Sun Java System Access Manager 7 2005Q4 管理ガイド

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

Part No: 819–3481

060411@14774

目次

はじめに

『Sun Java System Access Manager 7 2005Q4 管理ガイド』では、Sun Java™ System Access Manager コンソールの使用法、およびコマンド行インタフェースでユーザーとサービスのデータを管理する方法について説明します。

Access Manager は、Sun Java Enterprise System (Java ES) のコンポーネントです。Java ES は、ネットワーク環境またはインターネット環境に分散するエンタープライズアプリケーションのサポートに必要なサービスを提供する一連のソフトウェアコンポーネントです。

対象読者

本書は、Sun Java System のサーバーとソフトウェアを使用して Web アクセスプラットフォームを実装する IT 管理者およびソフトウェア開発者を対象としています。

お読みになる前に

本ガイドを読まれる方は、次の技術に精通していることが必要です。

- 『Sun Java System Access Manager 7 2005Q4 Technical Overview』で説明されている Access Manager の技術的概念
- 配備先プラットフォーム: Solaris または Linux オペレーティングシステム
- Access Manager を実行する Web コンテナ: Sun Java System Application Server、Sun Java System Web Server、BEA WebLogic、または IBM WebSphere Application Server
- 技術的概念: LDAP (Lightweight Directory Access Protocol)、Java テクノロジ、JavaServer Pages (JSP) テクノロジ、ハイパーテキスト転送プロトコル (HTTP)、ハイパーテキストマークアップ言語 (HTML)、および XML (eXtensible Markup Language)

関連マニュアル

以下の関連マニュアルが用意されています。

- 14 ページの「Access Manager の主要マニュアル」
- 15 ページの「Sun Java Enterprise System 製品のマニュアル」

Access Manager の主要マニュアル

Access Manager の主要マニュアルセットには、以下のタイトルが含まれます。

- 『Sun Java System Access Manager 7 2005Q4 リリースノート』は、製品のリリース後にオンラインで参照できます。このリリースの最新情報の説明、既知の問題と制限事項、インストールに関する注意事項、ソフトウェアまたはマニュアルに関する問題の報告方法など、最新の情報を提供します。
- 『Sun Java System Access Manager 7 2005Q4 Technical Overview』は、Access Manager コンポーネントがどのように連携してアクセス制御機能を統合し、企業資産や Web ベースアプリケーションを保護するかについて、その概要を示します。Access Manager の基本的な概念と用語についても説明します。
- 『Sun Java System Access Manager 7 2005Q4 配備計画ガイド』は、ソリューションのライフサイクルに基づく Sun Java System Access Manager の計画と配備のソリューションを示します。
- 『Sun Java System Access Manager 7 2005Q4 Performance Tuning Guide』は、Access Manager とその関連コンポーネントを調整して最適なパフォーマンスを得る方法について説明します。
- 『Sun Java System Access Manager 7 2005Q4 管理ガイド』は、Access Manager コンソールの使用法、およびコマンド行インタフェースでユーザーとサービスのデータを管理する方法について説明します。
- 『Sun Java System Access Manager 7 2005Q4 Federation and SAML Administration Guide』は、Liberty Alliance Project 仕様に基づく Federation モジュールに関する情報を提供します。Liberty Alliance Project 仕様に基づく統合サービスに関する情報、Liberty ベースの環境を有効にするための手順、フレームワークを拡張するためのアプリケーションプログラミングインタフェース (API) の概要などが含まれます。
- 『Sun Java System Access Manager 7 2005Q4 Developer's Guide』は、Access Manager をカスタマイズし、組織の現在の技術インフラストラクチャーにその機能を統合する方法について説明します。製品とその API のプログラミングに関する情報も含まれます。
- 『Sun Java System Access Manager 7 2005Q4 C API Reference』は、Access Manager の公開された C API を構成するデータ型、構造体、および関数の概要を示します。
- 『Java API Reference 』(Part No. 819-2141) は、Access Manager の Java パッケージの実装に関する情報を提供します。
- 『Sun Java System Access Manager Policy Agent 2.2 User's Guide』は、Access Manager で利用可能なポリシー機能とポリシーエージェントの概要を示します。

『リリースノート』の更新と主要マニュアルの訂正へのリンクは、Sun Java Enterprise System ドキュメントの Web サイトの Access Manager のページにあります。更新されたマニュアルには、改訂日が記載されています。

Sun Java Enterprise System 製品のマニュアル

次の製品のマニュアルを参照すると、役に立つ情報が見つかることがあります。

- Directory Server
- Web Server
- Application Server
- Web Proxy Server

関連するサードパーティーの Web サイトの参照

このマニュアルでは、追加の関連情報を示すためにサードパーティーの URL を参照しています。

注 – このマニュアルに記載されたサードパーティーの Web サイトの利用可能性について Sun は責任を負いません。これらのサイトや情報源を通して入手される内容、広告、製品、およびその他の資料について、Sun は保証することも、賠償責任などの責任を負うこともありません。これらのサイトや情報源を通して入手される内容、物品、およびサービスを使用または信用することにより発生する、または発生したと主張される、実際の、または申し立てられている損害や損失について、Sun は賠償責任などいかなる責任も負いません。

マニュアル、サポート、およびトレーニング

Sun のサービス	URL	内容
マニュアル	http://jp.sun.com/documentation/	PDF 文書および HTML 文書をダウンロードできます。
サポートおよびトレーニング	http://jp.sun.com/supportraining/	技術サポート、パッチのダウンロード、および Sun のトレーニングコース情報を提供します。

表記上の規則

このマニュアルでは、次のような字体や記号を特別な意味を持つものとして使用します。

表 P–1 表記上の規則

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、コード例を示します。	.login ファイルを編集します。 ls -a を使用してすべてのファイルを表示します。 machine_name% you have mail.
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区別して示します。	machine_name% **su** Password:
aabbcc123	変数を示します。実際に使用する特定の名前または値で置き換えます。	ファイルを削除するには、rm *filename* と入力します。
『』	参照する書名を示します。	『コードマネージャー・ユーザーズガイド』を参照してください。
「」	参照する章、節、ボタンやメニュー名、強調する単語を示します。	第 5 章「衝突の回避」を参照してください。 この操作ができるのは、「スーパーユーザー」だけです。
\	枠で囲まれたコード例で、テキストがページ行幅を超える場合に、継続を示します。	sun% **grep '^#define ** **XV_VERSION_STRING'**

コード例は次のように表示されます。

- C シェル

  machine_name% **command y|n** [*filename*]

- C シェルのスーパーユーザー

  machine_name# **command y|n** [*filename*]

- Bourne シェルおよび Korn シェル

  $ **command y|n** [*filename*]

- Bourne シェルおよび Korn シェルのスーパーユーザー

```
# command y|n [filename]
```

[ ] は省略可能な項目を示します。上記の例は、*filename* は省略してもよいことを示しています。

| は区切り文字 (セパレータ) です。この文字で分割されている引数のうち 1 つだけを指定します。

キーボードのキー名は英文で、頭文字を大文字で示します (例: Shift キーを押します)。ただし、キーボードによっては Enter キーが Return キーの動作をします。

ダッシュ (-) は 2 つのキーを同時に押すことを示します。たとえば、Ctrl-D は Control キーを押したまま D キーを押すことを意味します。

コメントの送付先

Sun では、マニュアルの改善のために、皆様からのコメントおよび提案をお待ちしております。

コメントを送るには、http://docs.sun.com にアクセスして「コメントの送信」をクリックしてください。オンラインフォームに、マニュアルのタイトルと Part No. を入力してください。Part No. は、マニュアルのタイトルページか先頭に記述されている 7 桁または 9 桁の番号です。

たとえば、このマニュアルのタイトルは『Sun Java System Access Manager 7 2005Q4 管理ガイド』で、Part No. は 819-3481 です。

パ ー ト I

Access Managerの設定

これは『Sun Java System Access Manager™ 7 2005Q4 管理ガイド』の第 1 部です。Access Manager のインストール後に実行できる設定オプションについて説明します。次の章で構成されています。

◆ ◆ ◆ 第 1 章

Access Manager 7 2005Q4 の設定スクリプト

この章では、amconfig スクリプトとサイレントモード入力ファイルのサンプル (amsamplesilent) を使って Sun Java™ System Access Manager を設定および配備する方法について説明します。内容は次のとおりです。

Access Manager 7 2005Q4 インストール概要

新たにインストールする場合は、Sun Java Enterprise System (Java ES) インストーラを実行して、常に Access Manager 7 2005Q4 の最初のインスタンスをインストールします。インストーラを実行すると、Access Manager の設定オプションから次のうちどちらかを選択できます。

- 「今すぐ設定」オプションでは、Access Manager インストールパネル上で選択した内容 (またはデフォルトの内容) で、インストール中に最初のインスタンスを設定します。
- 「あとで設定」オプションでは、Access Manager 7 2005Q4 のコンポーネントをインストールしたあと、インストール後にそれらを手動で設定するか、39 ページの「Access Manager のインスタンスの設定と再設定」の説明に従って Access Manager スクリプトを実行する必要があります。このオプションを選択すると、現在インストールしている製品はどれも設定されません。たとえば、Access Manager と Application Server のインストールを選択し、「あとで設定」オプションを選択すると、どちらのアプリケーションも設定されません。

注 – Access Manager Web コンテナとして BEA WebLogic または IBM WebSphere Application Server をインストールしている場合、Access Manager のインストール時に「あとで設定」オプションを選択する必要があります。詳細については、第 2 章を参照してください。

インストーラの詳細については、『Sun Java Enterprise System 2005Q4 Installation Guide for UNIX』 を参照してください。

Java Enterprise System インストーラは、Access Manager 7 2005Q4 の `amconfig` スクリプトとサンプルのサイレントモード入力ファイル (`amsamplesilent`) を、Solaris システムの場合は *AccessManager-base* `/SUNWam/bin` ディレクトリに、Linux システムの場合は *AccessManager-base*`/identity/bin` ディレクトリに、それぞれインストールします。

AccessManager-base は、Access Manager のベースインストールディレクトリを表します。デフォルトのベースインストールディレクトリは、Solaris システムでは `/opt` であり、Linux システムでは `/opt/sun` となります。しかし、インストーラを実行する際、必要に応じて別のディレクトリを指定することもできます。

`amconfig` スクリプトは最上位レベルのスクリプトで、要求された処理を実行する際、必要に応じてほかのスクリプトを呼び出します。詳細については、36 ページの「Access Manager の `amconfig` スクリプト」を参照してください。

サンプルの設定スクリプト入力ファイル (`amsamplesilent`) は、`amconfig` スクリプトをサイレントモードで実行するときに指定する必要がある入力ファイルの作成に使用できるテンプレートです。

このサンプルの設定スクリプト入力ファイルは、Access Manager の設定変数を格納した ASCII テキストファイルです。`amconfig` スクリプトを実行する前に、`amsamplesilent` ファイルをコピー (および、必要に応じて名前を変更) し、各自のシステム環境に基づいてファイル内の変数を編集します。設定変数は次のような構成になっています。

変数名=値

次に例を示します。

```
DEPLOY_LEVEL=1
 NEW_INSTANCE=true
 SERVER_HOST=ishost.example.com
```

設定スクリプト入力ファイルで設定できる変数のリストについては、23 ページの「Access Manager の設定スクリプト入力ファイルのサンプル」を参照してください。

注意 – amconfig スクリプトをサイレントモードで実行するときに使用するサンプルの設定スクリプト入力ファイルの形式は、Java Enterprise System のサイレントインストールの状態ファイルの形式には従わず、また必ずしも同じ変数名を使用するとは限りません。このファイルには、管理者パスワードなどの機密データが含まれています。このファイルは、必要に応じてセキュリティー保護するか、削除してください。

Access Manager の amconfig スクリプト処理

Sun Java Enterprise System インストーラを使用して Access Manager の最初のインスタンスをインストールしたあと、amconfig スクリプトを実行して、サイレントモード入力ファイル内の変数の値に応じた次の操作を行うことができます。

- Access Manager の最初のインスタンスを配備し設定します。または、同じホストシステム上に Access Manager の追加インスタンスを配備し設定します。たとえば、Web コンテナの追加のインスタンスを設定したあと、その Web コンテナのインスタンス用の新しい Access Manager インスタンスの配備と設定ができます。
- Access Manager の最初のインスタンスと、すべての追加インスタンスの両方を再設定します。
- Access Manager のすべてのサーバーサービスまたは SDK サービスのみを配備し設定します。これにより、次の製品に対するサポートを有効にします。
  - BEA WebLogic
  - IBM WebSphere Application Server

  コンソールや連携管理モジュールなどの、特定の Access Manager コンポーネントを配備し設定します。
- amconfig スクリプトを使って配備した Access Manager のインスタンスやコンポーネントをアンインストールします。

Access Manager の設定スクリプト入力ファイルのサンプル

Java Enterprise System インストーラの実行後は、Access Manager の設定スクリプト入力ファイルのサンプル (amsamplesilent) が、Solaris システムでは *AccessManager-base*/SUNWam/bin ディレクトリに、Linux システムでは *AccessManager-base*/identity/bin ディレクトリにあります。

設定変数を設定するには、まず、amsamplesilent ファイルをコピーしてファイル名を変更します。次に、コピーしたファイル内の変数を、実行したい処理に合わせて変更します。このファイルの例については、42 ページの「設定スクリプト入力ファイルの例」を参照してください。

このサイレントモード入力ファイルのサンプルには、次のような設定変数があります。

配備モード変数

この節では、必要な DEPLOY_LEVEL 変数の値を説明しています。この変数は、`amconfig` スクリプトが実行する処理を規定します。

表 1–1 Access Manager DEPLOY_LEVEL 変数

処理	**DEPLOY_LEVEL** 変数の値と説明
インストール	1 = 新しいインスタンスに対して、Access Manager を完全インストール (デフォルト) 2 = Access Manager のコンソールのみをインストール 3 = Access Manager SDK コンソールのみをインストール 4 = SDK のみをインストールし、コンテナを設定 5 = 連携管理モジュールのみをインストール 6 = サーバーのみをインストール 7 = Access Manager をインストールし、Portal Server とともに配備するようにコンテナを設定 注意: DEPLOY_MODE=7 は、Access Manager を Portal Server とともに配備する場合にのみ使用します。 配備方法によっては、異なる Web コンテナを使用して、1 つのホストサーバー上にコンソールのみ、またはサーバーのみをインストールした方がよいことがあります。最初に Java ES インストーラを実行して、「あとで設定」オプションを使用してすべての Access Manager サブコンポーネントをインストールします。次に、`amconfig` スクリプトを実行してコンソールとサーバーのインスタンスを設定します。

表 1–1 Access Manager DEPLOY_LEVEL変数　(続き)

処理	DEPLOY_LEVEL変数の値と説明
アンインストール (設定解除)	11 = 完全にアンインストール 12 = コンソールのみをアンインストール 13 = SDK のみをアンインストール 14 = SDK のみをアンインストールし、コンテナの設定を解除 15 = 連携管理をアンインストール 16 = サーバーのみをアンインストール 17 = Portal Server とともに配備されている場合、Access Manager をアンインストールし、コンテナの設定を解除 注意: DEPLOY_MODE=17 は、Access Manager が Portal Server とともに配備されている場合にのみ使用します。
再インストール (再配備または再設定とも呼ぶ)	21 = すべての (コンソール、パスワード、サービス、共通) Web アプリケーションを再配備します。 26 = すべての (コンソール、パスワード、サービス、共通) Web アプリケーションの配備を取り消します。

Access Managerの設定変数

この節では、Access Manager の設定変数について説明します。

表 1–2 Access Manager の設定変数

変数	説明
AM_REALM	Access Manager のモードを指示します。 ■ enabled: Access Manager は、Access Manager 7 2005Q4 の機能およびコンソールを使用してレルムモードで動作します。 ■ disabled: Access Manager は、Access Manager 6 2005Q1 の機能およびコンソールを使用する旧バージョンモードで動作します。 デフォルト: enabled 注意 – デフォルトでは、Access Manager レルムモードは有効になっています。Access Manager を Portal Server、Messaging Server、Calendar Server、Delegated Administrator、または Instant Messaging とともに配備している場合、`amconfig` スクリプトを実行する前に旧バージョンモード (AM_REALM=disabled) を選択する必要があります。

表 1–2 Access Managerの設定変数　(続き)

変数	説明
BASEDIR	Access Managerパッケージをインストールするベースディレクトリ。 デフォルト: PLATFORM_DEFAULT Solarisシステムでは PLATFORM_DEFAULT は `/opt` Linuxシステムでは PLATFORM_DEFAULT は `/opt/sun`
SERVER_HOST	Access Managerが実行中 (またはインストール予定) であるシステムの完全修飾ホスト名。 リモート SDKインストールの場合、この変数はリモートクライアントのホストではなく Access Managerがインストールされている (またはする予定の) ホスト。 この変数の設定は、Webコンテナ設定での対応する変数と一致させることをお勧めします。たとえばApplication Server 8の場合、この変数を AS81_HOSTと一致させます。
SERVER_PORT	Access Managerポート番号。デフォルト: 58080 リモート SDKインストールの場合、この変数はリモートクライアントのホストではなく Access Managerがインストールされている (またはする予定の) ホストのポート番号。 この変数の設定は、Webコンテナ設定での対応する変数と一致させることをお勧めします。たとえばApplication Server 8の場合、この変数を AS81_PORTと一致させます。
SERVER_PROTOCOL	サーバープロトコル: http または https。デフォルト: http リモート SDKインストールの場合、この変数はリモートクライアントのホストではなく Access Managerがインストールされている (またはする予定の) ホストのプロトコル。 この変数の設定は、Webコンテナ設定での対応する変数と一致させることをお勧めします。たとえばApplication Server 8の場合、この変数を AS81_PROTOCOLと一致させます。
CONSOLE_HOST	コンソールがインストールされたサーバーの完全修飾ホスト名。 デフォルト: Access Managerのホストに指定された値
CONSOLE_PORT	コンソールがインストールされ、接続待機している Webコンテナのポート。 デフォルト: Access Managerのポートに指定された値

表 1–2 Access Managerの設定変数 (続き)

変数	説明
CONSOLE_PROTOCOL	コンソールがインストールされたWebコンテナのプロトコル。 デフォルト: サーバープロトコル
CONSOLE_REMOTE	Access Managerサービスのコンソールがリモートにある場合は、trueに設定。そうでない場合はfalseに設定。デフォルト: false
DS_HOST	Directory Serverの完全修飾ホスト名。
DS_PORT	Directory Serverのポート。デフォルト: 389。
DS_DIRMGRDN	ディレクトリマネージャーのDN: Directory Serverへの無制限のアクセス権を持つユーザー。 デフォルト: `"cn=Directory Manager"`
DS_DIRMGRPASSWD	ディレクトリマネージャーのパスワード 25 ページから始まる「Access Managerの設定変数」のADMINPASSWDの説明の中の、特殊文字に関する注記を参照してください。
ROOT_SUFFIX	ディレクトリの初期またはルートサフィックス。使用中のDirectory Serverにこの値が必ず存在する必要があります。 25 ページから始まる「Access Managerの設定変数」のADMINPASSWDの説明の中の、特殊文字に関する注記を参照してください。
ADMINPASSWD	管理者 (amadmin) のパスワード。amldapuserのパスワードとは異なるパスワードにする必要があります。 注: パスワード中に、スラッシュ (/) または円マーク (\\) などの特殊文字が含まれる場合には、これらの文字を引用符 (”) で囲む必要があります。次に例を示します。 `ADMINPASSWD='\\\\\\\\\\\####///'` ただし、実際のパスワードの文字に引用符を使うことはできません。
AMLDAPUSERPASSWD	amldapuserのパスワード。amadminのパスワードとは異なるパスワードにする必要があります。 25 ページから始まる「Access Managerの設定変数」のADMINPASSWDの説明の中の、特殊文字に関する注記を参照してください。

表 1–2 Access Managerの設定変数 (続き)

変数	説明
CONSOLE_DEPLOY_URI	Access Managerの管理コンソールサブコンポーネントに関連したHTMLページ、クラス、およびJARファイルにアクセスするためのURIプレフィックス。 デフォルト: `/amconsole`
SERVER_DEPLOY_URI	アイデンティティー管理とポリシーサービスのコアサブコンポーネントに関連したHTMLページ、クラス、およびJARファイルにアクセスするためのURIプレフィックス。 デフォルト: `/amserver`
PASSWORD_DEPLOY_URI	Access Managerを実行中のWebコンテナが、入力された文字列と対応する配備アプリケーションとの間で行うマッピングを決めるURI。 デフォルト: `/ampassword`
COMMON_DEPLOY_URI	COMMON_DEPLOY_URI Webコンテナ上の共通ドメインサービスにアクセスするURIプレフィックス。 デフォルト: `/amcommon`
COOKIE_DOMAIN	Access Managerがユーザーにセッション IDを付与する場合にブラウザに返す、信頼できるDNSドメインの名前。少なくとも1つの値が存在する必要があります。形式は、通常、ピリオドのあとにサーバーのドメイン名を付けたものになります。 例: `.example.com`
JAVA_HOME	JDKインストールディレクトリのパス。デフォルト: `/usr/jdk/entsys-j2se`。この変数は、(`amadmin`などの) コマンド行インタフェースの実行可能ファイルによって使用されるJDKを指定します。バージョンは1.4.2またはそれ以降である必要があります。
AM_ENC_PWD	パスワードの暗号化鍵: Access Managerがユーザーパスワードを暗号化するために使用する文字列。デフォルト: なし。値を何も設定しなかった場合、ユーザーのパスワード暗号化鍵は`amconfig`によって生成されます。このため、ユーザーが直接指定した場合でも、`amconfig`によって生成された場合でも、インストール環境には、パスワードの暗号化鍵が存在することになります。 重要: Access Managerまたはリモート SDKの複数のインスタンスを配備する場合、すべてのインスタンスに対して同一のパスワード暗号化鍵を使用する必要があります。追加のインスタンスを配備するとき、最初のインスタンスの`AMConfig.properties`ファイル内の`am.encryption.pwd`プロパティの値をコピーして使用します。

表 1–2 Access Manager の設定変数　(続き)

変数	説明
PLATFORM_LOCALE	プラットフォームのロケール。デフォルト: `en_US` (米語)
NEW_OWNER	インストール後の Access Manager ファイルの新しい所有者。デフォルト: `root`
NEW_GROUP	インストール後の Access Manager ファイルの新しいグループ。デフォルト: `other` Linux へのインストールの場合は、NEW_GROUP の値に `root` を設定します。
PAM_SERVICE_NAME	オペレーティングシステムに付属し、Unix 認証モジュールに対して使用される PAM 設定またはスタックからの PAM サービスの名前 (通常、Solaris の場合は `other`、Linux の場合は `password`)。デフォルト: `other`。
XML_ENCODING	XML のエンコーディング。デフォルト: `ISO-8859-1`
NEW_INSTANCE	ユーザーが新たに作成した Web コンテナインスタンスに、設定スクリプトが Access Manager を配備するかどうかを指定します。 ■ true = すでに存在するインスタンスではなくユーザーが作成した新しい Web コンテナインスタンスに対して Access Manager を配備する場合 ■ false = 最初のインスタンスを設定する、またはインスタンスを再設定する場合。 デフォルト: false
SSL_PASSWORD	このリリースでは使用されません。

Web コンテナの設定変数

Access Manager 用の Web コンテナを指定するには、サイレントモード入力ファイル内の WEB_CONTAINER 変数を設定します。Access Manager 7 2005Q4 によってサポートされる Web コンテナのバージョンについては、『Sun Java System Access Manager 7 2005Q4 リリースノート』を参照してください。

表 1–3 Access Manager WEB_CONTAINER 変数

値	Web コンテナ
WS6 (デフォルト)	30 ページの「Sun Java System Web Server 6.1 SP5」
AS8	31 ページの「Sun Java System Application Server 8.1」
WL8	32 ページの「BEA WebLogic Server 8.1」

表 1–3 Access Manager WEB_CONTAINER 変数　(続き)

値	Web コンテナ
WAS5	33 ページの「IBM WebSphere 5.1」

Sun Java System Web Server 6.1 SP5

この節では、サイレントモード入力ファイル内の Web Server 6.1 2005Q4 SP5 用設定変数について説明しています。

表 1–4 Web Server 6.1 設定変数

変数	説明
WS61_INSTANCE	Access Manager が配備される、または配備解除される Web Server インスタンス名。 デフォルト: https-*web-server-instance-name* ここで *web-server-instance-name* は Access Manager ホスト (25 ページの「Access Manager の設定変数」で説明されている変数) を表します。
WS61_HOME	Web Server のベースインストールディレクトリ。 デフォルト: `/opt/SUNWwbsvr`
WS61_PROTOCOL	30 ページの「Sun Java System Web Server 6.1 SP5」 で説明されている変数によって設定され、Access Manager が配備される Web Server インスタンスが使用するプロトコル: http または https。 デフォルト: Access Manager プロトコル (25 ページの「Access Manager の設定変数」で説明されている変数)
WS61_HOST	Web Server インスタンス (30 ページの「Sun Java System Web Server 6.1 SP5」 で説明されている変数) 用の完全修飾ホスト名。 デフォルト: Access Manager ホストインスタンス (25 ページの「Access Manager の設定変数」で説明されている変数)
WS61_PORT	Web Server が接続を待機しているポート。 デフォルト: Access Manager ポート番号 (25 ページの「Access Manager の設定変数」で説明されている変数)
WS61_ADMINPORT	Web Server 管理サーバー が接続を待機しているポート。 デフォルト: 8888
WS61_ADMIN	Web Server 管理者のユーザー ID。 デフォルト: `"admin"`

Sun Java System Application Server 8.1

この節では、サイレントモード入力ファイル内の Application Server 8.1 用設定変数について説明しています。

表 1–5 Application Server 8.1 の設定変数

変数	説明
AS81_HOME	Application Server 8.1 がインストールされているディレクトリへのパス。 デフォルト: `/opt/SUNWappserver/appserver`
AS81_PROTOCOL	Application Server インスタンスによって使用されるプロトコル: http または https。 デフォルト: Access Manager プロトコル (25 ページの「Access Manager の設定変数」で説明されている変数)
AS81_HOST	Application Server インスタンスが接続を待機している完全修飾ドメイン名 (FQDN)。 デフォルト: Access Manager ホスト (25 ページの「Access Manager の設定変数」で説明されている変数)
AS81_PORT	Application Server インスタンスが接続を待機しているポート。 デフォルト: Access Manager ポート番号 (25 ページの「Access Manager の設定変数」で説明されている変数)
AS81_ADMINPORT	Application Server 管理サーバー が接続を待機しているポート。 デフォルト: 4849
AS81_ADMIN	Application Server が表示されているドメインでの Application Server 管理サーバーの管理者の名前。 デフォルト: `admin`
AS81_ADMINPASSWD	Application Server が表示されているドメインでの Application Server の管理者パスワード。 25 ページから始まる「Access Manager の設定変数」の ADMINPASSWD の説明の中の、特殊文字に関する注記を参照してください。
AS81_INSTANCE	Access Manager を実行する Application Server インスタンスの名前。 デフォルト: `server`

表 1–5 Application Server 8.1 の設定変数　(続き)

変数	説明
AS81_DOMAIN	この Access Manager インスタンスを配備したいドメインに対する Application Server ディレクトリへのパス。 デフォルト: `domain1`
AS81_INSTANCE_DIR	Application Server が、インスタンス用のファイルを保存するディレクトリへのパス。 デフォルト: `/var/opt/SUNWappserver/domains/domain1`
AS81_DOCS_DIR	Application Server がコンテンツ文書を保存するディレクトリ。 デフォルト: `/var/opt/SUNWappserver/domains/domain1/docroot`
AS81_ADMIN_IS_SECURE	Application Server 管理インスタンスが SSL を使用しているかどうかを指定します。 ■ true: セキュリティー保護されたポート (HTTPS プロトコル) が有効になっています。 ■ false: セキュリティー保護されたポート (HTTPS プロトコル) が無効になっています。 デフォルト: true (有効) `ampsamplesilent` には、アプリケーションサーバーの管理ポートがセキュリティー保護されているかどうかを指定する追加の設定があります。 ■ true: アプリケーションサーバーの管理ポートはセキュリティー保護されています (HTTPS プロトコル)。 ■ false: アプリケーションサーバーの管理ポートはセキュリティー保護されていません (HTTP プロトコル)。 デフォルト: true (有効)。

BEA WebLogic Server 8.1

この節では、サイレントモード入力ファイル内の BEA WebLogic Server 8.1 用設定変数について説明しています。

表 1–6 BEA WebLogic Server 8.1 設定変数

変数	説明
WL8_HOME	WebLogic のホームディレクトリ。デフォルト: `/usr/local/bea`
WL8_PROJECT_DIR	WebLogic プロジェクトディレクトリ。デフォルト: `user_projects`

表 1–6 BEA WebLogic Server 8.1 設定変数　(続き)

変数	説明
WL8_DOMAIN	WebLogic ドメイン名。デフォルト: `mydomain`
WL8_SERVER	WebLogic サーバー名。デフォルト: `myserver`
WL8_INSTANCE	WebLogic インスタンス名。デフォルト: `/usr/local/bea/weblogic81 ($WL8_HOME/weblogic81)`
WL8_PROTOCOL	WebLogic プロトコル。デフォルト: http
WL8_HOST	WebLogic ホスト名。デフォルト: サーバーのホスト名
WL8_PORT	WebLogic ポート。デフォルト: 7001
WL8_SSLPORT	WebLogic SSL ポート。デフォルト: 7002
WL8_ADMIN	WebLogic 管理者。デフォルト: `"weblogic"`
WL8_PASSWORD	WebLogic 管理者のパスワード。 25 ページから始まる「Access Manager の設定変数」の ADMINPASSWD の説明の中の、特殊文字に関する注記を参照してください。
WL8_JDK_HOME	WebLogic JDK のホームディレクトリ。デフォルト: 32 ページの「BEA WebLogic Server 8.1」 `/jdk142_04`
WL8_CONFIG_LOCATION	WebLogic 起動スクリプトの場所の親ディレクトリに設定する必要があります。

IBM WebSphere 5.1

この節では、サイレントモード入力ファイル内の IBM WebSphere Server 5.1 用設定変数について説明しています。

表 1–7 IBM WebSphere 5.1 設定変数

変数	説明
WAS51_HOME	WebSphere のホームディレクトリ。デフォルト: `/opt/WebSphere/AppServer`
WAS51_JDK_HOME	WebSphere JDK のホームディレクトリ。デフォルト: `/opt/WebSphere/AppServer/java`
WAS51_CELL	WebSphere セル。デフォルト: hostname 値
WAS51_NODE	WebSphere ノード名。デフォルト: WebSphere がインストールされたサーバーのホスト名。デフォルト: hostname 値
WAS51_INSTANCE	WebSphere インスタンス名。デフォルト: `server1`

表 1–7 IBM WebSphere 5.1 設定変数　(続き)

変数	説明
WAS51_PROTOCOL	WebSphere のプロトコル。デフォルト: http
WAS51_HOST	WebSphere のホスト名。デフォルト: サーバーのホスト名
WAS51_PORT	WebSphere のポート。デフォルト: 9080
WAS51_SSLPORT	WebSphere の SSL ポート。デフォルト: 9081
WAS51_ADMIN	WebSphere の管理者。デフォルト: "admin"
WAS51_ADMINPORT	WebSphere の管理者のポート。デフォルト: 9090

Directory Serverの設定変数

Access Manager 7 2005Q4 によってサポートされる Directory Server のバージョンについては、『Sun Java System Access Manager 7 2005Q4 リリースノート』 を参照してください。この節では、サイレントモード入力ファイル内の Directory Server 設定変数について説明しています。

表 1–8 Directory Server の設定変数

変数	説明
DIRECTORY_MODE	Directory Server モード 1 = Directory Information Tree (DIT) の新規インストールに使用します。 2 = 既存の DIT に使用します。ネーミング属性とオブジェクトクラスは同一です。したがって、設定スクリプトは `installExisting.ldif` と `umsExisting.ldif` ファイルをロードします。 設定スクリプトは、設定作業中に入力された値 (たとえば、BASE_DIR、SERVER_HOST、ROOT_SUFFIX など) を使って、LDIF やプロパティーファイルの更新も実行します。 この更新は「タグ交換」とも呼ばれますが、これは設定スクリプトがファイル内のダミーのタグを実際の設定値と入れ替えるためです。 3 = 手動でロードする時、既存の DIT に対して使用します。ネーミング属性とオブジェクトクラスは異なるので、設定スクリプトは `installExisting.ldif` と `umsExisting.ldif` ファイルをロードしません。スクリプトはタグ交換 (上記、モード 2 で説明) を行います。 LDIF ファイルを検査し、必要があれば修正して、LDIF ファイルとサービスを手動でロードします。 4 = 既存のマルチサーバーインストールに使用します。設定スクリプトは LDIF ファイルとサービスをロードしません。これは、この操作が既存の Access Manager のインストールに対するものだからです。スクリプトはタグ交換 (上記、モード 2 で説明) のみを行い、プラットフォームリストにサーバーエントリを追加します。 5 = 既存のアップグレードに使用します。スクリプトはタグ交換 (上記、モード 2 で説明) のみを行います。 デフォルト: 1
USER_NAMING_ATTR	ユーザーネーミング属性: その相対ネームスペース内部でのユーザーまたはリソースの一意な識別子。デフォルト: `uid`
ORG_NAMING_ATTR	ユーザーの会社または組織のネーミング属性。デフォルト: `o`
ORG_OBJECT_CLASS	組織オブジェクトクラス。デフォルト: `sunismanagedorganization`

表 1–8 Directory Server の設定変数　(続き)

変数	説明
USER_OBJECT_CLASS	ユーザーオブジェクトクラス。デフォルト: inetorgperson
DEFAULT_ORGANIZATION	デフォルトの組織名。デフォルト: サーバーホスト

Access Manager の amconfig スクリプト

Java Enterprise System インストーラを実行後、amconfig スクリプトが、Solaris システムでは *AccessManager-base* /SUNWam/bin ディレクトリに、Linux システムでは *AccessManager-base*/identity/bin ディレクトリにあります。

amconfig スクリプトは、サイレント設定入力ファイルを読み取ってから、必要に応じてサイレントモードでほかのスクリプトを呼び出し、要求された処理を実行します。

amconfig スクリプトを実行するには、次の構文を使います。

```
amconfig -s input-file
```

各表記の意味は次のとおりです。

-s は amconfig をサイレントモードで実行します。

input-file はサイレント設定入力ファイルで、実行したい操作用の設定変数を含んでいます。詳細については、23 ページの「Access Manager の設定スクリプト入力ファイルのサンプル」を参照してください。

amconfig スクリプトを実行するときには、以下の点を考慮してください。

- スーパーユーザー (root) として実行する必要があります。
- amsamplesilent ファイル (またはこのファイルのコピー) へのフルパスを指定してください。次に例を示します。

```
# cd /opt/SUNWam/bin
# ./amconfig -s ./amsamplesilent
```

または

```
# ./amconfig -s /opt/SUNWam/bin/amsamplesilent
```

注 – Access Manager 7 2005Q4 リリースでは、次のスクリプトはサポートされていません。

- create 引数を伴う amserver
- amserver.*instance*

またデフォルトでは、amserver start は認証ヘルパー amsecuridd および amunixd のみを開始します。amsecuridd 認証ヘルパーは、Solaris OS SPARC プラットフォームでのみ利用可能です。

Access Managerの配備シナリオ

Java Enterprise System インストーラを使って Access Manager の最初のインスタンスをインストールした後、サイレント設定入力ファイル内の設定変数を編集し、amconfig スクリプトを実行することにより、追加の Access Manager インスタンスを配備および設定することができます。

次のシナリオについて説明します。

- 37 ページの「Access Manager の追加のインスタンスの配備」
- 39 ページの「Access Manager のインスタンスの設定と再設定」
- 40 ページの「Access Manager のアンインストール」
- 41 ページの「すべての Access Manager インスタンスのアンインストール」

Access Managerの追加のインスタンスの配備

Access Manager の新しいインスタンスを配備する前に、Web コンテナ用管理ツールを使って新しい Web コンテナインスタンスを作成および開始する必要があります。詳細は、Web コンテナについての個別のマニュアルを参照してください。

- Web Server については、http://docs.sun.com/coll/1308.1を参照
- Application Server については、http://docs.sun.com/coll/1310.1を参照

ここで述べる手順は、「今すぐ設定」オプションを使ってインストールされた Access Manager インスタンスのみに該当します。Web コンテナとして WebLogic または WebSphere を使用する予定の場合、Access Manager のインストール時に「あとで設定」オプションを使用する必要があります。詳細については、第 2 章を参照してください。

追加の Access Manager インスタンスの配備

ここでは、異なるホストサーバー上に追加の Access Manager インスタンスを配備し、プラットフォームサーバーリストを更新する方法について説明します。

▼ 追加の Access Manager インスタンスを配備する

1 そのインスタンスの Web コンテナに応じた、管理者としてログインします。たとえば、Web Server 6.1 が新しいインスタンスの Web コンテナになる場合、スーパーユーザー (root) としてログインするか、Web Server 管理サーバーのユーザーアカウントとしてログインします。

2 amsamplesilent ファイルを、書き込み可能なディレクトリにコピーし、そのディレクトリをカレントディレクトリにします。たとえば、/newinstances というディレクトリを作成します。

ヒント: amsamplesilent ファイルのコピーを、配備する新しいインスタンスにふさわしい名前に変更します。たとえば、以下の各手順では、Web Server 6.1 に新しいインスタンスをインストールするために、amnewws6instance という名前の入力ファイルを使用しています。

3 新しい amnewws6instance ファイルで次の変数を設定します。

```
DEPLOY_LEVEL=1
 NEW_INSTANCE=true
```

amnewws6instance ファイル内のほかの変数に対して、新しく作成するインスタンスで必要な設定をします。これらの変数の説明については、次節以降の表を参照してください。

- 25 ページの「Access Manager の設定変数」
  - 29 ページの「Web コンテナの設定変数」
  - 34 ページの「Directory Server の設定変数」

    重要: すべての Access Manager インスタンスは、パスワード暗号化鍵に対して同じ値を使用する必要があります。このインスタンスに対して AM_ENC_PWD 変数を設定するには、最初のインスタンスの AMConfig.properties ファイル内の am.encryption.pwd プロパティーから値をコピーします。

    将来、このインスタンスをアンインストールする場合のために、amnewws6instance ファイルを保存しておきます。

4 新しい amnewws6instance ファイルを指定して、amconfig スクリプトを実行します。たとえば、Solaris システムでは、次のようになります。

```
# cd /opt/SUNWam/bin/
 # ./amconfig -s ./newinstances/amnewws6instance
```

-s オプションは amconfig スクリプトをサイレントモードで実行します。

amconfig スクリプトは、amnewws6instance ファイルの変数を使い、必要があればほかの設定スクリプトを呼び出して、新しいインスタンスを配備します。

▼ プラットフォームサーバーリストを更新する

追加のコンテナインスタンスを作成するには、Access Managerプラットフォームサーバーリストを更新して、コンテナの追加を反映させる必要があります。

1. 最上位の管理者として**Access Manager**コンソールにログインします。
2. 「サービス設定」タブをクリックします。
3. 「プラットフォーム」サービスをクリックします。
4. サーバーリストに追加する新しいインスタンスについて、次の情報を入力します。

   protocol://*fqdn*:*port*|*instance-number*

   インスタンス番号には、使われていない番号の中から、次に使用可能な番号を指定することをお勧めします。
5. 「追加」をクリックします。
6. 「保存」をクリックします。

Access Managerのインスタンスの設定と再設定

`amconfig`スクリプトを実行することにより、Java Enterprise Systemインストーラの「あとで設定」オプションを使ってインストールされたAccess Managerのインスタンスを設定できます。または、「今すぐ設定」オプションを使ってインストールされた最初のインスタンスを再設定できます。

たとえば、Access Managerの所有者とグループを変更するためにインスタンスを再設定してみます。

▼ Access Managerのインスタンスを設定または再設定する

1. そのインスタンスの**Web**コンテナに応じた、管理者としてログインします。たとえば、**Web Server 6.1**が**Web**コンテナであれば、スーパーユーザー**(root)**、または**Web Server**管理サーバーのユーザーアカウントでログインします。
2. インスタンスの配備に使用したサイレント設定入力ファイルを、書き込み可能なディレクトリにコピーし、そのディレクトリをカレントディレクトリにします。たとえば、**Web Server 6.1**用のインスタンスを再設定するために、以降の手順では`/reconfig`ディレクトリ内の入力ファイル`amnewinstanceforWS61`を使います。
3. `amnewinstanceforWS61`ファイルで、**DEPLOY_LEVEL**変数の値を、**24**ページの「配備モード変数」操作で説明した値のどれかに設定します。たとえば、完全インストールを再設定するには、**DEPLOY_LEVEL=21**と設定します。

4 amnewinstanceforWS61 ファイルでは、**NEW_INSTANCE** 変数を **false** と設定します。

```
NEW_INSTANCE=false
```

5 インスタンスを再設定するには、amnewinstanceforWS61 ファイル内のほかの変数も設定します。たとえば、インスタンスの所有者とグループを変更するには、**NEW_OWNER** と **NEW_GROUP** を新しい値に変更します。

以下のその他の変数の説明については、次節以降の表を参照してください。

- 25 ページの「Access Manager の設定変数」
  - 29 ページの「Web コンテナの設定変数」
  - 34 ページの「Directory Server の設定変数」

6 編集した入力ファイルを指定して、amconfig スクリプトを実行します。たとえば、**Solaris** システムでは、次のようになります。

```
# cd /opt/SUNWam/bin/
 # ./amconfig -s ./reconfig/amnewinstanceforWS61
```

-s オプションはスクリプトをサイレントモードで実行します。amconfig スクリプトは、amnewinstanceforWS61 ファイルの変数を使い、必要があればほかの設定スクリプトを呼び出して、インスタンスを再設定します。

Access Manager のアンインストール

amconfig スクリプトを実行してインストールした Access Manager のインスタンスをアンインストールできます。また、Access Manager インスタンスを一時的に設定解除できますが、Web コンテナインスタンスは削除しない限りそのまま残り、後日別の Access Manager インスタンスを再配備する際に使用できます。

▼ Access Manager のインスタンスをアンインストールする

1 そのインスタンスの **Web** コンテナに応じた、管理者としてログインします。たとえば、**Web Server 6.1** が **Web** コンテナであれば、スーパーユーザー **(root)**、または **Web Server** 管理サーバーのユーザーアカウントでログインします。

2 インスタンスの配備に使用したサイレント設定入力ファイルを、書き込み可能なディレクトリにコピーし、そのディレクトリをカレントディレクトリにします。たとえば、**Web Server 6.1** 用のインスタンスを設定解除するために、以降の手順では /unconfigure ディレクトリ内の入力ファイル amnewinstanceforWS61 を使います。

3 amnewinstanceforWS61 ファイルで、**DEPLOY_LEVEL** 変数の値を、**24** ページの「配備モード変数」操作で説明した値のどれかに設定します。たとえば、完全インストールのアンインストール **(**または設定解除**)** を行うには、**DEPLOY_LEVEL=11** と設定します。

4 編集した入力ファイルを指定して、amconfigスクリプトを実行します。たとえば、**Solaris**システムでは、次のようになります。

```
# cd /opt/SUNWam/bin/
 # ./amconfig -s ./unconfigure/aminstanceforWS61
```

-sオプションはスクリプトをサイレントモードで実行します。amconfigスクリプトはamnewinstanceforWS61ファイルを読み込み、インスタンスをアンインストールします。

Webコンテナインスタンスはそのまま残っているため、後日別のAccess Managerインスタンスを再配備する際に使用できます。

すべての**Access Manager**インスタンスのアンインストール

このシナリオでは、Access Manager 7 2005Q4のすべてのインスタンスとパッケージをシステムから完全に削除します。

▼ **Access Manager 7 2005Q4**をシステムから完全に削除する

1 スーパーユーザー**(root)**としてログインするか、スーパーユーザー**(root)**になります。

2 インスタンスを配備するのに使用した入力ファイル中で、**DEPLOY_LEVEL**変数の値を、24ページの「配備モード変数」操作で説明した値のどれかに設定します。たとえば、完全インストールのアンインストール**(**または設定解除**)**を行うには、**DEPLOY_LEVEL=11**と設定します。

3 41ページの「すべての**Access Manager**インスタンスのアンインストール」で編集したファイルを使用して、amconfigスクリプトを実行します。たとえば、**Solaris**システムでは、次のようになります。

```
# cd /opt/SUNWam/bin/
# ./amconfig -s ./newinstances/amnewws6instance
```

amconfigスクリプトはサイレントモードで動作し、インスタンスをアンインストールします。

アンインストールしたいインスタンスすべてに対してこれらの手順を繰り返します。ただし、Java Enterprise Systemインストーラを使ってインストールした最初のインスタンスは除きます。

4 最初のインスタンスをアンインストールし、すべての**Access Manager**パッケージをシステムから削除するには、**Java Enterprise System**アンインストーラを実行します。アンインストーラの詳細については、『**Sun Java Enterprise System 2005Q4 Installation Guide for UNIX**』を参照してください。

設定スクリプト入力ファイルの例

ここからは、WebLogic 8.1 を使った配備のための Access Manager 設定スクリプト入力ファイルの例を示します。

```
DEPLOY_LEVEL=1
BASEDIR=/opt
SERVER_HOST=ide-56.example.company.com
SERVER_PORT=7001
SERVER_PROTOCOL=http
CONSOLE_HOST=$SERVER_HOST
CONSOLE_PORT=$SERVER_PORT
CONSOLE_PROTOCOL=$SERVER_PROTOCOL
CONSOLE_REMOTE=false
DS_HOST=ide-56.example.company.com
DS_PORT=389
DS_DIRMGRDN=”cn=Directory Manager”
DS_DIRMGRPASSWD=11111111
ROOT_SUFFIX=”dc=company,dc=com”
ADMINPASSWD=11111111
AMLDAPUSERPASSWD=00000000
CONSOLE_DEPLOY_URI=/amconsole
SERVER_DEPLOY_URI=/amserver
PASSWORD_DEPLOY_URI=/ampassword
COMMON_DEPLOY_URI=/amcommon
COOKIE_DOMAIN=.iplanet.com
JAVA_HOME=/usr/jdk/entsys-j2se
AM_ENC_PWD=””
PLATFORM_LOCALE=en_US
NEW_OWNER=root
NEW_GROUP=other
XML_ENCODING=ISO-8859-1
NEW_INSTANCE=false
WEB_CONTAINER=WL8
WL8_HOME=/export/bea8
WL8_PROJECT_DIR=user_projects
WL8_DOMAIN=mydomain
WL8_CONFIG_LOCATION=$WL8_HOME/$WL8_PROJECT_DIR/domains
WL8_SERVER=myserver
WL8_INSTANCE=/export/bea8/weblogic81
WL8_PROTOCOL=http
WL8_HOST=ide-56.example.company.com
WL8_PORT=7001
WL8_SSLPORT=7002
WL8_ADMIN=”weblogic”
WL8_PASSWORD=”11111111”
WL8_JDK_HOME=$WL8_HOME/jdk142_04
DIRECTORY_MODE=1
```

```
USER_NAMING_ATTR=uid
ORG_NAMING_ATTR=o
ORG_OBJECT_CLASS=examplemanagedorganization
USER_OBJECT_CLASS=inetorgperson
DEFAULT_ORGANIZATION=
Sample Configuration Script Input File for WebLogic 8.1.x
```

◆ ◆ ◆ 第 2 章

2 サードパーティー Web コンテナのインストールと設定

この章では、Sun Java™ System Access Manager とともに配備されるサードパーティー Web コンテナをインストールおよび設定する手順について説明します。このリリースでは、Access Manager は BEA WebLogic 8.1 (およびその現行パッチ) と IBM WebSphere 5.1 (およびその現行パッチ) をサポートします。

WebLogic と WebSphere は Java Enterprise System の一部ではないため、それらは Java ES インストールプログラムとは別にインストールおよび設定する必要があります。一般的なインストール手順は次のとおりです。

- Web コンテナインスタンスをインストール、設定、および起動します。
- Java ES インストーラから Directory Server をインストールします。
- Java ES インストーラから「あとで設定」モードで Access Manager をインストールします。このモードは、Access Manager を未設定の状態のままにします。
- Access Manager 設定スクリプトを実行し、Access Manager を Web コンテナに配備します。
- Web コンテナを再起動します。

BEA WebLogic 8.1 のインストールと設定

WebLogic をインストールする前に、ホストドメインが DNS に登録されていることを確認します。また、WebLogic ソフトウェアの正しいバージョンをインストールしていることも確認します。詳細は、BEA 製品サイト (http://commerce.bea.com/index.jsp) を参照してください。

▼ WebLogic 8.1 をインストールおよび設定する

1 .zip または .gz 形式の、ダウンロードしたソフトウェアイメージを展開します。必ず、プラットフォームに合った適切な **zip/gzip** ユーティリティーを使用してください。ユーティリティーが適切でないと、展開中にチェックサムエラーが発生する場合があります。

2 ターゲットシステムのシェルウィンドウからインストールプログラムを実行します。

WebLogic インストールユーティリティーが指示する手順に従います (詳細なインストール手順については、http://e-docs.bea.com/wls/docs81/ を参照)。

インストールプロセスの実行時に、あとで Access Manager の設定で使用する次の情報を必ずメモしておいてください。

- FQDN (`WL8_HOST` パラメータで使用)
  - インストールディレクトリ
  - ポート番号

3 インストールが完了したら、次の場所にある **WebLogic** 設定ツールを実行し、ドメインおよびサーバーインスタンスを設定します。

WebLogic-base/WebLogic-instance/`common/bin/quickstart.sh`

デフォルトでは、WebLogic はサーバーインスタンスを `myserver` として、ドメインを `mydomain` として定義します。これらのデフォルトをそのまま使用することはほとんどありません。新しいドメインおよびインスタンスを作成する場合、Access Manager の設定および配備の情報を必ずメモしておいてください。手順については、WebLogic 8.1 のドキュメントを参照してください。

4 管理インスタンス上にインストールしている場合、次の場所にある `startWebLogic.sh` ユーティリティーを使って **WebLogic** を起動します。

WebLogic-base/WebLogic-Userhome `/domains/` *WebLogic-domain*`/startWebLogic.sh`

管理対象インスタンス上にインストールしている場合、次のコマンドを使って WebLogic を起動します。

WebLogic-base `/`WebLogic-Userhome`/domains/` WebLogic-domain `/startManagedWebLogic.sh` WebLogic-managed-instancename admin-url

IBM WebSphere 5.1 のインストールと設定

WebSphere をインストールする前に、ホストドメインが DNS に登録されていること、および、プラットフォームに合った正しいバージョンの WebSphere をインストールしていることを確認してください。詳細は、IBM 製品サポート Web サイト (http://www-306.ibm.com/software/websphere/support) を参照してください。

▼ WebSphere 5.1 をインストールおよび設定する

1 .zip または .gz 形式の、ダウンロードしたソフトウェアイメージを展開します。必ず、プラットフォームに合った適切な **zip/gzip** ユーティリティーを使用してください。ユーティリティーが適切でないと、展開中にチェックサムエラーが発生する場合があります。

2 ターゲットシステムのシェルウィンドウからインストールプログラムを実行します。パッチをインストールする予定の場合、まず **5.1** バージョンをインストールしてからパッチを適用します。詳細なインストール手順については、**http://publib.boulder.ibm.com/infocenter/ws51help/index.jsp** を参照してください。

インストールプロセスの実行時に、あとで Access Manager の設定で使用する次の情報を必ずメモしておいてください。

- ホスト名
  - ドメイン名
  - セル名
  - ノード名
  - ポート番号
  - インストールディレクトリ
  - WebSphere インスタンス名
  - 管理ポート

    デフォルトでは、WebSphere はサーバーインスタンスを server1 として定義しますが、このデフォルトを使用することはほとんどありません。新しいインスタンスを作成する場合、Access Manager の設定および配備の情報を必ずメモしておいてください。手順については、WebSphere 5.1 のドキュメントを参照してください。

3 インストールが成功したことを確認します。

a. 次のディレクトリに server.xml ファイルが存在することを確認します。

```
/opt/WebSphere/AppServer/config/cells/cell-name/noes/

node-name/servers/server1
```

b. サーバーの起動には、次の例のように startServer.sh コマンドを使用します。

```
/opt/WebSphere/AppServer/bin/startServer.sh server1
```

c. サンプル **Web** アプリケーションを見るには、**Web** ブラウザで、対応する **URL** を次の形式で入力します。

http:// *fqdn:portnumber/snoop*

4 インストールが成功したことを確認したら、stopServer.sh ユーティリティーを使用してサーバーを停止します。次に例を示します。

```
opt/WebSphere/AppServer/bin/stopServer.sh server1
```

5 **WebSphere 5.1** のパッチをインストールする場合は、updateWizard.sh コマンド行ユーティリティーを使って元の **5.1** インスタンス上にパッチをインストールします。

6 **WebSphere** を再起動し、インストールが成功したことを確認します。

Java ES を使った Directory Server と Access Manager のインストール

Access Manager をインストールするには、Java Enterprise System (Java ES) インストーラを 2 回別々に起動する必要があります。

▼ Directory Serverをインストールする

1 **(**ローカルまたはリモートで**) Directory Server** をインストールするために、「今すぐ設定」オプションを使って最初の **Java ES** 呼び出しを実行します。「今すぐ設定」オプションを使うと、インストール中に選択するオプション **(**またはデフォルト値**)** によって最初のインスタンスを設定できます。

2 「あとで設定」オプションを使って **Access Manager** をインストールするために、**2** 回目の **Java ES** 呼び出しを実行します。このオプションは、**Access Manager 2005Q4** コンポーネントをインストールします。インストール後、**Access Manager** を設定する必要があります。

WebLogic および WebSphere は Java ES とは別々にインストールされるので、インストーラには、コンテナを自動的に配備するために必要な設定データが含まれていません。この理由から、Access Manager のインストール時には「あとで設定」オプションを選択する必要があります。このオプションは、Access Manager の配備を次の状態のままにします。

- アクティブな Directory Server (ローカルまたはリモートのどちらか) には Access Manager DIT データがロードされていません。
  - Access Manager の設定ファイルは自動的にロードされません。
  - Access Manager Web アプリケーションの .war ファイルは生成されません。
  - Access Manager の配備およびインストール後設定プロセスは自動的に開始および実行されません。

    詳細なインストール手順については、『Sun Java Enterprise System インストールガイド』(http://docs.sun.com/doc/819-0808?l=ja) を参照してください。

Access Manager の設定

ターゲットシステムのローカルドライブ上に Access Manager をインストールし終わったら、WebLogic 8.1 または WebSphere 5.1 に対して Access Manager を手動で設定する必要があります。この手順は次の 3 つのステップから成ります。

▼ Access Manager を設定する

1 設定スクリプト入力ファイルを編集する

2 設定スクリプトを実行する

3 Web コンテナを再起動する

設定スクリプト入力ファイルの作成

Access Manager の設定スクリプト入力ファイルには、配備レベル、Access Manager、Web コンテナ、および Directory Server のすべての変数定義が含まれます。Access Manager には、設定スクリプト入力ファイルのテンプレートのサンプル (`amsamplesilent`) が付属します。これは、Solaris システムでは *AccessManager-base* `/SUNWam/bin` ディレクトリ、Linux システムでは *AccessManager-base* `/identity/bin` ディレクトリにあります。

`amsamplesilent` テンプレートを使って、独自の設定スクリプト入力ファイルを構築することができます。ファイルの編集手順と変数定義の一覧については、23 ページの「Access Manager の設定スクリプト入力ファイルのサンプル」を参照してください。

ファイルを編集する前に必ず、インストールされている Web コンテナの次の情報を入手してください。

BEA WebLogic と IBM WebSphere

- インストールディレクトリ
- インスタンスの名前と場所
- ホスト名
- FQDN
- 待機しているポート番号
- 管理 ID
- 使用されるプロトコル

BEA WebLogic のみ

- 管理パスワード
- 共有ライブラリの場所
- ドメインの名前と場所

- プロジェクトディレクトリ名
- JDK の場所

IBM WebSphere のみ

- セル名
- ノード名
- JDK の場所

設定スクリプトの実行

設定スクリプト入力ファイルを保存したら、`amconfig` スクリプトを実行して設定プロセスを完了します。次に例を示します。

```
AccessManager-base/SUMWam/bin/amconfig -s silentfile
```

silentfile は設定入力ファイルの絶対パスです。

このスクリプトを実行すると、次の処理が実行されます。

1. Access Manager スキーマをアクティブな Directory Server インスタンスにロードします。
2. Access Manager サービスデータを Directory Server インスタンスにロードします。
3. アクティブな Access Manager インスタンスが使用する Access Manager 設定ファイルを生成します。
4. Access Manager の Web アプリケーションデータを Web コンテナに配備します。
5. Access Manager の要件に合わせて、Web コンテナ設定をカスタマイズします。

Web コンテナの再起動

設定プロセスを完了したあとで、Web コンテナを再起動する必要があります。手順については、各製品のドキュメントを参照してください。

BEA WebLogic 8.1 については、http://e-docs.bea.com/wls/docs81 を参照してください。

IBM WebSphere 5.1 については、http://publib.boulder.ibm.com/infocenter/ws51help/index.jsp を参照してください。

◆ ◆ ◆ 第 3 章

Access Manager の SSL モードへの設定

SSL (Secure Socket Layer) を単純な認証で使用することで、機密性とデータの整合性とが保証されます。Access Manager を SSL モードにするには、通常は次のようにします。

- Access Manager をセキュリティー保護された Web コンテナで設定する
- Access Manager をセキュリティー保護された Directory Server に設定する

セキュリティー保護された **Sun Java Enterprise System Web Server** による **Access Manager** の設定

Web Server で実行する Access Manager を SSL モードに設定するには、次の手順を参照してください。

▼ セキュリティー保護された **Web Server** を設定する

1 **Access Manager** コンソールで、サービス設定モジュールに移動し、「プラットフォーム」サービスを選択します。「サーバーリスト」属性で `http://` プロトコルを削除し、`https://` プロトコルを追加します。「保存」をクリックします。

注 – 必ず「保存」をクリックしてください。そうしないと、次の手順に進むことはできますが、設定の変更内容はすべて失われ、それを修正するために管理者としてログインすることもできなくなります。

