次のエラーが返されることがあります。

```
"Error creating process: A required privilege is not held by the client"
```

「プロセスレベルトークンの置き換え」権限は、デフォルトのドメインコントローラのグループポリシーオブジェクトと、ワークステーションおよびサーバーのローカルセキュリティーポリシーで定義されます。この権限をシステムに設定するには、「管理ツール」フォルダの「ローカルセキュリティーポリシー」アプリケーションを開き、「ローカルポリシー」>「ユーザー権利の割り当て」>「プロセスレベルトークンの置き換え」に移動します。

SecretStore 証明書

SecretStore をサポートするには、SSL 証明書を NDS システムから Identity Manager アプリケーションサーバーにエクスポートする必要があります。

この証明書を取得する方法の 1 つは、ConsoleOne を使用して公開鍵をエクスポートすることです。ConsoleOne を起動して、SSL CertificateDNS オブジェクトに移動します。SSL CertificateDNS オブジェクトの「プロパティー」ダイアログで、「証明書」タブの「公開鍵証明書」を選択します。「エクスポート」をクリックして、証明書のエクスポートプロセスを開始します。非公開鍵をエクスポートする必要はありません。このファイルを DER 形式で保存します。

DER ファイルを Identity Manager アプリケーションサーバーにコピーします。次に、keytool またはその他の証明書管理ツールを使用して、証明書を `jdk\jre\lib\security\cacerts` の鍵ファイルに追加します。keytool ユーティリティーは、Java SDK に付属しています。keytool ユーティリティーについては、Java のマニュアルを参照してください。

Identity Manager のインストールに関する注意事項

NetWare NDS アダプタに必要な追加のインストール手順はありません。

リソースリストに NDS SecretStore リソースを追加するには、次の手順を実行します。

▼ NDS SecretStore リソースをリソースリストに追加する

1. 「管理するリソースの設定」ページの「カスタムリソース」セクションに次の値を追加します。

   ```
   com.waveset.adapter.NDSSecretStoreResourceAdapter
   ```

2. `jsso.jar` ファイルを *InstallDir*`\idm\WEB-INF\lib` ディレクトリにコピーします。`jsso.jar` ファイルは、**Novell SecretStore** または **Novell SecureLogin** を含む **NDS** クライアントがインストールされている次のいずれかの場所から取得できます。

   - *NovellInstallDir*`\ConsoleOne\version\lib\SecretStore`
     - *NovellInstallDir*`\ConsoleOne\version\lib\security`

使用上の注意

ここでは、NetWare NDS リソースアダプタの使用に関連する情報を提供します。 次のトピックで構成されています。

その他

- Active Sync モードの NetWare NDS アダプタは、アカウントの削除を検出しません。このため、アカウントの削除を検出するように調整してください。

- NDS アダプタはテンプレートの値 (ユーザーの DS や FS の権限、ホームディレクトリ権限、新しいオブジェクトのトラスティーなど) をサポートします。
- 「リソース」ページ上の表示に関する問題を避けるには、「Identity Manager User Name Attribute」パラメータを cn に設定します。
- NDS では、名前のセグメントを指定する際にコンマではなくピリオドを使用します。コンマを指定した場合、Identity Manager がエラーメッセージを返します。
- NDS リソースを設定して、ユーザーのホームディレクトリを作成できるようにするには、アカウント属性に次の 2 つの属性を追加する必要があります。

  Home Directory (文字列)。この属性の形式は次のとおりです。

  VolumeDN#NameSpaceType#DirectoryPath

  次に例を示します。

  `SERVER_SYS.MYORG#0#\Homes\bob_smith`。

  `NameSpaceType` は、次のいずれかです。

  - 0 は DOS の名前空間を示します。
  - 1 は Macintosh の名前空間を示します。
  - 2 は UNIX または NFS の名前空間を示します。
  - 3 は FTAM の名前空間を示します。
  - 4 は OS/2、Windows 95、または Windows NT の名前空間を示します。

    Create Home Directory (Boolean)。この属性は実際のディレクトリを作成するかどうかを示すフラグの役割を果たします。このフラグを true に設定すると、ディレクトリが作成されます。

  NDS アダプタで次のエラーが発生する場合があります。

  ```
  NWDSAddSecurityEquiv: 0xFFFFFD9B (-613): ERR_SYNTAX_VIOLATION
  ```

  この場合は、HKEY_LOCAL_MACHINE\Software\Waveset\Lighthouse\Gateway の次のレジストリキーの値を増やす必要がある可能性があります。

  - `nds_method_retry_count` (デフォルトは 10)
  - `nds_method_retry_sleep_interval` (デフォルトは 1000 ミリ秒)

  NetWare API は、`getResourceObjects` FormUtil メソッドの `searchFilter` オプションと互換性がありません。
- NDS リソースに接続するアカウントが NDS の `loginMaximumSimultaneous` 属性によって制限されている場合は、**Connection Limit** リソースパラメータを、loginMaximumSimultaneous に指定された値以下に設定してください。

パススルー認証に関する注意事項

Identity Manager 8.0 より前のバージョンでパススルー認証を実装する場合、レジストリキーを編集して、パススルー認証を実行する専用の独立したリソースアダプタを作成する必要がありました。このアダプタは、固有のゲートウェイを通じて NetWare リソースと通信していました。

Identity Manager 8.0 では、NetWare リソースに対するパススルー認証を単一のリソースおよびゲートウェイで実行できるようになりました。8.0 より前のバージョンでパススルー認証を実装していた場合に、単一のリソースおよびゲートウェイを使用したいときは、次の手順を実行します。

▼ パススルー認証 (8.0 より前のバージョン) を実装する

1. **NDS** ログインモジュールグループからパススルー認証リソースを削除します。
2. パススルー認証リソースを **Identity Manager** から削除する場合は、先に **System Configuration** オブジェクトで共通リソース 属性を削除または変更します。

```
<Attribute name='common resources'>
   <Object>
      <Attribute name='NDS Group'>
         <List>
            <String>NDS_Resource_Host</String>
            <String>NDS_Passthrough_Host</String>
         </List>
      </Attribute>
   </Object>
</Attribute>
```

   NDS グループに NDS リソースおよびパススルー認証ホストだけが含まれる場合は、`Attribute` 要素全体を削除します。それ以外の場合は、パススルー認証ホストを定義する文字列を削除します。
3. 「リソース」ページからパススルー認証リソースを削除します。
4. パススルー認証ホストでゲートウェイが不要になった場合は、ゲートウェイサービスを無効にしてアプリケーションを削除することができます。

ゲートウェイタイムアウト

NetWare アダプタでは、`RA_HANGTIMEOUT` リソース属性を使用してタイムアウト値を秒数で指定できます。この属性は、ゲートウェイに対する要求がタイムアウトしてハングしているとみなされるまでの時間を制御します。

次のように、この属性を Resource オブジェクトに手動で追加する必要があります。

```
<ResourceAttribute name='Hang Timeout' displayName='com.waveset.adapter.
    RAMessages:RESATTR_HANGTIMEOUT' type='int'
    description='com.waveset.adapter.RAMessages:
    RESATTR_HANGTIMEOUT_HELP' value='NewValue'>
 </ResourceAttribute>
```

この属性のデフォルト値は 0 です。これは Identity Manager がハングした接続を確認しないことを表します。

GroupWise での NDS ユーザーの管理

GroupWise との統合が有効な場合は、NDS アダプタで NDS ユーザーの GroupWise 属性を管理できます。NDS アダプタは、GroupWise ポストオフィスの NDS ユーザーの追加と削除をサポートします。AccountID、GatewayAccess、DistributionLists などの、ほかの GroupWise アカウント属性を取得または変更することもできます。

GroupWise 統合の有効化

GroupWise との統合を有効にするには、GroupWise ドメイン DN リソース属性の値を定義してください。この値は、管理する GroupWise ドメインの DN を指定します。この属性の値の例を次に示します。

```
CN=gw_dom.ou=GroupWise.o=MyCorp
```

NDS ツリーリソース属性は、配下に GroupWise ドメインが存在すると予測される NDS ツリーを定義します。つまり、GroupWise ドメインは、アダプタが管理する NDS ユーザーと同じツリーに配置してください。

NDS ユーザーの GroupWise ポストオフィスの管理

アカウント属性 `GW_PostOffice` は、GroupWise ポストオフィスを表します。

NDS ユーザーを GroupWise ポストオフィスに追加するには、`GW_PostOffice` アカウント属性を、GroupWise ドメインに関連付けられた既存のポストオフィスの名前に設定します。

NDS ユーザーを別の GroupWise ポストオフィスに移動するには、`GW_PostOffice` アカウント属性を、GroupWise ドメインに関連付けられた新しいポストオフィスの名前に設定します。

NDS ユーザーをポストオフィスから削除するには、`GW_PostOffice` アカウント属性を GroupWise 削除パターンリソース属性と同じ値に設定します。GroupWise 削除パターンリソース属性のデフォルト値は *TRASH* です。

SecretStore および Identity Manager の System Configuration オブジェクト

デフォルトでは、SecretStore を含む NetWare NDS アダプタを使用してリソースオブジェクトを管理することはできません。この機能を有効にするには、System Configuration オブジェクトを編集してください。

次の行を見つけます。

```
<!-- form mappings -->
   <Attribute name='form'>
      <Object>
```

これらの行の直後に、次の行を追加します。

```
<!-- NetWare NDS with SecretStore -->
<Attribute name='NetWare NDS with SecretStore Create Group Form'
value='NetWare NDS Create Group Form'/>
<Attribute name='NetWare NDS with SecretStore Update Group Form'
value='NetWare NDS Update Group Form'/>
<Attribute name='NetWare NDS with SecretStore Create Organization Form'
value='NetWare NDS Create Organization Form'/>
<Attribute name='NetWare NDS with SecretStore Update Organization Form'
value='NetWare NDS Update Organization Form'/>
<Attribute name='NetWare NDS with SecretStore Create Organizational Unit Form'
   value='NetWare NDS Create Organizational Unit Form'/>
<Attribute name='NetWare NDS with SecretStore Update Organizational Unit Form'
   value='NetWare NDS Update Organizational Unit Form'/>
<Attribute name='NetWare NDS with SecretStore Create User Form'
value='NetWare NDS Create User Form'/>
<Attribute name='NetWare NDS with SecretStore Update User Form'
value='NetWare NDS Update User Form'/>
```

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

ゲートウェイサービスを使用して NetWare NDS のリソースに接続することをお勧めします。ゲートウェイサービスでは、ネットワーク上でパスワード情報を交換するために TCP/IP ソケット接続 (3 DES) が使用されます。

標準 LDAP または SSLP 上の LDAP を使用して NetWare NDS サーバーに接続することもできます。このシナリオでは、LDAP リソースアダプタを使用します。

必要な管理特権

Identity Manager の管理者には、NetWare ユーザーを作成するための適切な NDS 権限が必要です。デフォルトでは、NetWare 管理者は、ディレクトリおよび NetWare ファイルシステムのすべての権限を持っています。

パスワード管理を行うために、NDS 管理者は、次のプロパティーに対する比較、読み取り、および書き込みの権限を持っている必要があります。

- Group Membership
- Locked By Intruder
- Login Intruder Attempts
- Login Intruder Reset Time
- Password Management

NDS SecretStore を使用して機能を実行する Identity Manager の管理者アカウントを、SecretStore 管理者として定義する必要があります。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	使用可。ただし、NDS ユーザーも Group Wise アカウントを持っている場合は、名前変更がサポートされません。
パススルー認証	あり
前アクションと後アクション	なし
データ読み込みメソッド	■ リソースから直接インポート ■ リソースの調整 ■ Active Sync

アカウント属性

ここでは、NetWare NDS アカウント属性のサポートについて説明します。

- 255 ページの「属性構文のサポート」
- 256 ページの「アカウント属性のサポート」

属性の構文 (または型) は、通常、属性がサポートされるかどうかを決定します。一般に、Identity Manager は boolean 型、文字列型、および整数型の構文をサポートします。

SYN_CI_LIST 構文を持つ属性 (Language など) と SYN_PO_ADDRESS 構文を持つ属性 (Postal Address など) の値は、$ で区切られた文字列のリストにするようにしてください。SYN_OCTET_STRING 属性の値は、Base 64 でエンコードした、オクテットストリームのバイト文字列にしてください。

属性構文のサポート

次の「サポートされる構文」と「サポートされない構文」では、属性構文のサポートについて説明します。

サポートされる構文

次の表に、サポートされる属性構文に関する情報を示します。

NDS 構文	属性タイプ	オブジェクト ID	構文 ID
Boolean	Boolean	1.3.6.1.4.1.1466.115.121.1.7	SYN_BOOLEAN
Case Exact String	String	1.3.6.1.4.1.1466.115.121.1.26	SYN_CE_STRING
		2.16.840.1.113719.1.1.5.1.2	
Case Ignore List	String	2.16.840.1.113719.1.1.5.1.6	SYN_CI_LIST
Case Ignore String	String	1.3.6.1.4.1.1466.115.121.1.15	SYN_CI_STRING
Class Name	String	1.3.6.1.4.1.1466.115.121.1.38	SYN_CLASS_NAME
Counter	Int	2.16.840.1.113719.1.1.5.1.22	SYN_COUNTER
Distinguished Name	String	1.3.6.1.4.1.1466.115.121.1.12	SYN_DIST_NAME
Fax Number	String	1.3.6.1.4.1.1466.115.121.1.22	SYN_FAX_NUMBER
Integer	Int	1.3.6.1.4.1.1466.115.121.1.27	SYN_INTEGER
Interval	Int	1.3.6.1.4.1.1466.115.121.1.27	SYN_INTERVAL
Numeric String	String	1.3.6.1.4.1.1466.115.121.1.36	SYN_NU_STRING
Octet String	String	1.3.6.1.4.1.1466.115.121.1.40	SYN_OCTET_STRING
Path	String	2.16.840.1.113719.1.1.5.1.15	SYN_PATH
Postal Address	String	1.3.6.1.4.1.1466.115.121.1.41	SYN_PO_ADDRESS
Printable String	String	1.3.6.1.4.1.1466.115.121.1.44	SYN_PR_STRING
Stream	String	1.3.6.1.4.1.1466.115.121.1.5	SYN_STREAM
Telephone Number	String	1.3.6.1.4.1.1466.115.121.1.50	SYN_TEL_NUMBER

NDS 構文	属性タイプ	オブジェクト ID	構文 ID
Time	Int	1.3.6.1.4.1.1466.115.121.1.24	SYN_TIME

サポートされない構文

次の表に、サポートされない構文に関する情報を示します。

NDS 構文	オブジェクト ID	構文 ID
Back Link	2.16.840.1.113719.1.1.5.1.23	SYN_BACK_LINK
EMail Address	2.16.840.1.113719.1.1.5.1.14	SYN_EMAIL_ADDRESS
Hold	2.16.840.1.113719.1.1.5.1.26	SYN_HOLD
Net Address	2.16.840.1.113719.1.1.5.1.12	SYN_NET_ADDRESS
Object ACL	2.16.840.1.113719.1.1.5.1.17	SYN_OBJECT_ACL
Octet List	2.16.840.1.113719.1.1.5.1.13	SYN_OCTET_LIST
Replica Pointer	2.16.840.1.113719.1.1.5.1.16	SYN_REPLICA_POINTER
Timestamp	2.16.840.1.113719.1.1.5.1.19	SYN_TIMESTAMP
Typed Name	2.16.840.1.113719.1.1.5.1.25	SYN_TYPED_NAME
Unknown	2.16.840.1.113719.1.1.5.1.0	SYN_UNKNOWN

アカウント属性のサポート

次の「サポートされるアカウント属性」と「サポートされないアカウント属性」では、属性のサポートについて説明します。

サポートされるアカウント属性

次の属性は、NDS リソースアダプタの「アカウント属性」ページに表示されます。

リソースユーザー属性	NDS 構文	属性タイプ	説明
Create Home Directory	Boolean	Boolean	ユーザーのホームディレクトリを作成するかどうかを示します。Home Directory パラメータを設定してください。
説明	Case Ignore String	String	ユーザーについて説明するテキスト。

リソースユーザー属性	NDS 構文	属性タイプ	説明
Facsimile Telephone Number	Facsimile Telephone Number	String	電話番号および (オプションで) ユーザーに関連するファクシミリ端末用のパラメータ。
Full Name	Case Ignore String	String	ユーザーのフルネーム。
Generational Qualifier	Case Ignore String	String	世代を示します。たとえば、Jr. や II)。
Given Name	Case Ignore String	String	ユーザーの名。
Group Membership	Distinguished Name	String	ユーザーが属するグループのリスト。
GW_AccountID	適用不可	String	GroupWise アカウンティングの「ユーザー情報」フィールドに指定するアカウント ID。
GW_DistributionLists	適用不可	String	ユーザーがメンバーになっている配布リスト。値は、有効な配布リストの識別名 (DN) にしてください。
GW_GatewayAccess	適用不可	String	GroupWise ゲートウェイへのアクセスを制限します。このフィールドが適用されるかどうかについては、使用しているゲートウェイのマニュアルを参照してください。
GW_Name	適用不可	String	GroupWise のメールボックス名。
GW_PostOffice	適用不可	String	GroupWise ドメインに関連付けられた既存のポストオフィスの名前。
Home Directory	Path	String	クライアントの現在の作業ディレクトリの場所。詳細は、「使用上の注意」を参照してください。
Initials	Case Ignore String	String	ユーザーのミドルネームのイニシャル。
Internet EMail Address	Case Ignore String	String	インターネット電子メールアドレスを指定します。
L	Case Ignore String	String	物理的または地理的な場所。
Locked By Intruder	Boolean	Boolean	ログイン試行の失敗回数が多過ぎたためにアカウントがロックされたことを示します。

リソースユーザー属性	NDS 構文	属性タイプ	説明
Login Grace Limit	Integer	Int	(古いパスワードの期限が切れたあとで) 古いパスワードを使用してそのアカウントにアクセスできる合計回数。
Login Maximum Simultaneous	Integer	Int	1 人のユーザーが同時に起動できる、認証されたログインセッションの数。
ou	Case Ignore String	String	組織単位の名前。
Password Allow Change	Boolean	Boolean	ユーザーがあるアカウントでログインしたときに、そのアカウントのパスワードを変更できるかどうかを決定します。
Password Expiration Interval	Interval	Int	パスワードがアクティブになっている期間。
Password Required	Boolean	Boolean	ユーザーがログインするにはパスワードが必要であることを設定します。
Password Unique Required	Boolean	Boolean	ユーザーパスワードを変更するときに、Passwords Used 属性に含まれるパスワードとは異なるパスワードを指定しなければならないことを設定します。
Surname	Case Ignore String	String	必須。個人が親から受け継ぎ (または結婚によって変更し)、一般に知られている名前。
Telephone Number	Telephone Number	String	ユーザーの電話番号。
タイトル	Case Ignore String	String	組織内部でユーザーに与えられた役職または職務。
userPassword	なし	暗号化されています	必須。ユーザーのパスワード。

次の表に、NDS User オブジェクトクラスで定義される追加のサポート対象属性の一覧を示します。

リソースユーザー属性	NDS 構文	属性タイプ	説明
Account Balance	Counter	Int	ユーザーがネットワークサービス (接続時間など) を購入するために持っているクレジット額。
Allow Unlimited Credit	Boolean	Boolean	ネットワークサービスを使用するために無制限のクレジット額をユーザーアカウントが持っているかどうかを示します。
audio	Octet String	String	バイナリ形式のオーディオファイル。
businessCategory	Case Ignore String	String	組織で実施されているビジネスの種類を示します。
carLicense	Case Ignore String	String	自動車の登録番号 (ナンバープレート)
departmentNumber	Case Ignore String	String	組織内の部署を特定します
displayName	Case Ignore String	String	管理者画面に表示される名前。
Employee ID	Case Ignore String	String	組織内の従業員を数値で示します
employeeType	Case Ignore String	String	従業員、契約社員などの雇用形態
Entrust:User	Case Exact String	String	Entrust ユーザーを指定します。
Higher Privileges	Distinguished Name	String	セキュリティーアクセス特権の代替セット。
homePhone	Telephone Number	String	ユーザーの自宅電話番号。
homePostalAddress	Postal Address	String	ユーザーの自宅住所。
jpegPhoto	Octet String	String	ユーザーの写真を格納している JPEG ファイル
labeledUri	Case Ignore String	String	ユーザーの URI (Uniform Resource Identifier)。
Language	Case Ignore List	String	言語の順序付けられたリスト
Last Login Time	Time	String	現在のセッションの直前のセッションのログイン日時。
ldapPhoto	Octet String	String	バイナリ形式のオブジェクトの写真。
Login Allowed Time Map	Octet String	String	アカウントに対して曜日ごとに 1 時間半の精度で許可されたログイン時間枠。

リソースユーザー属性	NDS 構文	属性タイプ	説明
Login Disabled	Boolean	Int	アカウントが無効になったことをユーザーに通知します。
Login Expiration Time	Time	String	クライアントが以降のログインをできなくなる日時。
Login Grace Remaining	Counter	Int	アカウントがロックされる前に許可される猶予ログインの回数。
Login Intruder Attempts	Counter	Int	現在の間隔内で発生したログイン試行の失敗回数。
Login Intruder Reset Time	Time	String	Intruder Attempts 変数が次にリセットされる時刻。
Login Script	Stream	String	ユーザーのログインスクリプト。
Login Time	Time	String	現在のセッションのログイン時刻。
manager	Distinguished Name	String	ユーザーのスーパーバイザ。
Minimum Account Balance	Integer	Int	指定されたサービスを利用するためにユーザーが自分のアカウントに持っている必要がある最小クレジット額 (または金額)。
mobile	Telephone Number	String	ユーザーの携帯電話番号。
NDSPKI:Keystore	Octet String	String	ラップされた非公開鍵が含まれています。
NRD:Registry Data	Stream	String	NetWare レジストリデータベース
NRD:Registry Index	Stream	String	NetWare レジストリデータベースのインデックス
pager	Telephone Number	String	ユーザーのポケットベル番号。
Password Expiration Time	Time	String	パスワードの期限が切れる日時を指定します。
preferredLanguage	Case Ignore String	String	ユーザーが読み書きする言語に関する設定。
Print Job Configuration	Stream	String	指定された印刷ジョブ設定に関する情報が含まれています。
Printer Control	Stream	String	DOS プリンタ定義ファイル (NET$PRN.DAT) に対する NDS の対応部分。

リソースユーザー属性	NDS 構文	属性タイプ	説明
Profile	Distinguished Name	String	ユーザーがログイン時にプロファイルを指定しなかった場合のログインプロファイル。
Profile Membership	Distinguished Name	String	オブジェクトが使用できるプロファイルのリスト。
Public Key	Octet String	String	認証された RSA 公開鍵
roomNumber	Case Ignore String	String	ユーザーのオフィスまたは部屋の番号。
secretary	Distinguished Name	String	ユーザーの管理補佐。
Security Equals	Distinguished Name	String	ユーザーのグループメンバーシップおよびセキュリティー等価を指定します。
Security Flags	Integer	Int	オブジェクトの NCP パケットシグニチャーレベル。
Timezone	Octet String	String	ユーザーのタイムゾーンオフセット。
UID (User ID)	Integer	Int	UNIX クライアントによって使用される一意のユーザー ID。
userCertificate	Octet String	String	証明書管理の証明書。
userSMIMECertificate	Octet String	String	Netscape Communicator の S/MIME に対応するユーザーの証明書。
x500UniqueIdentifier	Octet String	String	DN が再利用された場合のユーザーの識別に使用される識別子。

サポートされないアカウント属性

次のアカウント属性はサポートされません。

- Login Intruder Address
- Network Address
- Network Address Restriction
- Passwords Used
- Print Job Configuration
- Printer Control
- Private Key
- Server Holds
- Type Creator Map

リソースオブジェクトの管理

Identity Manager は、デフォルトで次の NetWare NDS オブジェクトをサポートします。文字列ベース、整数ベース、またはブールベースの属性も管理できます。

リソースオブジェクト	サポートされる機能	管理される属性
Group	作成、更新、削除	L、OU、O、CN、Description、Member、Owner
Organizational Unit	作成、更新、削除	OU、Description、L、Facsimile Telephone Number、Telephone Number
組織	作成、更新、削除	dn、O、Description、L、Facsimile Telephone Number、Telephone Number

アイデンティティーテンプレート

デフォルトのアイデンティティーテンプレートは次のとおりです。

```
CN=$accountId$.O=MYORG
```

デフォルトのテンプレートを有効な値で置き換えてください。

サンプルフォーム

ここでは、このリソースアダプタで利用できるサンプルフォームの一覧を示します。

組み込みのフォーム

Identity Manager には、次のフォームが組み込まれています。

- NDS Group Create Form
- NDS Group Update Form
- NDS Create Organizational Unit Form
- NDS Update Organizational Unit Form
- DS Create Organization Form
- NDS Update Organization Form

その他の利用可能なフォーム

`NDSUserForm.xml` フォームも使用できます。

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

- `com.waveset.adapter.NDSResourceAdapter`
- `com.waveset.adapter.NDSSecretStoreResourceAdapter`
- `com.waveset.adapter.AgentResourceAdapter`

Sun Identity Manager Gateway を介した NDS へのアクセスをシングルスレッド化または直列化するには、ゲートウェイマシンの `HKEY_LOCAL_MACHINE\SOFTWARE\Waveset\Lighthouse\Gateway` ノードに次のレジストリキーと値を設定します。

名前	種類	データ
`ExclusiveNDSContext`	REG_DWORD	■ 0: この機能を無効にします。コンテキストがマルチスレッド化されます。 ■ 1: コンテキストがシングルスレッド化されます。

ゲートウェイへの接続の問題を診断するために、次のメソッドでトレースを有効にすることもできます。

- `com.waveset.adapter.AgentResourceAdapter#sendRequest`
- `com.waveset.adapter.AgentResourceAdapter#getResponse`

◆ ◆ ◆ 第 24 章

24 Oracle

Oracle リソースアダプタは、com.waveset.adapter.OracleResourceAdapter クラスで定義されます。

注 – Identity Manager は、Oracle E-Business Suite (EBS) をサポートする Oracle ERP リソースアダプタも提供します。このアダプタの詳細は、第 25 章「Oracle ERP」 を参照してください。

このアダプタを使用して、Oracle にログインするためのユーザーアカウントをサポートします。カスタム Oracle テーブルがある場合、リソースアダプタウィザードを使用してカスタム Oracle テーブルリソースを作成する方法については、第 10 章「データベーステーブル」 を参照してください。

アダプタの詳細

リソースを設定する際の注意事項

なし

Identity Manager のインストールに関する注意事項

Oracle リソースアダプタは、カスタムアダプタです。インストールプロセスを完了するには、次の手順を実行する必要があります。

▼ Oracle リソースアダプタをインストールする

1 **Oracle** リソースを **Identity Manager** のリソースリストに追加するには、「管理するリソースの設定」ページの「カスタムリソース」セクションに次の値を追加する必要があります。

```
com.waveset.adapter.OracleResourceAdapter
```

2 **thin** ドライバを使用して **Oracle Real Application Cluster (RAC)** に接続する場合は、「リソースパラメータ」ページの「接続 **URL**」に、次の形式で値を指定します。

```
jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=on)
(ADDRESS=(PROTOCOL=TCP)(HOST=host01)(PORT=1521))
(ADDRESS=(PROTOCOL=TCP)(HOST=host02)(PORT=1521))
(ADDRESS=(PROTOCOL=TCP)(HOST=host03)(PORT=1521))
(CONNECT_DATA=(SERVICE_NAME=PROD)))
```

3 **Oracle Real Application Cluster** を使用しない環境で **JDBC thin** ドライバを使用する場合は、**JDBC thin** ドライバクラスが含まれる **JAR** ファイルを `$WSHOME$/WEB-INF/lib` ディレクトリにコピーします。**JAR** ファイルは、使用しているアプリケーションサーバーの **JDK** バージョンと互換性がある必要があります。

4 ほかのドライバを使用する場合は、「リソースパラメータ」ページにドライバと接続 **URL** を指定します。

使用上の注意

ここでは、ユーザータイプとカスケード削除に関する情報も含め、Oracle リソースアダプタの使用に関する依存関係と制限事項について説明します。

ユーザータイプ

Oracle データベースでは、次のタイプのユーザーが許可されます。

- 「ローカル」。ローカルユーザーは、Oracle によって完全に管理され、パスワードが必要です。Oracle は、これらのパスワードも管理します。このため、ユーザー名とパスワードは、アプリケーションの内部で設定された標準に完全に準拠させてください。
- 外部。外部ユーザーは、オペレーティングシステムまたは他社製のアプリケーションによって認証されます。Oracle は、ログイン認証を利用して、特定のオペレーティングシステムのユーザーが特定のデータベースユーザーにアクセスできることを確認します。

- グローバル。グローバルユーザーは、LDAP や Active Directory などのディレクトリサービスによって認証されます。ユーザーの名前は、完全な識別名 (DN) または NULL 文字列として指定してください。NULL 文字列を使用すると、ディレクトリサービスは認証されたグローバルユーザーを該当するデータベース機能にマップします。

外部ユーザーまたはグローバルユーザーを管理している場合は、Oracle リソースをそのインストール先であるマシンまたはディレクトリサービスも含むリソースグループに配置するようにしてください。

カスケード削除

noCascade アカウント属性は、ユーザーを削除したときにカスケード削除を行うかどうかを示します。デフォルトでは、カスケード削除が行われます。カスケード削除を無効にするには、次の手順に従います。

▼ カスケード削除を無効にする

1 **System Configuration** オブジェクトの updatableAttributes セクションに次のエントリを追加します。

```
<Attribute name='Delete'>
   <Object>
      <Attribute name='all'>
         <List>
            <String>noCascade</String>
         </List>
      </Attribute>
   </Object>
</Attribute>
```

2 プロビジョニング解除フォームに次のフィールドを追加します。

```
<Field name='resourceAccounts.currentResourceAccounts
[MyOracleResource].attributes.noCascade'>
   <Display class='Checkbox'>
      <Property name='title' value='Do NOT Cascade MyOracleResource Delete'/>
      <Property name='alignment' value='left'/>
   </Display>
   <Disable>
      <isnull>
         <ref>resourceAccounts.currentResourceAccounts[MyOracleResource]</ref>
      </isnull>
   </Disable>
</Field>
```

3 **Oracle** リソーススキーマに noCascade アカウント属性を追加します。
ユーザーがオブジェクトを所有していて、カスケードを無効にするオプションを選択した場合、Oracle はエラーをスローします。ユーザーは削除されません。

4 属性を無効にできるように、ユーザーフォームに noCascade フィールドを追加します。たとえば、次のようにします。

```
<Field name='global.noCascade'>
   <Disable>
      <s>TRUE</s>
   </Disable>
</Field>
```

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は、次のいずれかのドライバを使用して Oracle アダプタと通信できます。

- JDBC thin ドライバ
- JDBC OCI ドライバ
- 他社製のドライバ

必要な管理特権

管理者は、Oracle ユーザーを作成するために、CREATE USER、ALTER USER、および DROP USER システム特権を持っている必要があります。

Oracle および Oracle アプリケーションについては、管理者に次のデータベースビューの SELECT アクセス権を付与してください。

- DBA_PROFILES
- DBA_ROLE_PRIVS
- DBA_SYS_PRIVS
- DBA_TABLESPACES
- DBA_TS_QUOTAS
- DBA_USERS

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	なし
パススルー認証	あり
前アクションと後アクション	なし
データ読み込みメソッド	リソースから直接インポート

アカウント属性

次の表に、Oracle データベースユーザーのアカウント属性を示します。属性の型はすべて String です。すべての属性が省略可能です。

リソースユーザー属性	説明
noCascade	ユーザーのカスケード削除を行うかどうかを示します。
oracleAuthentication	次のいずれかの値にしてください。 ■ LOCAL (デフォルト値) ■ EXTERNAL ■ GLOBAL
oracleDefaultTS	ユーザーが作成するオブジェクトのデフォルトのテーブルスペースの名前。
oracleDefaultTSQuota	ユーザーが割り当てることができるデフォルトのテーブルスペースの最大サイズ。
oracleGlobalName	ユーザーのグローバル名。oracleAuthentication が GLOBAL に設定されている場合にのみ適用されます。
expirePassword	この属性は、ローカル Oracle アカウントにのみ適用されます。
oraclePrivs	ユーザーに割り当てられた 1 つ以上の特権。
oracleProfile	ユーザーに割り当てられた 1 つ以上のプロファイル。
oracleRoles	ユーザーに割り当てられた 1 つ以上のロール。
oracleTempTS	ユーザーの一時セグメントに対応するテーブルスペースの名前。

リソースユーザー属性	説明
oracleTempTSQuota	ユーザーが割り当てることができる一時テーブルスペースの最大サイズ。属性がスキーママップに表示されている場合、一時テーブルスペースに割り当て制限が常に設定されます。属性がスキーママップから削除された場合、一時テーブルスペースに割り当て制限が設定されません。Oracle 10gR2 リソースと通信するアダプタでは、属性を削除する必要があります。

リソースオブジェクトの管理

なし

アイデンティティーテンプレート

```
$accountId$
```

サンプルフォーム

組み込みのフォーム

なし

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

- com.waveset.adapter.OracleResourceAdapter
- com.waveset.adapter.JdbcResourceAdapter

◆ ◆ ◆ 第 25 章

Oracle ERP

Oracle ERP リソースアダプタは、com.waveset.adapter.OracleERPResourceAdapter クラスで定義されます。このアダプタは、Oracle E-Business Suite (EBS) をサポートします。

注 – Identity Manager は、Oracle データベースをサポートする Oracle リソースアダプタも提供します。このアダプタについては、第 24 章「Oracle」を参照してください。

アダプタの詳細

リソースを設定する際の注意事項

なし

Identity Manager のインストールに関する注意事項

Oracle ERP リソースアダプタは、カスタムアダプタです。インストールプロセスを完了するには、次の手順を実行する必要があります。

▼ Oracle ERP リソースアダプタをインストールする

1 Oracle リソースを Identity Manager のリソースリストに追加するには、「管理するリソースの設定」ページの「カスタムリソース」セクションに次の値を追加する必要があります。

```
com.waveset.adapter.OracleERPResourceAdapter
```

2 **thin** ドライバを使用して **Oracle Real Application Cluster (RAC)** に接続する場合は、「リソースパラメータ」ページの「接続 **URL**」に、次の形式で値を指定します。

```
jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=on)
(ADDRESS=(PROTOCOL=TCP)(HOST=host01)(PORT=1521))
(ADDRESS=(PROTOCOL=TCP)(HOST=host02)(PORT=1521))
(ADDRESS=(PROTOCOL=TCP)(HOST=host03)(PORT=1521))
(CONNECT_DATA=(SERVICE_NAME=PROD)))
```

3 **Oracle Real Application Cluster** を使用しない環境で **JDBC thin** ドライバを使用する場合は、**JDBC thin** ドライバクラスが含まれる **JAR** ファイルを `$WSHOME$/WEB-INF/lib` ディレクトリにコピーします。**JAR** ファイルは、使用しているアプリケーションサーバーの **JDK** バージョンと互換性がある必要があります。

4 ほかのドライバを使用する場合は、「リソースパラメータ」ページにドライバと接続 **URL** を指定します。

Oracle ERP アダプタは、ほかの変更を必要とせずに、Oracle E-Business Suite (EBS) バージョン 11.5.9 をサポートします。ただし、EBS バージョン 11.5.10 および 12 をサポートするには、次の変更が必要です。

5 スキーママップから `responsibilities` アカウント属性を削除し、`directResponsibilities` 属性と `indirectResponsibilities` 属性を追加します。

6 次のプロパティーを **Oracle ERP** ユーザーフォームの **FormRef** 属性に追加します。

- RESOURCE_NAME。ERP リソース名を指定します。
  - VERSION。ERP リソースのバージョンを指定します。使用できる値は、11.5.9、11.5.10、12 です。
  - RESP_DESCR_COL_EXISTS。fnd_user_resp_groups_direct テーブルに、説明の列が存在するかどうかを定義します。このプロパティーは、バージョンが 11.5.10 または 12 の場合に必要です。指定できる値は TRUE と FALSE です。

    たとえば Tabbed User Form は、EBS バージョン 12 をサポートするために次のような方法で変更する必要の可能性があります。

```
<FormRef name='Oracle ERP User Form'>
   <Property name='RESOURCE_NAME' value='Oracle ERP R12'/>
   <Property name='VERSION' value='12'/>
   <Property name='RESP_DESCR_COL_EXISTS' value='TRUE'/>
</FormRef>
```

使用上の注意

ここでは、Oracle ERP アダプタに適用できる次のリソースパラメータについて説明します。

Oracle アプリケーションのユーザー管理セキュリティー

ユーザーのセキュリティーは、Oracle アプリケーション内部の次の 3 レベルで制御されます。

- 機能的セキュリティー。システム内部の個々のメニューおよびメニューオプションへのユーザーアクセス特権を制御します。
- データセキュリティー。ユーザーが操作できるデータオブジェクトを制御します。
- ロールに基づくアクセス制御 (RBAC)。ロールを作成し、ロールに対して責任とアクセス権を割り当てることができます。

Oracle ERP アダプタは、機能的セキュリティーのみをサポートします。このため、このアダプタでは Oracle のデータオブジェクト、オブジェクトインスタンス、インスタンスセットの作成、更新、削除を一覧表示することはできません。また、ロールオブジェクト、ロール階層、またはロールカテゴリも作成および管理できません。

Oracle クライアント暗号化タイプ

このパラメータには、Oracle がサポートする有効な暗号化アルゴリズム名 (RC4_56、RC4_128 など) のリストを指定します。このリストが空の場合、そのリリースで Oracle がサポートするすべてのアルゴリズムが使用されます。クライアント/サーバーは、Oracle クライアント暗号化レベルの設定に従って、これらのうちどのアルゴリズムを使用するかについてネゴシエーションを行います。

注 – このタイプの暗号化をサポートするように Oracle サーバーも設定してください。

サポートされるアルゴリズムについては、『Oracle Advanced Security 管理者ガイド』を参照してください。thin JDBC クライアント用の有効な値のリストについては、「SQLNET.ENCRYPTION_TYPES_CLIENT」セクションを参照してください。

Oracle クライアント暗号化レベル

この値は、サーバー/クライアントがネゴシエーションを行って適用するセキュリティーのレベルを決定します。デフォルト値 (空白のままの場合) は、ACCEPTED で

す。有効な値は、REJECTED、ACCEPTED、REQUESTED、および REQUIRED です。このパラメータの使用法については、『Oracle Advanced Security 管理者ガイド』および SQLNET.ENCRYPTION_CLIENT の値を参照してください。

また、このタイプの暗号化をサポートするように Oracle サーバーを設定してください。

Oracle E-Business Suite (EBS) 管理ユーザー責任

この値は、Identity Manager Oracle EBS 管理ユーザーが EBS アプリケーションの初期化ルーチンを呼び出すために使用する EBS 責任を決定します。有効な責任のリストは、`fnd_responsibility_vl` テーブルにあります。詳細については、Oracle EBS のマニュアルも参照してください。

Identity Manager Oracle EBS 管理ユーザーが有効な EBS システムアカウントを持ち、このパラメータの値と一致する責任を持っている場合は、接続中に作成された Oracle セッションで Oracle EBS の監査メカニズムを使用してユーザーのアクションが監査されます。たとえば、`fnd_user` テーブルオブジェクトの `created_by` フィールドと `last_updated_by` フィールドは、Identity Manager Oracle EBS 管理ユーザーのユーザー ID で正しく更新されます。

セキュリティー設定属性の追加

`securingAttrs` アカウント属性は、Oracle E-business Suite のセキュリティー設定属性機能をサポートします。Identity Manager の「ユーザーの作成」ページでセキュリティー設定属性を設定するには、次の手順を実行します。

▼ セキュリティー設定属性を「ユーザーの作成」ページで設定する

1. 「**Add Securing Attribute**」チェックボックスを選択します。
2. 「**Enter Securing Attribute Search Pattern**」テキストボックスに、使用可能な属性の選択肢を絞り込むための検索パターンを入力します。ワイルドカードとして「**%**」を使用します。次に、「**Load Securing Attributes**」ボタンをクリックします。これで「**Oracle Securing Attributes**」選択ボックスに属性が読み込まれます。
3. ドロップダウンメニューから属性を選択すると、その属性が「**Securing Attributes**」テーブルに追加されます。

   テーブルから削除する属性を選択して「Remove Selected Securing Attribute」ボタンをクリックすることにより、セキュリティー設定属性を削除できます。

ユーザーの有効化

Oracle EBS ユーザーを有効にするには、owner 属性の値を指定する必要があります。有効化フォームに特定の値が追加されて有効化ビューを介して送信されないかぎり、デフォルトで値 CUST が使用されます。次のコーディング例では、デフォルトの所有者を MYOWNER に変更しています。

```
<Field name='resourceAccounts.currentResourceAccounts[MyOracleERP].
attributes.owner' type='string'>
   <Display class='Text'>
      <Property name='title' value='Owner'/>
   </Display>
   <Default>
      <s>MYOWNER</s>
   </Default>
</Field>
```

ユーザー責任の取得

listResourceObjects の呼び出しを使用して、ユーザーの責任およびその他の Oracle EBS オブジェクトを取得できます。次の表に、サポートされるオブジェクトタイプに関する情報を示します。

Object	サポートされるオプション	Comments
auditorResps	id、activeRespsOnly	ユーザーの監査責任のリストを返します。 id は、そのリソース ID の責任が返されることを示す文字列です。 activeRespsOnly を true に設定すると、アクティブな責任のみが返されます。デフォルトは false です。
responsibilities	id、activeRespsOnly	ユーザーの責任を返します。11.5.9 でのみ有効です。
directResponsibilities	id、activeRespsOnly	ユーザーの直接的な責任を返します。11.5.10 でのみ有効です。
indirectResponsibilities	id、activeRespsOnly	ユーザーの間接的な責任を返します。11.5.10 でのみ有効です。
responsibilityNames	なし	ユーザーに割り当てられた責任名のリストを返します。

Object	サポートされるオプション	Comments
applications	responsibilityName	責任名が指定されていない場合は、ユーザーに割り当てられたすべてのアプリケーションが返されます。
securityGroups	application	アプリケーションが指定されていない場合は、ユーザーに割り当てられたすべてのセキュリティーグループが返されます。
account	activeAccountsOnly	ユーザーのアカウントのリストを返します。true に設定すると、アクティブなアカウントのみが返されます。デフォルトは false です。
securingAttrs	searchPattern	指定された検索パターンと一致するセキュリティー設定属性のリストを返します。パターンが指定されなかった場合は、すべてのセキュリティー設定属性が返されます。

次のコーディング例では、ユーザーフォームにアクティブな責任を返すフィールドを追加しています。USER_NAME と RESOURCE_NAME を有効な値で置き換える必要があります。auditorResps は、responsibilities、directResponsibilities、または indirectResponsibilites で置き換えます。

```
<Field name='respNames' type='string'>
   <Display class='Text'>
      <Property name='title' value='Oracle ERP Responsibilities'/>
   </Display>
   <Expansion>
      <invoke name='listResourceObjects' class='com.waveset.ui.FormUtil'>
         <ref>display.session</ref>
         <s>auditorResps</s>
         <s>RESOURCE_NAME</s>
         <map>
            <s>id</s>
            <s>USER_NAME</s>
            <s>activeRespsOnly</s>
            <s>true</s>
            <s>attrsToGet</s>
            <list>
               <s>name</s>
            </list>
         </map>
         <s>null</s>
```

```
      </invoke>
   </Expansion>
</Field>
```

責任の監査

ユーザーに割り当てられた責任のサブ項目 (フォームや機能) を監視するには、auditorObject をスキーママップに追加します。auditorObject は、responsibility オブジェクトのセットを含む複雑な属性です。次の属性は、常に責任オブジェクトに返されます。

- responsibility
- userMenuNames
- menuIds
- userFunctionNames
- functionIds
- formIds
- formNames
- userFormNames
- readOnlyFormIds
- readWriteOnlyFormIds
- readOnlyFormNames
- readOnlyUserFormNames
- readWriteOnlyFormNames
- readWriteOnlyUserFormNames
- functionNames
- readOnlyFunctionNames
- readWriteOnlyFunctionNames

注 – readOnly 属性と ReadWrite 属性は、fnd_form_functions テーブルの PARAMETERS 列で次のいずれかのクエリーを行うことによって識別します。

- QUERY_ONLY=YES
- QUERY_ONLY="YES"
- QUERY_ONLY = YES
- QUERY_ONLY = "YES"
- QUERY_ONLY=Y
- QUERY_ONLY="Y"
- QUERY_ONLY = Y
- QUERY_ONLY = "Y"

「SOB または組織、あるいはその両方を返す」リソースパラメータを TRUE に設定すると、次の属性も返されます。

- setOfBooksName
- setOfBooksId
- organizationalUnitName
- organizationalUnitId

responsibility、setOfBooksName、setOfBooksId、organizationalUnitId、および organizationalUnitName 属性を除いて、属性名はスキーママップに追加されるアカウント属性名に一致します。アカウント属性には、ユーザーに割り当てられる値の集合が含まれます。responsibility オブジェクトに含まれている属性は、その責任に固有のものです。

auditorResps[] ビューは、responsibility 属性へのアクセスを提供します。次に示すフォームの部分は、ユーザーに割り当てられたすべてのアクティブな責任 (およびそれらの属性) を返します。

```
<defvar name='audObj'>
   <invoke name='get'>
      <ref>accounts[Oracle ERP 11i VIS].auditorObject</ref>
   </invoke>
</defvar>
<!-- this returns list of responsibility objects -->
<defvar name='respList'>
   <invoke name='get'>
      <ref>audObj</ref>
      <s>auditorResps[*]</s>
   </invoke>
</defvar>
```

たとえば、次のようにします。

- auditorResps[0].responsibility は、最初の責任オブジェクトの名前を返しま

す。
- auditorResps[0].formNames は、最初の責任オブジェクトの formNames を返します。

リソースアクションの使用

Oracle ERP アダプタは、リソースアクションをサポートします。これらのアクションを有効にするには、Javascript または BeanShell で記述されたスクリプトを設定する必要があります。このアダプタは、次のプロビジョニングアクションの実行後または実行前に、これらのスクリプトを呼び出します。

- 279 ページの「create 前アクションと後アクション」
- 280 ページの「update 前アクションと後アクション」
- 281 ページの「delete 前アクションと後アクション」
- 282 ページの「enable 前アクションと後アクション」
- 283 ページの「disable 前アクションと後アクション」
- 283 ページの「getUser 後アクション」

どのアクションスクリプトも、java.util.Map クラスで定義されているように、actionContext マップを受け取ります。マップに格納できる内容は、アクションごとに異なります。

スクリプトは、それ自体に渡された JDBC 接続を閉じることはできません。アダプタが適切な時期に自動的に接続を閉じます。

リソースアクションの実装については、第 50 章「リソースへのアクションの追加」を参照してください。サンプルスクリプトは、$WSHOME/sample/OracleERPActions.xml にあります。

create 前アクションと後アクション

アクションに渡される actionContext マップには次のエントリが含まれます。

キー	値の型	値の説明
conn	java.sql.Connection	顧客のデータベースへの JDBC 接続
adapter	com.waveset.adapter.OracleERPResourceAdapter	アダプタインスタンス
action	java.lang.String	「createUser」という文字列
timing	java.lang.String	before または after である必要があります
id	java.lang.String	作成するユーザーのアカウント ID

キー	値の型	値の説明
password	java.lang.String	存在する場合、この値は、新しいユーザーの復号化されたパスワードです。
attributes	java.util.Map	新しいユーザーに設定する属性のマップ。 ■ キーは、設定する属性を識別します ■ 値は、その属性に設定する復号化された値を指定します。
errors	java.util.List	最初は、この値は空のリストです。 処理中にエラーが発生した場合、スクリプトによってこのリストに java.lang.String オブジェクトを追加できます。
trace	com.sun.idm.logging.trace.Trace	実行のトレースに使用されるオブジェクト スクリプトは、このクラスのメソッドを使用することで、顧客の環境でデバッグ可能なものとなります。

エラー処理

スクリプト内から例外がスローされた場合は、失敗とみなされます。

スクリプトでエラーが発生した場合、スクリプトによって errors キーに適切な文字列を追加することもできます。errors リストに項目が存在する場合は、作成の失敗とみなされます。

update 前アクションと後アクション

アクションに渡される actionContext マップには次のエントリが含まれます。

キー	値の型	値の説明
conn	java.sql.Connection	データベースへの JDBC 接続
adapter	com.wavset.adapter.OracleERPResourceAdapter	アダプタインスタンス
action	java.lang.String	「updateUser」という文字列
timing	java.lang.String	before または after である必要があります
id	java.lang.String	更新するユーザーのアカウント ID。
password	java.lang.String	存在する場合、この値はユーザーの新しいパスワードの復号化された値です。

キー	値の型	値の説明
attributes	java.util.Map	既存のユーザーに設定する属性のマップ。 ■ キーは、設定する属性を識別します ■ 値は、その属性に設定する復号化された値です。 キーがない場合は、その属性が更新されないということです。
errors	java.util.List	最初は、この値は空のリストです。 処理中にエラーが発生した場合、スクリプトによってこのリストに java.lang.String オブジェクトを追加できます。
trace	com.sun.idm.logging.trace.Trace	実行のトレースに使用されるオブジェクト。 スクリプトは、このクラスのメソッドを使用することで、顧客の環境でデバッグ可能なものとなります。

エラー処理

スクリプト内から例外がスローされた場合は、失敗とみなされます。

スクリプトでエラーが発生した場合、スクリプトが errors キーに適切な文字列を追加することもできます。errors リストに項目が存在する場合は、更新の失敗とみなされます。

delete 前アクションと後アクション

アクションに渡される actionContext マップには次のエントリが含まれます。

キー	値の型	値の説明
conn	java.sql.Connection	データベースへの JDBC 接続
adapter	com.wavset.adapter.OracleERPResourceAdapter	アダプタインスタンス
action	java.lang.String	「deleteUser」という文字列
timing	java.lang.String	before または after である必要があります
id	java.lang.String	削除するユーザーのアカウント ID

キー	値の型	値の説明
errors	java.util.List	最初は、この値は空のリストです。 処理中にエラーが発生した場合、スクリプトによってこのリストに java.lang.String オブジェクトを追加できます。
trace	com.sun.idm.logging.trace.Trace	実行のトレースに使用されるオブジェクト。 スクリプトは、このクラスのメソッドを使用することで、顧客の環境でデバッグ可能なものとなります。

エラー処理

スクリプト内から例外がスローされた場合は、失敗とみなされます。

スクリプトでエラーが発生した場合、スクリプトによって errors キーに適切な文字列を追加できます。errors リストに項目が存在する場合は、削除の失敗とみなされます。

enable 前アクションと後アクション

アクションに渡される actionContext マップには次のエントリが含まれます。

キー	値の型	値の説明
conn	java.sql.Connection	データベースへの JDBC 接続
adapter	com.wavset.adapter.OracleERPResourceAdapter	アダプタインスタンス
action	java.lang.String	「enableUser」という文字列
timing	java.lang.String	before または after である必要があります
id	java.lang.String	無効にするユーザーアカウント ID
errors	java.util.List	最初は、この値は空のリストです。 処理中にエラーが発生した場合、スクリプトによってこのリストに java.lang.String オブジェクトを追加できます。
trace	com.sun.idm.logging.trace.Trace	実行のトレースに使用されるオブジェクト。 スクリプトは、このクラスのメソッドを使用することで、顧客の環境でデバッグ可能なものとなります。

エラー処理

スクリプト内から例外がスローされた場合は、失敗とみなされます。

スクリプトでエラーが発生した場合、スクリプトが errors キーに適切な文字列を追加することもできます。errors リストに項目が存在する場合は、失敗とみなされます。

disable 前アクションと後アクション

アクションに渡される actionContext マップには次のエントリが含まれます。

キー	値の型	値の説明
conn	java.sql.Connection	データベースへの JDBC 接続
adapter	com.wavset.adapter.OracleERP ResourceAdapter	アダプタインスタンス
action	java.lang.String	「disableUser」という文字列
timing	java.lang.String	before または after である必要があります
id	java.lang.String	無効にするユーザーアカウント ID
errors	java.util.List	最初は、この値は空のリストです。 処理中にエラーが発生した場合、スクリプトによってこのリストに java.lang.String オブジェクトを追加できます。
trace	com.sun.idm.logging.trace.Trace	実行のトレースに使用されるオブジェクト。 スクリプトは、このクラスのメソッドを使用することで、顧客の環境でデバッグ可能なものとなります。

エラー処理

スクリプト内から例外がスローされた場合は、失敗とみなされます。

スクリプトでエラーが発生した場合、スクリプトが errors キーに適切な文字列を追加することもできます。errors リストに項目が存在する場合は、失敗とみなされます。

getUser 後アクション

getUser アクションは、標準的なアダプタから取得されるカスタムアカウント属性だけでなく、追加のカスタムアカウント属性をデータベースから取得する必要がある

場合に便利です。このアクションを有効にするには、「GetUser After アクション」というラベルの付いたリソースパラメータを設定することにより、このリソースアクションの名前を指定します。

アクションに渡される actionContext マップには次のエントリが含まれます。

キー	値の型	値の説明
conn	java.sql.Connection	データベースへの JDBC 接続
adapter	com.wavset.adapter.OracleERP ResourceAdapter	アダプタインスタンス
action	java.lang.String	「getUser」という文字列
id	java.lang.String	取得するユーザーアカウント ID。
current 属性	java.util.Map	既存のユーザーに設定する属性のマップ。 ■ キーは、設定する属性を識別します ■ 値は、その属性に設定する復号化された値です。
changed 属性	java.util.Map	これは、空のマップとして渡されます。 スクリプトでは、次の目的のために、オプションでこのマップにデータを設定することができます。 ■ 新しいアカウント属性を Identity Manager のユーザービューに追加する場合、または ■ Identity Manager のユーザービューでアカウント属性の値を変更する場合 キーは、アカウント属性の名前 (スキーママップの右側で登録される) です。値は、アカウント属性に設定する値です。
errors	java.util.List	最初は、この値は空のリストです。 処理中にエラーが発生した場合、スクリプトによってこのリストに java.lang.String オブジェクトを追加できます。
trace	com.sun.idm.logging.trace.Trace	実行のトレースに使用されるオブジェクト。 スクリプトは、このクラスのメソッドを使用することで、顧客の環境でデバッグ可能なものとなります。

エラー処理

スクリプト内から例外がスローされた場合は、失敗とみなされます。

スクリプトでエラーが発生した場合、スクリプトによって errors キーに適切な文字列を追加できます。errors リストに項目が存在する場合は、取得の失敗とみなされます。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は、次のいずれかのドライバを使用して Oracle アダプタと通信できます。

- JDBC thin ドライバ
- JDBC OCI ドライバ
- 他社製のドライバ

Oracle アプリケーションのストアドプロシージャーでは、プロビジョニングで使用される一部のストアドプロシージャーに暗号化されていないパスワードを渡す必要があるため、Identity Manager と Oracle アプリケーションリソースの間に暗号化された通信を実装するようにしてください。

特定のバージョンの Oracle RDBMS およびドライバが提供する暗号化のサポートレベルを検証するには、Oracle のマニュアル『Oracle Advanced Security 管理者ガイド』および使用している JDBC ドライバのマニュアルをお読みください。

Oracle EBS のアクセス権

Oracle E-Business Suite では、次のテーブルとストアドプロシージャーに対するアクセス権が必要です。

注 – 管理者は、すべてのテーブルに対して select コマンドを実行できる必要があります。また、管理者は apps.fnd_user テーブルを更新できる必要があります。

テーブル	ストアドプロシージャー
apps.ak_attributes	apps.app_exception.raise_exception
apps.ak_attributes_tl	apps.fnd_global.apps_initialize
apps.ak_web_user_sec_attr_values	apps.fnd_global.user_id
apps.fnd_application	apps.fnd_message.get
apps.fnd_application_tl	apps.fnd_message.get_token
apps.fnd_application_vl	apps.fnd_message.set_name
apps.fnd_profile	apps.fnd_message.set_token
apps.fnd_responsibility	apps.fnd_profile.get
apps.fnd_responsibility_vl	apps.fnd_user_pkg.AddResp
apps.fnd_security_groups	apps.fnd_user_pkg.CreateUser
apps.fnd_security_groups_tl	apps.fnd_user_pkg.DisableUser
apps.fnd_security_groups_vl	apps.fnd_user_pkg.DelResp
apps.fnd_user	apps.fnd_user_pkg.UpdateUser
apps.fnd_user_resp_groups	apps.fnd_user_pkg.user_synch
apps.icx_parameters	apps.fnd_user_pkg.validatelogin
	apps.fnd_user_resp_groups_api.assignment_exists
	apps.fnd_user_resp_groups_api.insert_assignment
	apps.fnd_user_resp_groups_api.update_assignment
	apps.fnd_web_sec.change_password
	apps.fnd_web_soc.create_user
	apps.fnd_web_sec.validation_login
	apps.icx_user_sec_attr_pub.create_user_sec_attr
	apps.icx_user_sec_attr_pub.delete_user_sec_attr

注 – アダプタは、さらにほかのテーブルやストアドプロシージャーにアクセスする可能性もあります。詳細は、Oracle E-business Suite のマニュアルを参照してください。

Oracle によれば、Oracle EBS システム (`fnd_user_pkg` ストアドプロシージャーを含む) は、ORACLE EBS システムを APPS ユーザーとして管理するのに使用するように設計されました。Oracle は、代替管理ユーザーの作成を推奨していません。ただし、`APPS` 以外のユーザーで Oracle EBS を管理する必要がある場合は、Oracle にお問い合わせください。

代替管理ユーザーには、APPS ユーザーがすべての Oracle データ (テーブル、ビュー、ストアドプロシージャーを含む) に対して持っているのと同じアクセス権を与えてください。

また、そのユーザーにシノニムを設定して、APPS ユーザーがアクセス権を持っているテーブルにアクセスできるようにする必要があります。別のユーザーを使用し、そのユーザーに必要な許可とシノニムがまだない場合は、次のエラーが発生する可能性があります。

```
Error: ORA-00942: table or view does not exist
```

エラーを修正するには、必要な許可とシノニムを与えます。次のディレクトリに、サンプルの SQL*Plus スクリプトがあります。

```
$WSHOME/sample/other/CreateLHERPAdminUser.oracle.
```

このスクリプトは、必要に応じて変更して、代替 Oracle EBS 管理ユーザーを作成するために使用できます。使用手順は、スクリプトの先頭部分のコメントに記載されています。

パススルー認証の場合のみ、次の SQL コマンドを実行するために権限が必要です。

```
create or replace function wavesetValidateFunc1 (username IN varchar2,
  password IN varchar2)
RETURN varchar2 IS ret_val boolean;
BEGIN ret_val := apps.FND_USER_PKG.ValidateLogin(username, password);
IF ret_val = TRUE THEN RETURN 'valid';
ELSE RETURN NULL;
END IF;
END wavesetValidateFunc1;
```

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。このアダプタは、サポートされるプロビジョニング操作中に直接的なテーブル更新を発行しません。

機能	サポート状況
ユーザーの作成。	あり
開始日と終了日の設定。	あり
パスワードアクセス制限の設定。	あり

機能	サポート状況
パスワード有効期限の設定。	あり
パスワードの変更またはリセット。	はい。
ユーザーレコードに対する従業員 ID (HRMS リンク) の設定。	あり
ユーザーアカウントの Email 属性および Fax 属性の設定。	あり
ユーザーレコードに対する顧客 ID またはサプライヤ ID の設定。	あり
ユーザーに対する 1 つ以上の直接的な責任の割り当て。	あり
ユーザーアカウントに対するセキュリティー設定属性の割り当て。	あり
ユーザーに割り当てられた責任の削除または編集。	はい。 注意: 責任は、実際には削除されるのではなく、期限切れ (無効) になります。
アカウントの無効化。	あり
アカウントの再有効化。	あり
アカウントの削除。	はい。アカウントは、実際には期限切れ (無効) になります。
パススルー認証。	あり
データ読み込みメソッド: 調整、ファイルへの抽出、リソースから読み込み、ファイルから読み込み。	調整 リソースから読み込み
FND_USER テーブルのプロビジョニング。	あり
Oracle HRMS のプロビジョニング。	なし
create における FND_USER レコードの Oracle HRMS へのリンク。	あり
メニュー定義または個々の責任の管理。	なし
間接的な責任の割り当て。	省略可能。間接的な責任は読み取れますが、割り当てられません。
ユーザーセッション制限の設定 (ICX: Session Timeout、ICX: Limit Time、ICX: Limit Connect)。	なし
RBAC オブジェクトと割り当て。	なし

機能	サポート状況
特定のデータオブジェクト、データオブジェクトインスタンス、またはインスタンスセットに対するアクセス権セットの許可の使用。	なし
前アクションと後アクション。	あり
アカウントの名前の変更。	なし

アカウント属性

デフォルトの属性

次の表に、デフォルトの Oracle ERP アカウント属性を示します。すべての属性が省略可能です。

リソースユーザー属性	データ型	説明
owner	string	アカウントを作成した管理者。
start_date	string	アカウントが有効になる日付。
end_date	string	アカウントが期限切れになる日付。 アカウントを無効にするには、日付を過去の日付に設定します。 有効期限がないことを示すには、NULL 値を指定します。 Oracle EBS サーバーのローカル時間を使用してユーザーの有効期限を指定するには、end_date とともに sysdate または SYSDATE キーワードを使用します。
description	string	ユーザーの説明 (フルネームなど)。
password_date	string	最後にパスワードを変更した日付スタンプ。 Oracle ERP アダプタは、password_lifespan_days 属性の値を評価するときに、この日付スタンプを使用できます。たとえば、password_lifespan_days 属性に 90 を設定した場合、Oracle ERP は最後のパスワード変更日付 (password_date) に 90 日を加算して、パスワードが期限切れかどうかを判定します。 Oracle ERP アダプタは、パスワードの変更を行うたびに password_date を現在の日付に設定します。
password_accesses_left	string	ユーザーが現在のパスワードを使用できる回数。

リソースユーザー属性	データ型	説明
password_lifespan_accesses	string	パスワードの有効期間中のアクセス数
password_lifespan_days	string	パスワードの有効期間の合計日数。
employee_id	string	アプリケーションユーザー名が割り当てられた従業員のID。
employee_number	string	per_people_f テーブルの employee_number を表します。 create で値を入力すると、アダプタは per_people_f テーブルでユーザーレコードを検索し、person_id を取得して create API に渡し、fnd_user テーブルの employee_id 列に person_id を挿入しようとします。 create で employee_number を入力しなかった場合、リンクは行われません。 create で employee_number を入力し、その番号が見つからない場合、アダプタは例外をスローします。 employee_number がアダプタのスキーマにある場合、アダプタは、getUser で employee_number を返そうとします。
person_fullname	string	ユーザーのフルネーム。
npw_number	string	不確定の従業員番号。per_people_f テーブルの npw_number を表します。 create で値を入力すると、アダプタは per_people_f テーブルでユーザーレコードを検索し、person_id を取得して create API に渡し、fnd_user テーブルの employee_id 列に person_id を挿入しようとします。 create で npw_number を入力しなかった場合、リンクは行われません。 create で npw_number を入力し、その番号が見つからない場合、アダプタは例外をスローします。 npw_number がアダプタのスキーマにある場合、アダプタは、getUser で npw_number を返そうとします。 注意: employee_number 属性および npw_number 属性は相互排他です。両方を create で入力した場合は、employee_number が優先します。
email_address	string	ユーザーの電子メールアドレス。
fax	string	ユーザーのファックス番号。
customer_id	string	ユーザーの顧客 ID。
supplier_id	string	ユーザーのサプライヤ ID。

リソースユーザー属性	データ型	説明
responsibilities	string	ユーザーに割り当てられた責任の名前。Oracle EBS 11.5.9 でのみ有効です。 Oracle EBS サーバーのローカル時間を使用して責任の有効期限を指定するには、to_date とともに sysdate または SYSDATE キーワードを使用します。
responsibilityKeys	string	ユーザーの責任のリストに関連付けられたキー。
securingAttrs	string	セキュリティー設定属性のサポートを追加します。
expirePassword	boolean	パスワードが期限切れになるかどうかを示します。
directResponsibilities	string	ユーザーの直接的な責任を返します。11.5.10 でのみ有効です。
indirectResponsibilities	string	ユーザーの間接的な責任を返します。11.5.10 でのみ有効です。

追加属性

Oracle ERP アダプタでは、Identity Manager が責任の変更を監査するために使用できる複数の読み取り専用属性を追加できます。auditorResps 属性に返される値は、そのユーザーのアクティブな責任です。次の表に示す auditorObject 以外のすべての属性は、各責任のサブ項目から、存在する可能性があるメニューや機能をすべて差し引いた集合です。

auditorObject 属性も追加できます。この属性については、277 ページの「責任の監査」を参照してください。

次の表に、スキーママップに追加できる属性の一覧を示します。

属性	説明
auditorResps	ユーザーのアクティブな責任のリスト。
formIds	すべてのフォーム ID を連結します。readOnlyFormIds および readWriteOnlyFormIds によって返される値を含んでいます。
formNames	すべてのフォーム名を連結します。readOnlyFormNames および readWriteOnlyFormNames によって返される値を含んでいます。
functionIds	すべての機能 ID を連結します
functionNames	すべての機能名を連結します
menuIds	すべてのメニュー ID を連結します

属性	説明
readOnlyFormIds	すべての読み取り専用フォーム ID を連結します
readOnlyFormNames	すべての読み取り専用フォーム名を連結します
readOnlyFunctionNames	すべての読み取り専用機能名を連結します
readOnlyUserFormNames	すべての読み取り専用ユーザーフォーム名を連結します
readWriteOnlyFormIds	すべての読み取り/書き込み専用フォーム ID を連結します
readWriteOnlyFormNames	すべての読み取り/書き込み専用フォーム名を連結します
readWriteOnlyFunctionNames	すべての読み取り/書き込み専用機能名を連結します
readWriteOnlyUserFormNames	すべての読み取り/書き込み専用ユーザーフォーム名を連結します
userFormNames	すべてのユーザーフォーム名を連結します。readOnlyUserFormNames および readWriteOnlyUserFormNames によって返される値を含んでいます。
userFunctionNames	すべてのユーザー機能名を連結します
userMenuNames	すべてのユーザーメニュー名を連結します。