手順 2 ～手順 24 では、Web Server を設定します。

2 **Web Server** コンソールにログオンします。デフォルトのポート番号は、**8888** です。

3 **Access Manager** を実行している **Web Server** インスタンスを選択し、「**Manage**」をクリックします。
設定が変更されたことを知らせるポップアップウィンドウが表示されます。「了解」をクリックします。

4 画面の右上部にある「**Apply**」ボタンをクリックします。

5 「変更の適用」をクリックします。
Web Server が自動的に再起動されます。「OK」をクリックして先に進みます。

6 選択した **Web Server** インスタンスを停止します。

7 「**Security**」タブをクリックします。

8 「**Create Database**」をクリックします。

9 新しいデータベースのパスワードを入力し、「**OK**」をクリックします。
あとで使用するために、このデータベースパスワードを書き留めておくようにしてください。

10 証明書データベースが作成されたら、「**Request a Certificate**」をクリックします。

11 画面に表示されるフィールドにデータを入力します。
「Key Pair Field Password」フィールドは、手順 9 で入力した値と同じ値にします。場所のフィールドには、場所を完全名で入力する必要があります。「CA」などの省略形では動作しません。すべてのフィールドを定義する必要があります。「Common Name」フィールドには、使用している Web Server のホスト名を入力します。

12 フォームを送信すると、次のようなメッセージが表示されます。

```
--BEGIN CERTIFICATE REQUEST---

afajsdllwqeroisdaoi234rlkqwelkasjlasnvdknbslajowijalsdkjfalsdflasdf

alsfjawoeirjoi2ejowdnlkswnvnwofijwoeijfwiepwerfoiqeroijeprwpfrwl

--END CERTIFICATE REQUEST--
```

13 このテキストをコピーし、証明書要求として送信します。
ルート CA 証明書を取得するようにしてください。

14 証明書の含まれた証明書応答が返されます。たとえば次のようになります。

```
--BEGIN CERTIFICATE---
```

```
afajsdllwqeroisdaoi234rlkqwelkasjlasnvdknbslajowijalsdkjfalsdflasdf

alsfjawoeirjoi2ejowdnlkswnvnwofijwoeijfwiepwerfoiqeroijeprwpfrwl

--END CERTIFICATE---
```

15 このテキストをクリップボードにコピーするか、ファイルに保存します。

16 **Web Server** コンソールで、「**Install Certificate**」をクリックします。

17 「**Certificate for this Server**」をクリックします。

18 「鍵ペアファイルパスワード」フィールドに、証明書データベースのパスワードを入力します。

19 証明書を表示されたテキストフィールドに貼り付けます。またはラジオボタンをクリックし、テキストボックスにファイル名を入力します。「送信」をクリックします。
ブラウザに証明書と、証明書を追加するボタンが表示されます。

20 「**Install Certificate**」をクリックします。

21 「**Certificate for Trusted Certificate Authority**」をクリックします。

22 手順 **16** ～手順 **21** と同じ方法で、ルート **CA** 証明書をインストールします。

23 両方の証明書をインストールしたら、**Web Server** コンソールで「**Preferences**」タブをクリックします。

24 別のポートで **SSL** を有効にする場合は、「**Add Listen Socket**」を選択します。次に、「**Edit Listen Socket**」を選択します。

25 セキュリティー状態を「**Disabled**」から「**Enabled**」に変更し、「**OK**」をクリックして変更を送信してから、「**Apply**」および「**Apply Changes**」をクリックします。
手順 26 ～手順 29 では、Access Manager を設定します。

26 `AMConfig.properties` ファイルを開きます。このファイルの場所は、デフォルトで `/etc/opt/SUNWam/config` です。

27 プロトコルで `http://` が出現する箇所をすべて `https://` に変更します。ただし **Web Server** インスタンスディレクトリの箇所は除きます。これは `AMConfig.properties` でも指定していますが、そのままにしておきます。

28 `AMConfig.properties` ファイルを保存します。

29 **Web Server** コンソールで、**Web Server** インスタンスをホスティングする **Access Manager** の「**ON/OFF**」ボタンをクリックします。

Web Server で「Start/Stop」ページにテキストボックスが表示されます。

30 このテキストフィールドに、証明書データベースのパスワードを入力し、「**Start**」を選択します。

セキュリティー保護された **Sun Java System Application Server** による **Access Manager** の設定

SSL が有効になっている Application Server 上で Access Manager を実行するには、次の 2 つの手順で設定します。まず、インストールされた Access Manager に対して Application Server のインスタンスをセキュリティー保護します。次に、Access Manager 自体を設定します。

Application Server 6.2 を **SSL** で設定する

ここでは、Application Server 6.2 を SSL モードに設定する手順について説明します。

▼ **Application Server** インスタンスをセキュリティーで保護する

1 ブラウザに次のアドレスを入力して、**Sun Java System Application Server** コンソールに管理者としてログインします。

```
http://fullservername:port
```

デフォルトのポート番号は、4848 です。

2 インストール時に入力したユーザー名とパスワードを入力します。

3 **Access Manager** をインストールした (または、これからインストールする) **Application Server** インスタンスを選択します。設定が変更されたことが、右側のフレームに表示されます。

4 「変更の適用」をクリックします。

5 「再起動」をクリックします。**Application Server** が自動的に再起動されます。

6 左側のフレームで、「セキュリティー」をクリックします。

7 「データベースの管理」タブをクリックします。

8 「データベースを作成」が選択されていない場合は、それをクリックします。

9 新しいデータベースのパスワードを入力し、確認のパスワードを入力してから、「**OK**」をクリックします。あとで使用するために、このデータベースパスワードを書き留めておくようにしてください。

10 証明書データベースが作成されたら、「証明書管理」タブをクリックします。

11 「要求」リンクが選択されていない場合は、それをクリックします。

12 証明書要求のデータを次のように入力します。

a. 新規の証明書か、証明書の書き換えかを選択します。証明書の多くは、一定の期間が過ぎると期限切れになります。書き換え通知を自動的に送信する認証局 **(CA)** もあります。

b. 証明書要求を送信する方法を指定します。

要求を電子メールメッセージで受け取る CA の場合は、「CA 電子メールアドレス」を選択し、CA の電子メールアドレスを入力します。CA のリストを表示するには、「List of Available Certificate Authorities」をクリックします。

Certificate Server を使用している内部 CA に証明書を要求する場合は、「CA URL」をクリックし、Certificate Server の URL を入力します。この URL は、Certificate Server で証明書要求を処理するプログラムを指している必要があります。

c. 鍵ペアファイルのパスワードを入力します。これは、手順 **9** で指定したパスワードです。

d. 次の識別情報を入力します。

「共通名」: ポート番号も含む完全なサーバー名。

「要求者名」: 要求者の名前。

「電話番号」: 要求者の電話番号。

「共通名」: デジタル証明書のインストール先となる Sun Java System Application Server の完全修飾名。

「メールアドレス」: 管理者の電子メールアドレス。

「組織」: 組織の名前。認証局によっては、この属性に入力されたホスト名が、この組織に登録済みのドメインに属していることが必要になります。

「組織単位」: 部課名など、組織の運営単位の名前。

「地域」: 市区町村の名前。

「州または都道府県名」: 組織がアメリカ合衆国またはカナダで運営されている場合は、その州の名前。省略形は使用しないでください。

「国名」: 国を表す 2 文字の ISO コード。たとえば、アメリカ合衆国のコードは US です。

13 「**OK**」ボタンをクリックします。次のようなメッセージが表示されます。

```
--BEGIN NEW CERTIFICATE REQUEST---
afajsdllwqeroisdaoi234rlkqwelkasjlasnvdknbslajowijalsdkjfalsdfla
alsfjawoeirjoi2ejowdnlkswnvnwofijwoeijfwiepwerfoiqeroijeprwpfrwl
--END NEW CERTIFICATE REQUEST--
```

14 このテキスト全体をファイルにコピーし、「**OK**」をクリックします。ルート **CA** 証明書を取得するようにしてください。

15 **CA** を選択し、その **CA** の **Web** サイトにある指示に従ってデジタル証明書を取得します。証明書は **CMS**、**Verisign**、または **Entrust.net** から取得できます。

16 認証局からデジタル証明書を受け取ったら、そのテキストをクリップボードにコピーするか、ファイルに保存します。

17 **Application Server** コンソールに移動し、「インストール」リンクをクリックします。

18 「**Certificate for this Server**」を選択します。

19 「鍵ペアファイルパスワード」フィールドに、証明書データベースのパスワードを入力します。

20 「メッセージ」テキストフィールドに、証明書をヘッダーも含めて貼り付けるか、ファイル名を入力します。適切なラジオボタンをクリックします。

21 「**OK**」ボタンをクリックします。ブラウザに証明書と、証明書を追加するボタンが表示されます。

22 「サーバー証明書を追加」をクリックします。

23 すでに説明した方法に従って、ルート **CA** 証明書をインストールします。ただし、ここでは「証明書」の「信頼できる証明書発行局 **(CA)**」をクリックします。

24 両方の証明書をインストールしたら、左側のフレームで「**HTTP** サーバー」ノードを展開します。

25 「**HTTP** サーバー」の下にある「**HTTP** リスナー」を選択します。

26 `http-listener-1` を選択します。ソケットの情報がブラウザに表示されます。

27 `http-listener-1` で使用するポートの値を、**Application Server** のインストール時に入力した値から、より適切な値 **(443** など**)** に変更します。

28 「**SSL/TLS** を有効」を選択します。

29 「証明書のニックネーム」を選択します。

30 「戻すサーバー名」を指定します。手順 **12** で指定した「共通名」と同じにする必要があります。

31 「保存」をクリックします。

32 **Access Manager** ソフトウェアをインストールする **Application Server** インスタンスを選択します。設定が変更されたことが、右側のフレームに表示されます。

33 「変更の適用」をクリックします。

34 「再起動」をクリックします。**Application Server** が自動的に再起動されます。

Application Server 8.1 を SSL で設定する

Application Server 8.1 を SSL で設定する基本手順は、次のとおりです。詳細な手順については、Application Server 8.1 のマニュアルを参照してください。

1. Application Server 上で Application Server 管理コンソールを使ってセキュリティー保護されたポートを作成します。詳細については、次の場所にある『Sun Java System Application Server Enterprise Edition 8.1 管理ガイド』の「セキュリティーの設定」を参照してください。

   `http://docs.sun.com/app/docs/coll/1369.1?l=ja`

2. Web コンテナの信頼データベース内にそのサーバーの証明書を信頼する認証局 (CA) が存在していることを確認します。次に、Web コンテナに対するサーバー証明書を取得してインストールします。詳細については、次の場所にある『Sun Java System Application Server Enterprise Edition 8.1 管理ガイド』の「証明書と SSL の操作」を参照してください。

   `http://docs.sun.com/app/docs/coll/1369.1?l=ja`

3. Web コンテナを再起動します。

Access Manager の SSL モードへの設定

ここでは、Access Manager を SSL モードに設定する手順について説明します。Access Manager の SSL を設定する前に、配備先の Web コンテナが設定されていることを確認してください。

▼ Access Manager を SSL モードに設定する

1 **Access Manager** コンソールで、サービス設定モジュールに移動し、「プラットフォーム」サービスを選択します。「サーバーリスト」属性で、同じ **URL** を **HTTPS** プロトコルで追加し、**SSL** が有効になっているポート番号を追加します。「保存」をクリックします。

注 – Access Manager の 1 つのインスタンスが、2 つのポート (HTTP と HTTPS) で待機しているとき、未処理のまま蓄積されたクッキーを使って Access Manager にアクセスしようとすると、Access Manager は応答しなくなります。この設定はサポートされていません。

2 AMConfig.properties ファイルを開きます。デフォルトでは次の場所にあります。

```
/etc/opt/SUNWam/config.
```

3 プロトコルで http:// が出現する箇所をすべて https:// に変更します。また、ポート番号を、**SSL** が有効になっているポート番号に変更します。

4 AMConfig.properties ファイルを保存します。

5 **Application Server** を再起動します。

セキュリティー保護された **BEA WebLogic Server** による **AMSDK** の設定

BEA WebLogic Server は、最初にインストールして Web コンテナとして設定してから、SSL で AMSDK を使用して設定する必要があります。インストールの詳細については、BEA WebLogic Server のマニュアルを参照してください。Access Manager の Web コンテナとして WebLogic を設定するには、第 1 章を参照してください。

▼ セキュリティー保護された **WebLogic** インスタンスを設定する

1 クイックスタートメニューを使用してドメインを作成します。

2 **WebLogic** インストールディレクトリに移動し、証明書要求を生成します。

3 **CSR** テキストファイルを使用し、サーバー証明書を **CA** に申請します。

4 承認証明書をテキストファイルに保存します。たとえば、approvedcert.txt に保存します。

5 次のコマンドを使用し、cacerts でルート **CA** をロードします。

```
cd jdk141_03/jre/lib/security/

jdk141_03/jre/bin/keytool -keystore cacerts -keyalg RSA -import -trustcacerts -alias
"<alias name>" -storepass changeit -file /opt/bea81/cacert.txt
```

6 次のコマンドを使用し、サーバー証明書をロードします。

```
jdk141_03/jre/bin/keytool -import -keystore <keystorename> -keyalg RSA -import
-trustcacerts -file approvedcert.txt -alias "mykey"
```

7 ユーザー名とパスワードを使用し、**WebLogic** コンソールにログインします。

8 次の場所を参照します。

yourdomain> Servers> myserver> Configure Keystores

9 「**Custom Identity**」、次に「**Java Standard Trust**」を選択します。

10 キーストアの場所を入力します。たとえば `/opt/bea81/keystore` のように入力します。

11 キーストアパスワードとキーストアパスフレーズを入力します。次に例を示します。

キーストアパスワード: `JKS/Java Standard Trust` (WL 8.1 の場合は JKS のみ)

キーストアパスフレーズ: `changeit`

12 **SSL** 非公開鍵の別名とパスワードを確認してください。

注 – 完全な SSL ライセンスを使用しないと、SSL が起動しません。

---

13 **Access Manager** では、`AmConfig.properties` の次のパラメータが、インストール中に自動的に設定されます。設定されていない場合は、適切に編集できます。

```
com.sun.identity.jss.donotInstallAtHighestPriority=true [ AM 6.3 以上では不要]
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
```

JDK パスが次のようになっている場合は、keytool ユーティリティーを使用し、証明書データベースにルート CA をインポートします。

```
com.iplanet.am.jdk.path=/usr/jdk/entsys-j2se
```

次に例を示します。

```
/usr/jdk/entsys-j2se/jre/lib/security
/usr/jdk/entsys-j2se/jre/bin/keytool -keystore cacerts
-keyalg RSA -import -trustcacerts -alias "machinename" -storepass changeit -file
/opt/bea81/cacert.txt
```

keytool ユーティリティーは次のディレクトリにあります。

```
/usr/jdk/entsys-j2se/jre/bin/keytool
```

14 **Access Manager** `amadmin` コマンド行ユーティリティーから `-D"java.protocol.handler.pkgs=com.iplanet.services.comm"` を削除します。

15 **Access Manager** を **SSL** モードに設定します。詳細は、57 ページの「**Access Manager** の **SSL** モードへの設定」を参照してください。

セキュリティー保護された **IBM WebSphere Application Server** による **AMSDK** の設定

IBM WebShpere Server は、最初にインストールして Web コンテナとして設定してから、SSL で AMSDK を使用して設定する必要があります。インストール手順については、WebSphere Server のマニュアルを参照してください。Access Manager の Web コンテナとして WebLogic を設定するには、第 1 章を参照してください。

▼ セキュリティー保護された **WebSphere** インスタンスを設定する

1 **Websphere** の `/bin` ディレクトリの `ikeyman.sh` を起動します。

2 「署名者」メニューから認証局 **(CA)** からの証明書をインポートします。

3 「**Personal Certs**」メニューから **CSR** を生成します。

4 前の手順で作成された証明書を取得します。

5 「**Personal Certificates**」を選択し、サーバー証明書をインポートします。

6 **WebSphere** コンソールからデフォルト **SSL** 設定を変更し、暗号を選択します。

7 デフォルトの **IBM JSSE SSL** プロバイダを設定します。

8 次のコマンドを入力し、作成したファイルからアプリケーションサーバー **JVM** キーストアに、ルート **CA** 証明書をインポートします。

```
$ appserver_root-dir/java/bin/ keytool -import -trustcacerts -alias cmscacert
-keystore ../jre/lib/security/cacerts -file
/full_path_cacert_filename.txt
```

app-server-root-dir はアプリケーションサーバーのルートディレクトリであり、*full_path_cacert_filename.txt* は、証明書を含むファイルのフルパスです。

9 **Access Manager** において、`AmConfig.properties` の次のパラメータを、**JSSE** を使用するように更新します。

```
com.sun.identity.jss.donotInstallAtHighestPriority=true
com.iplanet.security.SecureRandomFactoryImpl=com.iplanet.
am.util.SecureRandomFactoryImpl
com.iplanet.security.SSLSocketFactorImpl=netscape.ldap.factory.
JSSESocketFactory
com.iplanet.security.encyptor=com.iplanet.services.unil.JCEEncryption
```

10 **Access Manager** を **SSL** モードに設定します。詳細は、**57** ページの「**Access Manager** の **SSL** モードへの設定」を参照してください。

Access Manager を SSL モードの Directory Server に設定する

ネットワーク上でセキュリティー保護された通信を確保するため、Access Manager には LDAPS 通信プロトコルが含まれています。LDAPS は LDAP の標準プロトコルで、SSL (Secure Socket Layer) 上で実行されます。SSL 接続を有効にするためには、まず Directory Server を SSL モードにして、次に Access Manager を Directory Server に接続します。基本的な手順は次のとおりです。

1. Directory Server 用の証明書を入手してインストールし、Directory Server が認証局 (CA) からの証明書を信頼するように設定します。
2. ディレクトリで SSL をオンにします。
3. SSL が有効化された Directory Service に接続するよう、認証、ポリシーおよびプラットフォームサービスを設定します。
4. セキュリティー保護された状態で Directory Server に接続できるよう Access Manager を設定します。

Directory Server を SSL モードに設定する

Directory Server を SSL モードに設定するには、サーバー証明書を入手してインストールし、CA からの証明書を信頼するように Directory Server を設定し、SSL を有効にする必要があります。これらの作業をどのように行うかについての詳細は、『*Directory Server* 管理ガイド』の中の第 11 章「認証と暗号化の管理」を参照してください。このマニュアルは、次の場所にあります。

http://docs.sun.com/app/docs/coll/DirectoryServer_04q2_ja
(`http://docs.sun.com/app/docs/coll/DirectoryServer_04q2_ja`)

Directory Server の SSL がすでに有効になっている場合は次の節に進んでください。そこで Access Manager を Directory Server に接続する方法の詳細について説明します。

SSL が有効化された Directory Server に Access Manager を接続する

Directory Server が SSL モードに設定されたら、Access Manager をセキュリティー保護された状態で Directory Server に接続する必要があります。

▼ Directory Server に Access Manager を接続する

1 **Access Manager** コンソールで、「サービス設定」モジュールの **LDAP** 認証サービスに移動します。

   a. **Directory Server** ポートを **SSL** ポートに変更します。

   b. 「**LDAP** サーバーへの **SSL** アクセスを有効」属性を選択します。

2 「サービス設定」モジュールのメンバーシップ認証サービスに移動します。

   a. **Directory Server** ポートを **SSL** ポートに変更します。

   b. 「**LDAP** サーバーへの **SSL** アクセスを有効」属性を選択します。

3 「サービス設定」の「ポリシー設定」サービスに移動します。

   a. **Directory Server** ポートを **SSL** ポートに変更します。

   b. 「**LDAP SSL** を有効」属性を選択します。

4 テキストエディタで `serverconfig.xml` を開きます。このファイルは、次の場所にあります。

   `/etc/opt/SUNWam/config`

   a. `<Server>` 要素で、次の値を変更します。

      `port` - Access Manager が待機するセキュリティー保護されたポート番号 (デフォルト値は 636) を指定します。

      `type` - SIMPLE を SSL に変更します。

   b. `serverconfig.xml` を保存して閉じます。

5 `AMConfig.properties` ファイルを開きます。デフォルトでは次の場所にあります。

   /etc/opt/ SUNWam/config

次のプロパティーを変更します。

a. `com.iplanet.am.directory.port = 636` (デフォルトを使う場合)

b. `com.iplanet.am.directory.sslenabled=true`

c. `AMConfig.properties` を保存します。

6 サーバーを再起動します。

パート II

アクセス制御

これは『Sun Java System Access Manager™ 7 2005Q4 管理ガイド』の第 2 部です。アクセス制御インタフェースを利用すると、レルムベースのリソースを保護および規制するための認証サービスと承認サービスを作成および管理できます。企業内のユーザーが情報を要求すると、Access Manager はユーザーのアイデンティティーを検証し、ユーザーが要求した特定のリソースにそのユーザーがアクセスすることを承認します。次の章で構成されています。

◆ ◆ ◆ 第 4 章

Access Manager コンソール

Access Manager コンソールは、さまざまなレベルのアクセス権を持つ管理者がさまざまな操作を行うための Web インタフェースです。たとえば、レルムや組織を作成したり、それらのレルムに対してユーザーの作成または削除を行ったり、レルムのリソースへのアクセスを保護および制限するために適用するポリシーを確立するなどの操作を行います。また、現在のユーザーセッションを表示または終了したり、セッションの連携設定の管理 (認証ドメインやプロバイダの作成、削除、変更) も行います。管理者権限を持たないユーザーの場合は、個人情報 (名前、電子メールアドレス、電話番号など) の管理、パスワードの変更、グループへの加入または加入の解除、ロールの表示などを行うことができます。Access Manager コンソールは、以下の 2 つの基本ビューで構成されます。

管理ビュー

管理者ロールを持つユーザーが Access Manager から認証されると、デフォルトのビューが管理ビューになります。このビューでは、管理者は Access Manager に関連するほとんどの管理タスクを実行できます。Access Manager は、レルムモードと旧バージョンモードの 2 つのモードでインストールできます。それぞれのモードには、固有のコンソールが使用されます。レルムモードと旧バージョンモードの詳細は、『Sun Java System Access Manager 7 2005Q4 Technical Overview』を参照してください。

レルムモードのコンソール

管理者はレルムモードのコンソールを使用して、レルムベースのアクセス制御、デフォルトのサービス設定、Web サービスおよび連携を管理できます。管理者ログイン画面にアクセスするには、ブラウザで次のアドレス構文を使用します。

protocol://*servername*/amserver/UI/Login

`protocol` には、配備方法に応じて http または https を指定します。

図 4–1 レルムモードの管理ビュー

旧バージョンモードのコンソール

旧バージョンモードのコンソールは、Access Manager 6.3 アーキテクチャーに基づいて設計されています。この旧バージョンの Access Manager アーキテクチャーでは、Sun Java System Directory Server に備えられている LDAP ディレクトリ情報ツリー (directory information tree、DIT) が使用されます。旧バージョンモードでは、ユーザー情報とアクセス制御情報が LDAP 組織に格納されます。旧バージョンモードを選択した場合、LDAP 組織はアクセス制御レルムに相当します。レルム情報は、LDAP 組織に統合されます。旧バージョンモードでは、「ディレクトリ管理」タブを使用して、Access Manager ベースのアイデンティティー管理を行うことができます。

管理者ログイン画面にアクセスするには、ブラウザで次のアドレス構文を使用します。

protocol`://`*servername*`/amserver/console`

`protocol` には、配備方法に応じて http または https を指定します。

図 4–2 旧バージョンモードの管理ビュー

旧バージョンモード 6.3 コンソール

Access Manager 6.3 の一部の機能は、Access Manager 7.0 コンソールでは使用できません。このため、管理者は 7.0 の旧バージョン配備から 6.3 コンソールにログインできるようになっています。Access Manager を構築する Sun Java System Portal Server またはその他の Sun Java System 通信製品の 主アイデンティティーリポジトリとして、Sun Java System Directory Server を使用しなければならない場合には、通常はこのコンソールを使用します。委任管理やサービスクラスなどのほかの機能には、このコンソールだけからアクセスできます。

注 – 6.3 旧バージョンモードコンソールと 7.0 旧バージョンモードコンソールを交互に使用しないでください。

6.3 コンソールにアクセスするには、ブラウザで次のアドレス構文を使用します。

protocol://*servername*/amconsole

`protocol` には、配備方法に応じて http または https を指定します。

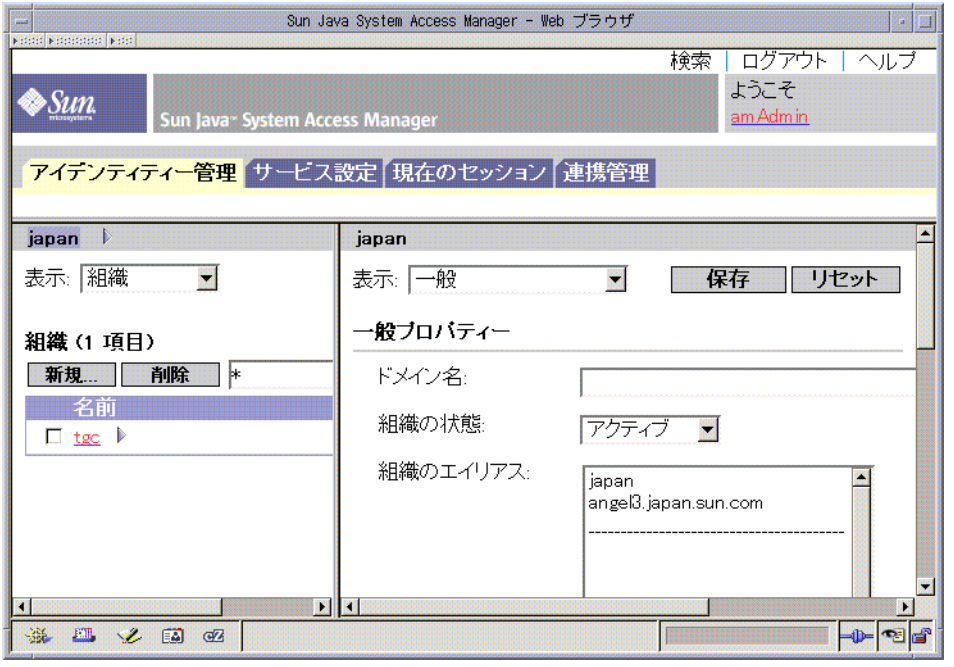

図 4–3 6.3 ベースのコンソールの管理ビュー

ユーザープロファイルビュー

管理者ロールが割り当てられていないユーザーが Access Manager から認証されると、それぞれのユーザープロファイルビューがデフォルトビューになります。ユーザープロファイルビューには、レルムモードまたは旧バージョンモードでアクセスできます。このビューにアクセスするには、「ログイン」ページでそれぞれのユーザー名とパスワードを入力する必要があります。

ユーザープロファイルビューでは、それぞれのユーザープロファイル固有の属性の値を修正できます。たとえば、名前、ホームアドレス、パスワードなどの属性を修正できます。ユーザープロファイルビューに表示された属性は、展開することができます。

図 4–4 ユーザープロファイルビュー

◆ ◆ ◆ 第 5 章

レルムの管理

アクセス制御レルムは、ユーザーまたはユーザーのグループと関連付けることのできる認証プロパティーおよび承認ポリシーのグループです。レルムデータは、指定されたデータストアの内部に Access Manager が作成する独自形式の情報ツリーに格納されます。Access Manager フレームワークは、各レルムに含まれるポリシーおよびプロパティーを Access Manager 情報ツリーの内部に集約します。デフォルトでは、Access Manager 7 は自動的に、ユーザーデータとは別の、Sun Java Enterprise System Directory Server 内の特別なブランチとして Access Manager 情報ツリーを挿入します。アクセス制御レルムは、任意の LDAPv3 データベースの使用中に使用できます。

レルムの詳細については、『Sun Java System Access Manager 7 2005Q4 Technical Overview』を参照してください。

「レルム」タブで、アクセス制御に関する次のプロパティーを設定できます。

- 74 ページの「認証」
- 75 ページの「サービス」
- 76 ページの「権限」

レルムの作成と管理

ここでは、レルムを作成および管理する方法について説明します。

▼ 新しいレルムを作成する

1 「アクセス制御」タブの下の「レルム」リストから「新規」を選択します。

2 次の一般属性を定義します。

名前　レルムの名前を入力します。

親　レルムを作成する位置を定義します。その下に新しいレルムが作成される親のレルムを選択します。

3 次のレルム属性を定義します。

レルムの状態	「アクティブ」または「非アクティブ」の状態を選択します。デフォルトは「アクティブ」です。この属性は、レルムの存続期間中であればいつでも「プロパティー」アイコンを選択して変更できます。「非アクティブ」を選択すると、ログイン時のユーザーアクセスが無効になります。
レルムまたはDNSのエイリアス	レルムのDNS名に対するエイリアス名を追加できます。この属性では、実際のドメインエイリアスだけを使用できます。ランダムな文字列は使用できません。

4 「了解」をクリックして保存するか、「取消し」をクリックして前のページに戻ります。

一般プロパティー

「一般プロパティー」ページには、レルムの基本属性が表示されます。これらのプロパティーを変更するには、「アクセス制御」タブの下の「レルム名」リストからレルムをクリックします。その後、次のプロパティーを編集します。

レルムの状態	「アクティブ」または「非アクティブ」の状態を選択します。デフォルトは「アクティブ」です。この属性は、レルムの存続期間中であればいつでも「プロパティー」アイコンを選択して変更できます。「非アクティブ」を選択すると、ログイン時のユーザーアクセスが無効になります。
レルムまたはDNSのエイリアス	レルムのDNS名に対するエイリアス名を追加できます。この属性では、実際のドメインエイリアスだけを使用できます。ランダムな文字列は使用できません。

プロパティーを編集したら、「保存」をクリックします。

認証

ユーザーがほかの認証モジュールを使ってログインできるようにするには、事前に一般認証サービスをサービスとしてレルムに登録する必要があります。コア認証サービスでは、Access Manager 7管理者がレルムの認証パラメータのデフォルト値を定義できます。その後、指定された認証モジュールでオーバーライド値が定義されない場合にこれらの値を使用できます。コア認証サービスに対するデフォルト値は`amAuth.xml`ファイルで定義され、インストール後にDirectory Serverに格納されます。

詳細については、第 7 章を参照してください。

サービス

Access Manager におけるサービスとは、Access Manager コンソールでひとまとめに管理される属性のグループのことです。社員の氏名、役職、電子メールアドレスなど、関連性のある情報を属性として扱うことができます。ただし、属性は一般に、メールアプリケーションや給与支払サービスのようなソフトウェアモジュール用の設定パラメータとして使用されます。

「サービス」タブでは、多数の Access Manager デフォルトサービスをレルムに追加し、設定できます。次のサービスを追加できます。

- 管理
- ディスカバリサービス
- 国際化設定
- パスワードリセット
- セッション
- ユーザー

注 – Access Manager は、サービスの .xml ファイルの必須属性に一部のデフォルト値が含まれるようにします。値のない必須属性のあるサービスがある場合は、デフォルト値を追加してサービスを再読み込みします。

▼ サービスをレルムに追加する

1. 新しいサービスを追加するレルムの名前をクリックします。
2. 「サービス」タブを選択します。
3. 「サービス」リスト内の「追加」をクリックします。
4. レルムに追加するサービスを選択します。
5. 「次へ」をクリックします。
6. レルム属性を定義して、サービスを設定します。サービス属性の詳細については、オンラインヘルプの「設定」を参照してください。
7. 「終了」をクリックします。

8 サービスのプロパティーを編集するには、「サービス」リスト内の名前をクリックします。

権限

権限は、レルムの内部に存在するロールまたはグループへのアクセス権を定義します。ロールまたはグループは、Access Manager アイデンティティー対象タイプに対するポリシー対象定義として使用されます。権限の割り当てまたは変更を行うには、編集するロールまたはグループの名前をクリックします。割り当てることができる権限には次のものがあります。

- ポリシープロパティーのみに対する読み取りおよび書き込みアクセス
- すべてのレルムプロパティーおよびポリシープロパティーに対する読み取りおよび書き込みアクセス
- すべてのプロパティーおよびサービスに対する読み取り専用アクセス

◆ ◆ ◆ 第 6 章

データストア

データストアは、ユーザー属性およびユーザー設定データを格納できるデータベースです。

Access Manager は、アイデンティティーリポジトリフレームワークに接続するアイデンティティーリポジトリプラグインを提供します。この新しいモデルにより、既存のユーザーデータベースに変更を加える必要なしに、Access Manager ユーザー情報を表示および取得できます。Access Manager フレームワークは、アイデンティティーリポジトリプラグインからのデータをほかの Access Manager プラグインからのデータと統合し、各ユーザーの仮想アイデンティティーを形成します。Access Manager はその後、複数のアイデンティティーリポジトリ間で、認証と承認のプロセスにユニバーサルアイデンティティーを使用できます。仮想ユーザーアイデンティティーは、ユーザーのセッション終了時に破棄されます。

LDAPv3 データストア

Access Manager をレルムモードと旧バージョンモードの両方でインストールするときに、任意の一般 LDAPv3 リポジトリの新しいデータストアインスタンスを作成できます。次の場合に LDAPv3 リポジトリタイプを選択することをお勧めします。

- ロール、サービスのクラス (CoS)、および以前のバージョンの Access Manager との互換性が必要でない場合。
- 既存のディレクトリを使用する場合。
- Sun Java System Directory Server 以外のディレクトリサーバーをアイデンティティーリポジトリに使用する場合。
- Access Manager からアイデンティティーリポジトリに書き込まない場合。
- 平坦なディレクトリ情報ツリー (DIT) を使用する場合。

▼ 新しい LDAPv3 データストアを作成する

次の節では、一般的な LDAPv3 データストアを接続する手順について説明します。

1. 新しいデータストアを追加するレルムを選択します。
2. 「データストア」タブをクリックします。
3. 「データストア」リストから「新規」をクリックします。
4. データストアの名前を入力します。
5. **LDAPv3** リポジトリプラグインの属性を定義します。
6. 「終了」をクリックします。

LDAPv3 リポジトリプラグインの属性

LDAPv3 リポジトリプラグインを設定するために、次の属性を使用できます。

プライマリ LDAP サーバー

接続先 LDAP サーバーの名前を入力します。「ホスト名.ドメイン名:ポート番号」の形式を使用することをお勧めします。

複数の「ホスト:ポート番号」エントリが入力された場合、リスト内の最初のホストへの接続が試みられます。リスト内の次のエントリは、現在のホストへの接続試行が失敗した場合にのみ試行されます。

LDAP バインド DN

現在接続している LDAP サーバーに対して認証を行うために Access Manager が使用する DN 名を指定します。バインドに使用される DN 名を持つユーザーには、「LDAPv3 でサポートされるタイプおよび操作」属性で設定した、正しい追加/変更/削除権限を付与することをお勧めします。

LDAP バインドパスワード

現在接続している LDAP サーバーに対して認証を行うために Access Manager が使用する DN パスワードを指定します。

LDAP バインドパスワード (確認)

パスワードを確認します。

LDAP 組織 DN

このデータストアリポジトリのマッピング先となる DN。これは、このデータストア内で実行されるすべての操作のベース DN となります。

LDAP SSL を有効

有効にすると、Access Manager は HTTPS プロトコルを使用してプライマリサーバーに接続します。

LDAP 接続プールの最小サイズ

接続プール内の接続の初期数を指定します。接続プールを利用すると、新しい接続を毎回作成する必要がなくなります。

LDAP 接続プールの最大サイズ

許容される接続数の上限を指定します。

検索で返される結果の最大数

検索操作で返されるエントリ数の上限を指定します。この制限に達すると、Directory Server は検索要求に一致するあらゆるエントリを返します。

検索タイムアウト

検索要求に割り当てられる最大の秒数を指定します。この制限に達すると、Directory Server は検索要求に一致するあらゆる検索エントリを返します。

LDAP の従う参照

このオプションを有効にすると、ある LDAP サーバーからの別の LDAP サーバーに対する参照が自動的に実行されます。

LDAPv3 リポジトリプラグインクラス名

LDAPv3 リポジトリを実装するクラスファイルの場所を指定します。

属性名マッピング

フレームワークが認識する共通属性をネイティブデータストアにマップできるようにします。たとえば、フレームワークがユーザー状態の判定に `inetUserStatus` を使用する場合に、ネイティブデータストアが実際には `userStatus` を使用することが可能です。属性定義では大文字と小文字が区別されます。

LDAPv3 プラグインでサポートされるタイプおよび操作

この LDAP サーバー上で許可されている、または実行可能な操作を指定します。この LDAPv3 リポジトリプラグインでサポートされている操作はデフォルト操作だけです。LDAPv3 リポジトリプラグインでサポートされている操作は次のとおりです。

- グループ — 読み取り、作成、編集、削除
- レルム — 読み取り、作成、編集、削除、サービス

- ユーザー — 読み取り、作成、編集、削除、サービス
- エージェント — 読み取り、作成、編集、削除

LDAP サーバー設定とタスクに基づいて、これらの操作からアクセス権を削除できますが、アクセス権の追加はできません。

LDAP ユーザー検索属性

このフィールドは、ユーザーの検索を実行するための属性タイプを定義します。たとえば、ユーザーの DN が「uid=k user5,ou=people,dc=iplanet,dc=com」の場合、ネーミング属性は uid です。(uid=*) がユーザーの検索フィルタに付加されます。

LDAP ユーザー検索フィルタ

ユーザーエントリの検索に使用する検索フィルタを指定します。たとえば、「LDAP ユーザー検索属性」が uid で、「LDAP ユーザー検索フィルタ」が (objectClass=inetorgperson) の場合、実際のユーザー検索フィルタは次のようになります。(&(uid=*)(objectClass=inetorgperson))

LDAP ユーザーオブジェクトクラス

ユーザーのオブジェクトクラスを指定します。ユーザーが作成されると、このユーザーオブジェクトクラスのリストがユーザーの属性リストに追加されます。

LDAP ユーザー属性

ユーザーと関連付けられる属性のリストを定義します。このリストにないユーザー属性の読み取りまたは書き込みは一切行うことができません。属性は大文字と小文字が区別されます。ここでオブジェクトクラスと属性スキーマを定義する前に、Directory Server でオブジェクトクラスと属性スキーマが定義されている必要があります。

LDAP グループ検索属性

このフィールドは、グループの検索を実行するための属性タイプを定義します。たとえば、グループ DN が「cn=group1,ou=groups,dc=iplanet,dc=com」で、グループのネーミング属性が cn の場合、(cn=*) がグループ検索フィルタに付加されます。

LDAP グループ検索フィルタ

グループエントリの検索に使用する検索フィルタを指定します。たとえば、「LDAP グループ検索属性」が cn で、「LDAP グループ検索フィルタ」が (objectclass=groupOfUniqueNames) の場合、実際のグループ検索フィルタは ((&(cn=*)(objectclass=groupOfUniqueNames)) になります。

LDAP グループコンテナネーミング属性

グループがコンテナ内に位置する場合に、グループコンテナのネーミング属性を指定します。コンテナ内に位置しない場合、この属性は空のままとされます。たとえば、「cn=group1,ou=groups,dc=iplanet,dc=com」のグループDN が ou=groups 内に位置する場合、グループコンテナネーミング属性は ou です。

LDAP グループコンテナ値

グループコンテナの値を指定します。たとえば、「cn=group1,ou=groups,dc=iplanet,dc=com」のグループ DN がコンテナ名 ou=groups 内に位置する場合、グループコンテナ値は groups になります。

LDAP グループオブジェクトクラス

グループのオブジェクトクラスを指定します。グループが作成されると、グループオブジェクトクラスのこのリストがグループの属性リストに追加されます。

LDAP グループ属性

グループと関連付けられる属性のリストを定義します。このリストにないグループ属性の読み取りまたは書き込みは一切行うことができません。属性は大文字と小文字が区別されます。ここでオブジェクトクラスと属性スキーマを定義する前に、Directory Server でオブジェクトクラスと属性スキーマが定義されている必要があります。

グループメンバーシップの属性名

DN が属する全グループの名前がその値である属性の名前を指定します。デフォルトは memberOf です。

グループメンバーの属性名

このグループに属している DN がその値である属性名を指定します。デフォルトは uniqueMember です。

グループメンバー URL の属性名

このグループに属しているメンバーを決定する LDAP URL がその値である、属性の名前を指定します。デフォルトは memberUrl です。

LDAP ピープルコンテナネーミング属性

ユーザーがピープルコンテナ内に位置する場合に、ピープルコンテナのネーミング属性を指定します。ユーザーがピープルコンテナ内に位置しない場合、このフィールドは空のままとされます。たとえば、ユーザー DN を「uid=kuser5,ou=people,dc=iplanet,dc=com,」とすると、ou=people がピープルコンテナの名前の場合、ネーミング属性は ou です。

LDAP ピープルコンテナ値

ピープルコンテナの値を指定します。デフォルトは people です。たとえば、ユーザー DN を「uid=kuser5,ou=people,dc=iplanet,dc=com」とすると、ou=people がピープルコンテナの名前の場合、ネーミング属性は ou で、people は「LDAP ピープルコンテナ値」です。

LDAP エージェント検索属性

このフィールドは、エージェントの検索を実行するための属性タイプを定義します。デフォルトは uid です。たとえば、エージェントの DN が「uid=kagent1,ou=agents,dc=iplanet,dc=com」の場合、エージェントのネーミング属性は uid です。(uid=*) がエージェントの検索フィルタに付加されます。

LDAP エージェントコンテナネーミング属性

エージェントがエージェントコンテナ内に位置する場合の、エージェントコンテナのネーミング属性。エージェントがエージェントコンテナ内に位置しない場合、このフィールドは空のままとされます。たとえば、ユーザー DN を「uid=kagent1,ou=agents,dc=iplanet,dc=com」とすると、エージェントネーミング属性は ou です。

LDAP エージェントコンテナ値

エージェントコンテナの値を指定します。エージェントがエージェントコンテナ内に位置しない場合は空のままとされます。前の例では、エージェントコンテナ値は agents になります。

LDAP エージェント検索フィルタ

エージェントの検索に使用するフィルタを定義します。実際のエージェント検索フィルタは、このフィールドの値の前に「LDAP エージェント検索属性」の値を付加することによって構築されます。

たとえば、「LDAP エージェント検索属性」が uid で、「LDAP ユーザー検索フィルタ」が (objectClass=sunIdentityServerDevice) の場合、実際のユーザー検索フィルタは次のようになります。(&(uid=*)(objectClass=sunIdentityServ erDevice))

LDAP エージェントオブジェクトクラス

エージェントのオブジェクトクラスを定義します。エージェントが作成されると、エージェントオブジェクトクラスのリストがエージェントの属性リストに追加されます。

LDAP エージェント属性

エージェントと関連付けられる属性のリストを定義します。このリストにないエージェント属性の読み取りまたは書き込みは一切行うことができません。属性は大文字と小文字が区別されます。ここでオブジェクトクラスと属性スキーマを定義する前に、Directory Server でオブジェクトクラスと属性スキーマが定義されている必要があります。

持続検索ベース DN

持続検索に使用するベース DN を定義します。一部の LDAPv3 サーバーは、ルートサフィックスレベルでの持続検索のみをサポートします。

再起動前の持続検索の最大アイドル時間

持続検索を再開するまでの最大アイドル時間を定義します。1 よりも大きい値を設定する必要があります。1 以下の値を設定すると、接続のアイドル時間とは無関係に検索を再開します。

Access Manager がロードバランサとともに配備される場合、一部のロードバランサは、指定された時間アイドル状態が続くとタイムアウトします。この場合、ロードバランサに対して指定された時間よりも小さい値を「再起動前の持続検索の最大アイドル時間」に設定することをお勧めします。

エラーコードのあとの再試行の最大数

「再試行する LDAPException エラーコード」で指定されたエラーコードが返された場合に、持続検索操作を再試行する回数の上限を定義します。

再試行の間の遅延時間

各再試行の前に待機する時間を指定します。これは、持続検索接続にのみ適用されます。

再試行する LDAPException エラーコード

持続検索操作を再試行させるエラーコードを指定します。この属性は持続検索のみに適用され、すべての LDAP 操作に適用されるわけではありません。

AMSDK リポジトリプラグイン

AMSDK アイデンティティーリポジトリは、Access Manager を旧バージョンモードでインストールするときに、自動的に Access Manager 情報ツリーと混合されます。レルムモードでは、AMSDK リポジトリのインストールは選択できますが、アイデンティティーリポジトリは Access Manager 情報ツリーと混合されません。次の場合に AMSDK リポジトリタイプを選択することをお勧めします。

- ロールや CoS など、Sun Java System Directory Server 固有の機能を利用する場合。
- 前のバージョンの Access Manager との互換性を確保する場合。

▼ 新しい **AMSDK** リポジトリプラグインを作成する

1 **Access Manager** リポジトリプラグインを設定するレルムを選択します。

2 「データストア」タブをクリックします。

3 「データストア」リストから「新規」をクリックします。

4 リポジトリプラグインの名前を入力します。

5 「**Access Manager** リポジトリプラグイン」を選択します。

6 「次へ」をクリックします。

7 次のフィールドを定義します。

Access Manager プラグインクラス名	Access Manager リポジトリプラグインを実装するクラスファイルの場所を指定します。
Access Manager 組織	Access Manager によって管理される、Directory Server 内の組織を指す DN。これは、このデータストア内で実行されるすべての操作のベース DN となります。

8 「終了」をクリックします。

◆ ◆ ◆ 第 7 章

7 認証の管理

認証サービスは、Access Manager の配備先にインストールされたすべてのデフォルト認証タイプに対して Web ベースのユーザーインタフェースを提供します。このインタフェースは、アクセスを要求するユーザーに対して、呼び出される認証モジュールに基づいたログイン条件画面を表示して認証資格を収集する動的かつカスタマイズ可能な手段を提供します。このインタフェースは、開発者が実用的な Web アプリケーションを作成するのに役立つ Java 2 Enterprise Edition (J2EE) プレゼンテーションフレームワークである Sun Java System™ Application Framework (*JATO* と呼ばれることもある) を使用して作成されています。

認証の設定

ここでは、配備の認証を設定する方法について説明します。最初の節では、デフォルトの認証モジュールタイプの概要について説明し、必要な事前の設定手順を示します。レルム、ユーザー、ロールなどに対して、同じ認証モジュールタイプの複数の設定インスタンスを設定できます。また、認証に成功するためには複数のインスタンスの条件に合格する必要があるようにするため、認証連鎖を追加することもできます。次の内容で構成されています。

認証モジュールタイプ

認証モジュールは、ユーザー ID やパスワードなどのユーザー情報を収集し、その情報をデータベース内のエントリで確認するプラグインです。ユーザーが認証条件を満たす情報を入力した場合、そのユーザーは要求するリソースへのアクセスを許可されます。ユーザーが認証条件を満たしていない情報を入力した場合、そのユーザーは要求したリソースへのアクセスを拒否されます。Access Manager は、次の 15 タイプの認証モジュールとともにインストールされます。

注 – 一部の認証モジュールタイプでは、認証インスタンスとして使用できるようにするには、事前の設定が必要です。必要に応じて、設定手順がモジュールタイプの説明にリスト表示されています。

コア

Access Manager では、コア認証モジュールばかりではなく、デフォルトで 15 種類の認証モジュールを提供しています。コア認証モジュールでは、認証モジュールの全体的な設定を行います。Active Directory 認証、匿名認証、証明書に基づく認証、HTTP 基本認証、JDBC 認証、LDAP 認証、任意の認証のモジュールを追加して有効にする前に、コア認証モジュールの追加と有効化を行う必要があります。コア認証モジュールおよび LDAP 認証モジュールは両方とも、デフォルトのレルムに対して自動的に有効になります。

「拡張プロパティー」ボタンをクリックすると、レルムに対して定義できる「コア」認証属性が表示されます。グローバル属性はレルムに適用できないので表示されません。

Active Directory

Active Directory 認証モジュールでは、LDAP モジュールと同様の認証が実行されますが、LDAP 認証モジュールの場合の Directory Server ではなく、Microsoft の Active Directory™ サーバーが使用されます。LDAP 認証モジュールを Active Directory サーバー用に設定できますが、このモジュールでは、LDAP と Active Directory 認証の両方を同一レルム下に存在させることができます。

注 – このリリースの Active Directory 認証モジュールでは、ユーザー認証のみがサポートされます。パスワードポリシーは LDAP 認証モジュールのみでサポートされます。

匿名 (anonymous)

デフォルトでは、このモジュールを有効にすると、ユーザーは匿名ユーザーとして Access Manager にログインできるようになります。「有効な匿名ユーザー」のリスト属性を設定して、このモジュールに匿名ユーザーのリストを定義することもできます。匿名アクセスを許可するということは、パスワードなしでアクセスさせるということです。匿名アクセスは、特定の種類のアクセス (読み取りのためのアクセスや検索のためのアクセスなど)、特定のサブツリー、またはディレクトリ内の個別のエントリに制限されます。

証明書

証明書に基づく認証では、個人用デジタル証明書 (PDC) を使用してユーザーを特定し、認証します。Directory Server に格納された PDC に一致すること、また証明書失効リスト (CRL) で確認されていることを求めるように、PDC を設定できます。

証明書に基づく認証モジュールをレルムに追加する前に、行う必要のある作業があります。まず、Access Manager とともにインストールした Web コンテナを保護し、証明書に基づく認証で使用できるように設定する必要があります。証明書に基づくモジュールを有効にする前に、Web Server に対するこれらの初期設定手順について、『*Sun ONE Web Server 6.1* 管理者ガイド』の第 6 章「証明書と鍵の使用」を参照してください。このマニュアルは、次の場所にあります。

```
http://docs.sun.com/db/prod/s1websrv#hic
```

または、次の場所にある『*Sun ONE Application Sever Administrator's Guide to Security*』を参照してください。

http://docs.sun.com/db/prod/s1appsrv#hic (`http://docs.sun.com/db/prod/s1appsrv#hic`)

注 – 証明書に基づくモジュールを使用して認証されるユーザーは、ブラウザ用に PDC を要求する必要があります。使用しているブラウザによって、手順が異なります。詳細は、お使いのブラウザのマニュアルを参照してください。

このモジュールを追加するためには、Access Manager にレルム管理者としてログインし、Access Manager と Web コンテナに対して SSL を設定し、クライアント認証を有効化しておく必要があります。詳細は、第 3 章を参照してください。

HTTP 基本

このモジュールは、HTTP プロトコルのビルトイン認証サポートである基本認証を使用します。Web サーバーはユーザー名とパスワードを求めるクライアント要求を発行し、その情報を認証済み要求の一部としてサーバーに返します。Access Manager ではユーザー名とパスワードを取得し、LDAP 認証モジュールに対してユーザーを内部的に認証します。HTTP 基本認証が正常に機能するために、LDAP 認証モジュールを追加する必要があります (HTTP 基本モジュールを単独で追加しても機能しない)。いったん認証に成功したユーザーには、再認証の際にユーザー名とパスワードの入力は要求されません。

JDBC

JDBC (Java Database Connectivity) 認証モジュールでは、JDBC 技術に対応したドライバを提供する SQL データベースを通して Access Manager でユーザーを認証できるようにするメカニズムが提供されます。SQL データベースへの接続は、JDBC ドライバを通して直接行うか、JNDI 接続プールで行います。

注 – このモジュールは、MySQL4.0 と Oracle 8i でテストされています。

LDAP

LDAP 認証モジュールを使用すると、ユーザーがログインするときに、特定のユーザー DN およびパスワードを使用して、LDAP Directory Server にバインドする必要があります。すべてのレルムに基づく認証では、デフォルトの認証モジュールです。ユーザーが Directory Server に存在するユーザー ID およびパスワードを指定すると、ユーザーは有効な Access Manager セッションへのアクセスが許可され、セットアップされます。コア認証モジュールおよび LDAP 認証モジュールは両方とも、デフォルトのレルムに対して自動的に有効になります。

メンバーシップ

メンバーシップ認証は、`my.site.com` または `mysun.sun.com` のように、パーソナライズされたサイトのように実装されます。モジュールが有効なときに、ユーザーは管理者の支援なしでアカウントを作成し、パーソナライズします。ユーザーは作成したアカウントを使用し、追加済みユーザーとしてアクセスできます。また、ユーザーはビューアのインタフェースにアクセスできます。ビューアのインタフェースは、認証データおよびユーザー設定として、ユーザープロファイルデータベースに保存されています。

MSISDN

MSISDN (Mobile Station Integrated Services Digital Network) 認証モジュールでは、携帯電話などのデバイスに関連するモバイル加入者 ISDN を使用して認証できます。これは対話型モジュールではありません。このモジュールでは加入者 ISDN が取得されて Directory Server で妥当性が検査され、番号が一致するユーザーが検索されます。

RADIUS

Access Manager は、すでにインストールされている RADIUS サーバーと連携するように設定できます。エンタープライズで認証のために旧バージョンの RADIUS サーバーを使用している場合に便利です。RADIUS 認証モジュールを有効にするには、次の 2 つの手順を行います。

1. RADIUS サーバーを設定します。

   詳しい手順については、RADIUS サーバーのマニュアルを参照してください。
2. RADIUS 認証モジュールを登録し、有効にします。

Sun Java System Application Server で RADIUS を設定する

RADUIS クライアントがそのサーバーに対してソケット接続を作成するとき、デフォルトでは、Application Server の `server.policy` ファイルで SocketPermission の connect アクセス権だけが与えられています。RADUIS 認証を正常に機能させるには、次のアクションを許可する必要があります。

- accept (受け入れ)
- connect (接続)
- listen (待機)
- resolve (解決)

ソケット接続のアクセス権を与えるには、Application Server の `server.policy` ファイルにエントリを追加します。SocketPermission は、ホストの指定と、そのホストへの接続方法を指定する一連のアクションとで構成されます。ホストは次のように指定されます。

```
host = hostname | IPaddress:portrange:portrange = portnumber
| -portnumberportnumber-portnumber
```

ホストは、DNS 名または IP アドレスの数値で表されるか、ローカルマシンの場合は localhost と表されます。DNS 名でホストを指定する場合は、ワイルドカード "*" を 1 つだけ使用できます。ワイルドカードを使用する場合は、`*.example.com` のように、左端に置く必要があります。

ポート (またはポート範囲) は省略可能です。`N-` という形式のポート指定は、`N` またはそれ以上の番号を持つすべてのポートを表します。ここで、`N` はポート番号です。`-N` という形式のポート指定は、`N` またはそれ以下の番号を持つすべてのポートを表します。

`listen` アクションは、ローカルホストで使用される場合のみ有効です。`resolve` (ホスト/IP 解決のネームサービスルックアップ) アクションは、ほかの任意のアクションが存在する場合に暗黙的に使用されます。

たとえば、SocketPermission を作成するときに次のアクセス権をコードに与えると、そのコードは `machine1.example.com` のポート `1645` に接続でき、またそのポート上で接続を受け入れることができます。

```
permission java.net.SocketPermission machine1.example.com:1645, "connect,accept";
```

同様に、次のアクセス権を与えられたコードは、ローカルホストのポート 1024 ～ 65535 に接続することと、これらのポートで接続受け入れおよび待機を行うことができます。

```
permission java.net.SocketPermission "machine1.example.com:1645", "connect,accept";
permission java.net.SocketPermission "localhost:1024-", "accept,connect,listen";
```

注 – リモートホストに対する接続受け入れや接続作成のアクセス権をコードに与えると、悪意のあるコードによって、本来アクセス権を持たない第三者に機密データが転送されたり共有されたりしやすくなるので、問題が発生することがあります。適切なアクセス権だけを与えるために、ポート番号を範囲で指定するのではなく、正確なポート番号を指定してください。

SafeWord

Secure Computing の SafeWord™ または SafeWord PremierAccessd™ 認証サーバーに対して送られる SafeWord 認証要求を処理するように、Access Manager を設定できます。Access Manager は、SafeWord 認証のクライアント部分を担当します。SafeWord サーバーは、Access Manager のインストールされているシステムにも、別のシステムにも置くことができます。

Sun Java System Application Server で SafeWord を設定する

SafeWord クライアントがそのサーバーに対してソケット接続を作成するとき、デフォルトでは、Application Server の `server.policy` ファイルで SocketPermission の `connect` アクセス権だけが与えられています。SafeWord 認証を正常に機能させるには、次のアクションを許可する必要があります。

- accept (受け入れ)
- connect (接続)
- listen (待機)
- resolve (解決)

ソケット接続のアクセス権を与えるには、Application Server の `server.policy` ファイルにエントリを追加します。SocketPermission は、ホストの指定と、そのホストへの接続方法を指定する一連のアクションとで構成されます。ホストは次のように指定されます。

```
host = (hostname | IPaddress)[:portrange] portrange =
portnumber | -portnumberportnumber-[portnumber]
```

ホストは、DNS 名または IP アドレスの数値で表されるか、ローカルマシンの場合は localhost と表されます。DNS 名でホストを指定する場合は、ワイルドカード "*" を 1 つだけ使用できます。ワイルドカードを使用する場合は、`*.example.com` のように、左端に置く必要があります。

ポート (portrange) は省略可能です。`N-` という形式のポート指定は、`N` またはそれ以上の番号を持つすべてのポートを表します。ここで、`N` はポート番号です。`-N` という形式のポート指定は、`N` またはそれ以下の番号を持つすべてのポートを表します。

`listen` アクションは、ローカルホストで使用される場合のみ有効です。`resolve` (ホスト/IP 解決のネームサービスルックアップ) アクションは、ほかの任意のアクションが存在する場合に暗黙的に使用されます。

たとえば、SocketPermission を作成するときに次のアクセス権をコードに与えると、そのコードは machine1.example.com のポート 1645 に接続でき、またそのポート上で接続を受け入れることができます。

```
permission java.net.SocketPermission machine1.example.com:5030, "connect,accept";
```

同様に、次のアクセス権を与えられたコードは、ローカルホストのポート 1024 〜 65535 に接続することと、これらのポートで接続受け入れおよび待機を行うことができます。

```
permission java.net.SocketPermission "machine1.example.com:5030", "connect,accept";
permission java.net.SocketPermission "localhost:1024-", "accept,connect,listen";
```

注 – リモートホストに対する接続受け入れや接続作成のアクセス権をコードに与えると、悪意のあるコードによって、本来アクセス権を持たない第三者に機密データが転送されたり共有されたりしやすくなるので、問題が発生することがあります。適切なアクセス権だけを与えるために、ポート番号を範囲で指定するのではなく、正確なポート番号を指定してください。