Oracle ERP アダプタでは、create および update の前アクションおよび後アクションを使用することにより、またはカスタムの getUser アクションを使用することにより、任意の追加カスタム属性をサポートできます。詳細は、279 ページの「リソースアクションの使用」を参照してください。

リソースオブジェクトの管理

Identity Manager は、次のネイティブオブジェクトをサポートします。

リソースオブジェクト	サポートされる機能	管理対象オブジェクト
responsibilityNames	更新	name、userMenuNames、menuIds、userFunctionNames、functionId

アイデンティティーテンプレート

```
$accountId$
```

サンプルフォーム

組み込みのフォーム

なし

その他の利用可能なフォーム

`OracleERPUserForm.xml`

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

- `com.waveset.adapter.OracleERPResourceAdapter`
- `com.waveset.adapter.JdbcResourceAdapter`
- `com.waveset.adapter.JActionUtil` (前アクションや後アクションを使用する場合)

◆ ◆ ◆ 第 26 章

OS/400

OS/400 リソースアダプタは、com.waveset.adapter.OS400ResourceAdapter クラスで定義されます。

アダプタの詳細

なし。

リソース設定の詳細

なし。

Identity Manager のインストールに関する注意事項

OS/400 リソースアダプタは、カスタムアダプタです。インストールプロセスを完了するには、次の手順を実行する必要があります。

▼ OS400 リソースアダプタをインストールする

1. **http://jt400.sourceforge.net** から **JTOpen** のバージョン **2.03** をダウンロードします。
2. **JTOpen** ファイルを解凍し、インストール手順に従います。必ずライブラリファイルを正しい場所に配置し、環境変数を指示どおりに設定してください。
   jt400.jar ファイルの入手方法については、IBM にお問い合わせください。
3. jt400.jar ファイルを *InstallDir*\WEB-INF\lib ディレクトリにコピーします。

4 **OS/400** リソースを **Identity Manager** のリソースリストに追加するには、「管理するリソースの設定」ページの「カスタムリソース」セクションに次の値を追加する必要があります。

```
com.waveset.adapter.OS400ResourceAdapter
```

使用上の注意

Identity Manager は、OS/400 リソース上のアカウントに関連付けられた OS/400 オブジェクトを処理するために 3 つのオプションをサポートします。このサポートを有効にするには、Identity Manager のサンプルディレクトリにある OS400Deprovision フォームを使用する必要があります。また、システム設定オブジェクトも編集する必要があります。このオブジェクトを設定する手順は、OS400Deprovision フォームのコメントで説明されています。有効にしたオプションは、ユーザーの OS/400 リソースアカウントを削除するときに「リソースアカウントの削除」ページに表示されます。

選択可能な削除オプションは次のとおりです。

- **DLT**。ユーザーのリソースアカントと、そのアカウントに関連付けられた OS/400 オブジェクトが削除されます。
- **NODLT**。関連付けられたオブジェクトがユーザーにある場合、そのユーザーのアカウントは削除されず、関連付けられた OS/400 オブジェクトは影響を受けません。
- **CHGOWN**。ユーザーのリソースアカウントが削除されて、関連付けられた OS/400 オブジェクトが指定された所有者に割り当てられます。CHGOWN は、デフォルトのオプションです。デフォルトでは、OS/400 オブジェクトは QDFTOWN プロファイルに割り当てられます。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は、SSL (Secure Sockets Layer) を使用して OS/400 アダプタと通信できます。その場合は、次の製品を実装してください。

- IBM iSeries Client Encryption ライセンスプログラム 5722-CE2 または 5722-CE3 の V5R1 以降のバージョンで提供される SSL オブジェクト。

このプログラムには、OS/400 リソース上の Java Toolbox を使用して Identity Manager から SSL 接続を行うのに必要な SSLight パッケージが含まれています。

必要な管理特権

このアダプタには、次の管理特権が必要です。

- **CRT**: OS/400 ユーザーを追加するために、管理者には、(1) *SECADM 特殊権限、(2) 初期プログラム、初期メニュー、ジョブ記述、メッセージキュー、出力キュー、およびアテンションキー処理プログラム (指定されている場合) に対する *USE 権限、(3) グループプロファイルと補足グループプロファイルが指定されている場合は、それらに対する *CHANGE 権限とオブジェクト管理権限が必要です。
- **CHG**: *SECADM 特殊権限、および変更されるユーザープロファイルに対する *OBJMGT 権限と *USE 権限が必要です。これらは、このコマンドを指定できます。現在のライブラリ、プログラム、メニュー、ジョブ記述、メッセージキュー、印刷デバイス、出力キュー、またはアテンションキー処理プログラムのパラメータを指定するには、これらに対する *USE 権限が必要です。
- **DLT**: ユーザーには、ユーザープロファイルに対する使用 (*USE) 権限とオブジェクト存在 (*OBJEXIST) 権限が必要です。ユーザーは、ユーザープロファイルに関連付けられ、所有されているメッセージキューを削除するために、存在、使用、および削除の権限を持っている必要があります。現在、ユーザーがユーザープロファイルに基づいて実行している場合や、ユーザープロファイルが何らかのオブジェクトを所有して OWNOBJOPT(*NODLT) が指定されている場合は、そのプロファイルを削除できません。あらかじめ、ユーザープロファイル内のすべてのオブジェクトを、オブジェクト所有者変更 (CHGOBJOWN) コマンドを使用して新しい所有者に転送するか、またはシステムから削除してください。OWNOBJOPT(*DLT) を指定してオブジェクトを削除する方法や、OWNOBJOPT(*CHGOWN user-profile-name) を指定して所有権を変更する方法もあります。ユーザーに許可された権限は、オブジェクト権限取り消し (RVKOBJAUT) コマンドによって明確に取り消す必要はありません。 ユーザープロファイルを削除したときに自動的に取り消されます。
- **DSP**: TYPE(*BASIC) と OUTPUT(*OUTFILE) を指定した場合にのみ、USRPRF(*ALL) または USRPRF(generic*-user-name) としてユーザー名を指定できます。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	なし

機能	サポート状況
パススルー認証	なし
前アクションと後アクション	あり
データ読み込みメソッド	■ リソースから直接インポート ■ リソースの調整

アカウント属性

次の表に、OS/400 アカウント属性に関する情報を示します。特に記載されていないかぎり、すべての属性は文字列です。

リソースユーザー属性	説明
accountId	必須。ユーザーのログオン ID。
password	必須。ユーザーのパスワード。この値は暗号化されています。
ASTLVL	操作支援レベル
ATNPGM	アテンションキー処理プログラム
CCSID	コード化文字セット識別子
CNTRYID	国識別子
CURLIB	現在のライブラリ
DAYS_UNTIL_PASSWORD_EXPIRES	パスワードの期限が切れるまでの日数。
DLVRY	デリバリモード
GID	グループ識別番号
GRPPRF	グループプロファイル
HIGHEST_SCHEDULING_PRIORITY	
HOMEDIR	ホームディレクトリ
INLMNU	初期メニュー
INLPGM	初期プログラム
JOBD	ジョブ記述
KBDBUF	キーボードバッファリング
LANGID	言語識別子

リソースユーザー属性	説明
LMTCPB	制限機能
LMTDEVSSN	デバイスセッションの制限
MAXSTG	最大記憶領域
MSGQ	メッセージキュー
OUTQ	出力キュー
OWNER	新しいオブジェクトの所有者
OWNOBJOPT	所有オブジェクトオプション
PRTDEV	印刷デバイス
PWDEXP	パスワードに有効期限を設定するかどうかを示します。
SPCAUT	特殊権限
SPCENV	特殊環境
SRTSEQ	ソート処理
STATUS	ユーザープロファイルのログインステータス
TEXT	ユーザーの説明
UID	ユーザー識別番号
USRCLS	ユーザークラス
USROPT	ユーザーオプション

リソースオブジェクトの管理

なし。

アイデンティティーテンプレート

```
$accountId$
```

サンプルフォーム

OS400UserForm.xml

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

```
com.waveset.adapter.OS400ResourceAdapter
```

◆ ◆ ◆ 第 27 章

27 PeopleSoft コンポーネント

PeopleSoft コンポーネントアダプタは、PeopleSoft コンポーネントインタフェースを使用した PeopleTools with HRMS をサポートします。このアダプタは読み取り専用です。このアダプタを使用して PeopleSoft アカウントを作成または変更することはできません。このアダプタは、Active Sync を使用してアカウント情報を Identity Manager に読み込みます。

このアダプタは、 `com.waveset.adapter.PeopleSoftComponentActiveSyncAdapter` クラスで定義されます。

アダプタの詳細

リソースを設定する際の注意事項

リソースをリソースアダプタに統合するには、次の PeopleSoft ツールを使用してください。

- Application Designer。Identity Manager プロジェクトを構築および設定するには、このツールを使用します。
- PeopleTools ブラウザベースアプリケーション。コンポーネントのインタフェース、ロール、およびユーザープロファイルを設定するには、このツールを使用します。

PeopleSoft を Identity Manager で使用できるように設定するには、次の手順に従います。

- 手順 1: 新しいプロジェクトを作成する
- 手順 2: Identity Manager オブジェクトを編集する
- 手順 3: プロジェクトを構築する
- 手順 4: `audittrigger` スクリプトを手動で実行する

- 手順 5: 選択したテーブルに対する監査を有効にする
- 手順 6: PeopleTools を設定する
- 手順 7: 監査ログを除去する

手順 1: 新しいプロジェクトを作成する

次の手順に従って、PeopleSoft Application Designer を使用して新しいプロジェクトを作成します。

▼ 新しいプロジェクトを作成する

1. **Application Designer** で「**File**」、「**New**」の順に選択して、新しいプロジェクトを作成します。次に、リストから「**Project**」を選択します。
2. 保存を実行してプロジェクトに名前を付けます。「**File**」、「**Save Project As...**」の順に選択して、プロジェクトの一意の名前 (たとえば、**IDM**) を入力します。
3. 302 ページの「手順 2: Identity Manager オブジェクトを編集する」のタスクを実行して、プロジェクト内にオブジェクトを作成します。

手順 2: Identity Manager オブジェクトを編集する

Identity Manager プロジェクトには、次の種類のオブジェクトが含まれています。

これらのオブジェクトは、Application Designer 内で作成してください。次に、これらのオブジェクトについてそれぞれ詳しく説明します。

フィールド

次のフィールドを作成します。

- AUDIT_PROC_ORDER。フィールドタイプを「Character」に、長さを「20」に設定します。
- AUDIT_PROC_END。フィールドタイプを「Character」に、長さを「20」に設定します。
- AUDIT_PROC_DATE。フィールドタイプを「Date」に設定します。

次に、AUDIT_PROC_ORDER フィールドを作成するための手順について説明します。

▼ AUDIT_PROC_ORDER フィールドを作成する

1 「**File**」、「**New...**」、「**Field**」の順に選択します。

2 「**Character**」フィールドタイプを選択します。

3 フィールドの長さを **20** に設定します。

4 ラベル **ID**「**AUDIT_PROC_ORDER**」を割り当てます。

5 「**File**」、「**Save**」の順に選択して、フィールドを保存します。フィールドに、「**AUDIT_PROC_ORDER**」という名前を付けます。

6 「**Insert**」、「**Current Definition**」の順に選択して、フィールドをプロジェクトに追加します。

レコード

Application Designer 内で定義するレコードは、3 つ (ビューが 2 つ、テーブルが 1 つ) あります。次のレコードの説明は、一般的な実装を示しています。レコードは、フィールドの追加や変更により、実装のニーズに合わせてカスタマイズできます。

AUDIT_EFFDT_LH ビュー

AUDIT_EFFDT_LH ビューは、PeopleSoft Active Sync リソースアダプタによってポーリングされます。Identity Manager は次のフィールドを使用して、まだ処理されていないイベントをクエリー検索します。

- AUDIT_PROC_ORDER。このフィールドには、Key、Search Key、List Box Item、および From Search Field の各キーを指定してください。
- AUDIT_PROC_END。このフィールドには、Key、Search Key、List Box Item、および Through Search Field の各フィールドを指定してください。
- EMPLID および EMPL_RCD。これらは、Identity Manager のクエリーで従業員データを取得するために使用される、必須のキー以外のプロパティーです。

AUDIT_EFFDT_LH テーブルのほかのすべてのフィールドは、省略可能です。

次の表では、AUDIT_EFFDT_LH ビューの Use Display 特性について説明します。

フィールド名	タイプ	キー	順序	方向	検索	List	システム	デフォルト
AUDIT_PROC_ORDER	Char	キー	1	昇順	あり	あり	なし	

フィールド名	タイプ	キー	順序	方向	検索	List	システム	デフォルト
AUDIT_PROC_END	Char	キー		昇順	あり	あり	なし	
AUDIT_STAMP	DtTm				なし	なし	なし	
EFFDT	Date				なし	なし	なし	%date
AUDIT_OPRID	Char				なし	なし	なし	
AUDIT_ACTN	Char				なし	なし	なし	
AUDIT_RECNAME	Char				なし	なし	なし	
EMPLID	Char				なし	なし	なし	”NEW’
EMPL_RCD	Nbr				なし	なし	なし	

最後の監査エントリの情報は、以降の AUDIT_EFFDT_LH ビューの検索で使用 (および更新) される「lastProcessed」設定オブジェクトとして Identity Manager に格納されます。lastProcessed 設定オブジェクトは PeopleSoft Active Sync リソースアダプタによって保守されるため、レコードが 2 回以上処理されることはありません。

次の SQL コードは、AUDIT_EFFDT_LH ビューを生成するために使用します。

```
SELECT audit1.AUDIT_PROC_ORDER AS AUDIT_PROC_ORDER
,audit1.AUDIT_PROC_ORDER AS AUDIT_PROC_END
,audit1.AUDIT_STAMP AS AUDIT_STAMP
,audit1.EFFDT AS EFFDT
,audit1.AUDIT_OPRID AS AUDIT_OPRID
,audit1.AUDIT_ACTN AS AUDIT_ACTN
,audit1.AUDIT_RECNAME AS AUDIT_RECNAME
,audit1.EMPLID AS EMPLID
,CAST(audit1.EMPL_RCD AS INTEGER) AS EMPL_RCD FROM PS_AUDIT_PRS_DATA audit1
WHERE audit1.AUDIT_PROC_DATE <= %CurrentDateIn
AND NOT EXISTS (
SELECT * FROM PS_AUDIT_PRS_DATA audit2
WHERE audit2.AUDIT_PROC_DATE <= %CurrentDateIn
AND audit2.AUDIT_PROC_ORDER > audit1.AUDIT_PROC_ORDER
AND (audit2.EMPLID = audit1.EMPLID AND audit2.EMPL_RCD = audit1.EMPL_RCD) );
```

この SQL コードサンプルの最後の行によって、有効な日付が設定されている操作は、その有効な日付が来るまで Identity Manager に表示されなくなります。

AUDIT_PRS_DATA テーブル

AUDIT_PRS_DATA テーブルには、次のフィールドが必要です。

- AUDIT_PROC_ORDER。このフィールドには、Key、Search Key、List Box Item、および From Search field の各キーを指定してください。また、このフィールドを Required に設定して、PeopleSoft がデータベース列に NULL 以外の整合性制約を適用するようにしてください。
- AUDIT_PROC_DATE。このフィールドには、Alternate Search Key と List Box Item を指定してください。また、このフィールドを Required に設定して、PeopleSoft がデータベース列に NULL 以外の整合性制約を適用するようにしてください。
- EMPLID および EMPL_RCD。これらは、Identity Manager のクエリーで従業員データを取得するために使用される、必須のキー以外のプロパティーです。

AUDIT_PRS_DATA テーブルのほかのすべてのフィールドは、省略可能です。

次の表では、AUDIT_PRS_DATA ビューの Use Display 特性について説明します。

フィールド名	タイプ	キー	順序	方向	検索	List	システム	デフォルト
AUDIT_PROC_ORDER	Char	キー	1	昇順	あり	あり	なし	
AUDIT_PROC_DATE	Date	Alt		昇順	なし	なし	なし	
AUDIT_STAMP	DtTm				なし	なし	なし	%date
AUDIT_OPRID	Char				なし	なし	なし	”ANON’
AUDIT_ACTN	Char				なし	なし	なし	”C’
AUDIT_RECNAME	Char				なし	なし	なし	”ANON’
EMPLID	Char				なし	なし	なし	”NEW’
EFFDT	Date				なし	なし	なし	%date
EMPL_RCD	Nbr				なし	なし	なし	

PERS_SRCH_LH ビュー

PERS_SRCH_LH ビューには、Key、Search Key、List Box Item の各キーが選択された EMPLID フィールドと EMPL_RCD フィールドを含める必要があります。ほかのすべてのフィールドは、Identity Manager と同期されるデータを提供します。Identity Manager のユーザーアカウントへのこれらのデータのマップは、PeopleSoft Active Sync フォームが行います。

次の表では、PERS_SRCH_LH ビューの Use Display 特性について説明します。

フィールド名	タイプ	キー	順序	方向	検索	List	システム
EMPLID	Char	キー	1	昇順	あり	あり	なし
EMPL_RCD	Nbr	キー	2	昇順	あり	あり	なし
NAME	Char				なし	あり	なし
LAST_NAME_SRCH	Char				なし	あり	なし
SETID_DEPT	Char				なし	あり	なし
DEPTID	Char				なし	あり	なし
ADDRESS1	Char				なし	あり	なし
EMPL_STATUS	Char				なし	あり	なし
FIRST_NAME	Char				なし	あり	なし
LAST_NAME	Char				なし	あり	なし
MIDDLE_NAME	Char				なし	あり	なし
REPORTS_TO	Char				なし	あり	なし
JOBCODE	Char				なし	あり	なし
COMPANY	Char				なし	あり	なし
NAME_INITIALS	Char				なし	あり	なし
COUNTRY	Char				なし	あり	なし
PHONE	Char				なし	あり	なし
CITY	Char				なし	あり	なし
STATE	Char				なし	あり	なし
POSTAL	Char				なし	あり	なし

次の SQL コードは、PERS_SRCH_LH ビューを生成するために使用します。

注 – なお、インストールメディアの peoplesoft/idm.zip ファイルには、次の SQL コードを複製した pers_srch_lh.sql という名前の SQL スクリプトファイルが含まれています。

```
SELECT P.EMPLID
 ,A.EMPL_RCD
 ,P.NAME
 ,P.LAST_NAME_SRCH
 ,A.SETID_DEPT
```

```
,A.DEPTID
,P.ADDRESS1
,A.EMPL_STATUS
,P.FIRST_NAME
,P.LAST_NAME
,P.MIDDLE_NAME
,A.REPORTS_TO
,A.JOBCODE
,A.COMPANY
,P.NAME_INITIALS
,P.COUNTRY
,P.PHONE
,P.CITY
,P.STATE
,P.POSTAL
FROM PS_Job A
, PS_PERSONAL_DATA P
WHERE A.EMPLID = P.EMPLID
AND A.EffDt = (
SELECT MAX(C.EffDt)
FROM PS_Job C
WHERE C.EmplID = A.EmplID
AND C.EMPL_RCD = A.EMPL_RCD
AND C.EffDt <= %CurrentDateIn)
AND A.EffSeq = (
SELECT MAX(D.EffSeq)
FROM PS_Job D
WHERE D.EmplID = A.EmplID
AND D.EMPL_RCD = A.EMPL_RCD
AND D.EffDt = A.EffDt)
```

WHERE 節は、指定した従業員 ID に対する現在の従業員レコードを返します。PeopleSoft では、1 人の従業員に対して複数のレコードが許可されており、それぞれに独自の有効日と有効シーケンスがあります。この節は、すでに有効である (有効日がすでに発生した) 有効日/有効シーケンスのすべてのペアの中で最新であるペアを持つレコードを返します。

この WHERE 節は、サンライズの日付が未来である従業員については NULL を返します。

ページ

Identity Manager プロジェクトでは、コンポーネントインタフェース専用の次のページも必要です。

- LH_AUDIT_EFFDT
- LH_EMPLOYEE_DATA

LH_AUDIT_EFFDT

LH_AUDIT_EFFDT ページには、AUDT_EFFDT_LH テーブルで定義されたフィールドが表示されます。このページは、PeopleSoft の GUI には表示されません。このため、フィールドの配置や順序は重要ではありません。

次の表に、LH_AUDIT_EFFDT ページの Use Display 特性を示します。すべての項目は、AUDT_EFFDT_LH レコードで定義されます。

ラベル	タイプ	フィールド
Unique order to process	Edit Box	AUDIT_PROC_ORDER
EmplID	Edit Box	EMPLID
Upper bound for search	Edit Box	AUDIT_PROC_END
Empl Rcd Nbr	Edit Box	EMPL_RCD
Date and Time Stamp	Edit Box	AUDIT_STAMP
Effective Date	Edit Box	EFFDT
User ID	Edit Box	AUDIT_OPRID
Action	Drop Down List	AUDIT_ACTN
Audit Record Name	Edit Box	AUDIT_RECNAME

LH_EMPLOYEE_DATA

LH_EMPLOYEE_DATA ページは、PERS_SRCH_LH ビューで定義されたフィールド用のコンテナです。すべての項目は、PERS_SRCH_LH レコードで定義されます。

次の表では、LH_EMPLOYEE_DATA ページの Use Display 特性について説明します。

ラベル	タイプ	フィールド
EmplID	Edit Box	EMPLID
名前	Edit Box	NAME
Last Name	Edit Box	LAST_NAME_SRCH
Department SetID	Edit Box	SETID_DEPT
Department	Edit Box	DEPTID
Address Line 1	Edit Box	ADDRESS1
Personnel Status	Edit Box	PER_STATUS
Employee Status	Edit Box	EMPL_STATUS

ラベル	タイプ	フィールド
First Name	Edit Box	FIRST_NAME
Last Name	Edit Box	LAST_NAME
Middle Name	Edit Box	MIDDLE_NAME
Reports To Position	Edit Box	REPORTS_TO
Job Code	Edit Box	JOBCODE
Company	Edit Box	COMPANY
Name Initials	Edit Box	NAME_INITIALS
Country	Edit Box	COUNTRY
Telephone	Edit Box	PHONE
City	Edit Box	CITY
State	Edit Box	STATE
Postal Code	Edit Box	POSTAL
Empl Rcd Nbr	Edit Box	EMPL_RCD

コンポーネント

コンポーネントは、ページとメニューを橋渡しします。ページを作成したら、そのページをメニューやビジネスプロセスで使用するために 1 つ以上のコンポーネントに追加してください。

次のページごとに別個のコンポーネントを作成します。

- LH_AUDIT_EFFDT
- LH_EMPLOYEE_DATA

デフォルトのコンポーネント名は、LH_AUDIT_EFFDT および LH_EMPLOYEE_COMP です。

次に、LH_AUDIT_EFFDT フィールドを作成するための手順について説明します。

▼ LH_AUDIT_EFFDT コンポーネントを作成する

1 「**File**」、「**New...**」、「**Component**」の順に選択します。

2 「**Insert**」、「**Page Into Component...**」の順に選択します。名前を「**LH_AUDIT_EFFDT**」として指定します。

3 「**File**」、「**Definition/Object Properties**」の順に選択します。次に、「**Use and Search Record AUDIT_EFFDT_LH**」に移動します。

4 「**Select File**」、「**Save**」の順に選択して、コンポーネントに **LH_AUDIT_EFFDT** という名前を付けます。

コンポーネントインタフェース

コンポーネントインタフェースは、ほかのアプリケーション (Identity Manager など) からの同期アクセスのために PeopleSoft コンポーネントを公開する PeopleTools オブジェクトです。作成したコンポーネントごとに別個のコンポーネントインタフェースを作成します。コンポーネントインタフェースのデフォルト名は、LH_AUDIT_EFFDT_COMP_INTF および LH_EMPLOYEE_COMP_INTF です。これらの値は、Active Sync ウィザードの「Active Sync の一般設定」ページで変更できます。

次に、LH_AUDIT_EFFDT_COMP_INTF コンポーネントインタフェースを作成するための手順について説明します。

▼ LH_AUDIT_EFFDT_COMP_INTF コンポーネントを作成する

1 「**File**」、「**New...**」、「**Component Interface**」の順に選択します。

2 **LH_AUDIT_EFFDT** など、ソースコンポーネントを指定します。プロンプトが表示されたら、「**Yes**」を選択します。

3 「**File**」、「**Save**」の順に選択します。名前 **LH_AUDIT_EFFDT_COMP_INTF** を指定します。

手順 3: プロジェクトを構築する

この手順に従って、プロジェクトを構築し、データベースに PeopleSoft のビューやテーブルを作成します。

Application Designer を使用してプロジェクトを構築するには、次の手順に従います。

▼ プロジェクトを構築する

1 「**Build**」、「**Project**」の順に選択します。「**Build**」ダイアログが表示されます。

2 「**Build Options**」領域で、「**Create Tables**」オプションと「**Create Views**」オプションを選択します。「**Build Execute Options**」領域で、「**Execute SQL now**」オプションを選択します。

3 「**Settings**」をクリックします。「**Build Settings**」ダイアログが表示されます。

4 「**Recreate table if it already exists**」オプションが選択されていることを確認します。

5 「**Logging**」タブをクリックします。

6 「**Logging Level**」領域で、「**Fatal errors, warnings and information messages**」オプションを選択します。

7 「**Logging Output**」領域で、一意のログファイル名を入力します。

8 「**OK**」をクリックしてから「**Build**」をクリックし、プロジェクトを構築して、ビューとテーブルを作成します。

Application Designer に、次のような警告メッセージが表示される場合があります。

```
Potentially data destructive settings are active. Continue the build process?
```

9 「**Yes**」をクリックして構築処理を続行します。

注 – プロジェクトのインポートと構築が終了したら、Application Designer でコンポーネントをテストしてください。PeopleSoft に含まれるプロジェクトインポート機能の信頼性は、リリースによって異なります。このため、オブジェクトの検証はとても重要です。

手順 **4: audittrigger** スクリプトを手動で実行する

`idm.zip` ファイルには、`audittrigger.oracle` という名前の Oracle SQL スクリプトが含まれています。このスクリプトは、`PS_AUDIT_PRS_DATA` テーブルの `AUDIT_PROC_DATE` 列と `AUDIT_PROC_ORDER` 列を維持するのに必要なトリガーと処理を作成します。

注 – `audittrigger.oracle` スクリプトは、Oracle 専用です。ほかのデータベースを使用する場合は、このスクリプトをそのデータベースで動作するように変換してください。

`audittrigger.oracle` スクリプトまたはそれに相当するものは、PeopleSoft プロジェクトを再構築するたびに実行してください。

手順 **5:** 監査を有効にする

Application Designer で、JOB テーブルと PERSONAL_DATA テーブル (場合によってはさらに POSITION_DATA テーブルと EMPLOYMENT テーブル) に対する監査を有効にします。これは、演算子と変更されたレコードの EMPLID を使用して簡単な略式レコードを書き込むレコードレベルの監査です。

▼ PeopleTools データベースオブジェクトを更新する

1 **Application Designer** を起動します。

2 「**File**」、「**Open**」の順に選択して、「**Open Object**」ダイアログを表示します。

3 「**Object type**」メニューから「**Record**」を選択し、「**Name**」フィールドに「**JOB**」と入力します。

4 「**Open**」をクリックしてレコードを開きます。

5 「**File**」、「**Properties**」の順に選択してレコードのプロパティーを開き、「**Use**」タブをクリックします。

6 「**Record Name**」フィールドで、「**AUDIT_PRS_DATA**」を選択します。

7 「**Audit Options**」領域で、「**Add**」オプション、「**Change**」オプション、および「**Delete**」オプションを選択します。「**Selective**」オプションにはチェックマークを付けないでください。

PERSONAL_DATA テーブルおよびデータ同期のトリガーになるその他のテーブルについて、これらの手順を繰り返します。

注 – 詳細は、Application Designer のマニュアルの「Creating Record Definitions」を参照してください。

手順 6: PeopleTools を設定する

設定プロセスを完了するには、PeopleTools ブラウザベース GUI を使用して、アクセス権リストにコンポーネントインタフェースを割り当て、ロールを作成してそのロールにアクセス権リストを割り当て、ユーザープロファイルにそのロールを割り当ててください。これらのエンティティーについては、PeopleTools のマニュアルを参照してください。

コンポーネントインタフェース

コンポーネントインタフェースの使用を承認する必要があります。

▼ コンポーネントインタフェースを承認する

1 **PeopleTools** ブラウザベース **GUI** にログインし、「**Home**」、「**People Tools**」、「**Maintain Security**」、「**Use**」、「**Permission Lists**」の順に移動します。**Peoplesoft 9** の場合、このパスは「**Home**」、「**People Tools**」、「**Security**」、「**Permissions & Roles**」、「**Permission List**」の順になります。

2 「**Add a New Value**」リンクを選択し、値 (たとえば、**LH_ALL**) を入力します。

3 ページ上部のタブセクションの右矢印を「**Component Interface**」タブが表示されるまでクリックします。次に、「**Component Interface**」タブをクリックします。

4 テキストボックスに既存のコンポーネントインタフェース (たとえば、**LH_AUDIT_EFFDT_COMP_INTF**) を入力します。

5 「**Edit**」リンクをクリックして、「**Component Interface Permissions**」ページに移動します。

6 「**Full Access**」ボタンをクリックして、すべてのメソッドに対するフルアクセスを有効にするか、ドロップダウンメニューを使用して個々のメソッドに対するアクセスを割り当てます。「**OK**」をクリックして「**Permission Lists**」ページに戻ります。

7 「**+ (プラス)**」ボタンをクリックします。さらにテキストボックスが表示されます。

8 テキストボックスに、ほかの既存のコンポーネントインタフェース (たとえば、**LH_EMPLOYEE_COMP_INTF**) を入力します。

9 手順 **5** および **6** を繰り返します。

10 変更を保存します。

▼ コンポーネントインタフェースに **PeopleSoft** ロールを割り当てる

1 「**Home**」「**People Tools**」、「**Maintain Security**」、「**Use**」、「**Roles**」の順に移動します。**Peoplesoft 9** の場合、このパスは「**Home**」、「**People Tools**」、「**Security**」、「**Permissions & Roles**」、「**Roles**」の順になります。

2 「**Add a New Value**」リンクを選択し、値 (たとえば、**LH_ROLE**) を入力します。

3 「**Permission Lists**」タブをクリックします。

4 既存のアクセス権リスト (たとえば、**LH_ALL**) を入力します。

5 変更を保存します。

▼ ロールをユーザープロフィルに割り当てる

1 「**Home**」、「**People Tools**」、「**Maintain Security**」、「**Use**」、「**User Profiles**」の順に移動します。**Peoplesoft 9** の場合、このパスは「**Home**」、「**People Tools**」、「**Security**」、「**User Profiles**」、「**User Profiles**」の順になります。

2 既存のユーザー **ID** を入力します。このユーザーは、**Identity Manager** の「リソースパラメータ」ページでユーザーとして指定できます。

注 – 新しいユーザーを作成することもできます。ユーザーアカウントの要件の詳細については、PeopleSoft のマニュアルを参照してください。

---

3 「**Roles**」タブを選択します。

4 「**+(プラス)**」ボタンをクリックします。さらにテキストボックスが表示されます。

5 ロールの名前 **(**たとえば、**LH_ROLE)** を入力します。

6 変更を保存します。

手順 **7:** 監査ログを除去する

Identity Manager は、監査ログから監査イベントを削除しません。PeopleSoft 管理者は、古い監査エントリを除去するタスクを設定する必要があります。このタスクは、未来の有効日を持つトランザクションを、Identity Manager が処理するまで維持する必要があります。つまり、`AUDIT_PROC_DATE` が未来であるエントリを除去してはいけません。

Identity Manager のインストールに関する注意事項

PeopleSoft コンポーネントリソースアダプタは、カスタムアダプタです。インストールプロセスを完了するには、次の手順を実行する必要があります。

▼ **PeopleSoft** コンポーネントリソースアダプタをインストールする

1 `psjoa.jar` ファイルをインストールメディアから *InstallDir*`\idm\WEB-INF\lib` ディレクトリにコピーします。

この jar ファイルのバージョン番号は、PeopleSoft のバージョンと一致する必要があります。

2 このリソースを **Identity Manager** のリソースリストに追加するには、「管理するリソースの設定」ページの「カスタムリソース」セクションに次の値を追加する必要があります。

```
com.waveset.adapter.PeopleSoftComponentActiveSyncAdapter
```

使用上の注意

ここでは、PeopleSoft コンポーネントリソースアダプタの使用に関連する情報を提供します。 次のトピックがあります。

クラスタ内のホストの制御

`waveset.properties` ファイルの `sources.`*ResourceName* `.hosts` プロパティーを使用して、Active Sync を使用してリソースの同期を行うクラスタ内のホストを選択できます。*ResourceName* は、リソースオブジェクトの名前に置き換えてください。

ActiveSync 設定

Active Sync ウィザードの「Active Sync の一般設定」ページで、「監査コンポーネントインタフェース名」と「従業員コンポーネントインタフェース名」を指定します。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は、Client Connection Toolkit (同期のみ) を使用してこのアダプタと通信します。

必要な管理特権

PeopleSoft に接続するユーザー名を、コンポーネントインタフェースにアクセスできる PeopleSoft ロールに割り当ててください。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの作成	なし
アカウントの更新	なし

機能	サポート状況
アカウントの削除	なし
アカウントの有効化/無効化	なし
パスワードの更新	なし
アカウントの名前の変更	なし
パススルー認証	なし
前アクションと後アクション	なし
データ読み込みメソッド	Active Sync

アカウント属性

次の表に、PeopleSoft コンポーネント Active Sync アダプタアカウント属性に関する情報を示します。

リソースユーザー属性	mapName	説明
accountId	EMPLID	必須。
ACTION	ACTION	最大 3 文字のアクションコード
ACTION_REASON	ACTION_REASON	最大 3 文字の理由コード
AUDIT_ACTN	AUDIT_ACTN	システムが監査するアクションのタイプ (A= 追加、C= 変更、D= 削除)。
AUDIT_OPRID	AUDIT_OPRID	システムによる監査のトリガーを発生させたオペレータ
AUDIT_STAMP	AUDIT_STAMP	日付と時刻のスタンプ
AUDIT_RECNAME	AUDIT_RECNAME	システムが監査したレコードの名前
EFFSEQ	EFFSEQ	有効シーケンス
EFFDT	EFFDT	有効日
Employee ID	EMPL_ID	ユーザーを一意に識別するために使用されるキーフィールド。
fullname	NAME	ユーザーのフルネーム。
firstname	FIRST_NAME	ユーザーの名。
lastname	LAST_NAME	ユーザーの姓。

リソースユーザー属性	mapName	説明
Middle Name	MIDDLE_NAME	ユーザーのミドルネーム
PS_PER_STATUS	PER_STATUS	担当者のステータス (従業員、非従業員など)
PS_EMPL_STATUS (AS アダプタでのステータス)	EMPL_STATUS	従業員のステータス (アクティブ、保留、終了など)
Home Address	ADDRESS1	ユーザーの自宅住所
Department	DEPTID	ユーザーの部署
Manager	REPORTS_TO	ユーザーのマネージャー
Job Title	JOBCODE	ユーザーの役職を識別するコード
Initials	NAME_INITIALS	ユーザーのイニシャル
Country	COUNTRY	3 文字の国コード
Company	COMPANY	会社名
Home Phone	PHONE	ユーザーの自宅電話番号
Home City	CITY	ユーザーが居住する市
Home State	STATE	ユーザーが居住する州
Home Zip	POSTAL	ユーザーの自宅郵便番号

リソースオブジェクトの管理

該当なし。

アイデンティティーテンプレート

```
$accountId$
```

サンプルフォーム

```
PeopleSoftForm.xml
```

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

```
com.waveset.adapter.PeopleSoftComponentActiveSyncAdapter
```

◆ ◆ ◆ 第 28 章

28 PeopleSoft コンポーネントインタフェースアダプタ

PeopleSoft コンポーネントインタフェースアダプタは、com.waveset.adapter.PeopleSoftCompIntfcAdapter クラスで定義されます。

このリソースアダプタは、コンポーネントインタフェースを介して PeopleSoft のデータを管理します。また、サポートされているバージョンの PeopleTools とともにその他の PeopleSoft アプリケーション (HR、Financials など) がシステムにインストールされている場合は、それらのアプリケーションも管理できます。

アダプタの詳細

リソースを設定する際の注意事項

PeopleSoft コンポーネントインタフェースアダプタは、デフォルトで USER_PROFILE コンポーネントインタフェースと DELETE_USER_PROFILE コンポーネントインタフェースをサポートするように設定されています。このアダプタでは、コンポーネントインタフェースが次のメソッドをサポートする場合に、カスタムコンポーネントインタフェースを使用してアカウントデータの作成、読み取り、更新も行えます。

- Create
- Get
- Find
- Save
- SetPassword

アカウントを削除するには、カスタムコンポーネントインタフェースが次のメソッドをサポートしている必要があります。

- Get
- Save

さらに、「リソースパラメータ」ページで指定されたユーザーが、呼び出されたコンポーネントインタフェースのメソッドを実行するためのアクセス権を持っている必要があります。

Identity Manager のインストールに関する注意事項

PeopleSoft コンポーネントインタフェースアダプタは、カスタムアダプタです。インストールプロセスを完了するには、次の手順を実行する必要があります。

▼ PeopleSoft コンポーネントアダプタをインストールする

1 次のファイルを **PeopleSoft** のインストールメディアから `$WSHOME/WEBINF/lib` ディレクトリにコピーします。

```
psjoa.jar
```

注 – `psjoa.jar` のバージョンはインストールされている PeopleSoft システムのバージョンと一致する必要があります。

---

2 このリソースを **Identity Manager** のリソースリストに追加するには、「管理するリソースの設定」ページの「カスタムリソース」セクションに次の値を追加する必要があります。

```
com.waveset.adapter.PeopleSoftCompIntfcAdapter
```

使用上の注意

PeopleSoft コンポーネントインタフェースアダプタは、PeopleSoft コンポーネントインタフェースでメソッドの呼び出しとプロパティーの設定を行うことで、ユーザーのプロビジョニングを実行します。コンポーネントインタフェースの定義は、PeopleSoft コンポーネントインタフェース設定オブジェクトに割り当てられます。このオブジェクトは、デバッグページまたは [IDMIDE テキストエンティティーを定義してください] を使用して変更できます。`$WSHOME/sample/PeopleSoftComponentInterfaces.xml` ファイルのコピーを編集して、編集したファイルを Identity Manager に読み込むこともできます。

このアダプタを使用したコンポーネントインタフェースの設定と実装の詳細については、次の各節を参照してください。

- 321 ページの「コンポーネントインタフェースマップの定義」
- 324 ページの「USER_PROFILE コンポーネントインタフェースへの FIND メソッドのサポートの追加」

- 325 ページの「PeopleSoft コンポーネントインタフェースのリソースオブジェクト」

コンポーネントインタフェースマップの定義

コンポーネントインタフェースマップには、アダプタで使用できるコンポーネントインタフェースのリストが含まれています。

- interfaces オブジェクト。コンポーネントインタフェースのリストを含みます。カスタムコンポーネントインタフェースがある場合は、マップに独自のコンポーネントインタフェースの定義を定義します。PeopleSoft コンポーネントインタフェース設定オブジェクトを編集し、定義を追加オブジェクトとして <Attribute name='interfaces'> 要素の下の <List> 要素に追加します。

使用可能なコンポーネントインタフェースは、それぞれ独自の定義を持っています。コンポーネントインタフェースの定義の主要な要素は次のとおりです。

- name。コンポーネントインタフェースのラベル。多くの場合、componentInterface 属性の値と一致しますが、これは必要条件ではありません。この値は、アダプタの「リソースパラメータ」ページのドロップダウンメニューに表示されます。
- componentInterface 属性。PeopleSoft で定義されたコンポーネントインタフェースの名前。
- getKey 属性。PeopleSoft の GET 操作を実行するときに設定されるコンポーネントインタフェースプロパティーの名前。getKey が定義されていない場合は、key 属性が代わりに使用されます。
- findKey 属性。PeopleSoft の FIND 操作を実行するときに設定されるコンポーネントインタフェースプロパティーの名前。findKey が定義されていない場合は、key 属性が代わりに使用されます。
- createKey 属性。PeopleSoft の CREATE 操作を実行するときに設定されるコンポーネントインタフェースプロパティーの名前。createKey が定義されていない場合は、key 属性が代わりに使用されます。
- key 属性。非推奨です。代わりに、getKey、findKey、または createKey を使用します。
- properties 属性。PeopleSoft コンポーネントインタフェースから読み取りまたは設定を行うことができるプロパティーのリスト。

  properties リスト内の各オブジェクトには、次の属性が必要です。

  - name。プロパティーの名前。これは、componentInterface プロパティーで識別される PeopleSoft コンポーネントインタフェースによって公開されたプロパティーの名前と正確に一致する必要があります。プロパティーの名前は、リソースユーザー属性の候補として「アカウント属性」ページのリストに表示されます。

これがコレクションプロパティーである場合は、追加属性を定義してください。コレクションプロパティーは、そのキープロパティーと、独自の入れ子構造を持つ単純プロパティーまたは複合プロパティー、あるいはその両方のセットを定義します。

- `isCollection` 属性。プロパティーがコレクションである場合は、この属性を true に設定します。
- `key` 属性。プロパティーがコレクションである場合は、この属性を、コレクションの各項目を一意に識別するプロパティーの名前に設定します。
- `properties` 属性。コレクションの各項目について読み取りまたは設定を実行できるプロパティーのリスト。任意の複雑さをサポートするために、このリストの各メンバーは、親と同じ許可された属性を持つオブジェクトになっています。つまり、リストには、メンバーごとに固有の `name`、`isCollection`、`key`、および `properties` 属性を含めることができます。

`disableRule` 属性。ユーザー無効状態を判定および設定するためのロジックを定義するオブジェクト。この属性には次の属性が含まれています。

- `property` 属性。確認するプロパティー。この値を、`componentInterface` オブジェクトの `properties` 属性に一覧表示します。
- `trueValue` 属性。ユーザーが無効になっていることを示す値。
- `falseValue` 属性。ユーザーが有効になっていることを示す値。

`supportedObjectTypes` 属性。アダプタを通してアクセス可能な、Identity Manager リソースオブジェクトタイプのリスト。各オブジェクトは一連の機能を定義します。

- `features` 属性。サポートされている機能のリスト。使用可能な機能のタイプには、表示、取得、一覧表示、検索、作成、名前を付けて保存、更新、名前の変更、および削除があります。

デフォルトでサポートされるコンポーネントインタフェース

デフォルトのコンポーネントインタフェース設定オブジェクトは、次のインタフェースを定義します。

- USER_PROFILE.。create、read、および update アクションを実行します。
- DELETE_USER_PROFILE.。ユーザーアカウントを削除します。
- ROLE_MAINT。PeopleSoft のロールのサポートを追加します。

USER_PROFILE コンポーネントインタフェース

デフォルトの USER_PROFLE コンポーネントインタフェース定義は、create、read、および update アクションの実行に使用されます。USER_PROFILE コンポーネントインタフェースが GETKEYS キーと FINDKEYS キーに対して UserID フィールドを割り当てるため、`key` 属性と `findKey` 属性は UserID に設定されます。

USER_PROFILE コンポーネントインタフェースのデフォルトの定義によって、使用可能なすべてのプロパティーが定義されているわけではありません。サンプルユーザーフォーム中で使用されているものを含むように簡素化されています。「アカウント属性」ページにほかのリソースユーザー属性を追加する必要がある場合は、まずコンポーネントインタフェース定義を更新する必要があります。コンポーネントインタフェース定義のリストに記載されていないリソースユーザー属性は、そのページに追加できません。

USER_PROFILE に定義されているほとんどのプロパティーは、単純なオブジェクトです。ただし、IDTypes オブジェクトと Roles オブジェクトはコレクションであり、複数の値を持つ可能性があります。IDTypes には、固有の属性のコレクションが含まれています。これらのオブジェクトには、`isCollection` 属性、コレクションのキー名、および少なくとも 1 つのプロパティーを含めてください。

DELETE_USER_PROFILE コンポーネントインタフェース

DELETE_USER_PROFILE コンポーネントインタフェース定義は、ユーザープロファイル定義を削除するために使用されます。OPRID キーは、削除するユーザープロファイルを決定します。このコンポーネントインタフェースにはプロパティーがないため、定義には何も表示されません。

ROLE_MAINT コンポーネントインタフェース

ROLE_MAINT コンポーネントインタフェース定義は、ロールリソースオブジェクトを一覧表示するように Identity Manager を設定する方法を示したサンプル実装の一部です。次に示す一般的なガイドラインに従って、ROLE_MAINT の例を実際の要件に合わせて変更することにより、ほかのリソースオブジェクトを一覧表示できます。

注 – PeopleSoft コンポーネントインタフェースアダプタは、リソースオブジェクトの一覧表示のみをサポートします。ほかのオブジェクト機能 (更新、作成、削除など) はサポートしません。

ROLE_MAINT コンポーネントインタフェース定義には、次の重要な特性があります。

- ROLENAME が FINDKEYS と GETKEYS の主キーであるため、`findKey` 属性と `getKey` 属性は ROLENAME に割り当てられます。
- DESCR と ROLESTATUS も FINDKEYS のキーですが、これらは主キーではないため、`findKey` の値としては表示されません。代わりに、これらは `properties` セクションに表示されます。
- `supportedObjectTypes` 属性は、Role オブジェクトを定義します。Role オブジェクトは検索機能と取得機能をサポートします。

USER_PROFILE コンポーネントインタフェースへの FIND メソッドのサポートの追加

デフォルトの USER_PROFILE コンポーネントインタフェースは、FIND メソッドをサポートしません。ただし、PeopleSoft コンポーネントインタフェースアダプタでアカウントの反復とリストをサポートするには、FIND メソッドが必要になります。

既存の USER_PROFILE コンポーネントに FIND メソッドのサポートを追加するには、次の手順を使用します。

▼ FIND メソッドのサポートを追加する

1. **USER_PROFILE** コンポーネントインタフェースを **PeopleSoft Application Designer** にロードします。

2. **USERMAINT** コンポーネントを表示している左側のウィンドウで、**PSOPRDEFN_SRCH** オブジェクトの下にある「**OPRID**」フィールドを選択します。

   このフィールドを、USER_PROFILE CI を表示している右側のウィンドウにドラッグします。

   フィールドをドロップすると、USER_PROFILE CI に新しいキー「FINDKEYS」が作成されます。そのキーの下に、サブキー「OPRID」があります。

3. **FINDKEYS** の下の **OPRID** 名を右クリックし、「**Edit Name**」を選択します。名前を **UserID** に変更します。

4. **USER_PROFILE CI** を右クリックし、「**Component Interface Properties**」を選択します。「**Standard Methods**」タブを選択し、「**Find**」チェックボックスを選択します。「**OK**」をクリックして「**Component Interface Properties**」ダイアログを閉じます。

5. **USER_PROFILE** コンポーネントインタフェースに対する変更を保存します。

   コンポーネントインタフェースの「METHODS」フィールドに、Find メソッドが表示されます。新しい FIND メソッドの機能を確認するため、コンポーネントインタフェースを右クリックし、「**Test Component Interface**」を選択します。

注 – PeopleSoft 管理者は、Create、Get、Save、および SetPassword の各メソッドに加え、コンポーネントインタフェースの Find メソッドに対してもフルアクセスを与えなければなりません。

PeopleSoft コンポーネントインタフェースのリソースオブジェクト

PeopleSoft コンポーネントインタフェースリソースの XML を編集することにより、リソースオブジェクトを管理できます。ObjectType 要素を追加するには、デバッグページまたは [IDMIDE テキストエンティティーを定義してください] を使用します。

たとえば、Role リソースオブジェクトのサポートを追加するには、このような ObjectType 要素を追加します。

```
<ObjectTypes>
<ObjectType name='Role' icon='role'>
   <ObjectFeatures>
      <ObjectFeature name='find'/>
   </ObjectFeatures>
   <ObjectAttributes idAttr='ROLENAME' displayNameAttr='ROLENAME' descriptionAttr='DESCR'>
      <ObjectAttribute name='ROLENAME' type='string'/>
      <ObjectAttribute name='DESCR' type='string'/>
      <ObjectAttribute name='ROLESTATUS' type='string'/>
   </ObjectAttributes>
</ObjectType>
</ObjectTypes>
```

ObjectType name (たとえば、Role) は、ただ 1 つのコンポーネントインタフェース定義の supportedObjectTypes リストに含まれるいずれかのオブジェクトの名前と一致する必要があります。各 ObjectFeature (たとえば、find) は、その同じ supportedObjectTypes の features リストでの対応する機能を持っている必要があります。一致するコンポーネントインタフェースは、そのリソース機能を実行するために使用されるコンポーネントインタフェースになります。複数に一致する場合は、最初に一致したものが使用されます。

次の例は、コンポーネントインタフェースマップに含まれる ROLE_MAINT コンポーネントインタフェースのコンポーネントインタフェース定義の一部です。オブジェクト名 Role が見つかり、機能リスト内の項目の 1 つは find という名前です。

```
<Attribute name='supportedObjectTypes' >
   <List>
      <Object name='Role'>
         <Attribute name='features' >
            <List>
               <Object name='find' />
               <Object name='get' />
            </List>
         </Attribute>
      </Object>
   </List>
</Attribute>
```

ユーザーフォーム

次のユーザーフォームフラグメントを使用して、PeopleSoft ロールのリストを検出できます。ROLENAME 属性と DESCR 属性が取得されます。

```
<invoke name='getResourceObjects' class='com.waveset.ui.FormUtil'>
   <ref>:display.session</ref>
   <s>Role</s>
   <s>PeopleSoft Component Interface</s>
   <map>
      <s>searchAttrsToGet</s>
      <list>
         <s>ROLENAME</s>
         <s>DESCR</s>
      </list>
    </map>
</invoke>
```

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は、Client Connection Toolkit (読み取り/書き込み) を使用してこのアダプタと通信します。

必要な管理特権

PeopleSoft に接続するユーザーを、管理対象のコンポーネントインタフェースのメソッドにアクセスできる PeopleSoft ロールに割り当てる必要があります。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの作成	あり
アカウントの更新	あり
アカウントの削除	あり

機能	サポート状況
アカウントの有効化/無効化	コンポーネントインタフェースマップに有効化/無効化のロジックが定義されている場合は、使用可
パスワードの更新	あり
アカウントの名前の変更	なし
パススルー認証	なし
前アクションと後アクション	なし
データ読み込みメソッド	■ リソースから直接インポート ■ 調整

アカウント属性

PeopleSoft コンポーネントインタフェースリソースのアカウント属性は、管理対象のコンポーネントインタフェースに依存します。

スキーママップの各エントリには、コンポーネントインタフェースマップ内のコンポーネントインタフェースに対して定義された、「properties」リスト中のいずれかのエントリに一致するリソースユーザー属性名があるはずです。スキーママップの編集時に「設定のテスト」ボタンをクリックすると、該当する一致を確認できます。

リソースユーザー属性名がコンポーネントインタフェースマップ内のコレクションプロパティーと一致する場合、アカウント属性の値はそのコレクションの XML 文字列表現になります。コレクションプロパティーの操作例については、サンプルユーザーフォームフィールド `accounts[PeopleSoft Component Interface].ps_roles` を参照してください。

注 – 新しいリソースインスタンスに対して定義されるデフォルトのスキーママップエントリは、デフォルトの USER_PROFILE および DELETE_USER_PROFILE コンポーネントインタフェースマップと使用する場合のみに対応します。これらのマップを変更したり、独自のマップを作成したりする場合は、それに応じてスキーママップを変更してください。

すべてのアカウント属性のタイプは String です。

Identity Manager ユーザー属性	リソースユーザー属性	説明
description	UserDescription	ユーザーの説明。
symbolicId	SymbolicID	必須。ユーザーの記号 ID。
idTypes	IDTypes	ユーザーに割り当てられたユーザータイプのリスト。
ps_roles	ロール	ユーザーに割り当てられたルールのリスト。
email	EmailAddress	ユーザーの電子メールアドレス。この属性は、古い PeopleTools リリースでのみ使用できます。この属性は、デフォルトではスキーママップ内に存在しません。
EmailAddresses	EmailAddresses	ユーザーの電子メールアドレスのリスト。この属性は、PeopleTools の 8.4x リリースでのみ使用できます。この属性は、デフォルトではスキーママップ内に存在しません。

リソースオブジェクトの管理

なし

アイデンティティーテンプレート

```
$accountId$
```

サンプルフォーム

次のフォームは、`$WSHOME/sample/forms` ディレクトリにあります。

- `PeopleSoftCompIntfcUserForm.xml`

  このユーザーフォームは、USER_PROFILE コンポーネントインタフェースが管理され、デフォルトアカウント属性が使用されている場合にのみ、期待どおりに機能します。このフォームは、スキーママップに `email` アカウント属性が追加されていることを前提としています。

  EmailAddress 属性は、古い PeopleTools リリースでのみ使用できます。USER_PROFILE が EmailAddress 属性をサポートしているかどうかは、PropleTools の管理者に確認してください。

  別のコンポーネントインタフェースを管理している場合や、別のスキーママップを使用している場合は、それに応じてユーザーフォームも変更する必要があります。

- `PeopleSoft_8_4X_CompIntfcUserForm.xml`

  このユーザーフォームは、USER_PROFILE コンポーネントインタフェースが管理されている場合にのみ期待どおりに機能します。このフォームは、スキーママップに EmailAddresses アカウント属性が追加されていることを前提としています。

  EmailAddresses 属性は、PeopleTools の新しい 8.4x リリースでのみ使用可能です。USER_PROFILE が EmailAddresses 属性をサポートしているかどうかは、PropleTools の管理者に確認してください。

トラブルシューティング

デバッグページを使用して、次のクラスでトレースオプションを設定します。

`com.waveset.adapter.PeopleSoftCompIntfcAdapter`

◆ ◆ ◆ 第 29 章

29 RACF

RACF リソースアダプタは、OS/390 メインフレーム上のユーザーアカウントとメンバーシップの管理をサポートします。このアダプタは、TN3270 エミュレータセッションで RACF を管理します。

RACF リソースアダプタは、`com.waveset.adapter.RACFResourceAdapter` クラスで定義されます。

アダプタの詳細

リソースを設定する際の注意事項

なし

Identity Manager のインストールに関する注意事項

RACF リソースアダプタは、カスタムアダプタです。インストールプロセスを完了するには、次の手順を実行する必要があります。

▼ RACF リソースアダプタをインストールする

1 **RACF** リソースを **Identity Manager** のリソースリストに追加するには、「管理するリソースの設定」ページの「カスタムリソース」セクションに次の値を追加する必要があります。

```
com.waveset.adapter.RACFResourceAdapter
```

2 適切な **JAR** ファイルを **Identity Manager** インストールの `WEB-INF/lib` ディレクトリにコピーします。

コネクションマネージャー	**JAR** ファイル
Host On Demand	IBM Host Access Class Library (HACL) は、メインフレームへの接続を管理します。HACL を含む推奨 JAR ファイルは `habeans.jar` です。これは、HOD に付属する HOD Toolkit (または Host Access Toolkit) とともにインストールされます。HACL のサポートされるバージョンは、HOD V7.0、V8.0、V9.0、および V10 に含まれるバージョンです。 habeans.jar ファイル ただし、このツールキットを利用できない場合は、HOD のインストールに含まれる次の JAR ファイルを `habeans.jar` の代わりに使用できます。 ■ `habase.jar` ■ `hacp.jar` ■ `ha3270.jar` ■ `hassl.jar` ■ `hodbase.jar` 詳細は、http://www.ibm.com/software/webservers/hostondemand/ を参照してください。
Attachmate WRQ	Sun 製品向け Attachmate 3270 メインフレームアダプタには、メインフレームへの接続の管理に必要なファイルが含まれます。 ■ `RWebSDK.jar` ■ `wrqtls12.jar` ■ `profile.jaw` この製品の入手については、Sun プロフェッショナルサービスにお問い合わせください。

3 `Waveset.properties` ファイルに次の定義を追加して、端末セッションを管理するサービスを定義します。

```
serverSettings.serverId.mainframeSessionType=
Valueserver Settings.default.mainframeSessionType=Value
```

Value は、次のように設定できます。

- 1 は、IBM Host On-Demand (HOD) を表します。
- 3 は、Attachmate WRQ を表します。

これらのプロパティーが明示的に設定されていなければ、Identity Manager はまず WRQ を使用し、次に HOD を使用します。

4 **Attachmate** ライブラリが **WebSphere** または **WebLogic** アプリケーションサーバーにインストールされている場合は、`com.wrq.profile.dir=`*LibraryDirectory* プロパティーを `WebSphere/AppServer/configuration/config.ini` または `startWeblogic.sh` ファイルに追加します。

これにより、Attachmate コードでライセンスファイルを検索できます。

5 `Waveset.properties` ファイルに加えた変更を有効にするために、アプリケーションサーバーを再起動します。

6 リソースへの **SSL** 接続の設定については、第 **53** 章「メインフレーム接続」を参照してください。

使用上の注意

ここでは、RACF リソースアダプタの使用に関する情報を示します。 次のトピックで構成されています。

管理者

TSO セッションでは、同時に複数の接続は許可されません。Identity Manager RACF 操作の同時実行を実現するには、複数の管理者を作成します。たとえば、2 人の管理者を作成すると、2 つの Identity Manager RACF 操作を同時に実行できます。少なくとも 2 人 (できれば 3 人) の管理者を作成するようにしてください。

クラスタ環境で実行する場合、クラスタ内のサーバーごとに管理者を定義する必要があります。これは、各サーバーの管理者が同じ管理者である場合にも適用されます。TSO では、クラスタ内のサーバーごとに異なる管理者が必要です。

クラスタリングを使用していない場合は、すべての行でサーバー名は Identity Manager のホストマシンの名前となります。

注 – ホストリソースアダプタは、同じホストに接続している複数のホストリソースでの親和性管理者に対して最大接続数を強制しません。代わりに、各ホストリソース内部の親和性管理者に対して最大接続数が強制されます。

同じシステムを管理する複数のホストリソースがあり、現在それらが同じ管理者アカウントを使用するように設定されている場合は、同じ管理者がリソースに対して同時に複数のアクションを実行しようとしていないことを確認するために、それらのリソースを更新しなければならない可能性があります。

追加セグメントのサポート

RACF アダプタは、デフォルトでサポートされているセグメントには含まれない属性をサポートするように設定できます。

▼ 属性をサポートするように RACF アダプタを設定する

1. セグメントを解析する **AttrParse** オブジェクトを作成します。カスタム **AttrParse** オブジェクトについては、第 49 章「AttrParse オブジェクトの実装」を参照してください。**AttrParse** オブジェクトの例は、`$WSHOME/web/sample/attrparse.xml` に定義されています。

2. `ResourceAttribute` 要素を **RACF** リソースオブジェクトに追加します。たとえば、次のようにします。

```
<ResourceAttribute name='WORKATTR Segment AttrParse'
   displayName='WORKATTR Segment AttrParse'
   description='AttrParse for WORKATTR Segment'
   value='Default RACF WORKATTR Segment AttrParse'>
</ResourceAttribute>
```

   この例では、`WORKATTR Segment AttrParse` というラベルのフィールドが「リソースパラメータ」ページに追加されます。`name` 属性に割り当てられる値は、*SegmentName* `Segment AttrParse` という形式である必要があります。

3. カスタムアカウント属性を定義する要素を **RACF** リソースオブジェクトに追加します。

```
<AccountAttributeType id='32' name='WORKATTR Account' syntax='string'
  mapName='WORKATTR.WAACCNT' mapType='string'>
</AccountAttributeType>
```

   `mapName` 属性の値は、SegmentName.AttributeName という形式である必要があります。アダプタがこの形式の `mapName` を検出すると、指定されたセグメントを RACF に対して要求し、*SegmentName* Segment AttrParse フィールドに指定されたオブジェクトを使用して解析します。

リソースアクション

RACF アダプタでは、login および logoff のリソースアクションが必要です。login アクションは、認証されたセッションに関してメインフレームとネゴシエーションを行います。logoff アクションは、そのセッションが不要になったときに接続を解除します。

login リソースアクションおよび logoff リソースアクションの作成については、565 ページの「メインフレームの例」を参照してください。

SSL 設定

Identity Manager は TN3270 接続を使用してリソースと通信します。

RACF リソースへの SSL 接続の設定については、第 53 章「メインフレーム接続」を参照してください。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は、TN3270 を使用して RACF アダプタと通信します。

必要な管理特権

ユーザープロファイル (ユーザー自身のものを含む) の非ベースセグメント内の情報を定義または変更するには、SPECIAL 属性または少なくともフィールドレベルのアクセスチェックを介したセグメントの UPDATE 権限を持っている必要があります。

ユーザープロファイルの内容またはユーザープロファイルの個々のセグメントの内容を一覧表示するには、LISTUSER コマンドを使用します。

ユーザープロファイル (ユーザー自身のものを含む) の非ベースセグメント内の情報を表示するには、SPECIAL 属性か AUDITOR 属性、または少なくともフィールドレベルのアクセスチェックを介したセグメントの READ 権限を持っている必要があります。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	あり
パススルー認証	なし
前アクションと後アクション	あり
データ読み込みメソッド	■ リソースから直接インポート ■ 調整

アカウント属性

次の表に、RACF アカウント属性に関する情報を示します。

リソースユーザー属性	データ型	説明
GROUPS	String	ユーザーに割り当てられたグループ
GROUP-CONN-OWNERS	String	グループ接続所有者
USERID	String	必須。ユーザーの名前
MASTER CATALOG	String	マスターカタログ
USER CATALOG	String	ユーザーカタログ
CATALOG ALIAS	String	カタログ別名
OWNER	String	プロファイルの所有者
NAME	String	ユーザーの名前
DATA	String	インストール定義データ
DFLTGRP	String	ユーザーのデフォルトグループ
EXPIRED	Boolean	パスワードを期限切れにするかどうかを示します。
PASSWORD INTERVAL	String	パスワード間隔
TSO.Delete Segment	Boolean	このフィールドを true に設定すると、TSO Segment が RACF ユーザーから削除されます。
TSO.ACCTNUM	String	ログオン時に使用されるユーザーのデフォルトの TSO アカウント番号
TSO.COMMAND	String	ログオン時のデフォルトのコマンド

リソースユーザー属性	データ型	説明
TSO.HOLDCLASS	String	ユーザーのデフォルトの TSO 保持クラス
TSO.JOBCLASS	String	ユーザーのデフォルトの TSO ジョブクラス
TSO.MAXSIZE	Int	ユーザーがログオン中に要求できる最大 TSO 領域サイズ
TSO.MSGCLASS	String	ユーザーのデフォルトの TSO メッセージクラス
TSO.PROC	String	ユーザーのデフォルトの TSO ログオン手順の名前
TSO.SIZE	Int	ユーザーがログオン中に領域サイズを要求しない場合の最小 TSO 領域サイズ
TSO.SYSOUTCLASS	String	ユーザーのデフォルトの TSO SYSOUT クラス
TSO.UNIT	String	手順による割り当てに使用される TSO デバイスまたはデバイスグループのデフォルトの名前
TSO.USERDATA	String	インストール定義データ
OMVS.ASSIZEMAX	Int	ユーザーの OMVS RLIMIT_AS (最大アドレス空間サイズ)
OMVS.CPUTIMEMAX	Int	ユーザーの OMVS RLIMIT_CPU (最大 CPU 時間)
OMVS.FILEPROCMAX	Int	ユーザーの OMVS プロセスあたりの最大ファイル数
OMVS.HOME	String	ユーザーの OMVS ホームディレクトリパス名
OMVS.MMAPAREAMAX	Int	ユーザーの OMVS 最大メモリーマップサイズ
OMVS.PROCUSERMAX	Int	ユーザーの OMVS UID あたりの最大プロセス数
OMVS.PROGRAM	String	ユーザーの初期 OMVS シェルプログラム
OMVS.THREADSMAX	Int	ユーザーの OMVS プロセスあたりの最大スレッド数
OMVS.UID	String	ユーザーの OMVS ユーザー識別子
CICS.OPCLASS	String	ユーザーが BMS (基本マッピングサポート) メッセージを受信する CICS オペレータクラス
CICS.OPIDENT	String	ユーザーの CICS オペレータ識別子
CICS.OPPRTY	String	ユーザーの CICS オペレータ優先順位
CICS.TIMEOUT	String	ユーザーがアイドル状態になってから CICS によってサインオフされるまでの時間
CICS.XRFSOFF	String	XRF 引き継ぎの発生時にユーザーが CICS によってサインオフされるかどうかを示す設定

リソースユーザー属性	データ型	説明
NETVIEW.CONSNAME	String	MCS コンソール識別子
NETVIEW.CTL	String	GLOBAL、GENERAL、または SPECIFIC コントロールを指定します。
NETVIEW.DOMAINS	String	ドメイン識別子
NETVIEW.IC	String	NetView オペレータがログインしたときにこの NetView によって実行される初期コマンドまたはコマンドリスト
NETVIEW.MSGRECVR	String	オペレータが非送信請求メッセージを受信するかどうかを示します (NO または YES)
NETVIEW.NGMFADMN	String	このオペレータが NetView グラフィックモニター機能を使用できるかどうかを示します (NO または YES)
NETVIEW.NGMFVSPN	String	
NETVIEW.OPCLASS	String	オペレータのクラス

アイデンティティーテンプレート

```
$accountId$
```

サンプルフォーム

組み込みのフォーム

なし

その他の利用可能なフォーム

RACFUserForm.xml

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

- com.waveset.adapter.RACFResourceAdapter
- com.waveset.adapter.HostAccess

◆ ◆ ◆ 第 30 章

30 RACF LDAP

RACF LDAP リソースアダプタは、OS/390 メインフレーム上のユーザーアカウントとメンバーシップの管理をサポートします。可能であれば、アダプタは z/OS Security Server に含まれる LDAP サーバーに接続し、ユーザーアカウントを管理します。その他すべての機能は、RACF システムへの標準的な呼び出しによって処理されます。

RACF LDAP リソースアダプタは、`com.waveset.adapter.RACF_LDAPResourceAdapter` クラスで定義されます。

このアダプタは、LDAP リソースアダプタを拡張します。LDAP 機能の実装については、LDAP アダプタのマニュアルを参照してください。

アダプタの詳細

Identity Manager のインストールに関する注意事項

RACF リソースアダプタは、カスタムアダプタです。インストールプロセスを完了するには、次の手順を実行する必要があります。

▼ RACF リソースアダプタをインストールする

1. **RACF LDAP** リソースを **Identity Manager** のリソースリストに追加するには、「管理するリソースの設定」ページの「カスタムリソース」セクションに次の値を追加する必要があります。

   ```
   com.waveset.adapter.RACF_LDAPResourceAdapter
   ```

2. 適切な **JAR** ファイルを **Identity Manager** インストールの `WEB-INF/lib` ディレクトリにコピーします。

コネクションマネージャー	JAR ファイル
Host On Demand	IBM Host Access Class Library (HACL) は、メインフレームへの接続を管理します。HACL を含む推奨 JAR ファイルは habeans.jar です。これは、HOD に付属する HOD Toolkit (または Host Access Toolkit) とともにインストールされます。HACL のサポートされるバージョンは、HOD V7.0、V8.0、V9.0、および V10 に含まれるバージョンです。 habeans.jar ファイル ただし、このツールキットを利用できない場合は、HOD のインストールに含まれる次の JAR ファイルを habeans.jar の代わりに使用できます。 ■ habase.jar ■ hacp.jar ■ ha3270.jar ■ hassl.jar ■ hodbase.jar 詳細は、http://www.ibm.com/software/webservers/hostondemand を参照してください。
Attachmate WRQ	Sun 製品向け Attachmate 3270 メインフレームアダプタには、メインフレームへの接続の管理に必要なファイルが含まれます。 ■ RWebSDK.jar ■ wrqtls12.jar ■ profile.jaw この製品の入手については、Sun プロフェッショナルサービスにお問い合わせください。

3 Waveset.properties ファイルに次の定義を追加して、端末セッションを管理するサービスを定義します。

```
serverSettings.serverId.mainframeSessionType=
Valueserver Settings.default.mainframeSessionType=Value
```

Value は、次のように設定できます。

- 1 は IBM Host On--Demand (HOD) を示します。
  - 3 は、Attachmate WRQ を表します。

    これらのプロパティーを明示的に設定しない場合、Identity Manager は WRQ、HOD の順に使用を試みます。

4 **Attachmate** ライブラリが **WebSphere** または **WebLogic** アプリケーションサーバーにインストールされている場合は、`com.wrq.profile.dir=`*LibraryDirectory* プロパティーを `WebSphere/AppServer/configuration/config.ini` または `startWeblogic.sh` ファイルに追加します。
これにより、Attachmate コードでライセンスファイルを検索できます。

5 `Waveset.properties` ファイルに加えた変更を有効にするために、アプリケーションサーバーを再起動します。

6 リソースへの **SSL** 接続の設定については、第 **53** 章「メインフレーム接続」を参照してください。

使用上の注意

管理者

TSO セッションでは、同時に複数の接続は許可されません。Identity Manager RACF 操作の同時実行を実現するには、複数の管理者を作成します。たとえば、2 人の管理者を作成すると、2 つの Identity Manager RACF 操作を同時に実行できます。少なくとも 2 人 (できれば 3 人) の管理者を作成するようにしてください。

クラスタ環境で実行する場合、クラスタ内のサーバーごとに管理者を定義する必要があります。これは、各サーバーの管理者が同じ管理者である場合にも適用されます。TSO では、クラスタ内のサーバーごとに異なる管理者が必要です。

クラスタリングを使用していない場合は、すべての行でサーバー名は Identity Manager のホストマシンの名前となります。

注 – ホストリソースアダプタは、同じホストに接続している複数のホストリソースでの親和性管理者に対して最大接続数を強制しません。代わりに、各ホストリソース内部の親和性管理者に対して最大接続数が強制されます。

同じシステムを管理する複数のホストリソースがあり、現在それらが同じ管理者アカウントを使用するように設定されている場合は、同じ管理者がリソースに対して同時に複数のアクションを実行しようとしていないことを確認するために、それらのリソースを更新しなければならない可能性があります。

追加セグメントのサポート

RACF LDAP アダプタは、デフォルトでサポートされているセグメントには含まれない属性をサポートするように設定できます。

▼ 属性をサポートするように RACF LDAP リソースアダプタを設定する

1 セグメントを解析する **AttrParse** オブジェクトを作成します。カスタム **AttrParse** オブジェクトについては、第 49 章「AttrParse オブジェクトの実装」を参照してください。**AttrParse** オブジェクトの例は、`$WSHOME/web/sample/attrparse.xml` に定義されています。

2 `ResourceAttribute` 要素を **RACF LDAP** リソースオブジェクトに追加します。たとえば、次のようにします。

```
<ResourceAttribute name='OMVS Segment AttrParse' displayName='OMVS Segment AttrParse'
   description='AttrParse for OMVS Segment' value='Default RACF OMVS Segment AttrParse'>
</ResourceAttribute>
```

この例では、`OMVS Segment AttrParse` というラベルのフィールドが「リソースパラメータ」ページに追加されます。`name` 属性に割り当てられる値は、*SegmentName* `Segment AttrParse` という形式である必要があります。

3 カスタムアカウント属性を定義する要素を **RACF LDAP** リソースオブジェクトに追加します。

```
<AccountAttributeType id='32' name='OMVS Mem Max Area Size' syntax='int'
  mapName='OMVS.MMAPAREAMAX' mapType='int'>
</AccountAttributeType>
```

`mapName` 属性の値は、SegmentName.AttributeName という形式である必要があります。アダプタがこの形式の `mapName` を検出すると、指定されたセグメントをリソースに対して要求し、*SegmentName* Segment AttrParse フィールドに指定されたオブジェクトを使用して解析します。

リソースアクション

RACF LDAP アダプタでは、login および logoff のリソースアクションが必要です。login アクションは、認証されたセッションに関してメインフレームとネゴシエーションを行います。logoff アクションは、そのセッションが不要になったときに接続を解除します。

login リソースアクションおよび logoff リソースアクションの作成については、565 ページの「メインフレームの例」を参照してください。

リソースを設定する際の注意事項

Z/OS Security Server は、RACF アカウントのソースとして機能するマシンと同じマシン上にインストールされる必要があります。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は TN3270 接続を使用してリソースと通信します。

RACF LDAP リソースへの SSL 接続の設定については、第 53 章「メインフレーム接続」を参照してください。

必要な管理特権

RACF LDAP リソースと接続する管理者には、RACF ユーザーの作成と管理を行うための十分な特権が与えられている必要があります。

「User DN」リソースパラメータフィールドで指定されたユーザーに、ユーザーの読み取り、書き込み、削除、および追加のアクセス権を付与する必要があります。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	あり
パススルー認証	なし
前アクションと後アクション	あり
データ読み込みメソッド	■ リソースから直接インポート ■ リソースの調整

アカウント属性

属性の構文 (または型) は、通常、属性がサポートされるかどうかを決定します。一般に、Identity Manager は Boolean 型、文字列型、整数型、およびバイナリ型の構文をサポートします。バイナリ属性は、バイト配列としてのみ安全に表現できる属性です。

次の表に、サポートされている LDAP 構文の一覧を示します。ほかの LDAP 構文でも、事実上 Boolean 型、文字列型、または整数型であれば、サポートされる可能性があります。オクテット文字列はサポートされません。

LDAP 構文	属性タイプ	オブジェクト ID
Audio	Binary	1.3.6.1.4.1.1466.115.121.1.4
Binary	Binary	1.3.6.1.4.1.1466.115.121.1.5
Boolean	Boolean	1.3.6.1.4.1.1466.115.121.1.7
Country String	String	1.3.6.1.4.1.1466.115.121.1.11
DN	String	1.3.6.1.4.1.1466.115.121.1.12
Directory String	String	1.3.6.1.4.1.1466.115.121.1.15
Generalized Time	String	1.3.6.1.4.1.1466.115.121.1.24
IA5 String	String	1.3.6.1.4.1.1466.115.121.1.26
Integer	Int	1.3.6.1.4.1.1466.115.121.1.27
Postal Address	String	1.3.6.1.4.1.1466.115.121.1.41
Printable String	String	1.3.6.1.4.1.1466.115.121.1.44
Telephone Number	String	1.3.6.1.4.1.1466.115.121.1.50

デフォルトのアカウント属性

次の属性が、RACF LDAP リソースアダプタの「アカウント属性」ページに表示されます。

リソースユーザー属性	データ型	説明
racfPassword	暗号化されています	リソースに対するユーザーのパスワード
RACF.GROUPS	String	ユーザーに割り当てられたグループ
RACF.GROUP-CONN-OWNERS	String	グループ接続所有者
RACF.USERID	String	必須。ユーザーの名前
RACF.MASTER CATALOG	String	マスターカタログ
RACF.USER CATALOG	String	ユーザーカタログ
RACF.CATALOG ALIAS	String	カタログ別名
racfOwner	String	プロファイルの所有者
racfProgrammerName	String	ユーザーの名前
racfInstallationData	String	インストール定義データ

リソースユーザー属性	データ型	説明
racfDefaultGroup	String	ユーザーのデフォルトグループ
RACF.EXPIRED	Boolean	パスワードを期限切れにするかどうかを示します。
RACF.PASSWORD INTERVAL	String	パスワード間隔
TSO.Delete Segment	Boolean	このフィールドを true に設定すると、TSO Segment が RACF ユーザーから削除されます。
SAFAccountNumber	String	ログオン時に使用されるユーザーのデフォルトの TSO アカウント番号
SAFDefaultCommand	String	ログオン時のデフォルトのコマンド
SAFHoldClass	String	ユーザーのデフォルトの TSO 保持クラス
SAFJobClass	String	ユーザーのデフォルトの TSO ジョブクラス
SAFMessageClass	String	ユーザーのデフォルトの TSO メッセージクラス
SAFDefaultLoginProc	String	ユーザーのデフォルトの TSO ログオン手順の名前
SAFLogonSize	Int	ユーザーがログオン中に領域サイズを要求しない場合の最小 TSO 領域サイズ
SAFMaximumRegionSize	Int	ユーザーがログオン中に要求できる最大 TSO 領域サイズ
SAFDefaultSysoutClass	String	ユーザーのデフォルトの TSO SYSOUT クラス
SAFDefaultUnit	String	手順による割り当てに使用される TSO デバイスまたはデバイスグループのデフォルトの名前
SAFUserdata	String	インストール定義データ
SAFDefaultCommand	String	TSO のデフォルトのコマンド
racfOmvsUid	String	ユーザーの OMVS ユーザー識別子
racfOmvsHome	String	ユーザーの OMVS ホームディレクトリパス名
racfOmvsInitialProgram	String	ユーザーの初期 OMVS シェルプログラム
racfOmvsMaximumCPUTime	Int	ユーザーの OMVS RLIMIT_CPU (最大 CPU 時間)

リソースユーザー属性	データ型	説明
racfOmvsMaximumAddress SpaceSize	Int	ユーザーの OMVS RLIMIT_AS (最大アドレス空間サイズ)
racfOmvsMaximumFilesPerProcess	Int	ユーザーの OMVS プロセスあたりの最大ファイル数
racfOmvsMaximumProcessesPerUID	Int	ユーザーの OMVS UID あたりの最大プロセス数
racfOmvsMaximumThreadsPerProcess	Int	ユーザーの OMVS プロセスあたりの最大スレッド数
racfOmvsMaximumMemoryMapArea	Int	ユーザーの OMVS 最大メモリーマップサイズ
racfTerminalTimeout	String	ユーザーがアイドル状態になってから CICS によってサインオフされるまでの時間
racfOperatorPriority	String	ユーザーの CICS オペレータ優先順位
racfOperatorIdentification	String	ユーザーの CICS オペレータ識別子
racfOperatorClass	String	ユーザーが BMS (基本マッピングサポート) メッセージを受信する CICS オペレータクラス
racfOperatorReSignon	String	XRF 引き継ぎの発生時にユーザーが CICS によってサインオフされるかどうかを示す設定
racfNetviewOperatorClass	String	オペレータのクラス
NETVIEW.NGMFVSPN	String	NetView Graphic Monitor Facility ビューを表示したり、ビュー内にリソースを表示したりする際の、オペレータの権限を定義します。
racfNGMFADMKeyword	String	このオペレータが NetView グラフィックモニター機能を使用できるかどうかを示します (NO または YES)
racfMessageReceiverKeyword	String	オペレータが非送信請求メッセージを受信するかどうかを示します (NO または YES)
racfNetviewInitialCommand	String	NetView オペレータがログインしたときにこの NetView によって実行される初期コマンドまたはコマンドリスト
racfDomains	String	ドメイン識別子

リソースユーザー属性	データ型	説明
racfCTLKeyword	String	GLOBAL、GENERAL、または SPECIFIC コントロールを指定します。
racfDefaultConsoleName	String	MCS コンソール識別子

デフォルトでサポートされるオブジェクトクラス

デフォルトでは、RACF LDAP リソースアダプタは、LDAP ツリーに新しいユーザーオブジェクトを作成するときに次のオブジェクトクラスを使用します。ほかのオブジェクトクラスが追加される場合もあります。

- racfuser
- racfUserOmvsSegment
- racfCicsSegment
- SAFTsoSegment
- racfNetviewSegment

リソースオブジェクトの管理

なし

アイデンティティーテンプレート

```
$accountId$
```

サンプルフォーム

なし

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

- com.waveset.adapter.RACF_LDAPResourceAdapter
- com.waveset.adapter.LDAPResourceAdapter
- com.waveset.adapter.LDAPResourceAdapterBase

◆ ◆ ◆ 第 31 章

Red Hat Linux および SuSE Linux

Red Hat Linux リソースアダプタと SuSE Linux リソースアダプタは、それぞれ `com.waveset.adapter.RedHatLinuxResourceAdapter` クラスと `com.waveset.adapter.SUSELinuxResourceAdapter` クラスで定義された 2 つの別個のアダプタです。

アダプタの詳細

リソースを設定する際の注意事項

リソースと Identity Manager 間の通信に SSH (Secure Shell) を使用する場合は、アダプタを設定する前に、リソースで SSH を設定します。

Identity Manager のインストールに関する注意事項

このリソースでは、追加のインストール手順は必要ありません。

使用上の注意

Linux リソースアダプタは、主に次のコマンドのサポートを提供します。

- `useradd`、`usermod`、 `userde1`
- `groupadd`、`groupmod`、 `groupdel`
- `passwd`

サポートされる属性およびファイルの詳細については、これらのコマンドに関する Linux マニュアルページを参照してください。

Linux リソースでユーザーアカウントのの変更を実行すると、グループメンバーシップは新しいユーザー名に移動されます次の条件に該当する場合は、ユーザーのホームディレクトリの名前も変更されます。

- 元のホームディレクトリの名前がユーザー名と一致していた。
- 新しいユーザー名と一致するディレクトリがまだ存在していない。

Linux リソースに接続するときは、root シェルとして Bourne Shell 準拠のシェル (sh, ksh) を root シェルとして Bourne 互換シェル (sh、ksh) を使用してください。

Linux アカウントを管理する管理アカウントは、英語 (en) または C ロケールを使用する必要があります。これは、ユーザーの .profile ファイルで設定できます。ユーザーのパスワードには制御文字 (たとえば、0x00 や 0x7f) を使用しないでください。

NIS が実装されている環境では、次の機能を実装することにより、一括プロビジョニング中のパフォーマンスを向上させることができます。

- `user_make_nis` という名前のアカウント属性をスキーママップに追加し、この属性を調整やその他の一括プロビジョニングワークフローで使用します。この属性を追加した場合、リソース上の各ユーザーが更新された後は、システムで NIS データベースへの接続手順がバイパスされます。
- すべてのプロビジョニングが完了した後で NIS データベースに変更を書き込むには、ワークフローで `NIS_password_make` という名前の ResourceAction を作成します。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は、次の接続を使用してこのアダプタと通信できます。

- Telnet
- SSH (SSH はリソース上に個別にインストールする)
- SSHPubKey

SSHPubKey 接続の場合、「リソースパラメータ」ページで非公開鍵を指定する必要があります。この鍵には `--- BEGIN PRIVATE KEY ---` および `--- END PRIVATE KEY --` のような注釈行を含める必要があります。公開鍵は、サーバー上の `/.ssh/authorized_keys` ファイルに配置する必要があります。

必要な管理特権

このアダプタでは、一般ユーザーとしてログインしてから su コマンドを実行し、root ユーザー (または root ユーザーと同等のアカウント) に切り替えて管理アクティビティーを実行できます。 また、root ユーザーとして直接ログインすることもできます。また、root ユーザーとして直接ログインすることもできます。

このアダプタは、sudo 機能 (バージョン 1.6.6 以降) もサポートします。この機能は、Solaris 9 に Companion CD からインストールできます。sudo 機能を使用すると、システム管理者は特定のユーザー (またはユーザーのグループ) に、root ユーザーまたは別のユーザーとして一部 (またはすべて) のコマンドを実行する能力を与えることができます。

さらに、sudo がリソースで有効になっている場合は、その設定が、root ユーザーのリソース定義ページでの設定よりも優先されます。

sudo を使用する場合は、Identity Manager 管理者に対して有効にされたコマンドの `tty_tickets` パラメータを true に設定する必要があります。詳細については、sudoers ファイルのマニュアルページを参照してください。

管理者は、sudo で次のコマンドを実行する特権が付与されている必要があります。

ユーザーとグループのコマンド		その他のコマンド	
■ `chsh`	■ `passwd`	■ `awk`	■ `ln`
■ `groupadd`	■ `useradd`	■ `cat`	■ `ls`
■ `groupdel`	■ `userdel`	■ `chmod`	■ `mv`
■ `groupmod`	■ `usermod`	■ `chown`	■ `ps`
■ `last`		■ `cp`	■ `rm`
		■ `cut`	■ `sed`
		■ `diff`	■ `sort`
		■ `echo`	■ `tail`
		■ `grep`	■ `touch`

yppasswd コマンドには、root のパスワードが必要になるため、このアダプタは sudo を使用した NIS コマンドの実行をサポートしていません。

テスト接続を使用して次のテストができます。

- 各コマンドが管理ユーザーのパスに存在するかどうか
- 管理ユーザーが `/tmp` に書き込めるかどうか
- 管理ユーザーに、特定のコマンドを実行する権限があるかどうか

テスト接続では、通常のプロビジョニング実行とは異なるコマンドオプションを使用できます。

このアダプタには、基本的な sudo 初期化機能とリセット機能が用意されています。ただし、リソースアクションが定義されていて、そこに sudo 認証を必要とするコマンドが含まれている場合は、UNIX コマンドとともに sudo コマンドを指定してください。たとえば、単に `useradd` と指定する代わりに `sudo useradd` を指定してください。sudo を必要とするコマンドは、ネイティブリソースに登録されている必要があります。それらのコマンドを登録するには、`visudo` を使用します。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	Linux は、Identity Manager の enable アクションと disable アクションをネイティブではサポートしません。Identity Manager は、ユーザーのパスワードを変更することによって、アカウントの有効化と無効化をシミュレートします。enable アクションでは変更されたパスワードが公開されますが、disable アクションでは公開されません。 その結果、enable アクションと disable アクションは update アクションとして処理されます。update で動作するように設定されている前アクションと後アクションすべてが実行されます。
アカウントの名前の変更	あり
パススルー認証	あり
前アクションと後アクション	あり
データ読み込みメソッド	■ リソースから直接インポート ■ リソースの調整

このリソース上のすべてのユーザーに対して、次のタスクを制御するリソース属性を定義できます。

- ユーザーの作成時にホームディレクトリを作成する
- ユーザーの作成時にユーザーのホームディレクトリにファイルをコピーする
- ユーザーの削除時にホームディレクトリを削除する

アカウント属性

次の表に、Red Hat Linux および SuSE Linux ユーザーのアカウント属性を示します。特に記載されていないかぎり、属性は省略可能です。属性の型はすべて String です。

リソースユーザー属性	**useradd** での指定方法	説明
accountId	login	必須。ユーザーのログイン名。
comment	- c comment	ユーザーのフルネーム。
dir	- d dir	ユーザーのホームディレクトリ。このアカウント属性で指定された値はすべて、「ホームベースディレクトリ」リソース属性で指定された値よりも優先されます。
expire	- e expiration date	アカウントにアクセスできる最終日付。
group	- g group	ユーザーの一次グループ。
inactive	- f days	アカウントが非アクティブになってからロックされるまでの日数。
secondary_group	- G group	ユーザーの二次グループのコンマ区切りリスト。 ロールを有効にしてこの属性をプロビジョニングするには、'csv=true' を Role オブジェクト XML の RoleAttribute 要素に追加する必要があります。
shell	-s/Path	ユーザーのログインシェル。 NIS マスターにプロビジョニングしている場合は、ユーザーシェルの値は NIS マスターに対してのみチェックされます。ユーザーがログオンする可能性のあるその他のマシンに対してチェックは実行されません。
time_last_login	lastlog コマンドから取得されます。	最終ログインの日時。この値は読み取り専用です。最終ログイン時間を取得するにはリソースの追加呼び出しが必要なため、この属性を追跡する必要がない場合は、この属性をスキーママップから削除してください。
uid	- u User ID	数字形式でのユーザー ID。

リソースオブジェクトの管理

Identity Manager は、次のネイティブ Solaris オブジェクトをサポートします。

リソースオブジェクト	サポートされる機能	管理される属性
Group	作成、更新、削除、名前の変更、名前を付けて保存	groupName、gid、users

アイデンティティーテンプレート

```
$accountId$
```

サンプルフォーム

組み込みのフォーム

- Red Hat Linux Group Create Form
- Red Hat Linux Group Update Form
- SuSE Linux Group Create Form
- SuSE Linux Group Update Form

その他の利用可能なフォーム

- RedHatLinuxUserForm.xml
- SUSELinuxUserForm.xml

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

- `com.waveset.adapter.RedHatLinuxResourceAdapterr`
- `com.waveset.adapter.SUSELinuxResourceAdapter`
- `com.waveset.adapter.SVIDResourceAdapter`
- `com.waveset.adapter.ScriptedConnection`

◆ ◆ ◆ 第 32 章

32 Remedy

Remedy リソースアダプタは、com.waveset.adapter.RemedyResourceAdapter クラスで定義されます。

アダプタの詳細

リソースを設定する際の注意事項

ARTCPPORT 環境変数および ARRPC 環境変数を設定した場合、それらの値は「**Remedy TCP** ポート」および「**Remedy RPC** ソケット」リソースパラメータに指定された値を上書きします。

Identity Manager のインストールに関する注意事項

複数の Remedy API ライブラリをゲートウェイがインストールされているディレクトリに配置する必要があります。これらのライブラリは、Remedy サーバーにあります。

Remedy 4.x および 5.x	Remedy 6.3	Remedy 7.0
■ arapi*XX*.dll ■ arrpc*XX*.dll ■ arutl*XX*.dll *XX* は Remedy のバージョンと一致します。たとえば Remedy 4.5 では arapi45.dll になります。	■ arapi63.dll ■ arrpc63.dll ■ arutl63.dll ■ icudt20.dll ■ icuin20.dll ■ icuuc20.dll	■ arapi70.dll ■ arrpc70.dll ■ arutl70.dll ■ icudt32.dll ■ icuin32.dll ■ icuuc32.dll

使用上の注意

- 356 ページの「ワークフロー」
- 357 ページの「ゲートウェイタイムアウト」

ワークフロー

Remedy の統合については、『Business Administrator's Guide』を参照してください。

Active Sync 機能を有効にしない場合、Remedy アダプタは Remedy チケットを Identity Manager ワークフローに自動的に統合します。

Active Sync 機能を使用する場合は、次の機能をサポートするようにアダプタを設定できます。

- Remedy チケットスキーマの問い合わせ
- 静的条件 (status = ”new’ など) に基づくチケットのフィルタリング
- 動的条件 (最後に取得されたチケットなど) に基づくチケットのフィルタリング
- チケットが一致するたびに起動されるワークフローの指定

Active Sync が有効な場合、Remedy アダプタは「更新検索フィルタ」、「付加する結合子」、および「**LAST FETCHED** フィルタ」の各リソースパラメータを使用して、返されるチケットを判定します。「更新検索フィルタ」、「**LAST FETCHED** フィルタ」、またはその両方を使用するようにしてください。

「更新検索フィルタ」パラメータは省略可能なパラメータで、Remedy の検索式を指定します。このパラメータには、Remedy ユーザーアプリケーションの詳細検索条件に入力できる有効な検索式を含めることができます。有効な検索式には、フィールド、選択値、およびキーワードを含めることができます。このアダプタは、検索式の有効性を確認しません。

次の例は、Remedy User アプリケーションに用意されている Help Desk Cases サンプルフォームで使用できる検索式を示しています。

- ’Status’ = "New"

- 'Case Type' = "Problem"

注 – Remedy のフィールド名は一重引用符で囲み、値は二重引用符で囲みます。

「LAST FETCHED フィルタ」パラメータを使用する場合は、「付加する結合子」パラメータも指定する必要があります。「付加する結合子」パラメータには、次のいずれかの値を含めることができます。

- AND。「更新検索フィルタ」フィールドと「LAST FETCHED フィルタ」フィールドの両方の条件が、論理的に真である必要があります。
- OR。「更新検索フィルタ」フィールドと「LAST FETCHED フィルタ」フィールドのいずれかの条件が、論理的に真である必要があります。

「LAST FETCHED フィルタ」パラメータはもう 1 つの Remedy 検索式を指定しますが、この式には Identity Manager で定義された 1 つ以上のユーザー属性を含めることができます。この機能を使用して、前のポーリングで返された値を現在のポーリングで返された値と比較する式を作成できます。たとえば、Remedy フォーム上の Case ID+ フィールドに各チケットの一意の ID が含まれる場合は、この値をポーリングごとに比較できます。現在のポーリングの値が前のポーリングの値より大きい場合は、チケットに関する情報を返します。次の式は、この機能を示しています。

```
'Case ID+' > "$(caseId)"
```

括弧内の値には、スキーママップページで指定された Waveset ユーザー属性を指定する必要があります。$(caseId) トークンは、前のポーリングで返された値に置き換えられます。たとえば、HD0000045 などの値になります。

注 – アダプタが最初にポーリングを行なったときは、前に取得された値が存在しないため、「**LAST FETCHED** フィルタ」は適用されません。このフィルタは、その後のすべてのポーリングで実行されます。

このアダプタは、「更新検索フィルタ」、「付加する結合子」、「**LAST FETCHED** フィルタ」の各リソースパラメータを連結し、次のような検索式を送信します。

```
'Status' = "New" AND 'Case ID+' > "HD00000045"
```

ゲートウェイタイムアウト

Remedy アダプタでは、RA_HANGTIMEOUT リソース属性を使用してタイムアウト値を秒単位で指定できます。この属性は、ゲートウェイに対する要求がタイムアウトしてハングしているとみなされるまでの時間を制御します。

次のように、この属性を Resource オブジェクトに手動で追加する必要があります。

```
<ResourceAttribute name='Hang Timeout' displayName='com.waveset.adapter.
RAMessages:RESATTR_HANGTIMEOUT' type='int' description='com.waveset.adapter.RAMessages:
RESATTR_HANGTIMEOUT_HELP' value='NewValue'>
 </ResourceAttribute>
```

この属性のデフォルト値は 0 です。これは Identity Manager がハングした接続を確認しないことを表します。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は、Remedy API を使用して Remedy アダプタと通信します。

必要な管理特権

Remedy サーバーへのログインに使用するアカウントは、Identity Manager によってアクセスされるすべての Remedy オブジェクトのアクセス権リストに含まれている必要があります。

プロビジョニングに関する注意事項

Remedy ユーザーの属性は、Remedy アプリケーション内で確立されるスキーマに基づいています。スキーマと、スキーマの操作に関する詳細については、Remedy のマニュアルを参照してください。

Remmedy アダプタは、次のプロビジョニングアクションをサポートします。

- ユーザーの作成、更新、削除
- パスワードの設定
- アカウントの反復処理
- アカウントの一覧表示
- 大文字と小文字を区別しない ID の許可
- アカウントログインおよびパスワード認証

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	適用不可

機能	サポート状況
パスワードの期限切れ	なし
アカウントの名前の変更	なし
パススルー認証	なし
前アクションと後アクション	なし
データ読み込みメソッド	■ Active Sync ■ リソースからインポート ■ 調整

アカウント属性

Remedyアダプタには、デフォルトのアカウント属性がありません。カスタム属性を追加する場合は、次のガイドラインを使用してください。

- フォームとワークフローでは、Waveset ユーザー属性値を使用できます。この属性には、有効な Remedy フィールド ID を指定する必要があります。Remedy フォームのすべてのフィールドに、フォーム内で一意となる整数のフィールド ID が必要です。

  Remedy Administrator の内部でフィールドの ID を表示するには、フォームを開いてそのフィールドを選択します。フィールド ID が「Find Field」ドロップダウンメニューに括弧付きで表示されます。
- リソースユーザー属性が「Remedy Diary」フィールドに対応している場合、その属性は複数の値を取ります。値リストの各値は、次の形式を取ります。

  Timestamp User Message

  各表記の意味は次のとおりです。

  Timestamp。1970 年 1 月 1 日 (UTC) を起点とする秒数を示す整数。

  User。ダイアリにメッセージを追加した Remedy ユーザー。

  Message。ダイアリのエントリ。
- Remedy アダプタにパスワードの変更を許可するには、次を実行してください。
  - 「パスワードのサポート」リソースパラメータを選択します。
  - アイデンティティーシステムユーザー属性名が `password` で、属性タイプが暗号化されているアカウント属性を、スキーママップに追加します。このリソースユーザー属性は、ユーザーパスワードを保持する Remedy フィールド ID にします。

リソースオブジェクトの管理

なし

アイデンティティーテンプレート

Remedy のアイデンティティーテンプレートは、Remedy システムによって生成されます。Identity Manager で確立されたアイデンティティーテンプレートは、すべて無視されます。

サンプルフォーム

なし

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

```
com.waveset.adapter.RemedyResourceAdapter
```

また、リソースインスタンスに対して次の Identity Manager ロギングパラメータを設定できます。

- ログファイルパス
- ログレベル
- アーカイブの最大数
- 最大有効期間の単位
- 最大有効期間
- ログファイルの最大サイズ

ゲートウェイへの接続の問題を診断するために、次のメソッドでトレースを有効にすることもできます。

- `com.waveset.adapter.AgentResourceAdapter#sendRequest`
- `com.waveset.adapter.AgentResourceAdapter#getResponse`

◆ ◆ ◆ 第 33 章

33 SAP

SAP リソースアダプタは、SAP R3 および R3 Enterprise をサポートします。

アダプタの詳細

リソースアダプタは、com.waveset.adapter.SAPResourceAdapter クラスで定義されます。

ユーザーが自分自身の SAP パスワードを変更できるようにするには、次の手順を実行します。

▼ ユーザーが自分のパスワードを変更できるようにする

1 「変更時にユーザーがパスワードを入力」リソース属性を設定します。

2 スキーママップの両側に WS_USER_PASSWORD を追加します。ユーザーフォームやその他のフォームを変更する必要はありません。

リソースを設定する際の注意事項

なし。

Identity Manager のインストールに関する注意事項

SAP リソースアダプタは、カスタムアダプタです。インストールプロセスを完了するには、次の手順を実行する必要があります。

▼ SAP リソースアダプタをインストールする

1 **http://service.sap.com/connectors** から **JCo (Java Connection)** ツールキットをダウンロードします。**SAP JCO** ダウンロードページにアクセスするには、ログインとパスワードが必要です。このツールキットには、`sapjco-ntintel-2.1.6.zip` のような名前が付けられます。この名前は、選択したプラットフォームやバージョンによって異なります。

注 – ダウンロードする JCo ツールキットが、アプリケーションサーバーが動作する Java のビットバージョンと一致していることを確認します。たとえば、JCo は Solaris x86 プラットフォーム上の 64 ビットバージョンでのみ使用できます。したがって、アプリケーションサーバーが Solaris x86 プラットフォーム上の 64 ビットバージョンで実行されている必要があります。

---

2 ツールキットを解凍し、インストール手順に従います。必ずライブラリファイルを正しい場所に配置し、環境変数を指示どおりに設定してください。

3 `sapjco.jar` ファイルを *InstallDir*`\WEB-INF\lib` ディレクトリにコピーします。

4 **SAP** リソースを **Identity Manager** のリソースリストに追加するには、「管理するリソースの設定」ページの「カスタムリソース」セクションに次の値を追加する必要があります。

```
com.waveset.adapter.SAPResourceAdapter
```

使用上の注意

ここでは、SAP リソースアダプタの使用に関する情報を示します。 次のトピックで構成されています。

全般的な注意事項

このリソースに関する全般的な注意事項は次のとおりです。

- アクティビティーグループごとに開始日と終了日を編集できるようにするには、SAPUserForm_with_RoleEffectiveDates_Timezone.xml フォームを読み込みます。このフォームは、ユーザーのタイムゾーンを選択する機能も備えています。
- `waveset.properties` ファイル内の `sources.`*ResourceName* `.hosts` プロパティーを使用して、Active Sync を使用してリソースの同期を行うクラスタ内のホストを選択できます。*ResourceName* は、リソースオブジェクトの名前に置き換える必要があります。
- サンプルユーザーフォームの `SAPUserForm.xml` と SAPUserForm_with_RoleEffectiveDates_Timezone.xml は、ユーザーのパスワードがすでに期限切れになっているフィールドの定義も含むようになりました。このフィールドの値が `true` で、Identity Manager 管理者がユーザーのパスワードを作成または変更した場合、そのユーザーは SAP へのログイン時に新しいパスワードを指定する必要があります。

SNC (Secure Network Communications) 接続の有効化

デフォルトでは、SAP アダプタは SAP Java Connector (JCo) を使用して SAP アダプタと通信します。SNC 接続の実装については、第 54 章「SNC (Secure Network Communications) 接続の有効化」を参照してください。

SAP JCO および RFC のトレース

SAPResourceAdapter と SAPHRActiveSyncAdapter には、SAP JCO および RFC のトレース用のリソース属性が用意されています。これらを使用して、Identity Manager と SAP システムの通信をトレースできます。属性名は、「SAP JCO トレースレベル」と「SAP JCO トレースディレクトリ」です。

環境内に次の環境変数を設定すると、SAP RFC トレースを有効にできます。これらの変数は、アプリケーションサーバーを起動する前に環境内に設定してください。これらの変数は、JCO が SAP システムとの通信に使用する共有ライブラリを制御します。

- RFC_TRACE: 0 または 1
- RFC_TRACE_DUMP: 0 または 1
- RFC_TRACE_DIR: トレースファイルのディレクトリへのパス
- CPIC_TRACE_DIR: トレースファイルのディレクトリへのパス

注 – JCO のトレースが必要でない場合は、トレースファイルが作成されないように、RFC_TRACE を 0 に設定してください。

CUA 環境での実動パスワードの変更

SAP では、パスワードはアカウントが存在するシステムのアカウント間で共有される機密であると見なされます。したがって CUA ランドスケープでは、ユーザーのパスワードの独自コピーが各 CUA クライアントで保守されています。CUA ランドスケープでの標準的なパスワードの変更方法では、クライアントシステムで実動パスワードを設定できません (実動パスワードとは、有効期限が切れていない、次回ログオン時に変更する必要のないパスワードです)。これらの方法では、ランドスケープ内のすべてのシステム (クライアントおよび集中システム) で、ユーザーの初期パスワードを設定できます。

パスワードを変更する機能モジュールは、リモートで実行できる必要があります。CUA ランドスケープでは、初期パスワードの SCUM 設定を「global」または「everywhere」に設定する必要があります。その他のケースでは、CUA 集中システムはクライアントのパスワードをリセットできません。特定の環境では、パスワード変更のエラーが発生します。アダプタでは、ユーザーが存在するすべてのシステムの CUA ランドスケープで、実動パスワードを設定できます。システムごとに、パスワードを変更するだけで設定を行えます。この機能を有効にするには、すべてのクライアントシステムに対して実行される CUA 集中システムに、特別な機能モジュールをインストールする必要があります。モジュールは、InstallDir\idm\sample\other にソースとして提供されます。このモジュールを、SAP 集中システムにインストールする必要があります。機能モジュールの名前は、「CUA Child Password Change Function Module」リソース属性で設定する必要があります。

CUA ランドスケープでパスワードが変更され、このモジュールが使用されている場合、1 回のパスワードの変更に対して複数のエラー (各クライアントと集中システムのそれぞれで 1 つずつ) が発生する場合があります。各システムは、それぞれ独自のパスワードポリシーを維持します。あるシステムの規則に準拠するパスワードが、別のシステムではポリシーエラーとなる場合もあります。特定のシステムのエラーにより、ほかのシステムが変更されないという意味ではありません。この動作は、CUA ランドスケープで SAP がパスワードを定義および操作する方法によって決まります。

CUA がアダプタで設定されているときに、モジュールが集中システムにインストールされていないか、属性がアダプタで設定されていない場合、実動パスワードの変更は集中システムのみに適用されます。初期パスワードの設定とパスワードリセットの実行 (つまり、期限切れのパスワード) は、この設定変更の影響を受けません。

アカウントの名前の変更

SAP アダプタは、CUA モードがアダプタで有効な場合を除き、アカウントの名前の変更をサポートするようになりました。アダプタは、この機能を実行するために、既存のアカウントを新しいアカウントにコピーして元のアカウントを削除します。SAP は、アカウントの名前の変更を推奨していませんが、SAP GUI から使用する

Transaction SU01 というユーザー管理アプリケーションではこのオプションを提供しています。したがって、Identity Manager もこのオプションをサポートします。SAP では名前の変更機能を将来のリリースでサポートしなくなる可能性があることに注意してください。

SAP GUI では非公開 API および SAP カーネルにアクセスできるため、名前の変更に別の方法を使用します。次の手順では、名前の変更操作を実行する方法について概要を説明します。

▼ SAP アダプタによる名前変更操作の実行

1. 既存のユーザーのユーザー情報を取得します。
2. **ALIAS** 属性が存在する場合は、**ALIAS** 属性を保存します。
3. 新しいユーザーを作成します。
4. 新しいユーザーでアクティビティーグループを設定します。
5. 新しいユーザーでプロファイルを設定します。
6. 古いユーザーの個別設定データを取得します。
7. 新しいユーザーの個別設定データを設定します。
8. 古いユーザーを削除します。
9. 古いユーザーで別名が設定されていた場合は、新しいユーザーで別名を設定します。

   手順 1 ～ 3 でエラーが発生した場合は、操作がただちに失敗します。手順 4 ～ 7 でエラーが発生した場合は、新しいユーザーが削除され、操作全体が失敗します。新しいユーザーが削除できない場合は、警告が WavesetResult に設定されます。手順 8 ～ 9 でエラーが発生した場合は、警告が WavesetResult に追加されますが、操作は成功します。

   名前の変更操作では、新しいパスワードを新しいユーザーに設定する必要があります。設定する最も簡単な方法は、Change User Password タスクを呼び出すように Rename User タスクをカスタマイズすることです。

Global Trade Services (GTS) のサポート

SAP アダプタの SAP Global Trade Services のサポートを有効にするには、次の表の「ロール名」に一覧表示された該当するロールを有効にします。SAP は、この表の「生成されるロール」列に一覧表示されたロールを生成します。生成されたロールを SAP GTS の該当するユーザープロファイルに割り当ててください。

ロールラベル	ロール名	生成されるロール
通関処理スペシャリスト	SAP_BW_SLL_CUS	SAP_BWC_SLL_CUS
特恵処理スペシャリスト	SAP_BW_SLL_PRE	SAP_BWC_SLL_PRE
還付金スペシャリスト	SAP_BW_SLL_RES	SAP_BWC_SLL_RES
法規制スペシャリスト	SAP_BW_SLL_LCO	SAP_BWC_SLL_LCO

追加のテーブルのサポート

SAP アダプタは、BAPI_USER_CREATE1 および BAPI_USER_CHANGE によって呼び出された任意の SAP テーブル、特に GROUPS テーブルおよび PARAMETER テーブルにプロビジョニングできます。GROUPS 以外の任意のテーブルについてこの機能を有効にするには、リソースユーザー属性を SAP_Table_Name->Table という形式でスキーママップに追加する必要があります。たとえば、PARAMETER->Table とします。属性は、複合データ型を割り当てられる必要があります。

アダプタは、GROUPS->USERGROUP アカウント属性という名前で、タイプが String であるアカウント属性を提供します。この属性は、GROUPS テーブルのデータを処理します。デフォルトでこの属性のタイプは String です。この属性のタイプが String に設定されている場合、アダプタは値を文字列のリストとして処理します。アダプタがほかのテーブルと同じ方法でこのテーブルのデータを処理するようにするには、データ型を複合に変更する必要があります。

$WSHOME/web/sample/forms/SAPUserForm.xml ファイルには、String のアカウント属性タイプおよび複合属性タイプを使用して GROUP テーブルを管理する方法を示すユーザーフォームの例が含まれています。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

- SAP Java Connector (JCo) 経由の BAPI
- SAP Secure Network Communications

必要な管理特権

SAP に接続するユーザー名を、SAP ユーザーにアクセスできるロールに割り当ててください。

プロビジョニングに関する注意事項

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	使用可。ただし CUA が有効な場合を除きます。
パススルー認証	なし
前アクションと後アクション	なし
データ読み込みメソッド	■ リソースから直接インポート ■ 調整

アカウント属性

次の表に、デフォルトの SAP アカウント属性に関する情報を示します。**Enable SAP GRC Access Enforcer?**」リソースパラメータが選択されている場合は、追加属性も提供されます。属性タイプはすべて String です。

アイデンティティーシステムユーザー属性	リソース属性名	説明
accountId	USERNAME->BAPIBNAME	必須。ユーザーのアカウント ID。
firstname	ADDRESS->FIRSTNAME	ユーザーの名
fullname	ADDRESS->FULLNAME	ユーザーの姓名
email	ADDRESS->E_MAIL	ユーザーの電子メールアドレス
lastname	ADDRESS->LASTNAME	必須。ユーザーの姓
groups	GROUPS->USERGROUP	SAP GROUPS テーブルのプロビジョニング。
l	WS_PasswordExpired	ログイン時にユーザーに新しいパスワードを強制的に入力させます。
accountLockedNoPwd	ISLOCKED->NO_USER_PW	ブール型。ユーザーがパスワードを設定していないためにアカウントがロックされているかどうかを示します。
accountLockedWrngPwd	ISLOCKED->WRNG_LOGON	ブール型。ログイン試行が失敗したためにアカウントがロックされているかどうかを示します。
personNumber	ADDRESS->PERS_NO	ユーザーを特定するための内部キー

アイデンティティーシステムユーザー属性	リソース属性名	説明
addressNumber	ADDRESS->ADDR_NO	一元的なアドレス管理に使用される、アドレスを特定するための内部キー
birthName	ADDRESS->BIRTH_NAME	旧姓 (出生時に与えられた姓)
middleName	ADDRESS->MIDDLENAME	ユーザーのミドルネーム
secondLastName	ADDRESS->SECONDNAME	第二姓
academicTitle	ADDRESS->TITLE_ACA1	学位 (Dr.、Prof. など)
academicTitle2	ADDRESS->TITLE_ACA3	第二学位
namePrefix	ADDRESS->PREFIX1	姓の前置語 (von、van der、de la など)
namePrefix2	ADDRESS->PREFIX2	姓の 2 つ目の前置語
titleSupplement	ADDRESS->TITLE_SPPL	名前の補足 (Lord、Lady など)
nickname	ADDRESS->NICKNAME	ユーザーのニックネーム
initials	ADDRESS->INITIALS	ミドルネームのイニシャル
nameFormat	ADDRESS->NAMEFORMAT	ユーザーの名前を完全な形式で表示する場合の、名前の構成要素の配置順序。この順序は、国ごとに異なる場合があります。
nameFormatCountry	ADDRESS->NAMCOUNTRY	名前の形式を判定するために使用される国名
languageKey	ADDRESS->LANGU_P	テキストの入力と表示に使用される言語
iso639Language	ADDRESS->LANGUP_ISO	ISO 639 言語コード
sortKey1	ADDRESS->SORT1_P	検索用語
sortKey2	ADDRESS->SORT2_P	二次検索用語
department	ADDRESS->DEPARTMENT	会社の住所の一部としての社内の部署
function	ADDRESS->FUNCTION	ユーザーの職能
buildingNumber	ADDRESS->BUILDING_P	ユーザーの職場があるビル番号
buildingFloor	ADDRESS->FLOOR_P	ユーザーの職場がある階
roomNumber	ADDRESS->ROOM_NO_P	ユーザーの職場がある部屋番号
correspondenceCode	ADDRESS->INITS_SIG	通信コード
inhouseMailCode	ADDRESS->INHOUSE_ML	内部郵便コード

アイデンティティーシステムユーザー属性	リソース属性名	説明
communicationType	ADDRESS->COMM_TYPE	ユーザーがどのような方法でビジネスパートナーと文書やメッセージを交換するかを示します。
title	ADDRESS->TITLE	敬称 (Mr.、Mrs. など)
titleP	ADDRESS->TITLE_P	敬称 (Mr.、Mrs. など)
addressName	ADDRESS->NAME	宛名
addressName2	ADDRESS->NAME_2	宛名の 2 行目
addressName3	ADDRESS->NAME_3	宛名の 3 行目
addressName4	ADDRESS->NAME_4	宛名の 4 行目
careOfName	ADDRESS->C_O_NAME	受取人が居住者と異なる場合の宛名部分 (c/o = 気付)
city	ADDRESS->CITY	ユーザーの市
district	ADDRESS->DISTRICT	市または地区の追加部分
cityNumber	ADDRESS->CITY_N	都市コード
districtNumber	ADDRESS->DISTRCT_NO	地区コード
cityPostalCode	ADDRESS->POSTL_COD1	ユーザーの郵便番号
poBoxPostalCode	ADDRESS->POSTL_COD2	私書箱を一意に割り当てるために必要な郵便コード。
companyPostalCode	ADDRESS->POSTL_COD3	企業に直接割り当てられる郵便コード。
poBox	ADDRESS->PO_BOX	ユーザーの私書箱
poBoxCity	ADDRESS->PO_BOX_CIT	私書箱の市
poBoxCityCode	ADDRESS->PBOXCIT_NO	私書箱の市 (宛名の市と異なる場合)。
postalDeliveryDistrict	ADDRESS->DELIV_DIS	郵便配達区域
transportZone	ADDRESS->TRANSPZONE	品物の受取人または供給元の地域圏
street	ADDRESS->STREET	ユーザーの街路住所
streetNumber	ADDRESS->STREET_NO	街路コード
streetAbbreviation	ADDRESS->STR_ABBR	街路の略称
houseNumber	ADDRESS->HOUSE_NO	街路住所の番号部分
houseNumber2	ADDRESS->HOUSE_NO2	第二住所番号

アイデンティティーシステムユーザー属性	リソース属性名	説明
street2	ADDRESS->STR_SUPPL1	街路行の上に出力される追加の住所フィールド。
street3	ADDRESS->STR_SUPPL2	街路行の上に出力される追加の住所フィールド。
street4	ADDRESS->STR_SUPPL3	街路行の下に出力される追加の住所フィールド。
street5	ADDRESS->LOCATION	街路行の下に出力される追加の住所フィールド。
oldBuilding	ADDRESS->BUILDING	連絡窓口住所のビルの番号または ID。
floor	ADDRESS->FLOOR	住所の階数
roomNumber	ADDRESS->ROOM_NO	住所の部屋番号
countryCode	ADDRESS->COUNTRY	住所の国名
countryCodeISO	ADDRESS->COUNTRYISO	住所の国を表す 2 文字の ISO コード
languageKey	ADDRESS->LANGU	テキストの入力と表示に使用される言語
languageKeyISO	ADDRESS->LANGU_ISO	ISO 639 言語コード
region	ADDRESS->REGION	州または都道府県
sort2	ADDRESS->SORT2	二次検索用語
timeZone	LOGONDATA->TZONE	タイムゾーンと UTC との時差 (時/分単位)
taxJurisdictionCode	ADDRESS->TAXJURCODE	税金の納入先となる税務機関。常に、品物が配達された市です。
telephoneNumber	ADDRESS->TEL1_NUMBR	電話番号 (市外局番を含み、国番号を除く)
telephoneExtension	ADDRESS->TEL1_EXT	内線電話番号
faxNumber	ADDRESS->FAX_NUMBER	FAX 番号 (市外局番を含み、国番号を除く)
faxExtension	ADDRESS->FAX_EXTENS	内線 FAX 番号
buildingNumber	ADDRESS->BUILD_LONG	住所のビルの番号または略称。
cuaSystems	SYSTEMS->CUASYSTEMS	Central User Administration システム名
profiles	PROFILES->BAPIPROF	ユーザーに割り当てられたプロファイル。

アイデンティティーシステムユーザー属性	リソース属性名	説明
activityGroups	ACTIVITYGROUPOBJECTS	ユーザーに割り当てられたロール。
lastLoginTime	LOGONDATA->LTIME	最新のログイン時間を一覧表示する読み取り専用属性。

リソースオブジェクトのサポート

管理対象オブジェクト

このアダプタは、SAP リソース上のオブジェクトを管理しません。

一覧表示可能なオブジェクト

次の表では、ユーザーフォーム内で listAllObjects メソッドを使用して呼び出すことのできる SAP オブジェクトについて説明します。

Object	説明
account	SAP リソースで定義されたユーザーを一覧表示します。
activityGroups	ユーザーが使用できるアクティビティーグループ (またはロール) を一覧表示します。(非 CUA モードのみ)
cuaSystems	CUA が有効な場合に、CUA 子の名前を一覧表示します。
Group	SAP リソースで使用可能なグループを一覧表示します。
localActivityGroups	CUA が有効な場合に、CUA 環境で特定の子システムに存在するアクティビティーグループを一覧表示します。
profiles	認証プロファイルの名前を一覧表示します。
table	SAP テーブルの列の内容を一覧表示します。option マップには次のパラメータが必要です。 name は、SAP テーブル名を表します。 offset は、テーブルの開始文字の列を表します。 length は、データフィールドの長さを表します。 これらの値の判断については、BAPI RFC_GET_TABLE_ENTRIES に関する SAP のマニュアルを参照してください。詳細は、366 ページの「追加のテーブルのサポート」を参照してください。
timeZones	SAP システムでサポートされる、使用可能なタイムゾーンを一覧表示します。

Object	説明
usertype	SAP システムで使用可能なユーザータイプを一覧表示します。

アイデンティティーテンプレート

```
$accountId$
```

サンプルフォーム

```
SAPForm.xml
SAPUserForm_with_RoleEffectiveDates_Timezone.xml
SAPHRActiveSyncForm.xml
```

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

- `com.waveset.adapter.SAPResourceAdapter`

インストールされている SAP Java Connector (JCO) のバージョンを判定し、それが正しくインストールされているかどうかを判定するには、次のコマンドを実行します。

```
java -jar sapjco.jar
```

このコマンドは、JCO のバージョンとともに、SAP システムと通信する JNI プラットフォーム依存ライブラリおよび RFC ライブラリを返します。

プラットフォーム依存ライブラリが見つからない場合は、SAP のマニュアルを参照して、SAP Java Connector の正しいインストール方法を調べてください。

◆ ◆ ◆ 第 34 章

SAP HR Active Sync

Identity Manager で提供される SAP HR Active Sync アダプタは、次のバージョンの SAP HR をサポートします。

- SAP HR 4.5、4.6、4.7 (読み取り専用アクセス)

アダプタの詳細

次の表に、SAP HR Active Sync アダプタの属性の概要を示します。

GUI 名	Class Name
SAP HR Active Sync	`com.waveset.adapter.SAPHRActiveSyncAdapter`

注 – Identity Manager 6.0 から、SAP HR Active Sync アカウント属性の形式が新しくなりました。スキーママップ内のリソースユーザー属性は、_ (下線) ではなく : (コロン) で区切られるようになりました。これにより、SAP HR の属性を、情報タイプ内の単純な属性ではなく、任意の深さの属性へのパスにすることができます。前述の製品のいずれかを前のバージョンから更新すると、デフォルトでは更新スクリプトの一部としてデフォルトの属性名が変更されます。属性の変換に問題があった場合は、ResourceUpdater がメッセージを出力します。ただし、変換が成功したことを確実にするため、アカウント属性を見直すようにしてください。

リソースを設定する際の注意事項

ここでは、SAP リソースアダプタと SAP HR Active Sync アダプタに特有の設定の注意点を示します。

- 374 ページの「論理システムの作成」

SAP Application Link Enabling (ALE) テクノロジにより、SAP と Identity Manager などの外部システム間の通信が有効になります。SAP HR Active Sync アダプタは、アウトバウンド ALE インタフェースを使用します。アウトバウンド ALE インタフェースでは、ベース論理システムがアウトバウンドメッセージの送信側およびインバウンドメッセージの受信側になります。SAP ユーザーは通常、従業員の雇用、役職データの更新、従業員の解雇などのデータベースの変更時に、ベース論理システム/クライアントにログインします。 論理システム/クライアントは、受信側クライアントにも定義されている必要があります。この論理システムは、アウトバウンドメッセージの受信側として動作します。Active Sync アダプタは、2 つのシステム間のメッセージタイプとして HRMD_A メッセージタイプを使用します。メッセージタイプにより、システム間で送信されるデータの特性が設定され、IDoc タイプとも呼ばれるデータの構造 (たとえば、HRMD_A05) への関連付けが行われます。

注 – HRMD_A IDoc を Application Link Enabling (ALE) で処理できるように SAP システムパラメータを設定してください。これにより、2 つのアプリケーションシステム間でデータ配布が可能になります。 これは「メッセージング」とも呼ばれます。

論理システムの作成

現在の SAP 環境によっては、論理システムの作成が不要な場合があります。以前に設定されたモデルビューに HRMD_A メッセージタイプを追加して、既存の分散モデルを変更するだけでよい場合もあります。ただし、論理システムと ALE ネットワークの設定については、SAP の推奨事項に従うことが重要です。次の手順では、新しい論理システムと新しいモデルビューを作成することを想定しています。

▼ 論理システムと新しいモデルビューを作成する

1. トランザクションコード **SPRO** を入力し、**SAP** 完全版 **IMG** (または組織に適用できるプロジェクト) を表示します。
2. 使用している **SAP** のバージョンに応じて、次のいずれかを実行します。

- **SAP HR 4.6** では、「ベースコンポーネント」、「Application Link Enabling (ALE)」、「システムの送信と受信」、「論理システム」、「定義: 論理システム」の順にクリックします。
  - **SAP HR 4.7** では、「SAP Web アプリケーションサーバー」、「Application Link Enabling (ALE)」、「システムの送信と受信」、「論理システム」、「定義: 論理システム」の順にクリックします。
  - **SAP HR 5.0** では、「SAP Netweaver」、「SAP Web アプリケーションサーバー」、「IDOC インタフェース/Application Link Enabling (ALE)」、「基本設定」、「論理システム」、「定義: 論理システム」の順にクリックします。
  - **SAP HR 6.0** では、「SAP Netweaver」、「Web アプリケーションサーバー」、「IDOC インタフェース/Application Link Enabling (ALE)」、「基本設定」>「論理システム」、「定義: 論理システム」の順にクリックします。

3 「編集」、「新規エントリ」の順にクリックします。

4 作成する論理システム **(IDMGR)** の名前と説明を入力します。

5 エントリを保存します。

論理システムへのクライアントの割り当て

▼ クライアントを論理システムに割り当てる

1 トランザクションコード **SPRO** を入力し、**SAP** 完全版 **IMG** (または組織に適用できるプロジェクト) を表示します。

2 使用している **SAP** のバージョンに応じて、次のいずれかを実行します。

- **SAP 4.6** では、「ベースコンポーネント」、「Application Link Enabling (ALE)」、「システムの送信と受信」、「論理システム」、「割当: 論理システム->クライアント」の順にクリックします。
  - **SAP 4.7** では、「アプリケーションサーバー」、「Application Link Enabling (ALE)」、「システムの送信と受信」、「論理システム」、「割当: 論理システム->クライアント」の順にクリックします。
  - **SAP 5.0** では、「SAP Netweaver」、「アプリケーションサーバー」、「IDOC インタフェース/Application Link Enabling (ALE)」、「基本設定」、「論理システム」、「割当: 論理システム->クライアント」の順にクリックします。
  - **SAP HR 6.0** では、「SAP Netweaver」、「Web アプリケーションサーバー」、「IDOC インタフェース/Application Link Enabling (ALE)」、「基本設定」>「論理システム」、「定義: 論理システム」の順にクリックします。

3 クライアントを選択します。

4 「ジャンプ」>「詳細」をクリックして、「クライアント変更:詳細」ダイアログボックスを表示します。

5 「論理システム」フィールドに、このクライアントに割り当てる論理システムを入力します。

6 「クライアント依存オブジェクトの変更と移送」セクションの「変更の自動記録」をクリックします。

7 エントリを保存します。

分散モデルの作成

▼ 分散モデルを作成する

1 送信側のシステム/クライアントにログインしていることを確認します。

2 トランザクションコード **BD64** を入力します。変更モードになっていることを確認します。

3 「編集」>「モデルビュー」>「登録」をクリックします。

4 作成するビューの技術的な短い名前、および開始日と終了日を入力し、「続行」をクリックします。

5 作成したビューを選択し、「メッセージタイプの追加」をクリックします。

6 送信側/論理システム名を定義します。

7 受信側/サーバー名を定義します。

8 「保護クライアントコピアーと比較ツール」セクションの「保護レベル:制限なし」をクリックします。

9 使用するメッセージタイプ **(HRMD_A)** を定義し、「続行」をクリックします。

10 「保存」をクリックします。

RFC サーバーモジュールの SAP ゲートウェイへの登録

初期化中に、Active Sync アダプタは SAP ゲートウェイに登録されます。ID として「IDMRFC」を使用します。この値は、SAP アプリケーションで設定された値と一致している必要があります。RFC サーバーモジュールでハンドルを作成できるように SAP アプリケーションを設定してください。

▼ RFC サーバーモジュールを RFC 宛先として登録する

1. **SAP** アプリケーションで、トランザクション **SM59** に移動します。
2. **TCP/IP** 接続ディレクトリを展開します。
3. 「登録 **(F8)**」をクリックします。
4. 「**RFC** 宛先」フィールドに **RFC** 宛先システムの名前 **(IDMRFC)** を入力します。
5. 接続タイプを **T** (外部プログラムを **TCP/IP** 接続を通して起動) に設定します。
6. 新しい **RFC** 宛先の説明を入力し、「保存」をクリックします。
7. 「起動型」区画の「登録サーバープログラム」ラジオボタンをクリックします。
8. 「アプリケーションサーバーで起動」区画の「プログラム **ID**」を設定します。**RFC** 宛先 **(IDMRFC)** と同じ値を使用するようにしてください。 次に、「保存」をクリックします。
9. **SAP** システムが **Unicode** システムの場合は、ポートを **Unicode** 用に設定してください。「特殊オプション」タブ (一部のシステムでは「**MDMP & Unicode**」タブ) をクリックして、「対象システムとの通信タイプ」セクションを探します。**Unicode** と非 **Unicode** の設定があります。
10. 上の方にある「接続テスト」ボタンと「ユニコードテスト」ボタンを使用して、**Identity Manager** リソースへの接続をテストします。テストにパスするには、アダプタを起動しておきます。

ポート定義の作成

ポートは、IDoc の送信先となる通信チャネルです。ポートには、送信側システムと受信側システム間の技術的なリンクが記述されます。このソリューションには RFC ポートを設定するようにしてください。

▼ ポート定義の作成

1. トランザクションコード **WE21** を入力します。
2. 「トランザクション **RFC**」を選択し、「作成」アイコンをクリックします。「**RFC** 宛先」に **IDMRFC** と入力します。
3. 変更を保存します。

パートナープロファイルの生成

パートナープロファイルは、システムによって自動的に生成されます。 また、ユーザーは手動でプロファイルを維持できます。

注 – 既存の分散モデルとパートナープロファイルを使用する場合は、パートナープロファイルを自動的に生成する必要はありません。代わりに、パートナープロファイルを変更して HRMD_A メッセージタイプを含めることができます。

▼ パートナープロファイルを自動的に生成する

1. トランザクションコード **BD82** を入力します。
2. モデルビューを選択します。これは、以前に作成されたモデルビューであるはずです。
3. 「すぐに **IDoc** をファイルへ転送」ラジオボタンと「即時開始」ラジオボタンが選択されていることを確認します。
4. 「実行」をクリックします。

ポート定義の修正

パートナープロファイルを生成したときに、ポート定義が間違って入力されている可能性があります。システムが正しく動作するには、ポート定義を修正する必要があります。

▼ ポート定義を修正する

1. トランザクションコード **WE20** を入力します。
2. 「パートナータイプ **LS**」を選択します。
3. 受信側のパートナープロファイルを選択します。

4 「送信パラメータ」を選択し、「表示」をクリックします。一部のシステムでは、「送信パラメータ」ボックスの下にある「+」アイコンをクリックします。

5 メッセージタイプ **HRMD_A** を選択します。

6 「送信オプション」をクリックし、受信側ポートを、作成した **RFC** ポート名 **(IDMGR)** に変更します。

7 **IDoc** を作成後すぐに送信するため、「出力モード」の「**IDoc** の即時転送」を選択します。

8 「**IDoc** タイプ」セクションから「基本タイプ」を選択します。

- SAP HR 4.6 では、HRMD_A05 を選択します。
- SAP HR 4.7 または 5.0 では、HRMD_A06 を選択します。

9 「続行/保存」をクリックします。

IDoc の生成

▼ IDoc を生成する

1 トランザクションコード **PFAL** を入力します。

2 オブジェクトタイプに、**person** オブジェクトの **P** を挿入します。

3 オブジェクト **ID** として従業員の **ID** を入力するか、従業員の範囲を選択します。

4 「実行」をクリックします。

5 ステータスが「ポートへのデータ受け渡し **OK**」に設定されていることを確認します。

6 **IDoc** が作成されました。**Active Sync** アダプタのログファイルを調べ、更新が受信されたことを確認します。

iDoc のオブジェクトタイプ

「objecttypes to read from SAP HR」リソース属性によって、SAP HR の異なる iDoc タイプを処理できます。Identity Manager は、iDoc の OTYPE を確認してオブジェクトタイプを判定します。この複数値属性は、P、CP、S、C、および O の任意の組み合わせをサポートします。

使用可能なオブジェクトタイプが、すべてリソースオブジェクトであるとは限りません。オブジェクトタイプには次のマッピングが適用されます。

- P、CP – ユーザーの iDocs
- S – 組織ロールの iDoc (ユーザーに関連付けられます)
- O – 組織の iDoc
- C – 職務の iDoc

オブジェクトタイプが設定されてない場合、Identity Manager は、ユーザーに関連する iDoc のタイプ P と CP を処理します。これらのオブジェクトタイプは、基本的なユーザー情報を提供します。

ユーザーに関連する iDoc は、iDoc データを処理するだけでなく、BAPI 呼び出しをトリガーします (リソースでトリガーしないように設定されている場合を除く)。オブジェクト O または C を処理する場合は、リソースでプロセス規則を設定する必要があります。プロセス規則によって、2 つのオブジェクトタイプの処理を許可する必要があります。ユーザーに関連するオブジェクト (iDoc タイプ P、CP、および S) には、これまでと同様、SAP HR PERNR に accountId がマップされます。O および C タイプにはユーザーとの関連がなく、accountId がマップされません。オブジェクトタイプの識別に使用できるその他の属性には、マップされた iDoc の OTYPE があります。

iDoc の属性はいずれも、リソース設定でマップされ、Identity Manager サーバーに返される必要があります。すべてのオブジェクトタイプは以降の処理をサポートします。

変更ポインタの有効化

変更ポインタをグローバルに有効化するには、次の手順に従います。

▼ 変更ポインタをグローバルに有効にする

1. トランザクションコード **BD61** を入力します。
2. 変更ポインタを有効にします。
   あるメッセージタイプに関して変更ポインタを有効にするには、次の手順に従います。
3. トランザクションコード **BD50** を入力します。
4. **HRMD_A** メッセージタイプまでスクロールします。
5. 「**HRMD_A**」チェックボックスを選択し、「保存」をクリックします。

変更ポインタ処理のジョブのスケジューリング

▼ 変更ポインタ処理のジョブをスケジュールする

1. トランザクションコード **SE38** を入力してバリアントの定義を開始します。
2. **RBDMIDOC** プログラムを選択し、「作成」アイコンをクリックします。
3. バリアントに名前を付け、説明を入力します。バリアント名は、ジョブをスケジュールするときに使用できるように記録しておきます。
4. **HRMD_A** メッセージタイプを選択し、「保存」をクリックします。バリアントの属性を選択するように求められます。バックグラウンド処理属性を選択します。
5. 「保存」をクリックします。

ジョブのスケジューリング

▼ ジョブをスケジュールする

1. トランザクションコード **SM36** を入力します。
2. ジョブに名前を付けます。
3. ジョブクラスを割り当てます。ジョブクラスは、ジョブを処理する優先順位です。クラス **A** は優先順位がもっとも高く、最初に処理されます。本稼働環境では、クラス **B** または **C** を割り当てます。
4. 開始時間をスケジュールします。「開始条件」をクリックし、「日付/時刻」をクリックします。スケジュールする開始時刻を入力します。 これは未来のイベントである必要があります。

   a. このジョブを周期的ジョブとして指定します。「周期値」をクリックし、ジョブを実行する頻度を指定して、**Enter** キーを押します。テストのため、この期間を **5** 分に設定します。

   b. 「保存」をクリックします。
5. ジョブステップを定義します。

   a. **ABAP** プログラム名 **(RBDMIDOC)** を入力します。

   b. 前の手順で作成したバリアントを選択します。

6 「保存」をクリックします (注意:「保存」は 1 回だけクリックする。 2 回以上クリックすると、ジョブが複数回実行されるようにスケジュールされる)。

変更ポインタの設定のテスト

▼ 変更ポインタの設定をテストする

1 SAP クライアントで、従業員を雇用します。

2 IDoc が作成されたことを確認します。IDoc が作成されたことは、次の 2 か所で確認できます。

- トランザクションコード WE02 を入力し、検索日付パラメータを入力して、生成された IDOC のリストを生成します。
- SAP HR Active Sync アダプタのログを確認します。

CPIC ユーザーの作成

SAP Basis ユーザーは、クライアントに依存します。このドライバを使用する SAP HR Active Sync アダプタごとに、CPIC にアクセスするシステムユーザーを作成します。