SAML

SAML (Security Assertion Markup Language) 認証モジュールでは、ターゲットサーバーで SAML アサーションの受信と確認が行われます。このモジュールが、Access Manager 2005Q1 から Access Manager 2005Q4 などのアップグレード後も含めて、ターゲットマシンで設定されている場合にかぎって、SAML SSO は動作します。

SecurID

RSA の ACE/Server 認証サーバーに対して送られる SecurID 認証要求を処理するように、Access Manager を設定できます。Access Manager は、SecurID 認証のクライアント部分を担当します。ACE/Server は、Access Manager のインストールされているシステムにも、別のシステムにも置くことができます。ローカルで管理されたユーザー ID を認証する (admintool (1M) 参照) には、ルートでアクセスする必要があります。

SecurID 認証では、認証ヘルパー amsecuridd を使用します。認証ヘルパーは Access Manager のメインのプロセスとは独立したプロセスです。起動すると、このヘルパーは設定情報を得るためにポートで待機します。Access Manager が nobody として、または root 以外のユーザー ID で実行するようにインストールされている場合でも、*AccessManager-base*/SUNWam/share/bin/amsecuridd プロセスは root ユーザーとして実行する必要があります。amsecuridd ヘルパーについては、第 20 章を参照してください。

注 – このリリースの Access Manager の場合、Linux プラットフォームと Solaris x86 プラットフォームでは SecurID 認証モジュールを使用できません。この 2 つのプラットフォームでは、SecurID 認証モジュールの登録、設定、有効化を行わないでください。SecurID 認証モジュールは、SPARC のみで使用できます。

UNIX

Access Manager がインストールされている Solaris または Linux システムで既知の UNIX ユーザー ID およびパスワードに対する認証要求を処理するように、Access Manager を設定できます。UNIX 認証ではレルム属性は 1 つだけしかなく、またグローバル属性は少ししかありませんが、システムの観点から検討すべき点があります。ローカルで管理されたユーザー ID を認証する (`admintool` (1M) 参照) には、ルートでアクセスする必要があります。

UNIX 認証では、認証ヘルパー `amunixd` を使用します。認証ヘルパーは Access Manager のメインのプロセスとは独立したプロセスです。起動すると、このヘルパーは設定情報を得るためにポートで待機します。UNIX ヘルパーは Access Manager ごとに 1 つだけあり、そのすべてのレルムで共用されます。

Access Manager が `nobody` として、または root 以外のユーザー ID で実行するようにインストールされている場合でも、*AccessManager-base*`/SUNWam/share/bin/amunixd` プロセスは root ユーザーとして実行する必要があります。UNIX 認証モジュールは、UNIX 認証要求を待機するために `localhost:58946` へのソケットを開くことで、`amunixd` デーモンを呼び出します。デフォルトのポートで `amunixd` ヘルパーを実行するには、次のコマンドを入力します。

```
./amunixd
```

デフォルト以外のポートで `amunixd` ヘルパーを実行するには、次のコマンドを入力します。

```
./amunixd [-c portnm] [ipaddress]
```

ipaddress と portnumber は、`AMConfig.properties` 内の `UnixHelper.ipadrs` 属性 (IPV4 形式) と `UnixHelper.port` 属性で指定されています。`amunixd` を `amserver` コマンド行ユーティリティーから実行することもできます。`amserver` は `AMConfig.properties` からポート番号と IP アドレスを取り出し、このプロセスを自動的に実行します。

`/etc/nsswitch.conf` ファイル内の `passwd` エントリでは、`/etc/passwd` および `/etc/shadow` ファイル、または NIS を認証で探すかどうかを指定します。

Windows デスクトップ SSO

Windows デスクトップ SSO 認証モジュールは、Windows 2000™ に使用する、Kerberos ベースのプラグインモジュールです。このサービスを使用すると、Kerberos Distribution Center (KDC) で認証されたユーザーは、ログインの条件を再度提示しなくても Access Manager に認証されます (シングルサインオン)。

ユーザーは、SPNEGO (Simple and Protected GSS-API Negotiation Mechanism) プロトコルで Access Manager に Kerberos トークンを送信します。この認証モジュールで Access Manager への Kerberos ベースのシングルサインオンを実行するには、ユーザーが、クライアントサイドにおいて、SPNEGO プロトコルをサポートして自分自身を認証する必要があります。一般的に、このプロトコルをサポートするすべてのユーザーは、このモジュールを使用して Access Manager に認証できます。クライアントサイドでトークンを使用できるかどうかにより、SPENGO トークンか Kerberos トークンがこのモジュールによって提供されます。どちらの場合でもプロトコルは同一です。Microsoft Windows 2000 以上で動作している Microsoft Internet Explorer 5.01 以上では、現在このプロトコルがサポートされています。Solaris 9 および 10 の Mozilla 1.4 では SPNEGO がサポートされますが、Solaris では SPNEGO がサポートされていないので、返されるトークンは KERBEROS トークンのみです。

注 – Kerberos V5 認証モジュールの新機能を使用するには、JDK 1.4 以上を使用する必要があります。この SPNEGO モジュールで Kerberos ベースの SSO を実行するには、Java GSS API を使用する必要があります。

Internet Explorer の既知の制限事項

WindowsDesktopSSO 認証に Microsoft Internet Explorer 6.x を使用しており、WindowsDesktopSSO モジュールで設定されている KDC レルムと一致する、ユーザーの Kerberos/SPNEGO トークンにこのブラウザでアクセスできない場合、WindowsDesktopSSO モジュールへの認証がエラーになったあとで、このブラウザはその他のモジュールに対して不正に動作します。この問題の直接的な原因は、Internet Explorer が WindowsDesktopSSO モジュールでエラーになると、ブラウザを再起動するまで、コールバックを要求されても、別のモジュールのコールバックを Access Manager に渡すことができなくなることです。このため、WindowsDesktopSSO のあとのすべてのモジュールは、ユーザー資格が NULL であるためにエラーとなります。

関連情報については、次の資料を参照してください。

http://support.microsoft.com/default.aspx?scid=kb;en-us;308074
(http://support.microsoft.com/default.aspx?scid=kb;en-us;308074)

http://www.wedgetail.com/jcsi/sso/doc/guide/troubleshooting.html#ieNTLM
(http://support.microsoft.com/default.aspx?scid=kb;en-us;308074)

Windows デスクトップ SSO の設定

Windows デスクトップ SSO 認証を有効にするプロセスには、次の 2 つの段階があります。

1. Windows 2000 のドメインコントローラにユーザーを作成します。
2. Internet Explorer をセットアップします。

▼ Windows 2000 のドメインコントローラにユーザーを作成する

1 ドメインコントローラで、**Access Manager** 認証モジュール用のユーザーアカウントを作成します。

   a. 「スタート」メニューから、「プログラム」>「管理ツール」に進みます。

   b. 「**Active Directory** ユーザーとコンピュータ」を選択します。

   c. **Access Manager** ホスト名をユーザー **ID (**ログイン名**)** として新しいユーザーを作成します。**Access Manager** ホスト名には、ドメイン名を含めないでください。

2 ユーザーアカウントをサービスプロバイダの名前と関連付け、**Keytab** ファイルを **Access Manager** がインストールされたシステムにエクスポートします。そのためには、次のコマンドを実行します。

```
ktpass -princ host/hostname.domainname@DCDOMAIN -pass password -mapuser userName-out
hostname.host.keytab
ktpass -princ HTTP/hostname.domainname@DCDOMAIN -pass
password -mapuser userName-out hostname
.HTTP.keytab
```

`ktpass` コマンドには、次のパラメータを使用できます。

hostname: Access Manager が稼働する、ドメイン名なしのホスト名です。

domainname: Access Manager のドメイン名です。

DCDOMAIN: ドメインコントローラのドメイン名です。この名前は、Access Manager のドメイン名とは異なる場合があります。

password: ユーザーアカウントのパスワードです。`ktpass` はパスワードを検証しないので、パスワードが正しいことを確認してください。

userName: ユーザーアカウント ID です。これはホスト名と同じにする必要があります。

注 – 両方の Keytab ファイルがセキュリティー保護されているようにします。

サービステンプレートの値は、次の例のようになっている必要があります。

「サービス主体」: `HTTP/machine1.EXAMPLE.COM@ISQA.EXAMPLE.COM`

「**Keytab** ファイル名」: `/tmp/machine1.HTTP.keytab`

「**Kerberos** レルム」: `ISQA.EXAMPLE.COM`

「**Kerberos** サーバー名」: `machine2.EXAMPLE.com`

「ドメイン名を含む主体を返す」: `false`

「認証レベル」: `22`

3 サーバーを再起動します。

▼ Internet Explorer をセットアップする

この手順は、Microsoft Internet Explorer™ 6 以上に当てはまります。これよりも前のバージョンを使用している場合は、Access Manager がブラウザのインターネットゾーンにあり、ネイティブ Windows 認証が有効であることを確認します。

1 「ツール」メニューで、「インターネット オプション」>「詳細設定」>「セキュリティー」に進みます。

2 「統合 **Windows** 認証を使用する」オプションを選択します。

3 「セキュリティー」>「イントラネット」に進みます。

a. 「レベルのカスタマイズ」を選択します。「ユーザー認証」の「ログオン」で「イントラネットゾーンでのみ自動的にログオンする」オプションを選択します。

b. 「サイト」に進み、すべてのオプションを選択します。

c. 「詳細設定」をクリックして、**Access Manager** をローカルゾーンに追加します **(**まだ追加されていない場合**)**。

Windows NT

Access Manager は、すでにインストールされている Windows NT サーバーまたは Windows 2000 サーバーで使用できるように設定できます。Access Manager は、NT 認証のクライアント部分を担当します。

1. NT サーバーを設定します。詳しい手順については、Windows NT サーバーのマニュアルを参照してください。
2. Windows NT 認証モジュールを追加し、有効にする前に、Samba クライアントを入手してインストールし、Solaris システム上の Access Manager と通信できるようにする必要があります。

Samba クライアントのインストール

Windows NT 認証モジュールをアクティブにするには、Samba Client 2.2.2 をダウンロードして次のディレクトリにインストールする必要があります。

```
AccessManager-base/SUNWam/bin
```

Samba Client は、Windows マシンと UNIX マシンを共存させるためのファイルサーバー兼プリントサーバーで、専用の Windows NT/2000 Server を必要としません。詳細とダウンロードについては、http://wwws.sun.com/software/download/products/3e3af224.html を参照してください。

Red Hat Linux とともに出荷される Samba クライアントは、次のディレクトリに置かれています。

```
/usr/bin
```

Linux 用 Windows NT 認証モジュールを使って認証を行うためには、クライアントのバイナリを Access Manager の次のディレクトリにコピーします。

AccessManager-base/sun/identity/bin

注 – 複数のインタフェースがある場合には、追加の設定が必要です。複数のインタフェースは smb.conf ファイルで設定し、それを mbclient へ伝えることにより、設定できます。

認証モジュールインスタンス

デフォルトの認証モジュールに基づいて、複数の認証モジュールインスタンスをレルム用に作成できます。同じ認証モジュールを元に、個別に設定した複数のインスタンスを追加できます。

▼ 新しい認証モジュールインスタンスを作成する

1. 新しい認証モジュールインスタンスを追加するレルムの名前をクリックします。
2. 「認証」タブを選択します。

注 –「管理者認証設定」ボタンにより、管理者専用に認証サービスを定義できます。この属性は、管理者とエンドユーザーの認証モジュールを別々のものにする必要がある場合に使用できます。この属性で設定したモジュールは、Access Manager コンソールにアクセスするときに選択されます。

---

3. 「モジュールインスタンス」リストの「新規」をクリックします。
4. 認証モジュールインスタンスの名前を入力します。名前は一意にする必要があります。
5. レルムの認証モジュールタイプの「タイプ」を選択します。
6. 「作成」をクリックします。
7. 新しく作成したモジュールインスタンスの名前をクリックし、そのモジュールのプロパティーを編集します。各モジュールタイプのプロパティーの定義については、オンラインヘルプの「認証」の節を参照してください。

8 複数のモジュールインスタンスを追加するときは、これらの手順を繰り返します。

認証連鎖

1 つ以上の認証モジュールが設定できるので、ユーザーは認証資格をすべての認証モジュールに渡す必要があります。これは、認証連鎖と呼ばれます。Access Manager での認証連鎖は、認証サービスに統合された JAAS フレームワークを使用して実現されます。モジュール連鎖は、認証設定サービスの下に設定されます。

▼ 新しい認証連鎖を作成する

1 新しい認証連鎖を追加するレルムの名前をクリックします。

2 「認証」タブを選択します。

3 「認証連鎖」リストの「新規」をクリックします。

4 認証連鎖の名前を入力します。

5 「作成」をクリックします。

6 「追加」をクリックし、連鎖に含める認証モジュールインスタンスを定義します。そのためには、「インスタンス」リストからモジュールインスタンス名を選択します。このリストに表示されるモジュールインスタンス名は、「モジュールインスタンス」属性で作成されます。

7 連鎖の条件を選択します。以上のフラグによって、認証モジュールの適用条件が確立されます。適用には階層があります。「必須」がもっとも高く、「オプション」がもっとも低くなります。

必要	認証にはモジュールインスタンスが必要です。認証に成功すると、「認証連鎖」リストの次のインスタンスへと認証が進行します。認証に失敗すると、制御がただちにアプリケーションに返されます。この場合、「認証連鎖」リストの次のインスタンスには認証が進行しません。
必須	認証には、このモジュールへの認証が必要です。この連鎖の必須モジュールのいずれかが失敗すると、最終的に認証連鎖全体が失敗します。ただし、必須モジュールが成功しても失敗しても、連鎖の次のモジュールへと制御が進行します。
十分	認証にモジュールインスタンスは必要ありません。認証に成功するとすぐに、制御がアプリケーションに返されます。この場合、モジュールインスタンスリストの次のインスタンスには認証が進行しません。認証に失敗すると、「認証連鎖」リストの次のインスタンスへと認証が進行します。

オプション	認証にモジュールインスタンスは必要ありません。認証に成功しても失敗しても、「認証連鎖」リストの次のインスタンスへと認証が進行します。

8 連鎖のオプションを入力します。これにより、モジュールの追加オプションがキーと値のペアとして有効になります。複数のオプションを指定するときは、スペースで区切ります。

9 次の属性を定義します。

「成功したログイン URL」	認証が成功した場合にユーザーをリダイレクトする URL を指定します。
「失敗したログイン URL」	認証が成功しなかった場合にユーザーをリダイレクトする URL を指定します。
「認証ポストプロセスクラス」	ログインが成功または失敗したあとに認証ポストプロセスのカスタマイズに使用する Java クラスの名前を定義します。

10 「保存」をクリックします。

認証タイプ

認証サービスは、さまざまな認証適用方法を提供します。それらの異なる認証方法にアクセスするには、ログイン URL パラメータを指定するか、認証 API を使用します。詳細については、『Sun Java System Access Manager 7 2005Q4 Developer's Guide』の第 5 章「Using Authentication APIs and SPIs」を参照してください。認証モジュールを設定する前に、特定の認証モジュール名を含むように、コア認証サービス属性のレルム認証モジュールを修正する必要があります。

認証設定サービスは、次の認証タイプ用の認証モジュールを定義するために使用します。

- 102 ページの「レルムに基づく認証」
- 105 ページの「組織に基づく認証」
- 107 ページの「ロールに基づく認証」
- 110 ページの「サービスに基づく認証」
- 113 ページの「ユーザーに基づく認証」
- 116 ページの「認証レベルに基づく認証」
- 118 ページの「モジュールに基づく認証」

認証モジュールは、これらの認証タイプのいずれかで定義すると、認証プロセスの成功または失敗に基づいて、ポストプロセス Java クラス仕様だけでなく、リダイレクト URL も提供するように設定できます。

認証タイプによってアクセスが決定される方法

各認証方法では、ユーザーは認証に成功するか失敗します。成功または失敗の決定後、各方法では次の手順を実行します。手順 1 ～ 3 は認証が成功した場合に実行され、手順 4 は成功した認証と失敗した認証の両方で実行されます。

1. Access Manager によって、認証されたユーザーが Directory Server データストアに定義されているかどうか、またプロファイルが有効であるかどうかが確認されます。

   コア認証モジュールの「ユーザープロファイル」属性は、「必須」、「動的」、「ユーザーエイリアスを使用して動的に」、または「無視」として定義できます。認証に成功すると、Access Manager によって、認証されたユーザーが Directory Server データストアに定義されているかどうかが確認され、「ユーザープロファイル」の値が「必須」である場合は、プロファイルが有効かどうかが確認されます。これはデフォルトの場合です。「ユーザープロファイル」が動的な設定である場合、認証サービスはユーザープロファイルを Directory Server のデータストアに作成します。「ユーザープロファイル」が「無視」に設定されている場合は、ユーザーの検証は行われません。

2. 認証ポストプロセス SPI が実行されます。

   コア認証モジュールには、値として認証ポストプロセスクラス名を含む「認証ポストプロセスクラス」属性が含まれています。`AMPostAuthProcessInterface` は、ポストプロセスインタフェースです。このインタフェースは、認証の成功または失敗時、またはログアウト時に実行できます。

3. セッショントークンで次のプロパティーが追加または更新され、ユーザーのセッションがアクティブになります。

   realm: これは、ユーザーが所属するレルムの DN です。

   Principal: ユーザーの DN です。

   Principals: ユーザーが認証を受けた名前のリストです。このプロパティーは、パイプで区切られたリストとして定義された複数の値を持つことができます。

   UserId: モジュールが返すユーザーの DN であるか、LDAP またはメンバーシップ以外のモジュールの場合はユーザー名です。すべての Principal は、同じユーザーにマッピングされる必要があります。UserId は、すべての Principal がマッピングされるユーザー DN です。

   注 – このプロパティーは、DN 以外の値になることがあります。

   UserToken: ユーザー名です。すべての Principal は、同じユーザーにマッピングされる必要があります。UserToken は、すべての Principal がマッピングされるユーザー名です。

   Host: クライアント用のホスト名または IP アドレスです。

   authLevel: ユーザーが認証を受けた最高のレベルです。

AuthType: ユーザーが認証を受けた認証モジュールの、パイプで区切られたリストです (例、`module1|module2|module3`)。

clientType: クライアントブラウザのデバイスタイプです。

Locale: クライアントのロケールです。

CharSet: クライアント用に定めらた文字セットです。

Role: ロールに基づく認証にのみ適用可能であり、ユーザーが属すロールです。

Service: サービスに基づく認証にのみ適用可能であり、ユーザーが属すサービスです。

4. Access Manager は、成功または失敗した認証のあとにユーザーをリダイレクトする場所についての情報を検索します。

   URL のリダイレクトは、Access Manager のページまたは URL のどちらかにすることができます。リダイレクトは、Access Manager が認証方法に基づいて、また認証が成功したか失敗したかによってリダイレクトを検索する優先順位のもとに行われます。この順序については、次の認証方法についての節の、URL のリダイレクトの部分で詳しく説明します。

URL のリダイレクト

認証設定サービスでは、成功または失敗した認証に対する URL のリダイレクトを割り当てることができます。その URL 自体は、認証設定サービスの「ログイン成功 URL」および「ログイン失敗 URL」属性で定義します。URL のリダイレクトを有効にするために、ロール、レルム、またはユーザー用に設定するように、認証設定サービスをレルムに追加し、利用可能にする必要があります。認証設定サービスの追加時は、LDAP で必須、というように認証モジュールを追加するようにしてください。

レルムに基づく認証

この認証方式により、ユーザーはレルムまたはサブレルムの認証を受けることができます。これは、Access Manager のデフォルトの認証方法です。レルムの認証方法は、コア認証モジュールをレルムに登録し、「レルム認証設定」属性を定義することによって設定します。

レルムに基づく認証ログイン URL

認証のレルムは、ユーザーインタフェースのログイン URL に `realm` パラメータまたは `domain` パラメータを定義して指定できます。認証の要求のレルムは、次の優先順位で判断されます。

1. `domain` パラメータ。
2. `realm` パラメータ。

3. 管理サービスの「DNS エイリアス名」属性の値。

   正しいレルムを呼び出したあと、ユーザーが認証を受ける認証モジュールは、コア認証サービスの「レルム認証設定」属性から取得されます。レルムに基づく認証を指定し、開始するログイン URL を次に示します。

   ```
   http://server_name.domain_name:port/amserver/UI/Login
   http://server_name.domain_name:port/amserver/UI/Login?domain=domain_name
   http://server_name.domain_name:port/amserver/UI/Login?realm=realm_name
   ```

   定義されたパラメータがない場合、レルムはログイン URL に指定されたサーバーホストとドメインから判断されます。

レルムに基づく認証リダイレクト URL

組織に基づく認証が成功または失敗した時に、Access Manager はユーザーのリダイレクト先の情報を検索します。この情報をアプリケーションが検索する優先順位を次に示します。

レルムに基づく認証が成功した場合のリダイレクト URL

レルムに基づく認証が成功した場合のリダイレクト URL は、次の場所を次の優先順位で確認することによって判断されます。

1. 認証モジュールで設定された URL。
2. goto ログイン URL パラメータで設定された URL。
3. ユーザーのプロファイル (amUser.xml) の iplanet-am-user-success-url 属性用に clientType カスタムファイルに設定された URL。
4. ユーザーのロールエントリの iplanet-am-auth-login-success-url 属性用に clientType カスタムファイルに設定された URL。
5. ユーザーのレルムエントリの iplanet-am-auth-login-success-url 属性用に clientType カスタムファイルに設定された URL。
6. グローバルデフォルトとして iplanet-am-auth-login-success-url 属性用に clientType カスタムファイルに設定された URL。
7. ユーザーのプロファイル (amUser.xml) の iplanet-am-user-success-url 属性に設定された URL。
8. ユーザーのロールエントリの iplanet-am-auth-login-success-url 属性に設定された URL。
9. ユーザーのレルムエントリの iplanet-am-auth-login-success-url 属性に設定された URL。
10. グローバルデフォルトとして iplanet-am-auth-login-success-url 属性に設定された URL。

レルムに基づく認証に失敗した場合のリダイレクト URL

レルムに基づく認証に失敗した場合のリダイレクト URL は、次の場所を次の順序で確認することによって判断されます。

1. 認証モジュールで設定された URL。
2. `gotoOnFail` ログイン URL パラメータで設定された URL。
3. ユーザーのエントリ (`amUser.xml`) の `iplanet-am-user-failure-url` 属性用に `clientType` カスタムファイルに設定された URL。
4. ユーザーのロールエントリの `iplanet-am-auth-login-failure-url` 属性用に `clientType` カスタムファイルに設定された URL。
5. ユーザーのレルムエントリの `iplanet-am-auth-login-failure-url` 属性用に `clientType` カスタムファイルに設定された URL。
6. グローバルデフォルトとして `iplanet-am-auth-login-failure-url` 属性用に `clientType` カスタムファイルに設定された URL。
7. ユーザーのエントリ (`amUser.xml`) の `iplanet-am-user-failure-url` 属性用に設定された URL。
8. ユーザーのロールエントリの `iplanet-am-auth-login-failure-url` 属性に設定された URL。
9. ユーザーのレルムエントリの `iplanet-am-auth-login-failure-url` 属性に設定された URL。
10. グローバルデフォルトとして `iplanet-am-auth-login-failure-url` 属性に設定された URL。

レルムに基づく認証を設定する

認証モジュールは、最初にコア認証サービスをレルムに追加することで、レルム用に設定できます。

▼ レルムの認証属性を設定する

1 認証連鎖を追加するレルムに移動します。

2 「認証」タブをクリックします。

3 プルダウンメニューから「デフォルト認証連鎖」を選択します。

4 プルダウンメニューから「管理者認証連鎖」を選択します。この属性は、管理者とエンドユーザーの認証モジュールを別々のものにする必要がある場合に使用できます。デフォルトの認証モジュールは **LDAP** です。

5 認証連鎖を定義したら、「保存」をクリックします。

組織に基づく認証

この認証タイプは、旧バージョンモードでインストールされた Access Manager の配備先にのみ適用されます。

この認証方法では、ユーザーが組織またはサブ組織に対する認証を受けることができます。これは、Access Manager のデフォルトの認証方法です。組織の認証方法は、コア認証モジュールを組織に登録し、「組織認証設定」属性を定義することによって設定します。

組織に基づく認証のログイン URL

認証のための組織は、ユーザーインタフェースのログイン URL に `org` パラメータまたは `domain` パラメータを定義して指定できます。認証の要求の組織は、次の優先順位で判断されます。

1. `domain` パラメータ。
2. `org` パラメータ。
3. 管理サービスの「`DNS` エイリアス名」 (組織のエイリアス名) 属性の値。

   正しい組織を呼び出したあと、ユーザーが認証を受ける認証モジュールは、コア認証サービスの「組織認証設定」属性から取得されます。組織に基づく認証を指定し、開始するログイン URL を次に示します。

   ```
   http://server_name.domain_name:port/amserver/UI/Login
   http://server_name.domain_name:port/amserver/UI/Login?domain=domain_name
   http://server_name.domain_name:port/amserver/UI/Login?org=org_name
   ```

   定義されたパラメータがない場合、組織はログイン URL に指定されたサーバーホストとドメインから判断されます。

組織に基づく認証のリダイレクト URL

組織に基づく認証が成功または失敗した時に、Access Manager はユーザーのリダイレクト先の情報を検索します。この情報をアプリケーションが検索する優先順位を次に示します。

組織に基づく認証が成功した場合のリダイレクト URL

組織に基づく認証が成功した場合のリダイレクト URL は、次の場所を次の優先順位で確認することによって判断されます。

1. 認証モジュールで設定された URL。
2. `goto` ログイン URL パラメータで設定された URL。
3. ユーザーのプロファイル (`amUser.xml`) の `iplanet-am-user-success-url` 属性用に `clientType` カスタムファイルに設定された URL。

4. ユーザーのロールエントリの iplanet-am-auth-login-success-url 属性用に clientType カスタムファイルに設定された URL。
5. ユーザーの組織エントリの iplanet-am-auth-login-success-url 属性用に clientType カスタムファイルに設定された URL。
6. グローバルデフォルトとして iplanet-am-auth-login-success-url 属性用に clientType カスタムファイルに設定された URL。
7. ユーザーのプロファイル (amUser.xml) の iplanet-am-user-success-url 属性に設定された URL。
8. ユーザーのロールエントリの iplanet-am-auth-login-success-url 属性に設定された URL。
9. ユーザーの組織エントリの iplanet-am-auth-login-success-url 属性に設定された URL。
10. グローバルデフォルトとして iplanet-am-auth-login-success-url 属性に設定された URL。

組織に基づく認証に失敗した場合のリダイレクト URL

組織に基づく認証に失敗した場合のリダイレクト URL は、次の場所を次の順序で確認することによって判断されます。

1. 認証モジュールで設定された URL。
2. gotoOnFail ログイン URL パラメータで設定された URL。
3. ユーザーのエントリ (amUser.xml) の iplanet-am-user-failure-url 属性用に clientType カスタムファイルに設定された URL。
4. ユーザーのロールエントリの iplanet-am-auth-login-failure-url 属性用に clientType カスタムファイルに設定された URL。
5. ユーザーの組織エントリの iplanet-am-auth-login-failure-url 属性用に clientType カスタムファイルに設定された URL。
6. グローバルデフォルトとして iplanet-am-auth-login-failure-url 属性用に clientType カスタムファイルに設定された URL。
7. ユーザーのエントリ (amUser.xml) の iplanet-am-user-failure-url 属性用に設定された URL。
8. ユーザーのロールエントリの iplanet-am-auth-login-failure-url 属性に設定された URL。
9. ユーザーの組織エントリの iplanet-am-auth-login-failure-url 属性に設定された URL。
10. グローバルデフォルトとして iplanet-am-auth-login-failure-url 属性に設定された URL。

組織に基づく認証を設定する

認証モジュールは、最初にコア認証サービスを組織に追加することで、組織用に設定できます。

▼ 組織の認証属性を設定する

1. 認証連鎖を追加する組織に移動します。
2. 「認証」タブをクリックします。
3. プルダウンメニューから「デフォルト認証連鎖」を選択します。
4. プルダウンメニューから「管理者認証連鎖」を選択します。この属性は、管理者とエンドユーザーの認証モジュールを別々のものにする必要がある場合に使用できます。デフォルトの認証モジュールは**LDAP**です。
5. 認証連鎖を定義したら、「保存」をクリックします。

ロールに基づく認証

この認証方法では、ユーザーはレルムまたはサブレルム内の (静的またはフィルタリングされた) ロールに対する認証を受けることができます。

注 – 認証設定サービスは、レルムに登録してからでなければロールにインスタンスとして登録できません。

認証を成功させるには、ユーザーはロールに属し、そのロールに設定された認証設定サービスインスタンスに定義された各モジュールに対する認証を受ける必要があります。ロールに基づく認証の各インスタンスに対して、次の属性を指定できます。

「競合の解決レベル」: 同一のユーザーが含まれることがある 2 つの異なるロールに定義された認証設定サービスインスタンスに対する優先レベルを設定します。たとえば、`User 1` が `Role 1` および `Role 2` に割り当てられている場合を想定します。ユーザーが認証を試みたときに、認証の成功または失敗時のリダイレクトや認証後プロセスに対して `Role 1` の優先順位がより高くなるように、`Role1` により高い競合解決レベルを設定することができます。

「認証設定」: ロールの認証プロセスに設定された認証モジュールを定義します。

「ログイン成功 **URL**」: 認証が成功した場合にユーザーがリダイレクトされる URL を定義します。

「ログイン失敗 **URL**」: 認証が失敗した場合にユーザーがリダイレクトされる URL を定義します。

「認証ポストプロセスクラス」: 認証後インタフェースを定義します。

ロールに基づく認証のログイン **URL**

ロールに基づく認証は、ユーザーインタフェースのログイン URL にロールパラメータを定義して指定できます。正しいロールを呼び出したあと、ユーザーが認証を受ける認証モジュールは、そのロールに定義された認証設定サービスインスタンスから取得されます。

このロールに基づく認証を指定し開始するログイン URL を次に示します。

```
http://server_name.domain_name:port/amserver/UI/Login?role=role_name
http://server_name.domain_name:port/amserver/UI/Login?realm=realm_name&role=role_name
```

realm パラメータが設定されていない場合、ロールが属すレルムはログイン URL そのものに指定されたサーバーホストおよびドメインから判断されます。

ロールに基づく認証のリダイレクト **URL**

ロールに基づく認証が成功または失敗した時に、Access Manager はユーザーのリダイレクト先の情報を検索します。この情報をアプリケーションが検索する優先順位を次に示します。

ロールに基づく認証が成功した場合のリダイレクト **URL**

ロールに基づく認証が成功した場合のリダイレクト URL は、次の場所を次の順序で確認することによって判断されます。

1. 認証モジュールで設定された URL。
2. `goto` ログイン URL パラメータで設定された URL。
3. ユーザーのプロファイル (`amUser.xml`) の `iplanet-am-user-success-url` 属性用に `clientType` カスタムファイルに設定された URL。
4. ユーザーが認証を受けたロールの `iplanet-am-auth-login-success-url` 属性用に `clientType` カスタムファイルに設定された URL。
5. 認証されたユーザーの別のロールエントリの `iplanet-am-auth-login-success-url` 属性用に `clientType` カスタムファイルに設定された URL。このオプションは、前のリダイレクト URL が失敗した場合の代替リダイレクト URL です。
6. ユーザーのレルムエントリの `iplanet-am-auth-login-success-url` 属性用に `clientType` カスタムファイルに設定された URL。
7. グローバルデフォルトとして `iplanet-am-auth-login-success-url` 属性用に `clientType` カスタムファイルに設定された URL。

8. ユーザーのプロファイル (amUser.xml) の iplanet-am-user-success-url 属性に設定された URL。
9. ユーザーが認証を受けたロールの iplanet-am-auth-login-success-url 属性に設定された URL。
10. 認証されたユーザーの別のロールエントリの iplanet-am-auth-login-success-url 属性に設定された URL。このオプションは、前のリダイレクト URL が失敗した場合の代替リダイレクト URL です。
11. ユーザーのレルムエントリの iplanet-am-auth-login-success-url 属性に設定された URL。
12. グローバルデフォルトとして iplanet-am-auth-login-success-url 属性に設定された URL。

ロールに基づく認証が失敗した場合のリダイレクト URL

ロールに基づく認証が失敗した場合のリダイレクト URL は、次の場所を次の順序で確認することによって判断されます。

1. 認証モジュールで設定された URL。
2. goto ログイン URL パラメータで設定された URL。
3. ユーザーのプロファイル (amUser.xml) の iplanet-am-user-failure-url 属性用に clientType カスタムファイルに設定された URL。
4. ユーザーが認証を受けたロールの iplanet-am-auth-login-failure-url 属性用に clientType カスタムファイルに設定された URL。
5. 認証されたユーザーの別のロールエントリの iplanet-am-auth-login-failure-url 属性用に clientType カスタムファイルに設定された URL。このオプションは、前のリダイレクト URL が失敗した場合の代替リダイレクト URL です。
6. ユーザーのレルムエントリの iplanet-am-auth-login-failure-url 属性用に clientType カスタムファイルに設定された URL。
7. グローバルデフォルトとして iplanet-am-auth-login-failure-url 属性用に clientType カスタムファイルに設定された URL。
8. ユーザーのプロファイル (amUser.xml) の iplanet-am-user-failure-url 属性に設定された URL。
9. ユーザーが認証を受けたロールの iplanet-am-auth-login-failure-url 属性に設定された URL。
10. 認証されたユーザーの別のロールエントリの iplanet-am-auth-login-failure-url 属性に設定された URL。このオプションは、前のリダイレクト URL が失敗した場合の代替リダイレクト URL です。
11. ユーザーのレルムエントリの iplanet-am-auth-login-failure-url 属性に設定された URL。

12. グローバルデフォルトとして iplanet-am-auth-login-failure-url 属性に設定された URL。

▼ ロールに基づく認証を設定する

1 認証設定サービスを追加するレルム (または組織) に移動します。

2 「対象」タブをクリックします。

3 「フィルタロール」または「ロール」です。

4 認証設定を設定するロールを選択します。
認証設定サービスがロールに追加されていない場合は、「追加」をクリックし、「認証サービス」を選択して「次へ」をクリックします。

5 プルダウンメニューから、有効にする「デフォルト認証連鎖」を選択します。

6 「保存」をクリックします。

注 – 新しいロールを作成している場合、そのロールに認証設定サービスは自動的に割り当てられません。ロールを作成する前に、ロールプロファイルページの上部で認証設定サービスを選択していることを確認してください。

ロールに基づく認証が有効になっているときは、LDAP 認証モジュールはデフォルトのままにでき、メンバーシップを設定する必要はありません。

サービスに基づく認証

この認証方法では、ユーザーはレルムまたはサブレルムに登録された特定のサービスまたはアプリケーションに対する認証を受けることができます。このサービスは、認証設定サービス内でサービスインスタンスとして設定され、インスタンス名が関連付けられます。認証を成功させるには、ユーザーはサービスに設定された認証設定サービスインスタンスに定義された各モジュールに対して認証を受ける必要があります。サービスに基づく認証の各インスタンスに対して、次の属性を指定できます。

「認証設定」: サービスの認証プロセスに設定された認証モジュールを定義します。

「ログイン成功 **URL**」: 認証が成功した場合にユーザーがリダイレクトされる URL を定義します。

「ログイン失敗 **URL**」: 認証が失敗した場合にユーザーがリダイレクトされる URL を定義します。

「認証ポストプロセスクラス」: 認証後インタフェースを定義します。

サービスに基づく認証のログイン URL

サービスに基づく認証は、ユーザーインタフェースのログイン URL にサービスパラメータを定義して指定できます。サービスを呼び出したあと、ユーザーが認証を受ける認証モジュールは、そのサービスに定義された認証設定サービスインスタンスから取得されます。

このサービスに基づく認証を指定し開始するログイン URL を次に示します。

```
http://server_name.domain_name:port/amserver/UI/
Login?service=auth-chain-name
```

および

```
http://server_name.domain_name:port/amserver/UI/Login?realm=realm_name&service=auth-chain-name
```

e

org パラメータが設定されていない場合、レルムはログイン URL そのものに指定されたサーバーホストとドメインから判断されます。

サービスに基づく認証のリダイレクト URL

サービスに基づく認証が成功または失敗した時に、Access Manager はユーザーのリダイレクト先の情報を検索します。この情報をアプリケーションが検索する優先順位を次に示します。

サービスに基づく認証が成功した場合のリダイレクト URL

サービスに基づく認証が成功した場合のリダイレクト URL は、次の場所を次の順序で確認することによって判断されます。

1. 認証モジュールで設定された URL。
2. goto ログイン URL パラメータで設定された URL。
3. ユーザーのプロファイル (amUser.xml) の iplanet-am-user-success-url 属性用に clientType カスタムファイルに設定された URL。
4. ユーザーが認証を受けたサービスの iplanet-am-auth-login-success-url 属性用に clientType カスタムファイルに設定された URL。
5. ユーザーのロールエントリの iplanet-am-auth-login-success-url 属性用に clientType カスタムファイルに設定された URL。
6. ユーザーのレルムエントリの iplanet-am-auth-login-success-url 属性用に clientType カスタムファイルに設定された URL。

7. グローバルデフォルトとして iplanet-am-auth-login-success-url 属性用に clientType カスタムファイルに設定された URL。
8. ユーザーのプロファイル (amUser.xml) の iplanet-am-user-success-url 属性に設定された URL。
9. ユーザーが認証を受けたサービスの iplanet-am-auth-login-success-url 属性に設定された URL。
10. ユーザーのロールエントリの iplanet-am-auth-login-success-url 属性に設定された URL。
11. ユーザーのレルムエントリの iplanet-am-auth-login-success-url 属性に設定された URL。
12. グローバルデフォルトとして iplanet-am-auth-login-success-url 属性に設定された URL。

サービスに基づく認証が失敗した場合のリダイレクト URL

サービスに基づく認証が失敗した場合のリダイレクト URL は、次の場所を次の順序で確認することによって判断されます。

1. 認証モジュールで設定された URL。
2. goto ログイン URL パラメータで設定された URL。
3. ユーザーのプロファイル (amUser.xml) の iplanet-am-user-failure-url 属性用に clientType カスタムファイルに設定された URL。
4. ユーザーが認証を受けたサービスの iplanet-am-auth-login-failure-url 属性用に clientType カスタムファイルに設定された URL。
5. ユーザーのロールエントリの iplanet-am-auth-login-failure-url 属性用に clientType カスタムファイルに設定された URL。
6. ユーザーのレルムエントリの iplanet-am-auth-login-failure-url 属性用に clientType カスタムファイルに設定された URL。
7. グローバルデフォルトとして iplanet-am-auth-login-failure-url 属性用に clientType カスタムファイルに設定された URL。
8. ユーザーのプロファイル (amUser.xml) の iplanet-am-user-failure-url 属性に設定された URL。
9. ユーザーが認証を受けたサービスの iplanet-am-auth-login-failure-url 属性に設定された URL。
10. ユーザーのロールエントリの iplanet-am-auth-login-failure-url 属性に設定された URL。
11. ユーザーのレルムエントリの iplanet-am-auth-login-failure-url 属性に設定された URL。
12. グローバルデフォルトとして iplanet-am-auth-login-failure-url 属性に設定された URL。

▼ サービスに基づく認証を設定する

認証モジュールは、認証設定サービスを追加すると、サービス用に設定されます。そのためには、次の手順を実行します。

1. サービスに基づく認証を設定するレルムを選択します。
2. 「認証」タブをクリックします。
3. 認証モジュールインスタンスを作成します。
4. 認証連鎖を作成します。
5. 「保存」をクリックします。
6. レルムのサービスに基づく認証にアクセスするには、次のアドレスを入力します。

   `http://`*`server_name.domain_name:port`*`/amserver/UI/Login?realm=`*`realm_name&service=auth-chain-name`*

ユーザーに基づく認証

この認証方法では、ユーザーはユーザー専用に設定された認証プロセスに対する認証を受けることができます。このプロセスは、ユーザーのプロファイルの「ユーザー認証設定」属性の値として設定されます。認証を成功させるには、ユーザーは定義された各モジュールに対して認証する必要があります。

ユーザーに基づく認証のログイン URL

ユーザーに基づく認証は、ユーザーインタフェースのログイン URL にユーザーパラメータを定義して指定できます。正しいユーザーを呼び出したあと、ユーザーが認証を受ける認証モジュールは、そのユーザーに定義されたユーザー認証インスタンスから取得されます。

このロールに基づく認証を指定し開始するログイン URL を次に示します。

```
http://server_name.domain_name:port/amserver/UI/Login?user=user_name
http://server_name.domain_name:port/amserver/UI/Login?org=org_name&user=user_name
```

realm パラメータが設定されていない場合、ロールが属すレルムはログイン URL そのものに指定されたサーバーホストおよびドメインから判断されます。

ユーザーエイリアスリスト属性

ユーザーに基づく認証の要求を受け取ると、認証サービスはまずユーザーが有効なユーザーであることを確認してから、ユーザーの認証設定データを取得します。ユーザーログイン URL パラメータの値に複数の有効なユーザープロファイルが関連付けられている場合は、すべてのプロファイルを指定されたユーザーにマップする必要があります。ユーザープロファイルのユーザーエイリアス属性 (`iplanet-am-user-alias-list`) には、ユーザーに属すその他のプロファイルを定義できます。マッピングが失敗すると、ユーザーは有効なセッションを拒否されます。ユーザーの 1 人がユーザーのマッピングの検証が行われない最上位の管理者であり、そのユーザーに最上位の管理者権限が与えられている場合は、例外です。

ユーザーに基づく認証のリダイレクト URL

ユーザーに基づく認証が成功または失敗した時に、Access Manager はユーザーのリダイレクト先の情報を検索します。この情報をアプリケーションが検索する優先順位を次に示します。

ユーザーに基づく認証が成功した場合のリダイレクト URL

ユーザーに基づく認証が成功した場合のリダイレクト URL は、次の場所を次の優先順位で確認することによって判断されます。

1. 認証モジュールで設定された URL。
2. `goto` ログイン URL パラメータで設定された URL。
3. ユーザーのプロファイル (`amUser.xml`) の `iplanet-am-user-success-url` 属性用に `clientType` カスタムファイルに設定された URL。
4. ユーザーのロールエントリの `iplanet-am-auth-login-success-url` 属性用に `clientType` カスタムファイルに設定された URL。
5. ユーザーのレルムエントリの `iplanet-am-auth-login-success-url` 属性用に `clientType` カスタムファイルに設定された URL。
6. グローバルデフォルトとして `iplanet-am-auth-login-success-url` 属性用に `clientType` カスタムファイルに設定された URL。
7. ユーザーのプロファイル (`amUser.xml`) の `iplanet-am-user-success-url` 属性に設定された URL。
8. ユーザーのロールエントリの `iplanet-am-auth-login-success-url` 属性に設定された URL。
9. ユーザーのレルムエントリの `iplanet-am-auth-login-success-url` 属性に設定された URL。
10. グローバルデフォルトとして `iplanet-am-auth-login-success-url` 属性に設定された URL。

ユーザーに基づく認証に失敗した場合のリダイレクト URL

ユーザーに基づく認証が失敗した場合のリダイレクト URL は、次の場所を次の順序で確認することによって判断されます。

1. 認証モジュールで設定された URL。
2. `gotoOnFail` ログイン URL パラメータで設定された URL。
3. ユーザーのエントリ (`amUser.xml`) の `iplanet-am-user-failure-url` 属性用に `clientType` カスタムファイルに設定された URL。
4. ユーザーのロールエントリの `iplanet-am-auth-login-failure-url` 属性用に `clientType` カスタムファイルに設定された URL。
5. ユーザーのレルムエントリの `iplanet-am-auth-login-failure-url` 属性用に `clientType` カスタムファイルに設定された URL。
6. グローバルデフォルトとして `iplanet-am-auth-login-failure-url` 属性用に `clientType` カスタムファイルに設定された URL。
7. ユーザーのエントリ (`amUser.xml`) の `iplanet-am-user-failure-url` 属性用に設定された URL。
8. ユーザーのロールエントリの `iplanet-am-auth-login-failure-url` 属性に設定された URL。
9. ユーザーのレルムエントリの `iplanet-am-auth-login-failure-url` 属性に設定された URL。
10. グローバルデフォルトとして `iplanet-am-auth-login-failure-url` 属性に設定された URL。

▼ ユーザーに基づく認証を設定する

1 ユーザーの認証を設定するレルムに移動します。

2 「対象」タブをクリックし、「ユーザー」をクリックします。

3 変更するユーザーの名前をクリックします。
ユーザープロファイルが表示されます。

注 – 新しいユーザーを作成している場合、そのユーザーに認証設定サービスは自動的に割り当てられません。ユーザーを作成する前に、サービスプロファイルで認証設定サービスを選択していることを確認してください。このオプションを選択しないと、ユーザーはロールに定義された認証設定を継承しません。

---

4 「ユーザー認証設定」属性で、適用する認証連鎖を選択します。

5 「保存」をクリックします。

認証レベルに基づく認証

それぞれの認証モジュールは、その認証レベルに整数値が関連付けられています。認証レベルを割り当てるには、「サービス設定」で認証モジュールの「プロパティー」矢印をクリックし、モジュールの「認証レベル」属性で対応する値を変更します。認証レベルが高いということは、1 つ以上の認証モジュールで認証を受けたそのユーザーの信頼性のレベルが高いということです。

ユーザーがそのモジュールに対する認証に成功すると、認証レベルがユーザーの SSO トークンに設定されます。複数の認証モジュールに対して認証を受ける必要があり、認証に成功した場合は、最高の認証レベルの値がユーザーの SSO トークンに設定されます。

ユーザーがサービスへのアクセスを試みる場合、サービスでは、そのユーザーの SSO トークンの認証レベルを確認することで、そのユーザーがアクセスを許可されているかどうかを判別できます。次に、設定された認証レベルで認証モジュールにパスするように、ユーザーをリダイレクトします。

ユーザーは特定の認証レベルで認証モジュールにアクセスすることもできます。たとえばユーザーが次の構文でログインします。

`http://`*`hostname:port/deploy_URI`*`/UI/Login?authlevel=`
`auth_level_value`

認証レベルが *auth_level_value* 以上であるすべてのモジュールが、ユーザーが選択するための認証メニューとして表示されます。一致するモジュールが 1 つしかなかった場合は、その認証モジュールのログインページが直接表示されます。

この認証の方法では、ID が認証を受けられるモジュールのセキュリティーレベルを、管理者が指定できます。各認証モジュールには、それぞれの「認証レベル」属性があり、この属性の値は任意の有効な整数として定義できます。認証レベルに基づく認証では、認証サービスは、ログイン URL パラメータに指定された値以上の認証レベルを持つ認証モジュールを含むメニューを持つモジュールログインページを表示します。ユーザーは、提示されたリストからモジュールを選択します。ユーザーがモジュールを選択すると、以降のプロセスはモジュールに基づく認証に基づきます。

認証レベルに基づく認証のログイン URL

認証レベルに基づく認証は、ユーザーインタフェースのログイン URL に authlevel パラメータを定義して指定できます。関連するモジュールのリストを示すログイン画面を呼び出したあと、ユーザーは認証を受けるモジュールを選択する必要があります。認証レベルに基づく認証を指定し開始するログイン URL を次に示します。

```
http://server_name.domain_name:port/amserver/UI/Login?authlevel=authentication_level
```

および

```
http://server_name.domain_name:port/amserver/UI/
Login?realm=realm_name&authlevel=authentication_level
```

realm パラメータが設定されていない場合、ユーザーが属すレルムはログイン URL そのものに指定されたサーバーホストおよびドメインから判断されます。

認証レベルに基づく認証のリダイレクト URL

認証レベルに基づく認証が成功または失敗した時に、Access Manager はユーザーのリダイレクト先の情報を検索します。この情報をアプリケーションが検索する優先順位を次に示します。

認証レベルに基づく認証が成功した場合のリダイレクト URL

認証レベルに基づく認証が成功した場合のリダイレクト URL は、次の場所を次の優先順位で確認することによって判断されます。

1. 認証モジュールで設定された URL。
2. goto ログイン URL パラメータで設定された URL。
3. ユーザーのプロファイル (amUser.xml) の iplanet-am-user-success-url 属性用に clientType カスタムファイルに設定された URL。
4. ユーザーのロールエントリの iplanet-am-auth-login-success-url 属性用に clientType カスタムファイルに設定された URL。
5. ユーザーのレルムエントリの iplanet-am-auth-login-success-url 属性用に clientType カスタムファイルに設定された URL。
6. グローバルデフォルトとして iplanet-am-auth-login-success-url 属性用に clientType カスタムファイルに設定された URL。
7. ユーザーのプロファイル (amUser.xml) の iplanet-am-user-success-url 属性に設定された URL。
8. ユーザーのロールエントリの iplanet-am-auth-login-success-url 属性に設定された URL。
9. ユーザーのレルムエントリの iplanet-am-auth-login-success-url 属性に設定された URL。
10. グローバルデフォルトとして iplanet-am-auth-login-success-url 属性に設定された URL。

認証レベルに基づく認証が失敗した場合のリダイレクト URL

認証レベルに基づく認証が失敗した場合のリダイレクト URL は、次の場所を次の順序で確認することによって判断されます。

1. 認証モジュールで設定された URL。
2. `gotoOnFail` ログイン URL パラメータで設定された URL。
3. ユーザーのエントリ (`amUser.xml`) の `iplanet-am-user-failure-url` 属性用に `clientType` カスタムファイルに設定された URL。
4. ユーザーのロールエントリの `iplanet-am-auth-login-failure-url` 属性用に `clientType` カスタムファイルに設定された URL。
5. ユーザーのレルムエントリの `iplanet-am-auth-login-failure-url` 属性用に `clientType` カスタムファイルに設定された URL。
6. グローバルデフォルトとして `iplanet-am-auth-login-failure-url` 属性用に `clientType` カスタムファイルに設定された URL。
7. ユーザーのエントリ (`amUser.xml`) の `iplanet-am-user-failure-url` 属性に設定された URL。
8. ユーザーのロールエントリの `iplanet-am-auth-login-failure-url` 属性に設定された URL。
9. ユーザーのレルムエントリの `iplanet-am-auth-login-failure-url` 属性に設定された URL。
10. グローバルデフォルトとして `iplanet-am-auth-login-failure-url` 属性に設定された URL。

モジュールに基づく認証

ユーザーは次の構文を使用して、特定の認証モジュールにアクセスできます。

`http://`*`hostname:port/deploy_URI`*`/UI/Login?module=`
`module_name`

認証モジュールにアクセスする前に、その認証モジュール名を含むように、コア認証サービス属性のレルム認証モジュールを修正する必要があります。認証モジュール名がこの属性に含まれていない場合、ユーザーが認証を試みると「認証モジュールが拒否されました」ページが表示されます。

この認証の方法では、ユーザーは認証を受けるモジュールを指定できます。指定するモジュールは、ユーザーがアクセスするレルムまたはサブレルムに登録する必要があります。これは、レルムのコア認証サービスの「レルム認証モジュール」属性に設定されます。モジュールに基づく認証の要求を受け取ると、認証サービスは、モジュールが指定されたように正しく設定されていることを確認し、モジュールが定義されていない場合は、ユーザーはアクセスを拒否されます。

モジュールに基づく認証のログイン URL

モジュールパラメータを定義して、ユーザーインタフェースのログイン URL にモジュールに基づく認証を指定できます。モジュールに基づく認証を指定し開始するログイン URL を次に示します。

```
http://server_name.domain_name:port/amserver/UI/Login?module=authentication_module_name
http://server_name.domain_name:port/amserver/UI/
Login?org=org_name&module=authentication_module_name
```

org パラメータが設定されていない場合、ユーザーが属すレルムはログイン URL そのものに指定されたサーバーホストおよびドメインから判断されます。

モジュールに基づく認証のリダイレクト URL

モジュールに基づく認証が成功または失敗した時に、Access Manager はユーザーのリダイレクト先の情報を検索します。この情報をアプリケーションが検索する優先順位を次に示します。

モジュールに基づく認証が成功した場合のリダイレクト URL

モジュールに基づく認証が成功した場合のリダイレクト URL は、次の場所を次の優先順位で確認することによって判断されます。

1. 認証モジュールで設定された URL。
2. goto ログイン URL パラメータで設定された URL。
3. ユーザーのプロファイル (amUser.xml) の iplanet-am-user-success-url 属性用に clientType カスタムファイルに設定された URL。
4. ユーザーのロールエントリの iplanet-am-auth-login-success-url 属性用に clientType カスタムファイルに設定された URL。
5. ユーザーのレルムエントリの iplanet-am-auth-login-success-url 属性用に clientType カスタムファイルに設定された URL。
6. グローバルデフォルトとして iplanet-am-auth-login-success-url 属性用に clientType カスタムファイルに設定された URL。
7. ユーザーのプロファイル (amUser.xml) の iplanet-am-user-success-url 属性に設定された URL。
8. ユーザーのロールエントリの iplanet-am-auth-login-success-url 属性に設定された URL。
9. ユーザーのレルムエントリの iplanet-am-auth-login-success-url 属性に設定された URL。
10. グローバルデフォルトとして iplanet-am-auth-login-success-url 属性に設定された URL。

モジュールに基づく認証に失敗した場合のリダイレクト URL

モジュールに基づく認証が失敗した場合のリダイレクト URL は、次の場所を次の順序で確認することによって判断されます。

1. 認証モジュールで設定された URL。
2. `gotoOnFail` ログイン URL パラメータで設定された URL。
3. ユーザーのエントリ (`amUser.xml`) の `iplanet-am-user-failure-url` 属性用に `clientType` カスタムファイルに設定された URL。
4. ユーザーのロールエントリの `iplanet-am-auth-login-failure-url` 属性用に `clientType` カスタムファイルに設定された URL。
5. ユーザーのレルムエントリの `iplanet-am-auth-login-failure-url` 属性用に `clientType` カスタムファイルに設定された URL。
6. グローバルデフォルトとして `iplanet-am-auth-login-failure-url` 属性用に `clientType` カスタムファイルに設定された URL。
7. ユーザーのロールエントリの `iplanet-am-auth-login-failure-url` 属性に設定された URL。
8. ユーザーのレルムエントリの `iplanet-am-auth-login-failure-url` 属性に設定された URL。
9. グローバルデフォルトとして `iplanet-am-auth-login-failure-url` 属性に設定された URL。

ユーザーインタフェースのログイン URL

認証サービスユーザーインタフェースには、Web ブラウザの場所ツールバーにログイン URL を入力してアクセスします。この URL は次のとおりです。

`http://`*AccessManager-root*`/.`*domain_name*`:`*port*` /`*service_deploy_uri*` /UI/Login`

注 – インストールの間に、*service_deploy_uri* は `amserver` として設定されます。このマニュアル全体にわたり、このデフォルトのサービス配備 URI が使用されています。

特定の認証方法や、成功、失敗した認証のリダイレクト URL を定義するために、ユーザーインタフェースのログイン URL にログイン URL パラメータを付加することもできます。

ログイン URL パラメータ

URL パラメータは、URL の終わりに付加される名前と値のペアです。このパラメータは疑問符 (?) で始まり、名前=値の形式をとります。たとえば、次のようにいくつかのパラメータを 1 つのログイン URL に結合できます。

```
http://server_name.domain_name:port/amserver/UI/
Login?module=LDAP&locale=ja&goto=http://www.sun.com
```

複数のパラメータを指定する場合は、アンパサンド (&) で区切ります。複数のパラメータを指定する場合は、次のガイドラインに従う必要があります。

- 各パラメータは、1 つの URL に 1 回のみ指定できます。たとえば、`module=LDAP&module=NT` は受け入れられません。
- `org` パラメータと `domain` パラメータは両方ともログインレルムを決定します。この場合、ログイン URL にはこの 2 つのパラメータどちらかを使用する必要があります。両方を使用する場合に優先順位を指定しないと、1 つのみが有効になります。
- `user`、`role`、`service`、`module`、および `authlevel` は、それぞれの基準に基づいて認証モジュールを定義するためのパラメータです。このため、ログイン URL にはこれらのパラメータのいずれか 1 つのみを使用する必要があります。複数のパラメータを使用する場合に優先順位を指定しないと、1 つのみが有効になります。

次の節では、ユーザーインタフェースのログイン URL に付加され、Web ブラウザの場所ツールバーに入力されたときに、さまざまな認証機能を実現するパラメータについて説明します。

注 – レルム全体に配布する認証 URL およびパラメータを単純なものにするには、管理者は単純な URL を持つ HTML ページを作成し、そのページにすべての設定された認証方法に対するより複雑なログイン URL へのリンクを含めることができます。

---

goto パラメータ

`goto=`*successful_authentication_URL* パラメータは、認証設定サービスの「ログイン成功 URL」に定義された値を置き換えます。このパラメータは、認証が成功すると指定された URL にリンクします。`goto= logout_URL` パラメータも、ユーザーのログアウト時に指定された URL にリンクするのに使用できます。次に認証成功 URL の例を示します。

```
http://server_name.domain_name:port/amserver/
UI/Login?goto=http://www.sun.com/homepage.html
```

次に `goto` ログアウト URL の例を示します。

```
http://server_name.domain_name:port/amserver/
UI/Logout?goto=http://www.sun.com/logout.html.
```

注 – Access Manager が認証成功リダイレクト URL を確認する優先順位が定められています。リダイレクト URL とそれらの順番は認証方法に基づいているので、この順番および関連情報については、「認証タイプ」の節で詳しく説明します。

gotoOnFail パラメータ

gotoOnFail=failed_authentication_URL パラメータは、認証設定サービスの「ログイン失敗 URL」に定義された値を置き換えます。ユーザーが認証に失敗すると、指定された URL にリンクします。次に gotoOnFail URL の例を示します。http://*server_name.domain_name*:*port* /amserver/UI/Login?gotoOnFail=http://www.sun.com/auth_fail.html

注 – Access Manager が認証失敗リダイレクト URL を確認する優先順位が定められています。リダイレクト URL とそれらの順番は認証方法に基づいているので、この順番および関連情報については、「認証タイプ」の節で詳しく説明します。

realm パラメータ

org=*realmName* パラメータを使用すると、指定されたレルムのユーザーとしてユーザーを認証することができます。

注 – 指定されたレルムのメンバーになっていないユーザーが、realm パラメータで認証を試みると、エラーメッセージを受け取ります。ただし、次の条件をすべて満たせば、Directory Server に動的にユーザープロファイルを作成できます。

- コア認証サービスの「ユーザープロファイル」属性に、「動的」または「ユーザーエイリアスを使用して動的に」が設定されている。
- ユーザーが、必要なモジュールに対する認証に成功している。
- ユーザーのプロファイルは、まだ Directory Server にない。