▼ CPIC ユーザーを作成する

1 SAP の「ユーザー管理」で、ユーザーダイアログボックスにユーザー名を入力し、「作成」アイコンをクリックします。

2 「アドレス」タブをクリックし、姓フィールドと書式フィールドにデータを入力します。

3 「Logon データ」タブをクリックし、初期パスワードを定義して、ユーザータイプを通信データに設定します。

4 「Profile」タブをクリックし、SAP_ALL、SAP_NEW、および S_A.CPIC の各プロファイルを追加します。

5 「保存」をクリックします。

注 – 最初に、ダイアログユーザーを作成して、SAP システムの設定をテストできます。処理に問題がある場合は、デバッガでダイアログユーザーを分析できます。また、SAP システムに一度ログインして、このユーザーのパスワードを設定するようにしてください。システムがテストされ、正常に動作したあとは、セキュリティー対策のために CPIC ユーザーに切り替えるようにしてください。

Identity Manager のインストールに関する注意事項

SAP リソースアダプタは、カスタムアダプタです。インストールプロセスを完了するには、次の手順を実行する必要があります。

▼ SAP リソースアダプタをインストールする

1. **http://service.sap.com/connectors** から **JCo (Java Connector)** ツールキットをダウンロードします。**SAP JCO** ダウンロードページにアクセスするには、ログインとパスワードが必要です。このツールキットには、`sapjco-ntintel-2.1.8.zip` のような名前が付けられます。この名前は、選択したプラットフォームやバージョンによって異なります。

   注 – ダウンロードする JCo ツールキットが、アプリケーションサーバーが動作する Java のビットバージョンと一致していることを確認します。たとえば、JCo は Solaris x86 プラットフォーム上の 64 ビットバージョンでのみ使用できます。したがって、アプリケーションサーバーが Solaris x86 プラットフォーム上の 64 ビットバージョンで実行されている必要があります。

2. ツールキットを解凍し、インストール手順に従います。必ずライブラリファイルを正しい場所に配置し、環境変数を指示どおりに設定してください。

3. `sapjco.jar` ファイルを *InstallDir*`\WEB-INF\lib` ディレクトリにコピーします。

4. **SAP Java Base IDoc Class Library** をダウンロードします。このライブラリは、`sapidoc-1.0.1.zip` のような名前の **ZIP** ファイルに格納されています。

5. ライブラリを解凍し、インストール手順に従います。

6. `sapidoc.jar` ファイルを *InstallDir*`\WEB-INF\lib` ディレクトリにコピーします。

7. **SAP Java Connector IDoc Class Library** をダウンロードします。このライブラリは、`sapidocjco-1.0.1.zip` のような名前の **ZIP** ファイルに格納されています。

8 ライブラリを解凍し、インストール手順に従います。

9 `sapidocjco.jar` ファイルを *InstallDir*`\WEB-INF\lib` ディレクトリにコピーします。

使用上の注意

ここでは、SAP HR Active Sync リソースアダプタの使用に関する情報を示します。 次のトピックで構成されています。

- 384 ページの「全般的な注意事項」
- 384 ページの「SNC (Secure Network Communications) 接続の有効化」
- 384 ページの「SAP JCO および RFC のトレース」

全般的な注意事項

このリソースに関する全般的な注意事項は次のとおりです。

- `waveset.properties` ファイル内の `sources.`*ResourceName* `.hosts` プロパティーを使用して、Active Sync を使用してリソースの同期を行うクラスタ内のホストを選択できます。*ResourceName* は、リソースオブジェクトの名前に置き換える必要があります。

SNC (Secure Network Communications) 接続の有効化

デフォルトでは、SAP アダプタは SAP Java Connector (JCo) を使用して SAP アダプタと通信します。SNC 接続の実装については、第 54 章「SNC (Secure Network Communications) 接続の有効化」を参照してください。

SAP JCO および RFC のトレース

SAPHRActiveSyncAdapter には、SAP JCO および RFC のトレース用のリソース属性が用意されています。これらを使用して、Identity Manager と SAP システムの通信をトレースできます。属性名は、「SAP JCO トレースレベル」と「SAP JCO トレースディレクトリ」です。

環境内に次の環境変数を設定すると、SAP RFC トレースを有効にできます。これらの変数は、アプリケーションサーバーを起動する前に環境内に設定してください。これらの変数は、JCO が SAP システムとの通信に使用する共有ライブラリを制御します。

- RFC_TRACE: 0 または 1
- RFC_TRACE_DUMP: 0 または 1
- RFC_TRACE_DIR: トレースファイルのディレクトリへのパス
- CPIC_TRACE_DIR: トレースファイルのディレクトリへのパス

注 – JCO のトレースが必要でない場合は、トレースファイルが作成されないように、RFC_TRACE を 0 に設定してください。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は、SAP Java Connector (JCo) 経由の BAPI を使用して SAP アダプタと通信します。

必要な管理特権

SAP HR に接続するユーザー名を、SAP HR ユーザーにアクセスできるロールに割り当ててください。

プロビジョニングに関する注意事項

デフォルトの SAP HR Active Sync アダプタは読み取り専用です。このアダプタを使用してアカウントを作成または変更することはできません。

機能	サポート状況
アカウントの有効化/無効化	なし
アカウントの名前の変更	なし
パススルー認証	なし
前アクションと後アクション	なし
データ読み込みメソッド	■ リソースから直接インポート ■ Active Sync (SAP HR Active Sync アダプタのみ) ■ 調整

アカウント属性

スキーママップ内のアカウント属性は、_ (下線) ではなく : (コロン) で区切られるようになりました。これにより、SAP HR の属性を、情報タイプ内の単純な属性ではなく、任意の深さの属性へのパスにすることができます。

属性パスの基本形式は次のとおりです。

```
infoType:subType:iDocDef:attrName
```

注 – 属性パスの *iDocDef* (IDoc 定義) セグメントと *attrName* セグメントは拡張できます。

有効な属性パスの例は、`0105:MAIL:E2P0105001:ID` などです。*infoType* は `0105`、*subType* は `MAIL`、*iDocDef* は `E2P0105001`、および *attrName* は `ID` です。

必要な属性が最初の IDoc 定義よりも深い場合は、*attrName* の前に任意の数の IDoc 定義をそれぞれ区切り文字の : (コロン) で区切って指定できます。たとえば、`0002::E2P0002001:E2Q0002002:PERNR` には次の要素が含まれています。

infoType。0002

subType。なし。属性にサブタイプがない場合は、NULL フィールドまたは空白文字を使用します。

*iDocDef*1。E2P0002001

iDocDef2。E2Q0002002

attrName。PERNR

IDoc 定義オブジェクトは GenericObject として返される場合もあります。前述の例を使用すると、E2Q0002002 の IDoc 定義を GenericObject として取得するには、リソースユーザー属性を `0002::E2P0002001:E2Q0002002` としてスキーママップに指定します。

さらに、属性がリストであることを示すために、[ ] (左角括弧と右角括弧) をパス名に付加できます。たとえば、ある特定の属性が複数の値を持つことができる場合、属性名に [ ] を付加すると、その属性の値はリストとして返されます。これは、たとえば次のようになります。

```
1001:B008:E2P1001001:VARYF[]
```

属性が複数の値を取るが、属性名に [ ] が付加されていない場合は、最後の値が属性の値として使用されます。

デフォルトでは、次の情報タイプがサポートされます。

Infotype	「名前」	サポートされるサブタイプ
0000	アクション	適用不可
0001	所属	適用不可

Infotype	「名前」	サポートされるサブタイプ
0002	個人データ	適用不可
0006	住所	01 (現住所)、03 (帰省先住所)
0105	通信	MAIL (電子メール)。 0010 (電子メール)

次の表に、SAP HR Active Sync のアカウント属性に関する情報を示します。

アクション属性

ユーザー属性	リソース属性名	説明
actions_end_date	0000::E2P0000001:ENDDA	終了日
actions_start_date	0000::E2P0000001:BEGDA	開始日
actions_sequence_number	0000::E2P0000001:SEQNR	同じキーを持つ情報タイプレコード数
actions_last_changed_by	0000::E2P0000001:UNAME	オブジェクトの変更者名
actions_last_changed	0000::E2P0000001:AEDTM	最終変更日
actions_change_reason	0000::E2P0000001:PREAS	マスターデータの変更理由
actions_flag1	0000::E2P0000001:FLAG1	予約項目/未使用項目
actions_flag2	0000::E2P0000001:FLAG2	予約項目/未使用項目
actions_flag3	0000::E2P0000001:FLAG3	予約項目/未使用項目
actions_flag4	0000::E2P0000001:FLAG4	予約項目/未使用項目
actions_reserved1	0000::E2P0000001:RESE1	予約項目/未使用項目 (項目長 2)
actions_reserved2	0000::E2P0000001:RESE2	予約項目/未使用項目 (項目長 2)
actions_type	0000::E2P0000001:MASSN	アクションタイプ
actions_reason	0000::E2P0000001:MASSG	アクションの理由
actions_customer_status	0000::E2P0000001:STAT1	カスタマ定義区分ステータス
actions_employment_status	0000::E2P0000001:STAT2	在籍区分ステータス
actions_special_payment_status	0000::E2P0000001:STAT3	特給区分ステータス

所属属性

ユーザー属性	リソース属性名	説明
org_admingroup	0001::E2P0001001:ADMINGROUP	管理者グループ
org_bus_area	0001::E2P0001001:BUS_AREA	事業領域
org_ch_on	0001::E2P0001001:CH_ON	最終変更日
org_changed_by	0001::E2P0001001:CHANGED_BY	オブジェクトの変更者名
org_cnfrm_flag	0001::E2P0001001:CNFRM_FLAG	確認フィールドの有無
org_co_area	0001::E2P0001001:CO_AREA	管理領域
org_comp_code	0001::E2P0001001:COMP_CODE	会社コード
org_contract	0001::E2P0001001:CONTRACT	労働契約
org_costcenter	0001::E2P0001001:COSTCENTER	コストセンター
org_egroup	0001::E2P0001001:EGROUP	従業員グループ
org_esubgroup	0001::E2P0001001:ESUBGROUP	従業員サブグループ
org_flag1	0001::E2P0001001:FLAG1	予約項目/未使用項目
org_flag2	0001::E2P0001001:FLAG2	予約項目/未使用項目
org_flag3	0001::E2P0001001:FLAG3	予約項目/未使用項目
org_flag4	0001::E2P0001001:FLAG4	予約項目/未使用項目
org_from_date	0001::E2P0001001:FROM_DATE	開始日
org_fund	0001::E2P0001001:FUND	基金
org_funds_ctr	0001::E2P0001001:FUNDS_CTR	基金センター
org_hist_flag	0001::E2P0001001:HIST_FLAG	履歴レコードフラグ
org_infotype	0001::E2P0001001:INFOTYPE	情報タイプ
org_job	0001::E2P0001001:JOB	ジョブ
org_jobtxt	0001::E2P0001001:JOBTXT	
org_leg_person	0001::E2P0001001:LEG_PERSON	法人
org_lock_ind	0001::E2P0001001:LOCK_IND	HR マスターデータレコードのロックインジケータ
org_name	0001::E2P0001001:NAME	従業員または応募者の、形式に合わせた名前

ユーザー属性	リソース属性名	説明
org_object_id	0001::E2P0001001:OBJECT_ID	オブジェクト識別
org_objecttype	0001::E2P0001001:OBJECTTYPE	オブジェクトタイプ
org_org_key	0001::E2P0001001:ORG_KEY	組織キー
org_org_unit	0001::E2P0001001:ORG_UNIT	Organizational Unit
org_orgtxt	0001::E2P0001001:ORGTXT	
org_p_subarea	0001::E2P0001001:P_SUBAREA	担当者のサブ領域
org_payarea	0001::E2P0001001:PAYAREA	給与支払領域
org_payr_admin	0001::E2P0001001:PAYR_ADMIN	給与支払管理者
org_perno	0001::E2P0001001:PERNO	担当者番号
org_pers_admin	0001::E2P0001001:PERS_ADMIN	HR マスターデータの管理者
org_pers_area	0001::E2P0001001:PERS_AREA	担当者領域
org_position	0001::E2P0001001:POSITION	Position
org_postxt	0001::E2P0001001:POSTXT	
org_reason	0001::E2P0001001:REASON	マスターデータの変更理由
org_ref_flag	0001::E2P0001001:REF_FLAG	参照フィールドの有無 (一次/二次コスト)
org_reserved1	0001::E2P0001001:RESERVED1	予約項目/未使用項目 (項目長 2)
org_reserved2	0001::E2P0001001:RESERVED2	予約項目/未使用項目 (項目長 2)
org_screenctrl	0001::E2P0001001:SCREENCTRL	情報タイプ画面制御
org_seqno	0001::E2P0001001:SEQNO	同じキーを持つ情報タイプレコード数
org_sort_name	0001::E2P0001001:SORT_NAME	従業員の名前 (姓名でソート可能)
org_subtype	0001::E2P0001001:SUBTYPE	サブタイプ
org_supervisor	0001::E2P0001001:SUPERVISOR	スーパーバイザ領域
org_textflag	0001::E2P0001001:TEXTFLAG	情報タイプのテキストの有無
org_time_admin	0001::E2P0001001:TIME_ADMIN	時間記録の管理者
org_to_date	0001::E2P0001001:TO_DATE	終了日

個人データリソース

ユーザー属性	リソース属性名	説明
academicgrade	0002::E2P0002001:ACADEMICGRADE	学位
aristrocratictitle	0002::E2P0002001:ARISTROCRATIC TITLE	名前の補足 (Lord、Lady など)
birthplace	0002::E2P0002001:BIRTHPLACE	従業員の出生地
countryofbirth	0002::E2P0002001:COUNTRYOFBIRTH	従業員の出生国
dateofbirth	0002::E2P0002001:DATEOFBIRTH	従業員の誕生日
employeeno	0002::E2P0002001:EMPLOYEENO	必須。従業員番号
firstname	0002::E2P0002001:FIRSTNAME	従業員の姓必須。
formofaddress	0002::E2P0002001:FORMOFADDRESS	敬称キー
fullname	0002::E2P0002001:FULLNAME	従業員のフルネーム
gender	0002::E2P0002001:GENDER	従業員の性別を示します
idnumber	0002::E2P0002001:IDNUMBER	担当者の ID 番号 (社会保障番号など)
initials	0002::E2P0002001:INITIALS	従業員のイニシャル
knownas	0002::E2P0002001:KNOWNAS	従業員が希望する呼び名。
language	0002::E2P0002001:LANGUAGE	言語キー
language_iso	0002::E2P0002001:LANGUAGE_ISO	ISO 639 言語コード
lastname	0002::E2P0002001:LASTNAME	従業員の名
maritalstatus	0002::E2P0002001:MARITALSTATUS	結婚歴キー
maritalstatussince	0002::E2P0002001:MARITALSTATUS SINCE	現在の結婚歴の有効開始日
middlename	0002::E2P0002001:MIDDLENAME	従業員のミドルネーム
name_format_indicator	0002::E2P0002001:NAME_FORMAT _INDICATOR	リスト内の従業員の名前形式 ID
nameatbirth	0002::E2P0002001:NAMEATBIRTH	出生時の名前または姓
nameofcountryofbirth	0002::E2P0002001:NAMEOFCOUNTRY OFBIRTH	出生国

ユーザー属性	リソース属性名	説明
nameofformofaddress	0002::E2P0002001:NAMEOFFORMOF ADDRESS	敬称の名前
nameofgender	0002::E2P0002001:NAMEOFGENDER	性別の名前
nameoflanguage	0002::E2P0002001:NAMEOFLANGUAGE	言語の名前
nameofmaritalstatus	0002::E2P0002001:NAMEOFMARITAL STATUS	結婚歴の名前
nameofnationality	0002::E2P0002001:NAMEOFNATIONALITY	国籍の名前
nameofreligion	0002::E2P0002001:NAMEOFRELIGION	宗教の名前
nameofsecondnationality	0002::E2P0002001:NAMEOFSECOND NATIONALITY	第二国籍の名前
nameofstateofbirth	0002::E2P0002001:NAMEOFSTATE OFBIRTH	出生州の名前
nameofthirdnationality	0002::E2P0002001:NAMEOF THIRD NATIONAL ITY	第三国籍の名前
nationality	0002::E2P0002001:NATIONALITY	従業員の第一国籍
numberofchildren	0002::E2P0002001:NUMBER OFCHILDREN	従業員の子供の数。
recordnr	0002::E2P0002001:RECORDNR	同じキーを持つ情報タイプレコード数
religion	0002::E2P0002001:RELIGION	宗教団体を特定するために使用される 2 文字のコード。
secondacadgrade	0002::E2P0002001:SECONDACADGRADE	第二学位
secondname	0002::E2P0002001:SECONDNAME	姓
secondnameprefix	0002::E2P0002001:SECONDNAMEPREFIX	姓の前置語
secondnationality	0002::E2P0002001:SECONDNATIONALITY	従業員の第二国籍
stateofbirth	0002::E2P0002001:STATEOFBIRTH	従業員が出生した州または都道府県
surnameprefix	0002::E2P0002001:SURNAMEPREFIX	姓の前置語 (von、van der、de la など)
thirdnationality	0002::E2P0002001:THIRDNATIONALITY	第三国籍

ユーザー属性	リソース属性名	説明
validbegin	0002::E2P0002001:VALIDBEGIN	従業員データが有効になる日付
validend	0002::E2P0002001:VALIDEND	従業員データが無効になる日付

住所リソース

ユーザー属性	リソース属性名	説明
addresstype_permanent_address	0006:1:E2P0006001:ADDRESS TYPE	現住所のアドレスタイプ
addresstype_home_address	0006:3:E2P0006003:ADDRESS TYPE	自宅住所のアドレスタイプ
city_permanent_address	0006:1:E2P0006001:CITY	現住所の市
city_home_address	0006:3:E2P0006003:CITY	自宅住所の市
coname_permanent_address	0006:1:E2P0006001:CONAME	従業員の現住所の気付 (c/o) の情報。
coname_home_address	0006:3:E2P0006003:CONAME	従業員の自宅住所の気付 (c/o) の情報。
country_permanent_address	0006:1:E2P0006001:COUNTRY	現住所の国コード
country_home_address	0006:3:E2P0006003:COUNTRY	自宅住所の国コード
district_permanent_address	0006:1:E2P0006001:DISTRICT	現住所の地区
district_home_address	0006:3:E2P0006003:DISTRICT	自宅住所の地区
nameofaddresstype_ permanent_address	0006:1:E2P0006001:NAMEOF ADDRESSTYPE	現住所に割り当てられたアドレスタイプ。
nameofaddresstype_home_address	0006:3:E2P0006003:NAMEOF ADDRESSTYPE	自宅住所に割り当てられたアドレスタイプ
nameofcountry_permanent_address	0006:1:E2P0006001:NAMEOF COUNTRY	現住所の国
nameofcountry_home_address	0006:3:E2P0006003:NAMEOF COUNTRY	自宅住所の国
nameofstate_permanent_address	0006:1:E2P0006001:NAMEOF STATE	現住所の州名または都道府県名

ユーザー属性	リソース属性名	説明
nameofstate_home_address	0006:3:E2P0006003:NAMEOF STATE	自宅住所の州名または都道府県名
postalcodecity_permanent_address	0006:1:E2P0006001:POSTALCODE CITY	現住所の郵便番号の市部分
postalcodecity_home_address	0006:3:E2P0006003:POSTALCODE CITY	自宅住所の郵便番号の市部分
recordnr_permanent_address	0006:1:E2P0006001:RECORDNR	
recordnr_home_address	0006:3:E2P0006003:RECORDNR	
scndaddressline_permanent_address	0006:1:E2P0006001:SCNDADDRESS LINE	現住所の第二住所行。
scndaddressline_home_address	0006:3:E2P0006003:SCNDADDRESS LINE	自宅住所の第二住所行。
state_permanent_address	0006:1:E2P0006001:STATE	現住所の州または都道府県
state_home_address	0006:3:E2P0006003:STATE	自宅住所の州または都道府県
streetandhouseno_permanent_address	0006:1:E2P0006001: STREETAND HOUSENO	現住所の街路名および番地
streetandhouseno_home_address	0006:3:E2P0006003:STREETAND HOUSENO	自宅住所の街路名および番地
telephonenumber_permanent_address	0006:1:E2P0006001:TELEPHONE NUMBER	現住所の第一電話番号
telephonenumber_home_address	0006:3:E2P0006003:TELEPHONE NUMBER	自宅住所の第一電話番号
validbegin_permanent_address	0006:1:E2P0006001:VALIDBEGIN	現住所が有効になる日付
validbegin_home_address	0006:3:E2P0006003:VALIDBEGIN	自宅住所が有効になる日付
validend_permanent_address	0006:1:E2P0006001:VALIDEND	現住所が無効になる日付
validend_home_address	0006:3:E2P0006003:VALIDEND	自宅住所が無効になる日付

通信リソース

ユーザー属性	リソース属性名	説明
commtype_communication_EMail	0105:0010:E2P0105001: COMMTYPE	通信タイプのキー (インターネット)
commtype_communication_EMail2	0105:MAIL:E2P0105001:COMMTYPE	通信タイプのキー (電子メール)
delimit_date_communication_EMail	0105:0010:E2P0105001:DELIMIT _DATE	インターネットアドレスを区切るためのキー日付
delimit_date_communication_EMail2	0105:MAIL:E2P0105001:DELIMIT _DATE	電子メールアドレスを区切るためのキー日付
email_communication_EMail	0105:0010:E2P0105001:ID	インターネットアドレス
email	0105:MAIL:E2P0105001:ID	電子メールアドレス
nameofcommtype_communication_EMail	0105:0010:E2P0105001:NAMEOFCOMM TYPE	通信タイプの名前 (インターネット)
nameofcommtype_communication_EMail2	0105:MAIL:E2P0105001:NAMEOFCOMM TYPE	通信タイプの名前 (電子メール)
recordnr_communication_EMail	0105:0010:E2P0105001:RECORDNR	
recordnr_communication_EMail2	0105:MAIL:E2P0105001:RECORDNR	
validbegin_communication_EMail	0105:0010:E2P0105001:VALIDBEGIN	インターネットアドレスが有効になる日付
validbegin_communication_EMail2	0105:MAIL:E2P0105001:VALIDBEGIN	電子メールアドレスが有効になる日付
validend_communication_EMail	0105:0010:E2P0105001:VALIDEND	インターネットアドレスが期限切れになる日付

ユーザー属性	リソース属性名	説明
validend_communication_EMail2	0105:MAIL:E2P0105001:VALIDEND	電子メールアドレスが期限切れになる日付

リソースオブジェクトの管理

適用不可

アイデンティティーテンプレート

$accountId$

サンプルフォーム

SAPForm.xml
SAPUserForm_with_RoleEffectiveDates_Timezone.xml
SAPHRActiveSyncForm.xml

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

- com.waveset.adapter.SAPHRActiveSyncAdapter

インストールされている SAP Java Connector (JCO) のバージョンを判定し、それが正しくインストールされているかどうかを判定するには、次のコマンドを実行します。

```
java -jar sapjco.jar
```

このコマンドは、JCO のバージョンとともに、SAP システムと通信する JNI プラットフォーム依存ライブラリおよび RFC ライブラリを返します。

プラットフォーム依存ライブラリが見つからない場合は、SAP のマニュアルを参照して、SAP Java Connector の正しいインストール方法を調べてください。

◆ ◆ ◆ 第 35 章

35 SAP Enterprise Portal

SAP Enterprise Portal リソースアダプタは、SAP NetWeaver Enterprise Portal をサポートします。このアダプタは、com.waveset.adapter.SAPPortalResourceAdapter クラスで定義されます。

アダプタの詳細

Identity Manager のインストールに関する注意事項

SAP Enterprise Portal アダプタに必要な追加のインストール手順はありません。

リソースを設定する際の注意事項

SAP Enterprise Portal に、idmservice.par ポータルアーカイブファイルを配備します。idmservice.par ファイルは、インストールイメージのルートフォルダにあります。

ポータルアーカイブは、SAP Enterprise Portal アダプタに必要な com.sap.portal.prt.soap.IDMService ポータルサービスを定義します。アダプタは、SOAP 呼び出しを通してポータルサービスと通信し、Portal 上のオブジェクトを管理します。

Portal 管理者は、idmservice.par をインストールする必要があります。この作業は、SAP Enterprise Portal の管理ユーザーインタフェースを使用して、アップロードするファイルとして idmservice.par を選択することによって、行います。

使用上の注意

SAP Enterprise Portal アダプタは、SAP User Management Engine (UME) を間接的に使用してユーザープロビジョニングを実行します。アダプタは Identity Manager ポータルサービスと通信します。続いて、ポータルサービスが直接 UME を呼び出します。

SAP Portal にインストールされた Identity Manager サービスと通信するには、「Identity Manager ポータルサービスのエンドポイント」リソース属性を設定する必要があります。

エンドポイントの例を次に示します。

```
https://myhost:50000/irj/servlet/prt/soap/com.sap.portal.
prt.soap.IDMService
```

「**SAP Portal** 管理者」リソース属性と「**SAP Portal** 管理者のパスワード」リソース属性は、SAP Portal の管理者のユーザー名とパスワードを定義します。

「設定のテスト」ボタンでは、Identity Manager ポータルサービスに対するステータス呼び出しを実行することにより、エンドポイント、ユーザー名、およびパスワードが有効かどうかが確認されます。

セキュリティーに関する注意事項

セキュリティーを向上させるため、次のように設定してください。

- `com.sap.portal.prt.soap.IDMService` ポータルサービスは、SAP Portal によって公開されている SSL 暗号化ポートを使用した場合にのみアクセスできるようにしてください。
- `com.sap.portal.prt.soap.IDMService/high_safety` セキュリティーゾーンを変更して、SAP super_admin ロールのみが含まれるようにしてください。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	なし
パススルー認証	あり

機能	サポート状況
前アクションと後アクション	なし
データ読み込みメソッド	■ リソースから直接インポート ■ リソースの調整

アカウント属性

次の表に、SAP Enterprise Portal ユーザーのアカウント属性を示します。特に記載されていないかぎり、アカウント属性の型はすべて String です。

Identity Manager ユーザー属性	リソースユーザー属性	説明
sap_groups	groups	ユーザーが直接のメンバーである SAP グループ
sap_roles	roles	ユーザーがディレクトリメンバーである SAP ロール
title	title	ユーザーの学位または貴族の称号
firstname	firstName	ユーザーの名
lastname	lastName	ユーザーの姓。
fullname	displayName	ユーザーの表示名
email	email	ユーザーのデフォルトの電子メールアドレス
telephone	telephone	ユーザーのデフォルトの電話番号
fax	fax	ユーザーのデフォルトの FAX 番号
cellPhone	cellPhone	ユーザーのデフォルトの携帯電話番号
street	street	ユーザーの自宅住所の街路
city	city	ユーザーの自宅住所の市
state	state	ユーザーの自宅住所の州または都道府県
zipcode	zip	ユーザーの自宅住所の郵便番号
country	country	ユーザーが居住する国を表す 2 つの英大文字による ISO 3166 コード。この値は、ロケールで指定された国と必ずしも一致しません。
timeZone	timeZone	ユーザーのタイムゾーン
locale	locale	ユーザーのロケール (en_US、fr_CA など)

Identity Manager ユーザー属性	リソースユーザー属性	説明
currency	currency	ユーザーの通貨を表す 3 文字の英大文字によるコード (USD、EUR、YEN など)
screenReader	screenReader	ブール型。ユーザーに対する画面表示を有効または無効にします。
department	department	ユーザーの部署
jobTitle	jobTitle	ユーザーの役職
salutation	salutation	ユーザーの敬称 (Mr.、Mrs.、Dr. など)

SAP Enterprise Portal

リソースオブジェクトの管理

SAP のグループとロールがサポートされます。

アイデンティティーテンプレート

```
$accountId$
```

サンプルフォーム

サンプルフォームは、`sample/forms/SAPPortalUserForm.xml` にあります。このサンプルフォームを使用する場合は、`sample/rules/SAPPortalUserFormRules.xml` もインポートする必要があります。

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

```
com.waveset.adapter.SAPPortalResourceAdapter
```

さらに、リソースインスタンスに対して次の Identity Manager ロギングパラメータを設定できます。

- ログファイルパス
- ログファイルの最大サイズ
- ログレベル

SAP Enterprise Portal サーバーのポータルサービスのログを表示するには、SAP サーバーのインストールファイルの `WEB-INF/portal/logs/idm.log` ファイルを参照してください。

ポータルサービスは、PORTAL-INF/logger/logger.xml ファイルの PAR で定義されているロガー idm_logger を使用します。デフォルトでは、idm_logger はすべてのメッセージのログを記録するように設定されています。

◆ ◆ ◆ 第 36 章

36 Scripted Gateway

このアダプタは、com.waveset.adapter.ScriptedGatewayResourceAdapter クラスで定義されます。

スクリプトゲートウェイアダプタは、Sun Identity Manager Gateway で実行されるバッチファイルで制御されるリソースを管理します。このアダプタは汎用アダプタであるため、高度な設定が可能です。

アダプタの詳細

リソースを設定する際の注意事項

なし

Identity Manager のインストールに関する注意事項

スクリプトホストリソースを Identity Manager のリソースリストに追加するには、「管理するリソースの設定」ページの「カスタムリソース」セクションに次の値を追加する必要があります。

```
com.waveset.adapter.ScriptedGatewayResourceAdapter
```

Sun Identity Manager Gateway (gateway.exe) は、アダプタの「ホスト」フィールドで指定したホストにインストールする必要があります。

使用上の注意

リソースアクション

スクリプトゲートウェイアダプタでは、ユーザーアカウントの作成、更新、削除、取得などの基本的なプロビジョニング機能を実行する一連のアクションを作成できます。これらの各アクションは、それぞれ Windows のバッチファイルに定義されます。

このアダプタは、次のプロビジョニングアクションをサポートします。

アクション	目的	必須であるか
create	新しいユーザーを作成します。	省略可能。ただし、指定されていない場合は、ユーザーを作成できません。
delete	既存のユーザーを削除します。	省略可能。ただし、指定されていない場合は、ユーザーを削除できません。
getAllUsers	リソース上のすべてのユーザーに関する情報を取得します。	はい。
getUser	既存ユーザーの属性を取得します。	はい。
update	既存ユーザーの属性を更新します。	省略可能。ただし、指定されていない場合は、ユーザーを更新できません。

`$WSHOME/sample/ScriptedGateway` ディレクトリには、理論上のゲートウェイスクリプトベースのホストアプリケーションにユーザーをプロビジョニングするのに使用できるリソースアクション定義のサンプルセットが格納されています。環境に合わせてそれらの定義をカスタマイズしてください。

リソースアクションの一般的な情報については、第 50 章「リソースへのアクションの追加」を参照してください。

スクリプト

スクリプトゲートウェイアダプタは、ゲートウェイ上で実行するバッチファイルとしてアクションを実装します。これらのスクリプトは、スクリプトを実行するマシ

ンにインストールされている Windows のバージョン上で実行されるように記述する必要があります。ゲートウェイを実行するアカウントと同じアカウントが、スクリプトも実行します。

スクリプトは、Windows の規則に従い、成功を示すリターンコード 0 で終了するようにしてください。0 以外のコード (スクリプトの作成者が定めた) を返すことは、操作が正しく完了しなかった可能性があるという意味になります。

スクリプトは、Windows の標準エラーや標準出力ストリームにテキストを出力できます。操作の種類、操作のコンテキスト、および失敗のタイプによっては、その操作の結果にテキストを表示することができます。

getUser および getAllUsers 操作では、このテキストは、各ユーザーの属性を特定するために標準出力ストリームで解析されます。

次のタイプの環境変数を、スクリプトにエクスポートできます。

- スキーママップの アイデンティティーシステム リソース属性列で定義されたアカウント属性はいずれも、そのアカウント属性の先頭に `WSUSER_` を付加することで、スクリプトで利用できるようになります。たとえば、アカウント属性の名前が Full Name の場合、その環境変数は `WSUSER_Full Name` という名前になります。
- `WSRSRC_` で始まる環境変数で、アダプタの設定を渡すことができます。もっとも重要な変数は、アダプタの名前を定義する `WSRSRC_Name` です。異なるリソースで同じスクリプトを実行する場合は、この変数を実装すると、それぞれのゲートウェイで同じ操作を行うスクリプトの複数のコピーを維持する手間を省けます。
- `WSOBJ_ID` 変数と `WSOBJ_NAME` 変数は、それぞれアカウント ID とアカウント名を定義します。これらの変数は、スクリプトゲートウェイアダプタでのみ使用できます。

次の例は、サンプルで生成される環境を示しています。

```
WSUSER_Email=testuser@waveset.com
WSUSER_First Name=JUnit
WSUSER_Full Name=JUnit TestUser
WSUSER_Last Name=TestUser
WSUSER_User ID=USER5647
WSUSER_ws_action_type=WindowsBatch
WSOBJ_ID=testuser
WSOBJ_NAME=testuser
WSRSRC_NAME=Scripted Gateway
WSRSRC_CLASS=com.waveset.adapter.ScriptedGatewayResourceAdapter
WSRSRC_Host=localhost
WSRSRC_List Objects Timeout=900000
WSRSRC_Request Timeout=30000
WSRSRC_TCP Port=9278
WSRSRC_connectionLimit=10
```

一般に、属性の値が NULL の場合は、対応する環境変数に長さが 0 の文字列が設定されるのではなく、その環境変数が省略されます。

スクリプトで使用可能な変数については、第 50 章「リソースへのアクションの追加」を参照してください。

結果処理

AttrParse メカニズムは、標準出力ストリームを通して getUser および getAllUsers アクションから返された結果を処理します。AttrParse オブジェクトの実装については、第 49 章「AttrParse オブジェクトの実装」を参照してください。

AttrParse は、getUser アクションに対してユーザー属性のマップを返します。getAllUsers アクションの場合は、マップのマップを生成します。返されるマップの各エントリには、次の内容が含まれます。

- 通常 AttrParse によって返されるようなユーザー属性のマップである値。
- アカウント ID または (ID が不明の場合は) 名前を示すキー。

属性と値を判定するには、AttrParse トークンである collectCsvHeader および collectCsvLines を使用してください。同じような操作を行うほかの AttrParse トークンを使用しないでください。

ゲートウェイタイムアウト

スクリプトゲートウェイでは、`RA_HANGTIMEOUT` リソース属性を使用してタイムアウト値を秒単位で指定できます。この属性は、ゲートウェイに対する要求がタイムアウトしてハングしているとみなされるまでの時間を制御します。

次のように、この属性を Resource オブジェクトに手動で追加する必要があります。

```
<ResourceAttribute name='Hang Timeout'
  displayName='com.waveset.adapter.RAMessages:RESATTR_HANGTIMEOUT' type='int'
  description='com.waveset.adapter.RAMessages:RESATTR_HANGTIMEOUT_HELP' value='
  NewValue'>
</ResourceAttribute>
```

この属性のデフォルト値は 0 です。これは Identity Manager がハングした接続を確認しないことを表します。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Sun Identity Manager Gateway が必要です。

必要な管理特権

スクリプトを実行する管理アカウントは、ゲートウェイで定義されているすべての操作について承認されている必要があります。

プロビジョニングに関する注意事項

次の表に、スクリプトゲートウェイアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの作成	あり
アカウントの更新	あり
アカウントの削除	あり
アカウントの有効化/無効化	あり
アカウントの名前の変更	なし
パススルー認証	なし
前アクションと後アクション	なし
データ読み込みメソッド	リソースから直接インポート 調整

アカウント属性

アカウント属性は多種多様であるため、スクリプトゲートウェイアダプタにはデフォルトのアカウント属性が用意されていません。

アイデンティティーシステムユーザー属性の名前が `accountId` であるアカウント属性を定義する必要があります。

リソースオブジェクトの管理

サポートされません。

アイデンティティーテンプレート

なし。有効な値を持つアイデンティティーテンプレートを設定する必要があります。

サンプルフォーム

なし

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

```
com.waveset.adapter.ScriptedGatewayResouceAdapter
```

◆ ◆ ◆ 第 37 章

37 スクリプトホスト

スクリプトホストリソースアダプタは、OS/390 メインフレーム上のアプリケーションユーザーアカウントの管理をサポートします。このアダプタは、TN3270 エミュレータセッションでホストアプリケーションを管理します。

このアダプタは汎用アダプタであるため、高度な設定が可能です。このアダプタには、管理対象のホストアプリケーションに関する前提条件はありません。代わりに、顧客が提供するスクリプトセットを呼び出すことによってホストアプリケーションとの対話を実行します。

スクリプトホストリソースアダプタは`com.waveset.adapter.ScriptedHostResourceAdapter`クラスで定義されます。

アダプタの詳細

リソースを設定する際の注意事項

なし

Identity Manager のインストールに関する注意事項

スクリプトホストリソースアダプタは、カスタムアダプタです。インストールプロセスを完了するには、次の手順を実行する必要があります。

▼ スクリプトホストリソースアダプタをインストールする

1 スクリプトホストリソースを **Identity Manager** のリソースリストに追加するには、「管理するリソースの設定」ページの「カスタムリソース」セクションに次の値を追加する必要があります。

```
com.waveset.adapter.ScriptedHostResourceAdapter
```

2 適切な **JAR** ファイルを **Identity Manager** インストールの `WEB-INF/lib` ディレクトリにコピーします。

コネクションマネージャー	**JAR** ファイル
Host On Demand	IBM Host Access Class Library (HACL) は、メインフレームへの接続を管理します。HACL を含む推奨 JAR ファイルは `habeans.jar` です。これは、HOD に付属する HOD Toolkit (または Host Access Toolkit) とともにインストールされます。HACL のサポートされるバージョンは、HOD V7.0、V8.0、V9.0、および V10 に含まれるバージョンです。 habeans.jar ファイル ただし、このツールキットを利用できない場合は、HOD のインストールに含まれる次の JAR ファイルを `habeans.jar` の代わりに使用できます。 ■ `habase.jar` ■ `hacp.jar` ■ `ha3270.jar` ■ `hassl.jar` ■ `hodbase.jar` 詳細は、http://www.ibm.com/software/webservers/hostondemand/ を参照してください。
Attachmate WRQ	Sun 製品向け Attachmate 3270 メインフレームアダプタには、メインフレームへの接続の管理に必要なファイルが含まれます。 ■ `RWebSDK.jar` ■ `wrqtls12.jar` ■ `profile.jaw` この製品の入手については、Sun プロフェッショナルサービスにお問い合わせください。

3 `Waveset.properties` ファイルに次の定義を追加して、端末セッションを管理するサービスを定義します。

```
serverSettings.serverId.mainframeSessionType=Value
serverSettings.default.mainframeSessionType=Value
```

Value は、次のように設定できます。

- 1 は、IBM Host On-Demand (HOD) を示します。
- 3 は、Attachmate WRQ を示します。

  これらのプロパティーが明示的に設定されていなければ、Identity Manager はまず WRQ を使用し、次に HOD を使用します。

4 **Attachmate** ライブラリが **WebSphere** または **WebLogic** アプリケーションサーバーにインストールされている場合は、`com.wrq.profile.dir=`*LibraryDirectory* プロパティーを `WebSphere/AppServer/configuration/config.ini` または `startWeblogic.sh` ファイルに追加します。

これにより、Attachmate コードでライセンスファイルを検索できます。

5 スクリプトホストアダプタでは、顧客が提供する **Javascript** が必要です。それらのスクリプトは **Mozilla Rhino** と互換性がある必要があります。**Identity Manager** には **Mozilla Rhino v1_5R2** が用意されており、`$WSHOME/WEB-INF/lib/javascript.jar` にあります。

改善された Javascript エラー報告機能が必要な場合は、最新バージョンの Mozilla Rhino (http://www.mozilla.org/rhino/) を使うことで、構文エラーやその他のエラーに対するより適確なエラーメッセージを参照することができます。デフォルトの `javascript.jar` を、Mozilla から入手した新しいバージョンに置き換えることもできます。

6 `Waveset.properties` ファイルに加えた変更を有効にするために、アプリケーションサーバーを再起動します。

7 リソースへの **SSL** 接続の設定については、第 **53** 章「メインフレーム接続」を参照してください。

使用上の注意

ここでは、スクリプトホストリソースアダプタの使用に関連する情報を提供します。次のトピックで構成されています。

管理者

ホストリソースアダプタは、同じホストに接続している複数のホストリソースでの親和性管理者に対して最大接続数を強制しません。代わりに、各ホストリソース内部の親和性管理者に対して最大接続数が強制されます。

同じシステムを管理する複数のホストリソースがあり、現在それらが同じ管理者アカウントを使用するように設定されている場合は、同じ管理者がリソースに対して同時に複数のアクションを実行しようとしていないことを確認するために、それらのリソースを更新しなければならない可能性があります。

リソースアクションの指定

スクリプトホストアダプタのリソースウィザードの「リソースパラメータ」ページに表示されるテキストボックスで、ログイン、作成、削除、繰り返しなどのさまざまなプロビジョニングアクションにリソースアクションを指定できます。これらのフィールドは、リポジトリに読み込まれる Rhino Javascript を格納する ResourceAction オブジェクトを参照します。

▼ 実行時に、アダプタは次の処理を行います。

1. 現在のプロビジョニングアクションに対応する **ResourceAction** から **Javascript** を読み込む。
2. 必要な **Java** 入力オブジェクトを **Javascript** で利用できるように準備する。
3. **Javascript** を起動する。
4. **Javascript** から返された結果 **(**または例外やエラー**)** を処理する。

   `$WSHOME/sample/ScriptedHost/ScreenSampleActions.xml` ファイルには、理論上のスクリーンベースのホストアプリケーションにユーザーをプロビジョニングするのに使用できる、リソースアクション定義のサンプルセットが格納されています。それらの定義を、アプリケーションに合わせてカスタマイズする必要があります。

   スクリプトホストアダプタは、次のプロビジョニングアクションに関するエンドユーザーのスクリプティングをサポートします。

アクション	説明	必須であるか
create	新しいユーザーを作成します。	省略可能。ただし、指定されていない場合は、ユーザーを作成できません。
delete	既存のユーザーを削除します。	省略可能。ただし、指定されていない場合は、ユーザーを削除できません。
disable	既存のユーザーを無効にします。	省略可能。ただし、指定されていない場合は、ユーザーを無効にできません。

アクション	説明	必須であるか
enable	既存のユーザーを有効にします。	省略可能。ただし、指定されていない場合は、ユーザーを有効にできません。
getAccountIterator	既存ユーザーの繰り返しの実行に使用されるオブジェクトを返します。	省略可能。ただし、getAccountIterator も listAll も指定されていない場合は、アカウントの反復処理を実行できません。
getUser	既存ユーザーの属性を取得します。	はい。
login	アプリケーションにログインします。	はい。
logoff	アプリケーションからログオフします。	はい。
listAll	既存ユーザー ID のリストを返します。	省略可能。ただし、getAccountIterator も listAll も指定されていない場合は、アカウントの反復処理を実行できません。
update	既存ユーザーの属性を更新します。	省略可能。ただし、指定されていない場合は、ユーザーを更新できません。

どのアクションスクリプトも、java.util.Map クラスで定義されているように、`actionContext` マップを受け取ります。マップに格納できる内容は、アクションごとに異なります。次のそれぞれの節では、各アクションについ説明し、そのアクションに関する次の情報を示します。

- コンテキスト。スクリプトの実行前にアダプタが Javascript 実行コンテキストに追加する `actionContext` マップで使用できる、一連のエントリについて説明します。
- エラー処理。異常やエラーの状況を、スクリプトがどのように処理するかを説明します。

前の表に示されたアクションの詳細については、次の各項を参照してください。

- 414 ページの「create アクション」
- 415 ページの「delete アクション」
- 415 ページの「disable アクション」
- 416 ページの「enable アクション」
- 417 ページの「getAccountIterator アクション」
- 418 ページの「getUser アクション」
- 420 ページの「listAll アクション」

create アクション

create アクションは、ホストアプリケーションにユーザーを作成します。create アクションが定義されていない場合は、新しいユーザーをホストアプリケーションに追加できません。

コンテキスト

actionContext マップには、次のエントリが含まれます。

キー	値の型	値の説明
`hostAccess`	com.waveset.adapter.HostAccess	メインフレームへの 3270 エミュレーションアクセスを提供します。
`adapter`	com.waveset.object.ScriptedHostResourceAdapter	アダプタインスタンス。
`action`	java.lang.String	「`create`」という文字列。
`id`	java.lang.String	作成するユーザーのアカウント ID。
`password`	java.lang.String	存在する場合、これは新しいユーザーの復号化されたパスワードです。
`attributes`	java.lang.Map	新しいユーザーに設定する属性のマップ。キーは、設定する属性を識別します。 値は、その属性に設定する復号化された値です。
`errors`	java.util.List	これは、最初は空のリストです。処理中にエラーが発生した場合にスクリプトがこのリストに java.lang.String オブジェクトを追加するように設定する必要があります。
`trace`	com.waveset.adapter.Trace	実行のトレースに使用されるオブジェクト。スクリプトは、このクラスのメソッドを使用することで、顧客の環境でデバッグ可能なものとなります。

エラー処理

アプリケーション固有のエラーが画面または応答に発生した場合、スクリプトが `errors` キーに適切な文字列を追加します。エラーが発生したと判断するために、さまざまな既知のエラー文字列の検索が必要になることがあります。

errors リストに項目が存在する場合は、作成の失敗とみなされます。さらに、スクリプト内から例外がスローされた場合は、作成の失敗とみなされます。

delete アクション

delete アクションは、指定したユーザーをホストアプリケーションから削除します。delete アクションが定義されていない場合は、ホストアプリケーションからユーザーを削除できません。

コンテキスト

actionContext マップには、次のエントリが含まれます。

キー	値の型	値の説明
id	java.lang.String	削除するユーザーのアカウント ID。
hostAccess	com.waveset.adapter.HostAccess	メインフレームへの 3270 エミュレーションアクセスを提供します。
adapter	com.waveset.object.ScriptedHostResourceAdapter	アダプタインスタンス
action	java.lang.String	「delete」という文字列。
trace	com.waveset.adapter.Trace	実行のトレースに使用されるオブジェクト。スクリプトは、このクラスのメソッドを使用することで、顧客の環境でデバッグ可能なものとなります。
errors	java.util.List	これは、最初は空のリストです。処理中にエラーが発生した場合にスクリプトがこのリストに java.lang.String オブジェクトを追加するように設定する必要があります。

エラー処理

アプリケーション固有のエラーが画面または応答に発生した場合、スクリプトが errors キーに適切な文字列を追加します。エラーが発生したと判断するために、さまざまな既知のエラー文字列の検索が必要になることがあります。

errors リストに項目が存在する場合は、削除の失敗とみなされます。さらに、スクリプト内から例外がスローされた場合は、削除の失敗とみなされます。

disable アクション

disable アクションは、ホストアプリケーション内の既存のユーザーを無効にします。このアクションが定義されていない場合は、ホストアプリケーションのユーザーを無効にできません。

コンテキスト

actionContext マップには、次のエントリが含まれます。

キー	値の型	値の説明
hostAccess	com.waveset.adapter.HostAccess	メインフレームへの 3270 エミュレーションアクセスを提供します。
action	java.lang.String	「disable」という文字列。
id	java.lang.String	無効にするアカウント ID。
errors	java.util.List	これは、最初は空のリストです。処理中にエラーが発生した場合にスクリプトがこのリストに java.lang.String オブジェクトを追加するように設定する必要があります。
trace	com.waveset.adapter.Trace	実行のトレースに使用されるオブジェクト。スクリプトは、このクラスのメソッドを使用することで、顧客の環境でデバッグ可能なものとなります。

エラー処理

アプリケーション固有のエラーが画面または応答に発生した場合、スクリプトが errors キーに適切な文字列を追加します。エラーが発生したと判断するために、さまざまな既知のエラー文字列の検索が必要になることがあります。

errors リストに項目が存在する場合は、無効化の失敗とみなされます。さらに、スクリプト内から例外がスローされた場合は、無効化の失敗とみなされます。

enable アクション

enable アクションは、ホストアプリケーション内の既存のユーザーを有効にします。このアクションが定義されていない場合は、ホストアプリケーションのユーザーを有効にできません。

コンテキスト

actionContext マップには次のエントリが含まれます。

キー	値の型	値の説明
hostAccess	com.waveset.adapter.HostAccess	メインフレームへの 3270 エミュレーションアクセスを提供します。
action	java.lang.String	「enable」という文字列。
id	java.lang.String	有効にするアカウント ID。
errors	java.util.List	これは、最初は空のリストです。処理中にエラーが発生した場合にスクリプトがこのリストに java.lang.String オブジェクトを追加するように設定する必要があります。
trace	com.waveset.adapter.Trace	実行のトレースに使用されるオブジェクト。スクリプトは、このクラスのメソッドを使用することで、顧客の環境でデバッグ可能なものとなります。

エラー処理

アプリケーション固有のエラーが画面または応答に発生した場合、スクリプトが errors キーに適切な文字列を追加します。エラーが発生したと判断するために、さまざまな既知のエラー文字列の検索が必要になることがあります。

errors リストに項目が存在する場合は、有効化の失敗とみなされます。さらに、スクリプト内から例外がスローされた場合は、有効化の失敗とみなされます。

getAccountIterator アクション

getAccountIterator アクションは、既存ユーザーの反復処理の実行に使用するオブジェクトを返します。

アカウントの反復処理 (調整、リソースから読み込み) を実行する場合は、このアクションか listAll アクションのいずれかを定義する必要があります。

getAccountIterator アクションが定義されていない場合は、listAll を呼び出してから listAll のリスト内の ID ごとに getUser を呼び出すことによって、アカウントの反復処理が実行されます。

getAccountIterator アクションが定義されておらず、listAll アクションも定義されていない場合は、アカウントの反復処理はサポートされません。

入力値

actionContext マップには、次のエントリが含まれます。

キー	値の型	値の説明
hostAccess	com.waveset.adapter.HostAccess	メインフレームへの 3270 エミュレーションアクセスを提供します。
adapter	com.waveset.object.ScriptedHostResourceAdapter	アダプタインスタンス
action	java.lang.String	「getAccountIterator」という文字列。
trace	com.waveset.adapter.Trace	実行のトレースに使用されるオブジェクト。スクリプトは、このクラスのメソッドを使用することで、顧客の環境でデバッグ可能なものとなります。

戻り値

スクリプトは、Java インタフェースの com.waveset.adapter.ScriptedHostAccessAdapter.ObjectIterator を実装する Java オブジェクトを返します。

```
public interface ObjectIterator {
    public boolean hasNext();
   public void next(java.util.Map nextObj);
    public void close();
}
```

next() メソッドの nextObj マップ引数は、getUser アクションで説明されている result エントリと同じ方法で、スクリプトによって指定されます。

エラー処理

スクリプト内から例外がスローされた場合は、繰り返しの失敗とみなされます。

スクリプトから返された Java オブジェクトでメソッドを呼び出しているときに例外のスローが発生した場合も、繰り返しの失敗とみなされます。

getUser アクション

getUser アクションは、ホストアプリケーションから次のいずれかの情報を取得します。

- アダプタが特定ユーザーのユーザー属性を解析できる、画面または応答の文字列。
- 特定ユーザーのユーザー属性のマップ。

getUser アクションは、必ず定義してください。

コンテキスト

actionContext マップには、次のエントリが含まれます。

キー	値の型	値の説明
hostAccess	com.waveset.adapter.HostAccess	メインフレームへの 3270 エミュレーションアクセスを提供します。
adapter	com.waveset.object.ScriptedHostResourceAdapter	アダプタインスタンス
action	java.lang.String	「getUser」という文字列。
attrsToGet	java.util.List	取得するユーザー属性を識別する文字列のリスト。このリストは、スキーママップの右側から取得されます。
id	java.lang.String	取得するユーザーのアカウント ID。
errors	java.util.List	これは、最初は空のリストです。処理中にエラーが発生した場合にスクリプトがこのリストに java.lang.String オブジェクトを追加するように設定する必要があります。
trace	com.waveset.adapter.Trace	実行のトレースに使用されるオブジェクト。スクリプトは、このクラスのメソッドを使用することで、顧客の環境でデバッグ可能なものとなります。
result	java.util.Map	スクリプトは、マップにエントリを追加して、ユーザー属性を返します。後述のエントリテーブルを参照してください。

result マップには、スクリプトによって次のエントリが入力される必要があります。

キー	値の型	値の説明
text	String	ユーザー属性に解析されるテキストを含みます。1 つ以上の画面または応答の内容であることもあります。 あとで、このマップの attrParse エントリで指定された AttrParse オブジェクトを使用して、この文字列からユーザー属性が抽出されます。一致するユーザーが見つからない場合は、このエントリをマップに入れないでください。 このフィールドをマップに追加しないでください。代わりに attrMap マップを入力します。

キー	値の型	値の説明
attrParse	String	このマップの text エントリの文字列からユーザー属性を解析するためにアダプタが使用する AttrParse オブジェクトの名前。このエントリは、常に text エントリと一緒に設定します。
attrMap	java.util.Map	スクリプトがユーザー属性を直接取得できる場合は、ユーザー属性のマップでこのエントリを設定できます。この attrMap エントリは、このマップの text エントリが存在しない場合にのみ適用されます。

エラー処理

一致するユーザーが見つからない場合、result マップは空のままにするようにしてください。

アプリケーション固有のエラーが画面または応答に発生した場合、スクリプトが errors キーに適切な文字列を追加します。エラーが発生したと判断するために、さまざまな既知のエラー文字列の検索が必要になることがあります。

errors リストに項目が存在する場合は、取得の失敗とみなされます。さらに、スクリプト内から例外がスローされた場合は、取得の失敗とみなされます。

listAll アクション

listAll アクションは、ホストアプリケーションで見つかったユーザー ID のリストを取得します。

listAll アクションが定義されていない場合は、このリソースインスタンスの FormUtil.listResourceObjects メソッドをフォームから呼び出すことはできません。

listAll アクションと getAccountIterator アクションのどちらも定義されていない場合、アカウントの反復処理 (調整、リソースから読み込み) はサポートされません。

コンテキスト

actionContext マップには、次のエントリが含まれます。

キー	値の型	値の説明
hostAccess	com.waveset.adapter.HostAccess	メインフレームへの 3270 エミュレーションアクセスを提供します。
adapter	com.waveset.object.ScriptedHostResourceAdapter	アダプタインスタンス

キー	値の型	値の説明
action	java.lang.String	「listAll」という文字列。
resultList	java.util.List	スクリプトがこのリストにエントリを追加します。スクリプトがリストに追加する各項目は、ホストアカウント ID に対応する文字列です。
errors	java.util.List	これは、最初は空のリストです。処理中にエラーが発生した場合にスクリプトがこのリストに java.lang.String オブジェクトを追加するように設定する必要があります。
trace	com.waveset.adapter.Trace	実行のトレースに使用されるオブジェクト。スクリプトは、このクラスのメソッドを使用することで、顧客の環境でデバッグ可能なものとなります。

エラー処理

アプリケーション固有のエラーが画面または応答に発生した場合、スクリプトが errors キーに適切な文字列を追加します。エラーが発生したと判断するために、さまざまな既知のエラー文字列の検索が必要になることがあります。

errors リストに項目が存在する場合は、取得の失敗とみなされます。さらに、スクリプト内から例外がスローされた場合は、取得の失敗とみなされます。

login アクション

login アクションは、カスタムホストアプリケーションのユーザーを管理するために必要なホストと、認証されたセッションのネゴシエーションを行います。このアクションは、必ず定義してください。

コンテキスト

actionContext マップには、次のエントリが含まれます。

キー	値の型	値の説明
hostAccess	com.waveset.adapter.HostAccess	メインフレームへの 3270 エミュレーションアクセスを提供します。
action	java.lang.String	「login」という文字列。
ユーザー	java.lang.String	ホストアプリケーション管理ユーザーのユーザー名。

キー	値の型	値の説明
password	com.waveset.util.EncryptedData	ホストアプリケーション管理ユーザーのパスワードを格納する暗号化されたオブジェクト。プレーンテキストに変換するには、decryptToString() を使用します。
errors	java.util.List	これは、最初は空のリストです。処理中にエラーが発生した場合にスクリプトがこのリストに java.lang.String オブジェクトを追加するように設定する必要があります。
trace	com.waveset.adapter.Trace	実行のトレースに使用されるオブジェクト。スクリプトは、このクラスのメソッドを使用することで、顧客の環境でデバッグ可能なものとなります。

エラー処理

アプリケーション固有のエラーが画面または応答に発生した場合、スクリプトが errors キーに適切な文字列を追加します。エラーが発生したと判断するために、さまざまな既知のエラー文字列の検索が必要になることがあります。

errors リストに項目が存在する場合は、ログインの失敗とみなされます。さらに、スクリプト内から例外がスローされた場合は、ログインの失敗とみなされます。

logoff アクション

logoff アクションは、ホストからの切断を実行します。これは、接続が不要になった場合に呼び出されます。このアクションは、必ず定義してください。

コンテキスト

actionContext マップには次のエントリが含まれます。

キー	値の型	値の説明
hostAccess	com.waveset.adapter.HostAccess	メインフレームへの 3270 エミュレーションアクセスを提供します。
action	java.lang.String	「logoff」という文字列。
errors	java.util.List	これは、最初は空のリストです。処理中にエラーが発生した場合にスクリプトがこのリストに java.lang.String オブジェクトを追加するように設定する必要があります。

キー	値の型	値の説明
trace	com.waveset.adapter.Trace	実行のトレースに使用されるオブジェクト。スクリプトは、このクラスのメソッドを使用することで、顧客の環境でデバッグ可能なものとなります。

エラー処理

アプリケーション固有のエラーが画面または応答に発生した場合、スクリプトが errors キーに適切な文字列を追加します。エラーが発生したと判断するために、さまざまな既知のエラー文字列の検索が必要になることがあります。

errors リストに項目が存在する場合は、ログオフの失敗とみなされます。さらに、スクリプト内から例外がスローされた場合は、ログオフの失敗とみなされます。

update アクション

update アクションは、ホストアプリケーションのユーザーを更新します。update アクションが定義されていない場合は、ホストアプリケーションのユーザーを更新できません。

コンテキスト

actionContext マップには、次のエントリが含まれます。

キー	値の型	値の説明
hostAccess	com.waveset.adapter.HostAccess	メインフレームへの 3270 エミュレーションアクセスを提供します。
adapter	com.waveset.object.ScriptedHostResourceAdapter	アダプタインスタンス
action	java.lang.String	「update」という文字列。
id	java.lang.String	変更するユーザーのアカウント ID。
password	java.lang.String	存在する場合、これはユーザーの新しい復号化されたパスワードです。
attributes	java.lang.Map	既存のユーザーで更新する属性のマップ。キーは、設定する属性を識別します。 値は、その属性に設定する復号化された値です。

キー	値の型	値の説明
errors	java.util.List	これは、最初は空のリストです。処理中にエラーが発生した場合にスクリプトがこのリストに java.lang.String オブジェクトを追加するように設定する必要があります。
trace	com.waveset.adapter.Trace	実行のトレースに使用されるオブジェクト。スクリプトは、このクラスのメソッドを使用することで、顧客の環境でデバッグ可能なものとなります。

エラー処理

アプリケーション固有のエラーが画面または応答に発生した場合、スクリプトが errors キーに適切な文字列を追加します。エラーが発生したと判断するために、さまざまな既知のエラー文字列の検索が必要になることがあります。

errors リストに項目が存在する場合は、更新の失敗とみなされます。さらに、スクリプト内から例外がスローされた場合は、更新の失敗とみなされます。

SSL 設定

Identity Manager は TN3270 接続を使用してリソースと通信します。

RACF リソースへの SSL 接続の設定については、第 53 章「メインフレーム接続」を参照してください。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は、TN3270 を使用してスクリプトホストアダプタと通信します。

必要な管理特権

ホストアプリケーションに接続する Identity Manager 管理者には、ホストアプリケーション内でユーザーの作成と管理を行うための十分な特権が与えられている必要があります。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	なし
アカウントの作成	あり
アカウントの更新	あり
アカウントの削除	あり
パススルー認証	なし
前アクションと後アクション	あり
データ読み込みメソッド	■ リソースから直接インポート ■ 調整

アカウント属性

スクリプトホストアダプタには、デフォルトのアカウント属性はありません。これは、管理対象のホストアプリケーションによってアカウント属性が異なるためです。

リソースオブジェクトの管理

サポート対象外

アイデンティティーテンプレート

$accountId$

サンプルフォーム

なし

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

- `com.waveset.adapter.ScriptedHostResourceAdapter`

- `com.waveset.adapter.HostAccess`

HostAccess クラスのトラブルシューティングの詳細については、TopSecret アダプタの「トラブルシューティング」を参照してください。

Javascript へのコンテキストには、渡される `com.waveset.adapter.Trace` オブジェクトが常に存在します。`com.waveset.adapter.ScriptedHostResourceAdapter` でトレースを有効にすると、Javascript でのトレースが有効になります。

また、一時的なトレースを標準出力に表示する場合は、Javascript で Java `System.out.println()` メソッドを呼び出すことができます。たとえば、次のようにします。

```
java.lang.System.out.println(“Hello World”);
```

◆ ◆ ◆ 第 38 章

38 スクリプト JDBC

Identity Manager には、すべてのデータベーススキーマおよび JDBC でアクセス可能なすべてのデータベースのユーザーアカウントの管理をサポートするための、スクリプト JDBC リソースアダプタが用意されています。このアダプタは、データベース内のアカウント変更をポーリングする Active Sync もサポートします。

アダプタの詳細

スクリプト JDBC リソースアダプタは汎用アダプタであるため、高度な設定が可能です。このアダプタには、管理対象のデータベーススキーマに関する前提条件はありません。代わりに、顧客が提供するスクリプトセットを呼び出すことによって JDBC によるデータベースとの対話を実行します。現在、顧客が提供するスクリプトは、Javascript (Rhino) または BeanShell で記述できます。

スクリプト JDBC リソースアダプタは、`com.waveset.adapter.ScriptedJdbcResourceAdapter` クラスで定義されます。

注 – SQL Server へのすべての接続は、同じバージョンの Microsoft SQL Server JDBC ドライバを使用して実行してください。使用可能なバージョンは 2005 または 2000 です。これには、リポジトリだけではなく、SQL Server のアカウントまたはテーブルを管理または要求するすべてのリソースアダプタ (Microsoft SQL アダプタ、Microsoft Identity Integration Server アダプタ、データベーステーブルアダプタ、スクリプト JDBC アダプタ、これらのアダプタをベースとするすべてのカスタムアダプタなど) が含まれます。異なるバージョンのドライバを使用しようとすると、競合エラーが発生します。

インストールの注意点

管理するデータベースに適した JDBC ドライバの JAR を、Identity Manager がインストールされた `WEB-INF\lib` ディレクトリにコピーします。

リソースを設定する際の注意事項

なし

使用上の注意

スクリプト JDBC アダプタによって呼び出される顧客提供のスクリプトは、Javascript または BeanShell で記述されている必要があります。Identity Manager はこれらのスクリプトを、Identity Manager リポジトリに名前付きの ResourceAction オブジェクトとして格納します。

各スクリプト JDBC リソースインスタンスは、名前に基づいて適切な ResourceAction オブジェクトを参照するリソース属性セットによって設定されます。実行時に、アダプタは 次の処理を行います。

▼ 実行時のアダプタのアクション

1. 現在のプロビジョニングアクション (作成、削除、更新など) に対応する **ResourceAction** からスクリプトを読み込む。
2. 必要な **Java** 入力オブジェクトをスクリプトで利用できるように準備する。
3. スクリプトを起動する。
4. スクリプトから返された結果 (または例外やエラー) を処理する。

この「使用上の注意」の残りの部分では、スクリプト JDBC アダプタのプロビジョニングアクション、および各プロビジョニングアクションに割り当てられたスクリプトに対して必要な動作について説明します。

スクリプトは、それ自体に渡された JDBC 接続を閉じることはできません。アダプタが適切な時期に自動的に接続を閉じます。

`sample/ScriptedJdbc` フォルダの下のファイル階層を参照してください。

各サンプルサブフォルダ (`SimpleTable`、`MultiValue`、および `StoredProc`) には、そのサンプルで使用するファイルセットについて説明する `README.txt` ファイルがあります。

スクリプト JDBC アダプタは、次のプロビジョニングアクションに関するエンドユーザーのスクリプティングをサポートします。

Action	説明	必要性
create	新しいユーザーを作成します。	省略可能。ただし、指定されていない場合は、ユーザーを作成できません。
delete	既存のユーザーを削除します。	省略可能。ただし、指定されていない場合は、ユーザーを削除できません。
disable	既存のユーザーをネイティブで無効にします。	省略可能。ただし、指定されていない場合は、ユーザーをネイティブで無効にできません。
enable	既存のユーザーをネイティブで有効にします。	省略可能。ただし、指定されていない場合は、ユーザーをネイティブで有効にできません。
getAccountIterator	既存ユーザーの繰り返しの実行に使用されるオブジェクトを返します。	省略可能。ただし、`getAccountIterator` も `listAll` も指定されていない場合は、アカウントの反復処理を実行できません。
getActiveSyncIterator	Active Sync 繰り返しの実行に使用されるオブジェクトを返します。	省略可能。ただし、指定されていない場合、Active Sync はサポートされません。
test	「設定のテスト」の間にカスタムテストを実行します。	省略可能。
getUser	既存ユーザーの属性を取得します。	省略可能。ただし、指定されていない場合、ユーザーアクションはサポートされません。
listAll	既存ユーザー (またはほかのオブジェクトタイプ) の ID のリストを返します。	省略可能。ただし、`getAccountIterator` も `listAll` も指定されていない場合は、アカウントの反復処理を実行できません。
update	既存ユーザーの属性の更新、名前の変更、またはパスワードの変更を行います。	省略可能。ただし、指定されていない場合は、ユーザーの属性、名前、またはパスワードを変更できません。
authenticate	ユーザー ID とパスワードを確認します。	省略可能。ただし、パススルー認証を実行する場合は必須です。

どの `action` スクリプトも、`java.util.Map` クラスで定義されているように、`actionContext` マップを受け取ります。マップに格納できる内容は、アクションごとに異なります。

前の表に示されたアクションの詳細については、この章内の次の各項を参照してください。

- 430 ページの「create アクション」
- 431 ページの「getUser アクション」

各項では、これらのアクションの説明に加えて、次の情報を提供しています。

- コンテキスト。スクリプトの実行前にアダプタが Javascript 実行コンテキストに追加する `actionContext` マップで使用できる、一連のエントリについて説明します。
- エラー処理。異常やエラー条件を、スクリプトがどのように処理するかを説明します。

create アクション

顧客のデータベースにユーザーを作成するには、`create` アクションを使用します。create アクションが定義されていない場合は、アダプタは顧客のデータベースに新しいユーザーを作成できません。