このパラメータから、レルムおよびそのロケールの設定に基づいて、正しいログインページが表示されます。このパラメータが設定されない場合は、デフォルトは最上位のレルムになります。たとえば、org URL は次のようになります。

```
http://server_name.domain_name:port/amserver/UI/Login?realm=sun
```

org パラメータ

org=*orgName* パラメータを使用すると、指定された組織のユーザーとしてユーザーを認証することができます。

注 – 指定された組織のメンバーになっていないユーザーが、org パラメータで認証を試みると、エラーメッセージを受け取ります。ただし、次の条件をすべて満たせば、Directory Server に動的にユーザープロファイルを作成できます。

- コア認証サービスの「ユーザープロファイル」属性に、「動的」または「ユーザーエイリアスを使用して動的に」が設定されている。
- ユーザーが、必要なモジュールに対する認証に成功している。
- ユーザーのプロファイルは、まだ Directory Server にない。

このパラメータから、組織およびそのロケールの設定に基づいて、正しいログインページが表示されます。このパラメータが設定されない場合は、デフォルトは最上位の組織になります。たとえば、org URL は次のようになります。

```
http://server_name.domain_name:port/amserver/UI/Login?org=sun
```

user パラメータ

user=*userName* パラメータは、ユーザーのプロファイルの「ユーザー認証設定」属性に設定されたモジュールに基づいて、認証を強制します。たとえば、あるユーザーのプロファイルを証明書モジュールを使用して認証するよう設定できる一方で、別のユーザーを LDAP モジュールを使用して認証するように設定できます。このパラメータを追加すると、ユーザーはユーザーの組織に設定された認証方法ではなく、ユーザー用に設定された認証プロセスに送られます。次に例を示します。

```
http://server_name.domain_name:port/amserver/UI/Login?user=jsmith
```

role パラメータ

role=roleName パラメータは、ユーザーを指定されたロール用に設定された認証プロセスに送ります。指定されたロールのメンバーになっていないユーザーが、このパラメータで認証を試みると、エラーメッセージを受け取ります。次に例を示します。

```
http://server_name.domain_name:port/amserver/UI/Login?role=manager
```

locale パラメータ

Access Manager は、認証プロセスとコンソール自身について、ローカライズされた (英語以外の言語に翻訳された) 画面を表示することができます。locale=*localeName* パラメータは、指定されたロケールをその他の定義されたロケールよりも優先させることができます。ログインのロケールは、次の順序で次の場所から設定を検索したあとに、クライアントに表示されます。

1. ログイン URL のロケールパラメータの値

`locale=`*localeName* パラメータの値は、定義されたその他のすべてのロケールよりも優先されます。

2. ユーザーのプロファイルに定義されたロケール

   URL パラメータがない場合は、ロケールはユーザープロファイルの「ユーザー設定言語」属性に設定された値に基づいて表示されます。

3. HTTP ヘッダーに定義されたロケール

   このロケールは、Web ブラウザによって設定されます。

4. コア認証サービスに定義されたロケール

   これは、コア認証モジュールの「デフォルト認証ロケール」属性の値です。

5. プラットフォームサービスに定義されたロケール

   これは、プラットフォームサービスの「プラットフォームロケール」属性の値です。

オペレーティングシステムのロケール

この優先順位から導き出されるロケールは、ユーザーのセッショントークンに格納され、Access Manager が、ローカライズされた認証モジュールのロードだけに使用します。認証に成功すると、ユーザーのプロファイルの「ユーザー設定言語」属性に定義されたロケールが使用されます。ロケールが設定されていない場合は、認証に使用されたロケールが引き続き使用されます。次に例を示します。

```
http://server_name.domain_name:port/amserver/UI/Login?locale=ja
```

注 – 画面のテキストおよびエラーメッセージのローカライズの方法については、Access Manager を参照してください。

---

module パラメータ

`module=`*moduleName* パラメータを使用すると、指定した認証モジュールによって認証を行うことができます。どのモジュールでも指定できますが、まずユーザーが所属するレルムに登録し、コア認証モジュールでそのレルムの認証モジュールの 1 つとして選択する必要があります。次に例を示します。

```
http://server_name.domain_name:port/amserver/UI/Login?module=Unix
```

注 – 認証モジュール名は、URL パラメータで使用する場合には大文字と小文字が区別されます。

---

service パラメータ

service=*serviceName* パラメータを使用すると、サービスの設定された認証スキームによってユーザーを認証できます。認証設定サービスを使用して、異なるサービスに異なる認証スキームを設定できます。たとえば、オンラインの給料支払いアプリケーションにはより安全な証明書認証モジュールを使用した認証が必要になり、レルムの社員のディレクトリアプリケーションには LDAP 認証モジュールのみが必要になるなどです。認証スキームを、それらの各サービスに設定および指定できます。次に例を示します。

```
http://server_name.domain_name:port/amserver/UI/Login?service=sv1
```

注 – 認証設定サービスを使用して、サービスに基づく認証のスキームを定義します。

arg パラメータ

arg=*newsession* パラメータを使用して、ユーザーの現在のセッションを終了し、新しいセッションを開始します。認証サービスは、1 回の要求でユーザーの既存のセッショントークンを破棄し、新しいログインを実行します。このオプションは通常、匿名の認証モジュールで使用されます。ユーザーは、まず匿名セッションで認証を受けてから、登録リンクまたはログインリンクをヒットします。次に例を示します。

```
http://server_name.domain_name:port/amserver/UI/Login?arg=newsession
```

authlevel パラメータ

authlevel=*value* パラメータは、指定された認証レベル値以上の認証レベルのモジュールを呼び出すように認証サービスに指示します。各認証モジュールは、固定整数の認証レベルで定義されます。次に例を示します。

```
http://server_name.domain_name:port/amserver/UI/Login?authlevel=1
```

注 – 認証レベルは、各モジュールの特定のプロファイルに設定されます。

domain パラメータ

このパラメータを使用すると、指定されたドメインとして識別されるレルムにユーザーがログインできます。指定するドメインは、レルムのプロファイルの「ドメイン名」属性に定義された値に一致する必要があります。次に例を示します。

```
http://server_name.domain_name:port/amserver/UI/Login?domain=sun.com
```

注 – 指定されたドメイン、つまりレルムのメンバーになっていないユーザーが、org パラメータで認証を試みると、エラーメッセージを受け取ります。ただし、次の条件をすべて満たせば、Directory Server に動的にユーザープロファイルを作成できます。

- コア認証サービスの「ユーザープロファイル」属性に、「動的」または「ユーザーエイリアスを使用して動的に」が設定されている。
- ユーザーが、必要なモジュールに対する認証に成功している。
- ユーザーのプロファイルは、まだ Directory Server にない。

iPSPCookie パラメータ

iPSPCookie=yes パラメータを使用すると、ユーザーは持続 Cookie でログインできます。持続 Cookie とは、ブラウザウィンドウが閉じられたあとも存在し続ける Cookie のことです。このパラメータを使用するには、ユーザーがログインするレルムのコア認証モジュールで「持続 Cookie」が有効になっている必要があります。ユーザーが認証されブラウザを閉じると、ユーザーは新しいブラウザセッションでログインすることが可能であり、再認証する必要なくコンソールにダイレクトされます。これは、コアサービスに指定された「Cookie の最大持続時間」属性の値まで有効です。次に例を示します。

```
http://server_name.domain_name:port/amserver/UI/Login?org=example&iPSPCookie=yes
```

IDTokenN パラメータ

このパラメータオプションを使用すると、ユーザーは URL または HTML 形式で認証資格を渡すことができます。IDTokenN=*value* パラメータを使用すると、ユーザーは認証サービスユーザーインタフェースにアクセスせずに認証を受けることができます。この処理は、ゼロページログインと呼ばれます。ゼロページログインは、1 つのログインページを使用する認証モジュールの場合にのみ機能します。IDToken0、IDToken1、...、IDTokenN の値は、認証モジュールのログインページのフィールドにマッピングされます。たとえば、LDAP 認証モジュールが、userID 情報に IDToken1 を、パスワード情報に IDToken2 を使用するとします。この場合、LDAP モジュールの IDTokenN URL は次のようになります。

```
http://server_name.domain_name:port/amserver/UI/
Login?module=LDAP&IDToken1=userID&IDToken2=password
```

LDAP がデフォルトの認証モジュールである場合は、module=LDAP を省略できます。

匿名認証の場合は、ログイン URL パラメータは次のようになります。

```
http://server_name.domain_name:port/amserver/UI/Login?module=Anonymous&IDToken1=anonymousUserID
```

注 – 以前のリリースのトークン名 Login.Token0、Login.Token1、...、Login.TokenN は、現在はサポートされていますが今後のリリースではサポートされません。新しい IDTokenN パラメータを使用することをお勧めします。

アカウントのロック

認証サービスには、*n* 回失敗すると、ユーザーが認証からロックアウトされる機能があります。この機能はデフォルトではオフになっていますが、Access Manager コンソールを使用して有効にできます。

注 – 無効なパスワード例外をスローするモジュールのみが、アカウントロック機能を利用できます。

コア認証サービスには、この機能を有効化およびカスタマイズするための次の属性 (ただし、これらに限定されない) が含まれています。

- 「ログイン失敗時のロックアウトモード」は、アカウントロックを有効にします。
- 「ログイン失敗時のロックアウト回数」は、ユーザーがロックアウトされるまでに認証を試みることができる回数を定義します。この回数は、ユーザー ID ごとにのみ有効であり、同一ユーザー ID が指定された回数だけ認証に失敗するとロックアウトされます。
- 「ログイン失敗時のロックアウト間隔」は、分単位で定義された時間内にユーザーのログイン失敗の回数が「ログイン失敗時のロックアウト回数」で定義された値に達した場合に、そのユーザーをロックアウトすることを意味します。
- 「ロックアウト通知の送信先電子メールアドレス」は、ユーザーロックアウト通知が送信される電子メールアドレスを指定します。
- 「ユーザーに警告を出すまでの失敗回数」は、認証の失敗回数がここで定義した値に達したら、警告メッセージをユーザーに表示することを意味します。これにより、ロックアウトの発生が迫っていることを知らせる警告をユーザーが受けたあとに、さらに実行できるログインの試行回数を、管理者が設定できます。
- 「ログイン失敗時のロックアウト持続時間」は、ロックアウト後、次に認証を再試行できるようになるまで、ユーザーが待たなければならない時間を分単位で定義します。
- 「ロックアウト属性名」は、物理ロックのためにユーザーのプロファイルのどの LDAP 属性を「非アクティブ」に設定するかを定義します。
- 「ロックアウト属性値」は、「ロックアウト属性名」に指定された LDAP 属性を「非アクティブ」または「アクティブ」のどちらに設定するかを定義します。

アカウントのロックアウトに関する電子メールの通知が、管理者に送信されます。アカウントロックのアクティビティーはログにも記録されます。

注 – Microsoft® Windows 2000 オペレーティングシステムでこの機能を使用する場合の特別な指示については、付録 A、「AMConfig.properties ファイル」の「Simple Mail Transfer Protocol (SMTP)」を参照してください。

Access Manager では、物理ロックとメモリーロックの 2 つのタイプのアカウントロックがサポートされます。次の節では、この 2 つについて説明します。

物理ロック

物理ロックは、Access Manager のデフォルトのロック動作です。このロックは、ユーザーのプロファイルの LDAP 属性の状態を非アクティブに変更することによって開始されます。「ロックアウト属性名」属性は、ロックの目的で使用する LDAP 属性を定義します。

注 – エイリアス化されたユーザーとは、LDAP プロファイルで「ユーザーエイリアスリスト」属性 (amUser.xml の `iplanet-am-user-alias-list`) を設定して既存の LDAP ユーザープロファイルにマッピングされるユーザーのことです。エイリアス化されたユーザーは、コア認証サービスの「エイリアス検索属性名」フィールドに `iplanet-am-user-alias-list` を追加することによって確認できます。つまり、エイリアス化されたユーザーがロックアウトされると、ユーザーがエイリアス化された実際の LDAP プロファイルがロックされます。これは、LDAP およびメンバーシップ以外の認証モジュールの物理ロックアウトにのみ関係します。

メモリーロック

メモリーロックは、「ログイン失敗時のロックアウト持続時間」属性の値を 0 よりも大きな値に変更すると有効になります。有効にすると、ユーザーのアカウントは指定された時間メモリー上でロックされます。指定された期間が過ぎると、このアカウントはロック解除されます。メモリーロック機能を使用する場合の考慮事項を次に示します。

- Access Manager が再起動されると、メモリー上でロックされたすべてのアカウントはロック解除されます。
- ユーザーのアカウントがメモリー上でロックされ、管理者がロックアウト持続時間を 0 に設定してアカウントロックメカニズムを物理ロックに変更すると、ユーザーのアカウントはメモリーでロック解除され、ロックカウントがリセットされます。

- メモリーのロックアウト後、LDAP およびメンバーシップ以外の認証モジュールを使用するときに、ユーザーが正しいパスワードでログインを試みると、「このレルムにユーザーのプロファイルがありません。」というエラーが返され、「ユーザーがアクティブではありません。」というエラーは返されません。

注 – ユーザーのプロファイルに「失敗 URL」属性を設定すると、ロックアウト警告メッセージもアカウントがロックされたことを示すメッセージも表示されず、ユーザーは定義された URL にリダイレクトされます。

認証サービスのフェイルオーバー

プライマリサーバーにハードウェアまたはソフトウェア上の問題で障害が発生した場合、または一時的にシャットダウンした場合には、認証サービスのフェイルオーバーにより、認証要求はセカンダリサーバーへ自動的にリダイレクトされます。

認証コンテキストは認証サービスが使用可能な Access Manager のインスタンス上でまず作成されなければなりません。Access Manager のこのインスタンスが使用できない場合は、認証フェイルオーバーメカニズムにより Access Manager の別のインスタンス上に認証コンテキストが作成されます。認証コンテキストは次のような順序でサーバーが使用可能かどうか確認します。

1. 認証サービス URL を AutoContext API に送ります。次に例を示します。

   ```
   AuthContext(orgName, url)
   ```

   この API を使う場合は、URL で参照されたサーバーのみを使用します。この場合、そのサーバー上で認証サービスが使用可能であっても、フェイルオーバーは起きません。
2. 認証コンテキストが `AMConfig.properties` ファイルの `com.iplanet.am.server*` 属性に定義されたサーバーをチェックします。
3. 手順 2 で失敗すると、認証コンテキストはネーミングサービスが利用可能なサーバーからのプラットフォームリストを照会します。ディレクトリサーバーの 1 つのインスタンスを共有する複数のインスタンスが、(主にフェイルオーバーを目的として) Access Manager 上にインストールされたときに、このプラットフォームリストが自動的に作成されます。

   たとえば、プラットフォームリストに `Server1`、`Server2`、および `Server3` の URL が含まれていると、認証コンテキストは `Server1`、`Server2`、および `Server3` のいずれかで認証が成功するまでループします。

   プラットフォームリストは、ネーミングサービスの有無に依存しているので、常に同一のサーバーから得られるわけではありません。さらに、ネーミングサービスのフェイルオーバーが最初に起こります。複数ネーミングサービス URL は `AMConfing.properties` の `com.iplanet.am.naming.url` プロパティーに定義されます。利

用可能な最初のネーミングサービス URL は、認証フェイルオーバーが発生する (プラットフォームサーバーリスト中の) サーバーのリストを持つサーバーを特定するのに使われます。

完全修飾ドメイン名のマッピング

完全修飾ドメイン名 (FQDN) のマッピングは、ユーザーが誤った URL を入力した (保護されたリソースにアクセスするために部分的なホスト名または IP アドレスを指定したなど) 場合に認証サービスが訂正を行うことができるようにします。FQDN のマッピングは、`AMConfig.properties` ファイルで `com.sun.identity.server.fqdnMap` 属性を変更することによって可能になります。このプロパティーは次の形式で指定します。

`com.sun.identity.server.fqdnMap[`*invalid-name* `]=`*valid-name*

invalid-name の値はユーザーが入力する可能性がある無効な FQDN ホスト名であり、*valid-name* はフィルタがユーザーをリダイレクトする実際のホスト名です。定められた要件に準拠するかぎり、コード例 1-1 に示すようにいくつでもマッピングを指定できます。このプロパティーを設定しない場合は、ユーザーは `com.iplanet.am.server.host=`*server_name* プロパティーに設定されたデフォルトのサーバー名に送信されます。このプロパティーも `AMConfig.properties` ファイルにあります。

例 7–1 `AMConfig.properties` の FQDN マッピング属性

```
com.sun.identity.server.fqdnMap[isserver]=isserver.mydomain.com
com.sun.identity.server.fqdnMap[isserver.mydomain]=isserver.mydomain.com
com.sun.identity.server.fqdnMap[
            IP address]=isserver.mydomain.com
```

FQDN のマッピングの使用例

このプロパティーは、サーバーにホストされたアプリケーションが複数のホスト名でアクセス可能な場合に、複数のホスト名のマッピングを作成するために使用できます。このプロパティーを使用して、特定の URL について訂正を行わないように Access Manager を設定することもできます。たとえば、IP アドレスを使用してアプリケーションにアクセスするユーザーにリダイレクトが必要ない場合は、この機能は次のようなマップエントリを指定して実現できます。

`com.sun.identity.server.fqdnMap[`*IP address* `]=`*IP address*

注 – 複数のマッピングを定義する場合は、無効な FQDN 名で値が重複しないようにします。そのようにしないと、アプリケーションにアクセスできなくなる場合があります。

持続 Cookie

持続 Cookie とは、Web ブラウザを閉じたあとも存在する Cookie のことであり、ユーザーが再認証なしに新しいブラウザセッションにログインすることを可能にします。Cookie の名前は、`AMConfig.properties` の `com.iplanet.am.pcookie.name` プロパティーに定義されます。デフォルト値は、`DProPCookie` です。Cookie の値は、3DES で暗号化された文字列であり、この文字列には、ユーザー DN、レルム名、認証モジュール名、最大セッション時間、アイドル時間、およびキャッシュ時間が含まれます。

▼ 持続 Cookie を有効にする

1. コア認証モジュールで「持続 `Cookie` モード」をオンにします。
2. コア認証モジュールで「`Cookie` の最大持続時間」属性の時間値を設定します。
3. ユーザーインタフェースのログイン **URL** に yes の値で **iPSPCookie** パラメータを付加します。

   ユーザーがこの URL を使用して認証を受けると、ブラウザを閉じた場合、新しいブラウザウィンドウを開くことができ、再認証なしにコンソールにリダイレクトされます。手順 2 で定義された時間が経過するまでこのようになります。

   持続 Cookie モードは、次の認証 SPI メソッドを使用してオンにできます。

   ```
   AMLoginModule.setPersistentCookieOn()
   ```

レガシーモードにおけるマルチ LDAP 認証モジュール設定

フェイルオーバーの形式として、あるいは、Access Manager コンソールで値フィールドが 1 つだけ提供されている場合に、属性に複数の値を設定するために、管理者は 1 つのレルムに複数の LDAP 認証モジュール設定を定義できます。これら追加の設定はコンソールに表示されませんが、要求を行っているユーザーの承認が初期検索で見つからない場合に、主設定とともに機能します。たとえば、1 つのレルムで 2 つの異なるドメインでの認証に LDAP サーバーを介した検索を定義したり、あるいは 1 つのドメインに複数のユーザーネーミング属性を設定できます。後者の場合、コンソールにはテキストフィールド

が 1 つのみあり、第 1 の検索基準でユーザーが見つからない場合は、LDAP モジュールは第 2 の検索範囲で検索します。追加の LDAP 構成を設定する手順を次に示します。

▼ 追加の LDAP 構成を設定する

1 **2 番目 (または 3 番目の) LDAP 認証設定に必要な属性および新しい値の完全なセットを含めた XML ファイルを作成します。**

利用可能な属性は、`/etc/opt/SUNWam/config/xml` にある `amAuthLDAP.xml` で参照できます。この手順で作成された XML ファイルは、`amAuthLDAP.xml` とは異なり、`amadmin.dtd` の構造に基づいています。このファイルには、任意のまたはすべての属性を定義できます。コード例 1-2 は、LDAP 認証設定に利用できるすべての属性の値が含まれる副設定ファイルの例です。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!--
  Copyright (c) 2002 Sun Microsystems, Inc. All rights reserved.
  Use is subject to license terms.
-->
<!DOCTYPE Requests
    PUBLIC "-//iPlanet//Sun ONE Access Manager 6.0 Admin CLI DTD//EN"
    "jar://com/iplanet/am/admin/cli/amAdmin.dtd"
>
<!--
  Before adding subConfiguration load the schema with
GlobalConfiguration defined and replace corresponding
 serviceName and subConfigID in this sample file OR load
 serviceConfigurationRequests.xml before loading this sample
-->
<Requests>
<realmRequests DN="dc=iplanet,dc=com">
    <AddSubConfiguration subConfigName = "ssc"
        subConfigId = "serverconfig"
        priority = "0" serviceName="iPlanetAMAuthLDAPService">

              <AttributeValuePair>
            <Attribute name="iplanet-am-auth-ldap-server"/>
            <Value>vbrao.red.iplanet.com:389</Value>
        </AttributeValuePair>
        <AttributeValuePair>
            <Attribute name="iplanet-am-auth-ldap-base-dn"/>
            <Value>dc=iplanet,dc=com</Value>
        </AttributeValuePair>
        <AttributeValuePair>
            <Attribute name="planet-am-auth-ldap-bind-dn"/>
            <Value>cn=amldapuser,ou=DSAME Users,dc=iplanet,dc=com</Value>
```

```
            </AttributeValuePair>
            <AttributeValuePair>
                <Attribute name="iplanet-am-auth-ldap-bind-passwd"/>
                <Value>
                      プレーンテキストのパスワード</Value>
            </AttributeValuePair>
            <AttributeValuePair>
                <Attribute name="iplanet-am-auth-ldap-user-naming-attribute"/>
                <Value>uid</Value>
            </AttributeValuePair>
            <AttributeValuePair>
                <Attribute name="iplanet-am-auth-ldap-user-search-attributes"/>
                <Value>uid</Value>
            </AttributeValuePair>
            <AttributeValuePair>
                <Attribute name="iplanet-am-auth-ldap-search-scope"/>
                <Value>SUBTREE</Value>
            </AttributeValuePair>
            <AttributeValuePair>
                <Attribute name="iplanet-am-auth-ldap-ssl-enabled"/>
                <Value>false</Value>
            </AttributeValuePair>
            <AttributeValuePair>
                <Attribute name="iplanet-am-auth-ldap-return-user-dn"/>
                <Value>true</Value>
            </AttributeValuePair>
            <AttributeValuePair>
                <Attribute name="iplanet-am-auth-ldap-auth-level"/>
                <Value>0</Value>
            </AttributeValuePair>
            <AttributeValuePair>
                <Attribute name="iplanet-am-auth-ldap-server-check"/>
                <Value>15</Value>
            </AttributeValuePair>

        </AddSubConfiguration>

    </realmRequests>
    </Requests>
```

2 手順 **1** で作成した **XML** ファイルで **iplanet-am-auth-ldap-bind-passwd** の値としてプレーンテキストのパスワードをコピーします。

この属性の値は、コード例に太字で示されています。

3 amadmin コマンド行ツールを使用して、**XML** ファイルをロードします。

```
./amadmin -u amadmin -w administrator_password -v -t name_of_XML_file.
```

この 2 番目の LDAP 設定は、コンソールを使用して表示も変更もできません。

ヒント – 複数 LDAP 設定に利用できるサンプルが用意されています。`/AccessManager-base/SUNWam/samples/admin/cli/bulk-ops/` にある `serviceAddMultipleLDAPConfigurationRequests.xml` コマンド行テンプレートを参照してください。手順については、`/AccesManager-base/SUNWam/samples/admin/cli/` にある `Readme.html` を参照してください。

セッションのアップグレード

認証サービスでは、1 つのレルムに対して同一ユーザーが実行した 2 回目の成功した認証に基づいて有効なセッショントークンのアップグレードを行うことができます。有効なセッショントークンを持つユーザーが、現在のレルムによってセキュリティー保護されているリソースに対して認証を試み、この 2 回目の認証が成功すると、セッションは新しい認証に基づく新しいプロパティーで更新されます。認証が失敗すると、ユーザーの現在のセッションがアップグレードなしに戻されます。有効なセッショントークンを持つユーザーが別のレルムによってセキュリティー保護されているリソースに対して認証を試みると、新しいレルムの認証を受けるどうかを尋ねるメッセージを受け取ります。この時点では、ユーザーは、現在のセッションを維持するか、または新しいレルムの認証を受けることができます。認証が成功すると、古いセッションは破棄され、新しいセッションが作成されます。

セッションのアップグレード時に、ログインページの時間切れになると、元の成功 URL へのリダイレクトが発生します。タイムアウト値は、次の条件に基づいて判断されます。

- 各モジュールに設定されたページタイムアウト値 (デフォルトは 1 分)
- `AMConfig.properties` の `com.iplanet.am.invalidMaxSessionTime` プロパティー (デフォルトは 10 分)
- `iplanet-am-max-session-time` (デフォルトは 120 分)

`com.iplanet.am.invalidMaxSessionTimeout` と `iplanet-am-max-session-time` の値は、ページタイムアウト値よりも大きい必要があり、そうでない場合はセッションアップグレード時に有効なセッション情報が失われ、前回の成功 URL へのリダイレクトは失敗します。

検証プラグインインタフェース

管理者は、レルムに適したユーザー名またはパスワード検証ロジックを作成し、そのロジックを認証サービスにプラグインできます。この機能は、LDAP およびメンバーシップの認証モジュールのみでサポートされます。ユーザーを認証したりパスワードを変更する前に、Access Manager はこのプラグインを呼び出します。検証が成功すると、認証が継続され、失敗すると、認証失敗ページがスローされます。プラグインは、サービス管理 SDK の一部である `com.iplanet.am.sdk.AMUserPasswordValidation` クラスを拡張します。SDK についての情報は、Access Manager Javadocs の `com.iplanet.am.sdk` パッケージを参照してください。

▼ 検証プラグインを作成して設定する

1. 新しいプラグインクラスは、`com.iplanet.am.sdk.AMUserPasswordValidation` クラスを拡張し、`validateUserID()` および `validatePassword()` メソッドを実装します。検証が失敗した場合は、`AMException` がスローされます。
2. プラグインクラスをコンパイルし、`.class` ファイルを必要な場所に配置します。実行時に **Access Manager** がプラグインにアクセスできるように、クラスパスを更新します。
3. 最上位の管理者として **Access Manager** コンソールにログインします。「サービス管理」タブをクリックし、管理サービスの属性にアクセスします。「ユーザー `ID` とパスワードの検証プラグインクラス」フィールドにパッケージ名を含むプラグインクラスの名前を入力します。
4. ログアウトし、ログインし直します。

JAAS 共有状態

JAAS 共有状態を有効にすることで、ユーザー ID とパスワードの両方を認証モジュール間で共有できます。各認証モジュールに対して次のオプションを定義します。

- レルム (または、組織)
- ユーザー
- サービス
- ロール

失敗した場合、モジュールは必要な資格を要求します。認証の失敗後、モジュールが停止するか、ログアウト共有状態がクリアされます。

JAAS 共有状態の有効化

JAAS 共有状態を設定するには、次のようにします。

- `iplanet-am-auth-shared-state-enabled` オプションを使用します。
- 共有状態オプションの使用法を次に示します。
  `iplanet-am-auth-shared-state-enabled=true`
- このオプションのデフォルトは、true です。
- この変数は、認証連鎖設定の「オプション」列で指定されます。

失敗すると、認証モジュールは、JAAS の仕様で提案される `tryFirstPass` オプションの動作ごとに必要な資格を要求します。

JAAS 共有状態ストアオプション

「JAAS 共有状態ストア」オプションを設定するには、次のようにします。

- `iplanet-amauth-store-shared-state-enabled` オプションを使用します。
- 「共有状態」オプションの使用法を次に示します。
  `iplanet-am-auth-store-shared-state-enabled=true`
- このオプションのデフォルトは、false です。
- この変数は、認証連鎖設定の「オプション」列で指定されます。

コミット、中断、またはログアウト後に、共有状態はクリアされます。

◆ ◆ ◆ 第 8 章

ポリシーの管理

この章では、Sun Java™ System Access Manager のポリシー管理機能について説明します。Access Manager のポリシー管理機能では、最上位レベル管理者または最上位レベルポリシー管理者が、すべてのレルムで使用できる特定サービスのポリシーの表示、作成、削除、修正を行うことができるようになります。レルムまたはサブレルムの管理者あるいはポリシー管理者が、レルムレベルでポリシーを表示、作成、削除、修正することもできます。

この章は、次の節で構成されています。

概要

ポリシーは、組織の保護されたリソースに対するアクセス権限を指定するルールを定義します。ビジネスには、保護、管理、監視しなければならない、リソース、アプリケーション、およびサービスがあります。ポリシーはこれらのリソースに対するアクセス権と使用を管理し、ユーザーがあるリソースに対して、いつ、どのようにアクションを実行できるかを定義します。ポリシーによって、特定の主体のリソースが定義されます。

注 – 主体には、個人、企業、ロール、グループなど、アイデンティティーを持つことができるすべてのものが該当します。詳細については、『Java™ 2 Platform Standard Edition Javadoc (http://java.sun.com/j2se/1.4.2/docs/api/java/security/Principal.html)』を参照してください。

---

1 個のポリシーでは、二者択一または任意設定の決定を定義できます。二者択一の決定は、「はい」/「いいえ」、「真」/「偽」 または「許可する」/「許可しない」の形式です。任意設定の決定では、属性の値を表します。たとえば、メールサービスは、ユーザーごとの最大保存容量の値セットを持つ `mailboxQuota` 属性を含んでいます。一般的に、ポリシーは主体が、どのような条件でどのリソースに何をできるかを定義するように設定されています。

ポリシー管理機能

ポリシー管理機能には、ポリシーの作成および管理を行うポリシーサービスが備わっています。ポリシーサービスにより、管理者は Access Manager の配備の中でリソースを保護するために、アクセス権を定義、変更、付与、無効化、および削除することができます。通常、ポリシーサービスには、データストアと、ポリシーの作成、管理、評価ができるインタフェースライブラリ、およびポリシーエンフォーサ (ポリシーエージェント) が含まれています。デフォルトでは、Access Manager は Sun Java Enterprise System Directory Server をデータ保存に使い、ポリシーの評価とポリシーサービスのカスタマイズのために Java と C の API を提供します。詳細は、『Sun Java System Access Manager 7 2005Q4 Developer's Guide』を参照してください。また、管理者は Access Manager コンソールを使用してポリシー管理を行うこともできます。Access Manager は、ダウンロード可能なポリシーエージェントを使用してポリシーを適用する、URL ポリシーエージェントサービスを提供します。

URL ポリシーエージェントサービス

Access Manager をインストールするときに、HTTP URL を保護するポリシーを定義するための URL ポリシーエージェントサービスが実装されます。このサービスにより、管理者はポリシーエンフォーサ、つまりポリシーエージェントにより、ポリシーの作成および管理を行えます。

ポリシーエージェント

ポリシーエージェントは企業のリソースが保存されているサーバーへのポリシー適用ポイント (Policy Enforcement Point、PEP) です。ポリシーエージェントは Access Manager とは別に Web サーバー上にインストールされており、ユーザーが保護された Web サーバー上のリソースを要求すると、追加の認証ステップとして働きます。この認証は、リソースが実行するあらゆるユーザー認証要求に追加されます。ポリシーエージェントは Web サーバーを保護し、一方、認証プラグインはリソースを保護します。

たとえば、リモートインストールされた Access Manager で保護されている人事部の Web サーバーにエージェントがインストールされているとします。このエージェントにより、適切なポリシーを持っていない担当者には機密の給与情報またはその他の秘密情報は表示されません。このポリシーは Access Manager の管理者が定義し、Access Manager の配備に保存され、リモート Web サーバーのコンテンツにユーザーがアクセスするのをポリシーエージェントが許可または拒否するのに使われます。

最新の Access Manager ポリシーエージェントは Sun Microsystems Download Center からダウンロードできます。

ポリシーエージェントのインストールおよび管理の詳細については、『Sun Java System Access Manager Policy Agent 2.2 User's Guide』を参照してください。

注 – ポリシーの評価に特定の順序はありませんが、評価の途中であるアクションの値が「許可しない」となったときには、ポリシー設定サービスにより「拒否決定で評価を続行」属性が有効になっていないかぎり、以降のポリシーの評価は中止されます。

Access Manager ポリシーエージェントが決定を適用するのは Web URL (`http://...`、または `https//...`) だけですが、Java と C の Policy Evaluation API を使ってエージェントをプログラミングすれば、ほかのリソースにもポリシーを適用可能です。

この場合、追加作業として、ポリシー設定サービスの「リソースコンパレータ」属性をデフォルトから次のように変更する必要があります。

```
serviceType=Name_of_LDAPService
|class=com.sun.identity.policy.plugins.SuffixResourceName|wildcard=*

|delimiter=,|caseSensitive=false
```

もしくは、`LDAPResourceName` などの実装により、`com.sun.identity.policy.interfaces.ResourceName` を実装して、その上で「リソースコンパレータ」を適切に設定するという方法もあります。

ポリシーエージェントプロセス

Web ブラウザがポリシーエージェントによって保護されたサーバー上の URL を要求すると、保護された Web リソースに対するプロセスが始まります。このサーバーにインストールされたポリシーエージェントはこの要求を傍受し、既存の認証資格をチェックします (セッショントークン)。

エージェントが要求を傍受し、既存のセッショントークンを検証したら、プロセスは以下のように続きます。

1. セッショントークンが有効であれば、ユーザーのアクセスは許可または拒否されます。ユーザーのトークンが無効であれば、以下の手順にあるようにユーザーを認証サービスにリダイレクトします。

   既存のセッショントークンが存在しない要求をエージェントが傍受した場合は、そのリソースが異なる認証方法で保護されているときでも、エージェントはユーザーをログインページにリダイレクトします。
2. ユーザーの資格が適切に認証されると、エージェントは Access Manager の内部サービスの接続に使う URL を定義するネーミングサービスに要求を出します。
3. ポリシーを適用しないリソースリストがエージェントに設定されている場合、リソースがそのリストに一致する場合には、アクセスが許可されます。

4. ネーミングサービスはポリシーサービス、セッションサービス、およびログサービスのロケータを返します。
5. エージェントはユーザーに適用されるポリシー決定を取得するためにポリシーサービスに要求を送信します。
6. アクセスされるリソースに関してのポリシー決定に基づいて、ユーザーのアクセスが許可または拒否されます。ポリシー決定へのアドバイスが異なる認証レベルまたは認証メカニズムを示している場合、エージェントはすべての基準が検証されるまで要求を認証サービスにリダイレクトします。

ポリシータイプ

Access Manager を使用して設定できるポリシーは、次の 2 種類です。

- 140 ページの「標準ポリシー」
- 145 ページの「参照ポリシー」

標準ポリシー

Access Manager では、アクセス権を定義するポリシーを標準ポリシーと呼びます。標準ポリシーは、ルール、対象、条件、および応答プロバイダから構成されます。

ルール

ルールは 1 つのリソース、1 つ以上のアクション、および 1 つの値からなります。各アクションには、1 つ以上の値を設定できます。

- リソースは保護される特定のオブジェクトを指します。たとえば、人事サービスを使ってアクセスする HTML ページまたはユーザーの給与情報です。
- アクションはリソースに対して実行される操作の名前です。Web サーバーアクションの例としては POST または GET があります。たとえば、人事サービスに対して自宅電話番号を変更するアクションを許可できます。
- 値は各アクションの可否を示します。たとえば、allow (許可する) または deny (許可しない) です。

注 – 一部のサービスに対しては、リソースなしでアクションを定義することも可能です。

対象

対象はポリシーが影響を与えるユーザーまたはユーザーの集合 (たとえば、グループ、または特定のロールを持つ複数のユーザー) を定義します。対象はポリシーに割り当てられます。対象の一般則は、ユーザーがポリシー中の少なくとも 1 つの対象のメンバーである場合にのみポリシーが適用される、というものです。デフォルトの対象は次のとおりです。

AM アイデンティティー対象	レルムの「対象」タブで作成して管理しているアイデンティティーを対象の値として追加できます。
Access Manager ロール	この対象には、任意の LDAP ロールを値として追加できます。LDAP ロールは、Directory Server ロール機能を使用するロール定義です。LDAP ロールは、Directory Server ロール定義が規定するオブジェクトクラスを持ちます。ポリシー設定サービスで LDAP ロール検索フィルタを変更して、検索範囲を絞り込みパフォーマンスを向上させることができます。
認証済みユーザー	有効な SSOToken を持つ任意のユーザーがこの対象のメンバーです。すべての認証済みユーザーは、ポリシーが定義されている組織とは別の組織に認証しても、この対象のメンバーになります。リソース所有者が、別の組織のユーザー用に管理されているリソースにアクセスできるようにする場合は、これが便利です。
LDAP グループ	ある LDAP グループの任意のメンバーをこの対象の値として追加できます。
LDAP ロール	この対象には、任意の LDAP ロールを値として追加できます。LDAP ロールは、Directory Server ロール機能を使用するロール定義です。LDAP ロールは、Directory Server ロール定義が規定するオブジェクトクラスを持ちます。ポリシー設定サービスで LDAP ロール検索フィルタを変更して、検索範囲を絞り込みパフォーマンスを向上させることができます。
LDAP ユーザー	この対象には、任意の LDAP ユーザーを値として追加できます。
組織	ある組織の任意のメンバーがこの対象のメンバーです。
Web サービスクライアント	有効な値は、信頼できる WSC の証明書に対応する、ローカル JKS キーストア内の信頼できる証明書の DN です。この対象は、Liberty Web サービスフレームワークに依存し、Liberty サービスプロバイダが WSC を承認するためにのみ使用する必要があります。SSOToken に含まれる主体の DN がこの対象の選択された値のいずれかに一致する場合、SSOToken が特定する Web サービスクライアント (WSC) がこの対象のメンバーです。 この対象をポリシーに追加する前に、キーストアが作成されていることを確認します。キーストアの設定に関する説明は、次の場所にあります。 *AccessManager-base* `/SUNWam/samples/saml/xmlsig/keytool.html`

Access Manager ロールと LDAP ロールの比較

Access Manager ロールは Access Manager を使用して作成します。これらのロールは Access Manager が規定するオブジェクトクラスを持ちます。LDAP ロールは、Directory Server ロール機能を使用するロール定義です。LDAP ロールは、Directory Server ロール定義が規定するオブジェクトクラスを持ちます。すべての Access Manager ロールは Directory Server のロールとして使用できます。しかし、すべての Directory Server ロールが必ずしも Access Manager ロールというわけではありません。LDAP ロールは、159 ページの「ポリシー設定サービス」を設定することにより、既存のディレクトリから利用できます。Access Manager のロールには、ホスティングする Access Manager のポリシーサービス経由でのみアクセスできます。ポリシー設定サービスで LDAP ロール検索フィルタを変更して、検索範囲を絞り込みパフォーマンスを向上させることができます。

入れ子ロール

入れ子ロールはポリシー定義の対象の LDAP ロールとして正しく評価できます。

条件

条件によって、ポリシーに制約を定義できます。たとえば、給与アプリケーション用のポリシーを定義する場合、アプリケーションへのアクセスを特定の時間帯だけに制限するようにアクションに対して条件を定義することができます。また、所定の IP アドレスまたは企業のイントラネットからの要求に対してのみアクションを許可するように条件を定義することもできます。

条件は、同じドメインの別の URI で別のポリシーを設定するために、補助的に使用されることもあります。たとえば、`http://org.example.com/hr/*jsp` は `org.example.net` ドメインより午前9 時～午後5 時の間だけアクセスでき、一方、`http://org.example.com/finance/*.jsp` は `org.example2.net` ドメインより午前5 時～午後11 時の間だけアクセスできる、といった具合にです。これは IP 条件と時間条件を使用して実現します。またルールのリソースを `http://org.example.com/hr/*.jsp` に指定することで、ポリシーは `http://org.example.com/hr` 以下、サブディレクトリ内を含むすべての JSP に適用されるようになります。

注 – 参照、ルール、リソース、対象、条件、属性、値の各用語は、policy.dtd 内の *Referral*、*Rule*、*ResourceName*、*Subject*、*Condition*、*Attribute*、*Value* の各要素に対応しています。

追加できるデフォルトの条件は、次のとおりです。

認証レベル	ユーザーの認証レベルが条件に設定された認証レベル以上である場合にポリシーが適用されます。 この属性は、認証の信頼レベルを示しています。

	認証レベルの条件を使用して、そのレルムに登録された認証モジュールレベル以外のレベルを指定できます。これは、別のレルムから認証を受けたユーザーにポリシーを適用する場合に役立ちます。 「LE 認証レベル」の場合、ユーザーの認証レベルが条件に設定された認証レベル以下である場合にポリシーが適用されます。認証レベルの条件を使用して、そのレルムに登録された認証モジュールレベル以外のレベルを指定できます。これは、別のレルムから認証を受けたユーザーにポリシーを適用する場合に役立ちます。
認証方式	プルダウンメニューから条件の認証方式を選択します。これらの認証方式は、レルムのコア認証サービスで定義されている認証モジュールです。
IP アドレス	IP アドレスの範囲に基づいて条件を設定します。定義できるフィールドは、次のとおりです。 ■ 「IP アドレス 開始 / 終了」: IP アドレスの範囲を指定します。 ■ 「DNS 名」: DNS 名を指定します。このフィールドには、完全修飾ホスト名または次の形式の文字列を指定できます。 *domainname* **.domainname*
セッション	ユーザーセッションのデータに基づいて条件を設定します。変更できるフィールドは、次のとおりです。 ■ 「最大セッション時間」: セッションを開始してからポリシーを適用する間の最大ユーザーセッション時間を指定します。 ■ 「セッションを終了」: 選択すると、「最大セッション時間」フィールドで定義した許可される最大値をセッション時間が超えた場合に、ユーザーセッションを終了します。 この条件を使用すれば、認証後の限られた期間だけリソースを使用可能にする方法で、機密リソースを保護できます。
セッションプロパティー	ユーザーの Access Manager セッションに設定されたプロパティーの値に基づいて要求にポリシーを適用できるかどうかを決定します。ポリシーの評価中に条件が「真」を返すのは、ユーザーのセッションに条件で定義されたすべての

	プロパティー値が存在する場合だけです。条件の中で複数の値を使用して定義されたプロパティーについては、トークンのプロパティーの値が少なくとも 1 つあれば十分です。たとえば、この条件を使用すれば、外部リポジトリの属性に基づいてポリシーを適用することができます。認証後のプラグインは、外部属性に基づいてセッションプロパティーを設定できます。
時間	時間の制約に基づいて条件を設定します。フィールドは次のとおりです。 ■ 「開始日付 / 終了日付」: 日付の範囲を指定します。 ■ 「時刻」: 1 日での時間の範囲を指定します。 ■ 「曜日」: 曜日を指定します。 ■ 「タイムゾーン」: タイムゾーンを標準またはカスタムで指定します。カスタムのタイムゾーンとして指定できるのは、Java で認識されるタイムゾーン ID だけです (PST など)。値を指定しない場合は、デフォルト値は Access Manager JVM に設定されたタイムゾーンになります。

応答プロバイダ

応答プロバイダは、ポリシーベースの応答属性を提供するプラグインです。応答プロバイダ属性は、ポリシー決定とともに PEP に送信されます。Access Manager に実装されているのは `IDResponseProvider` の 1 つだけです。このバージョンの Access Manager では、カスタム応答プロバイダはサポートされていません。エージェントの PEP は通常、これらの応答属性をヘッダーとしてアプリケーションに渡します。アプリケーションは通常、これらの属性を使用して、ポータルページなどのアプリケーションページをポリシーに基づいて設定します。

ポリシーアドバイス

条件で決定したようにポリシーを適用できない場合は、ポリシーを要求に適用できなかった理由を示すアドバイスメッセージを条件によって作成できます。このアドバイスメッセージは、ポリシー決定でポリシー適用ポイントに伝わります。ポリシー適用ポイントでは、このアドバイスを取得し、認証メカニズムにユーザーを戻してより高いレベルに認証するなど、適切なアクションを実行しようとします。アドバイスの適切なアクションを実行したあとでポリシーが適用可能になると、ユーザーはより高いレベルの認証を要求され、リソースにアクセスできるようになることがあります。

詳細は、次のクラスを参照してください。

```
com.sun.identity.policy.ConditionDecision.getAdvices()
```

条件が満たされない場合、アドバイスを提供するのは、`AuthLevelCondiiton` と `AuthSchemeCondition` のみです。

AuthLevelCondition アドバイスは、次のキーに関連します。

```
com.sun.identity.policy.plugin.AuthLevelCondition.AUTH_LEVEL_CONDITION_ADVICE
```

AuthSchemeCondition アドバイスは、次のキーに関連します。

```
com.sun.identity.policy.plugin.AuthLevelCondition.AUTH_SCHEME_CONDITION_ADVICE
```

カスタム条件でもアドバイスを作成できます。ただし、Access Manager ポリシーエージェントは、認証レベルアドバイスと認証方式アドバイスのみに応答します。カスタムエージェントを作成してより多くのアドバイスを理解させて応答させたり、既存の Access Manager エージェントを拡張してより多くのアドバイスを理解させて応答させたりすることができます。詳細は、『Sun Java System Access Manager Policy Agent 2.2 User's Guide』を参照してください。

参照ポリシー

管理者は、あるレルムのポリシーの定義と決定を別のレルムに委任することが必要になる場合があります。または、あるリソースに対するポリシー決定を別のポリシー製品に委任することもできます。参照ポリシーは、ポリシーの作成と評価の両方に対するポリシーの委任を管理します。1 つ以上のルールと、1 つ以上の参照で構成されます。

ルール

ルールは、ポリシーの定義と評価が参照されるリソースを定義します。

参照

参照は、ポリシーの評価をどの組織に対して参照するかを定義します。デフォルトでは、2 種類の参照があります。ピアレルムとサブレルムです。それぞれ、同じレベルのレルム、下位レベルのレルムを表します。詳細は、152 ページの「ピアレルムおよびサブレルムのポリシーの作成」を参照してください。

注 – 参照先のレルムでは、そのレルムをすでに参照済みのリソース (またはサブリソース) のポリシーのみを定義または評価できます。ただし、この制約は最上位のレルムには適用されません。

ポリシー DTD

作成して設定したポリシーは、Directory Server に XML 形式で保存されます。Directory Server では、XML でエンコードされたデータは 1 か所に保管されます。ポリシーは、amAdmin.dtd (またはコンソール) を使って定義され設定されますが、実際には policy.dtd に基づく XML として、Directory Server に保存されます。policy.dtd は、amAdmin.dtd から抽出されたポリシー要素タグ (ポリシー作成タグを除く) を含んでいます。したがって、ポリシーサービスは Directory Server からポリシーをロードすると、policy.dtd に基づいて XML をパースします。ポリシーをコマンド行から作成するときには、amAdmin.dtd のみが使われます。この節では、policy.dtd の構造について説明します。policy.dtd は次の場所にあります。

```
AccessManager-base/SUNWam/dtd (Solairs)
AccessManager-base/identity/dtd (Linux)
```

注 – 本章ではこれ以降、ディレクトリ情報は Solaris についてのみ記します。Linux のディレクトリ構造は異なっていることに注意してください。

Policy 要素

Policy はアクセス権、つまりポリシーのルールと、ルールの適用先、つまり対象を定義するルート要素です。また、ポリシーが参照 (委任) ポリシーかどうか、およびポリシーになんらかの制限 (または条件) があるかどうかも定義します。この要素には、*Rule*、*Conditions*、*Subjects*、*Referrals*、*response providers* というサブ要素のうち 1 つ以上が含まれることがあります。必須の XML 属性は name で、これはポリシーの名前を指定します。referralPolicy 属性は、ポリシーが参照ポリシーであるかどうかを識別します。指定がなければ標準ポリシーとして扱われます。オプションの XML 属性には *name* と *description* があります。

注 – ポリシーに *referral* タグを付けると、対象と条件はポリシー評価の際、無視されます。逆に、ポリシーに *normal* タグを付けると、Referrals は無視されます。

Rule 要素

Rule 要素では、ポリシーの詳細を定義します。*ServiceName*、*ResourceName* 、*AttributeValuePair* という 3 つのサブ要素を持つことができます。この要素は、リソース名やそこで実行されるアクションだけではなく、ポリシーが作成されたサービスやアプリケーションのタイプを定義します。アクションを持たないルールも定義できます。たとえば、参照ポリシールールにはアクションはありません。

注 – *ResourceName* 要素を含まないポリシーの定義も可能です。

ServiceName 要素

ServiceName 要素は、ポリシーを適用するサービスの名前を定義します。この要素は、サービスのタイプを表しています。ほかの要素は含みません。値は、そのサービスの XML ファイルで (`sms.dtd` に基づいて) 定義されているとおりです。*ServiceName* 要素の XML サービス属性はサービスの名前 (値は文字列) です。

ResourceName 要素

ResourceName 要素は対象となるオブジェクトを定義します。ポリシーは、このオブジェクトを保護するように設定されています。ほかの要素は含みません。*ResourceName* 要素の XML サービス属性は、オブジェクトの名前です。*ResourceName* の例としては、Web サーバー上の `http://www.sunone.com:8080/images`、ディレクトリサーバー上の `ldap://sunone.com:389/dc=example,dc=com` などが挙げられます。より具体的なリソースとしては、 `salary://uid=jsmith,ou=people,dc=example,dc=com` などが考えられます。この場合、処理対象のオブジェクトは John Smith の給与情報になります。

AttributeValuePair 要素

AttributeValuePair 要素はアクションとその値を定義します。この要素は148 ページの「Subject 要素」、149 ページの「Referral 要素」、および149 ページの「Condition 要素」のサブ要素として扱われます。これは *Attribute* 要素と *Value* 要素を含み、XML サービス属性は含んでいません。

Attribute 要素

Attribute 要素はアクションの名前を定義します。アクションとは処理、つまりリソースに対して行われるイベントのことです。POST や GET は Web サーバーリソースに対して行われるアクションであり、READ や SEARCH はディレクトリサーバーリソースに対して行われるアクションです。*Attribute* 要素は *Value* 要素とペアにする必要があります。*Attribute* 要素自体は、ほかの要素を含みません。*Attribute* 要素に対する XML サービス属性は、アクションの名前です。

Value 要素

Value 要素はアクションの値を定義します。Allow (許可する)/Deny (許可しない)、Yes (はい) /No (いいえ) はアクションの値の例です。ほかのアクションの値は、ブール型、数値型、または文字列型が可能です。値は、そのサービスの XML ファイルの中で (`sms.dtd` に基づいて) 定義されています。*Value* 要素はほかの要素を含まず、また XML サービス属性も含みません。

注 – 許可しないルールは許可するルールより優先度が高くなります。たとえば、あるポリシーはアクセスを拒否し、別のポリシーが許可すると、(両方のポリシーのほかの条件がすべて一致する場合) 結果は拒否となります。許可しないポリシーを使用すると、ポリシー間で潜在的に衝突が生じるおそれがあるため、十分に注意して拒否ポリシーを使用することをお勧めします。明示的な許可しないルールを使用すると、さまざまな対象 (ロールやグループメンバーシップなど) を通じてユーザーに割り当てられたポリシーが、アクセスを拒否する可能性があります。通常は、ポリシー定義プロセスでは、許可するルールのみを使うべきです。デフォルトで「許可しない」というのは、ほかに適用するポリシーがない場合に使用します。

Subjects 要素

Subjects サブ要素はポリシーが適用される主体の集合を特定します。この集合はグループのメンバーシップ、ロールの所有権、または個別ユーザーに基づいて選択されます。この要素は、*Subject* というサブ要素を持ちます。定義できる XML 属性は以下のとおりです。

name: 集合の名前を定義します。

description: 対象の説明を定義します。

includeType: 現在は使われていません。

Subject 要素

Subject サブ要素はポリシーを適用する主体の集合を特定します。この集合は、Subjects 要素が定義する集合をさらに絞り込んだものです。メンバーシップは、ロール、グループメンバーシップ、または単なる個別ユーザーのリストに基づきます。この要素は、147 ページの「AttributeValuePair 要素」というサブ要素を含みます。必須の XML 属性は `type` で、特定の定義済み対象を持つ、オブジェクトの一般的な集合を特定します。ほかの XLM 属性には、集合の名前を定義する `name`、対象のメンバーでないユーザーに対してポリシーを適用するかどうかに関して、集合が定義されたとおりになっているかどうかを定義する `includeType` があります。

注 – 複数の対象を定義した場合、ポリシーを適用するためには少なくとも 1 つの対象をユーザーに適用しなければなりません。`includeType` を false にして対象を定義するときは、ユーザーがその対象のメンバーではないことが必要です。

Referrals 要素

Referrals サブ要素はポリシー参照の集合を特定します。この要素は、*Referral* というサブ要素を持ちます。ともに定義できる XML 属性には、集合の名前を定義する `name`、説明を含む `description` があります。

Referral 要素

Referral サブ要素は個別のポリシー参照を特定します。この要素は、サブ要素として 147 ページの「AttributeValuePair 要素」 を取ります。必須の XML 属性は `type` で、特定の定義済み参照を持つ、割り当ての一般的な集合を特定します。また、集合の名前を定義する `name` 属性を持つこともできます。

Conditions 要素

Conditions サブ要素はポリシーの制限 (時間範囲、認証レベル、その他) の集合を特定します。この要素は複数の *Condition* サブ要素を含んでいなければなりません。ともに定義できる XML 属性には、集合の名前を定義する `name`、説明を含む `description` があります。

注 – conditions 要素は、ポリシーの中ではオプションの要素です。

Condition 要素

Condition サブ要素は特定のポリシーの制限 (時間範囲、認証レベル、その他) を特定します。この要素は、サブ要素として 147 ページの「AttributeValuePair 要素」 を取ります。必須の XML 属性は `type` で、特定の定義済み対象を持つ、オブジェクトの一般的な集合を特定します。また、集合の名前を定義する `name` 属性を持つこともできます。

ポリシーを有効にしたサービスの追加

サービススキーマの `<Policy>` 要素が `sms.dtd` に設定されている場合にのみ、そのサービスのリソースにポリシーを定義することができます。

デフォルトで、Access Manager は URL ポリシーエージェントサービス (`iPlanetAMWebAgentService`) を提供します。このサービスは、XML ファイル形式で定義され、次のディレクトリにあります。

```
/etc/opt/SUNWam/config/xml/
```

Access Manager にさらにポリシーサービスを追加することもできます。ポリシーサービスを作成したら、amadmin コマンド行ユーティリティーを使って、これを Access Manager に追加します。

▼ 新しいポリシーを有効にしたサービスを追加する

1 新しいポリシーサービスを sms.dtd に基づいて **XML** ファイルで作成します。新しいポリシーサービスファイルの雛型にできるポリシーサービス **XML** ファイルが **2** つ、**Access Manager** から提供されます。

amWebAgent.xml はデフォルトの URL ポリシーエージェントサービスのための XML ファイルです。これは /etc/opt/SUNWam/config/xml/ にあります。

SampleWebService.xml は、ポリシーサービスファイルのサンプルであり、SampleWebService.xml にあります。

2 新しいポリシーサービスをロードするディレクトリに **XML** ファイルを保存します。次に例を示します。

```
/config/xml/newPolicyService.xml
```

3 新しいポリシーサービスを amadmin コマンド行ユーティリティーを使ってロードします。次に例を示します。

```
AccessManager-base/SUNWam/bin/amadmin
    --runasdn "uid=amAdmin,ou=People,default_org,
root_suffix
    --password password
    --schema /config/xml/newPolicyService.xml
```

4 新しいポリシーサービスをロードしたあと、**Access Manager** コンソールから作業を行うか、または、amadmin で新しいポリシーをロードすることにより、ポリシー定義のルールを定義できます。

ポリシーの作成

Policy API と Access Manager コンソールを使用してポリシーを作成、変更、および削除でき、amadmin コマンド行ツールを使用してポリシーを作成および削除できます。また、amadmin ユーティリティーを使用して、ポリシーの一覧を XML 形式で取得して表示することもできます。この節では、amadmin コマンド行ユーティリティーと Access Manager コンソールを使用してポリシーを作成することを中心に説明します。Policy API の詳細は、『Sun Java System Access Manager 7 2005Q4 Developer's Guide』を参照してください。

通常ポリシーは XML ファイルで作成し、amadmin コマンド行ユーティリティーを使って Access Manager に追加し、Access Manager のコンソールを使って管理します (ただし、ポ

リシーをコンソールで作成することもできる)。これは、ポリシーが amadmin を使って直接変更できないからです。ポリシーを修正するには、そのポリシーを Access Manager から削除してから、修正したポリシーを amadmin を使用して追加します。

一般に、ポリシーはレルムツリー全体で使用するために、レルムまたはサブレルムレベルで作成します。

▼ amadmin でポリシーを作成する

1 ポリシーの **XML** ファイルを amadmin.dtd に基づいて作成します。このファイルは次のディレクトリにあります。

AccessManager-base /SUNWam/dtd

2 ポリシーの **XML** ファイルを作成したら、次のコマンドを使用してロードできます。

AccessManager-base/SUNWam/bin/amadmin
--runasdn "uid=amAdmin,ou=People,*default_org*,
root_suffix"
--password *password*
--data *policy.xml*

複数のポリシーを同時に追加するには、各 XML ファイルにポリシーを 1 つずつ置くのではなく、1 つの XML ファイルにすべてのポリシーを置きます。複数の XML ファイルでポリシーを次々とロードすると、内部ポリシーインデックスが破損したり、ポリシーの評価に参加できないポリシーが生じたりするおそれがあります。

ポリシーを amadmin で作成するときは、認証スキーム条件を作成中にレルムに認証モジュールを登録することの確認、レルム、LDAP グループ、LDAP ロール、および LDAP ユーザーの対象を作成中に、対応する LDAP オブジェクト (レルム、グループ、ロール、およびユーザー) が存在することの確認、IdentityServerRoles 対象を作成中に、Access Manager ロールが存在することの確認、そしてサブレルムまたはピアレルムの参照を作成中に、関連があるレルムが存在することの確認を行ってください。

SubrealmReferral、PeerRealmReferral、Realm 対象、IdentityServerRoles 対象、LDAPGroups 対象、LDAPRoles 対象、および LDAPUsers 対象の Value 要素のテキストには、完全な DN を指定する必要があります。

▼ Access Manager コンソールを使って標準ポリシーを作成する

1 ポリシーを作成するレルムを選択します。

2 「ポリシー」タブをクリックします。

3 「ポリシー」リストから「新規ポリシー」をクリックします。

4 ポリシーの名前と説明を入力します。

5 ポリシーをアクティブにする場合は、「アクティブ」属性で「はい」を選択します。

6 この時点では、標準ポリシーのフィールドすべてを定義する必要はありません。ポリシーの作成後、ルール、対象、条件、および応答プロバイダを追加できます。詳細は、153 ページの「ポリシーの管理」を参照してください。

7 「作成」をクリックします。

▼ Access Manager コンソールを使って参照ポリシーを作成する

1 ポリシーを作成するレルムを選択します。

2 「ポリシー」タブから「新規参照」をクリックします。

3 ポリシーの名前と説明を入力します。

4 ポリシーをアクティブにする場合は、「アクティブ」属性で「はい」を選択します。

5 この時点では、参照ポリシーのフィールドすべてを定義する必要はありません。ポリシーの作成後、ルールおよび参照を追加できます。詳細は、153 ページの「ポリシーの管理」を参照してください。

6 「作成」をクリックします。

ピアレルムおよびサブレルムのポリシーの作成

ピアレルムまたはサブレルムのポリシーを作成するには、まず親レルムまたは別のピアレルムで参照ポリシーを作成する必要があります。参照ポリシーのルールの定義には、サブレルムが管理するリソースプレフィックスを含める必要があります。親レルムまたは別のピアレルムで参照ポリシーを作成すれば、サブレルムまたはピアレルムで標準ポリシーを作成できます。

次の例では、`o=isp` は親レルム、`o=example.com` は、`http://www.example.com` のリソースとサブリソースを管理するサブレルムです。

▼ サブレルムのポリシーを作成する

1 o=isp で参照ポリシーを作成します。参照ポリシーについては、157 ページの「参照ポリシーの修正」の手順を参照してください。

参照ポリシーは、http://www.example.com をリソースとしてルールに定義し、参照内に example.com を値として持つ SubRealmReferral を含んでいる必要があります。

2 example.com というサブレルムに移動します。

3 これで isp によってリソースが example.com の管理に委ねられたので、http://www.example.com というリソース、または http://www.example.com から始まる任意のリソースに対して標準ポリシーを作成できます。

example.com で管理する別のリソースのポリシーを定義するには、追加の参照ポリシーを o=isp に作成する必要があります。

ポリシーの管理

標準または参照ポリシーを作成し、Access Manager に追加したあとは、ポリシーの管理は、Access Manager のコンソールを使用して、ルール、対象、条件と参照を変更することにより行えます。

標準ポリシーの修正

「ポリシー」タブを使用して、アクセス権を定義する標準ポリシーを変更することができます。複数のルール、対象、条件、およびリソースコンパレータを定義および設定できます。ここでは、標準ポリシーを変更する手順のいくつかについて説明します。

▼ 標準ポリシーのルールを追加または変更する

1 すでにポリシーを作成済みである場合は、ルールを追加するポリシーの名前をクリックします。ポリシーを作成済みでない場合は、151 ページの「Access Manager コンソールを使って標準ポリシーを作成する」を参照してください。

2 「ルール」メニューから「新規」をクリックします。

3 次のデフォルトのサービスタイプから、ルール用に 1 つ選択します。ポリシーに複数のサービスが使用できる場合は、さらに多くのサービスが一覧表示されます。

ディスカバリサービス	ディスカバリサービスクエリー用の認証アクションを定義し、指定されたリソースについて、Web サービスクライアントによるプロトコル呼び出しを変更します。

Liberty 個人プロファイルサービス	Liberty 個人プロファイルサービスクエリー用の認証アクションを定義し、指定されたリソースについて、Web サービスクライアントによるプロトコル呼び出しを変更します。
URL ポリシーエージェント	ポリシーを適用するための URL ポリシーエージェントサービスを提供します。このサービスにより、管理者はポリシーエンフォーサ、つまりポリシーエージェントにより、ポリシーの作成および管理を行えます。

4 「次へ」をクリックします。

5 ルールの名前とリソース名を入力します。

現在、ポリシーエージェントでサポートされているリソースは `http://` と `https://` だけです。また、ホスト名の代わりに IP アドレスを使用することはできません。

ホスト名、ポート名、およびリソース名にはワイルドカードを使用できます。次に例を示します。

```
http*://*:*/*.html
```

URL ポリシーエージェントサービスでは、ポート番号が入力されていない場合のデフォルトのポート番号は、`http://` では 80、`https://` では 443 となります。

6 ルールのアクションを選択します。**URL** ポリシーエージェントサービスを使用する場合は、次のアクションを選択できます。

- GET
- POST

7 アクションの値を選択します。

- 許可 — ルールに定義されたリソースに一致するリソースへのアクセスを許可
- 拒否 — ルールに定義されたリソースに一致するリソースへのアクセスを拒否
- 拒否するルールは許可するルールより優先度が高くなります。たとえばあるリソースに 2 つのポリシーがあり、1 つはアクセス拒否でもう 1 つはアクセス許可の場合、その結果はアクセスの拒否になります (両方のポリシーの条件が一致する場合)。拒否ポリシーを使用すると、ポリシー間で潜在的に衝突が生じるおそれがあるため、十分に注意して拒否ポリシーを使用することをお勧めします。ポリシー定義プロセスでは、許可するルールのみを使うべきです。リソースに適用するポリシーがない場合、アクセスは自動的に拒否されます。

  拒否ルールを明示的に使用すると、1 つ以上のポリシーでアクセスが許可される場合でも、異なる対象 (ロールやグループのメンバーシップ) を通じてユーザーに割り当てられたポリシーによって、リソースへのアクセスを拒否されるおそれがあります。たとえば、1 つのリソースについて、Employee ロールに適用される拒否ポリシーと、

Manager ロールに適用される許可ポリシーがあるとします。この場合、Employee ロールと Manager ロールの両方を割り当てられているユーザーへのポリシーの決定は拒否されます。

このような問題を解決する 1 つの方法は、条件プラグインを使ってポリシーを設計することです。上記の例では、Employee ロールに認証されたユーザーには拒否ポリシーを適用し、Manager ロールに認証されたユーザーには許可ポリシーを適用するという "ロール条件" を利用することで、2 つのポリシーを区別できます。Manager ロールにはより高い認証レベルが与えられることから、認証レベル条件を使用する方法もあります。

8 「終了」をクリックします。

▼ 標準ポリシーの対象を追加および変更する

1 すでにポリシーを作成済みである場合は、対象を追加するポリシーの名前をクリックします。ポリシーを作成済みでない場合は、151 ページの「Access Manager コンソールを使って標準ポリシーを作成する」を参照してください。

2 「対象」リストから、「新規」をクリックします。

3 デフォルトの対象タイプを次の中から選択します。対象タイプの説明は、140 ページの「対象」を参照してください。

4 「次へ」をクリックします。

5 対象の名前を入力します。

6 「排他的」フィールドを選択または選択解除します。

このフィールドが選択されていないと (デフォルト)、ポリシーは、対象のメンバーであるアイデンティティーに適用されます。このフィールドが選択されていると、ポリシーは、対象のメンバーではないアイデンティティーに適用されます。

ポリシーに複数の対象が存在する場合には、1 つ以上の対象のメンバーであるアイデンティティーにポリシーが適用されます。

7 検索を実行して、対象に追加するアイデンティティーを表示します。この手順は、「認証済みユーザー」対象や「Web サービスクライアント」対象には適用できません。

デフォルト (*) の検索パターンでは、すべてのエントリが表示されます。

8 対象に追加する個々のアイデンティティーを選択するか、または「すべて追加」を選択して一度にすべてのアイデンティティーを追加します。「追加」をクリックしてアイデンティティーを選択リストに移動します。この手順は、「認証済みユーザー」対象には適用されません。

9 「終了」をクリックします。

10 ポリシーから対象を削除するには、対象を選択して「削除」をクリックします。対象の名前をクリックすると、対象の定義を編集できます。

▼ 標準ポリシーに条件を追加する

1 すでにポリシーを作成済みである場合は、条件を追加するポリシーの名前をクリックします。ポリシーを作成済みでない場合は、151 ページの「Access Manager コンソールを使って標準ポリシーを作成する」を参照してください。

2 「条件」リストから、「新規」をクリックします。

3 条件タイプを選択して、「次へ」をクリックします。

4 条件タイプのフィールドを定義します。条件タイプの説明は、142 ページの「条件」を参照してください。

5 「終了」をクリックします。

▼ 標準ポリシーに応答プロバイダを追加する

1 すでにポリシーを作成済みである場合は、応答プロバイダを追加するポリシーの名前をクリックします。ポリシーを作成済みでない場合は、151 ページの「Access Manager コンソールを使って標準ポリシーを作成する」を参照してください。

2 「応答プロバイダ」リストから、「新規」をクリックします。

3 応答プロバイダの名前を入力します。

4 次の値を定義します。

StaticAttribute　その名前と値が `IDResponseProvider` インスタンスに定義され、ポリシーに保存されている応答属性。

DynamicAttribute　ここで選択する応答属性は、対応するレルムのポリシー設定サービス内で事前に定義されている必要があります。定義される属性名は、設定済みデータストア内に存在する属性名と同じになるようにしてください。属性の定義方法の詳細については、Access Manager のオンラインヘルプで、ポリシー設定属性定義の項目を参照してください。

5 「終了」をクリックします。

6 ポリシーから応答プロバイダを削除する場合は、そのプロバイダを選択し、「削除」をクリックします。名前をクリックすると、応答プロバイダの定義を編集できます。

参照ポリシーの修正

参照ポリシーを使用すると、あるレルムのポリシーの定義や判断を別のレルムに委任できます。カスタム参照を使用すると、任意のポリシー適用先からポリシー決定を取得できます。参照ポリシーを作成したら、関連付けられているルール、参照、および応答プロバイダを追加または変更できます。

▼ 参照ポリシーのルールを追加および変更する

1 すでにポリシーを作成済みである場合は、ルールを追加するポリシーの名前をクリックします。ポリシーを作成済みでない場合は、152 ページの「Access Manager コンソールを使って参照ポリシーを作成する」を参照してください。

2 「ルール」リストから「新規」をクリックします。

3 次のデフォルトのサービスタイプから、ルール用に 1 つ選択します。ポリシーに複数のサービスが使用できる場合は、さらに多くのサービスが一覧表示されます。

ディスカバリサービス	ディスカバリサービスクエリー用の認証アクションを定義し、指定されたリソースについて、Web サービスクライアントによるプロトコル呼び出しを変更します。
Liberty 個人プロファイルサービス	Liberty 個人プロファイルサービスクエリー用の認証アクションを定義し、指定されたリソースについて、Web サービスクライアントによるプロトコル呼び出しを変更します。
URL ポリシーエージェント	ポリシーを適用するための URL ポリシーエージェントサービスを提供します。このサービスにより、管理者はポリシーエンフォーサ、つまりポリシーエージェントにより、ポリシーの作成および管理を行えます。

4 「次へ」をクリックします。

5 ルールの名前とリソース名を入力します。

現在、ポリシーエージェントでサポートされているリソースは `http://` と `https://` だけです。また、ホスト名の代わりに IP アドレスを使用することはできません。

リソース名、ポート番号、およびプロトコルにはワイルドカードを使用できます。次に例を示します。

```
http://*:*/*.html
```

URL ポリシーエージェントサービスでは、ポート番号が入力されていない場合のデフォルトのポート番号は、`http://` では 80、`https://` では 443 となります。

リソースを `http://host*:*` として定義して、特定のマシンにインストールされたすべてのサーバーに対してリソースの管理を許可できます。また、次のリソースを定義して、組織のすべてのサービスに対する特定の組織権限を管理者に与えることができます。

`http://*.`*subdomain.domain.topleveldomain*

6 「終了」をクリックします。

▼ ポリシーの参照を追加または変更する

1 すでにポリシーを作成済みである場合は、応答プロバイダを追加するポリシーの名前をクリックします。ポリシーを作成済みでない場合は、152 ページの「Access Manager コンソールを使って参照ポリシーを作成する」を参照してください。

2 「ルール」リストから「新規」をクリックします。

3 「サービスタイプ」を選択します。

4 「ルール」フィールドにリソースを定義します。フィールドは次のとおりです。

参照— 現在の参照タイプが表示されます。

名前— 参照の名前を入力します。

リソース名— リソースの名前を入力します。

フィルター—「値」フィールドに表示する組織名を絞り込むためのフィルタを指定します。デフォルトでは、すべての組織名が表示されます。

値 — 参照の組織名を選択します。

5 「終了」をクリックします。

ポリシーから参照を削除するには、参照を選択して「削除」をクリックします。

参照名の横にある「編集」リンクをクリックすれば、参照の定義を編集できます。

▼ 参照ポリシーに応答プロバイダを追加する

1. すでにポリシーを作成済みである場合は、応答プロバイダを追加するポリシーの名前をクリックします。ポリシーを作成済みでない場合は、151 ページの「Access Manager コンソールを使って標準ポリシーを作成する」を参照してください。
2. 「応答プロバイダ」リストから、「新規」をクリックします。
3. 応答プロバイダの名前を入力します。
4. 次の値を定義します。

   StaticAttribute — その名前と値が `IDResponseProvider` インスタンスに定義され、ポリシーに保存されている応答属性。

   DynamicAttribute — その名前がポリシーの `IDResponseProvider` インスタンスで選択されただけの応答属性。値は、ポリシーが評価されるときに要求されたユーザーアイデンティティーに基づいて、 `IDRepostitories` から読み込まれます。

5. 「終了」をクリックします。
6. ポリシーから応答プロバイダを削除する場合は、そのプロバイダを選択し、「削除」をクリックします。名前をクリックすると、応答プロバイダの定義を編集できます。

ポリシー設定サービス

各組織のポリシーに関連する属性の設定を Access Manager コンソールから行うにはポリシー設定サービスを使用します。Access Manager ポリシーフレームワークで使用するリソース名の実装および Directory Server データストアを定義することもできます。ポリシー設定サービスに指定した Directory Server は、LDAP ユーザー、LDAP グループ、LDAP ロール、および組織ポリシー対象のメンバーシップの評価に使用されます。

対象結果の有効時間

ポリシー評価のパフォーマンスを上げるため、ポリシー設定サービスの「対象結果の有効時間」属性で定義されるとおり、メンバーシップ評価を一定の時間キャッシュします。これらのキャッシュされたメンバーシップ決定は「対象結果の有効時間」属性で定義された時間が経つまで使用されます。この時間が経過したあとは、ディレクトリ内のユーザーの現在の状態を反映するために、メンバーシップ評価が使用されます。

動的属性

これらは使用可能な動的属性の名前であり、ポリシーの応答プロバイダの動的属性を定義する際に一覧表示され、選択されます。定義される名前は、データリポジトリ内に定義された属性名と同じである必要があります。

amldapuserの定義

amldapuserはインストール時に作成されたユーザーで、ポリシー設定サービスに指定したDirectory Serverでデフォルトで使用されます。amldapuserは、レルムの管理者またはポリシー管理者が必要に応じて変更できます。

ポリシー設定サービスの追加

レルムを作成すると、そのレルムのためにポリシー設定サービスの属性が自動的に設定されます。ただし、これらの属性は必要に応じて変更できます。

リソースベースの認証

組織によっては高度な認証シナリオが必要です。この場合、ユーザー認証は、アクセスしようとするリソースごとに特定のモジュールで行われます。リソースベースの認証は、Access Managerの機能で、ユーザーはデフォルトの認証モジュールではなく、そのリソースを保護している認証モジュールから認証される必要があります。この機能は、ユーザーが初めて認証される時にのみ適用可能です。

注 – これは、134ページの「セッションのアップグレード」で説明しているリソースベースの認証とは別の機能です。その機能には何の制限もありません。

制限

リソースベースの認証には、次のような制限があります。

- リソースに適用可能なポリシーに認証モジュールが複数個含まれていた場合、そのどちらかの認証モジュールがシステムによって自動的に選択されます。
- このポリシーについて定義できる条件はレベルと方式だけです。
- この機能は、異なるDNSドメイン間では働きません。

▼ リソースベースの認証を設定する

Access Manager とポリシーエージェントをインストールしたら、リソースベースの認証を設定できます。そのためには、Access Manager が Gateway サーブレットを指す必要があります。

1 `AMAgent.properties` を開きます。

`AMAgent.properties` は Solaris 環境では `/etc/opt/SUNWam/agents/config/` にあります。

2 次の行をコメントアウトします。

```
#com.sun.am.policy.am.loginURL = http://Access
Manager_server_host.domain_name:port/amserver/UI/Login.
```

3 ファイルに次の行を追加します。

```
com.sun.am.policy.am.loginURL =
http://AccessManager_host.domain_name:port/amserver/gateway
```

注 – ゲートウェイサーブレットは Policy Evaluation API を使って開発します。このサーブレットを使えば、リソースベースの認証を実現するためのカスタムメカニズムを記述できます。『Sun Java System Access Manager 7 2005Q4 Developer's Guide』の第 6 章「Using the Policy APIs」を参照してください。

---

4 サーバーを再起動します。

◆ ◆ ◆ 第 9 章

9 対象の管理

「対象」インタフェースにより、レルム内部で基本的なアイデンティティー管理を行うことができます。「対象」インタフェースで作成するすべてのアイデンティティーは、Access Manager アイデンティティー対象タイプを使って作成されるポリシーに対する対象定義で使用できます。

作成および変更できるアイデンティティーには、次のものがあります。

ユーザー

ユーザーは、個人のアイデンティティーを表現します。グループ内でユーザーを作成および削除できます。また、ロールやグループにユーザーを追加したり、ロールやグループからユーザーを削除することができます。サービスをユーザーに割り当てることもできます。

▼ ユーザーを作成または変更する

1. 「ユーザー」タブをクリックします。
2. 「新規」をクリックします。
3. 次のフィールドのデータを入力します。

   「ユーザー **ID**」**:** このフィールドには、ユーザーが Access Manager へログインするために使用する名前を指定します。このプロパティーは、DN 以外の値になることがあります。

「名」:このフィールドには、ユーザーの名 (ファーストネーム) を指定します。

「姓」: このフィールドはユーザーの姓 (ラストネーム) を取得します。

「フルネーム」: このフィールドには、ユーザーのフルネームを指定します。

「パスワード」: このフィールドには、「ユーザー ID」フィールドで指定した名前のパスワードを指定します。

「パスワード (確認)」: 確認のためにパスワードを再入力します。

「ユーザー状態」: このオプションは、Access Manager による認証をユーザーに許可するかどうかを指定します。

4 「作成」をクリックします。

5 ユーザーの作成後は、ユーザーの名前をクリックすることによってユーザー情報を編集できます。ユーザー属性の詳細については、「ユーザー属性」を参照してください。実行できるその他の変更には、次のものがあります。

- 163 ページの「ユーザーを作成または変更する」
- 164 ページの「ロールおよびグループにユーザーを追加する」
- 164 ページの「サービスをアイデンティティーに追加する」

▼ ロールおよびグループにユーザーを追加する

1 変更するユーザーの名前をクリックします。

2 「ロール」または「グループ」を選択します。ユーザーにすでに割り当てられているロールおよびグループだけが表示されます。

3 「利用可能」リストからロールまたはグループを選択して「追加」をクリックします。

4 ロールまたはグループが「選択」リストに表示されたら、「保存」をクリックします。

▼ サービスをアイデンティティーに追加する

1 サービスを追加するアイデンティティーを選択します。

2 「サービス」タブをクリックします。

3 「追加」をクリックします。

4 選択したアイデンティティータイプに応じて、次のサービスのリストが表示されます。

- 認証設定

- ディスカバリサービス
- Liberty 個人プロファイルサービス
- セッション
- ユーザー

5 追加するサービスを選択して「次へ」をクリックします。

6 サービスの属性を編集します。サービスの説明を見るには、ステップ **4** でサービス名をクリックします。

7 「終了」をクリックします。

エージェント

Access Manager ポリシーエージェントは、Web サーバーおよび Web プロキシサーバー上のコンテンツを未承認の不正侵入から保護します。エージェントは、管理者によって設定されたポリシーに基づいて、サービスおよび Web リソースへのアクセスを制御します。

エージェントオブジェクトは、ポリシーエージェントプロファイルを定義します。また、Access Manager リソースを保護している特定のエージェントの認証情報やその他のプロファイル情報を Access Manager で保存できるようにします。管理者は Access Manager コンソールから、エージェントプロファイルを参照、作成、変更、および削除できます。

エージェントオブジェクト作成ページは、エージェントが Access Manager の認証を受ける UID およびパスワードを定義できる場所です。同一の Access Manager を使用して複数の AM/WS を設定した場合は、これにより、異なるエージェントに対して複数の ID を有効にすることができ、Access Manager から独立してそれらの ID を有効にしたり無効にしたりできます。また、マシンごとに `AMAgent.properties` を編集するのではなく、エージェントの設定値によっては集中的に管理することもできます。

▼ エージェントを作成または変更する

1 「エージェント」タブをクリックします。

2 「新規」をクリックします。

3 次のフィールドの値を入力します。

「名前」: エージェントの名前またはアイデンティティーを入力します。これは、エージェントが Access Manager にログインするために使用する名前です。1 バイト文字による名前のみ受け付けます。

「パスワード」: エージェントのパスワードを入力します。このパスワードは、LDAP 認証時にエージェントが使用するパスワードとは異なっている必要があります。

「パスワードを確認」: パスワードを確認します。

「デバイスの状態」: エージェントのデバイスの状態を入力します。「アクティブ」に設定すると、エージェントで Access Manager に対する認証の実行および Access Manager との通信が可能になります。「非アクティブ」に設定すると、エージェントは Access Manager に対して認証を実行できなくなります。

4 「作成」をクリックします。

5 エージェントを作成したあとで、さらに次のフィールドを編集できます。

「説明」: エージェントの簡単な説明を入力します。たとえば、エージェントのインスタンス名や、エージェントが保護しているアプリケーションの名前を入力できます。

「エージェントキー値」: キーと値のペアでエージェントのプロパティーを設定します。このプロパティーは、ユーザーに関する資格表明の要求をエージェントから受け付けるために Access Manager によって使用されます。現時点では 1 つのプロパティーだけが有効であり、その他のプロパティーはすべて無視されます。次の形式を使用します。

agentRootURL=`http://` *server_name*:*port*/

一意のポリシーエージェントアイデンティティーの作成

デフォルトでは、信頼できる環境で複数のポリシーエージェントを作成するときは、ポリシーエージェントに同一の UID およびパスワードが含まれます。UID およびパスワードが共有されるため、Access Manager はエージェントを区別できません。そのため、セッション Cookie が横取りされる可能性があります。

この弱点は、認証、承認、およびユーザーに関するプロファイル情報がアイデンティティープロバイダによって、サードパーティーまたは企業内の未承認のグループによって開発されたアプリケーションまたはサービスプロバイダに提供される場合に存在するようになることがあります。考えられるセキュリティー上の問題を次に示します。

- すべてのアプリケーションは同一の HTTP セッション Cookie を共有します。このため、不正なアプリケーションがセッション Cookie をハイジャックし、そのユーザーが偽装によって別のアプリケーションにアクセスできるようになります。
- アプリケーションが HTTPS プロトコルを使用していない場合、セッション Cookie はネットワーク盗聴される傾向があります。
- 1 つでもアプリケーションがハッキングされる可能性がある場合、インフラストラクチャー全体のセキュリティーが危険にさらされます。
- 不正なアプリケーションは、セッション Cookie を使用してユーザーのプロファイル属性を取得することができ、変更することも考えられます。ユーザーが管理権限を持っている場合、そのアプリケーションはさらに多くの損害を与える可能性があります。

▼ 一意のポリシーエージェントアイデンティティーを作成する

1 **Access Manager** 管理コンソールを使用して、エージェントごとにエントリを作成します。

2 エージェントの作成時に入力したパスワードに次のコマンドを実行します。このコマンドは、エージェントがインストールされているホストで起動してください。

```
AccessManager-base/SUNWam/agents/bin/crypt_util agent123
```

次の出力が得られます。

```
WnmKUCg/y3l404ivWY6HPQ==
```

3 新しい値を反映するように `AMAgent.properties` を変更し、エージェントを再起動します。例:

```
# The username and password to use for the Application
authentication module.

com.sun.am.policy.am.username = agent123
com.sun.am.policy.am.password = WnmKUCg/y3l404ivWY6HPQ==

# Cross-Domain Single Sign On URL
# Is CDSSO enabled.
com.sun.am.policy.agents.cdsso-enabled=true

# This is the URL the user will be redirected to after successful login
# in a CDSSO Scenario.
com.sun.am.policy.agents.cdcservletURL = http://server.example.com:port
/amserver/cdcservlet
```

4 新しい値を反映するように、**Access Manager** がインストールされている `AMConfig.properties` を変更し、**Access Manager** を再起動します。例:

```
com.sun.identity.enableUniqueSSOTokenCookie=true
com.sun.identity.authentication.uniqueCookieName=sunIdentityServerAuthNServer

com.sun.identity.authentication.uniqueCookieDomain=.example.com
```

5 **Access Manager** コンソールで、「設定」、「プラットフォーム」の順に選択します。

6 「**Cookie** ドメイン」リストで、次のように **Cookie** ドメイン名を変更します。

a. デフォルトの `iplanet.com` ドメインを選択し、「消去」をクリックします。

b. **Access Manager** インストールのホスト名を入力し、「追加」をクリックします。

例: `server.example.com`

次に示すように 2 つの Cookie がブラウザに設定されます。

- iPlanetDirectoryPro – server.example.com (ホスト名)
- sunIdentityServerAuthNServer – example.com (ホスト名)

フィルタロール

フィルタロールは、LDAP フィルタを使用して作成される動的なロールです。ユーザーはすべてフィルタを通してまとめられ、ロールの作成時にそのロールに割り当てられます。フィルタはエントリの属性と値のペア (ca=user* など) を検索して、その属性を含むユーザーをロールに自動的に割り当てます。

▼ フィルタロールを作成する

1. ナビゲーション区画で、ロールを作成する組織に移動します。
2. 「新規」をクリックします。
3. フィルタロールの名前を入力します。
4. 検索条件を入力します。

   例を示します。

   ```
   (&(uid=user1)(|(inetuserstatus=active)(!(inetuserstatus=*))))
   ```

   フィルタを空白のままにすると、次のロールが作成されます。

   ```
   (objectclass = inetorgperson)
   ```

5. 「作成」をクリックして、フィルタ条件に基づく検索を開始します。フィルタ条件によって定義されたアイデンティティーは、ロールに自動的に割り当てられます。
6. フィルタロールが作成されたら、ロールの名前をクリックして、そのロールに属するユーザーを表示します。「サービス」タブをクリックして、ロールにサービスを追加することもできます。

ロール

ロールのメンバーは、ロールを所有する LDAP エントリです。ロール自体の基準は、属性を持つ LDAP エントリとして定義されます。このエントリは、エントリの識別名 (DN) 属性で特定されます。ロールが作成されたら、サービスとユーザーを手動で追加できます。

▼ ロールを作成または変更する

1 「ロール」タブをクリックします。

2 「ロール」リストで「新規」をクリックします。

3 ロールの名前を入力します。

4 「作成」をクリックします。

▼ ユーザーをロールまたはグループに追加する

1 ユーザーを追加するロールまたはグループの名前をクリックします。

2 「ユーザー」タブをクリックします。

3 追加するユーザーを「利用可能」リストから選択して「追加」をクリックします。

4 ユーザーが「選択」リストに表示されたら、「保存」をクリックします。

グループ

グループは、共通の職務、特徴、または興味を持つユーザーの集合を表現します。通常、このグループ分けに権限は関連付けられません。グループは組織の内部とほかの管理対象グループの内部の 2 つのレベルで定義できます。

▼ グループを作成または変更する

1 「グループ」タブをクリックします。

2 「グループ」リストから「新規」をクリックします。

3 グループの名前を入力します。

4 「作成」をクリックします。
グループを作成したら、グループ名、「ユーザー」タブの順にクリックして、ユーザーをグループに追加できます。

パート III

ディレクトリ管理とデフォルトサービス

これは『Sun Java System Access Manager 7 2005Q4 管理ガイド』の第 3 部です。「ディレクトリ管理」の章では、Access Manager を旧バージョンモードで配備するときにディレクトリオブジェクトを管理する方法について説明します。その他の章では、Access Manager の一部のデフォルトサービスを設定および使用する方法について説明します。次の章で構成されています。

◆ ◆ ◆ 第 10 章

10 ディレクトリ管理

「ディレクトリ管理」タブは、Access Manager を旧バージョンモードでインストールした場合にのみ表示されます。このディレクトリ管理機能は、Sun Java System の Directory Server に対応した Access Manager の配備に必要なアイデンティティー管理ソリューションを提供します。

インストール時の旧バージョンモードオプションについては、『Sun Java Enterprise System 2005Q4 Installation Guide for UNIX』を参照してください。

ディレクトリオブジェクトの管理

「ディレクトリ管理」タブには、Directory Server オブジェクトの表示および管理に必要なすべてのコンポーネントが含まれています。この節では、オブジェクトタイプと、それらを設定する方法の詳細について説明します。Access Manager コンソールまたはコマンド行インタフェースを使用して、ユーザー、ロール、グループ、組織、サブ組織、およびコンテナの各オブジェクトを定義、修正、または削除できます。コンソールには、ディレクトリオブジェクトを作成および管理する権限が異なる、複数のデフォルト管理者が存在しています。ロールに基づいて、管理者を追加作成できます。管理者は、Access Manager でインストールしたときに、Directory Server 内に定義されます。次の Directory Server オブジェクトを管理できます。

組織

組織は、企業が部門とリソースの管理に使用する最上位レベルの階層構造を表します。インストール時に、Access Manager は最上位レベルの組織 (インストール時に定義) を動的に作成して、Access Manager の企業構成を管理します。インストール後に組織を追加作成して、企業を個別に管理できます。作成した組織はすべて、最上位レベルの組織の下に入ります。

▼ 組織を作成する

1 「ディレクトリ管理」タブをクリックします。

2 「組織」リストで、「新規」をクリックします。

3 フィールドの値を入力します。「名前」だけが必須です。フィールドは次のとおりです。

「名前」 組織の名前の値を入力します。

「ドメイン名」 ドメインネームシステム (DNS) を使用している場合は、DNS の完全な名前を入力します。

「組織の状態」 「アクティブ」または「非アクティブ」の状態を選択します。デフォルトは「アクティブ」です。これは、その組織の存続期間中であればいつでも、「プロパティー」アイコンを選択して変更できます。「非アクティブ」を選択すると、その組織にログインした場合、ユーザーアクセスが無効になります。

「組織のエイリアス」 このフィールドでは、組織のエイリアス名を指定します。URL ログインで、認証にエイリアスを使用できるようになります。たとえば `exampleorg` という組織があり、エイリアスとして `123` および `abc` を指定すると、次の URL を使用して組織にログインできます。

```
http://machine.example.com/amserver/UI/Login?
org=exampleorg

http://machine.example.com/amserver/UI/Login?org=abc

http://machine.example.com/amserver/UI/Login?org=123
```

組織のエイリアス名は、組織全体で一意でなければなりません。「一意の属性リスト」を使用して一意性を実現できます。

「DNS エイリアス名」 組織の DNS 名にエイリアス名を追加できます。この属性では、実際のドメインエイリアスだけを使用できます。ランダ

ムな文字列は使用できません。たとえばexample.comというDNSがあり、exampleorgという組織のエイリアスとしてexample1.comおよびexample2.comを指定すると、次のURLを使用して組織にログインできます。

```
http://machine.example.com/amserver/UI/

Login?org=exampleorg

http://machine.example1.com/amserver/

UI/Login?org=exampleorg

http://machine.example2.com/amserver/

UI/Login?org=exampleorg
```

「一意の属性リスト」　組織内のユーザー用に一意の属性名リストを追加できます。たとえば、電子メールアドレスを示す属性値を一意の属性リストに追加した場合、同一の電子メールアドレスを持つ2人のユーザーを作成することができなくなります。このフィールドには、コンマ区切りのリストも指定できます。リスト内の属性名は、どれも一意性を定義します。たとえば、このフィールドに次の属性名リストが指定されたとします。

```
PreferredDomain, AssociatedDomain
```

また、特定のユーザーに対して、PreferredDomainは`http://www.example.com`と定義されています。この場合、コンマ区切りのリスト全体が、そのURLに関して一意であると定義されます。「一意の属性リスト」にネーミング属性「ou」を追加しても、デフォルトのgroups、peopleコンテナでは一意性は要求されません。(ou=Groups、ou=People)。

すべてのサブ組織で一意性が要求されます。

4 「了解」をクリックします。

新しい組織が「組織」リストに表示されます。組織の作成時に定義したプロパティーを編集するには、編集対象の組織の名前をクリックし、プロパティーを変更して「保存」をクリックします。

▼ 組織を削除する

1 削除する組織名の横にあるチェックボックスを選択します。

2 「削除」をクリックします。

注 – 削除を実行するときに警告メッセージは表示されません。組織内のエントリがすべて削除されます。この操作を元に戻すことはできません。

ポリシーに組織を追加する

Access Manager オブジェクトは、ポリシーの対象定義を通じてポリシーに追加されます。ポリシーを作成または修正するときに、組織、ロール、グループ、ユーザーを対象として定義できます。対象を定義すると、ポリシーがオブジェクトに適用されます。詳細は、153 ページの「ポリシーの管理」を参照してください。

コンテナ

コンテナエントリは、オブジェクトクラスおよび属性が異なるために組織エントリが使用できない場合に使用します。Access Manager コンテナエントリと Access Manager 組織エントリは、必ずしも LDAP オブジェクトクラス `organizationalUnit` および `organization` と同等とはかぎらないことに留意してください。これらは抽象アイデンティティーエントリです。可能であれば、コンテナエントリではなく組織エントリを使用します。

注 – コンテナの表示は必要に応じて行います。コンテナを表示するには、「設定」>「コンソールプロパティー」の「管理」サービスでコンテナを表示するようにオプションを選択します。

▼ コンテナを作成する

1. 新しいコンテナを作成する組織またはコンテナのリンクを選択します。
2. 「コンテナ」タブをクリックします。
3. 「コンテナ」リストで「新規」をクリックします。
4. 作成するコンテナの名前を入力します。
5. 「了解」をクリックします。

▼ コンテナを削除する

1. 「コンテナ」タブをクリックします。
2. 削除するコンテナ名の横にあるチェックボックスを選択します。

3 「削除」をクリックします。

注 – コンテナを削除すると、そのコンテナに含まれるオブジェクトがすべて削除されます。すべてのオブジェクトとサブコンテナが対象になります。

グループコンテナ

グループコンテナを使用してグループを管理します。グループコンテナにはグループとほかのグループコンテナだけを含めることができます。グループコンテナの「グループ」は、すべての管理されているグループの親エントリとして動的に割り当てられます。必要に応じて、グループコンテナを追加することができます。

注 – グループコンテナの表示は必要に応じて行います。グループコンテナを表示するには、「設定」>「コンソールプロパティー」の「管理」サービスでグループコンテナを有効にするようにオプションを選択します。

▼ グループコンテナを作成する

1 新しいグループコンテナを追加する組織またはグループコンテナのリンクを選択します。

2 「グループコンテナ」タブを選択します。

3 「グループコンテナ」リストで「新規」をクリックします。

4 「名前」フィールドに値を入力して、「了解」をクリックします。「グループコンテナ」リストに新しいグループコンテナが表示されます。

▼ グループコンテナを削除する

1 削除対象のグループコンテナを含む組織に移動します。

2 「グループコンテナ」タブを選択します。

3 削除するグループコンテナの横にあるチェックボックスを選択します。

4 「削除」をクリックします。

グループ

グループは、共通の機能、特徴、または関心事を持つユーザーの集まりを表します。通常、このグループには関連付けられた権限はありません。グループは、組織内および管理されているほかのグループ内という、2 つのレベルに存在できます。ほかのグループ内に存在するグループは、サブグループと呼ばれます。サブグループは、親グループ内に「物理的に」存在する子ノードです。

Access Manager は、入れ子グループもサポートします。入れ子グループは、1 つのグループに含まれる既存のグループを表します。サブグループとは対照的に、入れ子グループは DIT 内のどこにでも存在できます。入れ子グループは、多数のユーザーに対するアクセス権の設定を簡単にします。

作成できるグループには、静的グループと動的グループの 2 種類があります。ユーザーを手動で追加できるのは静的グループのみです。動的グループでは、フィルタによってユーザーの追加が制御されます。入れ子グループまたはサブグループは、両方に追加できます。

静的グループ

静的グループは、指定した管理されているグループタイプに基づいて作成されます。グループメンバーは、`groupOfNames` または `groupOfUniqueNames` オブジェクトクラスを使用してグループエントリに追加されます。

注 – 管理されているグループタイプのデフォルトは dynamic です。このデフォルトは、管理サービス設定で変更できます。

動的グループ

動的グループは、LDAP フィルタを使用して作成されます。エントリはすべてフィルタを通してまとめられ、グループに動的に割り当てられます。フィルタはエントリの属性を検索して、その属性を含むエントリを返します。たとえば、建物番号に基づいてグループを作成する場合、フィルタを使用すると建物番号属性を含むすべてのユーザーのリストを返します。

注 – Access Manager は、Directory Server とともに参照整合性プラグインを使用するように設定されている必要があります。参照整合性プラグインが有効になっているときは、削除操作や名前の変更操作の直後に、指定された属性について整合性更新が実行されます。これにより、関連するエントリどうしの関係がデータベース全体で維持されます。Directory Server では、データベースインデックスによって検索パフォーマンスが向上します。このプラグインを有効にする方法の詳細は、『Sun Java System Access Manager 6 2005Q1 Migration Guide』を参照してください。

▼ 静的グループを作成する

1 新しいグループを作成する組織、グループ、またはグループコンテナに移動します。

2 「グループ」リストから「新規静的」をクリックします。

3 「グループ名」フィールドにグループの名前を入力します。「次へ」をクリックします。

4 「ユーザーのグループ加入を有効」属性を選択すると、ユーザーが自分でそのグループに加入できるようになります。

5 「了解」をクリックします。
グループの作成後、グループの名前を選択して「一般」をクリックすることにより、「ユーザーのグループ加入を有効」属性を編集できます。

▼ 静的グループのメンバーを追加または削除する

1 「グループ」リストから、メンバーを追加するグループを選択します。

2 「アクションの選択」メニューで実行するアクションを選択します。実行できるアクションは次のとおりです。

「新規ユーザー」 このアクションでは、新規ユーザーが作成され、ユーザー情報の保存時にユーザーがグループに追加されます。

「ユーザーの追加」 このアクションでは、既存のユーザーがグループに追加されます。このアクションを選択する場合は、追加するユーザーを指定する検索条件を作成します。条件の作成に使用するフィールドでは、「いずれか」または「すべて」演算子を使用します。「すべて」は、指定したすべてのフィールドに一致するユーザーを返します。「いずれか」は、指定したいずれか 1 つのフィールドに一致するユーザーを返します。フィールドを空白のままにすると、そのフィールドの属性に関しては条件を指定しなかったとみなされます。

検索条件を作成したら、「次へ」をクリックします。返されたユーザーのリストから、追加するユーザーを選択し、「終了」をクリックします。

「グループを追加」 このアクションでは、入れ子グループが現在のグループに追加されます。このアクションを選択すると、検索範囲、グループの名前 ("*" ワイルドカードを使用可能) を含む検索条件を作成し、ユーザーが自分でグループに加入できるかどうかを指定で

きます。情報を入力したら、「次へ」をクリックします。返されたグループのリストから、追加するグループを選択し、「終了」をクリックします。

「メンバーを消去」　このアクションでは、グループからメンバー (ユーザーとグループを含む) が消去されますが、メンバー自身の削除はされません。消去するメンバーを選択し、「アクションの選択」メニューから「メンバーを消去」を選択します。

「メンバーを削除」　このアクションでは、選択されたメンバー自身のエントリーが Directory Server から物理的に削除されます。削除するメンバーを選択し、「メンバーを削除」を選択します。

▼ 動的グループを作成する

1 新しいグループを作成する組織またはグループに移動します。

2 「グループ」タブをクリックします。

3 「新規動的」をクリックします。

4 「グループ名」フィールドにグループの名前を入力します。

5 **LDAP** 検索フィルタを作成します。

デフォルトでは、Access Manager は基本検索フィルタインタフェースを表示します。フィルタの作成に使用する基本フィールドでは、「いずれか」または「すべて」演算子を使用します。「すべて」は、指定したすべてのフィールドに一致するユーザーを返します。「いずれか」は、指定したいずれか 1 つのフィールドに一致するユーザーを返します。フィールドを空白のままにすると、そのフィールドの属性に関しては条件を指定しなかったとみなされます。

6 「了解」をクリックすると、検索条件に一致するすべてのユーザーが自動的にグループに追加されます。

▼ 動的グループのメンバーを追加または削除する

1 「グループ」リストで、メンバーを追加するグループの名前をクリックします。

2 「アクションの選択」メニューで実行するアクションを選択します。実行できるアクションは次のとおりです。

「グループを追加」　このアクションでは、入れ子グループが現在のグループに追加されます。このアクションを選択すると、検索範囲、グループの名前 ("*" ワイルドカードを使用可能) を含む検索条件を作成し、ユーザーが自分でグループに加入できるかどうかを指定で

きます。情報を入力したら、「次へ」をクリックします。返されたグループのリストから、追加するグループを選択し、「終了」をクリックします。

「メンバーを消去」　このアクションでは、グループからメンバー (グループを含む) が消去されますが、メンバー自身の削除はされません。消去するメンバーを選択し、「メンバーを消去」を選択します。

「メンバーを削除」　このアクションでは、選択されたメンバー自身のエントリーが Directory Server から物理的に削除されます。削除するメンバーを選択し、「メンバーを削除」を選択します。

ポリシーにグループを追加する

Access Manager オブジェクトは、ポリシーの対象定義を通じてポリシーに追加されます。ポリシーを作成または修正するときに、ポリシーの「対象」ページで、組織、ロール、グループ、ユーザーを対象として定義できます。対象を定義すると、ポリシーがオブジェクトに適用されます。詳細は、153 ページの「ポリシーの管理」を参照してください。

ピープルコンテナ

ピープルコンテナはデフォルトの LDAP 組織単位です。ユーザーはすべて、組織内で作成されるときにその組織単位に割り当てられます。ピープルコンテナは組織レベルで、あるいはサブピープルコンテナとしてピープルコンテナレベルで表示されます。ピープルコンテナにはほかのピープルコンテナとユーザーだけを含めることができます。必要に応じて、ピープルコンテナを組織に追加することができます。

注 – ピープルコンテナの表示は必要に応じて行います。ピープルコンテナを表示するには、管理サービスで「ピープルコンテナを有効」を選択します

▼ ピープルコンテナを作成する

1. ピープルコンテナを作成する組織またはピープルコンテナに移動します。
2. 「ピープルコンテナ」リストで「新規」をクリックします。
3. 作成するピープルコンテナの名前を入力します。
4. 「了解」をクリックします。

▼ ピープルコンテナを削除する

1 削除対象のピープルコンテナを含む組織またはピープルコンテナに移動します。

2 削除するピープルコンテナ名の横にあるチェックボックスを選択します。

3 「削除」をクリックします。

注 – ピープルコンテナを削除すると、そのピープルコンテナに含まれるオブジェクトがすべて削除されます。すべてのユーザーとサブピープルコンテナが対象になります。

ユーザー

ユーザーは、個人のアイデンティティーを表します。Access Manager のアイデンティティー管理モジュールを使用して、組織、コンテナ、およびグループに対するユーザーの作成と削除、ロールやグループに対するユーザーの追加と削除が可能です。サービスをユーザーに割り当てることもできます。

注 – `amadmin` と同じユーザー ID でサブ組織のユーザーを作成すると、`amadmin` のログインが失敗します。このような問題が起こったら、管理者はディレクトリサーバーコンソールを使って、そのユーザーの ID を変更する必要があります。これで、管理者がデフォルトの組織にログインできるようになります。さらに、認証サービスの「ユーザー検索の開始 DN」をピープルコンテナ DN に設定し、ログイン処理で一意のユーザーが特定できます。

▼ ユーザーを作成する

1 ユーザーを作成する組織、コンテナ、またはピープルコンテナに移動します。

2 「ユーザー」タブをクリックします。

3 「ユーザー」リストで「新規」をクリックします。

4 次の値のデータを入力します。

「ユーザー ID」	このフィールドは、ユーザーが Access Manager へログインするために使用する名前を取得します。このプロパティーは、DN 以外の値になることがあります。
「名」	このフィールドには、ユーザーの名 (ファーストネーム) を指定します。名 (ファーストネーム) の値と姓 (ラストネーム) の

	値によって、「現在ログイン中」フィールドのユーザーが識別されます。これは必須の値ではありません。
「姓」	このフィールドはユーザーの姓 (ラストネーム) を取得します。名 (ファーストネーム) の値と姓 (ラストネーム) の値によってユーザーが識別されます。
「フルネーム」	このフィールドはユーザーのフルネームを取得します。
「パスワード」	このフィールドには、ユーザーのパスワードを入力します。
「パスワード (確認)」	パスワードを確認します。
「ユーザー状態」	このオプションは、Access Manager による認証をユーザーに許可するかどうかを指定します。アクティブなユーザーだけが認証を受けることができます。デフォルト値は「アクティブ」です。

5 「了解」をクリックします。

▼ ユーザープロファイルを編集する

管理者ロールを割り当てられていないユーザーが Access Manager に認証されると、そのユーザーのユーザープロファイルがデフォルトの表示になります。また、適切な権限を持つ管理者はユーザープロファイルを編集できます。この表示では、ユーザーが各自の個人プロファイルに特有の属性値を編集できます。ユーザープロファイルビューに表示された属性は、展開することができます。オブジェクトおよびアイデンティティーのためにカスタマイズされた属性の追加については、『Access Manager Developer's Guide』を参照してください。

1 プロファイルが編集されるユーザーを選択します。デフォルトでは、「一般」表示となっています。

2 次のフィールドを編集します。

「名」
このフィールドには、ユーザーの名 (ファーストネーム) を指定します。

「姓」
このフィールドはユーザーの姓 (ラストネーム) を取得します。

「フルネーム」
このフィールドはユーザーのフルネームを取得します。

「パスワード」
「編集」リンクをクリックして、ユーザーのパスワードを追加し、確認します。

「電子メールアドレス」
このフィールドで、ユーザーの電子メールアドレスを指定します。

「社員番号」
このフィールドで、ユーザーの社員番号を指定します。

「電話番号」
このフィールドで、ユーザーの電話番号を指定します。

「ホームアドレス」
このフィールドで、ユーザーのホームアドレスを指定します。

「ユーザー状態」
このオプションは、Access Managerによる認証をユーザーに許可するかどうかを指定します。アクティブなユーザーだけがAccess Managerを使用して認証を受けることができます。デフォルト値は「アクティブ」です。プルダウンメニューから次のどちらかを選択することができます。

- 「アクティブ」— ユーザーはAccess Managerを使用して認証を受けることができます。
- 「非アクティブ」— ユーザーはAccess Managerを使用して認証を受けることはできませんが、ユーザープロファイルはそのままディレクトリに格納されます。

注 – ユーザー状態を「非アクティブ」に変えても、Access Managerによる認証に影響するだけです。Directory Serverは、*nsAccountLock*属性を使用してユーザーアカウント状態を判別しますが、Access Managerでの「ユーザー状態」の設定は、*nsAccountLock*属性には影響しません。Access Managerにて、ユーザー状態を「非アクティブ」にしたユーザーアカウントでも、Access Managerを必要としないタスクは実行できます。Access Manager認証だけではなく、ディレクトリのユーザーアカウントも無効にするには、*nsAccountLock*の値を「false」に設定します。サイトの委託管理者がユーザーを定期的に無効にしている場合は、*nsAccountLock*属性をAccess Managerのユーザープロファイルページに追加することを検討してください。詳細は、『Sun Java System Access Manager 7 2005Q4 Developer's Guide』を参照してください。

「アカウント有効期限」
この属性が存在し、その値が現在の日時以前であれば、認証サービスはログインを無効にします。この属性の形式は次のとおりです。*mm/dd/yyyy hh:mm*

「ユーザー認証設定」
この属性は、ユーザーの認証連鎖を設定します。

「ユーザーエイリアスリスト」
このフィールドは、ユーザーに適用される可能性のあるエイリアスを定義します。この属性に設定されたエイリアスを使用するために、`iplanet-am-user-alias-list`属性をLDAPサービスのユーザーエントリ検索属性フィールドに追加して、LDAPサービスを修正する必要があります。

「設定ロケール」
このフィールドは、ユーザーのロケールを指定します。

「成功 URL」
この属性は、認証が成功した場合にユーザーをリダイレクトする URL を指定します。

「失敗 URL」
この属性は、認証が失敗した場合にユーザーをリダイレクトする URL を指定します。

「パスワードリセットオプション」
ここでは、パスワードを忘れた場合に使用する質問を選択します。パスワードを忘れたときは、選択した質問に答えることで、パスワードを回復できます。

「ユーザーディスカバリのリソースオファリング」
ユーザーの、ユーザーディスカバリサービスのリソースオファリングを設定します。

「MSISDN 番号」
MSISDN 認証を使用している場合に、ユーザーの MSISDN 番号を定義します。

▼ ロールおよびグループにユーザーを追加する

1. 「ユーザー」タブをクリックします。
2. 変更するユーザーの名前をクリックします。
3. 「ロール」タブまたは「グループ」タブを選択します。
4. ユーザーを追加するロールまたはグループを選択し、「追加」をクリックします。
5. 「保存」をクリックします。

注 – ロールまたはグループからユーザーを削除するには、ロールまたはグループを選択し、「削除」をクリックして「保存」をクリックします。

ポリシーにユーザーを追加する

Access Manager オブジェクトは、ポリシーの対象定義を通じてポリシーに追加されます。ポリシーを作成または修正するときに、ポリシーの「対象」ページで、組織、ロール、グループ、ユーザーを対象として定義できます。対象を定義すると、ポリシーがオブジェクトに適用されます。詳細は、153 ページの「ポリシーの管理」を参照してください。

ロール

ロールとは、グループの概念に似た、Directory Server の 1 つのエントリメカニズムです。グループにはメンバーがあるように、ロールにもメンバーがあります。ロールのメンバーは、ロールを持つ LDAP エントリです。ロール自体の基準は、属性を持つ LDAP エン

トリとして定義されます。このエントリは、エントリの識別名 (DN) 属性で特定されます。Directory Server にはさまざまなタイプのロールがありますが、Access Manager で管理できるのは、管理ロールだけです。

注 – そのほかの Directory Server ロールタイプもディレクトリの配備で使用できますが、Access Manager コンソールで管理することはできません。ポリシーの対象定義にほかの Directory Server タイプを使用することもできます。ポリシー対象については、150 ページの「ポリシーの作成」を参照してください。

ユーザーには 1 つ以上のロールを持たせることができます。たとえば、セッションサービスとパスワードリセットサービスの属性を持つ契約社員ロールを作成できます。新しい契約社員が入社したときに、管理者は契約社員エントリの別の属性を設定しなくても、契約社員にこのロールを割り当てることができます。契約社員がエンジニアリング部門に属し、エンジニアリング社員に適用可能なサービスとアクセス権が必要な場合は、管理者は契約社員にエンジニアリングロールおよび契約社員ロールを割り当てることができます。

Access Manager では、ロールを使用して、アクセス制御の命令を適用します。Access Manager をはじめてインストールしたときに、管理者アクセス権を定義するアクセス制御命令 (ACI) が定義されます。次にこれらの ACI をロール (組織管理者ロール、組織ヘルプデスク管理者ロールなど) に割り当てます。このロールをユーザーに割り当てると、ユーザーのアクセス権が定義されます。

ユーザーは、管理サービスで「ユーザープロファイルページにロールを表示」属性が有効である場合だけ、割り当てられたロールを確認できます。

注 – Access Manager は、Directory Server とともに参照整合性プラグインを使用するように設定されている必要があります。参照整合性プラグインが有効になっているときは、削除操作や名前の変更操作の直後に、指定された属性について整合性更新が実行されます。これにより、関連するエントリどうしの関係がデータベース全体で維持されます。Directory Server では、データベースインデックスによって検索パフォーマンスが向上します。このプラグインを有効にする方法の詳細は、『Sun Java System Access Manager 6 2005Q1 Migration Guide』を参照してください。

ロールには、次の 2 種類があります。

- 静的ロール — 静的ロールは、ロールの作成時にユーザーを追加せずに作成されます。ロールを作成したあとで、特定のユーザーをそのロールに追加できます。これにより、ユーザーを指定されたロールに追加するときにより細かく制御できます。
- 動的ロール – 動的ロールは、LDAP フィルタを使用して作成されます。ユーザーはすべてフィルタを通してまとめられ、ロールの作成時にそのロールに割り当てられます。フィルタはエントリの属性と値のペア (`ca=user*` など) を検索して、その属性を含むユーザーをロールに自動的に割り当てます。

▼ 静的ロールを作成する

1 ロールを作成する組織に移動します。

2 「ロール」タブをクリックします。

組織の設定時にデフォルトのロールが作成され、「ロール」リストに表示されます。デフォルトのロールは次のとおりです。

コンテナヘルプデスク管理者: コンテナのヘルプデスク管理者ロールは、組織単位のすべてのエントリに対する読み取りアクセス権、およびそのコンテナ単位だけにあるユーザーエントリの `userPassword` 属性に対する書き込みアクセス権を持っています。

組織ヘルプデスク管理者: 組織ヘルプデスク管理者は、組織のすべてのエントリに対する読み取りアクセス権、および `userPassword` 属性に対する書き込みアクセス権を持っています。

注 – サブ組織を作成するときは、管理者ロールは親組織ではなくサブ組織に作成してください。

コンテナ管理者: コンテナ管理者ロールは、LDAP 組織単位のすべてのエントリに対する読み取りアクセス権と書き込みアクセス権を持っています。Access Manager では、LDAP 組織単位をコンテナと呼ぶことがあります。

組織ポリシー管理者: 組織ポリシー管理者は、組織のすべてのポリシーに対する読み取りアクセス権と書き込みアクセス権を持っており、組織内のすべてのポリシーについて作成、割り当て、修正、および削除ができます。

ピープル管理者 デフォルトで、新規に作成した組織のユーザーエントリはその組織のメンバーです。ピープル管理者は、組織のすべてのユーザーエントリに対する読み取りアクセス権と書き込みアクセス権を持っています。なお、このロールは、ロールおよびグループ DN を含む属性に対する読み取りアクセス権と書き込みアクセス権を持っていないため、ロールまたはグループの属性を変更したり、ロールまたはグループからユーザーを消去したりすることができません。

注 – ほかのコンテナは、Access Manager とともに設定して、ユーザーエントリ、グループエントリ、またはほかのコンテナを保持することができます。組織を構成したあとで、作成されたコンテナに管理者ロールを適用するには、デフォルトのコンテナ管理者ロールまたはコンテナヘルプデスク管理者を使用します。

グループ管理者: グループ作成時に作成されたグループ管理者は、特定グループのすべてのメンバーに対する読み取りアクセス権および書き込みアクセス権を持っており、新しいユーザーの作成、管理しているグループへのユーザーの割り当て、および作成したユーザーの削除を行うことができます。

グループを作成すると、そのグループを管理するのに必要な権限を持つグループ管理者ロールが自動的に作成されます。このロールはグループのメンバーに自動的には割り当てられません。グループの作成者、またはグループ管理者ロールへのアクセス権を持つ人が割り当てる必要があります。

最上位レベル管理者: 最上位レベル管理者は、最上位レベル組織のすべてのエントリに対する読み取りアクセス権と書き込みアクセス権を持っています。言い換えれば、最上位レベル管理者ロールには、Access Manager アプリケーション内のすべての設定主体に対する権限があります。

組織管理者: 組織管理者は、組織のすべてのエントリに対する読み取りアクセス権と書き込みアクセス権を持っています。組織を作成すると、その組織を管理するのに必要な権限を持つ組織管理者ロールが自動的に作成されます。

3 「新規静的」ボタンをクリックします。

4 ロールの名前を入力します。

5 ロールの詳細を入力します。

6 「タイプ」メニューからロールのタイプを選択します。

ロールは、管理者ロールまたはサービスロールにすることができます。ロールのタイプは、Access Manager コンソールが、コンソール内でどのユーザーをどの位置から始動させるかを決定するために使用します。管理者ロールは、ロールの所有者が管理者権限を持っていることをコンソールに通知します。サービスロールは、その所有者がエンドユーザーであることをコンソールに通知します。

7 「アクセス権」メニューから、ロールに適用する権限のデフォルトセットを選択します。これは、組織内のエントリにアクセスする権限です。ここで示すデフォルトの権限は順不同です。権限は次のとおりです。

アクセス権なし	ロールにアクセス権が設定されません。
組織管理者	組織管理者は設定済み組織のすべてのエントリに対する読み取りアクセス権と書き込みアクセス権を持っています。
組織ヘルプデスク管理者	組織ヘルプデスク管理者は、設定済み組織のすべてのエントリに対する読み取りアクセス権、および `userPassword` 属性に対する書き込みアクセス権を持っています。
組織ポリシー管理者	組織ポリシー管理者は、組織のすべてのポリシーに対する読み取りアクセス権と書き込みアクセス権を持っています。組織ポリシー管理者は、ピア組織に対する参照ポリシーを作成できません。 一般に、「アクセス権なし」ACI をサービスロールに割り当て、管理者ロールにはデフォルト ACI のいずれかを割り当てます。

▼ 静的ロールにユーザーを追加する

1 ユーザーを追加するロールの名前をクリックします。

2 「メンバー」リストで、「アクションの選択」メニューから「ユーザーの追加」を選択します。

3 検索条件を入力します。表示される1つ以上のフィールドを基に、ユーザーの検索方法を選択できます。フィールドは次のとおりです。

「一致」	フィルタ用として含めるフィールドを選択できます。「すべて」は、指定したすべてのフィールドに一致するユーザーを返します。「いずれか」は、指定したいずれか1つのフィールドに一致するユーザーを返します。
「名」	名 (ファーストネーム) でユーザーを検索します。
「ユーザー ID」	ユーザー ID でユーザーを検索します。
「姓」	姓 (ラストネーム) でユーザーを検索します。
「フルネーム」	フルネームでユーザーを検索します。
「ユーザー状態」	ユーザーの状態 (アクティブまたは非アクティブ) でユーザーを検索します。

4 「次へ」をクリックすると、検索が始まります。検索結果が表示されます。

5 ユーザー名の横にあるチェックボックスを選択して、返された名前の中からユーザーを選択します。

6 「終了」をクリックします。
これで、ユーザーがロールに割り当てられます。

▼ 動的ロールを作成する

1 ロールを作成する組織に移動します。

2 「ロール」タブをクリックします。
組織の設定時にデフォルトのロールが作成され、「ロール」リストに表示されます。デフォルトのロールは次のとおりです。

コンテナヘルプデスク管理者: コンテナのヘルプデスク管理者ロールは、組織単位のすべてのエントリに対する読み取りアクセス権、およびそのコンテナ単位だけにあるユーザーエントリの `userPassword` 属性に対する書き込みアクセス権を持っています。

組織ヘルプデスク管理者: 組織ヘルプデスク管理者は、組織のすべてのエントリに対する読み取りアクセス権、および userPassword 属性に対する書き込みアクセス権を持っています。

注 – サブ組織を作成するときは、管理者ロールは親組織ではなくサブ組織に作成してください。

コンテナ管理者: コンテナ管理者ロールは、LDAP 組織単位のすべてのエントリに対する読み取りアクセス権と書き込みアクセス権を持っています。Access Manager では、LDAP 組織単位をコンテナと呼ぶことがあります。

組織ポリシー管理者: 組織ポリシー管理者は、組織のすべてのポリシーに対する読み取りアクセス権と書き込みアクセス権を持っており、組織内のすべてのポリシーについて作成、割り当て、修正、および削除ができます。

ピープル管理者 デフォルトで、新規に作成した組織のユーザーエントリはその組織のメンバーです。ピープル管理者は、組織のすべてのユーザーエントリに対する読み取りアクセス権と書き込みアクセス権を持っています。なお、このロールは、ロールおよびグループ DN を含む属性に対する読み取りアクセス権と書き込みアクセス権を持っていないため、ロールまたはグループの属性を変更したり、ロールまたはグループからユーザーを消去したりすることができません。

注 – ほかのコンテナは、Access Manager とともに設定して、ユーザーエントリ、グループエントリ、またはほかのコンテナを保持することができます。組織を構成したあとで、作成されたコンテナに管理者ロールを適用するには、デフォルトのコンテナ管理者ロールまたはコンテナヘルプデスク管理者を使用します。

グループ管理者: グループ作成時に作成されたグループ管理者は、特定グループのすべてのメンバーに対する読み取りアクセス権および書き込みアクセス権を持っており、新しいユーザーの作成、管理しているグループへのユーザーの割り当て、および作成したユーザーの削除を行うことができます。

グループを作成すると、そのグループを管理するのに必要な権限を持つグループ管理者ロールが自動的に作成されます。このロールはグループのメンバーに自動的には割り当てられません。グループの作成者、またはグループ管理者ロールへのアクセス権を持つ人が割り当てる必要があります。

最上位レベル管理者: 最上位レベル管理者は、最上位レベル組織のすべてのエントリに対する読み取りアクセス権と書き込みアクセス権を持っています。言い換えれば、最上位レベル管理者ロールには、Access Manager アプリケーション内のすべての設定主体に対する権限があります。

組織管理者: 組織管理者は、組織のすべてのエントリに対する読み取りアクセス権と書き込みアクセス権を持っています。組織を作成すると、その組織を管理するのに必要な権限を持つ組織管理者ロールが自動的に作成されます。

3 「新規動的」ボタンをクリックします。

4 ロールの名前を入力します。

5 ロールの詳細を入力します。

6 「タイプ」メニューからロールのタイプを選択します。

ロールは、管理者ロールまたはサービスロールにすることができます。ロールのタイプは、Access Manager コンソール内でどのユーザーをどの位置から始動させるかを決定するために使用します。管理者ロールは、ロールの所有者が管理者権限を持っていることをコンソールに通知します。サービスロールは、その所有者がエンドユーザーであることをコンソールに通知します。

7 「アクセス権」メニューから、ロールに適用する権限のデフォルトセットを選択します。これは、組織内のエントリにアクセスする権限です。ここで示すデフォルトの権限は順不同です。権限は次のとおりです。

アクセス権なし	ロールにアクセス権が設定されません。
組織管理者	組織管理者は設定済み組織のすべてのエントリに対する読み取りアクセス権と書き込みアクセス権を持っています。
組織ヘルプデスク管理者	組織ヘルプデスク管理者は、設定済み組織のすべてのエントリに対する読み取りアクセス権、および `userPassword` 属性に対する書き込みアクセス権を持っています。
組織ポリシー管理者	組織ポリシー管理者は、組織のすべてのポリシーに対する読み取りアクセス権と書き込みアクセス権を持っています。組織ポリシー管理者は、ピア組織に対する参照ポリシーを作成できません。 一般に、「アクセス権なし」ACI をサービスロールに割り当て、管理者ロールにはデフォルト ACI のいずれかを割り当てます。

8 検索条件を入力します。フィールドは次のとおりです。

「一致」	演算子を含めるフィルタのフィールドに、演算子を含めることができます。「すべて」は、指定したすべてのフィールドに一致するユーザーを返します。「いずれか」は、指定したいずれか 1 つのフィールドに一致するユーザーを返します。
「名」	名 (ファーストネーム) でユーザーを検索します。
「ユーザー ID」	ユーザー ID でユーザーを検索します。
「姓」	姓 (ラストネーム) でユーザーを検索します。
「フルネーム」	フルネームでユーザーを検索します。

「ユーザー状態」　ユーザーの状態 (アクティブまたは非アクティブ) でユーザーを検索します。

9 「了解」をクリックして、フィルタ条件を基に、検索を開始します。そのフィルタ条件で定義されたユーザーがロールに自動的に割り当てられます。

▼ ロールからユーザーを消去する

1 変更するロールを含む組織に移動します。
アイデンティティー管理モジュールで「表示」メニューから「組織」を選択し、「ロール」タブを選択します。

2 変更するロールを選択します。

3 「表示」メニューから「ユーザー」を選択します。

4 消去する各ユーザーの横にあるチェックボックスを選択します。

5 「アクションの選択」メニューから「ユーザーの消去」をクリックします。
これで、ロールからユーザーが消去されます。

ポリシーにロールを追加する

Access Manager オブジェクトは、ポリシーの対象定義を通じてポリシーに追加されます。ポリシーを作成または修正するときに、ポリシーの「対象」ページで、組織、ロール、グループ、ユーザーを対象として定義できます。対象を定義すると、ポリシーがオブジェクトに適用されます。詳細は、153 ページの「ポリシーの管理」を参照してください。

◆ ◆ ◆ 第 11 章

11 現在のセッション

この章では、Access Manager のセッション管理機能について説明します。セッション管理モジュールでは、ユーザーセッションの情報を確認したり、ユーザーセッションを管理したりする手段を用意しています。さまざまなセッションの時間を追跡するほかに、管理者がセッションを終了することができます。システム管理者は、プラットフォームサーバーリストに表示されたロードバランササーバーを無視してください。

現在のセッションのインタフェース

「現在のセッション」モジュールインタフェースを使用すると、適切な権限を持った管理者は、Access Manager にログインしている任意のユーザーのセッション情報を参照できます。

セッション管理

セッション管理フレームには、現在管理されている Access Manager の名前が表示されます。

セッション情報

セッション情報ウィンドウには、Access Manager に現在ログイン中のすべてのユーザーと、各ユーザーのセッション時間が表示されます。表示フィールドは次のとおりです。

「ユーザー **ID**」: 現在ログイン中のユーザーのユーザー ID が表示されます。

「残り時間」: ユーザーの再認証までの、セッションの残り時間 (分単位) が表示されます。

「最大セッション時間」: ユーザーがログインした状態でいられる最大時間 (分単位) が表示されます。この時間が経過すると、セッションが期限切れになり、ユーザーはアクセスするために再度認証を受ける必要があります。

「アイドル時間」: ユーザーがアイドル状態になっている時間 (分単位) が表示されます。

「最大アイドル時間」: ユーザーの再認証が必要になるまでの残りの最大アイドル時間 (分単位) が表示されます。

時間の制限値は、管理者がセッション管理サービスに定義します。

「ユーザー ID」フィールドに入力して「フィルタ」をクリックすれば、特定のユーザーのセッションを表示できます。ワイルドカードも使用できます。

「更新」ボタンをクリックすれば、セッションの表示が更新されます。

セッションの終了

適切な権限を持った管理者は、ユーザーのセッションをいつでも終了させることができます。

▼ セッションを終了させる

1. 終了させるユーザーのセッションを選択します。
2. 「セッションを終了」をクリックします。

◆ ◆ ◆ 第 12 章

パスワードリセットサービス

Access Manager では、Access Manager によって保護されている特定のサービスやアプリケーションにアクセスするためのパスワードをユーザー自身がリセットできるように、パスワードリセットサービスが用意されています。パスワードリセットサービス属性は、最上位レベル管理者が定義します。この属性を使用して、ユーザーを検証するための証明情報 (秘密の質問形式) を制御し、新規または既存のパスワード通知の機構を制御し、不正なユーザーに適用するロックアウト間隔を設定します。

この章は、次の節で構成されています。

パスワードリセットサービスの登録

パスワードリセットサービスは、ユーザーが属しているレルムに対して登録する必要はありません。ユーザーが割り当てられている組織にパスワードリセットサービスが存在しない場合は、「サービス設定」の「パスワードリセットサービス」に定義されている値が継承されます。

▼ 別のレルムに存在するユーザーのパスワードリセットを登録する

1. そのユーザーのパスワードを登録するレルムに移動します。
2. レルム名をクリックし、「サービス」タブをクリックします。
   選択したレルムにレルム名が追加されていない場合は、「追加」ボタンをクリックします。

3 「パスワードリセット」を選択し、「次へ」をクリックします。
パスワードリセットサービス属性が表示されます。属性の定義については、オンラインヘルプを参照してください。

4 「終了」をクリックします。

パスワードリセットサービスの設定

パスワードリセットサービスの登録が完了したら、管理者権限を持っているユーザーがこのサービスを設定する必要があります。

▼ サービスを設定する

1 パスワードリセットサービスが登録されているレルムを選択します。

2 「サービス」タブをクリックします。

3 サービスリストから「パスワードリセット」をクリックします。

4 「パスワードリセット」属性が表示され、ここでパスワードリセットサービスの要件を定義できます。パスワードリセットサービスが有効になっていることを確認します (デフォルトでは有効)。少なくとも次の属性を定義する必要があります。

- ユーザー検証
  - 秘密の質問
  - バインド DN
  - バインドパスワード

    「バインド DN」属性には、パスワードをリセットする権限を持っているユーザー (ヘルプデスク管理者など) を指定する必要があります。Directory Server の制限により、バインド DN が `cn=Directory Manager` の場合はパスワードリセットは機能しません。

    残りの属性は省略可能です。これらのサービス属性の説明については、オンラインヘルプを参照してください。

注 – Access Manager では、ランダムなパスワードを生成するパスワードリセット Web アプリケーションが自動的にインストールされます。ただし、パスワードの生成や通知を行う独自のプラグインクラスを記述することもできます。このようなプラグインクラスのサンプルについては、次の場所にある Readme.html ファイルを参照してください。

PasswordGenerator:

```
AccessManager-base/SUNWam/samples/console/PasswordGenerator
```

NotifyPassword:

```
AccessManager-base/SUNWam/samples/console/NotifyPassword
```

5 独自の質問を定義するユーザーには、「個人的な質問を有効」属性を選択します。属性を定義し終えたら、「保存」をクリックします。

パスワードリセットのロックアウト

パスワードリセットサービスには、ユーザーが秘密の質問に正しく回答するまでの回数を制限するために、ロックアウト機能が用意されています。ロックアウト機能は、パスワードリセットサービス属性を使用して設定します。これらのサービス属性の説明については、オンラインヘルプを参照してください。パスワードリセットでは、メモリーロックアウトと物理的なロックアウトの 2 種類がサポートされています。

メモリーロックアウト

これは一時的なロックアウトです。「パスワードリセット失敗のロックアウト持続時間」属性の値が 0 より大きく、「パスワードリセット失敗のロックアウトを有効」属性が有効になっている場合にのみ機能します。ロックアウトされたユーザーは、パスワードリセット Web アプリケーションを使用してもパスワードをリセットできなくなります。「パスワードリセット失敗のロックアウト持続時間」に指定した時間が経過するまで、またはサーバーが再起動されるまで、ロックアウトは持続します。これらのサービス属性の説明については、オンラインヘルプを参照してください。

物理的なロックアウト

メモリーロックアウトより永続的なロックアウトです。「パスワードリセット失敗のロックアウトカウント」属性の値が 0 に設定され、「パスワードリセット失敗のロックアウトを有効」属性が有効になっている場合には、秘密の質問に正しく回答できなかったユーザーのアカウント状態が非アクティブに変更されます。これらのサービス属性の説明については、オンラインヘルプを参照してください。

エンドユーザーから見たパスワードリセット

以降の節では、ユーザーの観点からパスワードリセットサービスについて説明します。

パスワードリセットのカスタマイズ

管理者がパスワードリセットサービスを有効にし、属性を定義したら、ユーザーは Access Manager コンソールにログインして秘密の質問をカスタマイズできます。

▼ パスワードリセットをカスタマイズする

1. ユーザー名とパスワードを入力して認証に成功したら、**Access Manager** コンソールにログインします。
2. 「ユーザープロファイル」ページで、「パスワードリセットのオプション」を選択します。「質問と回答」画面が表示されます。
3. 管理者が定義した、このサービスで選択できる質問が表示されます。たとえば、次のような質問が表示されます。
   - ペットの名前は何でしょうか?
   - 好きなテレビ番組は何でしょうか?
   - 母親の旧姓は何でしょうか?
   - よく行くレストランの名前は何でしょうか?
4. 秘密の質問を選択します。管理者がこのレルムに定義した最大質問数 (パスワードリセットサービスに定義) まで選択できます。選択した質問への回答を指定します。これらの質問と回答を元に、自分でパスワードをリセットすることができます (次の節を参照)。管理者が「個人的な質問を有効」属性を選択している場合は、自分だけの秘密の質問と回答を入力できるように、テキストフィールドが表示されます。
5. 「保存」をクリックします。

パスワードを忘れた場合のリセット

パスワードを忘れた場合には、パスワードリセット Web アプリケーションによって新しいパスワードがランダムに生成され、それがユーザーに通知されます。パスワードを忘れた場合の標準的な手順を次に示します。

▼ パスワードを忘れた場合にリセットする

1 管理者から渡された **URL** を使って、パスワードリセット **Web** アプリケーションにログインします。次に例を示します。

`http://hostname:port /ampassword` (デフォルトのレルムの場合)

または

`http://hostname: port/`*deploy_uri* `/UI/PWResetUserValidation?realm=realmname`。realmname はレルムの名前です。

注 – パスワードリセットサービスがサブレルムで有効になっていても、親レルムで無効になっている場合は、次の構文を使ってサービスにアクセスする必要があります。

`http://hostname: port/`*deploy_uri*`/UI/PWResetUserValidation?realm=realmname`

---

2 ユーザー **ID** を入力します。

3 パスワードリセットサービスに定義されている質問のうち、パスワードリセット設定をカスタマイズした際にユーザーが選択した質問が表示されます。事前に「ユーザープロファイル」ページにログインしておらず、パスワードリセット設定をカスタマイズしていない場合には、パスワードは生成されません。

質問に正しく回答すると、新しいパスワードが生成され、電子メールで通知されます。また、回答が正しいかどうかにかかわらず、パスワードをリセットしようとしたことが通知されます。新しいパスワードおよびパスワードをリセットしようとしたことの通知を受け取るには、「ユーザープロファイル」ページに電子メールアドレスを入力しておく必要があります。

パスワードポリシー

安全なパスワードポリシーとして次のような条件をパスワードに適用すると、推測されやすいパスワードによるリスクを最小限に抑えることができます。

- ユーザーは定期的にパスワードを変更しなければならない。
- ユーザーは、容易に推測できないパスワードを指定しなければならない。
- 不正なパスワードを何度か使用すると、アカウントがロックされることがある。

Directory Server では、いくつかの方法により、ツリー内の任意のノードにパスワードポリシーを設定できます。詳細は、次の Directory Server のマニュアルを参照してください。

http://docs.sun.com/source/816-6700-10/aci.html#14773

http://docs.sun.com/source/816-6698-10/useracct.html#14386

◆ ◆ ◆ 第 13 章

ログサービス

Sun Java™ System Access Manager 7 2005Q4 には、ユーザーアクティビティー、トラフィックパターン、認証違反などの情報を記録するために、ログサービスが用意されています。また、管理者はデバッグファイルを利用して、インストールの障害追跡を行うことができます。

ログファイル

ログファイルには、ログサービスが監視するイベントが記録されます。管理者は、ログファイルを定期的に確認することをお勧めします。ログファイルのデフォルトのディレクトリは、SPARC システムの場合は `/var/opt/SUNWam/logs`、Linux システムの場合は `/var/opt/sun/identity` です。ログサービスのログファイルディレクトリを設定するときには、Access Manager コンソールを使用します。

ログファイルのデフォルトタイプ、記録される情報、ログファイルの形式の詳細については、『Sun Java System Access Manager 7 2005Q4 Technical Overview』の「How the Logging Feature Works」を参照してください。

ログサービスの属性定義については、Access Manager コンソールの「ヘルプ」ボタンをクリックしてオンラインヘルプを参照してください。

Access Manager サービスのログ

サービスログファイルには、アクセスログファイルとエラーログファイルの 2 種類があります。アクセスログファイルには、アクションが実行されたことと正常に実行されたアクションの結果が記録されます。エラーログファイルには、Access Manager サービスで発生したエラーが記録されます。フラットログファイルには、`.error` または `.access` という拡張子が付きます。データベース列名の最後には、Oracle データベースの場合は `_ERROR` または `_ACCESS`、MySQL データベースの場合は `_error` または `_access` が付きます。たとえば、コンソールイベントを記録するフラットファイルログには

amConsole.access という名前が付き、コンソールイベントを記録するデータベース列には AMCONSOLE_ACCESS という名前が付きます。以下の節では、ログサービスによって記録されるログファイルについて説明します。

セッションログ

ログサービスでは、次のセッションサービスイベントが記録されます。

- ログイン
- ログアウト
- セッションのアイドルタイムアウト
- 最大セッション数によるタイムアウト
- ログインの失敗
- セッションの再起動
- セッションの破棄

セッションログのファイル名は、amSSO で始まります。

コンソールログ

Access Manager コンソールログには、アイデンティティー関連のオブジェクト、ポリシー、およびサービスが作成、削除、および変更されたことが記録されます。たとえば、組織、組織単位、ユーザー、ロール、ポリシー、グループが記録されます。コンソールログには、パスワードなどのユーザー属性が変更されたことや、ロールとグループに対してユーザーが追加または削除されたことも記録されます。また、委託やデータストアのアクティビティーも記録されます。コンソールログのファイル名は、amConsole で始まります。

認証ログ

認証コンポーネントでは、ユーザーのログインおよびログアウトがログとして記録されます。認証ログのファイル名は、amAuthentication で始まります。

連携ログ

連携コンポーネントでは、連携関連のイベントなどがログとして記録されます。たとえば、認証ドメインが作成されたことや、ホストプロバイダが作成されたことが記録されます。連携ログのファイル名は、amFederation で始まります。

ポリシーログ

ポリシーコンポーネントでは、ポリシー関連のイベントなどがログとして記録されます。たとえば、ポリシー管理 (ポリシーの作成、削除、および変更) やポリシー評価が記録されます。ポリシーログのファイル名は、amPolicy で始まります。

エージェントログ

ポリシーエージェントログには、ユーザーがアクセスを許可または拒否されているログリソースに関する例外が記録されます。エージェントログのファイル名は、amAgent で始まります。amAgent ログは、エージェントサーバーだけに存在します。エージェントイベントのログは、Access Manager サーバー上の認証ログに記録されます。この機能の詳細については、ポリシーエージェントのマニュアルを参照してください。

SAML ログ

SAML コンポーネントでは、SAML 関連のイベントなどが記録されます。たとえば、表明およびアーティファクトが作成または削除されたこと、応答および要求の詳細、SOAP エラーなどが記録されます。SAML ログのファイル名は、amSAML で始まります。

amAdmin ログ

コマンド行ログには、コマンド行ツールを使用する操作中に発生したイベントエラーが記録されます。たとえば、サービススキーマがロードされたこと、ポリシーが作成されたこと、ユーザーが削除されたことなどが記録されます。コマンド行ログのファイル名は、amAdmin で始まります。

ログ機能

ログサービスにはいくつかの特殊な機能が用意されていて、追加機能として有効にできます。このような機能として、「セキュリティー保護されたログを有効」、「コマンド行ログ」、および「リモートログ」があります。

セキュリティー保護されたログ

このオプションの機能を追加すると、ログ機能のセキュリティーが強化されます。セキュリティー保護されたログを有効にすると、セキュリティーログに対する未承認の変更や改ざんを検出できます。この機能を使用するために、特にコーディングする必要はありません。セキュリティー保護されたログには、システム管理者が事前に登録した証明書が必要です。この MAC (Manifest Analysis and Certification) は、すべてのログレコード

について生成および格納されます。また、特別な「署名」ログレコードが定期的に挿入されます。このログレコードは、その時点までに書き込まれたログの内容に対する署名となります。これらの 2 つのレコードによって、ログが改ざんされていないことが保証されます。

▼ セキュリティー保護されたログを有効にする

1. Logger という名前の証明書を作成し、**Access Manager** を実行する配備コンテナにインストールします。配備コンテナの詳細については、マニュアルを参照してください。

2. **Access Manager** コンソールを使用して「ログサービス」設定の「セキュリティー保護されたログ」を有効にし、変更を保存します。管理者は、「ログサービス」のその他の属性のデフォルト値を変更することもできます。

   ログディレクトリがデフォルトのディレクトリ (/var/opt/SUMWam/logs) から変更されている場合は、アクセス権が 0700 に設定されていることを確認してください。このディレクトリが存在しない場合には、ログサービスによって作成されますが、そのアクセス権は 0755 に設定されます。

   また、デフォルトではないログディレクトリを指定した場合は、Web コンテナの server.policy ファイルで次のパラメータをその 新しいディレクトリに変更する必要があります。

   ```
   permission java.io.FilePermission “/var/opt/SUNWam/logs/*”,”delete,write”
   ```

3. *AccessManager-base*/SUNWam/config ディレクトリに証明書データベースパスワードを含むファイルを作成し、.wtpass という名前を付けます。

   注 – ファイル名とそのパスは、AMConfig.properties ファイルに設定できます。詳細については、付録 A の「証明書データベース」を参照してください。

   セキュリティー上の理由から、このファイルへの読み取りアクセス権を持つ管理者だけが配備コンテナを使用できるようにしてください。

   ---

4. サーバーを再起動します。

   このとき、セキュリティー保護されたログディレクトリをクリアすることをお勧めします。セキュリティー保護されたログを開始したときに、誤解を招きやすい検証エラーが /var/opt/SUNWam/debug/amLog ファイルに書き込まれることがあるからです。

   セキュリティーログに対する未承認の変更や改ざんを検出するには、検証プロセスによって /var/opt/SUNWam/debug/amLog に書き込まれたエラーメッセージを探してください。改ざんを手動で確認する場合は、VerifyArchive ユーティリティーを実行します。詳細については、第 19 章を参照してください。

コマンド行ログ

amadmin コマンド行ツールを使用して、Directory Server のアイデンティティーオブジェクト (組織、ユーザー、ロールなど) を作成、変更、および削除することができます。このツールを使用して、サービステンプレートをロード、作成、および登録することもできます。-t オプションを指定すれば、ログサービスでこれらのアクションを記録できます。AMConfig.properties の com.iplanet.am.logstatus プロパティーが有効 (ACTIVE) になっている場合は、ログレコードが作成されます。このプロパティーはデフォルトでは有効になっています。コマンド行ログのファイル名は、amAdmin で始まります。詳細については、第 14 章を参照してください。

ログプロパティー

AMConfig.properties ファイルには、ログ出力を制御するプロパティーが入っています。

com.iplanet.am.logstatus=ACTIVE	このプロパティーを使用して、ログの有効または無効を切り替えます。デフォルトでは ACTIVE になっています。
iplanet-am-logging.*service*.level= *level*	*service* にはデバッグログを記録するサービス名を指定します。この名前はそのままデバッグファイルの名前になります。*level* は java.util.logging.Level の値のいずれかであり、記録されるログの詳細レベルを表します。指定できるレベルは、SEVERE、WARNING、INFO、CONFIG、FINE、FINER、および FINEST です。ほとんどのサービスでは、INFO レベルより詳細なログは記録されません。

リモートログ

Access Manager では、リモートログがサポートされます。これにより、Access Manager SDK がインストールされたホストを使用するクライアントアプリケーションが、リモートマシン上に配備された Access Manager インスタンス上にログレコードを作成できるようになります。リモートログは、次のいずれかの場合に開始されます。

1. ある Access Manager インスタンスのネームサービスのログ URL にリモートの Access Manager インスタンスの URL が指定されていて、2 つのインスタンスの間に信頼関係が設定されている場合に、リモート Access Manager インスタンスにログが記録されます。
2. Access Manager SDK がリモート Access Manager インスタンスにインストールされていて、SDK サーバーで実行されているクライアント (または Java クラス) がログ API を使用している場合に、リモート Access Manager マシンにログが記録されます。

3. ログ API が Access Manager エージェントで使用されているとき。

▼ リモートログを有効にする

1 **Sun Java System Web Server** を使用する場合は、`server.xml` 設定ファイルに次の環境変数を設定する必要があります。

- `java.util.logging.manager=com.sun.identity.log.LogManager`
- `java.util.logging.config.file=/`*AccessManager-base*`/SUNwam/lib/LogConfig.properties`
- 使用する Java™ 2 Platform, Standard Edition が 1.4 以降である場合にこれを実現するには、コマンド行から次の呼び出しを行います。

  `java -cp /`*AccessManager-base*` /SUNWam/lib/am_logging.jar:/`*AccessManager-base*`/SUNWam/lib/xercesImpl.jar:/`*AccessManager-base*`/SUNWam/lib/xmlParserAPIs.jar:/`*AccessManager-base*`/SUNWam/lib/jaas.jar:/`*AccessManager-base*`/SUNWam/lib/xmlParserAPIs.jar:/`*AccessManager-base*`/SUNWam/lib/servlet.jar:/`*AccessManager-base*`/SUNWam/locale:/`*AccessManager-base*`/SUNWam/lib/am_services.jar:/`*AccessManager-base*`/SUNWam/lib/am_sdk.jar:/`*AccessManager-base*`/SUNWam/lib/jss311.jar:/ `*AccessManager-base*`/SUNWam/lib:.`

  `-Djava.util.logging.manager=com.sun.identity.log.LogManager`

  `-Djava.util.logging.config.file=/`*AccessManager-base*`/SUNwam/lib/LogConfig.properties <logTestClass>`
- 使用する Java 2 Platform, Standard Edition が 1.4 よりも前のものである場合にこれを実現するには、コマンド行から次の呼び出しを行います。

  `java -Xbootclasspath/a:/`*AccessManager-base*` /SUNWam/lib/jdk_logging.jar -cp /`*AccessManager-base*` /SUNWam/lib/am_logging.jar:/`*AccessManager-base*`/SUNWam/lib/xercesImpl.jar:/`*AccessManager-base*`/SUNWam/lib/xmlParserAPIs.jar:/`*AccessManager-base*`/SUNWam/lib/jaas.jar:/`*AccessManager-base*`/SUNWam/lib/xmlParserAPIs.jar:/`*AccessManager-base*`/SUNWam/lib/servlet.jar:/`*AccessManager-base*`/SUNWam/locale:/`*AccessManager-base*`/SUNWam/lib/am_services.jar:/`*AccessManager-base*`/SUNWam/lib/am_sdk.jar:/`*AccessManager-base*`/SUNWam/lib/jss311.jar:/ `*AccessManager-base*`/SUNWam/lib:.`

  `-Djava.util.logging.manager=com.sun.identity.log.LogManager`

  `-Djava.util.logging.config.file=/`*AccessManager-base*`/SUNwam/lib/LogConfig.properties <logTestClass>`

2 *AccessManager-base*`/SUNWam/lib` の `LogConfig.properties` に次のパラメータが設定されていることを確認します。

- `iplanet-am-logging-remote-handler=com.sun.identity.log.handlers.RemoteHandler`
- `iplanet-am-logging-remote-formatter=com.sun.identity.log.handlers.RemoteFormatter`
- `iplanet-am-logging-remote-buffer-size=1`

  リモートログでは、ログレコード数に基づいてバッファー機能がサポートされます。この値には、レコード数でログバッファーサイズを定義します。バッファーがいっぱいになったら、バッファーに保管されたすべてのレコードがサーバーにフラッシュされます。
- `iplanet-am-logging-buffer-time-in-seconds=3600`

  この値には、ログバッファーとクリーナのスレッドを呼び出すときの、タイムアウト期間を定義します。
- `iplanet-am-logging-time-buffering-status=OFF`

  この値には、ログバッファー (およびバッファークリーナのスレッド) を有効にするかどうかを定義します。デフォルトでは、この機能は無効になっています。

注 – ログファイルが空の場合、セキュリティー保護されたログに「verification failure」と表示される可能性があります。これは、作成されたファイルの数がアーカイブサイズに等しい場合、セキュリティー保護されたログが、このセットからアーカイブし、再起動するからです。ほとんどの場合、このエラーは無視してもかまいません。レコード数がアーカイブサイズに等しくなると、このエラーは表示されなくなります。

エラーログとアクセスログ

Access Manager には 2 種類のログファイルが存在します。アクセスログファイルとエラーログファイルです。

アクセスログファイルには、Access Manager 配備に関する一般的な監査情報が記録されます。ログには、認証の成功など、特定のイベントに対する単一のレコードが含まれる場合があります。またその同じイベントに対する複数のレコードが含まれる場合もあります。たとえば、管理者がコンソールを使って特定の属性の値を変更した場合、ログサービスは、その変更の試みを 1 つのレコードとしてログに記録します。ログサービスはさらに、その変更の実行結果も、2 番目のレコードとしてログに記録します。

エラーログファイルには、アプリケーション内で発生したエラーが記録されます。ある処理のエラーはエラーログに記録されますが、その処理が試みられたことはアクセスログファイルに記録されます。

フラットログファイルには、`.error`、`.access` のいずれかの拡張子が付けられます。データベースの列名は、`_ERROR`、`_ACCESS` のいずれかで終わります。たとえば、コンソールイ

ベントのログを記録するフラットファイルの名前が amConsole.access である場合、その同じイベントのログを記録するデータベース列の名前は、AMCONSOLE_ACCESS または amConsole_access になります。

次の表では、各 Access Manager コンポーネントが生成するログファイルについて簡単に説明します。

表 13–1 Access Manager コンポーネントのログ

コンポーネント	ログファイル名のプレフィックス	ログに記録される情報
セッション	amSSO	ログイン時刻、ログアウト時刻、タイムアウト制限などのセッション管理属性値。
管理コンソール	amConsole	アイデンティティー関連のオブジェクト、レルム、ポリシーの作成、削除、変更など、管理コンソール経由で実行されるユーザーアクション。
認証	amAuthentication	ユーザーのログインとログアウト。
アイデンティティー連携	amFederation	認証ドメインの作成やホストプロバイダの作成など、連携関連のイベント。連携ログのファイル名は、amFederation で始まります。
承認 (ポリシー)	amPolicy	ポリシーの作成、削除、変更やポリシー評価など、ポリシー関連のイベント。
ポリシーエージェント	amAgent	特定のユーザーからのアクセスが許可または拒否されたリソースに関する例外。amAgent ログは、ポリシーエージェントがインストールされたサーバー上に存在します。エージェントイベントのログは、Access Manager マシン上の認証ログに記録されます。
SAML	amSAML	表明、アーティファクトの作成または削除、応答や要求の詳細、SOAP エラーなど、SAML 関連のイベント。
コマンド行	amAdmin	コマンド行ツールによる操作中に発生したイベントエラー。例: サービススキーマの読み込み、ポリシーの作成、ユーザーの削除。

Access Manager のログファイルの一覧と説明については、付録 C を参照してください。

デバッグファイル

デバッグファイルは、ログサービスの機能ではありません。デバッグファイルは、ログ API とは別の API を使用して記録されます。デバッグファイルは、`/var/opt/SUNWam/debug` に格納されます。この場所は、デバッグ情報のレベルと一緒に、*AccessManager-base*`/SUNWam/lib/` ディレクトリの `AMConfig.properties` ファイルで設定できます。デバッグプロパティーの詳細については、付録 A を参照してください。

デバッグレベル

デバッグファイルに記録できる情報には、いくつかのレベルがあります。デバッグレベルは、`AMConfig.properties` の `com.iplanet.services.debug.level` プロパティーを使用して設定します。

1. off—デバッグ情報は記録されません。
2. error—このレベルは本稼働環境で使用されます。運用者は、本稼働環境ではデバッグファイルにエラーが記録されることのないように努めてください。
3. warning—現在、このレベルを使用することは推奨されていません。
4. message—コードトレースを使用するときに発生する可能性のある問題を警告します。ほとんどの Access Manager モジュールでは、このレベルを使用してデバッグメッセージが送信されます。

注 – warning および message レベルは、本稼働環境では使用してはいけません。パフォーマンスが大きく低下し、大量のデバッグメッセージが送信されます。

デバッグ出力ファイル

デバッグファイルは、モジュールがデバッグファイルに書き込むときに作成されます。したがって、デフォルトの「`error`」モードでは、デバッグファイルは生成されません。デバッグレベルを「`message`」に設定した状態で基本的なログインを実行すると、次のデバッグファイルが作成されます。

- amAuth
- amAuthConfig
- amAuthContextLocal
- amAuthLDAP
- amCallback
- amClientDetection
- amConsole
- amFileLookup
- amJSS
- amLog

- amLoginModule
- amLoginViewBean
- amNaming
- amProfile
- amSDK
- amSSOProvider
- amSessionEncodeURL
- amThreadManager

もっとも頻繁に使用されるファイルは、amSDK、amProfile、および認証に関連するすべてのファイルです。記録される情報には、日付、時刻、およびメッセージタイプ (Error、Warning、Message) などがあります。

デバッグファイルの使用

デバッグレベルは、デフォルトでは「error」に設定されています。デバッグファイルは、管理者が次の作業を行っているときに役立ちます。

- カスタム認証モジュールを作成するとき。
- Access Manager SDK を使用してカスタムアプリケーションを作成するとき。amProfile および amSDK デバッグファイルがこの情報を記録します。
- コンソールまたは SDK を使用しているときにアクセス権の障害を追跡するとき。amProfile および amSDK デバッグファイルは、この情報も記録します。
- SSL の障害を追跡するとき。
- LDAP 認証モジュールの障害を追跡するとき。amAuthLDAP デバッグファイルがこの情報を記録します。

デバッグファイルは、今後提供する予定の障害追跡ガイドと一緒に使用することをお勧めします。たとえば、SSL に障害が発生したときには、「message」レベルのデバッグを有効にして、amJSS デバッグファイルで証明書固有のエラーを探してみるとよいでしょう。

複数の **Access Manager** インスタンスとデバッグファイル

Access Manager には、多数のサーバーインスタンスを設定するときに使用できるように、ammultiserverinstall スクリプトが用意されています。複数のサーバーインスタンスがそれぞれ異なるデバッグディレクトリを使用するように設定されている場合、各インスタンスに対してそれぞれのデバッグディレクトリへの読み取りアクセス権と書き込みアクセス権を割り当てる必要があります。

パート IV

コマンド行リファレンス

このコマンド行リファレンスは、『Sun Java System Access Manager 7 2005Q4 管理ガイド』の第 4 部です。

ここで説明するすべてのコマンド行ツールは、デフォルトでは次の場所にあります。

```
AccessManager-base/SUNWam/bin (Solairs)
AccessManager-base/identity/bin (Linux)
```

次の章で構成されています。

◆ ◆ ◆ 第 14 章

amadmin コマンド行ツール

この章では、amadmin コマンド行ツールについて説明します。

amadmin コマンド行実行可能ファイル

コマンド行実行可能ファイル amadmin の第一目的は、XML サービスファイルをデータストアにロードすることと、DIT 管理タスクのバッチ処理を実行することです。amadmin は AccessManager-base/SUNWam/bin にあり、次の目的に使用します。

- XML サービスファイルのロード - 管理者は sms.dtd で定義された XML サービスファイル形式に従って記述されたサービスを Access Manager にロードします。すべてのサービスは amadmin を使用してロードする必要があります。Access Manager コンソールでインポートすることはできません。

注 – XML サービスファイルは、Access Manager で参照される XML データの静的 *BLOB* としてデータストアに格納されます。この情報は、LDAP だけを利用する Directory Server では使用されません。

- DIT に対するアイデンティティーオブジェクトのバッチ更新の実行 - 管理者は amadmin.dtd に定義されたバッチ処理用 XML ファイル形式を使用して、Directory Server DIT に対するバッチ更新を実行できます。たとえば、管理者が組織を 10 個、ユーザーを 1000 名、およびグループを 100 個作成する場合、この要求を 1 つ以上のバッチ処理用 XML ファイルに置いて、amadmin でロードすることで、1 回で作成できます。

注 – amadmin は、Access Manager コンソールの機能の一部だけをサポートしており、コンソールの代わりに使用することは想定していません。比較的小規模な管理作業にはコンソールを使用し、比較的大規模な管理作業には amadmin を使用することをお勧めします。

---

amadmin の構文

amadmin を使用するために従わなくてはならない構造的なルールが数多くあります。amadmin ツールの一般的な構文は次のとおりです。

- amadmin -u | --runasdn *DN* 名 -w | --password パスワード [-l | --locale ロケール名] [[-v | --verbose] | [-d |--debug]] -t | --data *XML* ファイル *1* [*XML* ファイル *2* ...]
- amadmin -u | --runasdn *DN* 名 -w | --password パスワード [-l | --locale ロケール名] [[-v | --verbose] | [-d | --debug]] -s | --schema *XML* ファイル *1* [*XML* ファイル *2* ...]
- amadmin -u | --runasdn *DN* 名 -w | --password パスワード [-l | --locale ロケール名] [[-v | --verbose] | [-d | --debug]] -r | --deleteService サービス名 *1* [サービス名 *2* ...]
- amadmin -u | --runasdn *DN* 名 -w | --password パスワード または -f | --passwordfile パスワードファイル [-c | --continue] [-l | --locale ロケール名] [[-v | --verbose] | [-d | --debug]] -m | --session サーバー名 パターン
- amadmin -h | --help
- amadmin -n | --version
- amadmin -u | --runasdn *DN* 名 -w | --password パスワード または - f |--passwordfile パスワードファイル [-l | --locale ロケール名] [[-v | --verbose] | [-d] |--debug]] -a |--addAttributes サービス名 スキーマタイプ *xml* ファイル [*xmlf* ファイル *2*] ...

注 – 2 連続するハイフンは、構文に示すとおりに入力する必要があります。

---

amadmin のオプション

次に、amadmin コマンド行パラメータオプションの定義について説明します。

--runasdn (-u)

--runasdn は、LDAP サーバーに対してユーザーを認証します。引数は、amadmin を実行できるように承認されたユーザーの識別名 (DN) です。たとえば次のようになります。

```
--runasdn uid=amAdmin,ou=People,o=iplanet.com,o=isp
```

DN は、ドメインコンポーネント間にスペースを挿入し、DN 全体を二重引用符で囲んだ形式にすることもできます。たとえば次のようになります。`--runasdn "uid=amAdmin, ou=People, o=iplanet.com, o=isp"`

--password (-w)

--password は必須のオプションであり、--runasdn オプションで指定した DN のパスワードを指定します。

--locale (-l)

--locale には、ロケール名を指定します。このオプションは、メッセージ言語のカスタマイズに使用できます。指定しない場合は、デフォルトのロケールである en_US が使用されます。

--continue (-c)

--continue は、エラーがある場合でも XML ファイルを処理し続けます。たとえば、同時にロードされる XML ファイルが 3 つあり、最初の XML ファイルがエラーになった場合、amadmin では残りのファイルをロードし続けます。continue オプションは、個別の要求のみに適用されます。

--session (-m)

--session (-m) は、セッションを管理したり、現在のセッションを表示したりします。--runasdn を指定するときは、AMConfig.properties のスーパーユーザーの DN、または最上位の管理ユーザーの ID と同じでなければなりません。

次の例では、特定のサービスホスト名に対するすべてのセッションを表示します。

```
amadmin -u uid=amadmin,ou=people,dc=iplanet,dc=com
-v  -w 12345678 -m http://sun.com:58080
```

次の例では、特定のユーザーのセッションを表示します。

```
amadmin -u uid=amadmin,ou=people,dc=iplanet,dc=com -v
 -w 12345678 -m http://sun.com:58080 username
```

セッションを中断するには、対応するインデックス番号をパターンに指定します。複数のセッションを中断するには、複数のインデックス番号をスペース区切りでパターンに指定します。

次のオプションを使用する場合

amadmin -m | --session サーバー名パターン

パターンには、ワイルドカード (*) も使用できます。このパターンにワイルドカード (*) を使用する場合は、メタ文字 (\\) を使ってシェルからエスケープする必要があります。

--debug (-d)

--debug は、/var/opt/SUNWam/debug ディレクトリに作成される amAdmin ファイルにメッセージを書き込みます。このメッセージは技術的には詳細なものですが、多言語対応ではありません。amadmin の操作ログを生成するには、データベースのログ書き込み時に、データベースドライバのクラスパスを手作業で追加する必要があります。たとえば、mysql にログを書き込むときに、amadmin に次の行を追加します。

```
CLASSPATH=$CLASSPATH:/opt/IS61/SUNWam/lib/mysql-connector-java-3.0.6-stable-bin.jar
export CLASSPATH
```

--verbose (-v)

--verbose は、amadmin コマンドの処理状況の全体を画面に出力します。ファイルには詳細な情報を出力しません。コマンド行のメッセージ出力は、多言語対応です。

--data (-t)

--data には、インポートされるバッチ処理用 XML ファイルの名前を指定します。1 つ以上の XML ファイルを指定できます。この XML ファイルではさまざまなディレクトリオブジェクトを作成、削除、および読み取ることができるほか、サービスを登録および登録解除できます。

--schema (-s)

--schema は、Access Manager サービスの属性を Directory Server にロードします。サービス属性が定義されている XML サービスファイルを引数に取ります。この XML サービスファイルは、sms.dtd を基にしています。1 つ以上の XML ファイルを指定できます。

注 – DIT に対するバッチ更新を設定するか、サービススキーマおよび設定データをロードするかによって、--data または --schema オプションを指定する必要があります。

--deleteservice (-r)

--deleteservice は、サービスとそのスキーマだけを削除します。

--serviceName

--serviceName は、XML サービスファイルの Service name=... タグに指定されているサービス名の値です。この部分を 216 ページの「--serviceName」に示します。

例 14–1 sampleMailService.xml の一部

```
...
<ServicesConfiguration>
    <Service name="sampleMailService" version="1.0">
        <Schema
 serviceHierarchy="/other.configuration/sampleMailService"
            i18nFileName="sampleMailService"
            i18nKey="iplanet-am-sample-mail-service-description">
...
```

--help (-h)

--help は、amadmin コマンドの構文を表示する引数です。

--version (-n)

--version は、ユーティリティー名、製品名、製品バージョン、および法律上の通知を表示する引数です。

amadmin を連携管理に使用する

この節では、連携管理で使用する amadmin のパラメータを示します。連携管理の詳細は『Access Manager Federation Management Guide』を参照してください。

Liberty のメタに準拠した XML を Directory Server にロードする

```
amadmin -u|--runasdn <ユーザーの DN>
-w|--password <パスワード> または -f|--passwordfile <パスワードファイル>
-e|--entityname <エンティティー名>
-g|--import <XML ファイル>
```

--runasdn (-u)

ユーザーの DN

--password (-w)

ユーザーのパスワードです。

--passwordfile (-f)

ユーザーのパスワードが書かれているファイルの名前です。

--entityname (-e)

エンティティー名。たとえば、http://www.example.com などです。エンティティーは、1 つの組織に属していなければなりません。

--import (-g)

メタ情報を保持する XML ファイルです。このファイルは Liberty のメタ仕様と XSD に従わなければなりません。

エンティティーをデジタル署名なしで XML ファイルにエクスポートする

amadmin -u|--runasdn <ユーザーの DN>

```
-w|--password <パスワード> または -f|--passwordfile <パスワードファイル>
-e|--entityname <エンティティー名>
-o|--export <ファイル名>
```

--runasdn (-u)

ユーザーの DN

--password (-w)

ユーザーのパスワードです。

--passwordfile (-f)

ユーザーのパスワードが書かれているファイルの名前です。

--entityname (-e)

Directory Server にあるエンティティー名です。

--export (-o)

エンティティーの XML が書かれているファイルの名前です。XML は Liberty のメタ XSD に準拠していなければなりません。

エンティティーを XML デジタル署名付きで XML ファイルにエクスポートする

```
amadmin -u|--runasdn <ユーザーの DN>
-w|--password <パスワード> または -f|--passwordfile <パスワードファイル>
-e|--entityname <エンティティー名>
-q|--exportwithsig <ファイル名>
```

--runasdn (-u)

ユーザーの DN

--password (-w)

ユーザーのパスワードです。

--passwordfile (-f)

ユーザーのパスワードが書かれているファイルの名前です。

--entityname (-e)

Directory Server にあるエンティティー名です。

--exportwithsig (-o)

エンティティーの XML が書かれているファイルの名前です。このファイルはデジタル署名されています。XML は Liberty のメタ XSD に準拠していなければなりません。

リソースバンドルに **amadmin** を使用する

下の節では、amadmin 構文を使ってリソースバンドルの追加、検索、および削除を行う方法について説明します。

リソースバンドルを追加する

```
amadmin -u|--runasdn <ユーザーの DN> -w|--password <ユーザーのパスワード>

-b|--addresourcebundle <リソースバンドル名>

-i|--resourcebundlefilename <リソースバンドルファイル名>

[-R|--resourcelocale] <ロケール>
```

リソース文字列を得る

```
amadmin -u|--runasdn <ユーザーの DN> -w|--password <ユーザーのパスワード>

-z|--getresourcestrings <リソースバンドル名>

[-R|--resourcelocale] <ロケール>
```

リソースバンドルを削除する

```
amadmin -u|--runasdn <ユーザーの DN> -w|--password <ユーザーのパスワード>

-j|--deleteresourcebundle <リソースバンドル名>

[-R|--resourcelocale] <ロケール>
```

◆ ◆ ◆ 第 15 章

ampassword コマンド行ツール

この章では、amPassword コマンド行ツールについて説明します。この章は、次の節で構成されています。

ampassword コマンド行実行可能ファイル

Access Manager の ampassword ユーティリティーは、Solaris システム上では /opt/SUNWam/bin に、Linux システム上では /opt/sun/Identity/bin にあります。ampassword ユーティリティーを使用すると、管理者またはユーザーの Directory Server パスワードを変更できます。

▼ SSL モードで実行中の Access Manager で ampassword を実行するには

1. serverconfig.xml ファイルを修正します。このファイルは、次のディレクトリにあります。

   ```
   AccessManager-base/SUNWam/config/
   ```

2. サーバー属性 port を **Access Manager** を実行している **SSL** ポートに変更します。

3. type 属性を **SSL** に変更します。
   次に例を示します。

   ```
   <iPlanetDataAccessLayer>
   <ServerGroup name="default" minConnPool="1" maxConnPool="10">
       <Server name="Server1" host="sun.com" port="636" type="SSL" />
       <User name="User1" type="proxy">
           <DirDN>
   ```

```
                cn=puser,ou=DSAME Users,dc=iplanet,dc=com
        </DirDN>
        <DirPassword>
                 AQIC5wM2LY4Sfcy+AQBQxghVwhBE92i78cqf
         </DirPassword>
</User> ...
```

ampassword では、Directory Server 内のパスワードだけが変更されます。Access Manager のすべての認証テンプレートおよび ServerConfig.xml にあるパスワードは、手動で変更する必要があります。

◆ ◆ ◆ 第 16 章

bak2am コマンド行ツール

この章では、bak2am コマンド行ツールについて説明します。この章は、次の節で構成されています。

bak2am コマンド行実行可能ファイル

Access Manager の bak2am ユーティリティーは AccessManager-base/SUNWam/bin にあります。bak2am ユーティリティーでは、am2back ユーティリティーでバックアップした Access Manager コンポーネントを復元します。

bak2am の構文

Solaris オペレーティングシステムで bak2am ツールを使用するための一般的な構文は次のとおりです。

```
./bak2am [ -v | --verbose ] -z | --gzip tar.gz ファイル
./bak2am [ -v | --verbose ] -t | --tar tar ファイル
./bak2am -h | --help
./bak2am -n | --version
```

Microsoft Windows 2000 オペレーティングシステムで bak2am ツールを使用するための一般的な構文は次のとおりです。

```
bak2am [ -v | --verbose ] -d | --directory ディレクトリ名

bak2am -h | --help
bak2am -n | --version
```

注 – 2 連続するハイフンは、構文に示すとおりに入力する必要があります。

bak2am のオプション

--gzip バックアップ名

--gzip は、tar.gz 形式のバックアップファイルのフルパスとファイル名を指定します。デフォルトのパスは、AccessManager-base/backup です。Solaris 専用のオプションです。

--tar バックアップ名

--tar は、tar 形式のバックアップファイルのフルパスとファイル名を指定します。デフォルトのパスは、AccessManager-base/backup です。Solaris 専用のオプションです。

--verbose

--verbose は、バックアップユーティリティーを冗長モードで実行するときに使用します。

--directory

--directory は、バックアップのあるディレクトリを指定します。デフォルトのパスは、AccessManager-base/backup です。Microsoft Windows 2000 専用のオプションです。

--help

--help は、bak2am コマンドの構文を表示する引数です。

--version

--version は、ユーティリティー名、製品名、製品バージョン、および法律上の通知を表示する引数です。

◆ ◆ ◆ 第 17 章

17 am2bak コマンド行ツール

この章では、am2bak コマンド行ツールについて説明します。

am2bak コマンド行実行可能ファイル

Access Manager の am2bak ユーティリティーは AccessManager-base/SUNWam/bin にあります。am2bak ユーティリティーは、Access Manager のコンポーネントのすべてまたは一部をバックアップします。ログのバックアップ中は、Directory Server を実行している必要があります。

am2bak の構文

Solaris オペレーティングシステムで am2bak ツールを使用するための一般的な構文は次のとおりです。

```
./am2bak [ -v | --verbose ] [ -k | --backup バックアップ名 ] [ -l | --location 場所 ] [
[-c | --config] | [-b | --debug] | [-g | --log] | [-t | --cert] | [-d | --ds] | [-a |
--all]]*

./am2bak -h | --help

./am2bak -n | --version
```

Microsoft Windows 2000 オペレーティングシステムで am2bak ツールを使用するための一般的な構文は次のとおりです。

```
am2bak [ -v | --verbose ] [ -k | --backup バックアップ名 ] [ -l | --location 場所 ] [
[-c | --config] | [-b | --debug] | [-g | --log] | [-t | --cert] | [-d | --ds] | [-a |
--all]]*

am2bak -h | --help

am2bak -n | --version
```

注 – 2 連続するハイフンは、構文に示すとおりに入力する必要があります。

am2bak のオプション

--verbose (-v)

--verbose は、バックアップユーティリティーを冗長モードで実行するときに使用します。

--backup バックアップ名 *(-k)*

--backup バックアップ名 は、バックアップファイルの名前を定義します。デフォルトは ambak です。

--location (-l)

--location は、バックアップに使用するディレクトリの場所を指定します。デフォルトの場所は AccessManager-base/backup です。

--config (-c)

--config は、設定ファイルのみバックアップすることを指定します。

--debug (-b)

--debug は、デバッグファイルのみバックアップすることを指定します。

--log (-g)

--log は、ログファイルのみバックアップすることを指定します。

--cert (-t)

--cert は、証明書データベースファイルのみバックアップすることを指定します。

--ds (-d)

--ds は、Directory Server のみバックアップすることを指定します。

--all (-a)

--all は、Access Manager 全体を完全バックアップすることを指定します。

--help (-h)

`--help` は、`am2bak` コマンドの構文を表示する引数です。

--version (-n)

`--version` は、ユーティリティー名、製品名、製品バージョン、および法律上の通知を表示する引数です。

▼ バックアップ手順を実行するには

1. ルートユーザーでログインします。
   このスクリプトを実行するには、ルートユーザーのアクセス権が必要です。

2. 必要に応じて、正しいパスを使用していることを確認するためのスクリプトを実行します。
   このスクリプトでは、次の Solaris™ オペレーティング環境ファイルをバックアップします。

   - 設定ファイルおよびカスタマイズファイル
     - `AccessManager-base/SUNWam/config/`
       - `AccessManager-base/SUNWam/locale/`
       - `AccessManager-base/SUNWam/servers/httpacl`
       - `AccessManager-base/SUNWam/lib/*.properties` (Java プロパティーファイル)
       - `AccessManager-base/SUNWam/bin/amserver.` インスタンス名
       - `AccessManager-base/SUNWam/servers/https-` すべてのインスタンス
       - `AccessManager-base/SUNWam/servers/web-apps-` すべてのインスタンス
       - `AccessManager-base/SUNWam/web-apps/services/WEB-INF/config`
       - `AccessManager-base/SUNWam/web-apps/services/config`
       - `AccessManager-base/SUNWam/web-apps/applications/WEB-INF/classes`
       - `AccessManager-base/SUNWam/web-apps/applications/console`
       - `/etc/rc3.d/K55amserver.`すべてのインスタンス
       - `/etc/rc3.d/S55amserver.`すべてのインスタンス
       - `DirectoryServer-base/slapd-` *host* `/config/schema/`
       - `DirectoryServer-base/slapd-` *host* `/config/slapd-collations.conf`
       - `Access Manager/slapd-` *host* `/config/dse.ldif`

     ログファイルおよびデバッグファイル

       - `var/opt/SUNWam/logs` (Access Manager ログファイル)
       - `var/opt/SUNWam/install` (Access Manager インストールログファイル)
       - `var/opt/SUNWam/debug` (Access Manager デバッグファイル)

     証明書

       - `Access Manager/SUNWam/servers/alias`

- `Access Manager/alias`

  スクリプトでは、次の Microsoft® Windows 2000 オペレーティングシステム ファイルもバックアップされます。

設定ファイルおよびカスタマイズファイル

- `AccessManager-base/web-apps/services/WEB-INF/config/*`
- `AccessManager-base/locale/*`
- `AccessManager-base/web-apps/applications/WEB-INF/classes/*.properties` (Java プロパティーファイル)
- `AccessManager-base/servers/https-` *host*`/config/jvm12.conf`
- `AccessManager-base/servers/https-` *host*`/config/magnus.conf`
- `AccessManager-base/servers/https-` *host*`/config/obj.conf`
- `DirectoryServer-base/slapd-host/config/schema/*.ldif`
- `DirectoryServer-base/slapd-host/config/slapd-collations.conf`
- `DirectoryServer-base/slapd-host/config/dse.ldif`

ログファイルおよびデバッグファイル

- `var/opt/logs` (Access Manager ログファイル)
- `var/opt/debug` (Access Manager デバッグファイル)

証明書

- `AccessManager-base/servers/alias`
- `AccessManager/alias`

◆ ◆ ◆ 第 18 章

amserver コマンド行ツール

この章では、amserver コマンド行ツールについて説明します。この章は、次の節で構成されています。

amserver コマンド行実行可能ファイル

amserver コマンド行実行可能ファイルでは、それぞれ UNIX 認証モジュールと SecurID 認証モジュールに関連する amunixd ヘルパーと amsercuridd ヘルパーの起動と停止を行います。

amserver の構文

amserver ツールの一般的な構文は次のとおりです。

```
./amserver { start | stop }
```

start

start は、ヘルパーを開始するコマンドです。

stop

stop は、ヘルパーを停止するコマンドです。

◆ ◆ ◆ 第 19 章

VerifyArchive コマンド行ツール

この章では、VerifyArchive コマンド行ツールについて説明します。この章は、次の節で構成されています。

VerifyArchive コマンド行実行可能ファイル

VerifyArchive は、ログアーカイブを検証するために使用します。ログアーカイブとは、タイムスタンプ付きのログと、対応するキーストアのセットのことです。キーストアには、ログファイルの改ざんを検出するための MAC およびデジタル署名を生成するために使用する鍵が含まれます。アーカイブの検証では、アーカイブ内の、改ざんされたり削除されたりした可能性のあるファイルを検出します。

VerifyArchive では、指定された logName に対して、すべてのアーカイブセットと、各アーカイブセットに属するすべてのファイルを抽出します。VerifyArchive を実行すると、各ログレコードで改ざんを探します。改ざんが検出されると、改ざんのあったファイルとそのレコードの番号を知らせるメッセージが出力されます。

VerifyArchive では、アーカイブセットから削除されたファイルも確認します。削除されたファイルが検出されると、検証に失敗したことを知らせるメッセージが出力されます。改ざんまたは削除されたファイルが検出されなかった場合は、アーカイブの検証が正常に終了したことを知らせるメッセージが返されます。

注 – 管理者権限を持っていないユーザーが amverifyarchive を実行すると、エラーが発生する場合があります。

VerifyArchive の構文

すべてのパラメータは必須です。構文は次のとおりです。