コンテキスト

`actionContext` マップには次のエントリが含まれます。

キー	値の型	値の説明
`conn`	java.sql.Connection	顧客のデータベースへの JDBC 接続
`adapter`	com.waveset.adapter. ScriptedJdbc ResourceAdapter	アダプタインスタンス
`action`	java.lang.String	「`createUser`」という文字列
`id`	java.lang.String	作成するユーザーのアカウント ID
`password`	java.lang.String	存在する場合、この値は、新しいユーザーの復号化されたパスワードです。

キー	値の型	値の説明
attributes	java.util.Map	新しいユーザーに設定する属性のマップ。 ■ キーは、設定する属性を識別します ■ 値は、その属性に設定する復号化された値を指定します。
errors	java.util.List	最初は、この値は空のリストです。 処理中にエラーが発生した場合、スクリプトによってこのリストに java.lang.String オブジェクトを追加できます。
trace	com.waveset.adapter.Trace	実行のトレースに使用されるオブジェクト スクリプトは、このクラスのメソッドを使用することで、顧客の環境でデバッグ可能なものとなります。

エラー処理

スクリプト内から例外がスローされた場合は、失敗とみなされます。

スクリプトでエラーが発生した場合、スクリプトによって errors キーに適切な文字列を追加することもできます。errors リストに項目が存在する場合は、作成の失敗とみなされます。

getUser アクション

getUser アクションは、顧客のデータベースから既存のユーザー属性のマップを取得します。getUser アクションが定義されていない場合は、アダプタはユーザーアクションを実行できません。

コンテキスト

actionContext マップには次のエントリが含まれます。

キー	値の型	値の説明
conn	java.sql.Connection	顧客のデータベースへの JDBC 接続
adapter	com.wavset.adapter.ScriptedJdbcResourceAdapter	アダプタインスタンス
action	java.lang.String	「getUser」という文字列
id	java.lang.String	取得するユーザーアカウント ID。

キー	値の型	値の説明
attrsToGet	java.util.List	取得するユーザー属性を識別する文字列のリスト。このリストは、スキーママップの右側から取得されます。
result	java.util.Map	■ ユーザーが現在データベースに存在しない場合、スクリプトはこのマップを空のままにします。 ■ ユーザーが存在する場合は、このあとにある、想定されるマップの説明を参照してください。
errors	java.util.List	最初は、この値は空のリストです。 処理中にエラーが発生した場合、スクリプトによってこのリストに java.lang.String オブジェクトを追加できます。
trace	com.waveset.adapter.Trace	実行のトレースに使用されるオブジェクト。 スクリプトは、このクラスのメソッドを使用することで、顧客の環境でデバッグ可能なものとなります。

アダプタは、result マップに次のエントリが入力されることを想定しています。

キー	値の型	値の説明
attrMap	java.util.Map	スクリプトがユーザー属性を直接取得できる場合は、ユーザー属性のマップでこのエントリを設定できます。属性名は、リソースのスキーママップの「リソースユーザー属性」列で定義されます。
isDisabled	java.lang.Boolean または java.lang.String	スクリプトによって Boolean.TRUE または true の文字列に設定されている場合、そのユーザーは無効とみなされます。

エラー処理

スクリプト内から例外がスローされた場合は、失敗とみなされます。

スクリプトでエラーが発生した場合、スクリプトによって errors キーに適切な文字列を追加できます。errors リストに項目が存在する場合は、取得の失敗とみなされます。

deleteアクション

顧客のデータベースからユーザーを削除するには、deleteアクションを使用します。deleteアクションが定義されていない場合、アダプタは顧客のデータベースからユーザーを削除できません。

コンテキスト

actionContextマップには次のエントリが含まれます。

キー	値の型	値の説明
conn	java.sql.Connection	顧客のデータベースへのJDBC接続
adapter	com.wavset.adapter.ScriptedJdbcResourceAdapter	アダプタインスタンス
action	java.lang.String	「deleteUser」という文字列
id	java.lang.String	削除するユーザーアカウントID。
errors	java.util.List	最初は、この値は空のリストです。 処理中にエラーが発生した場合、スクリプトによってこのリストにjava.lang.Stringオブジェクトを追加できます。
trace	com.waveset.adapter.Trace	実行のトレースに使用されるオブジェクト。 スクリプトは、このクラスのメソッドを使用することで、顧客の環境でデバッグ可能なものとなります。

エラー処理

スクリプト内から例外がスローされた場合は、失敗とみなされます。

スクリプトでエラーが発生した場合、スクリプトによってerrorsキーに適切な文字列を追加できます。errorsリストに項目が存在する場合は、削除の失敗とみなされます。

updateアクション

顧客のデータベース内の既存ユーザーを更新するには、updateアクションを使用します。更新には、属性の変更、パスワードの変更、または名前の変更を含めることができます。updateアクションが定義されていない場合は、顧客のデータベース内のユーザーを更新できません。

コンテキスト

actionContext マップには次のエントリが含まれます。

キー	値の型	値の説明
conn	java.sql.Connection	顧客のデータベースへの JDBC 接続
adapter	com.wavset.adapter.ScriptedJdbcResourceAdapter	アダプタインスタンス
action	java.lang.String	「updateUser」という文字列
id	java.lang.String	既存ユーザーのアカウント ID
attributes	java.util.Map	新しいユーザーに設定する属性のマップ。 ■ キーは、設定する属性を識別します ■ 値は、その属性に設定する復号化された値です。 属性のマップエントリが存在しない場合は、その属性を変更しないでください。
newId	java.lang.String	存在する場合、スクリプトは既存ユーザーのアカウント ID (id 属性の値で識別される) を、newId 属性値で指定された新しいアカウント ID に変更する必要があります。
password	java.lang.String	存在する場合、この値はユーザーの新しいパスワードの復号化された値です。
errors	java.util.List	最初は、この値は空のリストです。 処理中にエラーが発生した場合、スクリプトによってこのリストに java.lang.String オブジェクトを追加できます。
trace	com.waveset.adapter.Trace	実行のトレースに使用されるオブジェクト。 スクリプトは、このクラスのメソッドを使用することで、顧客の環境でデバッグ可能なものとなります。

エラー処理

スクリプト内から例外がスローされた場合は、失敗とみなされます。

スクリプトでエラーが発生した場合、スクリプトが errors キーに適切な文字列を追加することもできます。errors リストに項目が存在する場合は、更新の失敗とみなされます。

enableアクション

顧客のデータベース内のユーザーを有効にするには、enableアクションを使用します。顧客のデータベース内のユーザーのスキーマが有効/無効の概念をサポートする場合に、このアクションを実装します。enableアクションが定義されていない場合、アダプタは顧客のデータベース内のユーザーを直接有効にできません。

コンテキスト

actionContextマップには次のエントリが含まれます。

キー	値の型	値の説明
conn	java.sql.Connection	顧客のデータベースへのJDBC接続
adapter	com.wavset.adapter.ScriptedJdbcResourceAdapter	アダプタインスタンス
action	java.lang.String	「enableUser」という文字列
id	java.lang.String	無効にするユーザーアカウントID
errors	java.util.List	最初は、この値は空のリストです。 処理中にエラーが発生した場合、スクリプトによってこのリストにjava.lang.Stringオブジェクトを追加できます。
trace	com.waveset.adapter.Trace	実行のトレースに使用されるオブジェクト。 スクリプトは、このクラスのメソッドを使用することで、顧客の環境でデバッグ可能なものとなります。

エラー処理

スクリプト内から例外がスローされた場合は、失敗とみなされます。

スクリプトでエラーが発生した場合、スクリプトがerrorsキーに適切な文字列を追加することもできます。errorsリストに項目が存在する場合は、失敗とみなされます。

disableアクション

顧客のデータベース内のユーザーを無効にするには、disableアクションを使用します。顧客のデータベース内のユーザーのスキーマが有効/無効の概念をサポートする場合に、このアクションを実装します。disableアクションが定義されていない場合、アダプタは顧客のデータベース内のユーザーを直接無効にできません。

コンテキスト

actionContext マップには次のエントリが含まれます。

キー	値の型	値の説明
conn	java.sql.Connection	顧客のデータベースへの JDBC 接続
adapter	com.wavset.adapter.ScriptedJdbcResourceAdapter	アダプタインスタンス
action	java.lang.String	「disableUser」という文字列
id	java.lang.String	無効にするユーザーアカウント ID
errors	java.util.List	最初は、この値は空のリストです。 処理中にエラーが発生した場合、スクリプトによってこのリストに java.lang.String オブジェクトを追加できます。
trace	com.waveset.adapter.Trace	実行のトレースに使用されるオブジェクト。 スクリプトは、このクラスのメソッドを使用することで、顧客の環境でデバッグ可能なものとなります。

エラー処理

スクリプト内から例外がスローされた場合は、失敗とみなされます。

スクリプトでエラーが発生した場合、スクリプトが errors キーに適切な文字列を追加することもできます。errors リストに項目が存在する場合は、失敗とみなされます。

listAll アクション

顧客のデータベース内にあるユーザー (またはほかのオブジェクトタイプ) の ID のリストを取得するには、listAll アクションを使用します。listAll アクションが定義されていない場合は、FormUtil.listResourceObjects メソッドをこのリソースインスタンスのためにフォームから呼び出すことはできません。

さらに、listAll アクションまたは getAccountIterator アクションが定義されていない場合、アカウントの反復処理 (調整、「リソースから読み込み」) はサポートされません。

コンテキスト

actionContext マップには次のエントリが含まれます。

キー	値の型	値の説明
conn	java.sql.Connection	顧客のデータベースへの JDBC 接続
adapter	com.wavset.adapter.ScriptedJdbcResourceAdapter	アダプタインスタンス
action	java.lang.String	「listAllObjects」という文字列。
objectType	java.lang.String	リストするオブジェクト ID のタイプを示します。 通常、ユーザー ID を表示するには account オブジェクトタイプを使用します。ほかのオブジェクトタイプの ID を生成するようにスクリプトが記述されている場合は、ほかのオブジェクトタイプの ID (group など) を使用できます。
options	java.util.Map	listResourceObjects 呼び出しに渡すことができる追加の (省略可能な) オプション。
resultList	java.util.List	スクリプトがこのリストにエントリを追加します。 スクリプトがこのリストに追加する各項目は文字列 ID です。
errors	java.util.List	最初は、この値は空のリストです。 処理中にエラーが発生した場合、スクリプトによってこのリストに java.lang.String オブジェクトを追加できます。
trace	com.waveset.adapter.Trace	実行のトレースに使用されるオブジェクト。 スクリプトは、このクラスのメソッドを使用することで、顧客の環境でデバッグ可能なものとなります。

エラー処理

スクリプト内から例外がスローされた場合は、失敗とみなされます。

スクリプトでエラーが発生した場合、スクリプトによって errors キーに適切な文字列を追加することもできます。errors リストに項目が存在する場合は、失敗とみなされます。

getAccountIterator アクション

既存ユーザーの繰り返しの実行に使用されるアダプタにオブジェクトを返すには、getAccountIterator アクションを使用します。

アカウントの反復処理 (調整、「リソースから読み込み」) を実行するには、このアクションまたは listAll アクションを定義してください。getAccountIterator アク

ションが定義されていない場合は、listAll を呼び出してから listAll のリスト内の ID ごとに getUser を呼び出すことによって、アカウントの反復処理が実行されます。

さらに、getAccountIterator アクションまたは listAll アクションが定義されていない場合は、アカウントの反復処理はサポートされません。

コンテキスト

actionContext マップには次のエントリが含まれます。

キー	値の型	値の説明
conn	java.sql.Connection	顧客のデータベースへの JDBC 接続。
adapter	com.wavset.adapter.ScriptedJdbcResourceAdapter	アダプタインスタンス
action	java.lang.String	「getAccountIterator」という文字列。
result	java.util.Map	後述の result の説明を参照してください。
errors	java.util.List	最初は、この値は空のリストです。 処理中にエラーが発生した場合、スクリプトによってこのリストに java.lang.String オブジェクトを追加できます。
trace	com.waveset.adapter.Trace	実行のトレースに使用されるオブジェクト。 スクリプトは、このクラスのメソッドを使用することで、顧客の環境でデバッグ可能なものとなります。

アダプタは、result マップに次のエントリが入力されることを想定しています。

キー	値の型	値の説明
iterator	com.waveset.adapter.script.ScriptedIterator	スクリプトによって、この値を ScriptedIterator インタフェースの生成インスタンスに設定する必要があります。 `public interface ScriptedIterator { public boolean hasNext(); public void next(java.util.Map nextObj); public void close();}` nextObj マップについては、次の表を参照してください。 オブジェクトは、顧客のデータベース内のすべてのユーザーを反復処理できる必要があります。 サンプルは、BeanShell および Javascript でこれを行う方法を示しています。

アダプタは、next メソッドに渡される nextObj マップに、iterator によって各繰り返しユーザーの属性が入力されることを想定しています。

キー	値の型	値の説明
attrMap	java.util.Map	スクリプトがユーザー属性を直接取得できる場合は、ユーザー属性のマップでこのエントリを設定できます。属性名は、リソースのスキーママップの「リソースユーザー属性」列で定義されます。
isDisabled	java.lang.Boolean または java.lang.String	スクリプトによって Boolean.TRUE または true の文字列に設定されている場合、そのユーザーは無効とみなされます。

エラー処理

スクリプト内から例外がスローされた場合は、失敗とみなされます。

スクリプトでエラーが発生した場合、スクリプトによって errors キーに適切な文字列を追加することもできます。errors リストに項目が存在する場合は、失敗とみなされます。

getActiveSyncIterator アクション

getActiveSyncIterator アクションは、Active Sync 繰り返しの実行に使用されるアダプタにオブジェクトを返します。

リソースで Active Sync をサポートする場合は、このアクションを定義してください。

コンテキスト

actionContext マップには次のエントリが含まれます。

キー	値の型	値の説明
conn	java.sql.Connection	顧客のデータベースへの JDBC 接続
adapter	com.wavset.adapter.ScriptedJdbcResourceAdapter	アダプタインスタンス
action	java.lang.String	「getActiveSyncIterator」という文字列。
options	java.util.Map	このマップには、lastProcessed キーを持つエントリを含めることができます。このエントリ値は、Active Sync で正常に処理された最後のユーザーの属性のマップです。 lastProcessed エントリを使用して iterator から対象外のユーザーを除外するクエリーを作成する方法の例については、SimpleTable サンプル (SimpleTable-activeSyncIter-bsh.xml スクリプト) を参照してください。
activeSyncLogger	com.waveset.adapter.logging.IActiveSyncLogger	リソースの Active Sync ログファイルへのログエントリの書き込みに使用されるオブジェクト。
result	java.util.Map	後述の result の説明を参照してください。
errors	java.util.List	最初は、この値は空のリストです。 処理中にエラーが発生した場合、スクリプトによってこのリストに java.lang.String オブジェクトを追加できます。
trace	com.waveset.adapter.Trace	実行のトレースに使用されるオブジェクト。 スクリプトは、このクラスのメソッドを使用することで、顧客の環境でデバッグ可能なものとなります。

アダプタは、result マップに次のエントリが入力されることを想定しています。

キー	値の型	値の説明
iterator	com.waveset.adapter.script.ScriptedIterator	スクリプトによって、この値を ScriptedIterator インタフェースの生成インスタンスに設定する必要があります。 public interface ScriptedIterator { public boolean hasNext(); public void next(java.util.Map nextObj); public void close();} nextObj マップについては、次の表を参照してください。 オブジェクトは、顧客のデータベース内のすべてのユーザーを反復処理できる必要があります。 サンプルは、BeanShell および Javascript でこれを行う方法を示しています。

アダプタは、next メソッドに渡される nextObj マップに、iterator によって各繰り返しユーザーの属性が入力されることを想定しています。

キー	値の型	値の説明
attrMap	java.util.Map	スクリプトがユーザー属性を直接取得できる場合は、ユーザー属性のマップでこのエントリを設定できます。属性名は、リソースのスキーママップの「リソースユーザー属性」列で定義されます。
isDisabled	java.lang.Boolean または java.lang.String	スクリプトによって Boolean.TRUE または true の文字列に設定されている場合、そのユーザーは無効とみなされます。

エラー処理

スクリプト内から例外がスローされた場合は、失敗とみなされます。

スクリプトでエラーが発生した場合、スクリプトによって errors キーに適切な文字列を追加することもできます。errors リストに項目が存在する場合は、失敗とみなされます。

authenticate アクション

顧客のデータベースに対してユーザー ID/パスワードを認証するには、authentication アクションを使用します。authentication アクションが定義されていない場合、そのリソースではパススルー認証をサポートできません。

コンテキスト

actionContext マップには次のエントリが含まれます。

キー	値の型	値の説明
conn	java.sql.Connection	顧客のデータベースへの JDBC 接続
adapter	com.wavset.adapter.ScriptedJdbcResourceAdapter	アダプタインスタンス
action	java.lang.String	「authenticateUser」という文字列。
id	java.lang.String	認証するユーザーのアカウント ID。
password	java.lang.String	認証対象の復号化されたパスワード。
result	java.util.Map	スクリプトは、ユーザーのパスワードが期限切れになっていることを示す expired キーと Boolean.TRUE 値を持つエントリを追加できます。
errors	java.util.List	最初は、この値は空のリストです。 処理中にエラーが発生した場合、スクリプトによってこのリストに java.lang.String オブジェクトを追加できます。
trace	com.waveset.adapter.Trace	実行のトレースに使用されるオブジェクト。 スクリプトは、このクラスのメソッドを使用することで、顧客の環境でデバッグ可能なものとなります。

エラー処理

スクリプトが失敗なく実行された場合、ID とパスワードは有効とみなされます。

スクリプト内から例外がスローされた場合は、認証の失敗とみなされます。

スクリプトでエラーが発生した場合、スクリプトによって適切な文字列を errors キーにエイリアスすることができます。errors リストに項目が存在する場合は、認証の失敗とみなされます。

test アクション

定義されている場合、test アクションは、リソースの「設定のテスト」の間に呼び出されます。通常、test スクリプトは、必要なデータベーステーブルにアダプタがアクセスできることを確認するために使用されます。

コンテキスト

actionContext マップには次のエントリが含まれます。

キー	値の型	値の説明
conn	java.sql.Connection	顧客のデータベースへの JDBC 接続
adapter	com.wavset.adapter.Scripted Jdbc ResourceAdapter	アダプタインスタンス
action	java.lang.String	「test」という文字列。
errors	java.util.List	最初は、この値は空のリストです。 処理中にエラーが発生した場合、スクリプトによってこのリストに java.lang.String オブジェクトを追加できます。
trace	com.waveset.adapter.Trace	実行のトレースに使用されるオブジェクト。 スクリプトは、このクラスのメソッドを使用することで、顧客の環境でデバッグ可能なものとなります。

エラー処理

スクリプト内から例外がスローされた場合は、失敗とみなされます。

スクリプトでエラーが発生した場合、スクリプトが errors キーに適切な文字列を追加することもできます。errors リストに項目が存在する場合は、テストの失敗とみなされます。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	あり
アカウントの作成	あり
アカウントの更新	あり
アカウントの削除	あり
パススルー認証	あり
パスワードの更新	あり

機能	サポート状況
データ読み込みメソッド	■ リソースから直接インポート ■ 調整 ■ Active Sync

アカウント属性

アカウント属性は管理対象のデータベーススキーマによってかなり異なるため、スクリプト JDBC アダプタにはデフォルトのアカウント属性が用意されていません。

このアダプタでは、Oracle の BLOBなどのバイナリデータ型がサポートされます。対応する属性は、スキーママップでバイナリとしてマークされている必要があります。バイナリ属性の例には、グラフィックスファイル、オーディオファイル、証明書などがあります。

セキュリティーに関する注意事項

サポートされる接続および必要な管理特権を確認するには、管理するデータベースの製品マニュアルを参照してください。

リソースオブジェクトの管理

リソースオブジェクトの管理では、すべてのオブジェクトを表示する機能のみがサポートされます。このアダプタでは、すべてのリソースオブジェクトタイプの ID のリストを取得できます。

アイデンティティーテンプレート

```
$accountId$
```

サンプルフォーム

- `MultiValueUserForm.xml`
- `SimpleTableUserForm.xml`

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスまたはパッケージでトレースオプションを設定します。

- `com.waveset.adapter.ScriptedJdbcResourceAdapter`

- `com.waveset.adapter.JdbcResourceAdapter`
- `com.waveset.adapter.script`

スクリプトに渡されるアクションコンテキストでは
`com.sun.idm.logging.trace.Trace` オブジェクトが常に渡されます。

スクリプトのトレースを有効にするには、com.waveset.adapter.ScriptedJdbcResourceAdapter でトレースを有効にします。

さらに、次のスクリプトを使用して、出力のトレースや書き込みを実行できます。

- BeanShell では、次の行で行トレースを有効にします。

```
this.interpreter.TRACE=true;
```

- BeanShell では、次の Java 形式の文によって 標準出力 に文字列を書き込みます。

```
java.lang.System.out.println(“Hello World”);
```

- Javascript では、次の Java 形式の文によって標準出力に文字列を書き込みます。

```
Packages.java.lang.System.out.println(“Hello World”);
```

Active Sync が実行されている場合は、リソースインスタンスに対して次の Identity Manager Active Sync ロギングパラメータを設定できます。

- ログアーカイブの最大数
- アクティブログの最大有効期間
- ログファイルの最大サイズ
- ログファイルパス
- ログレベル

◆ ◆ ◆ 第 39 章

SecurID ACE/Server

Identity Manager には、RSA SecurID ACE/Server をサポートするためのリソースアダプタが用意されています。

アダプタの詳細

次の表に、これらのアダプタの属性を要約します。

GUI 名	クラス名
SecurID ACE/Server	`com.waveset.adapter.SecurIdResourceAdapter`
SecurID ACE/Server UNIX	`com.waveset.adapter.SecurIdUnixResourceAdapter`

リソースを設定する際の注意事項

SecurID が Windows 上にインストールされている場合、このアダプタは、インストールされているバージョンの RSA ACE/Server に付属する apidemon と接続します。apidemon を、ACE/Server のインストールディレクトリ (デフォルトでは、`c:\ace\utils\toolkit\apidemon.exe`) から `c:\winnt\system32` または `c:\windows\system32` にコピーします。RSA ACE 6.1 の apidemon.exe は、`ACEInstallDir\prog` ディレクトリにあります。

UNIX アダプタは、RSA ACE/Server Administration Toolkit TCL API を使用します。API は、*ACEInstallDir* `/utils/tcl/bin` ディレクトリに配置する必要があります。*ACEInstallDir* の値は、リソースパラメータとして指定されます。ツールキットは、RSA 発行の『Customizing Your RSA ACE/Server Administration』に記載されているとおりに設定してください。

さらに、Identity Manager で RSA ユーザーやほかの ACE データベースオブジェクトを管理できるように、次の条件に適合していることを必ず確認してください。

- 「管理者ログイン」リソースパラメータ (Windows アダプタの場合) または「ログインユーザー」リソースパラメータ (UNIX アダプタの場合) で指定された SecurID ユーザー名が、ACE/Server に存在している。存在しない場合は、同じデフォルトログイン名で ACE ユーザーを作成します。
- この SecurID ユーザーは、トークンコードではなくパスワードを使用して ACE/Server にログインする必要がある。RSA ACE/Server ユーザーのパスワードは、アダプタで指定されたものと同じ値に設定します。

  現在の RSA ACE/Server システムポリシーでは必要な文字 (たとえば英数字による PIN) を使用したパスワードの設定が許可されない場合や、ユーザーパスワードの有効期限のデフォルト設定を変更する必要がある場合は、RSA ACE/Server Database コンソールでシステムパラメータを編集します。

  RSA ACE Server の管理者コンソールで変更したパスワードは、このユーザーが最初にログインしたときに期限切れとなる 1 回限りのパスワードです。RSA ACE Agent の Test Authentication 機能を使用してログインし、ユーザーのパスワードをすぐに期限切れにならないパスワードに変更します。パスワードを同じ値に変更してもかまいません。そうすれば、リソースアダプタで指定されたパスワードとも同じままになります。
- Windows では、Identity Manager のゲートウェイが稼働するホスト用に RSA ACE Agent Host を追加してください。これは、RSA ACE Server が稼働しているシステムの Database Administration - Host Mode コンソールインタフェースで設定できます。DNS のホスト名とネットワークアドレスを設定し、アクセスできるユーザーを指定してください。さらに、エージェントタイプを「Net OS Agent」に設定してください。
- SecurId グループ名またはサイト名にコンマが含まれていると、Identity Manager は名前を正しく解析できない場合があります。SecurId グループ名およびサイト名にはコンマを使用しないでください。

Identity Manager のインストールに関する注意事項

SecurID が Windows 上にインストールされている場合、Identity Manager のゲートウェイは、RSA ACE/Server がインストールされているシステムと同じシステム上で稼働させる必要があります。

使用上の注意

ここでは、SecurID ACE/Server リソースアダプタの使用に関連する情報を提供します。 次のトピックで構成されています。

- 449 ページの「UNIX でのパススルー認証の有効化」
- 449 ページの「複数のトークンの有効化」

- 453 ページの「パスワードポリシー」

UNIX でのパススルー認証の有効化

UNIX では RSA C API がサポートされないため、SecurID ACE/Server UNIX アダプタでパススルー認証を有効にするプロセスは単純ではありません。このアダプタでパススルー認証を実行するには、次のようなコンポーネント間の対話が必要になります。

Identity Manager <--> SecurID Unix リソースアダプタ <--> SecurID Windows アダプタ <--> Sun Identity Manager Gateway <--> RSA ACE Agent for Windows <--> RSA UNIX Server

SecurID ACE/Server UNIX アダプタでパススルー認証を有効にするときは、設定および実装で次の点に注意してください。

- Sun Identity Manager Gateway と RSA ACE Agent Host は、同じ Windows ホスト上にある必要があります。詳細については、「リソースを設定する際の注意事項」を参照してください。
- UNIX RSA サーバー自体がクライアントとして表示される場合、ユーザーの認証に使用するアカウントは UNIX リソースで定義されている必要があります。詳細については、「リソースを設定する際の注意事項」を参照してください。
- SecurID ACE/Server UNIX アダプタで、「ACE サーバー認証リソース」リソースパラメータの値を指定する必要があります。この値は、有効な SecurID ACE/Server (Windows 用) アダプタで指定されたリソース名と一致している必要があります。
- SecurID の認証ポリシーでは、UNIX SecurID サーバーが RSA ACE Agent for Windows を認識する必要があります。`sdconf.rec` ファイルを Windows ホスト上に配置し、正しく設定する必要があります。
- ユーザーがパススルー認証を使用するには、RSA ACE Agent for Windows をアクティブにしてください。
- Identity Manager を、SecurID ACE/Server または SecurID ACE/Server UNIX のログインモジュールを使用するように設定する必要があります。
- 認証対象のユーザーは、Identity Manager ロールと組織で設定されている必要があります。

複数のトークンの有効化

どちらの SecurID リソースアダプタでも、デフォルトのスキーママップは、管理者が 1 つのトークンを指定できるように設定されます。*InstallDir**samples**forms* ディレクトリにある SecurID User Form を使用する場合は、次の手順を実行して最大 3 つのトークンを有効にします。

▼ 最大 3 つのトークンを有効にする

1 次の **SecurID User Form** のセクションを編集します。

```
<FieldLoop for='tokenNum'>   <expression>      <ref>oneTokenList</ref>   </expression>
```

`oneTokenList` を `threeTokenList` に変更します。

2 **User Form** を **Identity Manager** に読み込みます。

3 **SecurID ACE/Server** スキーママップの左側で、次の **Identity Manager** ユーザー属性の名前を変更します。

元の **Identity Manager** ユーザー属性	変更後の **Identity Manager** ユーザー属性
`tokenClearPin`	`token1ClearPin`
`tokenDisabled`	`token1Disabled`
`tokenLost`	`token1Lost`
`tokenLostPassword`	`token1LostPassword`
`tokenLostExpireDate`	`token1LostExpireDate`
`tokenLostExpireHour`	`token1LostExpireHour`
`tokenLostLifeTime`	`token1LostLifeTime`
`tokenPinToNTC`	`token1PinToNTC`
`tokenPinToNTCSequence`	`token1PinToNTCSequence`
`expirePassword`	`token1NewPinMode`
`password`	`token1Pin`
`tokenResync`	`token1Resync`
`tokenFirstSequence`	`token1FirstSequence`
`tokenNextSequence`	`token1NextSequence`
`tokenSerialNumber`	`token1SerialNumber`
`tokenUnassign`	`token1Unassign`

4 **2** 番目のトークンを格納するために、次のフィールドをスキーママップに追加します。

Identity Manager ユーザー属性	リソースユーザー属性
token2ClearPin	token2ClearPin
token2Disabled	token2Disabled
token2Lost	token2Lost
token2LostPassword	token2LostPassword
token2LostExpireDate	token2LostExpireDate
token2LostExpireHour	token2LostExpireHour
token2LostLifeTime	token2LostLifeTime
token2NewPinMode	token2NewPinMode
token2PinToNTC	token2PinToNTC
token2PinToNTCSequence	token2PinToNTCSequence
password	token2Pin
token2Resync	token2Resync
token2FirstSequence	token2FirstSequence
token2NextSequence	token2NextSequence
token2SerialNumber	token2SerialNumber
token2Unassign	token2Unassign

5 2番目のトークンを格納するために、次のフィールドをスキーママップに追加します。

Identity Manager ユーザー属性	リソースユーザー属性
token3ClearPin	token3ClearPin
token3Disabled	token3Disabled
token3Lost	token3Lost
token3LostPassword	token3LostPassword
token3LostExpireDate	token3LostExpireDate
token3LostExpireHour	token3LostExpireHour
token3LostLifeTime	token3LostLifeTime
token3NewPinMode	token3NewPinMode

Identity Manager ユーザー属性	リソースユーザー属性
token3PinToNTC	token3PinToNTC
token3PinToNTCSequence	token3PinToNTCSequence
password	token3Pin
token3Resync	token3Resync
token3FirstSequence	token3FirstSequence
token3NextSequence	token3NextSequence
token3SerialNumber	token3SerialNumber
token3Unassign	token3Unassign

ステータスによるトークンの取得

SecurId アダプタは、トークン型、ステータス、有効期限など、指定された特性セットに適合するトークンのリストを返すことができます。たとえば、ユーザーフォームの次の部分は、割り当てられていない 128 ビットトークンすべてのリストを返します。

```
<defvar name='unassignedTokens'>
   <invoke name='listResourceObjects' class='com.waveset.ui.FormUtil'>
      <ref>:display.session</ref>
      <s>ListTokensByField</s>
      <ref>resource</ref>
      <map>
         <s>field</s>
         <s>7</s>
         <s>compareType</s>
         <s>2</s>
         <s>value</s>
         <s>128</s>
         <s>templateParameters</s>
         <ref>accounts[$(resource)].templateParameters</ref>
      </map>
      <s>false</s>
   </invoke>
</defvar>
```

field、compareType、および value の各文字列に代入できる値は、RSA Sd_ListTokensByField 関数のマニュアルに定義されています。詳細については、RSA 発行の『Customizing Your RSA ACE/Server Administration』を参照してください。

パスワードポリシー

Identity Manager で英字を含むパスワードを使用していて、SecurID では PIN に英字が許可されない場合は、次のメッセージが表示されます。

```
SecurId ACE/Server: (realUpdateObject) Sd_SetPin Error Alpha characters not allowed
```

このエラーを解決するには、リソースの Identity Manager パスワードポリシーが英字を含めないように変更するか、またはリソースの PIN 制限が英字を許可するように変更します。

ゲートウェイタイムアウト

SecurID ACE/Server for Windows アダプタでは、`RA_HANGTIMEOUT` リソース属性を使用してタイムアウト値を秒単位で指定できます。この属性は、ゲートウェイに対する要求がタイムアウトしてハングしているとみなされるまでの時間を制御します。

次のように、この属性を Resource オブジェクトに手動で追加する必要があります。

```
<ResourceAttribute name='Hang Timeout' displayName='com.waveset.adapter.RAMessages:
RESATTR_HANGTIMEOUT' type='int' description='com.waveset.adapter.RAMessages:
RESATTR_HANGTIMEOUT_HELP' value='NewValue'>
 </ResourceAttribute>
```

この属性のデフォルト値は 0 です。これは Identity Manager がハングした接続を確認しないことを表します。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は、次のいずれかを使用して SecurID ACE/Server アダプタと通信することができます。

- Sun Identity Manager Gateway (Windows のみ)
- Telnet (UNIX のみ)
- SSH (UNIX のみ)
- SSHPubKey (UNIX のみ)

SSHPubKey 接続の場合、「リソースパラメータ」ページで非公開鍵を指定する必要があります。この鍵には `--- BEGIN PRIVATE KEY ---` および `--- END PRIVATE KEY --` のような注釈行を含める必要があります。公開鍵は、サーバー上の `/.ssh/authorized_keys` ファイルに配置する必要があります。

必要な管理特権

「ログイン ユーザー」リソースパラメータ (UNIX の場合) または「管理者ログイン」リソースパラメータ (Windows の場合) で指定されたユーザーは、ユーザー関連タスクとトークン関連タスクを実行できる管理者ロールに割り当てられている必要があります。

テスト接続を使用して次のテストができます。

- 各コマンドが管理ユーザーのパスに存在するかどうか
- 管理ユーザーが /tmp に書き込めるかどうか
- 管理ユーザーに、特定のコマンドを実行する権限があるかどうか

テスト接続では、通常のプロビジョニングの実行とは異なるコマンドオプションを使用できます。

注 – Resource SecurID Administrators レポートには、SecurID リソースで使用可能な管理者が一覧表示されます。このレポートには、管理者の名前、管理レベル、管理タスクリスト、管理サイト、管理グループなど、各管理者のプロパティーが示されます。このレポートは、.csv と .pdf のどちらの形式でもダウンロードできます。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	あり
パススルー認証	あり
前アクションと後アクション	なし
データ読み込みメソッド	■ リソースからインポート ■ 調整

アカウント属性

次の表に、SecurID ACE/Server アカウント属性に関する情報を示します。特に記載されていないかぎり、属性のデータ型はすべて String です。

SecurID ACE/Server アダプタは、複数の値を含むカスタムアカウント属性 (SecurId の User Extension Data) をサポートしません。

Identity Manager ユーザー属性	リソースユーザー属性	説明
adminGroup	adminGroup	管理者がメンバーになっているグループ。これは読み取り専用属性です。
adminLevel	adminLevel	ユーザーの管理レベル。値には、レルム、サイト、またはグループを指定できます。これは読み取り専用属性です。
adminSite	adminSite	管理者がアクセスできるサイト。これは読み取り専用属性です。
adminTaskList	adminTaskList	管理者が実行できるタスクセットの名前。これは読み取り専用属性です。
adminTaskListTasks	adminTaskListTasks	管理者が実行できる個々のタスク。これは読み取り専用属性です。
allowedToCreatePin	allowedToCreatePin	ユーザーが PIN の指定を許可されていることを示す、読み取り専用の Boolean 型属性。PIN が指定されていない場合は、システムによってユーザーの PIN が生成されます。
clients	clients	ユーザーがメンバーになっているクライアントを指定します。
accountId	defaultLogin	ACE/Server のユーザーのアカウント ID。最大 48 文字。
defaultShell	defaultShell	ユーザーのデフォルトのシェル。最大 256 文字。
expirePassword	WS_PasswordExpired	パスワードが期限切れになるかどうかを示します。パスワードが期限切れになると、SecurID アカウントは New PIN モードに配置されます。これは書き込み専用属性です。
firstname	firstname	必須。ユーザーの名。最大 24 文字。
groups	groups	ユーザーがメンバーになっているグループを指定します。
lastname	lastname	必須。ユーザーの姓。最大 24 文字。
remoteAlias	remoteAlias	リモートレルムでのユーザーのログイン名。
remoteRealm	remoteRealm	リモートユーザーの場合にユーザーが所属するレルム。
requiredToCreatePin	requiredToCreatePin	ユーザーが PIN を指定する必要があることを示す、読み取り専用の Boolean 型属性。
tempEndDate	tempEndDate	一時モードが終了する日付。

Identity Manager ユーザー属性	リソースユーザー属性	説明
tempEndHour	tempEndHour	一時モードが終了する時間。
tempStartDate	tempStartDate	一時モードが開始する日付。
tempStartHour	tempStartHour	一時モードが開始する時間。
tempUser	tempUser	一時モードに入るユーザーまたは一時モードから抜けるユーザーを設定します。
tokenClearPin	token1ClearPin	ユーザー更新で設定されている場合、ユーザーの PIN がクリアされます。
tokenDisabled	token1Disabled	ユーザー更新で設定されている場合、ユーザーの PIN が無効になります。
tokenLost	token1Lost	ユーザー更新で true に設定されている場合、アカウントは RSA 内で緊急アクセスモードになります。
tokenLostPassword	token1LostPassword	値がブランクではない場合、LOST トークンは、指定された値を一時的なパスコードとして使用します。値がブランクの場合は、RSA が一時的なパスコードを割り当てるという従来の動作が実行されます。これは書き込み専用属性です。
tokenLostExpireDate	token1LostExpireDate	LOST トークンの一時パスワードが期限切れになる日付を指定します。この属性は、tokenLostPassword がブランクではなく、tokenLostLifeTime がブランクか 0 の場合にのみ意味を持ちます。これは書き込み専用属性です。 この属性は、サンプルユーザーフォームには実装されていません。
tokenLostExpireHour	token1LostExpireHour	LOST トークンの一時パスワードが期限切れになる時間を指定します。たとえば、午後 4 時を表すには 16 と指定します。 この属性は、tokenLostPassword がブランクではなく、tokenLostLifeTime がブランクか 0 の場合にのみ意味を持ちます。これは書き込み専用属性です。 この属性は、サンプルユーザーフォームには実装されていません。

Identity Manager ユーザー属性	リソースユーザー属性	説明
tokenLostLifeTime	token1LostLifeTime	一時的なパスコードを受け付ける期間を時間単位で指定します。このフィールドは、takenLostPassword の値に関係なく使用できます。これは書き込み専用属性です。
tokenFirstSequence	token1FirstSequence	トークンを再同期する必要がある場合に、元のトークンを指定します。これは書き込み専用属性です。
tokenNewPinMode	token1NewPinMode	ユーザーアカウントが New PIN モードに配置されている場合に、ユーザーの新しい PIN を指定します。
tokenNextSequence	token1NextSequence	トークンを再同期する必要がある場合に、新しいトークンを指定します。これは書き込み専用属性です。
tokenPin	token1Pin	暗号化された値。ユーザーの PIN。
tokenPinToNTC	token1PinToNTC	true に設定されている場合、指定された割り当て済みトークンの PIN を次のトークンコードに設定するプロセスを開始します。
tokenPinToNTCSequence	token1PinToNTCSequence	ユーザーの現在のトークンコードを指定します。
tokenResync	token1Resync	トークンを再同期するかどうかを示します。この属性は、tokenFirstSequence 属性と tokenNextSequence 属性を有効にします。これは書き込み専用属性です。
tokenSerialNumber	token1SerialNumber	トークンシリアル番号。12 文字にしてください。この要件を満たすように、必要な数の 0 を先頭に挿入します。
tokenUnassign	token1Unassign	ユーザーから削除するトークンを指定します。これは書き込み専用属性です。
userType	userType	**Remote** と **Local** のいずれかにする必要があります。

リソースオブジェクトの管理

Identity Manager は、デフォルトで次の SecurID ACE/Server オブジェクトをサポートします。

表 39–1 サポートされる SecurID ACE/Server オブジェクト

リソースオブジェクト	サポートされる機能	管理される属性
group	リスト、ビュー	グループ名、このグループに割り当てられたユーザーのリスト、このグループでアクティブ化されているクライアントのリスト
clients	リスト、ビュー	クライアント名、このクライアントに割り当てられたユーザーのリスト、このクライアントでアクティブ化されているグループのリスト

アイデンティティーテンプレート

$accountId$

サンプルフォーム

SecurID User Form

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

- `com.waveset.adapter.SecurIdResourceAdapter`
- `com.waveset.adapter.SecurIdUnixResourceAdapter`
- `com.waveset.adapter.SVIDResourceAdapter`

Windows システムのゲートウェイへの接続に伴う問題を診断するため、次のメソッドでもトレースを有効にすることができます。

- `com.waveset.adapter.AgentResourceAdapter#sendRequest`
- `com.waveset.adapter.AgentResourceAdapter#getResponse`

◆ ◆ ◆ 第 40 章

40 シェルスクリプト

Identity Manager には、リソースをホストするシステム上でシェルスクリプトによって制御されるリソースを管理するための、シェルスクリプトリソースアダプタが用意されています。このアダプタは汎用アダプタであるため、高度な設定が可能です。

このアダプタは、`com.waveset.adapter.ShellScriptResourceAdapter` クラスで定義されます。

アダプタの詳細

リソースを設定する際の注意事項

ERROR_CODE_LIMIT 属性を使用して、エラーを表すエラーコードを定義できます。ここで指定した値を超えるコードはエラーを表します。この値より小さいコードは、情報または警告を表すコードとして使用されます。この値を設定しない場合、Identity Manager は標準の動作を行います。この場合、0 以外のリターンコードはすべてエラーを表します。このオプションの属性をリソース定義に追加できます。

Identity Manager のインストールに関する注意事項

このリソースを Identity Manager のリソースリストに追加するには、「管理するリソースの設定」ページの「カスタムリソース」セクションに次の値を追加する必要があります。

使用上の注意

ユーザーパスワードに制御文字 (0x00、0x7f など) を使用しないでください。

リソースアクション

シェルスクリプトアダプタでは、ユーザーアカウントの作成、更新、削除、取得などの基本的なプロビジョニング機能を実行する一連のアクションを作成できます。これらの各アクションは、シェルスクリプトで定義されます。シェルスクリプトアダプタは、リソースアクションを UNIX リソースアダプタとして実行することで機能します。リソースアクションを実行するには、このアダプタで次の操作が必要です。

- 作成、削除、および更新の操作を、/tmp ディレクトリで実行する。
- mkdir、umask、touch、cat、chmod、rm -f、rmdir、find、set などのコマンドを実行する機能と、<、<<、>、>> などの演算子を使用する機能を設定する。

このアダプタでは、次の表に示すプロビジョニングアクションがサポートされます。

アクション	目的	必要性
create	新しいユーザーを作成します。	省略可能。ただし、指定されていない場合は、ユーザーを作成できません。
delete	既存のユーザーを削除します。	省略可能。ただし、指定されていない場合は、ユーザーを削除できません。
getAllUsers	リソース上のすべてのユーザーに関する情報を取得します。	省略可能。ただし、指定されていない場合は、調整や「リソースから読み込み」などのアカウント反復処理に依存する操作は実行できません。
getUser	既存ユーザーの属性を取得します。	はい。
update	既存ユーザーの属性を更新します。	省略可能。ただし、指定されていない場合は、ユーザーを更新できません。

`$WSHOME/sample/ShellScript` ディレクトリには、理論上のシェルスクリプトベースのホストアプリケーションにユーザーをプロビジョニングするのに使用できるリソースアクション定義のサンプルセットが格納されています。環境に合わせてそれらの定義をカスタマイズしてください。

リソースアクションの一般的な情報については、第 50 章「リソースへのアクションの追加」を参照してください。

スクリプト

シェルスクリプトアダプタは、リソースホスト上で実行するシェルスクリプトファイルとしてアクションを実装します。これらのスクリプトは、リソースホスト上でスクリプトを実行するアカウント用に設定されているシェルで動作するように記述してください。

スクリプトは規則に従い、成功を示すリターンコード 0 で終了するようにしてください。0 以外のコード (スクリプトの作成者が定めた) を返すことは、操作が正しく完了しなかった可能性があるという意味になります。

スクリプトは、標準エラーや標準出力ストリームにテキストを出力できます。操作の種類、操作のコンテキスト、および失敗のタイプによっては、その操作の結果にテキストを表示することができます。

getUser および getAllUsers 操作では、このテキストは、各ユーザーの属性を特定するために標準出力ストリームで解析されます。

次のタイプの環境変数を、スクリプトにエクスポートできます。

- スキーママップの アイデンティティーシステム リソース属性列で定義されたアカウント属性はいずれも、そのアカウント属性の先頭に `WSUSER_` を付加することで、スクリプトで利用できるようになります。たとえば、アカウント属性の名前が Full Name の場合、その環境変数は `WSUSER_Full_Name` という名前になります。スペースは下線に置き換えられます。
- `WSRSRC_` で始まる環境変数で、アダプタの設定を渡すことができます。もっとも重要な変数は、アダプタの名前を定義する `WSRSRC_Name` です。異なるリソースで同じスクリプトを実行する場合は、この変数を実装すると、それぞれのホストで同じ操作を行うスクリプトの複数のコピーを維持する手間を省けます。

次のコード例は、サンプルで生成される環境を示しています。

```
WSRSRC_Host='129.153.147.151'; export WSRSRC_Host
WSRSRC_Port='22'; export WSRSRC_Port
WSRSRC_Login_User='root'; export WSRSRC_Login_User
WSRSRC_password='074B7E28F5927C90:1C65216:108540A69DE:-7FFD|zGEBDGD3VRs='; export WSRSRC_password
WSRSRC_Login_Shell_Prompt=']#'; export WSRSRC_Login_Shell_Prompt
WSRSRC_Root_User='root'; export WSRSRC_Root_User
WSRSRC_credentials='074B7E28F5927C90:1C65216:108540A69DE:-7FFD|zGEBDGD3VRs='; export WSRSRC_credentials
WSRSRC_Root_Shell_Prompt=']#'; export WSRSRC_Root_Shell_Prompt"
WSRSRC_Connection_Type='SSH'; export WSRSRC_Connection_Type"
WSRSRC_Maximum_Connections='10'; export WSRSRC_Maximum_Connections"
WSRSRC_Connection_Idle_Timeout='900'; export WSRSRC_Connection_Idle_Timeout"
WSRSRC_Display_Name_Attribute='accountId'; export WSRSRC_Display_Name_Attribute"
WSRSRC_NAME='ShellTest'; export WSRSRC_NAME"
WSRSRC_ID='#ID#074B7E28F5927C90:B122A1:108E3E4CFAA:-7FFC'; export WSRSRC_ID"
WSRSRC_TYPE='Resource'; export WSRSRC_TYPE"
WSRSRC_CLASS='class com.waveset.object.Resource'; export WSRSRC_CLASS"
```

一般に、属性の値が NULL の場合は、対応する環境変数に長さが 0 の文字列が設定されるのではなく、その環境変数が省略されます。

スクリプトで使用可能な変数については、第 50 章「リソースへのアクションの追加」を参照してください。

結果処理

AttrParse メカニズムは、標準出力ストリームを通して getUser アクションと getAllUsers アクションから返された結果を処理します。このメカニズムについては、第 49 章「AttrParse オブジェクトの実装」を参照してください。

getUser アクションの場合、AttrParse はユーザー属性のマップを返します。getAllUsers アクションの場合は、マップのマップを生成します。返されるマップの各エントリには、次の内容が含まれます。

- 通常 AttrParse で返されるものと同様のユーザー属性のマップを示す値。
- アカウント ID または (ID が不明の場合は) 名前を示すキー。

collectCsvHeader および collectCsvLines AttrParse トークンを使用すると、属性と値を特定できます。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は、次の接続を使用してシェルスクリプトアダプタと通信します。

- Telnet
- SSH (SSH はリソース上に個別にインストールする)
- SSHPubKey

SSHPubKey 接続の場合、「リソースパラメータ」ページで非公開鍵を指定する必要があります。この鍵には `--- BEGIN PRIVATE KEY ---` および `--- END PRIVATE KEY --` のような注釈行を含める必要があります。公開鍵は、サーバー上の `/.ssh/authorized_keys` ファイルに配置する必要があります。

必要な管理特権

スクリプトを実行する管理アカウントは、スクリプトで定義されているすべての操作について承認されている必要があります。

プロビジョニングに関する注意事項

次の表に、シェルスクリプトアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの作成	あり
アカウントの更新	あり
アカウントの削除	あり
アカウントの有効化/無効化	あり
アカウントの名前の変更	あり
パススルー認証	なし
前アクションと後アクション	なし
データ読み込みメソッド	`getAllUsers`アクションが定義されている場合は、次のデータ読み込み方法がサポートされます。 ■ リソースから直接インポート ■ 調整

アカウント属性

アカウント属性は多種多様であるため、シェルスクリプトアダプタにはデフォルトのアカウント属性が用意されていません。

アカウントには、アイデンティティーシステムユーザー属性の名前が accountId であるアカウント属性が必要です。

リソースオブジェクトの管理

サポートされません。

アイデンティティーテンプレート

なし。有効な値を持つアイデンティティーテンプレートを設定する必要があります。

サンプルフォーム

サンプルユーザーフォームはありませんが、リソースと AttrParse 定義の例が次の場所にあります。

```
$WSHOME/sample/ShellScript/ShellScriptResourceObjects55.xml
```

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

```
com.waveset.adapter.ShellScriptResouceAdapter
```

◆ ◆ ◆ 第 41 章

Siebel CRM

Siebel CRM リソースアダプタは、com.waveset.adapter.SiebelCRMResourceAdapter クラスで定義されます。

アダプタの詳細

Identity Manager のインストールに関する注意事項

Siebel CRM リソースアダプタは、カスタムアダプタです。インストールプロセスを完了するには、次の手順を実行する必要があります。

▼ Siebel CRM リソースアダプタをインストールする

1 **Siebel CRM** リソースをリソースリストに追加するには、「管理するリソースの設定」ページの「カスタムリソース」セクションに次の値を追加する必要があります。

```
com.waveset.adapter.SiebelCRMResourceAdapter
```

2 次の表に従って、適切な JAR ファイルを、 *InstallDir*\idm\WEB-INF\lib ディレクトリにコピーします。

JAR ファイルのバージョンは、Siebel CRM リソースのバージョンと一致している必要があります。

Siebel 7.0	Siebel 7.7、7.8、8.0
■ SiebelJI_Common.jar ■ SiebelJI_enu.jar ■ SiebelJI.jar	■ Siebel.jar ■ SiebelJI_enu.jar

注 – *InstallDir*\idm\WEB-INF\lib ディレクトリには、バージョンが異なる Siebel の JAR ファイルをコピーしないでください。バージョン間で競合が発生する可能性があります。

リソースを設定する際の注意事項

なし

使用上の注意

ビジネスオブジェクトとビジネスコンポーネントの選択

デフォルトでは、Siebel CRM アダプタでのアカウントプロビジョニングには Employee Siebel ビジネスオブジェクトの *Employee* Siebel ビジネスコンポーネントが使用されます。ただし、アカウントプロビジョニングにどの Siebel ビジネスオブジェクトのどの Siebel ビジネスコンポーネントを使用するかを、アダプタに設定できます。

- 異なるビジネスオブジェクトを使用するには、「アカウントビジネスオブジェクト」リソースパラメータを、それに応じた設定にします。
- 異なるビジネスコンポーネントを使用するには、「アカウントビジネスコンポーネント」リソースパラメータに目的のビジネスコンポーネントの名前を設定します。

注 – 指定したビジネスオブジェクトに含まれるビジネスコンポーネントを指定してください。

Siebel Tools Client を使用して、ビジネスコンポーネントを検査し、プロビジョニングに使用可能な属性を確認できます。デフォルトのスキーママップには、デフォルトの Employee ビジネスコンポーネントで利用できる一般的な属性がいくつか含まれています。

Siebel 環境を管理するために属性の追加、削除、または変更が必要になることがあります。特に、デフォルト以外のビジネスオブジェクトやビジネスコンポーネントを使用するようにアダプタを設定した場合は、その可能性が高くなります。

次の手順は、Siebel Tools クライアントを使用して、Identity Manager が Siebel 環境に対してプロビジョニングできる属性を検索する基本的な方法を示します。

▼ Siebel 環境にプロビジョニングする属性を識別する

1. **Siebel Tools** の **Object Explorer** を開きます。
2. 「**Business Component**」アイコンをクリックします。
3. スクロールダウンするか、またはクエリーを作成して、目的のビジネスコンポーネントを選択します。
4. **Object Explorer** 内で「**Fields**」を選択します。

   そのビジネスコンポーネントで使用可能なフィールドのリストが表示されます。

   Object Explorer に表示されるフィールドの「Name」列の値は、通常、設定した Siebel CRM リソースのスキーママップ内の右側 (リソースユーザー属性) で使用されます。

   一般に、これらのフィールドはどれでもある程度まで管理できます。ただし、複数値フィールドや選択リストフィールドを管理する場合は、次に示すように、異なる形式でスキーママップの右側に指定してください。

   - 複数値フィールドの場合: 右側には *field*@@ *keyAttr* の形式を使用する必要があります。各表記の意味は次のとおりです。
     - *field* は、複数値フィールドの名前を表します。
     - *keyAttr* は、複数値リストの各項目を一意に識別するために使用する、関連付けられた複数値ビジネスコンポーネント内のフィールドの名前を表します。

       例: `Position@@Name`

     選択リストフィールドの場合: 右側には *field*!! *keyAttr* の形式を使用する必要があります。各表記の意味は次のとおりです。
     - *field* は、選択リストフィールドの名前を表します。
     - *keyAttr* は、選択リストの項目を一意に識別するために使用する、関連付けられた選択リストビジネスコンポーネント内のフィールドの名前を表します。

       例: `Employee Organization!!`名前

複数値グループの第一の値の管理

複数値グループ (MVG) に、第一として指定された単一のメンバーがすでに含まれている場合、アダプタは次のアクションを実行します。

- 受信する MVG に、Identity Manager に現在定義されている値とは異なる単一の値が含まれている場合は、新しい値が挿入され、第一としてマークされます。このとき、以前の値は Identity Manager から削除されます。

- 第一以外の値が追加された場合、デフォルトでは、第一の値はそのまま変わりません。

現在 MVG に複数の値があり、そのうちの 1 つが第一として指定されている場合は、次のようになります。

- 第一以外の値がセットから削除された場合、現在の第一が第一のままになります。
- MVG の値セットが新しい単一の値で置き換えられた場合は、新しい単一の値が挿入されて第一として指定されます。このとき、以前の値はすべて削除されます。
- 第一以外の値が追加された場合、デフォルトでは、第一の値はそのまま変わりません。

複数の値が存在する場合に第一マーカーを既存の値から新しい値に移動するには、スキーママップにアカウント属性を追加してください。この属性の名前は、「`Primary` *MVG_Name*"」の形式にする必要があります。*MVG_Name* は、`Employee Organization Id` や `Position` などの値です。したがって、その属性は、`Primary Employee Organization Id` や `Primary Position` のような名前になります。その後、ユーザーフォームで、`Primary` 属性に目的の値を設定します。

高度なナビゲーション

Siebel CRM アダプタの高度なナビゲーション機能を使用すると、子ビジネスコンポーネントを作成および更新できます。これは、Identity Manager に通常は実装されない高度な機能です。

高度なナビゲーション機能により、子ビジネスコンポーネントの作成および更新に必要な次の情報を任意で指定できます。

- ビジネスオブジェクト名
- 親ビジネスコンポーネント名
- 親検索属性
- ターゲットビジネスコンポーネント
- ターゲット検索属性
- インスコープ属性 (ビジネスコンポーネントで設定/更新対象となる属性)
- オプションの協働動作 (co-action)

作成および更新動作時に、高度なナビゲーション規則を使用できます。この規則はほかの種類の動作には使用できません。

Siebel CRM アダプタの高度なナビゲーション機能を実装するには、次の作業を実行してください。

- 右側のリソースユーザー属性の名前が PARENT_COMP_ID となっているスキーママップに属性を追加します。

- デバッグページを使用して、リソースの XML に次の ResourceAttribute を手動で追加します。

```
<ResourceAttribute name='AdvancedNavRule'
    displayName='Advanced Nav Rule'
    value='MY_SIEBEL_NAV_RULE'>
</ResourceAttribute>
```

  MY_SIEBEL_NAV_RULE を有効な規則名に置き換えてください。

- 高度なナビゲーション規則を記述します。この規則には、次の 2 つの変数が存在するようにしてください。

  `resource.action`。この値は `create` または `update` のいずれかにする必要があります。

  `resource.objectType`。通常のアカウント保守の場合、この値は `account` になります。

  この規則から、次の名前と値のペアが 1 つ以上含まれるマップを返す必要があります。

属性	定義
`busObj`	ビジネスオブジェクトの名前。
`parentBusComp`	`busObj` の親ビジネスコンポーネントの名前。このビジネスコンポーネントの最初の修飾された (`parentSearchAttr` を参照) レコードに移動することで、ビジネスオブジェクトのコンテキストが更新されます。
`parentSearchAttr`	`parentBusComp` で検索フィールドとして使用する属性。検索する値は、リソースユーザー属性名が PARENT_COMP_ID の属性に対する値として存在している必要があります。
`busComp`	作成または更新するファイナルビジネスコンポーネントの名前。作成の場合、このビジネスコンポーネントの新規レコードがビジネスオブジェクト内に作成されます。更新の場合、このビジネスコンポーネントの最初の修飾された (`searchAttr` を参照) レコードに移動することで、更新するビジネスコンポーネントレコードが選択されます。
`searchAttr`	`busComp` で検索フィールドとして使用する属性。検索する値はユーザーのアカウント ID です。
`attributes`	設定または更新される `busComp` 内のフィールドセットを指定する文字列のリスト。このリストは、実行されるアクション用にリソースのスキーママップで定義された属性よりも優先されます。

属性	定義
coAction	要求されたアクション (resource.action) が create の場合、作成後すぐに更新も実行するようにアダプタに指示するには、coAction の値に update を指定します。Create では設定できない必須フィールドがあり、そのために create を論理的に完了するには update も実行する必要がある場合、この指定が必要になることがあります。resource.action が create で、coAction が update に設定されていないかぎり、この属性は無視されます。

ナビゲーション規則の例については、$WSHOME/sample/rules/SiebelNavigationRule.xml を参照してください。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	なし
アカウントの名前の変更	あり
アカウントの作成	あり
アカウントの更新	あり
アカウントの削除	あり
パススルー認証	あり
前アクションと後アクション	なし
データ読み込みメソッド	■ リソースから直接インポート ■ 調整

アカウント属性

デフォルトのスキーママップは、Employee ビジネスオブジェクトと Employee ビジネスコンポーネントが設定されていることを前提としています。Siebel 環境を管理するために属性の追加、削除、または変更が必要になることがあります。特に、デフォルト以外のビジネスオブジェクトやビジネスコンポーネントを使用するようにアダプタを設定した場合は、その可能性が高くなります。

アイデンティティーシステムユーザー属性	リソースユーザー属性	説明
accountId	Login Name	ユーザーのログイン名
firstname	First Name	ユーザーの名
lastname	Last Name	ユーザーの姓
Responsibility	Responsibility@@Name	従業員に割り当てる責任のリストを含む複数値属性。この属性は、ユーザーフォームで複数選択ボックスを使用して管理してください。 「Responsibility」フィールドは、サンプルの Siebel CRM ユーザーフォームで複数選択ボックスとして設定されています。
Position	Position@@Name	従業員に割り当てる役職名のリストを含む複数値属性。 割り当てる役職名はすべて Siebel に存在している必要があります。 第一役職名を割り当てるには、スキーママップに Primary Position 属性を追加して、第一にする役職名を設定します。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は、HTTP または RSA を使用して Siebel CRM アダプタと通信できます。詳細については、Siebel のユーザーマニュアルを参照してください。

必要な管理特権

アダプタで設定された管理ユーザー名およびパスワードに、指定されたビジネスコンポーネントの新規レコードの作成および既存レコードの更新を行うための十分な特権が Siebel 内で与えられていることを必ず確認してください。

リソースオブジェクトの管理

デフォルトでは、Siebel CRM アダプタは、次の Siebel オブジェクトをサポートします。

リソースオブジェクト	サポートされる機能	管理される属性
Employee:Position	■ Create ■ 更新 ■ 削除 ■ 名前の変更	■ 「名前」 ■ Division ■ Primary Employee ■ 説明

必要に応じて、追加のリソースオブジェクトタイプをサポートするようにアダプタを手動で設定できます。 これを行うには、次の手順に従ってリソースプロトタイプ XML を編集します。

▼ リソースプロトタイプ XML を編集する

1. **XML** のデフォルトの *Employee:Position* オブジェクトタイプの例のあとに、新しい <ObjectType> 要素を追加します。
2. Employee を、目的の **Siebel** ビジネスオブジェクトの名前に置き換えます。
3. Position を、目的の **Siebel** ビジネスコンポーネントの名前に置き換えます。
4. 組み込まれている <ObjectAttributes> 要素に、ビジネスコンポーネントの各項目を一意に識別するために使用される <ObjectAttribute> を指定する idAttr 属性が含まれていることを確認します。

アイデンティティーテンプレート

デフォルトのアイデンティティーテンプレートは $accountId$ です。

サンプルフォーム

このリソースアダプタには、次のサンプルフォームが用意されています。

Form	ファイル
SiebelCRM ユーザーフォーム	sample/SiebelCRMUserForm.xml
SiebelCRM Create Employee:Position Form	sample/SiebelCRMpositioncreate.xml
SiebelCRM Update Employee:Position Form	sample/SiebelCRMpositionupdate.xml

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

```
com.waveset.adapter.SiebelCRMResourceAdapter
```

さらに、リソースインスタンスに対して次の Identity Manager Active Sync ロギングパラメータを設定できます。

- ログアーカイブの最大数
- アクティブログの最大有効期間
- ログファイルの最大サイズ
- ログファイルパス
- ログレベル

◆ ◆ ◆ 第 42 章

42 SiteMinder

Identity Manager では、さまざまな SiteMinder 機能をサポートするアダプタを提供しています。

アダプタの詳細

Identity Manager は、次の SiteMinder 機能をサポートするためのアダプタを提供します。

- 管理者アカウント
- LDAP リポジトリユーザー
- データベーステーブルリポジトリユーザー

GUI 名	クラス名
SiteminderAdmin	com.waveset.adapter.SiteminderAdminResourceAdapter
SiteminderLDAP	com.waveset.adapter.SiteminderLDAPResourceAdapter
SiteminderExampleTable	com.waveset.adapter.SiteminderExampleTableResourceAdapter

リソースを設定する際の注意事項

Identity Manager で SiteMinder リソースアダプタをセットアップする前に、SiteMinder で次の手順を完了する必要があります。

▼ SiteMinder リソースアダプタを設定する

1 信頼できるホストを登録します。

   a. **Web** アプリケーションサーバーのホスト設定オブジェクト (ポリシーサーバー **IP** によるデフォルト設定のコピー) を作成します。

   b. エージェントのインストールディレクトリから `smreghost` を使用して、アプリケーションサーバーを登録します。

2 エージェントを作成します。

   a. エージェントの名前を入力します。

   b. 「**Support 4.x Agents**」を選択します。

   c. エージェントタイプとして「**Siteminder / WebAgent**」を選択します。

   d. クライアントの **IP** アドレスを入力します。

   e. 共有キーを入力します。

   Identity Manager で SiteMinder リソースアダプタを正常に設定するには、エージェント名および共有キーを確認しておく必要があります。

Identity Manager のインストールに関する注意事項

SiteMinder リソースアダプタは、カスタムアダプタです。インストールプロセスを完了するには、次の手順を実行する必要があります。

▼ SiteMinder リソースアダプタをインストールする

1 「管理するリソースの設定」ページの「カスタム リソース」セクションに、次のいずれかの値を追加します。

- `com.waveset.adapter.SiteminderAdminResourceAdapter`
  - `com.waveset.adapter.SiteminderLDAPResourceAdapter`
  - `com.waveset.adapter.SiteminderExampleTableResourceAdapter`

2 次の **JAR** ファイルを `$WSHOME/WEB-INF/lib` ディレクトリにコピーします。

- `smjavaagentapi.jar`

- smjavasdk2.jar

バージョンの競合が発生しないようにするために、Web エージェントディレクトリから JAR ファイルを取得します。これらのファイルが Web エージェントディレクトリに見つからない場合、これらのファイルは Netegrity\SiteMinder\SDK-2.2\java ディレクトリにもあります。

3 **SiteMinder Admin** リソースアダプタを使用する予定の場合は、アプリケーションサーバー起動スクリプトか、またはアプリケーションサーバーの起動前の環境に、**LIBPATH** (アプリケーションサーバープラットフォームによっては **LD_LIBPATH** または **SHLIB_PATH**) を設定してください。

たとえば Solaris では、Web エージェントは次のディレクトリにインストールされ、そこに nete_wa_env.sh というファイルが含まれます。

```
/opt/netegrity/siteminder/webagent
```

WebLogic の場合は、Weblogic.sh を起動するために、/bea/wlserver_*Version*/config/mydomain に次の行を追加します。

```
# In order to pickup the Siteminder libraries, the Netegrity
# Web agent libs need to be added to LIBPATH,
# LD_LIBRARY_PATH, and SHLIB_PATH
. /opt/netegrity/siteminder/webagent/nete_wa_env.sh
```

これらの行によって、SiteMinder Admin リソースアダプタが使用する Javaネイティブインタフェースメソッドに適した変数が設定されます。

作業が完了したら、Identity Manager アプリケーションサーバーを再起動します。

使用上の注意

なし。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は、SSL 経由の JNDI を使用して SiteMinder と通信します。

必要な管理特権

「User DN」リソースパラメータで指定されたユーザーに、ユーザーの読み取り、書き込み、削除、および追加のアクセス権を付与する必要があります。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	SiteMinder LDAP および Table では使用可SiteMinder Admin では使用不可
アカウントの名前の変更	なし
パススルー認証	あり
前アクションと後アクション	なし
データ読み込みメソッド	リソースからインポート

アカウント属性

SiteMinder Admin

次の表に、SiteMinder Admin アダプタのデフォルトのアカウント属性を示します。

アイデンティティーシステム ユーザー属性	種類	説明
description	String	管理者の説明
smAdminAuth	String	管理者承認が定義されたユーザー
smAdminDomains	String	ドメインを管理する管理者権限
smAdminAuthDir	String	ユーザーディレクトリ - LDAP、ODBC、WinNT、カスタム、AD
smAdminAuthScheme	String	管理者の認証スキーム: フォームを使用した「基本」認証、または接続中にクライアント証明書を使用した「X.509」
smAdminScope	String	クレデンシャルが適用されるホスト、ポート、および認証に対して定義された管理者スコープ