```
amverifyarchive -l logName -p path -u
uname -w password
```

VerifyArchive のオプション

logName

logName は、検証されるログの名前 (amConsole、amAuthentication など) を指定します。VerifyArchive では、指定された logName に対してアクセスログとエラーログの両方を検証します。たとえば amConsole を指定すると、amConsole.access および amConsole.error ファイルが検証されます。また、logName に amConsole.access または amConsole.error と指定することで、検証をこれらのログに制限できます。

path

path は、ログファイルが格納されているディレクトリのフルパスです。

uname

uname は、Access Manager 管理者のユーザー ID です。

password

password は、Access Manager 管理者のパスワードです。

◆ ◆ ◆ 第 20 章

amsecuridd ヘルパー

この章では、amsecuridd ヘルパーについて説明します。この章は、次の節で構成されています。

amsecuridd ヘルパーコマンド行実行可能ファイル

Access Manager の SecurID 認証モジュールは、Security Dynamic ACE/Client C API と amsecuridd ヘルパーを使って実装されます。このヘルパーは、Access Manager の SecurID 認証モジュールと SecurID Server の間の通信を行います。SecurID 認証モジュールは、localhost:57943 へのソケットを開いて amsecuridd デーモンを呼び出し、SecurID 認証要求を待機します。

注 – 57943 はデフォルトのポート番号です。このポート番号がすでに使用されている場合は、SecurID 認証モジュールの SecurID ヘルパー認証ポート属性で別のポート番号を指定できます。このポート番号は、すべての組織で一意でなければなりません。

---

amsecuridd へのインタフェースは、stdin を介したクリアテキスト形式なので、ローカルホスト接続だけが許可されます。amsecuridd は、バックエンドで SecurID リモート API (バージョン 5.x) を使ってデータを暗号化します。

amsecuridd ヘルパーは、認定情報を受け取るために、デフォルトではポート番号 58943 で待機します。このポートがすでに使用されている場合は、AMConfig.properties ファイルの securidHelper.ports 属性でポートを変更できます。このファイルはデフォルトで、AccessManager-base/SUNWam/config/ にあります。securidHelp.ports 属性には、amsecuridd ヘルパーの各インスタンスのポートが、スペース区切りのリストとして格納されています。AMConfig.properties に加えた変更を保存したら、Access Manager を再起動してください。

注 – 異なる sdconf.rec ファイルを持つ別々の ACE/Server と通信する組織ごとに、個別の amsecuridd インスタンスを実行する必要があります。

amsecuridd の構文

構文は次のとおりです。

```
amsecuridd [-v] [-c ポート番号]
```

amsecuridd のオプション

-v

冗長モードをオンにし、/var/opt/SUNWam/debug/securidd_client.debug にログを記録します。

-c ポート番号

待機ポート番号を設定します。デフォルトは 58943 です。

amsecuridd ヘルパーの実行

amsecuridd は、デフォルトで *AccessManager-base* /SUNWam/share/bin にあります。デフォルトのポートでヘルパーを実行するには、オプションを指定せずに次のコマンドを入力します。

```
./amsecuridd
```

デフォルト以外のポートでヘルパーを実行するには、次のコマンドを入力します。

```
./amsecuridd [-v] [-c ポート番号]
```

amsecuridd を amserver コマンド行ユーティリティーから実行することもできますが、常にデフォルトポートでの実行になります。

必要なライブラリ

このヘルパーを実行するには、次のライブラリが必要です。これらのほとんどは、オペレーティングシステムの /usr/lib/ にあります。

- libnsl.so.1
- libthread.so.1

- libc.so.1
- libdl.so.1
- libmp.so.2
- librt.so.1
- libaio.so.1
- libmd5.so.1

注 – libaceclnt.so が見つかるように、LD_LIBRARY_PATH を *AccessManager-base*/Sunwam/lib/ に設定します。

パート V

付録

この付録は『Sun Java System Access Manager 7 2005Q4 管理ガイド』の第 5 部であり、エラーコードの一覧とファイルリファレンスを収録しています。次の付録で構成されています。

◆ ◆ ◆ 付 録 A

AMConfig.properties ファイル

AMConfig.properties は、Access Manager のメインの設定ファイルです。一部を除いて、このファイル内のプロパティーを編集することができます。この章では、AMConfig.properties に含まれるプロパティー、デフォルトのプロパティー値、および、Access Manager の動作を妨げることなく変更可能な値の変更方法について説明します。

この章は、次の節で構成されています。

AMConfig.properties ファイルについて

インストールの時点で、AMConfig.properties は etc/opt/SUNWam/config ディレクトリに位置しています。

AMConfig.properties では、1 行につき 1 つのプロパティーが定義され、個々のプロパティーは対応する値を持ちます。プロパティーと値は大文字と小文字が区別されます。スラッシュとアスタリスク (/*) で始まる行はコメントであり、アプリケーションはコメントを無視します。アスタリスクとスラッシュ (*/) で終わる行はコメントの終わりを表します。

AMConfig.properties 内のプロパティーを変更したあとで、変更を有効にするには Access Manager を再起動する必要があります。

Access Manager コンソール

- com.iplanet.am.console.deploymentDescriptor
  値はインストールの間に設定されます。例: /amconsole
- com.iplanet.am.console.host
  値はインストールの間に設定されます。例: *hostName.domain.Name*.com
- com.iplanet.am.console.port
  値はインストールの間に設定されます。例: 80
- com.iplanet.am.console.protocol
  値はインストールの間に設定されます。例: http

Access Manager サーバーインストール

- com.iplanet.am.install.basedir
  これは読み取り専用のプロパティーです。プロパティー値を変更しないでください。
  値はインストールの間に設定されます。例: /opt/SUNWam/web-src/services/WEB-INF
- com.iplanet.am.install.vardir
  これは読み取り専用のプロパティーです。プロパティー値を変更しないでください。
  値はインストールの間に設定されます。例: /var/opt/SUNWam
- com.iplanet.am.installdir

これは読み取り専用のプロパティーです。プロパティー値を変更しないでください。

値はインストールの間に設定されます。例: `/opt/SUNWam`

- `com.iplanet.am.jdk.path`

  値はインストールの間に設定されます。例: `/usr/jdk/entsys-j2se`

- `com.iplanet.am.locale`

  値はインストールの間に設定されます。例: `en_US`

- `com.iplanet.am.server.host`

  値はインストールの間に設定されます。例: *hostName.domainName*`.com`

- `com.iplanet.am.server.port`

  値はインストールの間に設定されます。例: `80`

- `com.iplanet.am.server.protocol`

  値はインストールの間に設定されます。例: `http`

- `com.iplanet.am.version`

  値はインストールの間に設定されます。例: `7 2005Q4`

- `com.sun.identity.server.fqdnMap[ ]`

  ユーザーが不正な URL を入力したとき、Access Manager 認証サービスが訂正アクションを実行できるようにします。これはたとえば、保護されたリソースにアクセスするために、ユーザーがホスト名の一部を指定した場合や IP アドレスを使用した場合に役立ちます。

  このプロパティーの構文は、対応する有効な名前にマップされた無効な FQDN 値を表します。プロパティーで使用する形式は `com.sun.identity.server.fqdnMap[`*invalid-name*`]=`*valid—name* です。この例で、*invalid-name* はユーザーが指定する可能性がある無効な FQDN ホスト名、*valid—name* はフィルタによってユーザーがリダイレクトされる FQDN ホスト名です。同一の無効 FQDN に対して重複する値が存在すると、アプリケーションがアクセス不可能になる可能性があります。また、このプロパティーで無効な値を使用した場合にも、アプリケーションがアクセス不可能になる可能性があります。このプロパティーを使用して、複数のホスト名をマップできます。これは、サーバー上でホストされるアプリケーションに複数のホスト名でアクセス可能な場合に役立ちます。

  このプロパティーを使用して、特定のホスト名 URL に対して訂正アクションが発生しないよう Access Manager を設定できます。これはたとえば、IP アドレスを直接指定してアプリケーションリソースにアクセスするユーザーに対し、リダイレクトなどの訂正アクションを発生させない必要がある場合に役立ちます。

  マップエントリは次のように指定できます。`com.sun.identity.server.fqdnMap[`*IP*`]=`*IP*

  このようなプロパティーは、プロパティー定義が有効であり、ここまでに説明した要件に従っている限りは何個でも指定できます。次に例を示します。

  `com.sun.identity.server.fqdnMap[`*isserver*`]=`*isserver.mydomain.com*
  `com.sun.identity.server.fqdnMap[`*isserver.mydomain*`]=`*isserver.mydomain.com*
  `com.sun.identity.server.fqdnMap[`*IP address*`]=`*isserver.mydomain.com*

am.util

- com.iplanet.am.util.xml.validating

  デフォルト値は no です。Access Manager の XMLUtils クラスを使用して XML ドキュメントをパースするときに妥当性検査が必要かどうかを決定します。このプロパティーは、com.iplanet.services.debug.level プロパティーの値が warning または message に設定されているときに限り有効です。指定できる値は yes および no です。XML ドキュメントの妥当性検査は、このプロパティーの値が yes であり、かつ com.iplanet.services.debug.level プロパティーの値が warning または message に設定されている場合にのみ有効になります。

amSDK

各 SDK キャッシュエントリは、ユーザー用に AMObject 属性値の集合を格納します。

- com.iplanet.am.sdk.cache.maxSize

  デフォルト値は 10000 です。キャッシュが有効なときの SDK キャッシュのサイズを指定します。1 以上の整数を指定します。それ以外の場合は、デフォルトサイズ (10000 ユーザー) が使用されます。

- com.iplanet.am.sdk.userEntryProcessingImpl

  このプロパティーは、com.iplanet.am.sdk.AMUserEntryProcessed インタフェースを実装して、ユーザーの作成、削除、および変更操作に対する一部のポストプロセスを実行するプラグインを指定します。このプロパティーを使用する場合は、上のインタフェースを実装する完全修飾クラス名を指定してください。

- com.iplanet.am.sdk.caching.enabled

  これを true に設定するとキャッシュが有効になり、false に設定するとキャッシュが無効になります。デフォルトは false です。

Application Server インストール

- com.iplanet.am.iASConfig

  値はインストールの間に設定されます。例: APPSERVERDEPLOYMENT

  このプロパティーは、Access Manager が iPlanet Application Server 上で実行されているかどうかを調べるために使用されます。

認証

- com.sun.identity.auth.cookieName

  デフォルト値は AMAuthCookie です。認証プロセスの間に認証サービスによって、セッションハンドラ ID を設定される Cookie 名を指定します。このプロセスが成功または失敗して完了すると、この Cookie はクリアまたは消去されます。

- com.sun.identity.authentication.ocsp.responder.nickname

  値はインストールの間に設定されます。そのレスポンダに対する認証局 (CA) 証明書ニックネーム。例: Certificate Manager - sun。設定する場合、CA 証明書が Web Server の証明書データベースに存在している必要があります。

- com.sun.identity.authentication.ocsp.responder.url

  値はインストールの間に設定されます。例: http://ocsp.sun.com/ocsp

  このインスタンスのグローバル OCSP レスポンダ URL を指定します。OCSP レスポンダ URL を設定する場合、OCSP レスポンダニックネームも設定する必要があります。設定しないと、両方とも無視されます。両方が設定されない場合、ユーザーの証明書で提示された OCSP レスポンダ URL が OCSP 妥当性検査に使用されます。OCSP レスポンダ URL がユーザーの証明書で提示されない場合、OCSP 妥当性検査は実行されません。

- com.sun.identity.authentication.ocspCheck

  デフォルト値は true です。OCSP チェックを有効または無効にするためのグローバルパラメータ。この値が false の場合、証明書認証モジュールタイプの OCSP 機能は使用できません。

- com.sun.identity.authentication.special.users

  値はインストールの間に設定されます。例: cn=dsameuser,ou=DSAME Users,o=AMRoot|cn=amService-UrlAccessAgent,ou=DSAME Users,o=AMRoot

  この Access Manager 認証コンポーネント用の特別なユーザーを識別します。このユーザーは、完全ユーザー DN を使ったリモートアプリケーション認証を Access Manager サーバーに対して実行するために、クライアント API によって使用されます。ユーザーは常に、ローカルのディレクトリサーバーに対して認証されます。この特別なユーザー DN の値を複数指定する場合は、それぞれパイプ文字 (|) で区切られます。このプロパティーの使用は認証コンポーネントのみに制限されます。

- com.sun.identity.authentication.super.user

  値はインストールの間に設定されます。例: uid=amAdmin,ou=People,o=AMRoot

  この Access Manager インスタンスのスーパーユーザーを識別します。このユーザーはログインに LDAP を使用する必要があり、完全 DN を使用する必要があります。ユーザーは常に、ローカルの Directory Server に対して認証されます。

- com.sun.identity.authentication.uniqueCookieDomain

上の Cookie 名に対して Cookie ドメインを設定するために使用されます。この Cookie ドメインは、ネットワークにインストールされた CDC (Cross Domain Controller) サービスのすべてのインスタンスを網羅するように設定することをお勧めします。たとえば、Access Manager のすべてのインスタンスがドメイン `example.com` の内部にある場合は「`.example.com`」と設定します。

- `com.sun.identity.authentication.uniqueCookieName`

  デフォルト値は `sunIdentityServerAuthNServer` です。Access Manager がセッション Cookie ハイジャック対策モードで動作しているときに、Access Manager サーバーホスト URL に設定された Cookie 名を指定します。

- `com.iplanet.am.auth.ldap.createUserAttrList`

  動的にユーザーを作成するように認証サービスが設定されているときに、LDAP 認証の間に外部 Directory Server から取得される値を含むユーザー属性のリストを指定します。ローカル Directory Server で作成される新しいユーザーには、外部 Directory Server から取得された属性の値が付与されます。

  例: *attribute1*, *attribute2*, *attribute3*

証明書データベース

これらのプロパティーは、iPlanet Web Server が SSL 用に設定されるときに JSS ソケットファクトリを初期化するために設定します。

- `com.iplanet.am.admin.cli.certdb.dir`

  値はインストールの間に設定されます。例: `/opt/SUNWwbsvr/alias`

  証明書データベースのパスを指定します。

- `com.iplanet.am.admin.cli.certdb.passfile`

  値はインストールの間に設定されます。例: `/etc/opt/SUNWam/config/.wtpass`

  証明書データベースのパスワードファイルを指定します。

- `com.iplanet.am.admin.cli.certdb.prefix`

  値はインストールの間に設定されます。例: `https-`*hostName.domainName*`.com-`*hostName*`-`

  証明書データベースのプレフィックスを指定します。

Cookie

- `com.iplanet.am.cookie.encode`

  このプロパティーにより、Access Manager は Cookie 値を `URLencode` でエンコードできます。`URLencode` は、文字を HTTP で理解できる形式に変換します。

  値はインストールの間に設定されます。例: `false`

- `com.iplanet.am.cookie.name`

デフォルト値は iPlanetDirectoryPro です。有効なセッションハンドラ ID を設定するために認証サービスで使用する Cookie 名。この Cookie 名の値は、有効なセッション情報を取得するために使用されます。

- com.iplanet.am.cookie.secure

  Access Manager Cookie をセキュリティー保護されたモードで設定できるようにし、HTTP(s) などのセキュリティー保護されたプロトコルが使用されているときにブラウザが Access Manager Cookie だけを返すようにします。

  デフォルト値は false です。

- com.iplanet.am.console.remote

  値はインストールの間に設定されます。例: false

  コンソールがリモートマシン上にインストールされるか、あるいはローカルマシン上にインストールされて認証コンソールによって使用されるかを決定します。

- com.iplanet.am.pcookie.name

  持続 Cookie の Cookie 名を指定します。持続 Cookie は、ブラウザウィンドウが閉じられたあとも存在し続けます。持続 Cookie を有効にすると、ユーザーは再度認証を行わなくても、新しいブラウザセッションにログインできます。デフォルト値は DProPCookie です。

- com.sun.identity.cookieRewritingInPath

  デフォルト値は true です。このプロパティーは、Access Manager が Cookie なしのモードで動作するように設定されているときに認証サービスによって読み取られます。このプロパティーは、URL 内の追加パス情報として、「protocol://server:port/uri;*cookiename*=cookieValue?queryString」の形式を使って Cookie を書き換える必要があることを指定します。このプロパティーを指定しない場合、Cookie はクエリー文字列の一部として書き込まれます。

- com.sun.identity.enableUniqueSSOTokenCookie

  デフォルト値は false です。値が true に設定されているとき、Access Manager がセッション Cookie ハイジャック対策モードで動作していることを示します。

デバッグ

- com.iplanet.services.debug.directory

  デバッグファイルが作成される出力ディレクトリを指定します。値はインストールの間に設定されます。例: /var/opt/SUNWam/debug

- com.iplanet.services.debug.level

  デバッグレベルを指定します。デフォルト値は error です。指定できる値は次のとおりです。

off	デバッグファイルは作成されません。
error	エラーメッセージだけがログに書き込まれます。
warning	警告メッセージだけがログに書き込まれます。

`message` エラーメッセージ、警告メッセージ、および情報メッセージがログに書き込まれます。

Directory Server インストール

- `com.iplanet.am.defaultOrg`

  値はインストール時に設定されます。例: `o=AMRoot`

  Access Manager 情報ツリーにおける最上位のレルムまたは組織を指定します。
- `com.iplanet.am.directory.host`

  値はインストールの間に設定されます。例: *DirectoryServerHost.domainName*.`com`

  Directory Server の完全修飾ホスト名を指定します。
- `com.iplanet.am.directory.port`

  値はインストールの間に設定されます。例: `389`

  Directory Server のポート番号を指定します。
- `com.iplanet.am.directory.ssl.enabled`

  デフォルト値は `false` です。Secure Socket Layer (SSL) が有効かどうかを示します。
- `com.iplanet.am.domaincomponent`

  値はインストールの間に設定されます。例: `o=AMRoot`

  Access Manager 情報ツリーのドメインコンポーネント (dc) 属性を指定します。
- `com.iplanet.am.rootsuffix`

  値はインストールの間に設定されます。例: `o=AMRoot`

イベント接続

- `com.iplanet.am.event.connection.delay.between.retries`

  デフォルト値は 3000 です。イベントサービス接続を再試行する間隔をミリ秒単位で指定します。
- `com.iplanet.am.event.connection.ldap.error.codes.retries`

  デフォルト値は `80,81,91` です。イベントサービス接続の再試行を開始する LDAP 例外エラーコードを指定します。
- `com.iplanet.am.event.connection.num.retries`

  デフォルト値は `3` です。イベントサービス接続の再試行回数として許可する回数を指定します。
- `com.sun.am.event.connection.idle.timeout`

  デフォルト値は `0` です。持続検索が再開されるまでの時間を分単位で指定します。

このプロパティーは、ポリシーエージェントと Directory Server の間にロードバランサまたはファイアウォールがあり、TCP アイドルタイムアウトの発生時に持続検索接続が切断される場合に使用します。このプロパティーの値は、ロードバランサまたはファイアウォールの TCP タイムアウト時間よりも短く設定することをお勧めします。それにより、接続が切断される前に持続検索が再開することが保証されます。値 `0` は、検索が再開されないことを示します。リセットされるのはタイムアウトした接続だけです。

グローバルサービス管理

- `com.iplanet.am.service.secret`

  値はインストールの間に設定されます。例: `AQICPX9e1cxSxB2RSy1WG1+O4msWpt/6djZl`

- `com.iplanet.am.services.deploymentDescriptor`

  値はインストールの間に設定されます。例: `/amserver`

- `com.iplanet.services.comm.server.pllrequest.maxContentLength`

  デフォルト値は `16384` または 16k です。Access Manager が許容する `HttpRequest` の最大コンテンツ長を指定します。

- `com.iplanet.services.configpath`

  値はインストールの間に設定されます。例: `/etc/opt/SUNWam/config`

ヘルパーデーモン

- `com.iplanet.am.daemons`

  デフォルト値は `unix securid` です。

- `securidHelper.ports`

  デフォルト値は `58943` です。このプロパティーの値はスペース区切りのリストです。SecurID 認証モジュールおよびヘルパーに対して使用します。

- `unixHelper.ipaddrs`

  値はインストールの間に設定されます。`amserver` スクリプトによって読み込まれ、ヘルパーの起動時に UNIX ヘルパーに渡される IP アドレスのリストを指定します。このプロパティーには、IPv4 形式の信頼 IP アドレスをスペースで区切ったリストを指定できます。

- `unixHelper.port`

  デフォルト値は `58946` です。UNIX 認証モジュールタイプで使用されます。

アイデンティティー連携

- com.sun.identity.federation.alliance.cache.enabled

  デフォルト値は true です。true の場合、連携メタデータは内部的にキャッシュされます。

- com.sun.identity.federation.fedCookieName

  デフォルト値は fedCookie です。連携サービス Cookie の名前を指定します。

- com.sun.identity.federation.proxyfinder

  デフォルト値は com.sun.identity.federation.services.FSIDPProxyImpl です。プロキシする優先アイデンティティープロバイダを見つけるための実装を定義します。

- com.sun.identity.federation.services.signingOn

  デフォルト値は false です。Liberty 要求および応答の署名検証のレベルを指定します。

  true　Liberty 要求および応答は送信時に署名され、受け取られた Liberty 要求および応答は署名の有効性が検証されます。

  false　送受信される Liberty 要求および応答の署名の検証は行われません。

  optional　Liberty 要求および応答は、連携プロファイルによって要求された場合にのみ署名または検証されます。

- com.sun.identity.password.deploymentDescriptor

  値はインストールの間に設定されます。例: /ampassword

- com.sun.identity.policy.Policy.policy_evaluation_weights

  デフォルト値は 10:10:10 です。ポリシーの対象、ルール、および条件を評価するための比例処理コストを示します。指定された値は、ポリシーの対象、ルール、および条件が評価される順序に影響します。値は対象、ルール、および条件に対応する 3 つの整数を使って表されます。値はコロン (:) によって区切られます。区切られた各数値は、ポリシーの対象、ルール、および条件を評価するための比例処理コストを示します。

- com.sun.identity.session.application.maxCacheTime

  デフォルト値は 3 です。アプリケーションセッションの最長キャッシュ時間を分単位で指定します。デフォルトでは、このプロパティーを有効にしない限り、キャッシュの期限切れはありません。

- com.sun.identity.sm.ldap.enableProxy

  デフォルト値は false です。接続に使用する Proxy Server を指定します。バックエンドストレージで LDAPProxy がサポートされている場合、true に設定します。true の場合、接続に Proxy Server を使用します。false の場合、接続にプロキシは使用されません。

- com.sun.identity.webcontainer

  値はインストールの間に設定されます。例: WEB_CONTAINER

Web コンテナの名前を指定します。サーブレットまたは JSP は Web コンテナに依存してはいませんが、Access Manager は Servlet 2.3 API の `request.setCharacterEncoding()` を使用して、受信した英語以外の文字を正しくデコードします。Access Manager が Sun Java System Web Server 6.1 上に配備される場合、これらの API は機能しません。Access Manager は、Sun Java System Web Server バージョン 6.1 および S1AS7.0 において、`gx_charset` メカニズムを使用して受信データを正しくデコードします。指定できる値は `BEA6.1`、`BEA 8.1`、`IBM5.1`、または `IAS7.0` です。Web コンテナが Sun Java System Web Server の場合、タグは置換されません。

JSS プロキシ

これらのプロパティーは、SSL `ApprovalCallback` の値を識別します。`checkSubjectAltName` または `resolveIPAddress` 機能が有効な場合、`com.iplanet.am.admin.cli.certdb.prefix` のプレフィックス値を使用して、`com.iplanet.am.admin.cli.certdb.dir` ディレクトリに `cert7.db` および `key3.db` を作成する必要があります。その後、Access Manager を再起動します。

- `com.iplanet.am.jssproxy.checkSubjectAltName`

  デフォルト値は `false` です。このプロパティーを有効にすると、サーバー証明書に対象代替名 (`SubjectAltName`) 拡張が取り込まれ、Access Manager はこの拡張に含まれるすべての名前エントリを確認します。`SubjectAltName` 拡張に含まれる名前のいずれかがサーバー FQDN と一致する場合には、Access Manager は SSL ハンドシェークを継続します。このプロパティーを有効にするには、信頼できる FQDN のコンマ区切りのリストにこのプロパティーを設定します。次に例を示します。

  ```
  com.iplanet.am.jssproxy.checkSubjectAltName=
  amserv1.example.com,amserv2.example.com
  ```

- `com.iplanet.am.jssproxy.resolveIPAddress`

  デフォルト値は `false` です。

- `com.iplanet.am.jssproxy.trustAllServerCerts`

  デフォルト値は `false` です。このプロパティーを `true` に設定すると、Access Manager は名前の競合などの証明書関連の問題をすべて無視し、SSL ハンドシェークを継続します。セキュリティーが低下しないようにするために、このプロパティーを有効にするのは、テストを目的として使用する場合、またはエンタープライズネットワークが厳格に制御されている場合だけにします。セキュリティーが低下する可能性がある場合 (たとえば、あるサーバーが別のネットワークのサーバーに接続する場合) は、このプロパティーを有効にすることは避けてください。

- `com.iplanet.am.jssproxy.SSLTrustHostList`設定された場合、Access Manager は、アクセス対象のサーバーホストに対してプラットフォームサーバーリストを検査します。プラットフォームサーバーリストに含まれる 2 つのサーバーの完全修飾ドメイン名が一致する場合、Access Manager は SSL ハンドシェークを継続します。このプロパティーを設定するには、次の構文を使用します。

com.iplanet.am.jssproxy.SSLTrustHostList = *fqdn_am_server1* ,*fqdn_am_server2*, *fqdn_am_server3*

- com.sun.identity.jss.donotInstallAtHighestPriority

  デフォルト値は false です。JSS が最も高い優先度で JCE に追加されるかどうかを決定します。デジタル署名と暗号化にほかの JCE プロバイダを使用することが望ましい場合、true に設定します。

LDAP 接続

- com.iplanet.am.ldap.connection.delay.between.retries

  デフォルト値は 1000 です。再試行の間隔をミリ秒単位で指定します。

- com.iplanet.am.ldap.connection.ldap.error.codes.retries

  デフォルト値は 80,81,91 です。LDAP 接続の再試行を開始する LDAPException エラーコードを指定します。

- com.iplanet.am.ldap.connection.num.retries

  デフォルト値は 3 です。LDAP 接続の再試行回数として許可する回数を指定します。

Liberty Alliance 対話

- com.sun.identity.liberty.interaction.htmlStyleSheetLocation

  値はインストールの間に設定されます。例: /opt/SUNWam/lib/is-html.xsl

  対話ページを HTML で描画するスタイルシートのパスを指定します。

- com.sun.identity.liberty.interaction.wmlStyleSheetLocation

  値はインストールの間に設定されます。例: /opt/SUNWam/lib/is-wml.xsl

  対話ページを WML で描画するスタイルシートのパスを指定します。

- com.sun.identity.liberty.interaction.wscSpecifiedInteractionChoice

  デフォルト値は interactIfNeeded です。Web サービスコンシューマが対話に参加するかどうかを示します。指定できる値は次のとおりです。

interactIfNeeded	必要な場合にのみ対話します。無効な値が指定された場合にも使用されます。
doNotInteract	対話しません。
doNotInteractForData	データの場合は対話しません。

- com.sun.identity.liberty.interaction.wscSpecifiedMaxInteractionTime

デフォルト値は 80 です。許容可能な対話の持続期間に関する、Web サービスコンシューマの設定。値は秒単位で表されます。値が指定されないか、整数以外の値が指定された場合、デフォルト値が使用されます。

- com.sun.identity.liberty.interaction.wscWillEnforceHttpsCheck

  デフォルト値は yes です。URL にリダイレクトされる要求が HTTPS を使用するという要件を、Web サービスコンシューマが強制するかどうかを示します。有効な値は yes および no です。大文字と小文字は区別されません。Liberty 仕様に従う場合、値 yes を指定する必要があります。値を指定しない場合、デフォルト値が使用されます。

- com.sun.identity.liberty.interaction.wscWillInlcudeUserInteractionHeader

  デフォルト値は yes です。値を指定しない場合、デフォルト値が使用されます。Web サービスコンシューマが userInteractionHeader をインクルードするかどうかを示します。指定できる値は yes および no です。大文字と小文字は区別されません。

- com.sun.identity.liberty.interaction.wscWillRedirect

  デフォルト値は yes です。Web サービスコンシューマが、対話のためにユーザーをリダイレクトするかどうかを示します。有効な値は yes および no です。値を指定しない場合、デフォルト値が使用されます。

- com.sun.identity.liberty.interaction.wspRedirectHandler

  値はインストールの間に設定されます。例:
  http://*hostName.domainName*.com:*portNumber*/amserver/WSPRedirectHandler

  ユーザーエージェントのリダイレクトに基づいて Liberty WSF WSP リソース所有者対話を処理するために WSPRedirectHandlerServlet が使用する URL を指定します。これは通常、Liberty サービスプロバイダが動作しているのと同じ JVM 内で動作しています。

- com.sun.identity.liberty.interaction.wspRedirectTime

  デフォルトは 30 です。Web サービスプロバイダの対話の予測期間です。単位は秒です。値が指定されないか、整数以外の値が指定された場合、デフォルト値が使用されます。

- com.sun.identity.liberty.interaction.wspWillEnforceHttpsCheck

  デフォルト値は yes です。値を指定しない場合、デフォルト値が使用されます。returnToURL が HTTPS を使用するという要件を、Web サービスコンシューマが強制するかどうかを示します。有効な値は yes および no です。大文字と小文字は区別されません。Liberty 仕様に従う場合、値 yes を指定する必要があります。

- com.sun.identity.liberty.interaction.

  wspWillEnforceReturnToHostEqualsRequestHost

  Liberty 仕様に従う場合、値 yes を指定する必要があります。returnToHost と requestHost が一致することを Web サービスコンシューマが強制するかどうかを示します。有効な値は yes および no です。

- com.sun.identity.liberty.interaction.wspWillRedirect

デフォルトは yes です。値を指定しない場合、デフォルト値が使用されます。Web サービスプロバイダが、対話のためにユーザーをリダイレクトするかどうかを示します。有効な値は yes および no です。大文字と小文字は区別されません。

- com.sun.identity.liberty.interaction.wspWillRedirectForData

  デフォルト値は yes です。値を指定しない場合、デフォルト値が使用されます。Web サービスプロバイダが、データの対話のためにユーザーをリダイレクトするかどうかを示します。有効な値は yes および no です。大文字と小文字は区別されません。

- com.sun.identity.liberty.ws.interaction.enable

  デフォルト値は false です。

- com.sun.identity.liberty.ws.jaxb.namespacePrefixMappingList

  デフォルト値は

  ```
  =S=http://schemas.xmlsoap.org/soap/envelope/|sb=urn:liberty:sb:2003-08
  |pp=urn:liberty:id-sis-pp:2003-08|ispp=http://www.sun.com/identity/
  liberty/pp|is=urn:liberty:is:2003-08
  ```

  です。JAXB コンテンツツリーを DOM ツリーに整列化するときに使用されるネームスペースプレフィックスマッピングを指定します。構文は「prefix=namespace|prefix=namespace|...」です。

- com.sun.identity.liberty.ws.jaxb.packageList

  JAXBContext の構築時に使用される JAXB パッケージリストを指定します。各パッケージはコロン (:) で区切る必要があります。

- com.sun.identity.liberty.ws.security.TokenProviderImpl

  デフォルト値は com.sun.identity.liberty.ws.security.AMSecurityTokenProviderDescription です。

- com.sun.identity.liberty.ws.soap.certalias

  値はインストールの間に設定されます。Liberty SOAP バインディングのための SSL 接続で使用されるクライアント証明書エイリアス。

- com.sun.identity.liberty.ws.soap.messageIDCacheCleanupInterval

  デフォルト値は 60000 です。キャッシュクリーンアップイベントが開始するまでの経過時間をミリ秒単位で指定します。個々のメッセージは、メッセージの重複を避けるために個別の messageID を付与されてキャッシュに格納されます。受信時点からのメッセージの経過時間が staleTimeLimit の値を超えると、メッセージはキャッシュから削除されます。

- com.sun.identity.liberty.ws.soap.staleTimeLimit

  デフォルト値は 300000 です。メッセージが期限切れでもう信頼できないかどうかを決定します。メッセージのタイムスタンプを現在のタイムスタンプと比較して、ここで指定されたミリ秒単位の時間を超えて古い場合、メッセージは期限切れと判定されます。

- com.sun.identity.liberty.ws.soap.supportedActors

デフォルト値は http://schemas.xmlsoap.org/soap/actor/next です。サポートされる SOAP アクターを指定します。個々のアクターはパイプ文字 (|) で区切る必要があります。

- com.sun.identity.liberty.ws.ta.certalias

  値はインストールの間に設定されます。SAML または応答メッセージの SAML ベアラー (BEARER) トークンに署名するために使用される、信頼できる発行局の証明書エイリアスを指定します。

- com.sun.identity.liberty.ws.wsc.certalias

  値はインストールの間に設定されます。この Web サービスクライアントに対して Web サービスセキュリティートークンを発行するためのデフォルトの証明書エイリアスを指定します。

- com.sun.identity.liberty.ws.ta.certalias

  値はインストールの間に設定されます。SAML または応答メッセージの SAML ベアラー (BEARER) トークンに署名するために使用される、信頼できる発行局の証明書エイリアスを指定します。

- com.sun.identity.liberty.ws.trustedca.certaliases

  値はインストールの間に設定されます。

  信頼できる CA の証明書エイリアスを指定します。受信する要求の SAML または SAML ベアラー (BEARER) トークン。メッセージはこのリスト内の信頼 CA によって署名される必要があります。構文は次のとおりです。
  cert alias 1[:*issuer 1*]|*cert alias 2*[: *issuer 2*]|....
  例: myalias1:myissuer1|myalias2|myalias3:myissuer3
  値 issuer は、トークンが署名の内部に KeyInfo を持たないときに使用されます。トークンの発行者がこのリストに存在している必要があり、署名の検証には対応する証明書エイリアスが使用されます。KeyInfo が存在する場合、KeyInfo が一致する証明書エイリアスがキーストアに含まれている必要があり、証明書エイリアスがこのリストに存在する必要があります。

- com.sun.identity.liberty.ws.security.TokenProviderImpl

  値はインストールの間に設定されます。セキュリティートークンプロバイダの実装を指定します。

- com.sun.identity.saml.removeassertion

  デフォルト値は true です。参照解除された表明をキャッシュから削除するかどうかを示すフラグ。作成されてアーティファクトと関連付けられ、参照解除されている表明に適用されます。

ログサービス

- com.iplanet.am.logstatus

  ログを記録する (ACTIVE) か、記録しない (INACTIVE) かを指定します。値はインストールの間に ACTIVE に設定されます。

AMConfig.properties に追加できるログプロパティー

特定のログファイルに記録するログの詳細レベルは、AMConfig.properties ファイルに属性を追加することで設定できます。次の形式を使用します。

iplanet-am-logging.*logfileName* .level=*java.util.logging.Level*。*logfileName* は Access Manager サービスのログファイルの名前 (表1 を参照)、*java.util.logging.Level* は設定する属性値です。Access Manager サービスでは、INFO レベルでログが記録されます。SAML サービスおよびアイデンティティー連携サービスでは、より詳細なレベル (FINE、FINER、FINEST) でログを記録することもできます。例:

```
iplanet-am-logging.amSSO.access.level=FINER
```

特定のログファイルへのログの記録を無効にすることもできます。例:

```
iplanet-am-logging.amConsole.access.evel=OFF
```

表 A–1 Access Manager のログファイル

ログファイル名	記録されるログ
amAdmin.access	成功した amadmin コマンド行イベント
amAdmin.error	amadmin コマンド行のエラーイベント
amAuthLog.access	Access Manager ポリシーエージェント関連のイベント。この表に続く注を参照してください。
amAuthentication.access	成功した認証イベント
amAuthentication.error	認証の失敗
amConsole.access	コンソールイベント
amConsole.error	コンソールエラーイベント
amFederation.access	成功した連携イベント
amFederation.error	連携エラーイベント
amPolicy.access	ポリシー許可の格納イベント

表 A–1 Access Manager のログファイル　(続き)

ログファイル名	記録されるログ
amPolicy.error	ポリシー拒否の格納イベント
amSAML.access	成功した SAML イベント
amSAML.error	SAML エラーイベント
amLiberty.access	成功した Liberty イベント
amLiberty.error	Liberty エラーイベント
amSSO.access	シングルサインオンの作成と破棄
amSSO.error	シングルサインオンエラーイベント

注 – amAuthLog ファイルの名前は、AMAgent.properties のポリシーエージェントプロパティーによって決まります。Web ポリシーエージェントのプロパティーは、com.sun.am.policy.agents.config.remote.log です。J2EE ポリシーエージェントのプロパティーは、com.sun.identity.agents.config.remote.logfile です。デフォルトは amAuthLog.*host.domain.port* です。*host.domain* はポリシーエージェント Web サーバーを実行するホストの完全修飾ホスト名、*port* はその Web サーバーのポート番号です。複数のポリシーエージェントを配備している場合は、このファイルの複数のインスタンスを作成できます。Web エージェントおよび J2EE エージェントの場合には、com.sun.identity.agents.config.audit.accesstype プロパティーによって、どのデータのログをネットワーク経由で記録するが決まります。たとえば、ポリシー許可だけ、ポリシー拒否だけ、またはポリシー許可とポリシー拒否の両方を記録することができます。また、ポリシー許可およびポリシー拒否の両方を記録しないこともできます。

ネームサービス

- com.iplanet.am.naming.failover.url

  このプロパティーは Access Manager 7.0 では使用されなくなりました。

- com.iplanet.am.naming.url

  値はインストールの間に設定されます。例:
  http://*hostName.domainName*.com:*portNumber*/amserver/namingservice

  使用するネームサービス URL を指定します。

通知サービス

通知スレッドプールを設定するには、次のキーを使用します。

- com.iplanet.am.notification.threadpool.size

  デフォルト値は 10 です。スレッドの総数を指定することによって、プールのサイズを定義します。

- com.iplanet.am.notification.threadpool.threshold

  デフォルト値は 100 です。タスクキューの最大の長さを指定します。

  到着した通知タスクは処理のためにタスクキューに送られます。キューが最大の長さに達すると、キューに空きができるまで以後の着信要求は拒絶され、ThreadPoolException が返されます。

- com.iplanet.am.notification.url

  値はインストールの間に設定されます。例: http://*hostName.domainName*.com:*portNumber*/amserver/notificationservice

ポリシーエージェント

- com.iplanet.am.policy.agents.url.deploymentDescriptor

  値はインストールの間に設定されます。例: AGENT_DEPLOY_URI

- com.sun.identity.agents.app.username

  デフォルト値は UrlAccessAgent です。アプリケーション認証モジュールで使用するユーザー名を指定します。

- com.sun.identity.agents.cache.size

  デフォルト値は 1000 です。リソース結果キャッシュのサイズを指定します。キャッシュはポリシーエージェントがインストールされたサーバー上に作成されます。

- com.sun.identity.agents.header.attributes

  デフォルト値は「cn,ou,o,mail,employeenumber,c」です。ポリシー評価によって返されるポリシー属性を指定します。 a[,...] の形式を使用します。この例で、a はフェッチされるデータストア内の属性です。

- com.sun.identity.agents.logging.level

  デフォルト値は NONE です。ポリシークライアント API のログレベルの詳細度を制御します。デフォルト値は NONE です。指定できる値は次のとおりです。

  ALLOW　アクセスが許可された要求をログに記録します。

  DENY　アクセスが拒否された要求をログに記録します。

  BOTH　アクセスが許可された要求とアクセスが拒否された要求の両方をログに記録します。

NONE　　要求をログに記録しません。

- com.sun.identity.agents.notification.enabled

  デフォルト値は false です。ポリシークライアント API の通知を有効または無効にします。

- com.sun.identity.agents.notification.url

  ポリシークライアント SDK がポリシー変更通知を登録するために使用します。このプロパティーを正しく設定しないと、ポリシー通知が無効になります。

- com.sun.identity.agents.polling.interval

  デフォルト値は 3 です。この時間の経過後にエントリがクライアント API キャッシュから削除されるポーリング間隔を分単位で指定します。

- com.sun.identity.agents.resource.caseSensitive

  デフォルト値は false です。

  ポリシー評価の間に大文字と小文字の区別を有効にするか無効にするかを指定します。

- com.sun.identity.agents.true.value

  ポリシーアクションの true 値を示します。アプリケーションが PolicyEvaluator.isAllowed メソッドにアクセスする必要がない場合、この値は無視できます。この値によって、Access Manager が決定したポリシーをどのように解釈するかが決まります。デフォルト値は allow です。

- com.sun.identity.agents.resource.comparator.class

  デフォルト値は com.sun.identity.policy.plugins.URLResourceName です。

  リソース比較クラス名を指定します。指定できる実装クラスは、com.sun.identity.policy.plugins.PrefixResourceName および com.sun.identity.policy.plugins.URLResourceName です。

- com.sun.identity.agents.resource.delimiter

  デフォルト値はバックスラッシュ (/) です。リソース名の区切り文字を指定します。

- com.sun.identity.agents.resource.wildcard

  デフォルト値は * です。リソース名のワイルドカードを指定します。

- com.sun.identity.agents.server.log.file.name

  デフォルト値は amRemotePolicyLog です。Access Manager へのメッセージをログに記録するために使用するログファイルの名前を指定します。ファイルの名前だけが必要です。ファイルのディレクトリ名は、ほかの Access Manager 設定によって決定されます。

- com.sun.identity.agents.use.wildcard

  デフォルト値は true です。リソース名比較にワイルドカードを使用するかどうかを示します。

ポリシークライアント API

- com.sun.identity.policy.client.booleanActionValues

  iPlanetAMWebAgentService|POST|allow|deny

  デフォルト値は iPlanetAMWebAgentService|GET|allow|deny: です。

  ポリシーアクション名に対するブール型のアクション値を指定します。serviceName|actionName|trueValue|falseValue の形式を使用します。アクション名の値はコロン (:) で区切られます。

- com.sun.identity.policy.client.cacheMode

  デフォルト値は self です。クライアントポリシー評価のキャッシュモードを指定します。有効な値は subtree および self です。subtree に設定した場合、ポリシー評価は、実際に要求されたリソースのルートからのすべてのリソースについて、サーバーからポリシー決定を取得します。self に設定した場合、ポリシー評価は、実際に要求されたリソースのみについて、サーバーからポリシー決定を取得します。

- com.sun.identity.policy.client.clockSkew

  ポリシークライアントマシンとポリシーサーバーの間の時刻のずれを調整します。このプロパティーが存在せず、ポリシーエージェントの時刻がポリシーサーバーの時刻と異なる場合、誤ったポリシー決定が取得される場合があります。時刻同期サービスを実行して、ポリシーサーバーとポリシークライアントの時刻をできるだけ一致させる必要があります。このプロパティーは、時刻同期サービスの実行とは無関係に小さな時刻のずれの調整を行うために使用します。ポリシーエージェントの時刻からポリシーサーバーの時刻を引いた値を秒単位で指定します。ポリシーサーバー上でプロパティーをコメントアウトします。ポリシークライアントマシンまたはポリシーエージェントを実行しているマシン上で、行のコメントアウトを解除し、適切な値 (エージェントとサーバのクロック差、秒単位) を設定します。

- com.sun.identity.policy.client.resourceComparators=

  serviceType=iPlanetAMWebAgentService|class=

  異なるサービス名に対して使用される ResourceComparators を指定します。Access Manager コンソールから値をコピーします。「サービス設定」、「ポリシー設定」、「グローバル: リソースコンパレータ」の順に選択します。Access Managerからの複数の値は、区切り文字としてコロン (:) を使って連結します。

- com.sun.identity.policy.plugins.URLResourceName|wildcard

  デフォルト値は *|delimiter=/|caseSensitive=trueDescription です。

プロファイルサービス

- com.iplanet.am.profile.host

  このプロパティーは Access Manager 7 では使用されなくなりました。下位互換性のためにのみ提供されています。値はインストールの間に設定されます。例: *hostName.domainName*.com

- com.iplanet.am.profile.port

  このプロパティーは Access Manager 7 では使用されなくなりました。下位互換性のためにのみ提供されています。値はインストールの間に設定されます。例: **80**

レプリケーション

レプリケーションの設定には次のキーを使用します。

- com.iplanet.am.replica.delay.between.retries

  デフォルト値は **1000** です。再試行間隔をミリ秒単位で指定します。

- com.iplanet.am.replica.num.retries

  デフォルト値は **0** です。再試行の回数を指定します。

SAML サービス

- com.sun.identity.saml.assertion.version

  デフォルト値は 1.1 です。使用するデフォルトの SAML バージョンを指定します。指定できる値は 1.0 または 1.1 です。

- com.sun.identity.saml.checkcert

  デフォルト値は on です。KeyInfo に埋め込まれた証明書を、キーストア内の証明書と照合チェックするためのフラグ。キーストア内の証明書は、com.sun.identity.saml.xmlsig.keystore プロパティーによって指定されます。指定できる値は次のとおりです。on または off です。フラグが「on」の場合、*XML 署名検証のために*証明書がキーストア内に存在する必要があります。フラグが「off」の場合、*存在チェックをスキップします。*/

  on　　XML 署名検証のために、証明書がキーストア内に存在する必要があります。

  off　　存在チェックを無視します。

- com.sun.identity.saml.protocol.version

  デフォルト値は 1.1 です。使用するデフォルトの SAML バージョンを指定します。指定できる値は 1.0 または 1.1 です。

- com.sun.identity.saml.removeassertion

- com.sun.identity.saml.request.maxContentLength

  デフォルト値は 16384 です。SAML で使用される HTTP Request の最大コンテンツ長を指定します。

- com.sun.identity.saml.xmlsig.certalias

  デフォルト値は test です。

- com.sun.identity.saml.xmlsig.keypass

  値はインストールの間に設定されます。例: /etc/opt/SUNWam/config/.keypass

  SAML XML キーパスワードファイルのパスを指定します。

- com.sun.identity.saml.xmlsig.keystore

  値はインストールの間に設定されます。例: /etc/opt/SUNWam/config/keystore.jks

  SAML XML キーストアパスワードファイルのパスを指定します。

- com.sun.identity.saml.xmlsig.storepass

  値はインストールの間に設定されます。例: /etc/opt/SUNWam/config/.storepass

  SAML XML キーストアパスファイルのパスを指定します。

セキュリティー

- com.iplanet.security.encryptor

  デフォルト値は com.iplanet.services.util.JSSEncryption です。暗号化クラス実装を指定します。指定できるクラスは com.iplanet.services.util.JCEEncryption および com.iplanet.services です。util.JSSEncryption.

- com.iplanet.security.SecureRandomFactoryImpl

  デフォルト値は com.iplanet.am.util.JSSSecureRandomFactoryImpl です。SecureRandomFactory のファクトリクラス名を指定します。指定できる実装クラスは com.iplanet.am.util.JSSSecureRandomFactoryImpl (JSS を使用する) および com.iplanet.am.util.SecureRandomFactoryImpl (ピュア Java を使用する) です。

- com.iplanet.security.SSLSocketFactoryImpl

  デフォルト値は com.iplanet.services.ldap.JSSSocketFactory です。LDAPSocketFactory のファクトリクラス名を指定します。指定できるクラスは com.iplanet.services.ldap.JSSSocketFactory (JSS を使用する) および netscape.ldap.factory.JSSESocketFactory (ピュア Java を使用する) です。

- com.sun.identity.security.checkcaller

  デフォルト値は false です。Access Manager に対し、Java セキュリティーマネージャーのアクセス権チェックを有効または無効にします。デフォルトでは無効です。有効にした場合、Access Manager が配備されたコンテナの Java ポリシーファイルに適切な変更を行う必要があります。これにより、Access Manager の JAR ファイルに、重要な操

作を実行するための信頼を付与することができます。詳細は、com.sun.identity.security についての Java API リファレンス (Javadoc) エントリを参照してください。

- am.encryption.pwd

  値はインストールの間に設定されます。例: dSB9LkwPCSoXfIKHVMhIt3bKgibtsggd

  パスワードを暗号化および復号化するために使用されるキーを指定します。

セッションサービス

- com.iplanet.am.clientIPCheckEnabled

  デフォルト値は false です。すべての SSOToken の作成または検証において、クライアントの IP アドレスがチェックされるかどうかを指定します。

- com.iplanet.am.session.client.polling.enable

  これは読み取り専用のプロパティーです。プロパティー値を変更しないでください。

  デフォルト値は false です。クライアント側セッションのポーリングを有効にします。セッションポーリングモードとセッション通知モードは同時に有効にできません。ポーリングモードが有効になっている場合は、セッション通知が自動的に無効になります。セッション通知が有効になっている場合は、ポーリングモードが自動的に無効になります。

- com.iplanet.am.session.client.polling.period

  デフォルト値は 180 です。ポーリング期間を秒単位で指定します。

- com.iplanet.am.session.httpSession.enabled

  デフォルト値は true です。httpSession の使用を有効または無効にします。

- com.iplanet.am.session.invalidsessionmaxtime

  デフォルト値は 10 です。セッションが作成されてユーザーがログインしなくなった場合に、その無効なセッションがセッションテーブルから消去されるまでの時間を分単位で指定します。この値は、認証モジュールのプロパティーファイル内のタイムアウト値よりも常に大きくすることをお勧めします。

- com.iplanet.am.session.maxSessions

  デフォルト値は 5000 です。同時セッションの最大許容数を指定します。

  最大同時セッションの値がこの数値を超えた場合、ログインは最大セッションエラーを送出します。

- com.iplanet.am.session.purgedelay

  デフォルト値は 60 です。パージセッション操作を遅延する時間を分単位で指定します。

これは、セッションのタイムアウト後に、セッションがセッションサーバー内にとどまり続ける延長時間です。このプロパティーは、セッションがタイムアウトしたかどうかをチェックするために、SSO API 経由でクライアントアプリケーションによって使用されます。この延長期間が終了すると、セッションは破棄されます。ユーザーがログアウトする、またはセッションが Access Manager コンポーネントによって明示的に破棄される場合、セッションは延長期間の間保持されません。この延長期間の間、セッションは INVALID 状態です。

- `com.sun.am.session.caseInsensitiveDN`

  デフォルト値は `true` です。エージェント DN を比較します。値が `false` の場合、比較は大文字と小文字を区別します。

- `com.sun.am.session.enableHostLookUp`

  デフォルト値は `false` です。セッションロギングの間のホスト名解決を有効または無効にします。

SMTP

- `com.iplanet.am.smtphost`

  デフォルト値は `localhost` です。メールサーバーホストを指定します。

- `com.iplanet.am.smtpport`

  デフォルト値は `25` です。メールサーバーポートを指定します。

統計サービス

- `com.iplanet.am.stats.interval`

  デフォルト値は `60` です。統計ロギングの間隔を秒単位で指定します。最小値は 5 秒で、これは CPU の飽和状態を回避するための設定です。5 秒未満の値が指定された場合、Access Manager はこの値を 5 秒と認識します。

- `com.iplanet.services.stats.directory`

  値はインストールの間に設定されます。例: `/var/opt/SUNWam/stats` デバッグファイルが作成されるディレクトリを指定します。

- `com.iplanet.services.stats.state`

  デフォルト値は `file` です。統計ログの場所を指定します。指定できる値は次のとおりです。

  `off` 統計はログに記録されません。

  `file` 統計は指定されたディレクトリ下のファイルに書き込まれます。

  `console` 統計は Web Server のログファイルに書き込まれます。

◆ ◆ ◆ 付 録 B

serverconfig.xml ファイル

serverconfig.xml ファイルは、Sun Java™ System Access Manager のデータストアとして使用される Directory Server に関する設定の情報を提供します。この章では、ファイルの要素、フェイルオーバーのためにファイルを設定する方法、複数のインスタンスを定義する方法、コンソールの配備を取り消す方法、コンソールファイルをサーバーから削除する方法について説明します。この章は、次の節で構成されています。

概要

serverconfig.xml は / *AccessManager-base* /SUNWam/config/ums ディレクトリにあります。このファイルには、Directory Server への LDAP 接続プールを確立するために Identity SDK が使用するパラメータが格納されます。このファイルは、製品の他の機能が使用することはありません。このファイルでは 2 つのユーザーが定義されます。user1 は Directory Server プロキシユーザーであり、user2 は Directory Server 管理者です。

プロキシユーザー

プロキシユーザーは、任意のユーザーの権限 (たとえば、組織管理者またはエンドユーザー) を獲得することができます。プロキシユーザーにバインドされた接続とともに接続プールが作成されます。Access Manager は、cn=puser,ou=DSAME Users,dc=example,dc=com というDN でプロキシ ユーザーを作成します。このユーザーは、Directory Server に対して行われるすべてのクエリーに使用されます。プロキシユーザーは、Directory Server ですでに設定されているプロキシユーザー ACI を利用するので、必要なときにユーザーに代わってアクションを実行できます。プロキシユーザーは、すべてのクエリー (サービス設定や組織情報の取得など) の受け渡し経路となる開いた接続を維持します。プロキシユーザーのパスワードは常に暗号化されます。263 ページの「プロキシユーザー」は、serverconfig.xml に格納された暗号化パスワードの例を示しています。

例 B–1 serverconfig.xml でのプロキシユーザーの定義

```
<User name="User1" type="proxy">
<DirDN>
cn=puser,ou=DSAME Users,dc=example,dc=com
</DirDN>
<DirPassword>
AQICkc3qIrCeZrpexyeoL4cdeXih4vv9aCZZ
</DirPassword>
</User>
```

管理ユーザー

管理ユーザーは、Access Manager SDK が、特定のユーザーにリンクされていない操作 (サービス設定情報の取得など) を Directory Server に対して実行するときにバインド目的で使用されます。263 ページの「プロキシユーザー」はこれらの操作を管理ユーザーの代わりに実行しますが、バインドではまず管理ユーザーの資格を検証する必要があります。インストールの間に、Access Manager は `cn=dsameuser,ou=DSAME Users,dc=example,dc=com` を管理ユーザーとして作成します。263 ページの「プロキシユーザー」は、`serverconfig.xml` に格納された、`dsameuser` の暗号化パスワードの例を示しています。

例 B–2 serverconfig.xml での管理ユーザーの定義

```
<User name="User2" type="admin">
<DirDN>
cn=dsameuser,ou=DSAME Users,dc=example,dc=com
</DirDN>
<DirPassword>
AQICkc3qIrCeZrpexyeoL4cdeXih4vv9aCZZ
</DirPassword>
</User>
```

server-config の文書型定義

server-config.dtd は、serverconfig.xml の構造を定義します。このファイルは *AccessManager-base* /SUNWam/dtd ディレクトリにあります。この節では、DTD の主な要素を定義します。266 ページの「MiscConfig 要素」は serverconfig.xml ファイルの例です。

iPlanetDataAccessLayer 要素

iPlanetDataAccessLayer はルート要素です。この要素では、XML ファイルごとに複数のサーバーグループを定義できます。この要素の直接のサブ要素は265 ページの「ServerGroup 要素」です。この要素には属性はありません。

ServerGroup 要素

ServerGroup は、1 つまたは複数のディレクトリサーバーへのポインタを定義します。ディレクトリサーバーの種類は、マスターサーバーまたはレプリカサーバーのいずれかです。*ServerGroup* を修飾するサブ要素には、265 ページの「Server 要素」、266 ページの「User 要素」、266 ページの「BaseDN 要素」、および266 ページの「MiscConfig 要素」があります。*ServerGroup* の XML 属性は、サーバーグループの名前、LDAP 接続プールに対して開くことのできる接続の最小数 (1) を定義する *minConnPool*、および、最大数 (10) を定義する *maxConnPool* です。複数の ServerGroup 要素の定義はサポートされていません。

注 – Access Manager は、Directory Server にアクセスするために接続プールを使用します。すべての接続は Access Manager の起動時に開かれ、以後閉じられることはありません。接続は再利用されます。

Server 要素

Server は特定の Directory Server インスタンスを定義します。サブ要素はありません。*Server* の必須 XML 属性は、ユーザーにわかりやすいサーバーの名前、ホスト名、Directory Server が動作するポート番号、および、開かれる必要のある LDAP 接続のタイプ (シンプルまたは SSL) です。

注 – Server 要素を使った自動フェイルオーバーの例については、267 ページの「フェイルオーバーまたは複数マスター設定」を参照してください。

User 要素

User には、Directory Server インスタンスに対するユーザー設定を定義するサブ要素が含まれます。*User* を修飾するサブ要素には、*DirDN* および *DirPassword* があります。この要素の必須 XML 属性は、ユーザーの名前とユーザーのタイプです。*type* の値は、ユーザーの権限と、Directory Server インスタンスに対して開かれる接続のタイプを識別します。以下のオプションがあります。

- auth— Directory Server に対して認証されるユーザーを定義します。
- proxy— Directory Server プロキシユーザーを定義します。詳細は、263 ページの「プロキシユーザー」を参照してください。
- rebind: 再バインドに使用できる資格を持つユーザーを定義します。
- admin— Directory Server の管理権限を持つユーザーを定義します。詳細は、264 ページの「管理ユーザー」を参照してください。

DirDN 要素

DirDN には、定義されたユーザーの LDAP 識別名 (DN) が含まれます。

DirPassword 要素

DirPassword には、定義されたユーザーの暗号化されたパスワードが含まれます。

注意 – 重要な点として、パスワードと暗号化鍵は配備単位全体で一貫した状態に保たれます。たとえば、この要素で定義されるパスワードは Directory Server にも格納されます。1 つの場所でパスワードを変更する場合、両方の場所でそのパスワードを更新する必要があります。また、このパスワードは暗号化されます。`am.encryption.pwd` プロパティーで定義された暗号化鍵が変更される場合、`serverconfig.xml` 内のすべてのパスワードを「`ampassword --encrypt` パスワード」を使用して再暗号化する必要があります。

BaseDN 要素

BaseDN は、サーバーグループのベース識別名 (DN) を定義します。サブ要素および XML 属性はありません。

MiscConfig 要素

MiscConfig は、キャッシュサイズなどの任意の LDAP JDK 機能を定義するためのプレースホルダーです。サブ要素はありません。この要素の必須の XML 属性は、機能の名前とその定義値です。

例 B–3 serverconfig.xml

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!--
 Copyright (c) 2002 Sun Microsystems, Inc. All rights reserved.

 Use is subject to license terms.

-->
<iPlanetDataAccessLayer>
        <ServerGroup name="default" minConnPool="1" maxConnPool="10">
                <Server name="Server1" host="
               ishost.domain_name" port="389"
type="SIMPLE" />
                <User name="User1" type="proxy">
                        <DirDN>
                                cn=puser,ou=DSAME Users,dc=example,dc=com
                        </DirDN>
                        <DirPassword>
                                AQICkc3qIrCeZrpexyeoL4cdeXih4vv9aCZZ
                        </DirPassword>
                </User>
                <User name="User2" type="admin">
                        <DirDN>
                                cn=dsameuser,ou=DSAME Users,dc=example,dc=com
                        </DirDN>
                        <DirPassword>
                                AQICkc3qIrCeZrpexyeoL4cdeXih4vv9aCZZ
                        </DirPassword>
                </User>
                <BaseDN>
                        dc=example,dc=com
                </BaseDN>
        </ServerGroup>
</iPlanetDataAccessLayer>
```