アイデンティティーシステム ユーザー属性	種類	説明
smManageSystemDomainObjects	String	エージェント、エージェントグループ、エージェント設定オブジェクト、ホスト設定オブジェクト、ユーザーディレクトリ、ポリシードメイン、アフィリエイトドメイン、管理者、認証スキーマ、登録スキーマ、エージェントタイプ、SQL クエリースキーマ、パスワードポリシー、信頼できるホスト、アイデンティティー環境などのシステムオブジェクトを管理する管理者の権限
smManageDomainObjects	String	十分な特権を持つ管理者が、レルム、規則、規則グループ、応答、応答グループ、変数、ポリシーなどのドメインオブジェクトを管理する管理者の権限
smManageUsers	String	ユーザーを管理する作成/編集/削除特権を使用して設定/設定解除する管理者権限
smManageKeysPwdPolicies	String	キーや、ユーザーに適用されるパスワードポリシーを管理する特権を持つ管理者
smManageReports	String	レポートを管理する管理者権限
smManageTrustedHosts	String	サーバーが信頼しているホスト

SiteMinder サンプルテーブル

次の表に、SiteMinder サンプルテーブルアダプタのデフォルトのアカウント属性を示します。

アイデンティティーシステム ユーザー属性	種類	説明
userID	Integer	ユーザーの一意の ID。
firstName	String	ユーザーの名。
lastName	String	ユーザーの姓。
email	String	ユーザーの電子メールアドレス。
telephoneNumber	String	ユーザーの電話番号。
expirePassword	Boolean	ログイン時にユーザーに新しいパスワードを強制的に入力させます。
pin	String	ユーザーの PIN。
mileage	Integer	SiteMinder のマニュアルを参照してください。

アイデンティティーシステム ユーザー属性	種類	説明
groups	String	アカウントが所属するグループ ID。

SiteMinder LDAP

次の表に、SiteMinder LDAP アダプタのデフォルトのアカウント属性を示します。

アイデンティティーシステム ユーザー属性	種類	説明
accountId	String	ユーザー ID。この属性は、uid リソース ユーザー属性に対応します。
accountId	String	必須。ユーザーのフルネーム。この属性は、cn リソースユーザー属性に対応します。
password	暗号化されています	ユーザーのパスワード。
firstname	String	ユーザーの名。
lastname	String	ユーザーの姓。
expirePassword	Boolean	ログイン時にユーザーに新しいパスワードを強制的に入力させます。
statusFlags	String	SiteMinder のマニュアルを参照してください。
ldapGroups	String	ユーザーの LDAP グループメンバーシップ。
modifyTimeStamp	String	ユーザーエントリが変更された日時を示します。
objectClass	String	ユーザーのオブジェクトクラス。

リソースオブジェクトの管理

なし

アイデンティティーテンプレート

$accountId$

サンプルフォーム

SiteminderAdminUserForm.xml

SiteminderExampleTableUserForm.xml

SiteminderLDAPUserForm.xml

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

- com.waveset.adapter.SiteminderAdminResourceAdapter
- com.waveset.adapter.SiteminderLDAPResourceAdapter
- com.waveset.adapter.SiteminderExampleTableResourceAdapter

◆ ◆ ◆ 第 43 章

43 Solaris

Solaris リソースアダプタは、com.waveset.adapter.SolarisResourceAdapter クラスで定義されます。

アダプタの詳細

リソースを設定する際の注意事項

リソースと Identity Manager 間の通信に SSH (Secure Shell) を使用する場合は、アダプタを設定する前に、リソースで SSH を設定します。

Solaris で NIS アカウントを管理する場合は、SPARC システムではパッチ 125549-01 を、x86 システムではパッチ 125550–01 をインストールして、logins コマンドと Solaris アダプタのパフォーマンスを向上させます。

Identity Manager のインストールに関する注意事項

このリソースでは、追加のインストール手順は必要ありません。

使用上の注意

Solaris リソースアダプタは主に、次の Solaris コマンドのサポートを提供します。

- useradd、usermod、userdel
- groupadd、groupmod、groupdel
- passwd

サポートされる属性およびファイルの詳細については、これらのコマンドに関する Solaris マニュアルページを参照してください。

このアダプタは、Solaris Trusted Extensions をサポートしていません。

Solaris リソースでユーザーアカウントの名前を変更すると、グループメンバーシップは新しいユーザー名に移動されます。次の条件に該当する場合は、ユーザーのホームディレクトリの名前も変更されます。

- 元のホームディレクトリの名前がユーザー名と一致していた。
- 新しいユーザー名と一致するディレクトリがまだ存在していない。

UNIX リソース (AIX、HP-UX、Solaris、または Linux) に接続するときは、root シェルとして Bourne 互換シェル (sh、ksh) を使用してください。

UNIX アカウントを管理する管理アカウントには、英語 (en) または C ロケールを使用してください。これは、ユーザーの `.profile` ファイルで設定できます。

NIS が実装されている環境では、次の機能を実装することにより、一括プロビジョニング中のパフォーマンスを向上させることができます。

- `user_make_nis` という名前のアカウント属性をスキーママップに追加し、この属性を調整やその他の一括プロビジョニングワークフローで使用します。この属性を追加した場合、リソース上の各ユーザーが更新された後は、システムで NIS データベースへの接続手順がバイパスされます。
- すべてのプロビジョニングが完了した後で NIS データベースに変更を書き込むには、ワークフローで `NIS_password_make` という名前の ResourceAction を作成します。

Solaris リソースの新しいユーザーアカウントは、passwd(1) コマンドが実行されるまでロックされたままになります。Solaris のユーザーアカウントが作成されたあと、`passwd -s <user>` を実行すると、ステータスはロック中 (LK) として表示されます。アカウントをネイティブに作成したあと、Solaris Risk Analysis レポートの「Locked out Accounts」セクションに、新しく作成したアカウントが表示されます。新しく作成されたアカウントは、Risk Analysis レポートの「Accounts With No Password」セクションには表示されません。

ユーザーパスワードに制御文字 (0x00、0x7f など) を使用しないでください。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は、次の接続を使用して Solaris アダプタと通信できます。

- Telnet
- SSH (SSH はリソース上に個別にインストールする)
- SSHPubKey

SSHPubKey 接続の場合、「リソースパラメータ」ページで非公開鍵を指定する必要があります。この鍵には `--- BEGIN PRIVATE KEY ---` および `--- END PRIVATE KEY --` のような注釈行を含める必要があります。公開鍵は、サーバー上の `/.ssh/authorized_keys` ファイルに配置する必要があります。

必要な管理特権

このアダプタでは、一般ユーザーとしてログインしてから su コマンドを実行し、root ユーザー (または root ユーザーと同等のアカウント) に切り替えて管理アクティビティーを実行できます。 また、root ユーザーとして直接ログインすることもできます。また、root ユーザーとして直接ログインすることもできます。

このアダプタは、sudo 機能 (バージョン 1.6.6 以降) もサポートします。この機能は、Solaris 9 に Companion CD からインストールできます。sudo 機能を使用すると、システム管理者は特定のユーザー (またはユーザーのグループ) に、root ユーザーまたは別のユーザーとして一部 (またはすべて) のコマンドを実行する能力を与えることができます。

さらに、sudo がリソースで有効になっている場合は、その設定が、root ユーザーのリソース定義ページでの設定よりも優先されます。

sudo を使用する場合は、Identity Manager 管理者に対して有効にされたコマンドの `tty_tickets` パラメータを true に設定する必要があります。詳細については、sudoers ファイルのマニュアルページを参照してください。

管理者は、sudo で次のコマンドを実行する特権が付与されている必要があります。

ユーザーとグループのコマンド		NIS コマンド	その他のコマンド	
■ auths	■ passwd	■ make	■ awk	■ ls
■ groupadd	■ profiles	■ ypcat	■ cat	■ mv
■ groupdel	■ roles	■ ypmatch	■ chmod	■ rm
■ groupmod	■ useradd	■ yppasswd	■ chown	■ sed
■ last	■ userdel		■ cp	■ sleep
■ listusers	■ usermod		■ cut	■ sort
■ logins			■ diff	■ tail
			■ echo	■ touch
			■ grep	■ which

テスト接続を使用して次のテストができます。

- 各コマンドが管理ユーザーのパスに存在するかどうか
- 管理ユーザーが /tmp に書き込めるかどうか
- 管理ユーザーに、特定のコマンドを実行する権限があるかどうか

注 – テスト接続では、通常のプロビジョニングの実行とは異なるコマンドオプションを使用できます。

このアダプタには、基本的な sudo 初期化機能とリセット機能が用意されています。ただし、リソースアクションが定義されていて、そこに sudo 認証を必要とするコマンドが含まれている場合は、UNIX コマンドとともに sudo コマンドを指定してください。たとえば、単に useradd と指定する代わりに sudo useradd を指定してください。sudo を必要とするコマンドは、ネイティブリソースに登録されている必要があります。それらのコマンドを登録するには、visudo を使用します。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	Solaris は、Identity Manager の enable アクションと disable アクションをネイティブではサポートしません。Identity Manager は、ユーザーのパスワードを変更することによって、アカウントの有効化と無効化をシミュレートします。enable アクションでは変更されたパスワードが公開されますが、disable アクションでは公開されません。 その結果、enable アクションと disable アクションは update アクションとして処理されます。update で動作するように設定されている前アクションと後アクションすべてが実行されます。
アカウントの名前の変更	あり
パススルー認証	あり
前アクションと後アクション	あり
データ読み込みメソッド	■ リソースから直接インポート ■ リソースの調整

このリソース上のすべてのユーザーに対して、次のタスクを制御するリソース属性を定義できます。

- ユーザーの作成時にホームディレクトリを作成する
- ユーザーの作成時にユーザーのホームディレクトリにファイルをコピーする
- ユーザーの削除時にホームディレクトリを削除する

アカウント属性

次の表に、Solaris ユーザーのアカウント属性を示します。特に記載されていないかぎり、属性は省略可能です。属性の型はすべて String です。

アイデンティティーシステムユーザー属性	リソースユーザー属性	説明
accountId	accountId	必須。ユーザーのログイン名。
説明	comment	ユーザーのフルネーム。
Home directory	dir	ユーザーのホームディレクトリ。このアカウント属性で指定された値はすべて、「ホームベースディレクトリ」リソース属性で指定された値よりも優先されます。

アイデンティティーシステムユーザー属性	リソースユーザー属性	説明
Expiration date	expire	アカウントにアクセスできる最終日付。この属性は、NIS アカウントではサポートされていません。
Primary group	group	ユーザーの一次グループ。
Inactive	inactive	アカウントが非アクティブになってからロックされるまでの日数。NIS アカウントではサポートされていません。
Secondary groups	secondary_group	ユーザーの二次グループのコンマ区切りリスト。 ロールを有効にしてこの属性をプロビジョニングするには、'csv=true' を Role オブジェクト XML の RoleAttribute 要素に追加する必要があります。
Login shell	shell	ユーザーのログインシェル。 NIS マスターにプロビジョニングしている場合は、ユーザーシェルの値は NIS マスターに対してのみチェックされます。ユーザーがログオンする可能性のあるその他のマシンに対してチェックは実行されません。
Last login time	time_last_login	最終ログインの日時。この値は読み取り専用です。
User ID	uid	数字形式でのユーザー ID。
Authorizations	authorization	付与された権限のコンマ区切りリスト。
Profiles	profile	プロファイルのコンマ区切りリスト。
Roles	ロール	ロールのコンマ区切りリスト。
expirePassword	force_change	ログイン時にユーザーに新しいパスワードを強制的に入力させます。この属性は、デフォルトではスキーママップに一覧表示されていません。

リソースオブジェクトの管理

Identity Manager は、次のネイティブ Solaris オブジェクトをサポートします。

リソースオブジェクト	サポートされる機能	管理される属性
Group	作成、更新、削除、名前の変更、名前を付けて保存	groupName、gid、users

アイデンティティーテンプレート

```
$accountId$
```

サンプルフォーム

組み込みのフォーム

- Solaris Group Create Form
- Solaris Group Update Form

その他の利用可能なフォーム

SolarisUserForm.xml

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

- `com.waveset.adapter.SolarisResourceAdapter`
- `com.waveset.adapter.SVIDResourceAdapter`
- `com.waveset.adapter.ScriptedConnection`

◆ ◆ ◆ 第 44 章

Sun Java System Communications Services アダプタ

Identity Manager では、Sun Java™ System Messaging Server (Messaging Server) と Sun Java System Calendar Server (Calendar Server) をサポートする、Sun Java System Communications Services リソースアダプタが提供されます。これらのシステムは、LDAP Schema 2 を実装している必要があります。また、Sun Java System Directory Server をユーザーストアとして使用する必要があります。

Sun Java System Communications Services リソースアダプタは、`com.waveset.adapter.SunCommunicationsServicesResourceAdapter` クラスで定義されます。

アダプタの詳細

このアダプタは、LDAP リソースアダプタを拡張します。あとのトピックに示す LDAP 固有の機能の実装については、LDAP アダプタのマニュアルを参照してください。

Communications Services アダプタは、標準の Directory Server のインストールに、プロビジョニングサービスを提供します。Directory Server のレプリケーションの更新履歴ログを読み取り、それらの変更を Identity Manager ユーザーまたはカスタムワークフローに適用することもできます。

リソースを設定する際の注意事項

Sun Java System Directory Server リソースを Communications Services アダプタで使用するように設定するには、更新履歴ログを有効にし、変更者情報の追跡を有効にするように、サーバーを設定する必要があります。この操作は、ディレクトリサーバーの設定タブで行います。

▼ Communications Services アダプタで使用するように Directory Server リソースを設定する

1 「レプリケーション」フォルダをクリックし、「**Enable change log**」ボックスを選択します。**5.0** 以降のサーバーでは、**RetroChangelog** スナップインも有効にします。設定タブで、プラグインオブジェクトに移動し、旧バージョン形式の更新履歴ログプラグインを選択して有効にします。

2 新しく作成または変更したエントリの特殊な属性を管理するようにサーバーが設定されていることを確認するには、**Directory Server** コンソールで、「設定」をクリックし、左側の区画でナビゲーションツリーのルートエントリを選択します。

3 「設定」をクリックし、「エントリの変更時間を記録」ボックスにチェックマークが付いていることを確認します。

サーバーは、イベントが Identity Manager から起動されたかどうかを判断するために、新しく作成または変更したエントリに次の属性を追加します。

- **creatorsName**: そのエントリを最初に作成したユーザーの DN。
- **modifiersName**: そのエントリを最後に変更したユーザーの DN。

Identity Manager のインストールに関する注意事項

このリソースでは、追加のインストール手順は必要ありません。

使用上の注意

サービスアカウント

管理アカウントの CN=Directory Manager を使用するのではなく、Communications Services に接続するための Identity Manager サービスアカウントを作成します。Directory Server 管理ツールを使用して、各ベースコンテキストで ACI (アクセス制御命令) を介してアクセス権を設定します。

ACI でのアクセス権をソースに基づいて設定します。アダプタからアイデンティティー情報の源泉となるソースに接続する場合は、読み取り、検索、および (場合によっては) 比較のアクセス権のみを設定します。アダプタを書き戻し用に使用する場合は、書き込みと (場合によっては) 削除のアクセス権を設定します。

注 – 更新履歴ログの監視にアカウントを使用する場合は、cn=changelog で ACI も作成するようにしてください。更新履歴ログのエントリに対しては書き込みも削除もできないため、アクセス権は読み取りと検索のみに設定するとよいでしょう。

waveset.properties ファイル内の sources.*ResourceName* .hosts プロパティーを使用して、Active Sync を使用してリソースの同期を行うクラスタ内のホストを選択できます。*ResourceName* は、リソースオブジェクトの名前に置き換える必要があります。

前アクションと後アクション

Sun Communications Services リソースアダプタは、前アクションと後アクションを実行しません。代わりに、リソースウィザードの「アクションプロキシリソースアダプタ」フィールドを使用して、アクションを実行するように設定されたプロキシリソースアダプタを指定できます。

次のサンプルスクリプトは、ユーザーの作成後にプロキシリソースで実行できます。

```
SET PATH=c:\Sun\Server-Root\lib
SET SYSTEMROOT=c:\winnt
SET CONFIGROOT=C:/Sun/Server-Root/Config
mboxutil -c -P user/%WSUSER_accountId%.*
```

次のサンプルスクリプトは、ユーザーが削除されたときに、そのユーザーのメールボックスを削除します

```
SET PATH=c:\Sun\Server-Root\lib
SET SYSTEMROOT=c:\winnt
SET CONFIGROOT=C:/Sun/Server-Root/Config
mboxutil -d -P user/%WSUSER_accountId%.*
```

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は、TCP/IP または SSL 経由の Java Naming and Directory Interface (JNDI) を使用して、Communications Services アダプタと通信します。

- TCP/IP を使用する場合は、リソース編集ページでポート 389 を指定します。
- SSL を使用する場合は、ポート 636 を指定します。

必要な管理特権

「ユーザー DN」リソースパラメータに値 `cn=Directory Manager` を指定すると、Identity Manager 管理者には、アカウント管理に必要なアクセス権が付与されます。別の識別名を指定する場合は、そのユーザーに、ユーザーの読み取り、書き込み、削除、および追加のアクセス権を付与してください。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	あり
パススルー認証	あり
前アクションと後アクション	使用不可。ただし、プロキシリソースアダプタを指定できます。
データ読み込みメソッド	■ リソースから直接インポート ■ リソースの調整 ■ Active Sync

アカウント属性

属性の構文 (または型) は、通常、属性がサポートされるかどうかを決定します。一般に、Identity Manager は Boolean 型、文字列型、整数型、およびバイナリ型の構文をサポートします。バイナリ属性は、バイト配列としてのみ安全に表現できる属性です。

次の表に、サポートされている LDAP 構文の一覧を示します。ほかの LDAP 構文でも、事実上 Boolean 型、文字列型、または整数型であれば、サポートされる可能性があります。オクテット文字列はサポートされません。

LDAP 構文	属性タイプ	オブジェクト ID
Audio	Binary	1.3.6.1.4.1.1466.115.121.1.4
Binary	Binary	1.3.6.1.4.1.1466.115.121.1.5
Boolean	Boolean	1.3.6.1.4.1.1466.115.121.1.7

LDAP 構文	属性タイプ	オブジェクト ID
Country String	String	1.3.6.1.4.1.1466.115.121.1.11
DN	String	1.3.6.1.4.1.1466.115.121.1.12
Directory String	String	1.3.6.1.4.1.1466.115.121.1.15
Generalized Time	String	1.3.6.1.4.1.1466.115.121.1.24
IA5 String	String	1.3.6.1.4.1.1466.115.121.1.26
Integer	Int	1.3.6.1.4.1.1466.115.121.1.27
Postal Address	String	1.3.6.1.4.1.1466.115.121.1.41
Printable String	String	1.3.6.1.4.1.1466.115.121.1.44
Telephone Number	String	1.3.6.1.4.1.1466.115.121.1.50

デフォルトのアカウント属性

次の属性が、Communications Services リソースアダプタの「アカウント属性」ページに表示されます。特に記載されていないかぎり、属性の型はすべて String です。

アイデンティティーシステムユーザー属性	リソースユーザー属性	説明
accountId	uid	User ID
accountId	cn	必須。ユーザーのフルネーム。
password	userPassword	暗号化されています
firstname	givenname	ユーザーの名。
lastname	sn	必須。ユーザーの姓。
email	mail	ユーザーの完全修飾電子メールアドレス。
modifyTimeStamp	modifyTimeStamp	ユーザーエントリが変更された日時を示します。 デフォルトでは、この属性は Sun Communications Services アダプタでのみ表示されます。
objectClass	objectClass	変更を監視するオブジェクトクラス。
alternateEmail	mailalternateaddress	この受信者の代替電子メールアドレス。

アイデンティティーシステムユーザー属性	リソースユーザー属性	説明
mailDeliveryOption	maildeliveryoption	メール受信者の配信オプションを指定します。インバウンドメッセージの複数の配信経路をサポートするために、ユーザーエントリまたはグループエントリに、1 つ以上の値を指定できます。この属性が inetMailGroup または inetMailUser で使用されるかどうかによって、値の適用方法が異なります
mailHost	mailhost	この受信者に送信されたメッセージの最終宛先となる、メール転送エージェント (MTA) の完全修飾ホスト名。
mailForwardingAddress	mailforwardingaddress	インバウンドメッセージ用の 1 つ以上の転送アドレスを指定します。
inetUserStatus	inetuserstatus	グローバルサーバーアクセスに関するユーザーのアカウントのステータスを指定します。指定できる値は、active、inactive、または deleted です。
mailQuota	mailquota	ユーザーのメールボックスに許可されたディスク容量 (バイト単位)。
mailAutoReplySubject	mailautoreplysubject	自動返信応答の件名として使用されるテキスト。
mailAutoReplyText	mailautoreplytext	受信者のドメイン内のユーザーを除くすべての送信者に送信された自動返信テキスト。
mailAutoReplyTextInternal	mailautoreplytextinternal	受信者のドメインから送信者に送信された自動返信テキスト。
vacationStartDate	vacationstartdate	不在返信開始日時 (*YYYYMMDDHHMMSS*Z 形式)。
vacationEndDate	vacationenddate	不在返信終了日時 (*YYYYMMDDHHMMSS*Z 形式)。
mailAutoReplyMode	mailautoreplymode	ユーザーのメールアカウントの自動返信モード。指定できる値は、echo と reply です。

デフォルトでサポートされるオブジェクトクラス

デフォルトでは、Sun Java System Communications Services リソースアダプタは、LDAP ツリーに新しいユーザーオブジェクトを作成するときに次のオブジェクトクラスを使用します。ほかのオブジェクトクラスが追加される場合もあります。

- top
- person
- inetUser
- organizationalPerson
- inetOrgPerson
- ipUser
- userPresenceProfile
- iplanet-am-managed-person
- inetMailUser
- inetLocalMailRecipient
- icscalendaruser

top オブジェクトクラス

top オブジェクトクラスには、デフォルトでアカウント属性として表示される `objectClass` 属性を含めます。top オブジェクトクラスは、`person` などのいくつかのオブジェクトクラスによって拡張されます。

person オブジェクトクラス

次の表に、LDAP person オブジェクトクラスで定義される追加のサポート対象属性を示します。

リソースユーザー属性	LDAP 構文	属性タイプ	説明
`description`	`Directory string`	String	ユーザーの特定の関心事についての簡潔でわかりやすい説明
`seeAlso`	`DN`	String	ほかのユーザーへの参照。
`telephoneNumber`	`Telephone number`	String	第一電話番号

inetUser オブジェクトクラス

inetUser オブジェクトクラスは、ユーザーアカウント、またはサービスが提供される任意のオブジェクトとして定義されたリソースアカウントを表します。メールアカウントを作成するために、`inetMailUser` および `ipUser` とともに使用されます。ユーザーアカウントを作成するときに、このオブジェクトクラスは `inetOrgPerson` によって作成されたベースエントリを拡張します。

次の表に、inetUser オブジェクトクラスで定義される追加のサポート対象属性の一覧を示します。

リソースユーザー属性	LDAP 構文	属性タイプ	説明
inetUserStatus	Directory string	String	グローバルサーバーアクセスに関するユーザーのアカウントのステータスを指定します。指定できる値は、active、inactive、および deleted です。

organizationalPerson オブジェクトクラス

次の表に、LDAP Organizationalperson オブジェクトクラスで定義される追加のサポート対象属性を示します。このオブジェクトクラスは、Person オブジェクトクラスから属性を継承することもできます。

リソースユーザー属性	LDAP 構文	属性タイプ	説明
destinationIndicator	Printable string	String	この属性は、電報サービスに使用されます。
facsimileTelephoneNumber	Facsimile telephone number	String	第一 FAX 番号。
internationaliSDNNumber	Numeric string	String	オブジェクトに関連付けられた国際 ISDN 番号を指定します。
l	Directory string	String	都市、国、その他の地理的領域などの地域の名前
ou	Directory string	String	組織単位の名前
physicalDeliveryOfficeName	Directory string	String	配達物の送付先となるオフィス。
postalAddress	Postal address	String	ユーザーの勤務先オフィスの所在地。
postalCode	Directory string	String	郵便配達用の郵便番号。
postOfficeBox	Directory string	String	このオブジェクトの私書箱番号。
preferredDeliveryMethod	Delivery method	String	受取人への優先される送付方法
registeredAddress	Postal Address	String	受信者に配達を受け入れてもらう必要がある電報や速達文書の受け取りに適した郵便の宛先。
st	Directory string	String	州名または都道府県名。
street	Directory string	String	郵便の宛先の番地部分。
teletexTerminalIdentifier	Teletex Terminal Identifier	String	オブジェクトに関連付けられたテレテックス端末の識別子

リソースユーザー属性	LDAP 構文	属性タイプ	説明
telexNumber	Telex Number	String	国際表記法によるテレックス番号
title	Directory string	String	ユーザーの役職を格納します。このプロパティーは、一般に、プログラマーのような職種ではなく、「シニアプログラマー」のような正式な役職を示すために使用されます。通常、Esq. や DDS などの敬称には使用されません。
x121Address	Numeric string	String	オブジェクトの X.121 アドレス。

inetOrgPerson オブジェクトクラス

次の表に、LDAP inetOrgPerson オブジェクトクラスで定義される追加のサポート対象属性を示します。このオブジェクトクラスは、organizationalPerson オブジェクトクラスから属性を継承することもできます。

リソースユーザー属性	LDAP 構文	属性タイプ	説明
audio	Audio	Binary	オーディオファイル。
businessCategory	Directory string	String	組織で実施されているビジネスの種類。
carLicense	Directory string	String	自動車の登録番号 (ナンバープレート)
departmentNumber	Directory string	String	組織内の部署を特定します
displayName	Directory string	String	エントリを表示するときに優先的に使用されるユーザーの名前
employeeNumber	Directory string	String	組織内の従業員を数値で示します
employeeType	Directory string	String	従業員、契約社員などの雇用形態
homePhone	Telephone number	String	ユーザーの自宅電話番号。
homePostalAddress	Postal address	String	ユーザーの自宅住所。
initials	Directory string	String	ユーザーのフルネームの各部のイニシャル。
jpegPhoto	JPEG	Binary	JPEG 形式のイメージ。
labeledURI	Directory string	String	ユーザーに関連付けられた URI (Universal Resource Indicator) とオプションのラベル。

リソースユーザー属性	LDAP 構文	属性タイプ	説明
mail	IA5 string	String	1 つ以上の電子メールアドレス。
manager	DN	String	ユーザーのマネージャーのディレクトリ名。
mobile	Telephone number	String	ユーザーの携帯電話番号。
o	Directory string	String	組織の名前。
pager	Telephone number	String	ユーザーのポケットベル番号。
preferredLanguage	Directory string	String	優先される、ユーザーの書き言葉または話し言葉の言語。
roomNumber	Directory string	String	ユーザーのオフィスまたは部屋の番号。
secretary	DN	String	ユーザーの管理補佐のディレクトリ名。
userCertificate	certificate	Binary	バイナリ形式の証明書。

ipUser

ipUser オブジェクトクラスは、個人用のアドレス帳コンテナとサービス指定子のクラスへの参照を保持します。

次の表に、ipUser オブジェクトクラスで定義される追加のサポート対象属性の一覧を示します。

リソースユーザー属性	構文	属性タイプ	説明
inetCoS	String、multi-valued	String	ユーザーエントリの属性に値を供給するサービスクラス (CoS) テンプレートの名前を指定します。
memberOfPAB	String、multi-valued	String	このエントリが属する個人用アドレス帳の一意名。
maxPabEntries	Integer、single-valued	Integer	ユーザーが個人用アドレス帳ストアに保持できる個人用アドレス帳エントリの最大数。
pabURI	String、single valued	String	このユーザーの個人用アドレス帳エントリのコンテナを指定する LDAP URI。

userPresenceProfile

userPresenceProfile オブジェクトクラスは、ユーザーのプレゼンス情報を格納します。

このオブジェクトクラスには、デフォルトのアカウント属性として存在する `vacationStartDate` 属性と `vacationEndDate` 属性が含まれることもあります。

iplanet-am-managed-person

iplanet-am-managed-person オブジェクトクラスには、Sun Java System Access Manager でユーザーを管理するために必要な属性を含みます。

次の表に、ipUser オブジェクトクラスで定義される追加のサポート対象属性の一覧を示します。

リソースユーザー属性	構文	属性タイプ	説明
`iplanet-am-modifiable-by`	DN、multi-valued	String	ユーザーエントリを変更できるアクセス権を持つ管理者のロール DN。
`iplanet-am-role-aci-description`	String、multi-valued	String	ロールに所属する ACI の説明。
`iplanet-am-static-group-dn`	DN、multi-valued	String	ユーザーが所属する静的グループの DN を定義します。
`iplanet-am-user-account-life`	Date string、single-valued	String	アカウントの有効期限を、yyyy/mm/dd hh:mm:ss の形式で指定します。

inetMailUser

inetMailUser は、メッセージングサービスのユーザーを定義するために、`inetOrgPerson` によって作成されたベースエントリを拡張します。メールアカウントを表し、`inetUser` および`inetLocalMailRecipient` とともに使用されます。

次の表に、inetMailUser オブジェクトクラスで定義される追加のサポート対象属性の一覧を示します。

リソースユーザー属性	構文	属性タイプ	説明
`dataSource`	String、single-valued	String	タグまたは識別子を格納するテキストフィールド。
`mailAllowedServiceAccess`	String、single-valued	String	アクセスフィルタ (規則) を格納します。

リソースユーザー属性	構文	属性タイプ	説明
mailAntiUBEService	String、multi-valued	String	迷惑メールを処理するプログラムに関する指示。
mailAutoReplyTimeOut	Integer、single-valued	Integer	任意のメール送信者への連続自動返信応答の間隔 (時間単位)。
mailConversionTag	String、multi-valued	String	ユーザーエントリまたはグループエントリの一意の変換動作を指定するメソッド。
mailDeferProcessing	String、single-valued	String	現在のユーザーエントリまたはグループエントリのアドレス拡張をすぐに実行するか、保留するかを制御します。
mailEquivalentAddress	String、multi-valued	String	メールルーティングに関しては mailAlternateAddress と同じですが、この属性はヘッダーを書き換えません。
mailMessageStore	String、single-valued	String	ユーザーのメッセージストアパーティション名を指定します。
mailMsgMaxBlocks	Integer、single-valued	Integer	このユーザーまたはグループに送信できる最大メッセージサイズ (MTA ブロック数単位)。
mailMsgQuota	Integer、single-valued	Integer	ユーザーに許可される最大メッセージ数
mailProgramDeliveryInfo	String、multi-valued	String	プログラムの配信に使用される 1 つ以上のプログラムを指定します。
mailSieveRuleSource	String、multi-valued	String	ユーザーエントリに対するメッセージフィルタスクリプトの作成に使用される SIEVE 規則 (RFC 3028 に準拠) が含まれます。
mailSMTPSubmitChannel	String、single-valued	String	この属性は、保証付きメッセージ配信の設定、またはその他の特別なサービスクラスの設定に関連する要因となります。
mailUserStatus	String、single-valued	String	メールユーザーの現在のステータス。active、inactive、deleted、hold、overquota、remo のいずれかにできます。
nswmExtendedUserPrefs	String、multi-valued	String	ソート順序とメール送信者アドレスなど、Messenger Express の設定を定義するペアを保持します。

inetLocalMailRecipient

inetLocalMailRecipient オブジェクトクラスは、ローカルの電子メール受信者を表す LDAP エントリを指定する方法、受信者の電子メールアドレスを指定する方法、および受信者に適したルーティング情報を提供する方法を示す情報を格納します。

次の表に、inetLocalMailRecipient オブジェクトクラスで定義される追加のサポート対象属性の一覧を示します。このオブジェクトクラス内のほかの属性はすべて、デフォルトでアカウント属性として存在しています。

リソースユーザー属性	LDAP 構文	属性タイプ	説明
mailRoutingAddress	String、single-valued	String	mailHost と一緒に使用して、ここでアドレスを処理するか、別のシステムに転送するかを決定します。

icsCalendarUser

icsCalendarUser オブジェクトクラスは、Calendar Server ユーザーを定義します。

次の表に、icsCalendarUser オブジェクトクラスで定義される追加のサポート対象属性の一覧を示します。このオブジェクトクラス内のほかの属性はすべて、デフォルトでアカウント属性として存在しています。

リソースユーザー属性	LDAP 構文	属性タイプ	説明
icsAllowedServiceAccess	String、single-valued	String	ユーザーのカレンダサービスを無効にします。
icsCalendar	String、single-valued	String	ユーザーまたはリソースのデフォルトのカレンダの ID (calid)。Calendar Manager の必須属性です。
icsCalendarOwned	String、multi-valued	String	このユーザーが所有するカレンダ。
icsDWPHost	String、single-valued	String	DWP (Database Wire Protocol) ホスト名を格納します。 これにより、カレンダ ID は、カレンダとそのデータを格納する DWP サーバーに解決されます。
icsExtendedUserPrefs	String、multi-valued	String	カレンダのユーザー設定の拡張。
icsFirstDay	String、single-valued	Integer	ユーザーのカレンダに表示される週の最初の日。

リソースユーザー属性	LDAP 構文	属性タイプ	説明
icsSet	String、multi-valued	String	カレンダの 1 グループを定義します。この属性の値は 6 つの部分からなる文字列で、各部分はドル記号 ($) で区切られます。
icsStatus	String、single-valued	String	この属性は、カレンダサービスをドメインに割り当てるときに設定します。指定できる値は、active、inactive、および deleted です。
icsSubscribed	String、multi-valued	String	このユーザーが登録しているカレンダのリスト。
icsTimezone	String	String	ユーザー設定で明示的に指定されていない場合に、このユーザーカレンダまたはリソースカレンダで使用するデフォルトのタイムゾーン。
preferredLanguage	String、single-valued	String	優先される、ユーザーの書き言葉または話し言葉の言語。

リソースオブジェクトの管理

Identity Manager は、デフォルトで次の LDAP オブジェクトをサポートします。文字列ベース、整数ベース、またはブールベースの属性も管理できます。

リソースオブジェクト	オブジェクトクラス	サポートされる機能	管理される属性
Group	groupOfUniqueNames iplanet-am-managed-group iplanet-am-managed-filtered-group iplanet-am-managed-assignable-group iplanet-am-managed-static-group inetMailGroup inetLocalRecipient	作成、更新、削除、名前の変更、名前を付けて保存、検索	cn、description、owner、uniqu

リソースオブジェクト	オブジェクトクラス	サポートされる機能	管理される属性
Domain	domain	検索	dc
	organization		
	inetdomainauthinfo		
	sunManagedOrganization の		
	sunNameSpace		
	mailDomain の		
	icsCalendarDomain		
Organizational Unit	organizationalUnit	作成、名前の変更、名前を付けて保存、検索	ou
	iplanet-am-managed-people-container		
組織	organization	作成、名前の変更、名前を付けて保存、検索	o

アイデンティティーテンプレート

なし。有効な値を持つアイデンティティーテンプレートを設定してください。

サンプルフォーム

- Sun Java System Communications Services ActiveSync Form
- Sun Java System Communications Services Create Group Form
- Sun Java System Communications Services Create Organizational Unit Form
- Sun Java System Communications Services Create Organization Form
- Sun Java System Communications Services Update Group Form
- Sun Java System Communications Services Update Organizational Unit Form

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

- `com.waveset.adapter.SunCommunicationsServicesResourceAdapter`
- `com.waveset.adapter.LDAPResourceAdapter`
- `com.waveset.adapter.LDAPResourceAdapterBase`

◆ ◆ ◆ 第 45 章

Sybase ASE

Sybase ASE リソースアダプタは、Sybase Adaptive Server Enterprise をサポートします。このアダプタは、`com.waveset.adapter.SybaseASEResourceAdapter` クラスで定義されます。このアダプタは、非推奨の Sybase アダプタ (`com.waveset.adapter.SybaseResourceAdapter`) を置き換えます。

アダプタの詳細

このアダプタを使用して、Sybase Adaptive Server Enterprise にログインするためのユーザーアカウントをサポートします。カスタム Sybase テーブルがある場合、リソースアダプタウィザードを使用してカスタム Sybase テーブルリソースを作成する方法については、第 10 章「データベーステーブル」を参照してください。

リソースを設定する際の注意事項

なし

Identity Manager のインストールに関する注意事項

Sybase ASE リソースアダプタは、カスタムアダプタです。インストールプロセスを完了するには、次の手順を実行する必要があります。

▼ Sybase ASE リソースアダプタをインストールする

1 *SybaseInstallDir*`\jConnect-5_5\classes\jconn2.jar` ファイルを `$WSHOME$/WEB-INF/lib` ディレクトリにコピーします。

2 「管理するリソースの設定」ページの「カスタムリソース」セクションに次の値を追加します。

```
com.waveset.adapter.SybaseASEResourceAdapter
```

次に、「保存」をクリックします。

使用上の注意

なし

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は、SSL 経由の JDBC を使用してこのアダプタと通信します。

必要な管理特権

次の表に、システムプロシージャーの実行に必要なアクセス権の一覧を示します。

システムプロジージャー	必要なアクセス権
sp_addlogin、sp_droplogin	システム管理者またはシステムセキュリティー担当者
sp_adduser、sp_droplogin	データベース所有者、システム管理者、またはシステムセキュリティー担当者
sp_changegroup	データベース所有者、システム管理者、またはシステムセキュリティー担当者
sp_displayroles	システム管理者またはシステムセキュリティー担当者
sp_helpuser	なし
sp_locklogin	システム管理者またはシステムセキュリティー担当者
sp_modifylogin	システム管理者のみ、sp_modifylogin を実行してデフォルトのデータベースを変更できます。すべてのユーザーは、sp_modifylogin を実行して自分のログインアカウントを変更できます。

システムプロジージャー	必要なアクセス権
sp_password	システムセキュリティー担当者のみ、sp_password を実行してほかのユーザーのパスワードを変更できます。すべてのユーザーは、sp_password を実行して自分のパスワードを変更できます。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	なし
パススルー認証	あり
前アクションと後アクション	なし
データ読み込みメソッド	■ リソースから直接インポート ■ リソースの調整

アカウント属性

次の表に、デフォルトのアカウント属性の一覧を示します。デフォルトの属性はすべて文字列です。

アイデンティティーシステムユーザー属性	リソース属性名	説明
serverRoles	serverRoles	ユーザーが割り当てられているデータベースサーバーロール。
defaultDB	defaultDB	ユーザーがデフォルトで使用するデータベース。

複数のデータベースを管理する可能性があるため、Identity Manager の管理者は、各データベースを管理するためのアカウント属性を追加する必要があります。ほかの管理対象データベースの属性と区別するため、これらの属性には属性名の一部としてデータベース名を含めてください。

アイデンティティーシステム ユーザー属性	データ型	説明
userNameDBName	String	データベース上のアカウントのユーザー名。データベースの userName を設定することによってアカウントにデータベースへのアクセス権が与えられ、データベースの userName を消去することによってアクセス権が削除されます。
groupDBName	String	データベース上のアカウントのグループ。

リソースオブジェクトのサポート

管理対象オブジェクト

このアダプタは、Sybase ASE リソース上のオブジェクトを管理しません。

一覧表示可能なオブジェクト

次の表では、ユーザーフォーム内で listAllObjects メソッドを使用して呼び出すことのできる Sybase オブジェクトについて説明します。

Object	説明
allDatabases	リソース上のデータベースを一覧表示します。
dbGroups	リソース上で管理されているデータベース内のグループを一覧表示します。
managedDatabases	リソースで管理されているデータベースを一覧表示します。このリストは、「データベース」リソース属性で設定されます。
serverRoles	ユーザーが割り当てられているデータベースサーバーロールを一覧表示します。

アイデンティティーテンプレート

$accountId$

サンプルフォーム

SybaseASEUserForm

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

- `com.waveset.adapter.SybaseASEResourceAdapter`
- `com.waveset.adapter.JdbcResourceAdapter`

◆ ◆ ◆ 第 46 章

Tivoli Access Manager

Tivoli Access Manager リソースアダプタは、`com.waveset.adapter.AccessManagerResourceAdapter` クラスで定義されます。

アダプタの詳細

リソースを設定する際の注意事項

ここでは、Access Manager リソースの設定手順を説明します。 次のような手順があります。

- IBM Tivoli Access Manager リソースを Identity Manager で使用するための一般的な設定手順
- Access Manager を Identity Manager の Web Access Control として使用するための手順

一般的な設定

IBM Tivoli Access Manager リソースを Identity Manager で使用するように設定する場合は、次の手順に従います。

▼ Tivoli Access Manager を設定する

1. **IBM Tivoli Access Manager Java Runtime Component** を **Identity Manager** サーバーにインストールします。
2. 使用しているアプリケーションサーバーの **JVM** へのパスを含むように **PATH** 変数を設定します。
3. `pdjrtecfg -action config` コマンドを実行して、次の **Access Manager** の `.jar` ファイルを **JRE** の `lib/ext` ディレクトリにインストールします。

- ibmjceprovider.jar
  - ibmjsse.jar
  - ibmpkcs.jar
  - jaas.jar
  - local_policy.jar
  - PD.jar
  - US_export_policy.jar
  - ibmjcefw.jar

    詳細については、『IBM Tivoli Access Manager Base インストール・ガイド』を参照してください。

4 *InstallDir*\idm\WEB-INF\lib ディレクトリから次の **JAR** ファイルを削除します。ただし、使用しているアプリケーションサーバーによっては、これらのファイルが **Identity Manager** 製品のインストール時に削除されていることもあります。

- jsse.jar
  - jcert.jar
  - jnet.jar
  - cryptix-jce-api.jar
  - cryptix-jce-provider.jar

5 java.security ファイルに、次の行を追加します (ファイルにない場合)。

```
security.provider.2=com.ibm.crypto.provider.IBMJCEsecurity.provider.3=
com.ibm.net.ssl.internal.ssl.Provider
```

各行の security.provider のあとに続く数字は、Java がセキュリティープロバイダクラスを参照する順序を指定するものです。これらの値が一意になるようにしてください。ユーザーの環境によってシーケンス番号はさまざまである可能性があります。java.security ファイル内にすでに複数のセキュリティープロバイダがある場合は、上記で指定された順序で新しいセキュリティープロバイダを挿入し、既存のセキュリティープロバイダの番号を付け直します。既存のセキュリティープロバイダを削除したり、プロバイダを重複させたりしないでください。

6 アプリケーションサーバーに **VM** パラメータを追加します。

```
-Djava.protocol.handler.pkgs=com.ibm.net.ssl.internal.www.protocol
```

必要に応じて、複数のパッケージを | (パイプ記号) で区切って追加できます。たとえば、次のようにします。

```
-Djava.protocol.handler.pkgs=sun.net.www.protocol| \  com.ibm.net.ssl.
  internal.www.protocol
```

7 **IBM Tivoli Access Manager Authorization Server** が設定済みで稼動していることを確認します。

8 `SvrSslCfg` コマンドを実行します。

たとえば、次のようにします。

```
java com.tivoli.pd.jcfg.SvrSslCfg -action config \
-admin_id sec_master -admin_pwd secpw \
-appsvr_id PDPermissionjapp -host amazn.myco.com \
-mod local -port 999 -policysvr ampolicy.myco.com:7135:1 \
-authzsvr amazn.myco.com:7136:1 -cfg_file c:/am/configfile \
-key_file c:/am/keystore -cfg_action create
```

`am` ディレクトリがあらかじめ存在している必要があります。正常に完了したら、次のファイルが `c: \am` ディレクトリに作成されます。

- `configfile`
- `keystore`

詳細については、『IBM Tivoli Access Manager Authorization Java Classes デベロッパーズ・リファレンス』および『IBM Tivoli Access Manager Administration Java Classes デベロッパーズ・リファレンス』を参照してください。

Web Access Control の設定

次の手順では、Tivoli Access Manager を Identity Manager の Web Access Control として使用する場合の、一般的な設定手順を説明します。この手順の一部では、Tivoli Access Manager ソフトウェアに関する詳細な知識が必要になります。

▼ Tivoli Access Manager を Web Access Control として設定する一般的な手順

1 **IBM Tivoli Access Manager Java Runtime Component** を **Identity Manager** サーバーにインストールして設定します。

2 **Identity Manager** サーバーで **JDK** セキュリティー設定を設定します。

3 **Identity Manager** サーバーで **Access Manager SSL Config** ファイルを作成します。

4 **Access Manager** 内に **Identity Manager** の **URL** に対するジャンクションを作成します。詳細については、**Tivoli Access Manager** の製品マニュアルを参照してください。

次の `pdadmin` コマンドの例は、ジャンクションの作成方法を示しています。

```
pdadmin server task WebSealServer create -t Connection
 / -p Port -h Server -c ListOfCredentials -r -i
 JunctionName
```

5 **WebSeal Proxy Server** 用に **Identity Manager Base HREF** プロパティーを設定します。

6 **Access Manager** リソースアダプタを設定します。

7 **Access Manager** ユーザーを **Identity Manager** に読み込みます。

8 **Identity Manager** の **Access Manager** に対するパススルー認証を設定します。

ユーザーが Access Manager を通して Identity Manager の URL にアクセスする際に、ユーザーのアイデンティティーが HTTP ヘッダーで Identity Manager に渡されます。Identity Manager は渡されたアイデンティティーを使用して、ユーザーが Access Manager と Identity Manager に存在することを確認します。ユーザーが Identity Manager 管理者インタフェースにアクセスしようとした場合は、Identity Manager のセキュリティー設定でユーザーに Identity Manager の管理特権があることが確認されます。エンドユーザーは Access Manager に対しても検証され、Identity Manager アカウントがあるかどうか確認されます。

Identity Manager のインストールに関する注意事項

注 – IBM Tivoli Access Manager を WebSphere アプリケーションサーバーとともにインストールする場合は、Identity Manager のインストール中に `jsse.jar`、`jcert.jar`、および `jnet.jar` ファイルを `WEB-INF\lib` ディレクトリにコピーしないでください。これらのファイルをコピーすると競合が発生します。

Access Manager リソースアダプタは、カスタムアダプタです。インストールプロセスを完了するには、次の手順を実行してください。

▼ Access Manager リソースアダプタをインストールする

1 `pd.jar` ファイルを、**Access Manager** のインストールメディアから `$WSHOME/WEB-INF/lib` ディレクトリにコピーします。

2 「管理するリソースの設定」ページの「カスタムリソース」セクションに次の値を追加します。

```
com.waveset.adapter.AccessManagerResourceAdapter
```

使用上の注意

ここでは、Access Manager リソースアダプタの使用に関連する依存関係と制限について示します。

このリソースで Identity Manager のシングルサインオンまたはパススルー認証機能を使用する場合は、Access Manager を Identity Manager プロキシサーバーとして使用してください。プロキシサーバーについては、『Identity Manager Deployment Guide』を参照してください。

GSO クレデンシャルの作成

Identity Manager の「ユーザーの作成」ページから、GSO Web リソースまたは GSO リソースグループのクレデンシャルを設定するには、次の手順を実行します。

▼ **GSO Web リソースまたは GSO リソースグループのクレデンシャルを設定する**

1. 「**GSO Web** クレデンシャルの追加」または「**GSO** リソースグループクレデンシャル」を選択します。
2. 該当する **GSO** クレデンシャルのドロップダウンメニューから、ターゲットを選択します。
3. リソースのユーザー **ID** とパスワードをテキストフィールドに入力します。
4. 該当するフィールドを編集することで、リソースクレデンシャルのユーザー **ID** またはパスワード、あるいはその両方を編集できます。セキュリティー上の理由により、クレデンシャルのパスワードを検出することはできません。

GSO クレデンシャルの削除

クレデンシャルを削除するには、削除対象のクレデンシャルをテーブルで選択して、対応する「削除」ボタンをクリックします。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は、SSL 経由の JNDI を使用して Access Manager と通信します。

必要な管理特権

管理ユーザーには、ユーザー、グループ、Web リソース、およびリソースグループを作成、更新、および削除するための特権が必要です。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	なし
パススルー認証	あり
前アクションと後アクション	なし
データ読み込みメソッド	リソースから直接インポート 調整

アカウント属性

属性	データ型	説明
firstname	String	必須。ユーザーの名。
lastname	String	必須。ユーザーの姓。
registryUID	String	必須。ユーザーレジストリに格納されているアカウント名。
description	String	ユーザーについて説明したテキスト。
groups	String	ユーザーがメンバーになっている Access Manager グループ。
noPwdPolicy	Boolean	パスワードポリシーを適用するかどうかを示します。
ssoUser	Boolean	ユーザーにシングルサインオン機能を持たせるかどうかを示します。
expirePassword	Boolean	パスワードが期限切れになるかどうかを示します。
importFromRgy	Boolean	ユーザーレジストリからグループデータをインポートするかどうかを示します。
deleteFromRgy	Boolean	ユーザーを削除するべきかどうかを示します。
syncGSOCreds	Boolean	GSO のパスワードを Access Manager のパスワードと同期させるかどうかを示します。

属性	データ型	説明
gsoWebCreds	String	ユーザーがアクセス権を持つ Web リソースクレデンシャルのリスト。
gsoGroupCreds	String	ユーザーがアクセス権を持つリソースグループクレデンシャルのリスト。

リソースオブジェクトの管理

Identity Manager は、次のオブジェクトをサポートします。

リソースオブジェクト	サポートされる機能	管理される属性
Group	作成、検索、削除、更新	name、description、registry name、member

アイデンティティーテンプレート

アカウント名の構文は次のとおりです。

```
$accountId$
```

サンプルフォーム

Identity Manager には、`AccessManagerUserForm.xml` サンプルフォームが用意されています。

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

```
com.waveset.adapter.AccessManagerResourceAdapter
```

◆ ◆ ◆ 第 47 章

Top Secret

Top Secret リソースアダプタは、TN3270 エミュレータセッションを使用して、OS/390 メインフレーム上のユーザーアカウントおよびメンバーシップの管理をサポートします。

アダプタの詳細

Top Secret リソースアダプタは、`com.waveset.adapter.TopSecretResourceAdapter` クラスで定義されます。

リソースを設定する際の注意事項

Top Secret Active Sync アダプタは、FTP を使用して TSSAUDIT 機能から出力を取得することにより動作します。その後、出力を解析して、アカウントの作成、変更、および削除を探します。この機能は、Top Secret Recovery ファイルのデータからレポートを生成します。そのため、Recovery ファイルを有効にし、Active Sync のポーリング間隔内に発生するすべての変更を十分保持できる大きさにします。Active Sync アダプタによる次のポーリングまでに出力が利用可能になるように TSSAUDIT ユーティリティーを実行するためのジョブをスケジュールするとよいでしょう。

オプションの世代データグループ (GDG) に TSSAUDIT の出力結果を格納するように設定できます。GDG には、前のバージョンの TSSAUDIT の出力が格納されます。Active Sync アダプタでは、通常の時間に実行できないイベントが失われないようにするために、GDG からの取得がサポートされています。このアダプタを、失われた可能性があるイベントを複数の世代に戻って取得するように設定できます。

次のサンプル JCL は、TSSAUDIT バッチジョブを実行します。

```
//LITHAUS7  <<<< Supply Valid Jobcard >>>>>>
//* ***************************************************************
//* *  THIS JOB RUNS THE TSS AUDIT PROGRAM 'CHANGES'
```

```
//* *    & CREATES A GDG MEMBER FOR IDENTITY MANAGER
//* *  You may choose to use standard MVS Delete/Defines or
//* *   request a system programmer to establish a small GDG
//* ***************************************************************
//AUDIT01  EXEC   PGM=TSSAUDIT,
//          PARM='CHANGES DATE(-01)'
//AUDITOUT DD DSN=auth hlq.LITHAUS.ADMIN.DAILY(+1),
//          DISP=(NEW,CATLG),UNIT=SYSDA,RECFM=FB,LRECL=133,
//          BLKSIZE=2793,SPACE=(CYL,(2,1),RLSE)
//RECOVERY DD   DSN=your.TSS.recovery.file ,DISP=SHR
//AUDITIN  DD DUMMY
```

Identity Manager のインストールに関する注意事項

Top Secret リソースアダプタは、カスタムアダプタです。インストールプロセスを完了するには、次の手順を実行する必要があります。

▼ Top Secret リソースアダプタをインストールする

1. **Top Secret** リソースを **Identity Manager** のリソースリストに追加するには、「管理するリソースの設定」ページの「カスタム リソース」セクションに次の値を追加する必要があります。

   ```
   com.waveset.adapter.TopSecretResourceAdapter
   ```

2. 適切な **JAR** ファイルを **Identity Manager** インストールの `WEB-INF/lib` ディレクトリにコピーします。

コネクションマネージャー	JAR ファイル
Host On Demand	IBM Host Access Class Library (HACL) は、メインフレームへの接続を管理します。HACL を含む推奨 JAR ファイルは habeans.jar です。これは、HOD に付属する HOD Toolkit (または Host Access Toolkit) とともにインストールされます。HACL のサポートされるバージョンは、HOD V7.0、V8.0、V9.0、および V10 に含まれるバージョンです。 habeans.jar ファイル ただし、このツールキットを利用できない場合は、HOD のインストールに含まれる次の JAR ファイルを habeans.jar の代わりに使用できます。 ■ habase.jar ■ hacp.jar ■ ha3270.jar ■ hassl.jar ■ hodbase.jar 詳細は、http://www.ibm.com/software/webservers/hostondemand/ (http://www.ibm.com/software/webservers/hostondemand/) を参照してください。
Attachmate WRQ	Sun 製品向け Attachmate 3270 メインフレームアダプタには、メインフレームへの接続の管理に必要なファイルが含まれます。 ■ RWebSDK.jar ■ wrqtls12.jar ■ profile.jaw この製品の入手については、Sun プロフェッショナルサービスにお問い合わせください。

3 Waveset.properties ファイルに次の定義を追加して、端末セッションを管理するサービスを定義します。

```
serverSettings.serverId.mainframeSessionType=Value
serverSettings.default.mainframeSessionType=Value
```

Value は、次のように設定できます。

- 1 は、IBM Host On-Demand (HOD) を表します。
- 3 は、Attachmate WRQ を表します。

これらのプロパティーを明示的に設定しない場合、Identity Manager は WRQ、HOD の順に使用を試みます。

4 **Attachmate** ライブラリが **WebSphere** または **WebLogic** アプリケーションサーバーにインストールされている場合は、`com.wrq.profile.dir=`*LibraryDirectory* プロパティーを `WebSphere/AppServer/configuration/config.ini` または `startWeblogic.sh` ファイルに追加します。

これにより、Attachmate コードでライセンスファイルを検索できます。

5 `Waveset.properties` ファイルに加えた変更を有効にするために、アプリケーションサーバーを再起動します。

6 リソースへの **SSL** 接続の設定については、第 **53** 章「メインフレーム接続」を参照してください。

使用上の注意

ここでは、Top Secret リソースアダプタの使用に関する情報を示します。 次の内容で構成されています。

管理者

TSO セッションでは、同時に複数の接続は許可されません。Identity Manager Top Secret 操作の同時実行を実現するには、複数の管理者を作成します。たとえば、2 人の管理者を作成すると、2 つの Identity Manager Top Secret 操作を同時に実行できます。少なくとも 2 人 (できれば 3 人) の管理者を作成するようにしてください。

CICS セッションでは、管理者あたりのセッション数は制限されませんが、必要に応じて複数の管理者を定義できます。

クラスタ環境で実行する場合、クラスタ内のサーバーごとに管理者を定義する必要があります。この定義は、CICS の場合と同様に、管理者が同一の場合も必要です。TSO では、クラスタ内のサーバーごとに異なる管理者が必要です。

クラスタリングを使用していない場合は、すべての行でサーバー名は Identity Manager のホストマシンの名前となります。

注 – ホストリソースアダプタは、同じホストに接続している複数のホストリソースでの親和性管理者に対して最大接続数を強制しません。代わりに、各ホストリソース内部の親和性管理者に対して最大接続数が強制されます。

同じシステムを管理する複数のホストリソースがあり、現在それらが同じ管理者アカウントを使用するように設定されている場合は、同じ管理者がリソースに対して同時に複数のアクションを実行しようとしていないことを確認するために、それらのリソースを更新しなければならない可能性があります。

リソースアクション

Top Secret アダプタには、login および logoff のリソースアクションが必要です。login アクションは、認証されたセッションに関してメインフレームとネゴシエーションを行います。logoff アクションは、そのセッションが不要になったときに接続を解除します。

login リソースアクションおよび logoff リソースアクションの作成については、565 ページの「メインフレームの例」を参照してください。

SSL 設定

Identity Manager は TN3270 接続を使用してリソースと通信します。

RACF LDAP リソースへの SSL 接続の設定については、第 53 章「メインフレーム接続」を参照してください。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	なし
パススルー認証	なし
前アクションと後アクション	あり
データ読み込みメソッド	■ リソースから直接インポート ■ 調整 ■ Active Sync

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は、TN3270 を使用して Top Secret アダプタと通信します。

必要な管理特権

管理者に次の特権を付与してください。

- TSS ADMIN 関数を通して、管理スコープ下で CREATE ACID を実行するための ACID (CREATE) 権限
- TSS ADMIN 関数を通して、リソース所有権をスコープ内の ACID に割り当てるための RESOURCE (OWN) 権限
- TSS ADMIN 関数を通して、多くのセキュリティー属性を割り当てるための MISC1、MISC2、および MISC9 権限

アカウント属性

次の表に、デフォルトの Top Secret アカウント属性に関する情報を示します。

アイデンティティーシステム属性名	リソース属性名	データ型	説明
Profiles	PROFILE	String	ユーザーに割り当てられたプロファイル。この属性には複数の値を設定できます。
accountId	ACID	String	必須。アカウント ID
fullname	NAME	String	ユーザーの姓名
Installation Data	INSTDATA	String	インストールデータ
TSOO Access	TSO_ACCESS	Boolean	ユーザーが TSO にアクセスできるかどうかを示します
TSOLPROC	TSO.TSOLPROC	String	TSO ログインプロシージャー
OMVS Access	OMVS_ACCESS	Boolean	ユーザーが OMVS にアクセスできるかどうかを示します
Groups	GROUP	String	ユーザーに割り当てられたグループのリスト

アイデンティティーシステム属性名	リソース属性名	データ型	説明
Default Group	DFLTGRP	String	ユーザーのデフォルトグループ
UID	OMVS.UID	String	OMVS ユーザー ID
OMVSPGM	OMVS.OMVSPGM	String	ユーザーの初期 OMVS プログラム
HOME	OMVS.HOME	String	ユーザーの OMVS ホームディレクトリ
Attributes	ATTRIBUTE	String	アカウント属性のリスト

次の表に、デフォルトではスキーママップに表示されない、サポート対象のアカウント属性を示します。これらの属性のデータの種類は String です。

リソース属性名	説明
CICS.OPTIME	CICS で端末ユーザーがタイムアウトになったとみなされるまでの時間を制御します。
CICS.OPID	CICS オペレータ ID を指定します。
DEPT	部署名を指定します。
DIV	部門名を指定します。
ZONE	ゾーン名を指定します。
FACILITY	ACID がアクセスできる機能またはアクセスできない機能のリストを指定します。
DATASET	ユーザーのデータセットのリストを指定します。
CORPID	企業 ID のリストを指定します。
OTRAN	所有可能なトランザクションのリストを指定します。
TSOACCT	TSO アカウント番号のリストを指定します。
SOURCE	関連付けられた ACID がシステムに入る場合に使用するソースリーダーまたは端末プレフィックスのリストを指定します。
TSO.TRBA	ブロードキャストデータセット内の、ユーザーのメールディレクトリエントリの相対ブロックアドレス (RBA) を指定します。
TSO.TSOCOMMAND	TSO ログオン時に発行されるデフォルトのコマンドを指定します。
TSO.TSODEFPRFG	デフォルトの TSO パフォーマンスグループを割り当てます。
TSO.TSODEST	TSO ユーザーに対して TSO が生成した JCL のデフォルトの出力先識別子を指定します。

リソース属性名	説明
TSO.TSOHCLASS	TSO ユーザーに対して TSO が生成した JCL のデフォルトの保持クラスを割り当てます。
TSO.TSOJCLASS	TSO ユーザーから TSO が生成したジョブカードのデフォルトのジョブクラスを割り当てます。
TSO.TSOLACCT	TSO ログオンで使用されるデフォルトのアカウント番号を指定します。
TSO.TSOLSIZE	TSO のデフォルトの領域サイズを K バイト単位で割り当てます。
TSO.TSOMCLASS	TSO ユーザーに対して TSO が生成した JCL のデフォルトのメッセージクラスを割り当てます。
TSO.TSOMSIZE	TSO ユーザーがログオン時に指定できる最大領域サイズを K バイト単位で定義します。
TSO.TSOOPT	TSO ユーザーがログオン時に指定できるデフォルトのオプションを割り当てます。
TSO.TSOSCLASS	TSO ユーザーに対して TSO が生成した JCL のデフォルトの SYSOUT クラスを割り当てます。
TSO.TSOUDATA	サイトで定義されたデータフィールドを TSO ユーザーに割り当てます。
TSO.TSOUNIT	TSO 下での動的割り当てに使用されるデフォルトの単位名を割り当てます。
TSO.TUPT	ユーザープロファイルテーブルの値を指定します。

ほかの Top Secret リソース属性のサポートの詳細については、サービス組織にお問い合わせください。

アイデンティティーテンプレート

```
$accountId$
```

サンプルフォーム

組み込みのフォーム

なし

その他の利用可能なフォーム

```
TopSecretUserForm.xml
```

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

- `com.waveset.adapter.HostAccess`
- `com.waveset.adapter.TopSecretResourceAdapter`

hostAccess オブジェクトは、Identity Manager でトレースされることもあります。デバッグページでトレースされるクラスは `com.waveset.adapter.HostAccess` です。メインフレームに送信されたキーストロークと待機メッセージを識別するにはトレースレベル 3 で十分です。トレースレベル 4 では、送信された正確なメッセージと、メインフレームからの応答が表示されます。

注 – トレースファイルの場所が有効であることを確認します。デフォルトでは、トレースファイルは *InstallDir*`/idm/config` の下のアプリケーションディレクトリに配置されます。アプリケーションが WAR から配備されている場合は、パスにディレクトリの絶対パスのハードコードが必要になることがあります。クラスタ環境では、トレースファイルをネットワーク共有に書き込むようにしてください。

ソースのトレースのほかに、キーストロークを送信する前の画面テキストを常にログに記録しておくことも役に立つ可能性があります。これは、ファイル書き込み側で実現できます。コマンドのシーケンスは次のとおりです。

▼ キーストロークの送信前に常に画面テキストをログに記録する

1 `var file = new java.io.File(”<filename>’);var writer = new java.io.BufferedWriter(new java.io.FileWriter(file));writer.write(hostAccess.getScreen());writer.flush();`

2 `hostAccess.sendKeysAndWait(<cmd>,<msg>);`

3 `writer.newLine();`

4 `writer.write(hostAccess.getScreen());`

5 `writer.flush();`

6 `writer.close();`

<filename> は、アプリケーションサーバーのローカルファイルシステム上のファイルの場所を参照するようにしてください。書き込み側は、`flush()` メソッドが呼び出されると、その場所へのハンドルを開いて、バッファーに格納されている内容を書き込みます。`close()` メソッドは、ファイルへのハンドルを解放します。`getScreen()`

メソッドをこの関数に渡すと、デバッグのために画面の内容のダンプを取得できます。このトレースは、画面が正しくナビゲートされて、ログイン/ログアウトが正常に実行されたら削除するようにしてください。

◆ ◆ ◆ 第 48 章

48 Windows NT

Windows NT リソースアダプタは、現在ゲートウェイでサポートされている Windows OS のバージョンでの、Windows ローカルアカウントの管理のみでサポートされます。

アダプタの詳細

Windows NT リソースアダプタは、`com.waveset.adapter.NTResourceAdapter` クラスで定義されます。

リソースを設定する際の注意事項

ここでは、双方向に信頼された複数のドメイン間での、Windows NT のプロビジョニングについて説明します。単一のドメインから複数のドメインを管理する場合は、次の制約が適用されます。

注 – この節では次の用語を使用します。

- ゲートウェイドメイン - ゲートウェイマシンが所属するドメイン。
- リソース管理アカウント - Identity Manager リソースで定義されている管理アカウント。
- サービスアカウント - ゲートウェイサービスを実行しているアカウント。

次の信頼関係を確立する必要があります。

- ゲートウェイドメインは、リソース管理アカウントが定義されている各ドメインを信頼する必要があります。

- ゲートウェイはリソース管理アカウントを使用してローカルにログインします。したがって、そのドメインはアカウントが存在するドメインを信頼する必要があります。
- ゲートウェイドメインは、パススルー認証を行う各ドメインを信頼する必要があります。
- ゲートウェイはローカルにログインしてユーザーアカウントを認証します。したがって、そのドメインはこれらのアカウントのドメインを信頼する必要があります。
- リソース管理アカウントは、アカウントの管理に使用する各ドメインの Account Operators グループのメンバーである必要があります。これらの各ドメインは、リソース管理アカウントを含むドメインを信頼する必要があります。
- アカウントのドメインがローカルグループのドメインに信頼されていなければ、アカウントをローカルグループに追加することはできません。
- サービスアカウントのドメインは、ゲートウェイドメインに信頼されている必要があります。

ゲートウェイサービスが開始されるときに、サービスアカウントのローカルログインが行われます。リソース管理アカウントのいずれかがサービスアカウントと異なる場合、またはドメインのいずれかでパススルー認証を実行する場合、サービスアカウントには、ゲートウェイドメインに「Act As Operating System」と「走査チェックのバイパス」のユーザー権限が必要です。これらの権限は、サービスアカウントで別のユーザーとしてログインするために必要です。

ホームディレクトリを作成する場合は、ディレクトリを作成するファイルシステム上で、リソース管理アカウントがディレクトリを作成できる必要があります。ホームディレクトリをネットワークドライブに作成する場合、リソース管理アカウントには、ゲートウェイプロセスの Temp または TMP 環境変数で定義されたファイルシステムか、これらの変数が定義されていない場合はゲートウェイプロセスの作業ディレクトリ (WINNT または WINNT\system32) に対して、書き込みアクセスが必要です。

前アクション、後アクション、またはリソースアクションを実行する場合、リソース管理アカウントには、ゲートウェイプロセスの TEMP または TMP 環境変数で定義されたファイルシステムか、これらの変数が定義されていない場合はゲートウェイプロセスの作業ディレクトリ (WINNT または WINNT\system32) に対して、読み取りと書き込みアクセスが必要です。

ゲートウェイはスクリプトとスクリプトの出力を、これらのディレクトリのいずれかに書き込みます。ディレクトリは記載されている順に選択されます。

ドメインごとに個別のリソースアダプタを設定します。同じゲートウェイホストを使用できます。

各ユーザーのドメイン固有のリソース属性 (ドメインと、場合によっては管理者とパスワード) をオーバーライドすることにより、単一のリソースを使用して複数のドメインを管理することもできます。

注 –

- ドメインはそのドメイン自身を信頼するため、2 つのドメインが実際には同じである場合、一部の信頼関係は明示的にする必要がありません。
- すべての管理対象ドメインのリソース管理アカウントに、同じアカウントを使用することができます。また、適切な信頼関係、グループメンバーシップ、およびユーザー権限を設定すれば、サービスアカウントにも同じアカウントを使用できます。

Identity Manager のインストールに関する注意事項

Windows NT アダプタに必要な追加のインストール手順はありません。

使用上の注意

スクリプトゲートウェイでは、RA_HANGTIMEOUT リソース属性を使用してタイムアウト値を秒単位で指定できます。この属性は、ゲートウェイに対する要求がタイムアウトしてハングしているとみなされるまでの時間を制御します。次のように、この属性を Resource オブジェクトに手動で追加する必要があります。

この属性のデフォルト値は 0 です。これは Identity Manager がハングした接続を確認しないことを示します。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の要件について説明します。

サポートされる接続

Identity Manager は、Sun Identity Manager Gateway を使用してこのアダプタと通信します。

必要な管理特権

管理者には、リソース上のユーザーとグループを作成および保守する権限が必要です。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	あり
パススルー認証	あり
前アクションと後アクション	あり
データ読み込みメソッド	■ リソースからインポート ■ 調整

Windows 2003 が Windows 2000 モードで動作している場合に、Active Directory のパススルー認証をサポートするには、次の管理特権が必要です。

- ゲートウェイをユーザーとして実行するように設定する場合、Windows NT および Windows 2000/Active Directory リソースでパススルー認証を実行するには、このユーザーに「Act As Operating System」のユーザー権限が必要です。ユーザーには、「走査チェックのバイパス」ユーザー権限も必要ですが、この権限はデフォルトですべてのユーザーで有効になっています。
- 認証されるアカウントには、ゲートウェイシステム上で「ネットワーク経由でコンピュータへアクセス」ユーザー権限が必要です。
- Identity Manager がユーザーの権限を更新するときに、セキュリティーポリシーが伝播されるまでに時間がかかる場合があります。ポリシーが伝達されたら、ゲートウェイを再起動します。
- アカウント認証を実行する場合は、LOGON32_LOGON_NETWORK ログオンタイプと LOGON32_PROVIDER_DEFAULT ログオンプロバイダを指定して、LogonUser 関数を使用します。LogonUser 関数は、Microsoft Platform Software Development Kit で提供されています。

アカウント属性

次の表に、Windows NT アカウント属性に関する情報を示します。

リソースユーザー属性	タブ/NT フィールド	属性タイプ
AccountLocked	全般/アカウントのロックアウト	Boolean

リソースユーザー属性	タブ/NT フィールド	属性タイプ
description	全般/説明	String
fullname	全般/フルネーム	String
groups	所属するグループ/所属するグループ	String
HomeDirDrive	Profile Connect	String
HomeDirectory	プロファイル/ローカルパス	String
LoginScript	プロファイル/ログオンスクリプト	String
PasswordNeverExpires	全般/パスワードを無期限にする	Boolean
Profile	プロファイル/プロファイルパス	String
userPassword	Password	暗号化されています
WS_PasswordExpired	全般/ユーザーは次回ログオン時にパスワードの変更が必要	Boolean
PasswordAge	デフォルトでは表示されません。最後にパスワードを変更してからの時間を示します。実装するには、java.util.Date クラスを使用して値を人間が読める形式に変換します。	Int

リソースオブジェクトの管理

Identity Manager は次のオブジェクトをサポートします。

リソースオブジェクト	サポートされる機能	管理される属性
Group	作成、更新、削除	description、member

アイデンティティーテンプレート

$accountId$

サンプルフォーム

組み込みのフォーム

Windows NT Create Group Form

Windows NT Update Group Form

その他の利用可能なフォーム

NTForm.xml

トラブルシューティング

Identity Manager のデバッグページを使用して、次のクラスでトレースオプションを設定します。

com.waveset.adapter.NTResourceAdapter

◆ ◆ ◆ 第 49 章

AttrParse オブジェクトの実装

AttrParse オブジェクトは、ユーザーリストの解析に使用される文法をカプセル化します。これは主に、一度に 1 画面分のデータを受け取って、目的の解析結果を出力する必要がある、メインフレームベースのリソースアダプタで使用されます。この技術はスクリーンスクレーピングとも呼ばれます。シェルスクリプトアダプタとスクリプトゲートウェイアダプタでも、getUser アクションと getAllUsers アクションで AttrParse が使用されます。

AttrParse オブジェクトを使用するアダプタでは、画面が Java 文字列としてモデル化されます。AttrParse オブジェクトのインスタンス化には、1 つ以上のトークンが含まれます。各トークンによって画面の各部分が定義されます。これらのトークンは、画面の文字列をトークン化して、アダプタがユーザーリストからユーザープロパティーを検索できるようにするために使用されます。

ユーザーリストの解析後、AttrParse からユーザー属性名と値のペアのマップが返されます。

設定

AttrParse オブジェクトは、ほかのすべての Identity Manager オブジェクトと同じように、持続的記憶領域の XML に直列化されます。そのため、AttrParse オブジェクトを、顧客の環境の相違をサポートするように設定できます。たとえば、ACF2 メインフレームのセキュリティーシステムは、多くの場合、追加のフィールドやフィールド長を含むようにカスタマイズされます。AttrParse オブジェクトはリポジトリにあるため、それらの相違に対応するための変更や設定が可能であり、カスタムアダプタを作成する必要がありません。

すべての Identity Manager 設定オブジェクトと同じように、変更するオブジェクトをコピーして名前を変更してから、変更するようにしてください。

▼ AttrParse オブジェクトを編集する

1 デバッグページで、「**List Objects**」ボタンの横にあるドロップダウンメニューから「**AttrParse**」を選択します。「**List Objects**」をクリックします。

2 利用可能なオブジェクトのリストから、編集するオブジェクトを選択します。

3 任意の **XML** エディタで、そのオブジェクトのコピー、編集、および名前の変更を行います。

4 「設定」ページで、「交換ファイルのインポート」を選択し、新しいファイルを **Identity Manager** にインポートします。

5 リソースで、その **AttrParse** リソース属性の名前を新しい **AttrParse** 文字列の名前に変更します。

Identity Manager に用意されている AttrParse オブジェクトの例については、`sample\attrparse.xml` ファイルを参照してください。このファイルには、スクリーンスクレーピングアダプタで使用されるデフォルトの AttrParse オブジェクトのリストが記載されています。

AttrParse 要素とトークン

AttrParse 要素

AttrParse 要素は、AttrParse オブジェクトを定義します。

属性

属性	説明
`name`	AttrParse オブジェクトを一意に定義します。この値は、アダプタの「リソースパラメータ」ページで指定されます。

データ

ユーザーリストを解析する 1 つ以上のトークン。AttrParse オブジェクトでサポートされるトークンは次のとおりです。

- 540 ページの「collectCsvHeader トークン」
- 541 ページの「collectCsvLines トークン」
- 541 ページの「eol トークン」

例

次の例では、行の最初の 19 文字を読み取り、余分な空白を削除し、値としてのその文字列を USERID リソース属性に代入します。次に、5 つの空白文字をスキップし、NAME リソース属性を抽出します。この属性は最大 21 文字で、空白は削除されます。サンプルでは、「Phone number:」の文字列をチェックしています。電話番号が解析され、PHONE リソース属性に割り当てられます。電話番号は、「Phone number:」の末尾の空白文字のあとから始まり、次に現れる空白文字で終わります。末尾の空白文字は削除されます。

```
<AttrParse name='Example AttrParse'>
   <str name='USERID' trim='true' len='19'/>
   <skip len='5'/>
   <str name='NAME' trim='true' len='21'/>
   <t offset='-1'>Phone number: </t>
   <str name='PHONE' trim='true' term=' '/>
</AttrParse>
```

次の文字列は、このサンプル AttrParse の文法に適合します。・記号は空白文字を表しています。

```
gwashington123•••••ABCD•George•Washington••••Phone•number:•123-1234•
alincoln••••••••••XYZ••Abraham•Lincoln••••••Phone•number:•321-4321•
```

1 番目の場合、解析後のユーザー属性マップには、次の内容が含まれます。

```
USERID="gwashington123", NAME="George Washington", PHONE="123-1234"
```

同様に、2 番目のユーザー属性マップには次の内容が含まれます。

```
USERID="alincoln", NAME="Abraham Lincoln", PHONE="321-4321"
```

テキストの残りの部分は無視されます。

collectCsvHeader トークン

collectCsvHeader トークンは、コンマ区切り (CSV) ファイルのヘッダーとして指定された行を読み取ります。

スクリプトゲートウェイアダプタとシェルスクリプトアダプタは、このトークンを使用します。collectCsvHeader および collectCsvLines トークンは、スクリプトゲートウェイアダプタが使用する唯一のトークンです。

ヘッダー内の各名前は、リソースアダプタのスキーママップのリソースユーザー属性と同じ名前にします。ヘッダー内の文字列がリソースユーザー属性名と一致しない場合、後続データ行内の対応する位置にある名前と値は無視されます。

属性

属性	説明
idHeader	アカウント ID とみなすヘッダーの値を指定します。この属性は省略可能ですが、指定することをお勧めします。指定されていない場合は、nameHeader 属性の値が使用されます。
nameHeader	ヘッダー内でアカウントの名前とみなす値を指定します。多くの場合、これは idHeader と同じ値です。 指定されていない場合は、idHeader の値が使用されます。この属性は省略可能ですが、指定することをお勧めします。
delim	省略可能です。ヘッダー内の値を区切る文字列。デフォルト値は,(コンマ) です。
minCount	ヘッダーが有効であるためには、delim 属性で指定した文字列が少なくともいくつヘッダーに存在しなければならないかを指定します。
trim	省略可能です。true に設定されている場合、値の始めや終わりに空白があれば、それらの空白を削除します。デフォルトは false です。
unQuote	省略可能です。true に設定されている場合、値が引用符で囲まれていれば、引用符を削除します。デフォルトは false です。

データ

なし

例

次の例は、accountId をアカウント ID として使用する値に指定してします。空白および引用符は値から削除されます。

```
<collectCsvHeader idHeader='accountId' delim=',' trim='true' unQuote='true'/>
```

collectCsvLines トークン

collectCvsLines トークンは、コンマ区切り (CSV) ファイルの行を解析します。このトークンの前に collectCvsHeader トークンを呼び出しておきます。

スクリプトゲートウェイアダプタとシェルスクリプトアダプタは、このトークンを使用します。collectCsvHeader および collectCsvLines トークンは、スクリプトゲートウェイアダプタが使用する唯一のトークンです。

属性

次の属性のいずれかが指定されていない場合、その値は、前に発行された collectCsvHeader トークンから継承されます。

属性	説明
idHeader	アカウント ID とみなす値を指定します。
nameHeader	アカウントの名前とみなす値を指定します。
delim	省略可能です。ヘッダー内の値を区切る文字列。デフォルト値は , (コンマ) です。
trim	省略可能です。true に設定されている場合、値の始めや終わりに空白があれば、それらの空白を削除します。デフォルトは false です。
unQuote	省略可能です。true に設定されている場合、値が引用符で囲まれていれば、引用符を削除します。デフォルトは false です。

データ

なし

例

次の例は、値から空白と引用符を削除します。

```
<collectCsvLines trim='yes' unQuote='yes'/>
```

eol トークン

eol トークンは、行末文字 (\n) に一致します。解析位置は、次の行の最初の文字に進められます。

属性

なし

データ

なし

例

次のトークンは行末文字に一致します。

```
<eol/>
```

flag トークン

flag トークンは、多くの場合、アカウントプロパティーを定義するフラグがユーザーアカウントに存在するかどうかを判定するために、opt トークン内で使用されます。このトークンは、指定された文字列を検索します。そのテキストが見つかると、AttrParse は boolean 型の true を属性に代入し、そのエントリを属性マップに追加します。

解析位置は、一致したテキストのあとの最初の文字に進められます。

属性

属性	説明
name	属性値マップで使用する属性の名前。この名前は、通常はリソースアダプタのスキーママップ上のリソースユーザー属性と同じですが、これは必要条件ではありません。
offset	トークンのテキストを検索する前にスキップする文字数。offset には次の値を指定できます。 ■ 1 またはそれ以上の値を指定すると、指定された数の文字を移動してから、トークンのテキストを検索します。 ■ 0 を指定すると、現在の解析位置でテキストを検索します。これはデフォルト値です。 ■ -1 を指定すると、現在の解析位置でトークンのテキストを検索しますが、termToken 属性が存在する場合、解析位置は termToken 属性で指定された文字列までになります。

属性	説明
termToken	検索対象のテキストが存在しないことを示すインジケータとして使用する文字列。この文字列は、多くの場合、画面出力上の次の行の最初の単語またはラベルです。 解析位置は、termToken 文字列のあとの文字になります。 termToken 属性は、len 属性が負の値 (-1) の場合にのみ使用できます。

データ

検索するテキスト。

例

▼ flag トークンの例

1 次のトークンは、現在の解析位置で AUDIT を検索し、見つかった場合は、ユーザー属性マップに AUDIT_FLAG=true を追加します。

```
<flag offset='-1' name='AUDIT'>AUDIT_FLAG</flag>
```

2 次のトークンは、現在の解析位置で *xxxx*CICS を検索します。*xxxx* は、空白文字を含む任意の 4 文字です。この文字列が見つかった場合、**AttrParse** は CICS=true をユーザー属性マップに追加します。

```
<flag offset='4' name='CICS'>CICS</flag>
```

int トークン

int トークンは、整数型のアカウント属性をキャプチャーします。属性名と整数値がアカウント属性マップに追加されます。解析位置は、その整数のあとの最初の文字に進められます。

属性

属性	説明
name	属性値マップで使用する属性の名前。この名前は、通常はリソースアダプタのスキーママップ上のリソースユーザー属性と同じですが、これは必要条件ではありません。

属性	説明
len	求める整数の正確な長さを示します。長さには次の値を指定できます。 ■ 1 またはそれ以上を指定すると、指定された数の文字をキャプチャーして、そのテキストが整数値であるかどうか、または noval 属性で指定された文字と一致するかどうかを調べます。 ■ -1 を指定すると、次の文字が noval 属性と等しくないかぎり、現在の解析位置から始まるもっとも長い文字列を使用して解析します。これはデフォルト値です。
noval	省略可能です。属性が整数値を持っていないことを示す画面上のラベル。基本的には、これは null 値のインジケータです。解析位置は、noval 文字列のあとの最初の文字に進められます。

データ

なし

例

▼ int トークンの例

1 次のトークンは、6 桁の整数を検索し、その桁数の整数値を SALARY 属性の属性値マップに追加します。

```
<int name='SALARY' len='6'/>
```

値 010250 が見つかった場合、AttrParse は SALARY=10250 を値マップに追加します。

2 次のトークンは、任意の桁数を検索し、その整数値を AGE 属性の属性マップに追加します。

```
<int name='AGE' len='-1' noval='NOT GIVEN'/>
```

たとえば、値 34 が見つかった場合、AGE=34 が属性マップに追加されます。NOT GIVEN という文字列の場合、値は AGE属性の属性マップに追加されません。

loop トークン

loop トークンは、トークンに含まれている要素を、入力がなくなるまで繰り返し実行します。

属性

なし

データ

一様ではありません。

例

次の例は、CSV ファイルの内容を読み取ります。

```
<loop>
   <skipLinesUntil token=',' minCount='4' />
   <collectCsvHeader idHeader='accountId' />
   <collectCvsLines />
</loop>
```

multiLine トークン

multiLine トークンは、複数の行で繰り返すパターンに一致します。次の行が multiLine の内部 AttrParse 文字列に一致する場合、解析後の出力はアカウント属性マップの最上位に追加されます。解析位置は、内部 AttrParse 文字列と一致しない最初の行に進められます。

属性

属性	説明
opt	内部 AttrParse 文字列が省略可能である可能性があることを示します。 内部 AttrParse 文字列に一致する行がない可能性があることと、次のトークンによる解析を続行することを示します。

データ

データ行を解析する任意の AttrParse トークン。

例

次の multiLine トークンは、GROUPS[space][space][space]= タグと、空白文字で区切られたグループリストが含まれている複数のグループ行を検索します。

```
<multiLine opt='true'>
   <t>GROUPS[space][space][space]=</t>
   <str name='GROUP' multi='true' delim=' ' trim='true'/>
   <skipToEol/>
</multiLine>
```

次の文字列が入力として読み取られた場合、AttrParse は GROUPS = {Group1,Group2,Group3,Group4} をアカウント属性マップに追加します。

```
GROUPS[space][space][space]= Group1[space]Group2\n
GROUPS[space][space][space]= Group3[space]Group4\n
Unrelated text...
```

opt トークン

opt トークンは、複数のトークンで構成される文字など、任意の複雑な文字列を解析します。検索トークンが存在する場合、内部 AttrParse 文字列を使用して画面の次の部分を解析します。任意セクションが存在する場合、解析位置は、任意セクションの末尾のあとの文字に進められます。それ以外の場合は、解析位置は変更されません。

属性

なし

データ

apMatch トークンと、それに続く AttrParse トークンで構成されます。

apMatch。オプションのセクションがあるかどうかを判定するためのトークンを含みます。apMatch は、opt トークン内だけで使用できるサブトークンです。apMatch トークンには、常にサブトークンとして flag トークンが含まれます。

AttrParse。画面の任意部分の解析方法を指定します。このバージョンの AttrParse 要素では、name 引数を使用しません。それ以外のすべてのトークンを含めることができます。

例

次の opt トークンは、CONSNAME= テキストトークンへの一致を探します。見つかった場合は、長さが 8 の文字列を解析して、空白を削除し、その文字列を NETVIEW.CONSNAME 属性のアカウント属性マップに追加します。

```
<opt>
   <apMatch>
      <t offset='-1'> CONSNAME= </t>
   </apMatch>
   <AttrParse>
      <str name='NETVIEW.CONSNAME' len='8' trim='true' />
   </AttrParse>
</opt>
```

skip トークン

skip トークンは、スキップできる画面領域や、解析するユーザーに関する有用な情報が含まれていない画面領域をトークン化します。解析位置は、スキップされた文字のあとの最初の文字に進められます。

属性

属性	説明
len	画面上でスキップする文字数を示します。

データ

なし

例

次の例では、最初のトークンは 17文字をスキップし、2 番目のトークンは 1 文字だけスキップします。

```
<skip len='17'/>
<skip len='1'/>
```

skipLinesUntil トークン

skipLinesUntil トークンは、指定した文字列が minCount で指定した数以上見つかるまで、入力行をスキップします。

属性

属性	説明
token	検索する文字列。
minCount	必須の token 属性で指定された文字列のインスタンスの最小数。

データ

なし

例

次のトークンは、2 つのコンマが含まれている行の次の行まで前方にスキップします。解析位置は、その行の最初の文字になります。

```
<skipLinesUntil token=',' minCount='2'/>
```

skipToEol トークン

skipToEol トークンは、現在の解析位置から行の終わりまでのすべての文字をスキップします。解析位置は、次の行の最初の文字に進められます。

属性

なし

データ

なし

例

次のトークンは、現在の行の終わりまですべての文字をスキップします。解析位置は、次の行の最初の文字になります。

```
<skipToEol/>
```

skipWhitespace トークン

skipWhitespace トークンは、空白文字をスキップするために使用します。システムは、Java の空白文字の定義を使用します。解析位置は、空白以外の最初の文字に進められます。

属性

なし

データ

なし

例

次のトークンは、現在の解析位置ですべての空白をスキップします。

```
<skipWhitespace/>
```

str トークン

str トークンは、文字列のアカウント属性をキャプチャーします。属性名と文字列値がアカウント属性マップに追加されます。解析位置は、その文字列のあとの最初の文字に進められます。

属性

属性	説明
name	属性値マップで使用する属性の名前。この名前は、通常はリソースアダプタのスキーママップ上のリソースユーザー属性と同じですが、これは必要条件ではありません。
len	求める文字列の正確な長さを示します。長さには次の値を指定できます。 ■ 1 またはそれ以上を指定すると、文字が noval 属性と等しくないかぎり、指定された数の文字がキャプチャーされます。 ■ -1 を指定すると、次の文字が noval 属性と等しくないかぎり、現在の解析位置から次の空白文字までのすべての文字がキャプチャーされます。これは、デフォルトです。
term	文字列を解析していて、この属性で指定した値と一致する文字をキャプチャーしたら、この str トークンの解析を停止します。len 引数が 1 またはそれ以上の場合、str トークンは、長さ len に達するかまたは term 文字をキャプチャーするか、いずれか早い方の時点で終了します。
termToken	検索対象のテキストが存在しないことを示すインジケータとして使用する文字列。この文字列は、多くの場合、画面出力上の次の行の最初の単語またはラベルです。 解析位置は、termToken 文字列のあとの文字になります。属性マップに追加される文字列は、termToken が見つかるまでのすべての文字になります。 termToken 属性は、len 属性が負の値 (-1) の場合にのみ使用できます。
trim	省略可能です。アカウント属性マップに追加する前に、戻り値または複数値 (multi 属性が指定されている場合) から空白を削除するかどうかを示す true または false の値。デフォルト値は false です。
noval	属性が文字列値を持っていないことを示す画面上のラベル。基本的には、これは null 値のインジケータです。解析位置は、noval 文字列のあとの最初の文字に進められます。
multiLine	文字列が画面の複数行にまたかるかどうかを示す true または false の値。 この属性は、len 属性が存在し、0 より大きい値が指定されている場合にのみ使用できます。multiLine が存在する場合、len 属性に指定された文字数が解析されるまで、行末文字はスキップされます。

属性	説明
multi	得られた文字列が、さらに解析して各サブ値を検索する必要がある複数値属性であるかどうかを示す true または false の値。複数値は、appendSeparator を使用してまとめて追加するか、または値のリストに変換することができます。
delim	複数値文字列を解析するための区切り文字。この属性は、multi 属性が指定されている場合にのみ使用できます。 これが指定されていない場合、複数値の str トークンは空白文字で区切られているとみなされます。
append	appendSeparator を使用して複数値をまとめて文字列に追加するかどうかを示す true または false の値。append が存在しない場合、複数値はアカウント属性値マップのリストに追加されます。この属性は、multi 属性と一緒に使用されます。
appendSeparator	append トークンの複数値を区切る文字列を示します。この属性は、append 属性が true に設定されている場合にのみ有効です。appendSeparator が存在しない場合、append 属性は区切り文字を使用しません。代わりに、複数値を連結して結果の文字列にします。

データ

なし

例

- 次のトークンは、長さが 21 文字の文字列を検索し、前後の空白を削除します。

  <str name='NAME' trim='true' len='21'/>

  [space][space]George Washington[space][space] という文字列の場合、AttrParse は NAME="George Washington" をアカウント属性マップに追加します。
- 次のトークンは、長さが 21 文字の文字列を検索し、前後の空白を削除します。

  <str name='NAME' trim='true' len='21'/>

  [space][space]George Washington[space][space] という文字列の場合、AttrParse は NAME="George Washington" をアカウント属性マップに追加します。
- 次のトークンは、) (右括弧) で終わる任意の長さの文字列を検索します。

  <str name='STATISTICS.SEC-VIO' term=')' />

  2– Monday, Wednesday -)text という文字列の場合、AttrParse は STATISTICS.SEC-VIO="2– Monday, Wednesday - " をアカウント属性マップに追加します。
- 次のトークンは、現在の解析位置から現在の行の終わりまで、空白文字で区切られた単語のリストを検索します。

  <str name='GROUP' multi='true' delim=' ' trim='true'/>

`Group1 Group2 newGroup lastGroup\n` という文字列があった場合、AttrParse はグループ名文字列のリスト {`Group1`, `Group2`, `newGroup`, `lastGroup`} を GROUP 属性のアカウント属性マップに追加します。

- 次のトークンも、同じような機能を果たしますが、アカウント属性マップが、次のようにコロン (:) で連結される点が前の例と異なります。

  `GROUP={Group1:Group2:newGroup:lastGroup}`

  <str name='GROUP' multi='true' delim=' ' trim='true' append='true' appendSeperator=':' />

t トークン

t トークンは、テキストをトークン化するために使用します。通常は、スクリーンスクレーピング中にラベルを認識し、解析している画面上の場所に関する知識を提供するために使用されます。解析位置は、一致したテキストのあとの最初の文字に進められます。構文解析部は常に、テキスト行内の左から右に進行します。

属性

属性	説明
`offset`	トークンのテキストを検索する前にスキップする文字数。offset には次の値を指定できます。 ■ 1 またはそれ以上の値を指定すると、指定された数の文字を移動してから、トークンのテキストを検索します。 ■ 0 を指定すると、現在の解析位置でテキストを検索します。これはデフォルト値です。 ■ -1 を指定すると、現在の解析位置でトークンのテキストを検索しますが、termToken 属性が存在する場合、解析位置は termToken 属性で指定された文字列までになります。
`termToken`	このトークンの解析を停止することを示す文字列。解析位置は、termToken 文字列のあとの文字になります。 termToken 属性は、offset 属性が負の値 (-1) の場合にのみ使用できます。

データ

検索するテキスト

例

- 次のトークンは、現在の解析位置で `Address Line 1:[space]` を検索します。

  <t offset='-1'>Address Line 1: </t>

- 次のトークンは、現在の解析位置で *xx*`Zip Code:[space]` を検索します。*xx* は、空白文字を含む任意の 2 文字です。

  <t offset='2'>Zip Code: </t>

- 次のトークンは、現在の解析位置で `Phone:[space]` を検索します。AttrParse は、`Employee ID` という文字列を最初に見つけると、エラーを生成します。

  <t offset='-1' termToken='Employee ID'>Phone: </t>

◆ ◆ ◆ 第 50 章

リソースへのアクションの追加

この章では、リソースアダプタのアクションを作成および実装する方法について説明します。アダプタがアクションをサポートしているかどうかについては、各アダプタのマニュアルを参照してください。

アクションとは

アクションとは、スクリプトアクションのネイティブサポートが存在する場合に、管理するリソースのコンテキスト内で実行するスクリプトです。たとえば、UNIX オペレーティングシステムによるシステムでは、アクションは一連の UNIX シェルコマンドです。Microsoft Windows 環境では、アクションは CMD コンソール内で実行可能な DOS 形式のコンソールコマンドになります。アクションは Identity Manager リポジトリ内にオブジェクトして存在します。メインフレーム環境では、アクションは、メインフレームとの間でキーストロークやコマンドを送受信できる Javascript スクリプトです。Oracle ERP では、アクションは、JDBC 接続を使用して Oracle データベースの追加カスタムフィールドを管理する Javascript または Beanshell スクリプトです。このアダプタについては、第 25 章「Oracle ERP」を参照してください。

アクションは、リソースアカウントオブジェクトに対して直接実行される作業ではなく、そのリソースアカウントの作成、更新、または削除の前またはあとに実行される作業を行う場合に使用します。リソースアクションでは、ユーザーを作成したあとに実行される、新規ユーザーのディレクトリへのファイルのコピーや、そのユーザーに関する UNIX の SUDOers ファイルの更新などのネイティブアクティビティーがサポートされます。このタイプの作業は、カスタムリソースアダプタを使用することにより実行できます。ただし、カスタムリソースアダプタを配備するよりも、アクションを追加したリソースアダプタを配備するほうが簡単です。

アクションには次の 3 種類の結果メッセージが関連付けられます。

- **Success**。Identity Manager の成功メッセージを表示します。

- **Success with action output**。Identity Manager の成功メッセージと、標準エラーおよび出力情報を表示します。
- **Failure**。Identity Manager の失敗メッセージと、標準エラーおよび出力情報を表示します。

サポートされるプロセス

次のプロセスは前アクションと後アクションをサポートします。

- create
- update
- delete
- enable
- disable
- login と logoff (メインフレームアダプタのみ)

アクションの定義

アクションは、次の構造を持っています。

```
<ResourceAction name='Name'>
    <ResTypeAction restype='ResourceType' actionType='Language' timeout='Milliseconds'>
       <act>
       ...
       </act>
    </ResTypeAction>
 </ResourceAction>
```

各表記の意味は次のとおりです。

- *Name* は、リソースアクションの名前です。
- *ResourceType* は、リソースのタイプ (AIX、HP-UX など) です。
- *Milliseconds* (省略可能) は、アクションの完了を待つ時間です。
- *Language* (省略可能) は、スクリプトの言語です。このパラメータは、Oracle ERP アダプタで必要です。Oracle ERP アダプタは、`Javascript` および `Beanshell` の `actionType` 値をサポートしています。

`<act>` 要素はアクションを定義します。この要素には、リソース上で実行されるコードが含まれます。たとえば、次の XML は Solaris リソースのアクションを定義しています。

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE Waveset PUBLIC 'waveset.dtd' 'waveset.dtd'>
<Waveset>
```

```
    <ResourceAction name='after-create'>
       <ResTypeAction restype='Solaris' timeout='60000'>
          <act>
          #!/bin/ksh
          echo "$WSUSER_accountId says Hello World!"
          # exit $DISPLAY_INFO_CODE if there is not a failure, but you want
          # the output to be propagated to the UI
          #exit 0
          exit $DISPLAY_INFO_CODE
          </act>
       </ResTypeAction>
    </ResourceAction>
</Waveset>
```

注 – <act> 要素内に含まれるコードは、UNIX スクリプト (ksh または sh) や Windows バッチスクリプトで使用されるコードと同じです。

環境変数の使用

環境変数はエクスポートされ、アクションで利用できるようになります。これらの環境変数は、ユーザーに関する値 (リソーススキーママップの「アイデンティティーシステム リソース属性」列で定義される) を持つ、スキーマにマップされたすべての属性を、先頭に WSUSER_ を付加して構成します。たとえば、前述の例では、Solaris リソーススキーママップで定義された AccountId 属性の先頭に WSUSER_ を付加した形式の、環境変数 WSUSER_AccountId が使用されています。これらの変数がそれぞれのシェル内で環境変数として認識されるように、Solaris では変数名の前に $ (ドル記号) が付加されます。

OS/400 はコマンド言語に変数の代入機能がないため、リソースアダプタは変数名を検索し、リソースにコマンド行を送信する前に代入を実行します。変数を認識させるために、変数の前後に $ を付加する必要があります。特に、OS/400 スクリプトで WSUSER_AccountId を使用するには、コマンド行に $accountId$ を入力します。「WSUSER」を削除することに注意してください。

使用例:

```
<ResTypeAction restype="OS/400" timeout="6000">
<act>
CRTOUTQ OUTQ(SYSTEME/$accountId$)
</act>
</ResTypeAction>
```

後アクションの実装

Identity Manager は更新の際に、変更された属性だけをリソースにプッシュします。アクションは変更されていない属性にアクセスできません。変更されていない可能性のある属性が必要な後アクションを記述する場合は、次の回避方法を検討してください。

▼ 変更されていない属性にアクセスする

1. リソースのスキーママップに、アクセスする必要のあるアカウント属性を模倣する余分な属性を追加します。たとえば、`fullname` アカウント属性にアクセスする必要がある場合は、`shadow_fullname` という名前の属性を作成します。スキーママップの「リソースユーザー属性」列で、この新しい属性に `IGNORE_ATTR` の値を追加して、アダプタが属性を使用するのを防ぎます。

2. この属性に入力されるように、値をユーザーフォームに設定します。

```
<Field name='accounts[ResourceName].shadow_fullname'>
    <Expansion>
       <ref>accounts[ResourceName].fullname</ref>
    </Expansion>
 </Field>
```

3. アクション内で `%WSUSER_shadow_fullname%` を参照して、値を取得できるようにします。

   Identity Manager は、`IGNORE_ATTR` に設定されている属性を取得しません。その結果、Identity Manager は `shadow_fullname` などの属性の内容を新しい値と見なします。この属性は常にアダプタにプッシュされ、後アクションに使用できます。

アクションファイルの作成

アクションファイルを作成するときは、次に示す事項に留意してください。

- スキーママップの Identity Manager の「リソースユーザー属性」列の変数名を変更する場合は、このオブジェクトでも名前を変更する必要があります。
- アクションは XML 表現に含まれるため、一部の文字をエスケープする必要があります。それらの文字は、次のようにエスケープしてください。

  `&` (アンパサンド): `&`

  `<` (小なり): `<`
- UNIX リソースでは、属性名内のスペースは `_` (下線) で置き換えられます。Windows リソースでは、スペースが維持されます。
- 複数値属性は、次のようなコンマ区切りリストで構成されます。

```
WSUSER_groups=staff,admin,users
```

- ゲートウェイベースのアダプタでは、複数値属性にパイプ区切りリストが使用されます。次に例を示します。

  ```
  WSUSER_NotesGroups=group1|group2|group3
  ```

- Active Directory リソースでは、アクションは、拡張機能を有効にした Windows コマンドインタプリタの cmd.exe を使用して実行されます。

  ユーザー操作の前に実行するアクションでは、ゼロの値を返す必要があります。そうしないと、操作はエラー終了となります。

- 例外がスローされないかぎり、Javascript は正常に完了したとみなされます。

Identity Manager へのアクションファイルの読み込み

アクションを Identity Manager にインポートするには、次の手順に従います。

▼ アクションファイルをインポートする

1. **Identity Manager** 管理者インタフェースにログインします。
2. メニューバーで、「設定」、「交換ファイルのインポート」の順に選択します。
3. アクションが含まれている **XML** ファイルを入力するか、ファイルを参照して選択し、「インポート」をクリックします。

アクションの実装

アクションの定義が完了したら、次の手順に従ってそのアクションを実装します。

▼ アクションを実装する

1. **Identity Manager** ユーザーフォームでフィールドを定義します。
2. アクションを呼び出すリソースのスキーママップにエントリを追加します。

手順 1: Identity Manager ユーザーフォームフィールドを定義する

ユーザー操作の前またはあとに実行するアクションを割り当てるユーザーフォームフィールドを作成します。

- フィールド名。アクションの実行時期と操作対象を示します。
- フィールドの値。アクション名を含みます。

次の例では、ユーザー作成操作のあとに実行する after-create というアクションを定義しています。

```
<Field name='global.create after action'>
    <Expansion>
       <s>after-create</s>
    </Expansion>
</Field>
```

フィールド名の形式は次のとおりです。

```
{create|update|delete} {before|after} action
```

Identity Manager のフォームについては、『Deployment Reference』を参照してください。

手順 2: スキーママップエントリを追加する

アクションを実行するリソースのスキーママップにエントリを追加します。次の手順に従います。

▼ スキーママップにエントリを追加する

1. **Identity Manager** のメニューバーで「リソース」をクリックし、リソースを選択します。
2. 「リソースの編集」ページで、「リソーススキーマの編集」をクリックします。
3. スキーママップで、「属性の追加」をクリックして、スキーママップに行を追加します。
4. 「アイデンティティーシステム ユーザー属性」列に、「**`create after action`**」と入力します。
5. 「リソースユーザー属性」列に、「**`IGNORE_ATTR`**」と入力します。**`IGNORE_ATTR`** エントリによって、その属性は通常のアカウント属性処理では無視されます。

6 「保存」をクリックします。

Active Directory の例

ここでは、リソースアダプタで次の操作が実行されたあとに、Active Directory リソースで実行できるアクションの例を示します。

- ユーザーの作成
- ユーザーアカウントの更新または編集
- ユーザーの削除

例 1: ユーザーの作成後のアクション

この手順では、Active Directory リソースで新規ユーザーの作成後に実行するアクションを含める方法を示します。

▼ ユーザーの作成後に実行するアクションを含める

1 リソースのスキーママップの「**Identity Manager** ユーザー属性」列に、「**`create after action`**」と入力します。

2 「属性タイプ」列で、「**string**」を選択します。

3 「リソースユーザー属性」列に、「**`IGNORE_ATTR`**」と入力します。「必須」、「監査」、「読み取り専用」、および「書き込み専用」の各列は、チェックマークを外したままにします。

4 ユーザーの作成または編集に使用するユーザーフォームに次のコードを追加します。

```
<Field name='resourceAccounts.currentResourceAccounts[AD].attributes.
create after action'>
    <Expansion>
       <s>AfterCreate</s>
    </Expansion>
 </Field>
```

5 次の **XML** ファイルを作成して、**Identity Manager** にインポートします。ファイルのパスは、環境に合わせて変更してください。

```
<?xml version='1.0' encoding='UTF-8'?>
 <!DOCTYPE Waveset PUBLIC 'waveset.dtd' 'waveset.dtd'>
 <Waveset>
    <ResourceAction name='AfterCreate'>
```

```
      <ResTypeAction restype='Windows Active Directory' timeout='6000'>
         <act>
         echo create >> C:\Temp\%WSUSER_accountId%.txt
         exit
         </act>
      </ResTypeAction>
   </ResourceAction>
</Waveset>
```

例 2: ユーザーアカウントの更新または編集後のアクション

この手順では、Active Directory リソースでユーザーの更新または編集後に実行するアクションを含める方法を示します。

▼ ユーザーの更新後または編集後に実行するアクションを含める

1 **Active Directory** スキーママップの「**Identity Manager** ユーザー属性」列に、「**update after action**」と入力します。

2 「属性タイプ」列で、「**string**」を選択します。

3 「リソースユーザー属性」列に、「**IGNORE_ATTR**」と入力します。「必須」、「監査」、「読み取り専用」、および「書き込み専用」の各列は、チェックマークを外したままにします。

4 ユーザーの作成および編集に使用するユーザーフォームに次のフィールドを追加します。

```
<Field name='resourceAccounts.currentResourceAccounts[AD].
attributes.update after action'>
    <Expansion>
       <s>AfterUpdate</s>
    </Expansion>
</Field>
```

5 次の **XML** ファイルを作成して、**Identity Manager** にインポートします。ファイルのパスは、環境に合わせて変更してください。

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE Waveset PUBLIC 'waveset.dtd' 'waveset.dtd'>
<Waveset>
   <ResourceAction name='AfterUpdate'>
      <ResTypeAction restype='Windows Active Directory' timeout='6000'>
         <act>
```

```
          echo update >> C:\Temp\%WSUSER_accountId%.txt
          exit
          </act>
       </ResTypeAction>
    </ResourceAction>
 </Waveset>
```

例 3: ユーザーの削除後のアクション

この手順では、Active Directory リソースでユーザーの削除後に実行するアクションを含める方法を示します。

▼ ユーザーの削除後に実行するアクションを含める

1. リソースのスキーママップの「**Identity Manager** ユーザー属性」列に、「**`delete after action`**」と入力します。
2. 「属性タイプ」列で、「**string**」を選択します。
3. 「リソースユーザー属性」列に、「**`IGNORE_ATTR`**」と入力します。「必須」、「監査」、「読み取り専用」、および「書き込み専用」の各列は、チェックマークを外したままにします。
4. 「**Deprovision Form**」ユーザーフォームの `</Include>` タグのあとに次のフィールドを追加します。

```
<Field name= 'resourceAccounts.currentResourceAccounts[AD].attributes.
delete after action'>
    <Expansion>
       <s>AfterDelete</s>
    </Expansion>
 </Field>
```

5. 次の **XML** ファイルを作成して、**Identity Manager** にインポートします。ファイルのパスは、環境に合わせて変更してください。

```
<?xml version='1.0' encoding='UTF-8'?> <!DOCTYPE Waveset PUBLIC
    'waveset.dtd' 'waveset.dtd'>
 <Waveset>
    <ResourceAction name='AfterDelete'>
       <ResTypeAction restype='Windows Active Directory' timeout='6000'>
          <act>
          echo delete >> C:\Temp\%WSUSER_accountId%.txt
          exit
          </act>
       </ResTypeAction>
```

```
    </ResourceAction>
 </Waveset>
```

6 **Active Directory** リソースの **XML** を編集し、「**delete after action**」スキーママッピングに情報を追加します。新しく追加する部分を含む、このリソースの完全なスキーママッピングの例を次に示します。ここでは、ビュー関連の情報を追加します。

```
<AccountAttributeType id='12' name='delete after action' syntax='string'
         mapName='IGNORE_ATTR' mapType='string'>
    <Views>
       <String>Delete</String>
    </Views>
 </AccountAttributeType>
```

Domino の例

Domino リソースでは、前アクションと後アクションがサポートされます。

現在は、LotusScript と cmd シェルの 2 種類のアクションがサポートされています。どの操作アクションにも、実行される任意の数のアクションを実装できます。

次の例は、LotusScript および cmd シェルのリソースアクションの使用方法を示しています。

LotusScript の例

```
<ResourceAction name='iterateAttributes' createDate='1083868010032'>
   <ResTypeAction restype='Domino Gateway' actionType='lotusscript'>
      <act>
         Sub Initialize
            Main
         End Sub
         Sub Main
            Dim session As New NotesSession
            Dim doc As NotesDocument
            Set doc = session.DocumentContext
            Forall i In doc.Items
               Dim attrVal As Variant
               attrVal = doc.GetItemValue(i.Name)
            End Forall
         End Sub
      </act>
   </ResTypeAction>
</ResourceAction>
```

cmd シェルの例

```
<ResourceAction name='getDirectoryContents' createDate='1083868010032'>
   <ResTypeAction restype='Domino Gateway'>
      <act>dir</act>
   </ResTypeAction>
</ResourceAction>
```

注 – actionType が null の場合は、cmd スクリプトタイプがデフォルトとして使用されます。

LotusScript の実行

Domino では、LotusScript の実行はデータベースに接続されたエージェントによって処理されます。Domino アダプタは、次のいずれかの方法で LotusScript を実行します。

入力	結果
agentName	エージェントを実行します。
agentName およびスクリプト	スクリプトを用いてエージェントを更新し、そのエージェントを実行します。
agentName、agentCreate、およびスクリプト	スクリプトを用いてエージェントを作成し、そのエージェントを実行します。

次に示すカスタマイズされたアカウント属性は、LotusScript で使用できます。これらの属性のいずれかを使用する場合は、その属性を Domino ゲートウェイスキーママップに追加します。「リソースユーザー属性」列には値として「IGNORE_ATTR」を指定します。

- agentName。実行するエージェントの名前を指定します。この属性は必ず指定します。 そうしないと、エラーが返されます。
- agentServer。エージェントがインストールされている、エージェントを実行するデータベースの場所を指定します。この属性が存在しない場合は、「登録 サーバー コンピュータ」リソースパラメータ (REG_SERVER) に指定された値がデフォルトとして使用されます。
- agentDBName。エージェントを検索できるデータベースの名前を指定します。この属性では、リソースの「名前データベース」リソースパラメータ (NAB) で指定された値がデフォルトとして使用されます。

- agentCreate。指定されたエージェントが見つからない場合に、アダプタで新しいエージェントを作成するかどうかを示すフラグを指定します。この属性のデフォルト値は false です。NULL 以外の値にすると、このフラグは有効になります。

注 – agentCreate を指定する場合は、実行する LotusScript も指定してください。

LotusScript への引数

エージェントの引数は、バックエンド NotesSession クラスからの専用プロパティーで、LotusScript へのノートハンドルに指定されます。これは次のように定義できます。

```
NotesDocument = NotesSession.DocumentContext
```

アクションスクリプトルーチンによって NotesDocument をインスタンス化し、そのフィールド値を LotusScript サブルーチンへのパラメータとして読み取ることができます。

ドキュメントに定義された任意の引数の名前と値を取得する LotusScript の例を次に示します。

```
Dim session As New NotesSession
Dim doc As NotesDocument
Set doc = session.DocumentContext

Forall i In doc.Items
   Dim attrVal As Variant
   attrVal = doc.GetItemValue(i.Name)
   Print(" Attribute Name: " + i.Name + " Value: " + attrVal(0))
End Forall
```

NT アクションの場合と同じように、アクションの呼び出し中に定義された属性はすべて、先頭に WSUSER_ が付加されて NotesDocument に配置されます。

cmd シェルの実行

アクションは、拡張機能を有効にした Windows コマンドインタプリタ cmd.exe を使用して実行されます。ユーザー操作の前に実行するアクションでは、ゼロの値を返す必要があります。そうしないと、操作はエラー終了となります。

cmd シェルへの引数

NT/ADSI cmd アクションと同様に、環境変数がエクスポートされ、アクションで利用できるようになります。これらの環境変数は、ユーザーに関する値 (リソーススキーママップの「Identity Manager ユーザー属性」列で定義される) を持つ、スキーマにマップされたすべての属性を、先頭に WSUSER_ を付加して構成します。

複数値属性は、次のようなパイプ区切りリストで構成されます。

```
WSUSER_groups=staff|admin|users
```

メインフレームの例

ACF2、RACF、および Top Secret アダプタでは、login および logoff のリソースアクションが必要です。login アクションは、認証されたセッションに関してメインフレームとネゴシエーションを行います。logoff アクションは、そのセッションが不要になったときに接続を解除します。

thin クライアントのホストアクセス 3270 エミュレータは、スクリプトセッション内のコマンドの実行を簡素化するために、リソースアダプタによるリソースアクションのコンテキストに提供されます。このエミュレータは、`com.waveset.object.HostAccess` クラスで定義されます。リソースアクションに渡される hostAccess オブジェクトで使用可能なメソッドに関する詳細については、HostAccess に関する JavaDoc を参照してください。

リソースアクションのコンテキスト

グローバル変数のいくつかは、スクリプトアクションのコンテキストで使用します。

オブジェクト	説明
hostAccess	TN3270 エミュレータ。`com.waveset.adapter.HostAccess` のインスタンス。メインフレームとの間でキーストロークとコマンドを送受信するために使用されます。
hostAccessLogin	`com.waveset.adapter.HostAccessLogin` インタフェースを実装するクラスのインスタンス。主に、ログインプロセス中にイベントが失敗した場合に必要となる、`logoff()` メソッドを実装するために使用されます。
identity	リソースのユーザーの accountId を含む文字列。
user	ログオンする管理ユーザー名を含みます。
userAttrs	アクションで必要な各リソースユーザー属性の値を含む `java.util.Map` のインスタンス。
password	メインフレームユーザーのパスワードを格納する暗号化されたオブジェクト。プレーンテキストに変換するには password.decryptToString() を使用します。
system	メインフレームシステム名

オブジェクト	説明
out	java.io.PrintStream のインスタンス。Javascript がこのストリームに書き込む場合 (たとえば out.print("Hello") など)、その内容がトレースされ、リソースアクションの結果として UI に示されます。
err	java.io.PrintStream のインスタンス。Javascript がこのストリームに書き込む場合 (たとえば err.print("Error") など)、その内容がトレースされ、リソースアクションの結果として UI に示されます。

SendKeys メソッドのニーモニックキーワード

次の表では、3270 エミュレータを通して実行可能な、英数字以外の値のキー入力をシミュレートする特殊機能について説明します。

機能	ニーモニックキーワード	機能	ニーモニックキーワード
Attention	[attn]	F1	[pf1]
Backspace	[backspace]	F2	[pf2]
Backtab	[backtab]	F3	[pf3]
Beginning of Field	[bof]	F4	[pf4]
Clear	[clear]	F5	[pf5]
Cursor Down	[down]	F6	[pf6]
Cursor Left	[left]	F7	[pf7]
Cursor Right	[right]	F8	[pf8]
Cursor Select	[cursel]	F9	[pf9]
Cursor Up	[up]	F10	[pf10]
Delete Character	[delete]	F11	[pf11]
DUP Field	[dup]	F12	[pf12]
Enter	[enter]	F13	[pf13]
End of Field	[eof]	F14	[pf14]
Erase EOF	[eraseeof]	F15	[pf15]
Erase Field	[erasefld]	F16	[pf16]
Erase Input	[erinp]	F17	[pf17]
Field Mark	[fieldmark]	F18	[pf18]

機能	ニーモニックキーワード	機能	ニーモニックキーワード
ホーム	[home]	F19	[pf19]
Insert	[insert]	F20	[pf20]
New Line	[newline]	F21	[pf21]
PA1	[pa1]	F22	[pf22]
PA2	[pa2]	F23	[pf23]
PA3	[pa3]	F24	[pf24]
Page Up	[pageup]		
Page Down	[pagedn]		
Reset	[reset]		
System Request	[sysreq]		
Tab Field	[tab]		

サンプルリソースアクション

次のコーディング例は、メインフレームのリソース上で一般に実行されるアクションを示しています。

- 567 ページの「login アクション」
- 568 ページの「logoff アクション」
- 569 ページの「RACF データセット規則のアクション」

login アクション

次のコードは、login および logoff リソースアクションの完全なサンプルです。このサンプルは、Top Secret リソースを使用する、ある特定の顧客の環境に合わせた内容になっています。したがって、コマンド、プロンプト、コマンドシーケンスなどのテキストは、配備環境によって異なる可能性があります。これらのリソースアクションは、XML 内の Javascript をラップします。

```
<ResourceAction name='ACME Login Action'>
   <ResTypeAction restype='TopSecret'>
      <act>
         var TSO_MORE = " ***";
         var TSO_PROMPT = " READY";
          var TS_PROMPT = " ?";
         hostAccess.waitForString("ENTER YOUR APPLICATION NAME");
         hostAccess.sendKeys("tso[enter]");
          hostAccess.waitForString("ENTER USERID— ");
```

```
            hostAccess.sendKeys(user + "[enter]");
            hostAccess.waitForString("TSO/E LOGON");
            hostAccess.sendKeys(password);
            hostAccess.sendKeys("[enter]");
            var pos = hostAccess.searchText("  -Nomail", false);
            if (pos != 0) {
               hostAccess.setCursorPos(pos);
               hostAccess.sendKeys("S");
            }
            pos = hostAccess.searchText("  -Nonotice", false);
            if (pos != 0) {
               hostAccess.setCursorPos(pos);
               hostAccess.sendKeys("S");
            }
            hostAccess.sendKeys("[enter]");
            hostAccess.waitForStringAndInput(TSO_MORE);
            hostAccess.sendKeys("[enter]");
            hostAccess.waitForStringAndInput(TSO_MORE);
            hostAccess.sendKeys("[enter]");
            hostAccess.waitForStringAndInput("ISPF");
            hostAccess.sendKeys("=x[enter]");
            hostAccess.waitForString(TSO_PROMPT);
            var resp =hostAccess.doCmd("PROFILE NOPROMPT MSGID NOINTERCOM
NOPAUSE NOWTPMSG PLANGUAGE(ENU) SLANGUAGE(ENU) NOPREFIX[enter]",
TSO_PROMPT, TSO_MORE);
            hostAccess.waitForStringAndInput("ENTER LOGON:");
            hostAccess.sendKeys(system + "[enter]");
            hostAccess.waitForStringAndInput("USER-ID.....");
            hostAccess.sendKeys(user + "[tab]" + password);
            hostAccess.sendKeys("[enter]");
            var stringsToHide = new java.util.ArrayList();
            stringsToHide.add(password.decryptToString());
            hostAccess.waitForString("==>", stringsToHide);
            hostAccess.waitForInput();
            hostAccess.sendKeys("[pf6]");
            hostAccess.waitForInput();
         </act>
      </ResTypeAction>
   </ResourceAction>
```

logoff アクション

```
<ResourceAction name='ACME Logoff Action'>
   <ResTypeAction restype='TopSecret'>
      <act>
         var TSO_PROMPT = " READY";
         hostAccess.sendKeys("[clear]end[enter]");
         hostAccess.waitForString(TSO_PROMPT);
```

```
        hostAccess.sendKeys("logoff[enter]");
      </act>
   </ResTypeAction>
</ResourceAction>
```

RACF データセット規則のアクション

RACF リソースパラメータのページで「データセット規則の作成および削除」パラメータが選択されている場合は、Identity Manager によってデータセット規則が直接管理されます。ユーザー独自のデータセット規則を設定するには、次のようなアクションを定義します。

```
<ResourceAction name='create after action'>
   <ResTypeAction restype='RACF'>
      <act>
         var TSO_PROMPT = " READY";
         var TSO_MORE = " ***";
         var cmd1 = "addsd '"+identity+".test1.**' owner('"+identity+"')[enter]";
         var result1 = hostAccess.doCmd(cmd1, TSO_PROMPT, TSO_MORE);
      </act>
   </ResTypeAction>
</ResourceAction>
```

ビューの拡張

ビューに属性を追加できます。属性はすべて登録されている必要があります。

Identity Manager でのさまざまなプロビジョニングアクティビティーにおいて利用できるユーザー属性は、そのアクションを完了するために必要な属性に限定されます。たとえば、ユーザーを編集する場合には、割り当てられたリソースの中で更新可能と定義されているユーザー属性のみが利用できます。一方、パスワードの変更プロセスでは、要求を実行するための属性のサブセットのみを必要とします。

属性の登録

属性は、次のいずれかの場所に登録できます。

場所	属性をここに登録する条件
リソース内の `AccountAttributeType` 定義	... 更新する属性が、そのタイプのすべてのリソースではなく、特定のリソースのみに適用されます。

場所	属性をここに登録する条件
System Configuration オブジェクト	... 特定タイプのすべてのリソースに適用されるグローバル登録を行います。このような登録は、XML フォーマットで行います。

異なる属性を異なるビューに登録できます。たとえば、lock 属性をパスワードビューに登録したり、firstname 属性を名前の変更ビューに登録したり、リソースアクションを有効化ビュー、無効化ビュー、またはプロビジョニング解除ビューに登録したりできます。

注 – 前アクションと後アクションの場合は、作成または更新のユーザープロセスを除くすべてのプロセスのビューを拡張してください。ビューの拡張については、「Identity Manager Views」を参照してください。

グローバル登録

グローバル登録を行うには、次のパスを持つ System Configuration オブジェクトに属性を追加します。

```
updatableAttributes.ViewName.ResourceTypeName
```

ここで、*ViewName* は Password、Reset、Enable、Disable、Rename、または Delete のいずれかで、ResourceTypeName はリソースタイプの名前です。all というタイプ名は、すべてのリソースに適用される登録用に予約されています。

この属性の値には、<String> のリストを指定する必要があります。各文字列は、更新する属性の名前です。次の例は、すべてのリソースを対象とした delete before action という属性をプロビジョニング解除ビューに登録します。

```
<Attribute name='updatableAttributes'>
    <Object>
       <Attribute name='Delete'>
          <Object>
             <Attribute name='all'>
                <List>
                   <String>delete before action</String>
                </List>
            </Attribute>
         </Object>
      </Attribute>
       <Attribute name='Enable'>
          <Object>
             <Attribute name='all'>
                <List>
                   <String>enable before action</String>
                </List>
```

```
            </Attribute>
          </Object>
        </Attribute>
    </Object>
</Attribute>
```

リソース別登録

リソースに固有の登録を行うには、Identity Manager の「デバッグ」ページでリソースオブジェクトを修正し、AccountAttributeType 要素に <Views> 下位要素を挿入します。<Views> には、この属性が更新されるビューの名前を示す文字列のリストを指定する必要があります。

```
<AccountAttributeType name='lastname' mapName='sn' mapType='string'>
    <Views>
       <String>Rename</String>
    </Views>
</AccountAttributeType>
```

ビューでは、変更する属性が、次のオブジェクトの内部に配置されます。

`resourceAccounts.currentResourceAccounts[`*ResourceTypeName*`].attributes`

例:

```
<Field name= 'resourceAccounts.currentResourceAccounts[OS400ResourceName].
    attributes.delete before action' hidden='true'>
    <Expansion>
       <s>os400BeforeDeleteAction</s>
    </Expansion>
</Field>
```

◆ ◆ ◆ 第 51 章

51 LDAP パスワードの同期

この章では、Sun Java™ System Directory Server (以前は Sun ONE Directory Server および iPlanet Directory Server と呼ばれていた) から Identity Manager システムへのパスワードの同期をサポートするための、Identity Manager 製品の拡張機能について説明します。

概要

Directory Server では、パブリックなプラグイン API を介して、サードパーティーがパスワードの変更を処理できるようになっています。カスタムプラグインであるパスワードキャプチャープラグインは、Directory Server でのパスワード変更をキャプチャーするために開発されました。

パスワードキャプチャープラグインには、次の役割があります。

- LDAP ADD および LDAP MODIFY の操作時にパスワード変更を検知する。
- 共有キーを使用して新しいパスワード値を暗号化する。
- 元の LDAP 操作に対して、`idmpasswd` 属性とその値 (暗号化されたパスワード値) のペアを挿入します。

パスワードキャプチャープラグインを実装する前に、Directory Server の旧バージョン形式の更新履歴ログプラグインを、ディレクトリサーバーにインストールする必要があります。旧バージョン形式の更新履歴ログプラグインは、ディレクトリサーバーコアによる操作が実行されたあと、`idmpasswd` 属性の変更を更新履歴ログデータベースに記録します。

Active Sync を有効にしている LDAP リソースアダプタは、定期的に更新履歴ログデータベースをポーリングし、関連した変更を解析して、それらの変更を Identity Manager に送ります。LDAP アダプタは、`idmpasswd` 属性を解析し、共有キーを使用してパスワードを復号化し、実際のパスワードをシステムのほかの部分で利用できるようにします。

パスワードキャプチャー処理

パスワードキャプチャープラグインは、サーバーが LDAP ADD または LDAP MODIFY 操作を処理しようとするたびに、Directory Server コアによって呼び出されます。このプラグインは変更を調べて、パスワード変更があると、idmpasswd 属性と値のペアを挿入します。この値は暗号化されたパスワードです。

パスワードキャプチャープラグインによってキャプチャーされたパスワードは、共有キーを使用して暗号化されます。設定された LDAP リソースアダプタによってそのパスワードが復号化されるときに、同じ共有キーが使用されます。

変更がサーバーに受け入れられると、旧バージョン形式の更新履歴ログプラグインは、旧バージョン形式の更新履歴ログデータベースにその変更 (idmpasswd 属性の新しい値を含む) を記録します。LDAP リソースアダプタは、idmpasswd 属性の変更を処理し、暗号化された文字列の形式で、Identity Manager 内のほかのコンポーネントがその値を利用できるようにします。

idmpasswd 属性は、ユーザーがパスワードを変更するときに Directory Server の通常のデータベースには表示されません。

旧バージョン形式の更新履歴ログデータベース内のパスワード

暗号化されたパスワードは、旧バージョン形式の更新履歴ログデータベースに記録されます。旧バージョン形式の更新履歴ログプラグインは、旧バージョンの更新履歴ログデータベースから定期的にエントリを削除するように設定することができます。データベースのエントリ削除の適切な設定は、ターゲットの環境によって異なります。削除間隔が短すぎると、短時間のネットワーク機能停止やほかのサービスの中断に対処できないことがあり、LDAP リソースアダプタは一部の変更を見逃す可能性があります。反対に、データベースのサイズが大きくなりすぎると、データベース内に暗号化されたパスワードを保持することに付随するセキュリティー上のリスクが増える可能性があります。

プラグインはハッシュされたパスワードを取得しません。

旧バージョン形式の更新履歴ログデータベースのサフィックス (cn=changelog) の内容へのアクセスを制限するようにしてください。そのために、読み取りアクセス権は、LDAP リソースアダプタのみに許可します。

スキーマの変更

idmpasswd 属性は、オペレーショナル属性として定義されます。オペレーショナル属性は、ターゲットエントリのオブジェクトクラス定義の変更を一切必要としませ

ん。そのため、パスワード同期機能を使用するために Directory Server の既存ユーザーまたは新規ユーザーを変更する必要はありません。

idmpasswd 属性は、スキーマで次のように定義されます。

```
attributeTypes: ( idmpasswd-oid NAME 'idmpasswd' DESC 'IdM Password'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.40{128} USAGE directoryOperation X-ORIGIN '
Identity Manager' )
```

プラグインのログレベル

プラグインがサポートするログレベルは、SEVERE、WARNING、INFO、CONFIG、FINE、FINER、および FINEST です。SEVERE では最小限の情報が記録され、FINEST ではもっとも詳細なログが記録されます。デフォルトのレベルは INFO ログレベルです。

Identity Manager での LDAP パスワード同期の設定

LDAP アダプタを使用して LDAP パスワードを同期するには、次の作業を実行します。

- LDAP リソースアダプタを設定します。
- パスワード同期機能を有効にします。

手順 1: LDAP リソースアダプタを設定する

パスワード同期をサポートするように LDAP リソースアダプタを設定するには、次の手順を使用します。

▼ パスワード同期をサポートするように LDAP リソースアダプタを設定する

1. **LDAP Password ActiveSync Form** を **Identity Manager** にインポートします。このフォームは、`$WSHOME/sample/forms/LDAPPasswordActiveSyncForm.xml` で定義されています。
2. リソースの **Active Sync** ウィザードで、入力フォームを「**LDAP Password ActiveSync Form**」に設定します。

手順 2: パスワード同期機能を有効にする

LDAP リソースアダプタでパスワード同期を有効にするために、Identity Manager にはカスタム JSP ページが用意されています。管理者はこのページで次の操作を行えます。

- 任意の LDAP リソースアダプタでパスワード同期を有効にする
- パスワードキャプチャープラグインのインストールに必要な設定 LDIF ファイルを生成する
- 必要に応じて、パスワード暗号化キーおよびパスワード暗号化ソルトを再生成する。これはオプションの機能です。

LDIF ファイルは、次の 3 つのエントリで構成されます。

- スキーマの変更。`idmpasswd` オペレーショナル属性の使用を許可するように Directory Server スキーマを更新します。
- プラグインの定義。プラグインを Directory Server に登録し、プラグイン有効にします。
- プラグインの設定。プラグインの基本的な設定を行います。たとえば、難読化されたパスワード暗号化キーは、この設定エントリに含まれます。

これらの機能を実装するには、次の手順を使用します。

▼ パスワード同期機能を実装する

1. **Identity Manager** の「パスワード同期の設定」ページを開きます。このページには、`http://`*PathToIdentityManager*`/configure/passwordsync.jsp` からアクセスします。
2. 「リソース」メニューから、パスワードの同期に使用する **LDAP** リソースを選択します。
3. 「アクション」メニューから、「パスワード同期の有効化」を選択します。
4. 「**OK**」をクリックします。ページが再描画され、「アクション」メニューに新しい項目が表示されます。
5. 「アクション」メニューから、「プラグイン設定 **LDIF** をダウンロードします」を選択します。
6. 「**OK**」をクリックします。ページが再描画され、いくつかの新しいオプションが表示されます。
7. 「**Directory Server** のバージョン」メニューからバージョンを選択します。

8 「オペレーティングシステムタイプ」メニューから、リソースのオペレーティングシステムを選択します。

9 「プラグインのインストールディレクトリ」フィールドに、プラグインをインストールするホスト上のディレクトリを入力します。

10 「**OK**」をクリックして、**LDIF** ファイルを生成およびダウンロードします。必要に応じて、ここで暗号化キーを再生成してもかまいません。

11 「アクション」メニューから、「暗号化キーを再生成します」を選択します。

12 「**OK**」をクリックします。暗号化パラメータが更新されます。

注 – Directory Server ユーザーがデフォルトのオブジェクトクラス (`person`、`organizationalPerson`、または `inetorgperson`) を持たない場合は、「プラグイン設定 LDIF をダウンロードします」を選択したときに作成される LDIF ファイルを編集する必要があります。`idm-objectclass` 属性で指定したデフォルト値を、環境に実装されているオブジェクトクラスに置換する必要があります。これにより、プラグインはパスワードの変更をキャプチャーできるようになります。

たとえば、ユーザーが `account`、`posixaccount`、および `shadowaccount` オブジェクトクラスで定義されている場合、`idm-objectclass` 属性に指定されているデフォルト値を、これらのオブジェクトクラスのいずれか (複数可) で置換します。

たとえば、次のようにします。

```
idm-objectclass: account
      idm-objectclass:  posixaccount
```

複数値属性は、コンマ区切りの文字列で指定しないでください。一致させる idm-objectclass の値は、LDIF 設定に 1 行に 1 つずつ入力する必要があります。`idm-objectclass` 値のいずれかに一致するエントリに対してパスワードがキャプチャーされます。

パスワード同期を有効にしたら、リソースの Active Sync ウィザードパラメータページの「リソース固有の設定」ページに、次の属性が表示されます。

- パスワード同期の有効化
- パスワード暗号化キー
- パスワード暗号化ソルト

「パスワード同期の有効化」フィールドのみ、このページで変更できます。暗号化属性は、JSP ページでのみ更新するようにしてください。

パスワードキャプチャープラグインのインストールと設定

プラグインのインストールを開始する前に、必ずリソースの設定を完了してください。詳細は、575 ページの「Identity Manager での LDAP パスワード同期の設定」を参照してください。

注 – Directory Server インスタンスがマルチマスターレプリケーション環境にセットアップされている場合は、マスターレプリカごとにプラグインをインストールおよび設定する必要があります。

パスワードキャプチャープラグインをインストールするには、次の一般的な手順を実行する必要があります。これらの作業の実行の詳細については、製品マニュアルを参照してください。

▼ パスワードキャプチャープラグインのインストールの概要

1. 設定 **LDIF** ファイルをターゲット **Directory Server** にアップロードします。**Directory Server** に付属する **LDAP** コマンド行ユーティリティーを使用できます。次に例を示します。

   ```
   /opt/iPlanet/shared/bin/ldapmodify -p 1389 -D "cn=directory manager" -w
   secret -c -f /tmp/pluginconfig.ldif
   ```

2. **Directory Server version 5.2 P4** 以前の場合のみ、プラグインバイナリ (`idm-plugin.so`) を **Directory Server** が実行されているホストに配置します。この例では、`/opt/SUNWidm/plugin` です。ディレクトリサーバーを実行するユーザーは、プラグインライブラリを読み取れる必要があります。そうでなければ、**Directory Server** の起動に失敗します。

3. **Directory Server** を再起動します (たとえば、`/opt/iPlanet/slapd-examplehost/restart-slapd`)。**Directory Server** を再起動したあとに、パスワードキャプチャープラグインは読み込まれません。

注 –

- マルチマスターレプリケーション環境では、インストールごとに新しいプラグイン設定を生成してください (各ホストでオペレーティングシステムタイプとプラグインのインストールディレクトリが同じである場合は除く)。このような環境では、インストールごとに 576 ページの「手順 2: パスワード同期機能を有効にする」の手順を繰り返します。
- プラグインの設定に変更を加えた場合は、必ず Directory Server を再起動する必要があります。

パスワードキャプチャープラグインが有効になったあとで、クライアントがパスワード変更を行うには、`userPassword` 属性と `idmpasswd` 属性の両方に対する MODIFY 権限が必要です。それに応じて、ディレクトリツリー内のアクセス制御情報の設定を調整してください。これは通常、ディレクトリマネージャー以外の管理者がほかのユーザーのパスワードを更新できる場合に必要になります。

◆ ◆ ◆ 第 52 章

Active Directory Synchronization Failover

ここでは、Active Directory 同期フェイルオーバーの処理方法について説明します。このカスタマイズを実行すると、新しいドメインコントローラに切り替えたときに発生する繰り返しイベントの数を制限できます。

Active Directory 同期フェイルオーバーでは、処理を継続できる設定可能な一連のドメインコントローラから `HighestCommittedUSN` の履歴を定期的に収集および維持するタスクを使用します。Active Sync ドメインコントローラがダウンした場合は、もう 1 つのタスクを実行することで、フェイルオーバードメインコントローラの 1 つを指すように Active Directory リソースの設定を変更できます。Active Directory で行われた変更がすべてのドメインコントローラにレプリケートされるまで少し時間がかかることがあるため、Active Directory Active Sync では、フェイルオーバードメインコントローラで新しい変更の処理のみを開始すればよいというわけではありません。そうではなく、ダウンする前のドメインコントローラにレプリケートされていない可能性がある、フェイルオーバードメインコントローラに加えられた古い変更も調べる必要があります。このため、レプリケーションの遅延を十分に見込んだ過去の時点にそのフェイルオーバードメインコントローラに関して保存された `HighestCommittedUSN` を使用します。これにより、Active Sync がイベントを見逃すことを防止できますが、一部の変更が 2 回処理される可能性もあります。

必要なコンポーネント

この手順には、次のコンポーネントが必要です。

- Active Directory Synchronization Failure プロセス。 Active Directory リソースで、「On Synchronization Failure Process」Active Directory リソース属性によって定義されます。
- Active Directory Recovery Collector タスク
- Active Directory Failover タスク

「On Synchronization Failure Process」リソース属性

Active Directory のアクティブな同期に関する「On Synchronization Failure Process」リソース属性は、同期失敗時に実行されるプロセスの名前を指定します。デフォルトでは、このリソース属性の値は空です。

この属性は、Identity Manager 管理者に、Active Directory 同期失敗の発生時にプロセスを実行できる機能を提供します。

Active Directory 失敗時のプロセス

リソース属性で指定されたプロセスは、失敗時にリソースによって起動されます。同期失敗の発生を知らせる電子メールを Active Directory 管理者に送信するプロセスを起動するようにしてください。電子メールの本文に、アダプタのポーリングメソッドから返されたエラーメッセージを含むこともあります。

また、指定されたエラーが発生したときに、管理者による承認を得てから、同期フェイルオーバータスクを自動的に呼び出すビジネスプロセスを設計することもできます。

プロセスのコンテキスト

ネイティブプロセスでは次の引数を使用できます。

引数	説明
`resourceName`	失敗が発生したリソースを識別します
`resultErrors`	ポーリングメソッドから返されたエラーを示す文字列を一覧表示します
`failureTimestamp`	失敗が発生した時刻を示します

Active Directory Recovery Collector タスク

Identity Manager 管理者インタフェースの「タスクスケジュール」ページで、Active Directory Recovery Collector タスクをスケジュールして起動できます。このプロセスは、リソースオブジェクトインタフェースを使用して各ドメインコントローラの `rootDSE` オブジェクトと交信します。タスクのスケジュールによって、ドメインコントローラからデータが収集される頻度が決まります。

このタスクは、リソース復元情報を収集し、ADSyncRecovery_resourceName という名前の設定オブジェクトに格納します。この設定オブジェクトを拡張した GenericObject には各ドメインコントローラで収集された HighestCommittedUSN とタイムスタンプ (ミリ秒単位) のリストが格納されます。

資格各実行中に、このタスクは HighestCommittedUSN の古い値を復元データから除去します。daysToKeepUSNS 引数で、このデータを格納する期間を設定できます。

引数

引数	説明
resourceName	Identity Manager がバックアップデータを収集する Active Directory リソースを指定します。
backupDCs	復元データについて問い合わせる完全修飾ドメインコントローラホスト名を一覧表示します。このリストには元のホストを含めることができるので、含めるようにしてください。これにより、Identity Manager がリソースの処理を継続する必要がある場合、Identity Manager はソースリソースホストを含めることができます。 グローバルカタログとの同期をとる場合は、このリストのバックアップホストがグローバルカタログと見なされます。
daysToKeepUSNS	Identity Manager にデータを格納する日数を指定します (デフォルトでは 7 日)。

Active Directory Failover タスク

このタスクは、失敗が発生したリソースと IAPI オブジェクトが、代替ドメインコントローラと usnChanged 開始ポイントを使用するように再設定します。タスク入力フォームに、格納されたフェイルオーバーデータから、指定されたホストで利用可能な usn-changed 時間が表示されます。

いくつかのエラーから、フェイルオーバーが適している状況を識別できます。フェイルオーバータスクの自動呼出しで発生する可能性がある問題の一例に、java.net.UnknownHostException エラーメッセージがあります。このメッセージで示されるエラーは、少なくとも次の 2 つの理由で発生することがあります。

- 一時的なルーティングの問題により、ゲートウェイマシンからホストに到達できない。
- ホストに到達できず、予定された休止によりその後 8 時間ホストが停止される。

フェイルオーバーモード

Active Directory フェイルオーバーを用いて問題を解決するには、次の 2 つの方法のどちらかを使用できます。

- 手動モード。問題が発生したときに、どのバックアップドメインコントローラと USN を使用するかを管理者が指定します。これは、Identity Manager インタフェースからタスクを実行している場合にのみ利用できるモードです。
- 半自動モード。半自動モードでは、フェイルオーバー解決プロセスを半自動化できます。半自動モードでは、タスクは収集されたデータを使用して、使用する最適なバックアップドメインコントローラと USN を特定します。タスクは、以下の計算式で算出される `TargetTimestamp` の値を超えない範囲でもっとも近い収集ポイントを探します。

  ここで、`TargetTimestamp = (FailureTimestamp - replicationTime)` です。

  半自動モードは、Identity Manager 管理者インタフェースからは利用できません。

引数

特定のエラーに半自動フェイルオーバーの起動が適していると判断した場合は、次のタスク引数を設定します。(エラー時ワークフローは、Active Directory 同期フェイルオーバータスクを起動する必要があります。)これらの引数を設定することにより、失敗が発生したリソースと IAPI オブジェクトが、代替ドメインコントローラと `usnChanged` 開始ポイントを使用するように再設定されます。

引数	説明
`resourceName`	失敗が発生した場所を名前またはリソース ID によって特定します。
`autoFailover`	自動フェイルオーバーを設定するかどうかを指定します。`true` に設定します。
`failureTimestamp`	失敗が発生した時刻を示します。この値は、onSync エラープロセスから取得されます。
`replicationTime`	Active Directory 環境でデータをレプリケートするための最長時間 (時間単位) を指定します。

処理を継続するドメインコントローラおよび開始ポイントとなる保存された `HighestCommittedUSN` 番号を手動で指定するには、次の引数を指定します。

引数	説明
`resourceName`	失敗が発生したリソースの名前または ID を指定します。

引数	説明
backupDC	同期プロセスを開始するホストの名前を指定します。
usnDate	収集されたデータから収集された HighestCommittedUSN の変更値に関連付けるために使われるタイムスタンプです。これは、半自動モードで targetTime が計算されるのと同じように計算されます。
restartActiveSync	新しいドメインコントローラへの切り替えが完了したあとに Active Sync を起動するかどうかを指定します。

リソースオブジェクトの変更

Active Directory Recovery Collector タスクでは、使用されている値に基づいて LDAPHostname リソース属性値か GlobalCatalog リソース属性値のどちらかが更新されます。サブドメイン検索リソース属性が true に設定されていて、グローバルカタログ属性の値が空でない場合は、グローバルカタログサーバー属性が変更されます。それ以外の場合は、LDAPHostname がバックアップドメインコントローラの名前に変更されます。

IAPI オブジェクトの変更

Active Directory Recovery Collector タスクでは、次回の実行時に調べる変更を Active Directory リソースアダプタに知らせるために、IAPI オブジェクトも更新されます。このタスクでは、lastUpdated 属性値と lastDeleted 属性値の両方の HighCommitedUSN 値が更新されます。

Active Directory 同期フェイルオーバーの設定

手順 1: Active Directory Synchronization Recovery Collector タスクを設定する

- データを保持する最大時間数を設定します。デフォルト値は 7 日です。この値により、どれくらい以前の HighestCommittedUSN 値を保持するかを制御します。

  設定する必要がある Active Sync リソースごとに 1 つのワークフローを設定します。

- Identity Manager 管理者インタフェースの「タスク」ページで、このタスクをスケジュールします。HighestCommittedUSN 値について各ホストに問い合わせる頻度を規定するポーリング間隔は、タスクスケジュールによって設定されます。

  このタスクが実行されると、Active Directory アダプタは、各ドメインコントローラの rootDSE から HighestCommittedUSN 番号を取得するように求められます。取得した値は、Identity Manager 設定オブジェクトに格納されます。定義され

た Active Sync リソースごとに 1 つの設定オブジェクトが生成され、代替ドメインコントローラの `HighestCommittedUSN` 値が格納されます。

手順 2: Active Directory エラー時プロセスの Active Sync 属性を定義する

各 Active Directory Active Sync リソースでは、Identity Manager によって、リソースの同期中に失敗が発生したときに呼び出される `onError` プロセスが定義されます。Active Directory リソースでエラー時プロセスが定義されていると、アクティブな同期中にリソースでポーリングメソッドが呼び出されたときにエラーが発生した場合に、このプロセスが呼び出されます。このプロセスでは、IAPI オブジェクトからの結果がチェックされ、エラーが発生した場合は、定義されたプロセスが呼び出されます。

このプロセスを、エラーが発生したときに電子メールで管理者に通知するように設定します。Identity Manager によって別のドメインコントローラに処理が継続されるように、エラーが保証されているかどうかを管理者が判断できるように、電子メールの本文にエラーテキストを含めます。

そのエラーテキストにより、管理者は、長期にわたる停止の可能性があるか、すぐに解決できる一時的な問題 (次回のポーリングで解決される一時的なルーティングの問題など) による障害であるかを知らされます。

手順 3: 失敗が発生したリソースの Active Directory 同期フェイルオーバータスクを実行する

別のドメインコントローラへのフェイルオーバーが保証されているエラーがドメインコントローラから返された場合は、「タスク」ページから Active Directory 同期フェイルオーバータスクを実行します。

手動フェイルオーバーモードの場合は、フェイルオーバータスクに次の情報が必要です。

- ダウンしたドメインコントローラまたはリソースの名前
- 処理を継続する DC ホストの名前
- 使用する収集済み `HighestCommittedUSN` 値のタイムスタンプ

新しいドメインコントローラへの切り替えが完了したあとに Active Sync を再起動するかどうかも選択してください。

タスクの動作

Active Directory 同期フェイルオーバータスクは、実行時に次のように動作します。

▼ タスクのアクション

1. 失敗が発生したリソースの **Active Sync** プロセスを停止する
2. フェイルオーバー設定オブジェクトを読み取る
3. 必要なリソース属性値を変更する
4. オプションで、**Active Sync** プロセスを再起動する

同期失敗ワークフローの例

Active Directory リソースの「On Synchronization Failure Process」リソース属性として、次のサンプルワークフローを設定できます。このワークフローでは、`java.net.UnknownHostException` エラーメッセージを探します。このメッセージが見つかった場合は、管理者に通知電子メールを送信します。

```
<TaskDefinition name='Sample AD Sync On Error Workflow'
  executor='com.waveset.workflow.WorkflowExecutor'
   syncControlAllowed='true' execMode='sync'
   taskType='Workflow'>
   <Extension>
      <WFProcess title='Example AD Sync OnError Workflow'>
         <Variable name='resultErrors' input='true'>
           <Comments>Errors returned from the resource.
           </Comments>
         </Variable>
        <Variable name='resourceName' input='true'>
           <Comments>Name of the AD resource that returned the errors.
            </Comments>
         </Variable>
        <Variable name='failureTimestamp' input='true'>
           <Comments>Failure timestamp, when it occurred.
           </Comments>
         </Variable>
        <Activity name='start'>
           <Transition to='checkErrors'/>
         </Activity>
         <Activity name='checkErrors'>
           <Variable name='criticalError'>
            <Comments>Local variable to hold if we need to notify
            </Comments>
           </Variable>
        <Action name='iterateMessage'>
           <dolist name='msg'>
```

```
                <ref>resultErrors</ref>
                  <cond>
                    <match>
                <ref>msg</ref>
                  <s>java.net.UnknownHostException</s>
                    </match>
                      <set name='criticalError'>
                       <s>true</s>
                      </set>
                  </cond>
              </dolist>
            </Action>
           <Transition to='notify'>
              <notnull>
                <ref>criticalError</ref>
              </notnull>
            </Transition>
            <Transition to='end'/>
            </Activity>
           <Activity name='notify'>
              <Action application='notify'>
                <Argument name='template'
                          value='#ID#EmailTemplate:ADSyncFailoverSample'/>
                <Argument name='resultErrors' value='$(resultErrors)'/>
              </Action>
            <Transition to='end'/>
            </Activity>
           <Activity name='end'/>
        </WFProcess>
      </Extension>
</TaskDefinition>
```

◆ ◆ ◆ 第 53 章

メインフレーム接続

この章では、IBM の Host On Demand または Attachmate 3270 Mainframe Adapter for Sun Emulator Class Library を使用してメインフレームのリソースへの接続を確立する方法について説明します。

Host On Demand による SSL 設定

ここでは、このアダプタ用の SSL の設定方法について説明します。次のトピックがあります。

SSL または TLS を使用してアダプタを Telnet/TN3270 サーバーに接続する

SSL または TLS を使用して RACF リソースアダプタを Telnet/TN3270 サーバーに接続するには、次の手順を使用します。

▼ RACF アダプタを Telnet/TN3270 サーバーに接続する

1 **PKCS #12** ファイル形式の **Telnet/TN3270** サーバーの証明書を取得します。このファイルのパスワードとして hod を使用します。サーバーの証明書をエクスポートする方法については、使用しているサーバーのマニュアルを参照してください。一般的な手順は、**590** ページの「**PKCS #12** ファイルの生成」で説明しています。

2 **PKCS #12** ファイルから `CustomizedCAs.class` ファイルを作成します。最新バージョンの **HOD** を使用している場合は、次のコマンドを使用してこの作業を行います。

```
..\hod_jre\jre\bin\java -cp ../lib/ssliteV2.zip;
../lib/sm.zip com.ibm.eNetwork.HOD.convert.CVT2SSLIGHT CustomizedCAs.p12
hod CustomizedCAs.class
```

3 `CustomizedCAs.class` ファイルを **Identity Manager** サーバーのクラスパス内の任意の場所 (`$WSHOME/WEB-INF/classes` など) に配置します。

4 「セッションプロパティー」というリソース属性がリソースにまだ存在しない場合は、**[IDMIDE** テキストエンティティーを定義してください**]** またはデバッグページを使用して、この属性をリソースオブジェクトに追加します。`<ResourceAttributes>` セクションに、次の定義を追加します。

```
<ResourceAttribute name='Session Properties'
     displayName='Session Properties' description='Session Properties' multi='true'>
</ResourceAttribute>
```

5 リソースの「リソースパラメータ」ページに移動し、「セッションプロパティ」リソース属性に値を追加します。

```
SESSION_SSL
true
```

PKCS #12 ファイルの生成

次の手順は、SSL/TLS を使用して Host OnDemand (HOD) リダイレクタを使用する場合の、PKCS #12 ファイルの生成方法の概要を示しています。このタスクの実行の詳細については、HOD のマニュアルを参照してください。

▼ PKCS #12 ファイルを生成する: 一般的な手順

1 **IBM** 証明書管理ツールを使用して、新しい `HODServerKeyDb.kdb` ファイルを作成します。このファイルの一部として、新しい自己署名付き証明書をデフォルトのプライベート証明書として作成します。

`HODServerKeyDb.kdb` ファイルの作成時に、「証明書データベースにキーを追加しようとしてエラーが発生した」という内容のメッセージが表示された場合は、1 つ以上の信頼できる認証局証明書の期限が切れている可能性があります。IBM の Web サイトをチェックして、最新の証明書を取得します。

2 作成したプライベート証明書を **Base64 ASCII** として `cert.arm` ファイルにエクスポートします。

3 **IBM** 証明書管理ツールを使用して、`cert.arm` ファイルから署名者証明書にエクスポートされた証明書を追加することにより、`CustomizedCAs.p12` という名前の新しい **PKCS #12** ファイルを作成します。このファイルのパスワードとして `hod` を使用します。

トラブルシューティング

「セッションプロパティ」リソース属性に次の内容を追加することにより、HACL のトレースを有効にできます。

```
SESSION_TRACE
ECLSession=3 ECLPS=3 ECLCommEvent=3 ECLErr=3 DataStream=3 Transport=3 ECLPSEvent=3
```

注 – トレースパラメータは、改行文字を入れずに列挙してください。テキストボックス内でパラメータが折り返される場合は、そのままでかまいません。

Telnet/TN3270 サーバーにも、同じように利用できるログがあります。

WRQ による SSL 設定

Attachmate 3270 Mainframe Adapter for Sun Emulator Class Library は、IBM Host on Demand API と互換性があります。製品に付属するインストール手順に従ってください。続いて、Identity Manager で次の手順を実行します。

▼ WRQ で設定を行う

1 「セッションプロパティー」というリソース属性がリソースにまだ存在しない場合は、**[IDMIDE** テキストエンティティーを定義してください**]** またはデバッグページを使用して、この属性をリソースオブジェクトに追加します。`<ResourceAttributes>` セクションに、次の定義を追加します。

```
<ResourceAttribute name='Session Properties' displayName='Session Properties'
   description='Session Properties' multi='true'>
</ResourceAttribute>
```

2 リソースの「リソースパラメータ」ページに移動し、「セッションプロパティ」リソース属性に次の値を追加します。

```
encryptStream
true
hostURL
tn3270://hostname:SSLportkeystoreLocation
Path_To_Trusted_ps.pfx_file
```

ほかのリソースアダプタで **SSH** が使用されている場合の **Attachmate WRQ Libraries** の使用

Identity Manager 内で、SSH は JCraft クラスを使用して処理されます。このクラスは `jsch.jar` に含まれています。Sun 製品向け Attachmate 3270 メインフレームアダプタには、`RWebSDK.jar` に JCraft クラスのコピーが含まれています (実際には、Identity Manager は 3270 接続でこれらのクラスを使用しません)。2 つの JAR は同じバージョンの JCraft クラスを含んでいませんが、Web コンテナが JAR ファイルを読み込む順序によっては、競合が発生する可能性があります。

競合を避けるには、`RWebSDK.jar` をバックアップし、`RWebSDK.jar` を適切なツール (WinZip など) で編集し、`com.jcraft` クラスを削除したあと、ファイルを保存します。これにより、不要なバージョンの JCraft クラスが排除され、SSH は正しく機能するようになります。

`RWebSDK.jar` は、Identity Manager では配布されていません。Sun 製品用の Attachmate 3270 メインフレームアダプタの一部としてのみ使用できます。

◆ ◆ ◆ 第 54 章

SNC (Secure Network Communications) 接続の有効化

この章では、Access Enforcer、SAP、および SAP HR リソースアダプタが SNC (Secure Network Communications) を使用して安全に SAP システムと通信できるようにする方法について説明します。別のサードパーティー製品である Secude セキュリティーログインを入手する必要があります。この製品の詳細については、http://www.secude.com を参照してください。

SNC 接続を有効にするには、この製品をインストールして、Identity Manager の PSE (Personal Security Environment) を作成する必要があります。これらの作業の実行については、Secude セキュリティーログインの製品マニュアルを参照してください。

SNC 接続を有効にするには、次の作業を実行します。

SNC 通信のクレデンシャルの作成

SNC を正しく機能させるには、`cred_v2` という名前のクレデンシャルファイルを生成する必要があります。このファイルは、CREDDIR 環境変数で指定されたディレクトリに格納されます。このファイルに含まれるクレデンシャルを作成するには、`secude seclogin` コマンドを使用します。

```
$ secude seclogin -p idm.pse -a "Identity Manager" -O OS_User -l
```

`-a "Identity Manager"` 引数は省略可能です。`-O` 引数は、アプリケーションサーバーを実行するオペレーティングシステムユーザーの名前にするようにしてください。

Identity Manager の証明書の取得

SNC には、SAP システムとのセキュア接続を設定するための証明書が必要です。この証明書は、Identity Manager PSE から取得できます。この証明書を Identity Manager PSE からエクスポートし、base64 エンコーディングに変換する必要があります。

Identity Manager のアダプタ設定で使用する Base64 で符号化された証明書を取得するには、次のコマンドを使用します。最初のコマンドは、証明書を PKCS12 エンコーディングにエクスポートします。2 番目のコマンドは、この証明書を必要な base64 エンコーディングに変換します。

```
$ secude psemaint-p idm.pse export Cert PKCS12_File
$ secude encode -i 2048 PKCS12_File Base64_File
```

Identity Manager の識別名 (DN) の取得

Identity Manager PSE に含まれている証明書は、PSE の作成時に決定されました。PSE から Identity Manager の DN を取得するには、次のいずれかのコマンドを使用します。

UNIX の場合:

```
$ secude psemaint -p idm.pse show Cert 2>&1 | grep SubjectName
```

Windows の場合:

```
C:> secude psemaint -p idm.pse show Cert | findstr SubjectName
```

SAP システムの識別名 (DN) の取得

SAP システムの DN は、SAP システムにインストールされている証明書に含まれています。この DN を取得するには、SAP GUI を使用して SAP システムにログインします。

▼ SAP システムの DN を取得する

1. **STRUST** トランザクションを選択します。
2. 「**SNC (SAP Cryptolib)**」ノードを展開します。
3. **SAP** システムの証明書をダブルクリックして選択します。

4 右側のいちばん下の区画にある「所有者」フィールドが **DN** です。

Identity Manager アプリケーションサーバーの設定

Identity Manager のアプリケーションサーバーでは、次の環境変数を定義する必要があります。さらに、`CREDDIR` 変数で指定されたディレクトリに対する読み取り/書き込み権が必要です。

`CREDDIR` =*PathToPSELocation* (すべて)

`SNC_LIB`=*PathToSecudeLibrary*/ *secude_library* (すべて)

`LD_LIBRARY_PATH` =*PathToSecudeLibraries* (Solaris および Linux のみ)

`LIBPATH` =*PathToSecudeLibraries* (AIX のみ)

`SHLIB_PATH` =*PathToSecudeLibraries* (HP-UX のみ)

`PATH` =*PathToSecudeLibraries* (Windows のみ)

アダプタの設定

SAP アダプタには、SNC が正しく機能するために設定する必要のあるいくつかのリソースパラメータが必要です。この手順には、Identity Manager の証明書、Identity Manager の DN、および SAP システムの DN が必要です。

- SNC Protection Level。プライバシーのレベルを表す数値 (1 ～ 9)。この値は、SAP システムの値セットと一致する必要があります。
- SNC Name。先頭に `p:` を付加した、Identity Manager の識別名 (DN)。たとえば、`p:CN=IdentityManager,OU=IDM,O=Example,C=US` になります。
- SNC Partner Name。先頭に `p:` を付加した、SAP の DN。たとえば、`p:CN=SAPHost,OU=IDM,o=Example,c=us` になります。
- SNC X509 Certificate。Identity Manager の証明書を入力します。BEGIN および END CERTIFICATE の行を削除して、すべての改行文字を削除する必要があります。
- SNC ライブラリパス。SNC 暗号化ライブラリファイルのフルパス。ファイル拡張子 (`.so`、`.a`、または `.dll`) を含みます。

◆ ◆ ◆ 第 55 章

55 非推奨のリソースアダプタ

この章では、非推奨になったリソースアダプタの一覧を示します。これらの非推奨のアダプタについては、以前のバージョンの『リソースリファレンス』を参照してください。

非推奨のアダプタのリスト

表 55–1 非推奨のリソースアダプタ

アダプタ	**Comments**
ActivCard	置き換えのアダプタはありません。
Blackberry	代わりにスクリプトゲートウェイアダプタを使用します。 サンプルスクリプトは、`$WSHOME/web/sample/ScriptedGateway/BlackberryV4SampleScriptedGatewayObjects.xml` ファイルにあります。これらのスクリプトは、もとは「Microsoft Exchange とともに配備された場合の Blackberry Enterprise Server, Version 4.x のユーザー管理」のために提供されたユーティリティーに対してテストされました。これらのスクリプトは、正式にはサポートされていません。
Exchange 5.5	代わりに Windows Active Directory アダプタを使用します。
GroupWise	代わりに NetWare NDS アダプタを使用します。
LDAP Listener Active Sync	代わりに LDAP アダプタを使用します。
Natural	置き換えのアダプタはありません。
NDS Active Sync	代わりに NDS アダプタを使用します。
Siebel	代わりに Siebel CRM アダプタを使用します。

表 55–1 非推奨のリソースアダプタ (続き)

アダプタ	Comments
SQL Server	代わりに、MS SQL Server アダプタを使用します。
Sun ONE Identity Server	代わりに Sun Java System Access Manager または Sun Java System Access Manager レルムアダプタを使用します。
Sybase	代わりに Sybase ASE アダプタを使用します。
Windows NT	代わりに Windows Active Directory アダプタを使用します。

◆ ◆ ◆ 第 56 章

56 アイデンティティーコネクタの概要

この章では、Identity Manager で新しくサポートされた、アイデンティティーコネクタ機能について説明します。コネクタは、リソースアダプタに代わって、ネイティブリソースのアイデンティティーとその他のオブジェクトタイプをマッピングします。この章では、コネクタに関する次のトピックを紹介します。

アイデンティティーコネクタの開発と実装に関する最新情報については、`https://identityconnectors.dev.java.net` を参照してください。

アイデンティティーコネクタの概要

アイデンティティーコネクタは、リソースアダプタに似たコンポーネントで、Identity Manager とネイティブリソース (データベース、LDAP、ERP システムなど) との間のリンクを提供します。

アイデンティティーコネクタは、次の点でリソースアダプタよりも利点があります。

- 配備と開発が簡単になります。コネクタと Identity Manager の間には、リソースアダプタの場合ほど強い結び付きはありません。Java コネクタのバンドルを Web アプリケーション内の適切なディレクトリに配置するか、.NET バンドルをリモート .NET ディレクトリ内の適切なディレクトリに配置することで、管理可能なネイティブリソースのタイプをオンデマンドで拡張できます。Identity Manager は、新しく配備されたコネクタを自動的に検出します。

- コネクタのリリースサイクルは、Identity Manager のリリースサイクルに依存しません。コネクタのリリースと Identity Manager のリリースを同一にする必要がありません。現在使用している Identity Manager のバージョンに依存することなく、コネクタを配備に追加したり更新することができます。
- Identity Manager は、各コネクタを専用のクラスローダーで読み込みます。これにより、単一の Identity Manager サーバーでの、複数バージョンのネイティブ API の使用のサポートが強化されます。
- コネクタ (Java または .NET) の開発に、複雑でない独立したアイデンティティーコネクタ SPI を使用します。Identity Manager API を理解または使用する必要はありません。

既存のリソースからの移行

最終的には、リソースアダプタはコネクタに置き換えられます。ただし、このリリースでは、Identity Manager はこれまでのすべてのリソースアダプタをサポートします。厳密に移行を行う必要はありませんが、同等のコネクタを利用できる場合は移行することをお勧めします。

既存のリソースアダプタを置き換えることができる、新しいコネクタタイプを使用できる場合は、コネクタに切り替えられるように移行パスが用意されています。

一般的に、カスタマイズしたフォームやワークフローの数が多く複雑であるほど、変換プロセスは複雑になります。アダプタベースのリソースをコネクタベースのリソースに移行する準備を行うには、次の作業を実行します。

- 移行対象リソースに関連する既存のフォームおよびワークフローをすべて評価して、`searchFilter` が文字列に設定されているインスタンスを探します。
- これらを `connectorFilter` で置換します。`connectorFilter` エントリの値は、`<invoke>` により FilterBuilder クラスを使用して、フィルタのインスタンスとなります。

▼ コネクタベースのリソースに移行する: 一般的な手順

本稼働環境では、この移行を実行しないでください。移行では既存のリソースがインプレースアップグレードされ、既存のリソースは、これまでのリソースアダプタの代わりにコネクタを使用するように変更されます。リソースに対する以前のユーザーアカウントの割り当ては、すべて移行後も維持されます。移行では下位互換性が維持されるように十分に注意していますが、本稼働環境に進む前に、変換したリソースをテストすることを推奨します。

1 新しいコネクタをインストールします (まだインストールされていない場合)。

2. コネクタに用意されている **Identity Manager** に固有のインストール手順に従います。また、必要な **Exchange** ファイルもインポートします。

3. コネクタに用意されている移行手順の説明に従います。一般的には、「**Server Tasks**」、「**Run Tasks**」の順に選択して、宣言された移行サーバータスクを実行します。

コネクタの設定と管理

ここでは、配備で使用可能なコネクタを一覧表示する方法、コネクタコードをダウンロードする方法、コネクタのインストール方法、およびコネクタサーバーを登録する方法を説明します。次のトピックを説明します。

▼ 使用可能なコネクタを一覧表示する

このリリースでは、Identity Manager に Active Directory および SPML2 リソース用のコネクタが用意されています。これらのコネクタの詳細は、第 57 章「Active Directory コネクタ」および第 58 章「SPML コネクタ」を参照してください。

1. **Identity Manager** 管理インタフェースに、**Resource Administrator** 機能を持つ管理者としてログインします。

2. 「リソース」、「**Resource Type Actions**」、「管理するリソースの設定」の順に選択します。「**Resource Connectors**」領域に、**Identity Manager** で現在認識されているすべてのコネクタが表示されます。

コネクタのダウンロード

&Product_IDMgr がサポートするアイデンティティーコネクタは、`https://identityconnectors.dev.java.net` から追加ダウンロードできます。

Java コネクタのダウンロード

Identity Manager がサポートする Java コネクタは、1 つの JAR ファイルと 1 つの ZIP ファイルとして配布されます。ダウンロードするには、次の操作が必要です。

- JAR ファイルのバイナリを、Identity Manager Web アプリケーションの WEB-INF/bundles ディレクトリにコピーします。
- ZIP ファイルを Identity Manager Web アプリケーションに展開します。

詳細は、602 ページの「Java コネクタをインストールする」を参照してください。

.NET コネクタのダウンロード

Identity Manager がサポートする .NET コネクタは、2 つの ZIP ファイルとして配布されます。次の操作が必要です。

- 1 つの ZIP ファイルを、リモート .NET コネクタサーバーにインストールします。
- 別の ZIP ファイルを Identity Manager Web アプリケーションに展開します。

詳細は、「.NET コネクタのインストール」を参照してください。

Java コネクタのインストール

▼ Java コネクタをインストールする

Java コネクタは、1 つの JAR ファイルと 1 つの ZIP ファイルとして配信されます。

1. **Identity Manager Web** アプリケーションを停止します。
2. コネクタの **JAR** ファイルを、**Identity Manager Web** アプリケーションの **WEB-INF/bundles** ディレクトリにコピーします。
3. コネクタの **ZIP** ファイルを、**Identity Manager Web** アプリケーションのディレクトリに展開します。
4. **Identity Manager Web** アプリケーションを起動し、コネクタに固有のインストール手順に従います。

   これで、新しくインストールした Java コネクタが Identity Manager に認識されます。Identity Manager 管理者インタフェースに、Resource Administrator 機能を持つ管理者としてログインします。「リソース」、「Resource Type Actions」、「管理するリソースの設定」の順に選択し、新しい Java コネクタが一覧に表示されていることを確認します (LOCAL コネクタサーバーが関連付けらていれます)。
5. **(省略可能)** 新しいコネクタを使用する前に、**1** つ以上の **Exchange** ファイルのインポートが必要となる場合があります。

.NET コネクタのインストール

.NET コネクタを正常にインストールするには、次の手順が必要です。

- 603 ページの「.NET コネクタの実行可能 ZIP ファイルをインストールする」
- 603 ページの「.NET コネクタの Identity Manager ZIP ファイルをインストールする」

.NET の ZIP ファイルをインストールする前に、.NET コネクタサーバーをインストールして登録する必要があります。コネクタサーバーは 1 つまたは複数の .NET バンドルを管理し、Identity Manager と .NET バンドル間に送信される要求を処理します。.NET コネクタサーバーは、Identity Manager ゲートウェイに似ています。詳細は、次を参照してください。

- 604 ページの「.NET コネクタサーバーのインストール」
- 604 ページの「コネクタサーバーを登録する」

▼ .NET コネクタの実行可能 ZIP ファイルをインストールする

.NET コネクタバンドルは、2 つの ZIP ファイルとして配信されます。

注 – .NET コネクタの実行可能 ZIP ファイルをインストールする前に、.NET コネクタサーバーをインストールする必要があります。

.NET コネクタの実行可能 ZIP ファイルをインストールするには、次の手順に従います。

1. コネクタサーバーがすでにインストールされて実行中の場合は、**Connector Server** サービスを停止します。
2. **ZIP** ファイルをコネクタサーバーのインストールディレクトリに展開します。
3. **Connector Server** サービスを起動します。コネクタサーバーが **Identity Manager** でまだ宣言されていない場合は、「コネクタサーバーを登録する」を参照してください。

▼ .NET コネクタの Identity Manager ZIP ファイルをインストールする

1. **Identity Manager Web** アプリケーションを停止します。
2. コネクタの **ZIP** ファイルを、**Identity Manager Web** アプリケーションのディレクトリに展開し、**Identity Manager** を再起動します。
3. コネクタに固有のインストール手順に従います。
4. **(省略可能)** 新しいコネクタを使用する前に、**1** つ以上の **Exchange** ファイルのインポートが必要となる場合があります。

   この手順のあと、新しい .NET コネクタが Identity Manager に認識されるようになります。これを確認するには、Identity Manager 管理者インタフェースに、Resource Administrator 機能を持つ管理者としてログインします。「リソース」、「Resource Type Actions」、「管理するリソースの設定」の順に選択して、表に .NET コネクタが適切なコネクタサーバーとともに表示されることを確認します。

.NET コネクタサーバーのインストール

Identity Manager から .NET コネクタを使用する場合は、.NET コネクタサーバーをインストールして実行します。コネクタサーバーは 1 つまたは複数の .NET バンドルを管理し、Identity Manager と .NET バンドル間に送信される要求を処理します。.NET コネクタサーバーは、Identity Manager ゲートウェイに似ています。ただし、.NET コネクタサーバーは (コネクタを追加して) 簡単に拡張可能であり、コードが .NET で記述されている点が異なります。

コネクタサーバーを実行するマシンの最小の要件は、次のとおりです。

- Windows Server 2003 または 2008
- .NET 3.5 以降

コネクタサーバーを Windows ホストにインストールするには、`https://identityconnectors.dev.java.net` にある、コネクタサーバーのインストールに関する注意事項を参照してください。あとで使用するために、コネクタサーバーのインストールに関する次の情報を記録する必要があります。

- ホスト名または IP アドレス
- コネクタサーバーのポート
- コネクタサーバーのキー
- SSL が有効かどうか

新しくインストールしたコネクタサーバーを Identity Manager で宣言する方法については、604 ページの「コネクタサーバーを登録する」を参照してください。

▼ コネクタサーバーを登録する

各 .NET コネクタサーバーと通信するために必要な接続情報を、Identity Manager 内で宣言する必要があります。この接続情報が正しく宣言されていないと、Identity Manager は .NET コネクタサーバー内に配備された .NET コネクタにアクセスできません。

1. **Identity Manager** に、**Resource Administrator** 機能を持つ管理者としてログオンします。
2. 「設定」、「**Connector Servers**」の順に選択します。
3. 「**Connector Servers Definition**」ページで、「新規」をクリックします。
4. 「**New Connector Server**」で、必要なフィールドに入力します。各フィールドについては、オンラインヘルプを参照してください。
5. 「保存」をクリックします。**Identity Manager** がリモートコネクタサーバーと正常に通信できる場合は、新しいコネクタサーバー定義の「ステータス」列に「使用可能」と表示されます。

その他の管理に関するトピック

ここでは、Identity Manager 配備でのコネクタに関する次の管理タスクを説明します。

リソースが使用するコネクタサーバーまたはバージョンの変更

リソースを作成するときに、Identity Manager は選択したコネクタサーバーに関する情報をリソースオブジェクトに書き込みます。既存のリソースのコネクタサーバーを変更したり、コネクタのバージョンを変更することができます。

▼ リソースオブジェクト内のコネクタサーバー情報を変更する

1. 「リソース」ページで、編集するリソースを選択します。
2. 「リソースアクション」、「**Change Connector Parameters**」メニューオプションの順に選択します。選択できるのは、使用可能なコネクタのバージョンが少なくとも 1 つあるコネクタサーバーのみです。選択したコネクタサーバーで提供されるバージョンのみが表示されます。

コネクタベースリソースのタイムアウトの設定

コネクタベースのリソースを編集または作成するときに、Identity Manager は操作タイムアウトのフィールドセットを表示します。デフォルトでは、Identity Manager は操作タイムアウトの値を -1 に設定します。これは、タイムアウトが発生しないことを表します。このフィールドを 0 以外の値に設定すると、指定したタイムアウト間隔内にコネクタが操作を完了しないときに、操作がエラーによりタイムアウトします。Identity Manager は、タイムアウトの値を、`<OperationTimeouts>` タグ以下の Resource XML オブジェクトに格納します。値が -1 のタイムアウトは XML に格納されません。

接続プールのパラメータの編集

コネクタベースのリソースを編集するときに、リソースウィザードの最後のページに「Connector Pooling」の設定フィールドが表示されます。このページでは、次の属性に値を設定できます。

- `maxObjects`
- `maxIdle`
- `minIdle`
- `evictTimeout`
- `maxWait`

コネクタベースのリソースでのリソースアクションの使用

コネクタベースのリソースは、前アクションおよび後アクションとして使用するリソースアクションの定義に関して、アダプタベースのリソースと同じ規則に従います。Identity Manager は、作成、更新、削除、無効化、および有効化の操作を含む、前アクションと後アクションの使用をサポートします。

配備からのコネクタの削除

配備からコネクタを削除するには、コネクタに対応する .jar または DLL ファイルを削除します。コネクタを削除すると、Identity Manager はコネクタにアクセスできなくなります。Identity Manager リソースが実装で参照しているコネクタを配備から削除した場合、Identity Manager 内でそのリソースを使用すると、実行時エラーが発生します。この問題を避けるには、配備からコネクタを削除する前に Connectors-In-Use レポートを実行します。

デバッグとトラブルシューティング

Identity Manager のトレース機能

Identity Manager では、コネクタのパフォーマンスに関して次のタイプのトレースが用意されています。

- 607 ページの「API レイヤーのトレース」
- 607 ページの「Java コネクタに固有のトレース」
- 607 ページの「Java コネクタフフレームワークトレース」
- 607 ページの「.NET トレース」

注 – ローカル Java コネクタのトレースは、クラスレベルのみに制限されています。これは、ほかのクラスでサポートされているメソッドレベルのトレースとは異なります。Identity Manager は、リモートコネクタのトレースを管理する機能をサポートしていません。

API レイヤーのトレース

このレベルのトレースを使用すると、問題が Identity Manager 内にあるのか、またはコネクタ自身にあるのかを判断できます。このトレース方法は、リモートコネクタおよびローカルコネクタの両方で動作します。コネクタで API レベルのトレースを有効にするには、`org.identityconnectors.framework.impl.api.LoggingProxy` クラスでレベル 4 の Identity Manager トレースを有効にします。このタイプのトレースは、すべてのコネクタ API のメソッド呼び出しについて、引数と戻り値に注目します。

Java コネクタに固有のトレース

このレベルのトレースを使用すると、コネクタ内の問題をトラブルシューティングできます。このトレース方法は、ローカルの Java コネクタのみで動作します。このトレースを実装するには、コネクタ Java クラス (たとえば、`org.identityconnectors.datebasetable.DatabaseTableConnector`) で Identity Manager トレースを有効にします。コネクタコードによるすべてのログの呼び出しを、Identity Manager トレースファイルに出力します。

Java コネクタフフレームワークトレース

このトレースを実装するには、コネクタ Java クラス (たとえば、`org.identityconnectorsframework.*`) で Identity Manager トレースを有効にします。このトレース方法は、フレームワーク実装クラスによるすべての内部的なログ呼び出しで動作します。

.NET トレース

.NET コネクタは、標準の .NET トレース API を呼び出します。Identity Manager で集中管理されたトレースは行われません。Identity Manager では、.NET トレースファイルを表示できません。ローカルコネクタサーバーの設定ファイルを編集して、.NET トレースを設定する必要があります。

コネクタの JMX 監視

コネクタベースのリソースは、リソースアダプタベースのリソースと同じ標準の JMX 監視をサポートします。

- 標準 ActiveSync JMX

- 標準 (新規) リソース JMX

標準 Identity Manager トレースのデバッグページを使用して、ローカル Java コネクタのトレースを有効にできます。コネクタのログの呼び出しは、すべての Identity Manager トレースと同じトレースファイルに書き込まれます。

リモートコネクタのログは管理できません。リモートコネクタホストを実行しているマシンで、Windows のネイティブツールを使用して、リモートコネクタのログをローカルに設定する必要があります。

コネクタベースのリソースは、Identity Manager のほかの部分からは一般的なリソースと認識されるため、すでにリソースおよびリソースアダプタに用意されている JMX ツール (Active Sync JMX を含む) を使用して、コネクタベースのリソースの使用状況とパフォーマンスを監視できます。

コネクタフレームワーク API は、ローカル Java コネクタが使用する接続プールを維持します。現在のところ、この情報を表示または管理することはできません。リモートコネクタ用のコネクタ API でも、このためのツールは提供されていません。

◆ ◆ ◆ 第 57 章

57 Active Directory コネクタ

この章では、Active Directory コネクタのインストールと設定について説明します。Active Directory コネクタは、Active Directory リソースアダプタと重要な機能セットを共有します。

アイデンティティーコネクタのインストールと設定に関する最新情報については、`https://identityconnectors.dev.java.net` を参照してください。アイデンティティーコネクタの一般的な説明については、第 56 章「アイデンティティーコネクタの概要」を参照してください。

コネクタの詳細

バンドル名

Windows Active Directory コネクタ

バンドルバージョン

1.0.0.3663

リソースを設定する際の注意事項

ここでは、Identity Manager で使用する、次のコネクタベースの Active Directory リソースを設定する手順を説明します。

- コネクタサーバーの場所
- コネクタサーバーのサービスアカウント

コネクタサーバーの場所

「LDAP ホスト名」リソース属性が設定されていない場合、コネクタはディレクトリに対してサーバーレスバインドを実行します。サーバーレスバインドが機能するためには、ドメイン内にあって、管理対象のドメインまたはディレクトリを「認識している」システム上に、コネクタサーバーをインストールする必要があります。コネクタが管理するすべての Windows ドメインは、同じフォレストに所属している必要があります。フォレスト境界を越えるドメインの管理はサポートされていません。複数のフォレストがある場合は、各フォレストに少なくとも 1 つのコネクタをインストールしてください。

「LDAP ホスト名」リソース属性は、コネクタに特定の DNS ホスト名または IP アドレスとバインドするように指示します。これはサーバーレスバインドとは正反対です。ただし、LDAP ホスト名では、必ずしも特定のドメインコントローラを指定する必要はありません。AD ドメインの DNS 名を使用できます。コネクタの DNS サーバーが、その DNS 名に対して複数の IP アドレスを返すように設定されている場合、そのうちの 1 つがディレクトリバインドに使用されます。これによって単一のドメインコントローラに依存する必要がなくなります。

パススルー認証や前アクションと後アクションを含む一部の操作では、コネクタサーバーがドメインのメンバーであることが求められます。

コネクタサーバーのサービスアカウント

デフォルトでは、コネクタサーバーはローカルシステムアカウントとして実行されます。これは、「サービス」MMC スナップインで設定できます。

コネクタサーバーをローカルシステム以外のアカウントで実行する場合は、コネクタサーバーのサービスアカウントに「Act As Operating System」および「走査チェックのバイパス」ユーザー権限が必要です。ゲートウェイは、パススルー認証や、特定の状況でのパスワードの変更およびリセットに、これらの権限を使用します。

AD の管理の大部分は、リソース内で指定された管理アカウントを使用して行います。ただし、一部の操作はコネクタサーバーのサービスアカウントで実行します。つまり、コネクタサーバーのサービスアカウントに、これらの操作を実行するための適切なアクセス権が必要です。現在、これに該当する操作は次のとおりです。

- ホームディレクトリの作成
- 実行中のアクション (前アクションと後アクションを含む)

前アクションおよび後アクションのスクリプトを実行するときに、コネクタサーバーに「プロセスレベルトークンの置き換え」の権限が必要な場合があります。この権限は、コネクタサーバーが別のユーザー (リソース管理ユーザーなど) としてスクリプトのサブプロセスを実行しようとする場合に必要です。この場合、コネクタサーバーのプロセスには、そのサブプロセスに関連付けられたデフォルトのトークンを置き換える権限が必要です。

この権限がない場合は、サブプロセスの作成中に次のエラーが返されることがあります。

```
"Error creating process: A required privilege is not held by the client"
```

「プロセスレベルトークンの置き換え」権限は、デフォルトのドメインコントローラのグループポリシーオブジェクトと、ワークステーションおよびサーバーのローカルセキュリティーポリシーで定義されます。この権限をシステムに設定するには、「管理ツール」フォルダの「ローカルセキュリティーポリシー」アプリケーションを開き、「ローカルポリシー」>「ユーザー権利の割り当て」>「プロセスレベルトークンの置き換え」に移動します。

Identity Manager 上で設定する際の注意事項

コネクタサーバーの設定に関する最新情報については、`https://identityconnectors.dev.java.net/connector server.html` を参照してください。

使用上の注意

ここでは、Active Directory コネクタの使用に関連する依存関係と制限について示します。説明する内容は次のとおりです。

- パスワード履歴の確認
- Active Sync の設定
- パススルー認証用のドメインの指定

パスワード履歴の確認

エンドユーザーが自分のパスワードを変更するときに Active Directory アカウントのパスワード履歴を確認するには、AD パスワードを入力する必要があります。AD リソースでこの機能を有効にするには、「リソースパラメータ」ページで「変更時にユーザーがパスワードを入力」チェックボックスにチェックマークを付け、`WS_USER_PASSWORD` 属性をタイプを `encrypted` にしてアカウント属性に追加します。`WS_USER_PASSWORD` は、Identity Manager ユーザー属性およびリソースユーザー属性として追加する必要があります。

Active Sync の設定

Active Sync は常に同じドメインコントローラに接続する必要があるので、「子ドメインの検索」リソースパラメータが選択されていない場合は、特定のドメインコントローラのホスト名を指定するように LDAP ホスト名を設定します。「子ドメインの検索」オプションが選択されている場合は、「Sync Global Catalog Server」に特定のグローバルカタログサーバーを設定する必要があります。

新しいドメインコントローラに切り替えたときに発生する繰り返しイベントの数を制限する方法については、第 52 章「Active Directory Synchronization Failover」 を参照してください。

パススルー認証用のドメインの指定

デフォルト設定では、ユーザー ID とパスワードのみを送信することによって、パススルー認証が実現されます。これらの 2 つの属性は、`w2k_user` および `w2k_password` として、リソースオブジェクトの XML の `AuthnProperties` 要素で設定されます。ドメイン指定がない場合は、コネクタサーバーで既知の全ドメインが検索され、ユーザーを含むドメイン内のユーザー認証が試みられます。

信頼されたマルチドメイン環境では、次の 2 つの状況が考えられます。

- すべてのドメインに同期されたユーザー/パスワードの組み合わせが含まれる。
- ユーザー/パスワードの組み合わせがドメインに依存する。

ユーザー/パスワードの組み合わせが同期される場合は、Active Directory リソースが共通リソースとなるように設定します。共通リソースの設定については、『Business Administrator's Guide』を参照してください。

グローバルカタログにはフォレスト間の情報は含まれていないため、信頼される複数のドメインと Active Directory フォレストを含む環境では、これらの設定のいずれかを使用した認証に失敗する可能性があります。ドメイン数がロックアウトのしきい値よりも大きい場合は、ユーザーが不正なパスワードを入力すると、ユーザーのドメインでアカウントがロックアウトされる可能性もあります。

ユーザーがドメインに存在し、パスワードが同期されない場合は、ドメインでログインに失敗します。

1 つの Login Module Group で、ドメイン情報用に複数のデータソースを使用することはできません。

セキュリティーに関する注意事項

ここでは、サポートされる接続と特権の環境について説明します。

必要な管理特権

ここでは、必要な Active Directory のアクセス許可とパスワードのリセット権の要件について説明します。

Active Directory アクセス権

Active Directory リソース内で設定する管理アカウントには、Active Directory における適切なアクセス権が必要です。

表 57–1 Active Directory アクセス権

Identity Manager の機能	Active Directory アクセス権
Active Directory ユーザーアカウントの作成	ユーザーオブジェクトの作成 アカウントを有効な状態で作成するには、userAccountControl プロパティーの読み取り/書き込み権が必要です。パスワードの期限が切れた状態で作成するには、アカウント制限のプロパティーセット (userAccountControl プロパティーを含む) の読み取り/書き込みができるようにします。
Active Directory ユーザーアカウントの削除	ユーザーオブジェクトの削除
Active Directory ユーザーアカウントの更新	すべてのプロパティーの読み取り、すべてのプロパティーの書き込み 注意: プロパティーのサブセットのみが Identity Manager から管理されている場合は、これらのプロパティーのみに読み取りと書き込みのアクセスを許可できます。
AD ユーザーアカウントパスワードの変更/リセット AD ユーザーアカウントのロック解除 AD ユーザーアカウントの期限設定	ユーザーオブジェクトに関するアクセス許可: ■ 内容の一覧表示 ■ すべてのプロパティーの読み取り ■ 読み取りアクセス権 ■ パスワードの変更 ■ パスワードのリセット ユーザープロパティーに対するアクセス許可: ■ lockoutTime の読み取り/書き込み ■ アカウント制限の読み取り/書き込み ■ accountExpires の読み取り lockoutTime プロパティーに対するアクセス許可を設定するには、Windows 2000 Server リソースキットにある cacls.exe プログラムを使用してください。

パスワードのリセット

リソースオブジェクトの作成、削除、更新を実行する権限は期待するとおりのものです。アカウントには対応するオブジェクトタイプに対する作成権と削除権が必要で、ユーザーには、更新する必要のあるプロパティーに対する適切な読み取り/書き込み権が必要になります。

パススルー認証

Active Directory (AD) のパススルー認証をサポートするための要件は、次のとおりです。

- コネクタサーバーをユーザーとして実行するように設定する場合、そのユーザーアカウントには「Act As Operating System」および「走査チェックのバイパス」のユーザー権限が必要です。デフォルトでは、コネクタサーバーはローカルシステムアカウントとして実行され、このアカウントにはこれらの権限はすでに備わっています。また、「走査チェックのバイパス」ユーザー権限は、デフォルトですべてのユーザーに有効になっています。

注 – ユーザー権限を更新する必要のある場合、更新されたセキュリティーポリシーが伝播されるまでに遅延が生じる可能性があります。ポリシーが伝達されたら、コネクタサーバーを再起動する必要があります。

- 認証されるアカウントには、コネクタサーバーで「ネットワーク経由でコンピュータへアクセス」のユーザー権限が必要です。

コネクタサーバーでは、`LogonUser` 関数に `LOGON32_LOGON_NETWORK` ログオンタイプおよび `LOGON32_PROVIDER_DEFAULT` ログオンプロバイダを設定して、パススルー認証を実行します。`LogonUser` 関数は、Microsoft Platform Software Development Kit で提供されています。

プロビジョニングに関する注意事項

次の表に、このコネクタのプロビジョニング機能の概要を示します。

表 57–2 プロビジョニング機能

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	あり
パススルー認証	あり

表 57–2 プロビジョニング機能 (続き)

機能	サポート状況
前アクションと後アクション	あり Active Directory リソースは、前アクションと後アクションをサポートしています。これらのアクションは、ユーザーが要求を作成、更新、および削除するときに、コネクタサーバーでバッチスクリプトを使用してアクティビティーを実行します。詳細は、第 50 章「リソースへのアクションの追加」を参照してください。
データ読み込みメソッド	リソースから直接インポート リソースの調整 Active Sync

アカウント属性

属性の構文 (または型) は、通常、属性がサポートされるかどうかを決定します。一般に、Identity Manager は boolean 型、文字列型、および整数型の構文をサポートします。バイナリ文字列と、それに類似した構文はサポートされていません。

属性構文のサポート

ここでは、サポートされるアカウント構文とサポートされないアカウント構文について説明します。

サポートされる構文

次の表に、Identity Manager でサポートされている Active Directory 構文を示します。

表 57–3 サポートされる構文のリスト

AD 構文	Identity Manager の構文	構文 ID	OM ID	ADS タイプ
Boolean	Boolean	2.5.5.8	1	ADSTYPE_BOOLEAN
Enumeration	String	2.5.5.9	10	ADSTYPE_INTEGER
Integer	Int	2.5.5.9	2	ADSTYPE_INTEGER
DN String	String	2.5.5.1	127	ADSTYPE_DN_STRING

表 57–3 サポートされる構文のリスト (続き)

AD 構文	Identity Manager の構文	構文 ID	OM ID	ADS タイプ
Presentation Address	String	2.5.5.13	127	ADSTYPE_CASE_IGNORE_STRING
IA5 String	String	2.5.5.5	22	ADSTYPE_PRINTABLE_STRING
Printable String	String	2.5.5.5	19	ADSTYPE_PRINTABLE_STRING
Numeric String	String	2.5.5.6	18	ADSTYPE_NUMERIC_STRING
OID String	String	2.5.5.2	6	ADSTYPE_CASE_IGNORE_STRING
Case Ignore String (teletex)	String	2.5.5.4	20 人	ADSTYPE_CASE_IGNORE_STRING
Unicode String	String	2.5.5.12	64	ADSTYPE_OCTET_STRING
Interval	String	2.5.5.16	65	ADSTYPE_LARGE_INTEGER
LargeInteger	String	2.5.5.16	65	ADSTYPE_LARGE_INTEGER

サポートされない構文

次の表に、Identity Manager でサポートされない Active Directory 構文を示します。

表 57–4 サポートされない Active Directory の構文

構文	構文 ID	OM ID	ADS タイプ
DN with Unicode string	2.5.5.14	127	ADSTYPE_DN_WITH_STRING
DN with binary	2.5.5.7	127	ADSTYPE_DN_WITH_BINARY
OR-Name	2.5.5.7	127	ADSTYPE_DN_WITH_BINARY
Replica Link	2.5.5.10	127	ADSTYPE_OCTET_STRING
NT Security Descriptor	2.5.5.15	66	ADSTYPE_NT_SECURITY_DESCRIPTOR
Octet String	2.5.5.10	4	ADSTYPE_OCTET_STRING
SID String	2.5.5.17	4	ADSTYPE_OCTET_STRING
UTC Time String	2.5.5.11	23	ADSTYPE_UTC_TIME
Object(Access-Point)	2.5.5.14	127	n/a

Identity Manager は、Replica Link 構文を使用する jpegPhoto および thumbnailPhoto アカウント属性をサポートしています。これ以外にもサポートされている Replica Link 属性があるかもしれませんが、それらはテストが完了していません。

アカウント属性のサポート

ここでは、Identity Manager によってサポートされる Active Directory アカウント属性とサポートされない Active Directory アカウント属性を説明します。

サポートされるアカウント属性

次の表に、Identity Manager でサポートされるアカウント属性を示します。ほかの属性がサポートされる場合もあります。

これらの属性については、第 6 章「Active Directory」を参照してください。

表 57–5　ACCOUNT オブジェクトクラスの属性

名前	属性タイプ	作成	更新	複数値の許可
sAMAccountName	String	あり	なし	なし
givenName	String	あり	あり	なし
sn	String	あり	あり	なし
displayName	String	あり	あり	なし
mail	String	あり	あり	なし
telephoneNumber	String	あり	あり	なし
employeeID	String	あり	あり	なし
division	String	あり	あり	なし
mobile	String	あり	あり	なし
middleName	String	あり	あり	なし
description	String	あり	あり	あり
department	String	あり	あり	あり
manager	String	あり	あり	あり
title	String	あり	あり	あり
initials	String	あり	あり	あり
co	String	あり	あり	あり
company	String	あり	あり	あり
facsimileTelephoneNumber	String	あり	あり	あり
homePhone	String	あり	あり	あり

表 57–5 ACCOUNT オブジェクトクラスの属性 (続き)

名前	属性タイプ	作成	更新	複数値の許可
streetAddress	String	あり	あり	あり
l	String	あり	あり	あり
st	String	あり	あり	あり
postalCode	String	あり	あり	あり
TerminalServicesInitialProgram	String	なし	なし	あり
TerminalServicesWorkDirectory	String	あり	あり	あり
AllowLogon	Integer	あり	あり	あり
MaxConnectionTime	Integer	あり	あり	あり
MaxDisconnectionTime	Integer	なし	なし	あり
MaxIdleTime	Integer	あり	あり	あり
ConnectClientDrivesAtLogon	Integer	なし	なし	あり
ConnectClientPrintersAtLogon	Integer	なし	なし	あり
DefaultToManPrinter	Integer	なし	なし	あり
BrokenConnectionAction	Integer	なし	なし	あり
ReconnectionAction	Integer	なし	なし	あり
EnableRemoteControl	Integer	なし	なし	あり
TerminalServicesProfilePath	String	なし	なし	あり
TerminalServicesHomeDirectory	String	なし	なし	あり
TerminalServicesHomeDrive	String	なし	なし	あり
uSNChanged	String	なし	なし	あり
ad_container	String	なし	なし	あり
otherHomePhone	String	あり	あり	あり
distinguishedName	String	なし	なし	あり
objectClass	String	なし	なし	あり
homeDirectory	String	あり	あり	あり
PasswordNeverExpires	Boolean	あり	あり	あり

表 57–6 GROUP オブジェクトクラスの属性

名前	属性タイプ	作成	更新	複数値の許可
cn	String	なし	なし	あり
samAccountName	String	あり	あり	あり
description	String	あり	あり	あり
displayName	String	なし	なし	あり
managedBy	String	あり	あり	あり
mail	String	あり	あり	あり
groupType	Int	あり	あり	あり
objectClass	String	なし	なし	あり
member	String	なし	なし	あり
ad_container	String	なし	なし	あり

表 57–7 organizationalUnit オブジェクトクラスの属性

名前	属性タイプ	作成	更新	複数の属性の許可
ou	String	なし	なし	なし
displayName	String	なし	なし	なし

リソースオブジェクトの管理

Identity Manager は、次の Active Directory オブジェクトをサポートします。

表 57–8 サポートされる Active Directory オブジェクト

リソースオブジェクト	サポートされる機能	管理される属性
Group	作成、更新、削除	cn、samAccountName、description、managedby、member、mail、groupType、authOrig、name
DNS Domain	Find	dc
Organizational Unit	作成、削除、検索	ou
Container	作成、削除、検索	cn、description

リソースオブジェクト上で管理できる属性は、一般に、属性構文によって指示することもできます。これらのオブジェクトタイプの属性は、ユーザーアカウントの属性と類似しているので、同じようにサポートされています。

アイデンティティーテンプレート

Windows Active Directory は、階層ベースのリソースです。アイデンティティーテンプレートによって、ユーザーが作成するディレクトリツリー内のデフォルトの場所が指定されます。デフォルトのアイデンティティーテンプレートは次のとおりです。

```
CN=$fullname$,CN=Users,DC=mydomain,DC=com
```

デフォルトのテンプレートを有効な値に置き換えてください。

サンプルフォーム

ここでは、Active Directory リソースアダプタに用意されているサンプルフォームの一覧を示します。

組み込みのフォーム

- Active Directory ActiveSync フォーム
- Windows Active Directory コンテナ作成フォーム
- Windows Active Directory グループ作成フォーム
- Windows Active Directory 組織単位作成フォーム
- Windows Active Directory Create Person Form
- Windows Active Directory ユーザー作成フォーム
- Windows Active Directory コンテナ更新フォーム
- Windows Active Directory グループ更新フォーム
- Windows Active Directory 組織単位更新フォーム
- Windows Active Directory Update Person Form
- Windows Active Directory ユーザー更新フォーム

その他の利用可能なフォーム

```
ADUserForm.xml
```

トラブルシューティング

ログとトレースの情報については、第 56 章「アイデンティティーコネクタの概要」を参照してください。

◆ ◆ ◆ 第 58 章

58 SPML コネクタ

ここでは、SPML2 コネクタの接続と設定について説明します。

アイデンティティーコネクタのインストールと設定に関する最新情報については、`https://identityconnectors.dev.java.net` を参照してください。アイデンティティーコネクタの一般的な説明については、第 56 章「アイデンティティーコネクタの概要」を参照してください。

コネクタの詳細

`

バンドル名

SPML

バンドルバージョン

1.0

サポートされるネイティブリソース

DSML スキーマを使用する SPML 2.0 サーバー

設定の注意点

接続パラメータ

SPML コネクタには、次の設定パラメータがあります。

表 58–1 SPML 接続パラメータ

接続パラメータ	説明
`Login user`	SPML 2 サーバーに接続するときに使用するユーザー名
`password`	SPML 2 サーバーに接続するときに使用するパスワード
`Target System Url`	SPML 2 サーバーの URL

スクリプトパラメータ

スクリプトパラメータには、スクリプト作成に使用するスクリプト言語を定義する `scripting language` が含まれます。コネクタフレームワークには Groovy サポートが含まれます。SPML 2.0 はセッションを確立および維持する方法を指定しないため、SPML 2.0 コネクタでは、実行中に指定したポイントでスクリプトを実行して、セッション管理を実行できます。これらの実行のポイントは次のとおりです。

- 接続を確立したあと
- 要求を送信する前
- 応答を受信したあと
- 接続を破棄する前

接続を確立したあと、次の変数を定義して Post-Connect スクリプトが実行されます。

表 58–2 Post-Connect スクリプトの変数

スクリプト変数	説明
`connection`	確立された com.sun.openconnectors.framework.spi.Connection
`username`	接続で指定したユーザー名
`password`	接続で指定したパスワード
`memory`	スクリプトの実行間で持続される java.util.Map

要求が送信される前に、次の変数を定義して Pre-Send スクリプトが実行されます。

表 58–3 Per-Send スクリプトの変数

スクリプト変数	説明
request	送信される org.openspml.v2.msg.Request
memory	スクリプトの実行間で持続される java.util.Map

応答を受信したあと、次の変数を定義して Post-Receive スクリプトが実行されます。

表 58–4 Post-Receive スクリプトの変数

スクリプト変数	説明
response	受信した org.openspml.v2.msg.Response
memory	スクリプトの実行間で持続される java.util.Map

接続を終了する前に、次の変数を定義して Pre-Disconnect スクリプトが実行されます。

表 58–5 Pre-Disconnect スクリプトの変数

スクリプト変数	説明
connection	終了する com.sun.openconnectors.framework.spi.Connection
username	接続で指定したユーザー名
password	接続で指定したパスワード
memory	スクリプトの実行間で持続される java.util.Map

これらに加えて、属性がサーバーに送信される前や、サーバーから返される属性を受け取ったあと、属性を変更するスクリプトを実行できます。コネクタフレームワークは、サーバーで使用される名前に対応していない属性に対して予約語を使用するため (たとえば、名前に対して NAME)、このスクリプトが必要になる場合があります。

作成および変更操作中にスクリプトを実行して、属性の名前を変更できます。このスクリプトは使用する名前を返します。Map 'set' Name スクリプトでは、次の変数を使用できます。

表 58–6 Map 'set' Name スクリプトの変数

スクリプト変数	説明
name	属性の名前

表 58–6 Map 'set' Name スクリプトの変数 (続き)

スクリプト変数	説明
objectclass	オブジェクトクラスの名前
configuration	SPML 設定オブジェクト
memory	スクリプトの実行間で持続される java.util.Map

検索操作の結果として返される属性を変更するスクリプトを実行できます。スクリプトは使用する属性を返します。Map Attribute スクリプトでは、次の変数を使用できます。

表 58–7 Map Attribute スクリプトの変数

スクリプト変数	説明
attribute	com.sun.openconnectors.framework.common.objects.属性
objectClass	オブジェクトクラスの名前
configuration	SPMLConfiguration オブジェクト
memory	スクリプトの実行間で持続される java.util.Map

クエリー操作中に返される属性を変更するスクリプトを実行できます。スクリプトは使用する名前を返します。Map 'query' Name スクリプトは使用する名前を返します。

表 58–8 Map 'query' Name スクリプトの変数

スクリプト変数	説明
name	属性の名前
configuration	SPML 設定オブジェクト
memory	スクリプトの実行間で持続される java.util.Map

最後に、SPML のオブジェクトクラスとコネクタフレームワークのオブジェクトクラスのマッピングを指定する必要があります。この操作には、サポートされるコネクタフレームワークのオブジェクトクラス (たとえば、__ACCOUNT__) ごとに 1 つの行と、次の情報を含む 4 つの列を含むテーブルを使用します。

- コネクタフレームワークのオブジェクトクラス名
- SPML オブジェクトクラス名
- オブジェクトクラスを含む SPML ターゲット

- `org.identityconnectors.framework.common.objects.Name` にマップされる SPML オブジェクトクラスの属性

使用上の注意

サードパーティーからの注意事項

なし

デフォルトスキーマ

OperationalAttributes.PASSWORD_NAME (「パスワード」機能が設定されている場合)

OperationalAttributes.ENABLE_NAME (「サスペンド」機能が設定されている場合)

さらに、DSML スキーマで報告される属性が追加されます。

プロビジョニングに関する注意事項

次の表に、このアダプタのプロビジョニング機能の概要を示します。

機能	サポート状況
アカウントの有効化/無効化	あり
アカウントの名前の変更	なし
パススルー認証	なし
前アクションと後アクション	なし
データ読み込みメソッド	リソースから直接インポート、リソースの調整

索引

C

D

E

F

G

H

M

N

R

S

T

U

V

W

X

ス

名

有