フェイルオーバーまたは複数マスター設定

Access Manager では、`serverconfig.xml` 内で 265 ページの「ServerGroup 要素」、265 ページの「Server 要素」 として定義された任意の Directory Server への自動フェイルオーバーが可能です。フェイルオーバー目的または複数マスターのために、複数のサーバーを設定できます。設定された最初のサーバーがダウンすると、設定された 2 番目のサーバーが処理を引き継ぎます。267 ページの「フェイルオーバーまたは複数マスター設定」 では、`serverconfig.xml` での自動フェイルオーバー設定の例を示しています。

例 B–4 serverconfig.xml でのフェイルオーバー設定

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="yes"?>
<!--
PROPRIETARY/CONFIDENTIAL. Use of this product is subject to license terms.
Copyright 2002 Sun Microsystems, Inc. All rights reserved.
-->
<iPlanetDataAccessLayer>
     <ServerGroup name="default" minConnPool="1" maxConnPool="10">
          <Server name="Server1" host="
            amhost1.domain_name" port="389" type="SIMPLE" />
          <Server name="Server2" host="
            amhost2.domain_name" port="389" type="SIMPLE" />
          <Server name="Server3" host="
            amhost3.domain_name" port="390" type="SIMPLE" />
          <User name="User1" type="proxy">
               <DirDN>
                    cn=puser,ou=DSAME Users,dc=example,dc=com
               </DirDN>
               <DirPassword>
                    AQIC5wM2LY4Sfcy+AQBQxghVwhBE92i78cqf
               </DirPassword>
          </User>
          <User name="User2" type="admin">
               <DirDN>
                    cn=dsameuser,ou=DSAME Users,dc=example,dc=com
               </DirDN>
               <DirPassword>
                    AQIC5wM2LY4Sfcy+AQBQxghVwhBE92i78cqf
               </DirPassword>
          </User>
          <BaseDN>
               o=isp
          </BaseDN>
     </ServerGroup>
</iPlanetDataAccessLayer>
```

◆ ◆ ◆ 付 録 C

ログファイルリファレンス

この付録には、Access Manager の各機能領域で使用されるログファイルを表形式でまとめてあります。この付録の表には、ログファイルの次の項目を記載しています。

- ID — ログ識別番号。
- ログレベル — そのメッセージのログレベル属性。
- 説明 — そのログメッセージの説明。
- データ — そのメッセージが関連付けられているデータの種類。
- 発生原因 — そのログファイルメッセージが発生した理由。
- 対処方法 — 詳細な情報が必要なときに行う操作。

ログファイルの定義と場所については、『Sun Java System Access Manager 7 2005Q4 Technical Overview』を参照してください。

表 C–1 amAdmin コマンド行ユーティリティーのログリファレンス

ID	ログレベル	説明	データ	発生原因	対処方法
1	INFO	ユーザーがログインに失敗しました。	ユーザー ID	ユーザーがログインに失敗しました。	
2 TEST	INFO	ADMIN EXCEPTION を受け取りました	要素名エラーメッセージ	Admin 要求の処理中に ADMIN EXCEPTION を受け取ったとき。	詳細な情報が必要な場合は、amAdmin デバッグファイルを調べてください。
3	INFO	セッションが破棄されました	ユーザーの名前	セッションが破棄されたとき。	

表 C–1 amAdmin コマンド行ユーティリティーのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
11	INFO	サービススキーマがロードされました	スキーマ名	サービススキーマを正常にロードしたとき。	
12	INFO	サービスが削除されました	サービス名	サービスを正常に削除したとき。	
13	INFO	属性が追加されました	属性名	属性が正常に追加されたとき。	
21	INFO	このサービスのポリシーがありません	サービス名	ポリシールールを削除するフラグが指定されたけれども、サービスのポリシーがなかったとき。	
22	INFO	サービスのポリシースキーマが見つかりません	サービス名	ポリシールールを削除するフラグが指定されたけれども、サービスのポリシースキーマが見つからなかったとき	
23	INFO	ポリシーのサービスを削除しています	サービス名	ポリシールールを削除するフラグが指定されたサービスを削除しているとき。	
24	INFO	ポリシーのサービスの削除が完了しました	サービス名	ポリシールールを削除するフラグが指定されたサービスを削除しているとき。	

表 C–1 amAdmin コマンド行ユーティリティーのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
25	INFO	組織にポリシーを作成しました	ポリシー名 組織 *DN*	組織 DN にポリシーを作成したとき。	
26	INFO	組織からポリシーを削除しました	ポリシー名 組織 *DN*	組織 DN からポリシーを削除したとき。	
31	INFO	ロケールのリソースバンドルを Directory Server に追加します	リソースバンドル名リソースロケール	ロケールのリソースバンドルが Directory Server に正常に格納されたとき。	
32	INFO	デフォルトのリソースバンドルを Directory Server に追加します	リソースバンドル名	デフォルトのリソースバンドルが Directory Server に正常に格納されたとき。	
33	INFO	ロケールのリソースバンドルを Directory Server から削除しました	リソースバンドル名リソースロケール	ロケールのリソースバンドルを Directory Server から正常に削除したとき。	
34	INFO	ロケールのデフォルトリソースバンドルを Directory Server から削除しました	リソースバンドル名	デフォルトのリソースバンドルを Directory Server から正常に削除したとき。	
41	INFO	サービスのサービススキーマを変更しました	サービスの名前	サービスのサービススキーマを正常に変更したとき。	
42	INFO	サービスのサービスサブスキーマを削除しました	サブスキーマの名前サービスの名前	サービスのサービスサブスキーマを正常に削除したとき。	

表 C–1 amAdmin コマンド行ユーティリティーのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
43	INFO	サービスサブスキーマをサービスに追加しました	サービスの名前	サービスサブスキーマをサービスに正常に追加したとき。	
44	INFO	サブ設定をサービスに追加しました	サブ設定の名前 サービスの名前	サブ設定をサービスに正常に追加したとき。	
45	INFO	サービスのサブ設定を変更しました	サブ設定の名前 サービスの名前	サービスのサブ設定を正常に変更したとき。	
46	INFO	サービスのサブ設定を削除しました	サブ設定の名前 サービスの名前	サービスのサブ設定を正常に削除したとき。	
47	INFO	サービスのすべてのサービス設定を削除しました。	サービスの名前	サービスのすべてのサービス設定を正常に削除したとき。	
91	INFO	組織のサービスサブ設定を変更します	サブ設定名 サービス名組織 *DN*	組織のサービスサブ設定を正常に変更したとき。	
92	INFO	サービスサブ設定を組織に追加しました	サブ設定名サービス名組織 *DN*	サービスサブ設定を組織に正常に追加したとき。	
93	INFO	組織のサービスサブ設定を削除しました	サブ設定名サービス名組織 *DN*	組織のサービスサブ設定を正常に削除したとき。	
94	INFO	リモートプロバイダを組織に作成しました	プロバイダ名組織 *DN*	リモートプロバイダを組織に正常に作成したとき。	

表 C–1 amAdmin コマンド行ユーティリティーのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
95	INFO	組織のリモートプロバイダを変更しました	プロバイダ名 組織 *DN*	組織のリモートプロバイダを正常に変更したとき。	
96	INFO	組織のホストプロバイダを変更しました。	プロバイダ名 組織 *DN*	組織のホストプロバイダを正常に変更したとき。	
97	INFO	ホストプロバイダを組織に作成しました	プロバイダ名 組織 *DN*	ホストプロバイダを組織に正常に作成したとき。	詳細な情報が必要な場合は、アイデンティティーリポジトリのログを調べてください。
98	INFO	組織のリモートプロバイダを削除しました	プロバイダ名 組織 *DN*	組織のリモートプロバイダを正常に削除したとき。	
99	INFO	認証ドメインを組織に作成しました	トラストサークルの名前 組織 *DN*	認証ドメインを組織に正常に作成したとき。	
100	INFO	組織の認証ドメインを削除しました。	トラストサークルの名前 組織 *DN*	組織の認証ドメインを正常に削除したとき。	
101	INFO	組織の認証ドメインを変更しました。	トラストサークルの名前 組織 *DN*	組織の認証ドメインを正常に変更したとき。	
102	INFO	サービステンプレートを変更しようとしています	サービステンプレートの DN	サービステンプレートを変更しようとしたとき。	
103	INFO	サービステンプレートを変更しました	サービステンプレートの DN	サービステンプレートを正常に変更したとき。	

表 C–1 amAdmin コマンド行ユーティリティーのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
104	INFO	サービステンプレートを消去しようとしています	サービステンプレートの DN	サービステンプレートを消去しようとしたとき。	
105	INFO	サービステンプレートを消去しました	サービステンプレートの DN	サービステンプレートを正常に消去したとき。	
106	INFO	サービステンプレートを追加しようとしています	サービステンプレートの DN	サービステンプレートを追加しようとしたとき。	
107	INFO	サービステンプレートを追加しました	サービステンプレートの DN	サービステンプレートを正常に追加したとき。	
108	INFO	入れ子グループをグループに追加しようとしています	追加するグループの名前包含するグループの *DN*	入れ子グループをグループに追加しようとしたとき。	
109	INFO	入れ子グループをグループに追加しました	追加するグループの名前包含するグループの *DN*	入れ子グループをグループに正常に追加したとき。	
110	INFO	ユーザーをグループまたはロールに追加しようとしています	ユーザーの名前追加先のグループまたはロール	ユーザーをグループまたはロールに追加しようとしたとき。	
111	INFO	ユーザーをグループまたはロールに追加しました	ユーザーの名前追加先のグループまたはロール	ユーザーをグループまたはロールに正常に追加したとき。	
112	INFO	エンティティーを作成しようとしています。	エンティティーの DN	エンティティーを作成しようとしたとき。	

表 C–1 amAdmin コマンド行ユーティリティーのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
113	INFO	エンティティーを作成しました。	エンティティーの地域対応された名前エンティティーの *DN*	エンティティーを作成しました。	
114	INFO	ロールを作成しようとしています	ロール DN	ロールを作成しようとしました。	
115	INFO	ロールを作成しました	ロールの名前	ロールを作成したとき。	
116	INFO	グループコンテナを作成しようとしています	グループコンテナの名前	グループコンテナを作成しようとしたとき。	
117	INFO	グループコンテナを作成します	グループコンテナの名前	グループコンテナを作成したとき。	
118	INFO	グループを作成しようとしています。	グループの名前	グループを作成しようとしたとき。	
119	INFO	グループを作成します。	グループの名前	グループを作成したとき。	
120	INFO	ピープルコンテナを作成しようとしています。	ピープルコンテナの DN	ピープルコンテナを作成しようとしたとき。	
121	INFO	ピープルコンテナを作成します。	ピープルコンテナの DN	ピープルコンテナを作成したとき。	
122	INFO	サービステンプレートを組織またはロールに作成しようとしています	サービステンプレートの名前組織またはロールの名前	サービステンプレートを組織またはロールに作成しようとしたとき。	

表 C–1 amAdmin コマンド行ユーティリティーのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
123	INFO	サービステンプレートを組織またはロールに作成します	サービステンプレートの名前組織またはロールの名前	サービステンプレートを組織またはロールに作成したとき。	
124	INFO	コンテナを作成しようとしています	コンテナの名前	コンテナを作成しようとしたとき。	
125	INFO	コンテナを作成します。	コンテナの名前	コンテナを作成したとき。	
126	INFO	ユーザーを作成しようとしています。	ユーザーの名前	ユーザーを作成しようとしたとき。	
127	INFO	ユーザーを作成します。	ユーザーの名前	ユーザーを作成したとき。	
128	INFO	エンティティーを削除しようとしています。	エンティティーの DN	エンティティーを削除しようとしたとき。	
129	INFO	エンティティーを削除します。	エンティティーの地域対応された名前エンティティーの *DN*	エンティティーを削除したとき。	
130	INFO	ピープルコンテナを削除しようとしています	ピープルコンテナの DN	ピープルコンテナを削除しようとしたとき。	
131	INFO	ピープルコンテナを削除します	ピープルコンテナの DN	ピープルコンテナを削除したとき。	
132	INFO	ロールを削除しようとしています	ロールの名前	ロールを削除しようとしたとき。	
133	INFO	ロールを削除します	ロールの名前	ロールを削除したとき。	

表 C–1 amAdmin コマンド行ユーティリティーのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
134	INFO	組織のサービステンプレートを削除しようとしています	サービステンプレートの名前組織の名前	組織のサービステンプレートを削除しようとしたとき。	
135	INFO	組織のサービステンプレートを削除します	サービステンプレートの名前組織の名前	組織のサービステンプレートを削除したとき。	
136	INFO	コンテナを削除しようとしています。	コンテナの名前	コンテナを削除しようとしたとき。	
137	INFO	コンテナを削除します。	コンテナの名前	コンテナを削除したとき。	
138	INFO	エンティティーを変更しようとしています	エンティティーの地域対応された名前エンティティーの *DN*	エンティティーを変更しようとしたとき。	
139	INFO	エンティティーを変更します	エンティティーの地域対応された名前エンティティーの *DN*	エンティティーを変更したとき。	
140	INFO	ピープルコンテナを変更しようとしています。	ピープルコンテナの DN	ピープルコンテナを変更しようとしたとき。	
141	INFO	ピープルコンテナを変更します。	ピープルコンテナの DN	ピープルコンテナを変更したとき。	
142	INFO	コンテナを変更しようとしています。	コンテナの名前	コンテナを変更しようとしたとき。	
143	INFO	コンテナを変更します。	コンテナの名前	コンテナを変更したとき。	

表 C–1 amAdmin コマンド行ユーティリティーのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
144	INFO	サービスを組織に登録しようとしています。	サービスの名前組織の名前	サービスを組織に登録しようとしたとき	
145	INFO	サービスを組織に登録します。	サービスの名前組織の名前	サービスを組織に登録したとき	
146	INFO	サービスの登録を組織から解除しようとしています。	サービスの名前組織の名前	サービスの登録を組織から解除しようとしたとき	
147	INFO	サービスの登録を組織から解除します。	サービスの名前組織の名前	サービスの登録を組織から解除したとき	
148	INFO	グループの変更を試行します。	グループの名前	グループを変更しようとしました。	
149	INFO	グループを変更します。	グループの名前	グループを変更したとき	
150	INFO	入れ子グループをグループから消去しようとしています。	入れ子グループの名前グループの名前	入れ子グループをグループから消去しようとしたとき。	
151	INFO	入れ子グループをグループから消去します。	入れ子グループの名前グループの名前	入れ子グループをグループから消去したとき。	
152	INFO	グループを削除しようとしています	グループの名前	グループを削除しようとしたとき。	
153	INFO	グループを削除します	グループの名前	グループを削除したとき。	
154	INFO	ユーザーをロールから消去しようとしています	ユーザーの名前ロールの名前	ユーザーをロールから消去しようとしたとき。	

表 C–1 amAdmin コマンド行ユーティリティーのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
155	INFO	ユーザーをロールから消去します	ユーザーの名前ロールの名前	ユーザーをロールから消去したとき。	
156	INFO	ユーザーをグループから消去しようとしています	ユーザーの名前グループの名前	ユーザーをグループから消去しようとしたとき。	
157	INFO	ユーザーをグループから消去します	ユーザーの名前グループの名前	ユーザーをグループから消去したとき。	
201	INFO	アイデンティティーをレルム内のアイデンティティーに追加しようとしています。	追加するアイデンティティーの名前追加するアイデンティティーのタイプ追加先のアイデンティティーの名前追加先のアイデンティティーのタイプレルムの名前	アイデンティティーをレルム内のアイデンティティーに追加しようとしたとき。	
202	INFO	アイデンティティーをレルム内のアイデンティティーに追加します	追加するアイデンティティーの名前追加するアイデンティティーのタイプ追加先のアイデンティティーの名前追加先のアイデンティティーのタイプレルムの名前	アイデンティティーをレルム内のアイデンティティーに追加したとき。	

表 C–1 amAdmin コマンド行ユーティリティーのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
203	INFO	サービスをレルム内のアイデンティティーに割り当てようとしています。	サービスの名前アイデンティティーの名前アイデンティティーのタイプレルムの名前	サービスをレルム内のアイデンティティーに割り当てようとしたとき。	
204	INFO	サービスをレルム内のアイデンティティーに割り当てます。	サービスの名前アイデンティティーの名前アイデンティティーのタイプレルムの名前	サービスをレルム内のアイデンティティーに割り当てたとき。	
205	INFO	特定のタイプのアイデンティティー (複数) をレルムに作成しようとしています。	アイデンティティーのタイプレルムの名前	特定のタイプのアイデンティティー (複数) をレルムに作成しようとしたとき。	
206	INFO	特定のタイプのアイデンティティー (複数) をレルムに作成します。	アイデンティティーのタイプレルムの名前	特定のタイプのアイデンティティー (複数) をレルムに作成したとき。	
207	INFO	特定のタイプのアイデンティティーをレルムに作成しようとしています。	アイデンティティーの名前アイデンティティーのタイプレルムの名前	特定のタイプのアイデンティティーをレルムに作成しようとしたとき。	
208	INFO	特定のタイプのアイデンティティーをレルムに作成します。	アイデンティティーの名前アイデンティティーのタイプレルムの名前	特定のタイプのアイデンティティーをレルムに作成したとき。	

表 C–1 amAdmin コマンド行ユーティリティーのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
209	INFO	特定のタイプのアイデンティティーをレルムから削除しようとしています	アイデンティティーの名前アイデンティティーのタイプレルムの名前	特定のタイプのアイデンティティーをレルムから削除しようとしたとき。	
210	INFO	特定のタイプのアイデンティティーをレルムから削除します	アイデンティティーの名前アイデンティティーのタイプレルムの名前	特定のタイプのアイデンティティーをレルムから削除したとき。	
211	INFO	レルム内のアイデンティティーのサービスを変更しようとしています	サービスの名前アイデンティティーのタイプアイデンティティーの名前レルムの名前	レルム内のアイデンティティーのサービスを変更しようとしたとき。	
212	INFO	レルム内のアイデンティティーのサービスを変更します	サービスの名前アイデンティティーのタイプアイデンティティーの名前レルムの名前	レルム内のアイデンティティーのサービスを変更したとき。	
213	INFO	レルム内のアイデンティティーからアイデンティティーを消去しようとしています	消去するアイデンティティーの名前消去するアイデンティティーのタイプ消去元のアイデンティティーの名前消去元のアイデンティティーのタイプレルムの名前	レルム内のアイデンティティーからアイデンティティーを消去しようとしたとき。	

表 C–1 amAdmin コマンド行ユーティリティーのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
214	INFO	レルム内のアイデンティティーからアイデンティティーを消去します	消去するアイデンティティーの名前消去するアイデンティティーのタイプ消去元のアイデンティティーの名前消去元のアイデンティティーのタイプレルムの名前	レルム内のアイデンティティーからアイデンティティーを消去したとき。	
215	INFO	レルム内のアイデンティティーのサービス属性を設定しようとしています	サービスの名前アイデンティティーのタイプアイデンティティーの名前レルムの名前	レルム内のアイデンティティーのサービス属性を設定しようとしたとき。	
216	INFO	レルム内のアイデンティティーのサービス属性を設定します	サービスの名前アイデンティティーのタイプアイデンティティーの名前レルムの名前	レルム内のアイデンティティーのサービス属性を設定したとき。	
217	INFO	レルム内のアイデンティティーからサービスの割り当てを解除しようとしています	サービスの名前アイデンティティーのタイプアイデンティティーの名前レルムの名前	レルム内のアイデンティティーからサービスの割り当てを解除しようとしたとき。	
218	INFO	レルム内のアイデンティティーからサービスの割り当てを解除します	サービスの名前アイデンティティーのタイプアイデンティティーの名前レルムの名前	レルム内のアイデンティティーからサービスの割り当てを解除したとき。	

表 C–1 amAdmin コマンド行ユーティリティーのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
219	INFO	組織を作成しようとしています	組織の名前	組織を作成しようとしたとき。	
220	INFO	組織を作成します	組織の名前	組織を作成したとき。	
221	INFO	サブ設定を削除しようとしています	サブ組織の名前	サブ組織を削除しようとしたとき。	
222	INFO	サブ組織を削除します	サブ組織の名前	サブ組織を削除したとき。	
223	INFO	ロールを変更しようとしています	ロールの名前	ロールを変更しようとしたとき。	
224	INFO	ロールを変更します	ロールの名前	ロールを変更したとき。	
225	INFO	サブ組織を変更しようとしています	サブ組織の名前	サブ組織を変更しようとしたとき。	
226	INFO	サブ組織を変更します	サブ組織の名前	サブ組織を変更したとき。	
227	INFO	ユーザーを削除しようとしています。	ユーザーの名前	ユーザーを削除しようとしたとき。	
228	INFO	ユーザーを削除します。	ユーザーの名前	ユーザーを削除したとき。	
229	INFO	ユーザーを変更しようとしています。	ユーザーの名前	ユーザーを変更しようとしたとき。	
230	INFO	ユーザーを変更します。	ユーザーの名前	ユーザーを変更したとき。	
231	INFO	レルム内のサービス属性に値を追加しようとしています。	属性の名前サービスの名前レルムの名前	レルム内のサービス属性に値を追加しようとしたとき。	

表 C–1 amAdmin コマンド行ユーティリティーのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
232	INFO	レルム内のサービス属性に値を追加します。	属性の名前サービスの名前レルムの名前	レルム内のサービス属性に値を追加したとき。	
233	INFO	サービスをレルムに割り当てようとしています	サービスの名前レルムの名前	サービスをレルムに割り当てようとしたとき。	
234	INFO	サービスをレルムに割り当てます	サービスの名前レルムの名前	サービスをレルムに割り当てたとき。	
235	INFO	レルムを作成しようとしています	作成されるレルムの名前親レルムの名前	レルムを作成しようとしたとき。	
236	INFO	レルムを作成します	作成されるレルムの名前親レルムの名前	レルムを作成したとき。	
237	INFO	レルムを削除します。	再帰的かどうか削除されるレルムの名前	レルムを削除したとき。	
238	INFO	レルムを削除します。	再帰的かどうか削除されるレルムの名前	レルムを削除したとき。	
239	INFO	レルム内のサービスを変更しようとしています。	サービスの名前レルムの名前	レルム内のサービスを変更しようとしたとき。	
240	INFO	レルム内のサービスを変更します。	サービスの名前レルムの名前	レルム内のサービスを変更したとき。	
241	INFO	レルム内のサービスから属性を消去しようとしています	属性の名前サービスの名前レルムの名前	レルム内のサービスから属性を消去しようとしたとき。	
242	INFO	レルム内のサービスから属性を消去します	属性の名前サービスの名前レルムの名前	レルム内のサービスから属性を消去したとき。	

表 C–1 amAdmin コマンド行ユーティリティーのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
243	INFO	レルム内のサービスの属性から値を消去しようとしています	属性の名前サービスの名前レルムの名前	レルム内のサービスの属性から値を消去しようとしたとき。	
244	INFO	レルム内のサービスの属性から値を消去します	属性の名前サービスの名前レルムの名前	レルム内のサービスの属性から値を消去したとき	
245	INFO	レルム内のサービスの属性を設定しようとしています。	サービスの名前レルムの名前	レルム内のサービスの属性を設定しようとしたとき。	
246	INFO	レルム内のサービスの属性を設定します。	サービスの名前レルムの名前	レルム内のサービスの属性を設定します。	
247	INFO	サービスの割り当てをレルムから解除しようとしています。	サービスの名前レルムの名前	サービスを割り当てをレルムから解除しようとしたとき。	
248	INFO	サービスの割り当てをレルムから解除します。	サービスの名前レルムの名前	サービスの割り当てをレルムから解除したとき。	
249	INFO	サービスを組織設定に割り当てようとしています	サービスの名前レルムの名前	サービスを組織設定に割り当てようとしたとき。	
250	INFO	サービスを組織設定に割り当てます	サービスの名前レルムの名前	サービスを組織設定に割り当てたとき。	

表 C–1 amAdmin コマンド行ユーティリティーのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
251	INFO	組織設定へのサービスの割り当てが完了しませんでした	サービスの名前レルムの名前	組織設定に割り当てようとしたサービスが、その組織設定に割り当て可能なサービスでなかったとき。	
252	INFO	レルムへのサービスの割り当てが完了しませんでした	サービスの名前レルムの名前	レルムに割り当てようとしたサービスが、そのレルムに割り当て可能なサービスでなかったとき。	
253	INFO	組織設定からのサービスの割り当て解除しようとしています。	サービスの名前レルムの名前	サービスの割り当てを組織設定から解除しようとしたとき。	
254	INFO	サービスの割り当てを組織設定から解除します。	サービスの名前レルムの名前	サービスの割り当てを組織設定から解除したとき。	
255	INFO	組織設定またはレルムにないサービスの割り当てを解除します。	サービスの名前レルムの名前	組織設定またはレルムにないサービスの割り当て解除を要求したとき。	
256	INFO	組織設定内のサービスを変更しようとしています。	サービスの名前レルムの名前	組織設定内のサービスを変更しようとしたとき。	
257	INFO	組織設定内のサービスを変更します。	サービスの名前レルムの名前	組織設定内のサービスを変更したとき。	

表 C–1 amAdmin コマンド行ユーティリティーのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
258	INFO	組織設定またはレルムにないサービスを変更します。	サービスの名前レルムの名前	組織設定またはレルムにないサービスを変更しようとしたとき。	

表 C–2 認証のログリファレンス

ID	ログレベル	説明	データ	発生原因	対処方法
100	INFO	認証に成功しました	メッセージ	ユーザーが有効な証明情報を使って認証されたとき	
101	INFO	ユーザーベースの認証に成功しました。	メッセージ 認証タイプ ユーザー名	ユーザーが有効な証明情報を使って認証されたとき	
102	INFO	ロールベースの認証に成功しました	メッセージ 認証タイプ ロール名	ロールを持つユーザーが有効な証明情報を使って認証されたとき	
103	INFO	認証ベースのサービスに成功しました	メッセージ 認証タイプ サービス名	レルムに設定済みのサービスに対するユーザーの認証が、有効な証明情報を使って成功したとき	
104	INFO	認証レベルベースの認証に成功しました	メッセージ 認証 タイプ 認証レベル値	指定された認証レベル以上の認証レベルを持つ 1 つ以上の認証モジュールに提示された有効な証明情報を使ってユーザーが認証されたとき	

表 C–2 認証のログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
105	INFO	モジュールベースの認証に成功しました	メッセージ 認証タイプモジュール名	レルムの認証モジュールに対するユーザーの認証が、有効な証明情報を使って成功したとき	
200	INFO	認証に失敗しました	エラーメッセージ	提示された証明情報が不正または無効なときユーザーがロックアウトされているときまたはアクティブでないとき	必須の認証モジュールへの正しいまたは有効な証明情報を入力してください
201	INFO	認証に失敗しました	エラーメッセージ	入力された証明情報が無効なとき。	正しいパスワードを入力してください。
202	INFO	認証に失敗しました	エラーメッセージ	指定された設定 (認証連鎖) が存在しないとき。	この組織に指定されている設定を作成して設定してください。
203	INFO	認証に失敗しました	エラーメッセージ	このユーザーのユーザープロファイルが見つからなかったとき。	設定済みのデータストアプラグインにユーザーが存在しません。このレルムまたは組織のデータストアプラグインを正しく設定してください。
204	INFO	認証に失敗しました	エラーメッセージ	このユーザーがアクティブでないとき。	ユーザーをアクティブにしてください。

表 C–2 認証のログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
205	INFO	認証に失敗しました	エラーメッセージ	失敗の最大試行回数を超えたとき。ユーザーはロックアウトされています。	システム管理者に連絡してください。
206	INFO	認証に失敗しました	エラーメッセージ	ユーザーアカウントが期限切れのとき。	システム管理者に連絡してください。
207	INFO	認証に失敗しました	エラーメッセージ	ログインがタイムアウトになったとき。	もう一度ログインしてみてください。
208	INFO	認証に失敗しました	エラーメッセージ	認証モジュールが拒否されたとき。	このモジュールを設定するか、ほかのモジュールを使用してください。
209	INFO	認証に失敗しました	エラーメッセージ	許可された最大セッション数の上限に到達したとき。	セッションからログアウトするか、上限を大きくしてください。
210	INFO	認証に失敗しました	エラーメッセージ	組織またはレルムが存在しないとき。	有効な組織またはレルムを使用してください。
211	INFO	認証に失敗しました	エラーメッセージ	組織またはレルムがアクティブになっていないとき。	組織またはレルムをアクティブにしてください。
212	INFO	認証に失敗しました	エラーメッセージ	セッションを作成できないとき。	セッションサービスが設定されていて、最大セッション数に到達していないことを確認してください。

表 C–2 認証のログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
213	INFO	ユーザーベースの認証に失敗しました	エラーメッセージ 認証タイプ ユーザー名	ユーザーの認証設定 (1 つ以上の認証モジュールの連鎖) が設定されていないとき提示された証明情報が不正または無効なときユーザーがロックアウトされているかアクティブでないとき	ユーザーの認証設定 (1 つ以上の認証モジュールの連鎖) を設定してください必須の認証モジュールに対して正しいまたは有効な証明情報を入力してください
214	INFO	認証に失敗しました	エラーメッセージ 認証タイプ ユーザー名	ユーザーベースの認証。入力された証明情報が無効なとき。	正しいパスワードを入力してください。
215	INFO	認証に失敗しました	エラーメッセージ 認証タイプ ユーザー名	このユーザーに指定された設定 (認証連鎖) が存在しないとき。	このユーザーの指定された設定を作成および設定してください
216	INFO	認証に失敗しました	エラーメッセージ 認証タイプ ユーザー名	ユーザーベースの認証。このユーザーのユーザープロファイルが見つからなかったとき。	設定済みのデータストアプラグインにユーザーが存在しません。このレルムまたは組織のデータストアプラグインを正しく設定してください。
217	INFO	認証に失敗しました	エラーメッセージ 認証タイプ ユーザー名	ユーザーベースの認証。このユーザーがアクティブでないとき。	ユーザーをアクティブにしてください。

表 C–2 認証のログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
218	INFO	認証に失敗しました	エラーメッセージ 認証タイプ ユーザー名	ユーザーベースの認証。失敗の最大試行回数を超えたとき。ユーザーはロックアウトされています。	システム管理者に連絡してください。
219	INFO	認証に失敗しました	エラーメッセージ 認証タイプ ユーザー名	ユーザーベースの認証。ユーザーアカウントが期限切れのとき。	システム管理者に連絡してください。
220	INFO	認証に失敗しました	エラーメッセージ 認証タイプ ユーザー名	ユーザーベースの認証。ログインがタイムアウトになったとき。	もう一度ログインしてみてください。
221	INFO	認証に失敗しました	エラーメッセージ 認証タイプ ユーザー名	ユーザーベースの認証。認証モジュールが拒否されたとき。	このモジュールを設定するか、ほかのモジュールを使用してください。
222	INFO	認証に失敗しました	エラーメッセージ 認証タイプ ユーザー名	ユーザーベースの認証。許可された最大セッション数の上限に到達したとき。	セッションからログアウトするか、上限を大きくしてください。
223	INFO	認証に失敗しました	エラーメッセージ 認証タイプ ユーザー名	ユーザーベースの認証。組織またはレルムが存在しないとき。	有効な組織またはレルムを使用してください。
224	INFO	認証に失敗しました	エラーメッセージ 認証タイプ ユーザー名	ユーザーベースの認証。組織またはレルムがアクティブになっていないとき。	組織またはレルムをアクティブにしてください。

表 C–2 認証のログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
225	INFO	認証に失敗しました	エラーメッセージ 認証タイプ ユーザー名	ユーザーベースの認証。セッションを作成できないとき。	セッションサービスが設定されていて、最大セッション数に到達していないことを確認してください。
226	INFO	ロールベースの認証に失敗しました	エラーメッセージ 認証タイプ ロール名	ロールの認証設定 (1 つ以上の認証モジュールの連鎖) が設定されていないとき 提示された証明情報が不正または無効なとき ユーザーがこのロールに割り当てられていないとき ユーザーがロックアウトされているかアクティブでないとき	ロールの認証設定 (1 つ以上の認証モジュールの連鎖) を設定してください必須の認証モジュールに対して正しいまたは有効な証明情報を入力してください認証中のユーザーにこのロールを割り当ててください
227	INFO	認証に失敗しました	エラーメッセージ 認証タイプ ロール名	ロールベースの認証。入力された証明情報が無効なとき。	正しいパスワードを入力してください。
228	INFO	認証に失敗しました	エラーメッセージ 認証タイプ ロール名	このロールの指定された設定 (認証連鎖) が存在しないとき。	このロールの指定された設定を作成および設定してください。

表 C–2 認証のログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
229	INFO	認証に失敗しました	エラーメッセージ 認証タイプ ロール名	ロールベースの認証。このユーザーのユーザープロファイルが見つからなかったとき。	設定済みのデータストアプラグインにユーザーが存在しません。このレルムまたは組織のデータストアプラグインを正しく設定してください。
230	INFO	認証に失敗しました	エラーメッセージ 認証タイプ ロール名	ロールベースの認証。このユーザーがアクティブでないとき。	ユーザーをアクティブにしてください。
231	INFO	認証に失敗しました	エラーメッセージ 認証タイプ ロール名	ロールベースの認証。失敗の最大試行回数を超えたとき。ユーザーはロックアウトされています。	システム管理者に連絡してください。
232	INFO	認証に失敗しました	エラーメッセージ 認証タイプ ロール名	ロールベースの認証。ユーザーアカウントが期限切れのとき。	システム管理者に連絡してください。
233	INFO	認証に失敗しました	エラーメッセージ 認証タイプ ロール名	ロールベースの認証。ログインがタイムアウトになったとき。	もう一度ログインしてみてください。
234	INFO	認証に失敗しました	エラーメッセージ 認証タイプ ロール名	ロールベースの認証。認証モジュールが拒否されたとき。	このモジュールを設定するか、ほかのモジュールを使用してください。

表C–2 認証のログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
235	INFO	認証に失敗しました	エラーメッセージ 認証タイプ ロール名	ロールベースの認証。許可された最大セッション数の上限に到達したとき。	セッションからログアウトするか、上限を大きくしてください。
236	INFO	認証に失敗しました	エラーメッセージ認証タイプロール名	ロールベースの認証。組織またはレルムが存在しないとき。	有効な組織またはレルムを使用してください。
237	INFO	認証に失敗しました	エラーメッセージ 認証タイプ ロール名	ロールベースの認証。組織またはレルムがアクティブになっていないとき。	組織またはレルムをアクティブにしてください。
238	INFO	認証に失敗しました	エラーメッセージ 認証タイプ ロール名	ロールベースの認証。セッションを作成できないとき。	セッションサービスが設定されていて、最大セッション数に到達していないことを確認してください。
239	INFO	認証に失敗しました	エラーメッセージ 認証タイプ ロール名	ロールベースの認証。ユーザーがこのロールに割り当てられていないとき。	ユーザーをこのロールに追加してください。

表 C–2 認証のログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
240	INFO	サービスベースの認証に失敗しました	エラーメッセージ 認証タイプ サービス名	サービスの認証設定 (1 つ以上の認証モジュールの連鎖) が設定されていないとき提示された証明情報が不正または無効なときユーザーがロックアウトされているかアクティブでないとき	サービスの認証設定 (1 つ以上の認証モジュールの連鎖) を設定してください必須の認証モジュールに対して正しいまたは有効な証明情報を入力してください
241	INFO	認証に失敗しました	エラーメッセージ 認証タイプ サービス名	サービスベースの認証。入力された証明情報が無効なとき。	正しいパスワードを入力してください。
242	INFO	認証に失敗しました	エラーメッセージ 認証タイプ サービス名	このサービスの指定された設定 (認証連鎖) が存在しないとき。	指定された設定を作成および設定してください。
243	INFO	認証に失敗しました	エラーメッセージ 認証タイプ サービス名	サービスベースの認証。このユーザーのユーザープロファイルが見つからなかったとき。	設定済みのデータストアプラグインにユーザーが存在しません。このレルムまたは組織のデータストアプラグインを正しく設定してください。
244	INFO	認証に失敗しました	エラーメッセージ 認証タイプ サービス名	サービスベースの認証。このユーザーがアクティブでないとき。	ユーザーをアクティブにしてください。

表 C–2 認証のログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
245	INFO	認証に失敗しました	エラーメッセージ認証タイプサービス名	サービスベースの認証。失敗の最大試行回数を超えたとき。ユーザーがロックアウトされているとき。	システム管理者に連絡してください。
246	INFO	認証に失敗しました	エラーメッセージ認証タイプサービス名	サービスベースの認証。ユーザーアカウントが期限切れのとき。	システム管理者に連絡してください。
247	INFO	認証に失敗しました	エラーメッセージ認証タイプサービス名	サービスベースの認証。ログインがタイムアウトになったとき。	もう一度ログインしてみてください。
248	INFO	認証に失敗しました	エラーメッセージ認証タイプサービス名	サービスベースの認証。認証モジュールが拒否されたとき。	このモジュールを設定するか、ほかのモジュールを使用してください。
249	INFO	認証に失敗しました	エラーメッセージ認証タイプサービス名	サービスベースの認証。サービスが存在しないとき。	有効なサービスだけを使用してください。
250	INFO	認証に失敗しました	エラーメッセージ認証タイプサービス名	サービスベースの認証。許可された最大セッション数の上限に到達したとき。	セッションからログアウトするか、上限を大きくしてください。
251	INFO	認証に失敗しました	エラーメッセージ認証タイプサービス名	サービスベースの認証。組織またはレルムが存在しないとき。	有効な組織またはレルムを使用してください。

表 C–2 認証のログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
252	INFO	認証に失敗しました	エラーメッセージ 認証タイプ サービス名	サービスベースの認証。組織またはレルムがアクティブになっていないとき。	組織またはレルムをアクティブにしてください。
253	INFO	認証に失敗しました	エラーメッセージ 認証タイプ サービス名	サービスベースの認証。セッションを作成できないとき。	セッションサービスが設定されていて、最大セッション数に到達していないことを確認してください。
254	INFO	認証レベルベースの認証に失敗しました	エラーメッセージ 認証タイプ 認証レベル値	指定された認証レベル以上の認証レベル値を持つ認証モジュールがないとき指定された認証レベル以上の認証レベルを持つ *1* つ以上の認証モジュールに提示された証明情報が不正または無効なときユーザーがロックアウトされているかアクティブでないとき	必須の認証レベル以上の認証レベル値を持つ 1 つ以上の認証モジュールを設定してください指定された認証レベル以上の認証レベルを持つ *1* つ以上の認証モジュールに正しいまたは有効な証明情報を入力してください
255	INFO	認証に失敗しました	エラーメッセージ 認証タイプ 認証レベル値	レベルベースの認証。入力された証明情報が無効なとき。	正しいパスワードを入力してください。

表 C–2 認証のログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
256	INFO	認証に失敗しました	エラーメッセージ 認証タイプ 認証レベル値	レベルベースの認証。利用可能な認証設定がないとき。	認証設定を作成してください。
257	INFO	認証に失敗しました	エラーメッセージ 認証タイプ 認証レベル値	レベルベースの認証。このユーザーのユーザープロファイルが見つからなかったとき。	設定済みのデータストアプラグインにユーザーが存在しません。このレルムまたは組織のデータストアプラグインを正しく設定してください。
258	INFO	認証に失敗しました	エラーメッセージ 認証タイプ 認証レベル値	レベルベースの認証。このユーザーがアクティブでないとき。	ユーザーをアクティブにしてください。
259	INFO	認証に失敗しました	エラーメッセージ 認証タイプ 認証レベル値	レベルベースの認証。失敗の最大試行回数を超えたとき。ユーザーはロックアウトされています。	システム管理者に連絡してください。
260	INFO	認証に失敗しました	エラーメッセージ 認証タイプ 認証レベル値	レベルベースの認証。ユーザーアカウントが期限切れのとき。	システム管理者に連絡してください。
261	INFO	認証に失敗しました	エラーメッセージ 認証タイプ 認証レベル値	レベルベースの認証。ログインがタイムアウトになったとき。	もう一度ログインしてみてください。

表 C–2 認証のログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
262	INFO	認証に失敗しました	エラー メッセージ 認証タイプ 認証レベル値	レベルベースの認証。認証モジュールが拒否されたとき。	このモジュールを設定するか、ほかのモジュールを使用してください。
263	INFO	認証に失敗しました	エラー メッセージ 認証タイプ 認証レベル値	レベルベースの認証。認証レベルが無効なとき。	有効な認証レベルを指定してください。
264	INFO	認証に失敗しました	エラー メッセージ 認証タイプ 認証レベル値	レベルベースの認証。許可された最大セッション数の上限に到達したとき。	セッションからログアウトするか、上限を大きくしてください。
265	INFO	認証に失敗しました	エラー メッセージ 認証タイプ 認証レベル値	レベルベースの認証。組織またはレルムが存在しないとき。	有効な組織またはレルムを使用してください。
266	INFO	認証に失敗しました	エラー メッセージ 認証タイプ 認証レベル値	レベルベースの認証。組織またはレルムがアクティブになっていないとき。	組織またはレルムをアクティブにしてください。
267	INFO	認証に失敗しました	エラー メッセージ 認証タイプ 認証レベル値	レベルベースの認証。セッションを作成できないとき。	セッションサービスが設定されていて、最大セッション数に到達していないことを確認してください。

表C–2 認証のログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
268	INFO	モジュールベースの認証に失敗しました	エラーメッセージ 認証タイプ モジュール名	モジュールがレルムに登録されていないか 設定されていないとき 提示された証明情報が不正または無効なときユーザーがロックアウトされているかアクティブでないとき	認証モジュールをレルムに登録または設定してください正しいまたは有効な証明情報を認証モジュールに入力してください
269	INFO	認証に失敗しました	エラーメッセージ 認証タイプ モジュール名	モジュールベースの認証。入力された証明情報が無効なとき。	正しいパスワードを入力してください。
270	INFO	認証に失敗しました	エラーメッセージ 認証タイプ モジュール名	モジュールベースの認証。このユーザーのユーザープロファイルが見つからなかったとき。	設定済みのデータストアプラグインにユーザーが存在しません。このレルムまたは組織のデータストアプラグインを正しく設定してください。
271	INFO	認証に失敗しました	エラーメッセージ 認証タイプ モジュール名	モジュールベースの認証。このユーザーがアクティブでないとき。	ユーザーをアクティブにしてください。

表 C–2 認証のログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
272	INFO	認証に失敗しました	エラーメッセージ 認証タイプ モジュール名	モジュールベースの認証。失敗の最大試行回数を超えたとき。ユーザーがロックアウトされているとき。	システム管理者に連絡してください。
273	INFO	認証に失敗しました	エラーメッセージ 認証タイプ モジュール名	モジュールベースの認証。ユーザーアカウントが期限切れのとき。	システム管理者に連絡してください。
274	INFO	認証に失敗しました	エラーメッセージ 認証タイプ モジュール名	モジュールベースの認証。ログインがタイムアウトになったとき。	もう一度ログインしてみてください。
275	INFO	認証に失敗しました	エラーメッセージ 認証タイプ モジュール名	モジュールベースの認証。認証モジュールが拒否されたとき。	このモジュールを設定するか、ほかのモジュールを使用してください。
276	INFO	認証に失敗しました	エラーメッセージ 認証タイプ モジュール名	モジュールベースの認証。許可された最大セッション数の上限に到達したとき。	セッションからログアウトするか、上限を大きくしてください。
277	INFO	認証に失敗しました	エラーメッセージ 認証タイプ モジュール名	モジュールベースの認証。組織またはレルムが存在しないとき。	有効な組織またはレルムを使用してください。

表C–2 認証のログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
278	INFO	認証に失敗しました	エラーメッセージ 認証タイプ モジュール名	モジュールベースの認証。組織またはレルムがアクティブになっていないとき。	組織またはレルムをアクティブにしてください。
279	INFO	認証に失敗しました	エラーメッセージ 認証タイプ モジュール名	モジュールベースの認証。 セッションを作成できないとき。	セッションサービスが設定されていて、最大セッション数に到達していないことを確認してください。
300	INFO	ユーザーのログアウトが成功しました	メッセージ	ユーザーがログアウトしたとき	
301	INFO	ユーザーがユーザーベースの認証から正常にログアウトしました	メッセージ 認証タイプ ユーザー名	ユーザーがログアウトしたとき	
302	INFO	ユーザーがロールベースの認証から正常にログアウトしました	メッセージ 認証タイプ ロール名	このロールに割り当てられているユーザーがログアウトしたとき	
303	INFO	ユーザーがサービスベースの認証から正常にログアウトしました	メッセージ 認証タイプ サービス名	レルムに設定されているサービスからユーザーがログアウトしたとき	
304	INFO	ユーザーが認証レベルベースの認証から正常にログアウトしました。	メッセージ 認証タイプ 認証レベル値	ユーザーが、指定された認証レベル以上の認証レベル値を持つ1つ以上の認証モジュールからログアウトしたとき	

表 C–2 認証のログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
305	INFO	ユーザーがモジュールベースの認証から正常にログアウトしました	メッセージ 認証タイプ モジュール名	ユーザーがレルムの認証モジュールからログアウトしたとき	

表 C–3 Access Manager コンソールのログリファレンス

ID	ログレベル	説明	データ	発生原因	対処方法
1	INFO	アイデンティティーを作成しようとしています	アイデンティティー名 アイデンティティータイプ レルム名	レルム作成ページの「作成」ボタンをクリックしたとき。	
2	INFO	アイデンティティーの作成に成功しました。	アイデンティティー名 アイデンティティータイプ レルム名	レルム作成ページの「作成」ボタンをクリックしたとき。	
3	SEVERE	アイデンティティーの作成に失敗しました	アイデンティティー名 アイデンティティータイプ レルム名 エラーメッセージ	レルムにアイデンティティーを作成できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、データストアのログを調べてください。
4	SEVERE	アイデンティティーの作成に失敗しました	アイデンティティー名 アイデンティティータイプ レルム名 エラーメッセージ	データストアエラーが原因で、レルムにアイデンティティーを作成できないとき。	詳細な情報が必要な場合は、データストアのログを調べてください。

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
11	INFO	アイデンティティーを検索しようとしています	基本レルムアイデンティティータイプ検索パターン検索サイズの上限検索時間の上限	アイデンティティー検索ビューの「検索」ボタンをクリックしたとき。	
12	INFO	アイデンティティーの検索に成功しました	基本レルムアイデンティティータイプ検索パターン検索サイズの上限検索時間の上限	アイデンティティー検索ビューの「検索」ボタンをクリックしたとき。	
13	SEVERE	アイデンティティーの検索に失敗しました	アイデンティティー名アイデンティティータイプレルム名エラーメッセージ	レルム内のアイデンティティーに検索操作を実行できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、データストアのログを調べてください。
14	SEVERE	アイデンティティーの検索に失敗しました	アイデンティティー名アイデンティティータイプレルム名エラーメッセージ	データストアエラーが原因で、レルム内のアイデンティティーに検索操作を実行できないとき。	詳細な情報が必要な場合は、データストアのログを調べてください。

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
21	INFO	アイデンティティーの属性値を読み取ろうとしています	アイデンティティー名属性の名前	アイデンティティープロファイルビューを表示したとき。	
22	INFO	アイデンティティーの属性値の読み取りに成功しました	アイデンティティー名属性の名前	アイデンティティープロファイルビューを表示したとき。	
23	SEVERE	アイデンティティーの属性値の読み取りに失敗しました	アイデンティティー名属性の名前エラーメッセージ	アイデンティティーの属性値を読み取れないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、データストアのログを調べてください。
24	SEVERE	アイデンティティーの属性値の読み取りに失敗しました	アイデンティティー名属性の名前エラーメッセージ	データストアエラーが原因で、アイデンティティーの属性値を読み取れないとき。	詳細な情報が必要な場合は、データストアのログを調べてください。
25	SEVERE	アイデンティティーの属性値の読み取りに失敗しました	アイデンティティー名属性の名前エラーメッセージ	例外サービスマネージャー API が原因で、アイデンティティーの属性値を読み取れないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
31	INFO	アイデンティティーの属性値を変更しようとしています	アイデンティティー名 属性の名前	アイデンティティープロファイルビューの「保存」ボタンをクリックしたとき。	
32	INFO	アイデンティティーの属性値の変更に成功しました	アイデンティティー名 属性の名前	アイデンティティープロファイルビューの「保存」ボタンをクリックしたとき。	
33	SEVERE	アイデンティティーの属性値の変更に失敗しました	アイデンティティー名 属性の名前エラーメッセージ	アイデンティティーの属性値を変更できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、データストアのログを調べてください。
34	SEVERE	アイデンティティーの属性値の変更に失敗しました	アイデンティティー名 属性の名前エラーメッセージ	データストアエラーが原因で、アイデンティティーの属性値を変更できないとき。	詳細な情報が必要な場合は、データストアのログを調べてください。

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
41	INFO	アイデンティティーを削除しようとしています	レルム名削除されるアイデンティティーの名前	アイデンティティー検索ビューの「削除」ボタンをクリックしたとき。	
42	INFO	アイデンティティーの削除に成功しました	レルム名削除されるアイデンティティーの名前	アイデンティティー検索ビューの「削除」ボタンをクリックしたとき。	
43	SEVERE	アイデンティティーの削除に失敗しました	レルム名削除されるアイデンティティーの名前エラーメッセージ	アイデンティティーを削除できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、データストアのログを調べてください。
44	SEVERE	アイデンティティーの削除に失敗しました	レルム名削除されるアイデンティティーの名前エラーメッセージ	データストアエラーが原因で、アイデンティティーを削除できないとき。	詳細な情報が必要な場合は、データストアのログを調べてください。
51	INFO	アイデンティティーのメンバーシップ情報を読み取ろうとしています	アイデンティティーの名前 メンバーシップのアイデンティティータイプ	アイデンティティーのメンバーシップページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
52	INFO	アイデンティティーのメンバーシップ情報の読み取りに成功しました	アイデンティティーの名前 メンバーシップのアイデンティティータイプ	アイデンティティーのメンバーシップページを表示したとき。	
53	SEVERE	アイデンティティーのメンバーシップ情報の読み取りに失敗しました。	アイデンティティーの名前 メンバーシップのアイデンティティータイプエラーメッセージ	アイデンティティーのメンバーシップ情報を読み取れないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、データストアのログを調べてください。
54	SEVERE	アイデンティティーのメンバーシップ情報の読み取りに失敗しました。	アイデンティティーの名前 メンバーシップのアイデンティティータイプエラーメッセージ	データストアエラーが原因で、アイデンティティーのメンバーシップ情報を読み取れないとき。	詳細な情報が必要な場合は、データストアのログを調べてください。
61	INFO	アイデンティティーのメンバー情報を読み取ろうとしています	アイデンティティーの名前 メンバーのアイデンティティータイプ	アイデンティティーのメンバーページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
62	INFO	アイデンティティーのメンバー情報の読み取りに成功しました	アイデンティティーの名前 メンバーのアイデンティティータイプ	アイデンティティーのメンバーページを表示したとき。	
63	SEVERE	アイデンティティーのメンバー情報の読み取りに失敗しました	アイデンティティーの名前 メンバーのアイデンティティータイプ エラーメッセージ	アイデンティティーのメンバー情報を読み取れないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、データストアのログを調べてください。
64	SEVERE	アイデンティティーのメンバー情報の読み取りに失敗しました	アイデンティティーの名前 メンバーのアイデンティティータイプ エラーメッセージ	データストアエラーが原因で、アイデンティティーのメンバー情報を読み取れないとき。	詳細な情報が必要な場合は、データストアのログを調べてください。
71	INFO	メンバーをアイデンティティーに追加しようとしています	アイデンティティーの名前 追加されるアイデンティティーの名前	アイデンティティーに追加するメンバーを選択したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
72	INFO	アイデンティティーへのメンバーの追加に成功しました	アイデンティティーの名前追加されたアイデンティティーの名前	アイデンティティーに追加するメンバーを選択したとき。	
73	SEVERE	アイデンティティーへのメンバーの追加に失敗しました。	アイデンティティーの名前追加されるアイデンティティーの名前エラーメッセージ	メンバーをアイデンティティーに追加できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、データストアのログを調べてください。
74	SEVERE	アイデンティティーへのメンバーの追加に失敗しました。	アイデンティティーの名前追加されるアイデンティティーの名前エラーメッセージ	データストアエラーが原因で、アイデンティティーにメンバーを追加できないとき。	詳細な情報が必要な場合は、データストアのログを調べてください。
81	INFO	メンバーをアイデンティティーから消去しようとしています	アイデンティティーの名前消去されるアイデンティティーの名前	アイデンティティーから消去するメンバーを選択したとき。	
82	INFO	アイデンティティーからのメンバーの消去に成功しました。	アイデンティティーの名前消去されたアイデンティティーの名前	アイデンティティーから消去するメンバーを選択したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
83	SEVERE	アイデンティティーからのメンバーの消去に失敗しました。	アイデンティティーの名前 消去されるアイデンティティーの名前エラーメッセージ	アイデンティティーからメンバーを消去できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、データストアのログを調べてください。
84	SEVERE	アイデンティティーからのメンバーの消去に失敗しました。	アイデンティティーの名前消去されるアイデンティティーの名前エラーメッセージ	データストアエラーが原因で、アイデンティティーからメンバーを消去できないとき。	詳細な情報が必要な場合は、データストアのログを調べてください。
91	INFO	アイデンティティーに割り当てられているサービス名を読み取ろうとしています	アイデンティティーの名前	アイデンティティーのサービス割り当てビューの「追加」ボタンをクリックしたとき。	
92	INFO	アイデンティティーに割り当てられているサービス名の読み取りに成功しました	アイデンティティーの名前	アイデンティティーのサービス割り当てビューの「追加」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
93	SEVERE	アイデンティティーに割り当てられているサービス名の読み取りに失敗しました。	アイデンティティーの名前エラーメッセージ	アイデンティティーに割り当てられたサービス名を読み取れないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、データストアのログを調べてください。
94	SEVERE	アイデンティティーに割り当てられているサービス名の読み取りに失敗しました。	アイデンティティーの名前エラーメッセージ	データストアエラーが原因で、アイデンティティーに割り当てられているサービス名を読み取れないとき。	詳細な情報が必要な場合は、データストアのログを調べてください。
101	INFO	アイデンティティーに割り当て可能なサービス名を読み取ろうとしています。	アイデンティティーの名前	アイデンティティーのサービスページを表示したとき。	
102	INFO	アイデンティティーに割り当て可能なサービス名の読み取りに成功しました。	アイデンティティーの名前	アイデンティティーのサービスページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
103	SEVERE	アイデンティティーに割り当て可能なサービス名の読み取りに失敗しました。	アイデンティティーの名前エラーメッセージ	アイデンティティーに割り当て可能なサービス名を読み取れないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、データストアのログを調べてください。
104	SEVERE	アイデンティティーに割り当て可能なサービス名の読み取りに失敗しました。	アイデンティティーの名前エラーメッセージ	データストアエラーが原因で、アイデンティティーに割り当て可能なサービス名を読み取れないとき。	詳細な情報が必要な場合は、データストアのログを調べてください。
111	INFO	サービスをアイデンティティーに割り当てようとしています	アイデンティティーの名前サービスの名前	アイデンティティーのサービスビューの「追加」ボタンをクリックしたとき。	
112	INFO	アイデンティティーへのサービスの割り当てに成功しました	アイデンティティーの名前サービスの名前	アイデンティティーのサービスビューの「追加」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
113	SEVERE	アイデンティティーへのサービスの割り当てに失敗しました	アイデンティティーの名前サービスの名前エラーメッセージ	サービスをアイデンティティーに割り当てることができないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、データストアのログを調べてください。
114	SEVERE	アイデンティティーへのサービスの割り当てに失敗しました	アイデンティティーの名前サービスの名前エラーメッセージ	データストアエラーが原因で、アイデンティティーにサービスを割り当てることができないとき。	詳細な情報が必要な場合は、データストアのログを調べてください。
121	INFO	アイデンティティーからサービスの割り当てを解除しようとしています	アイデンティティーの名前サービスの名前	アイデンティティーのサービスビューの「消去」ボタンをクリックしたとき。	
122	INFO	アイデンティティーからのサービスの割り当ての解除に成功しました	アイデンティティーの名前サービスの名前	アイデンティティーのサービスビューの「消去」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
123	SEVERE	アイデンティティーからのサービスの割り当ての解除に失敗しました。	アイデンティティーの名前サービスの名前エラーメッセージ	アイデンティティーからサービスの割り当てを解除できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、データストアのログを調べてください。
124	SEVERE	アイデンティティーからのサービスの割り当ての解除に失敗しました。	アイデンティティーの名前サービスの名前エラーメッセージ	データストアエラーが原因で、アイデンティティーからサービスの割り当てを解除できないとき。	詳細な情報が必要な場合は、データストアのログを調べてください。
131	INFO	アイデンティティーのサービス属性値を読み取ろうとしています	アイデンティティーの名前サービスの名前	アイデンティティーのサービスプロファイルビューを表示したとき。	
132	INFO	アイデンティティーのサービス属性値の読み取りに成功しました	アイデンティティーの名前サービスの名前	アイデンティティーのサービスプロファイルビューを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
133	SEVERE	アイデンティティーのサービス属性値の読み取りに失敗しました。	アイデンティティーの名前サービスの名前エラーメッセージ	アイデンティティーのサービス属性値を読み取れないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、データストアのログを調べてください。
134	SEVERE	アイデンティティーのサービス属性値の読み取りに失敗しました。	アイデンティティーの名前サービスの名前エラーメッセージ	データストアエラーが原因で、アイデンティティーのサービス属性値を読み取れないとき。	詳細な情報が必要な場合は、データストアのログを調べてください。
141	INFO	サービス属性値をアイデンティティーに書き込もうとしています	アイデンティティーの名前サービスの名前	アイデンティティーのサービスプロファイルビューの「保存」ボタンをクリックしたとき。	
142	INFO	アイデンティティーへのサービス属性値の書き込みに成功しました	アイデンティティーの名前サービスの名前	アイデンティティーのサービスプロファイルビューの「保存」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
143	SEVERE	アイデンティティーへのサービス属性値の書き込みに失敗しました。	アイデンティティーの名前サービスの名前エラーメッセージ	サービス属性値をアイデンティティーに書き込めないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、データストアのログを調べてください。
144	SEVERE	アイデンティティーへのサービス属性値の書き込みに失敗しました。	アイデンティティーの名前サービスの名前エラーメッセージ	データストアエラーが原因で、サービス属性値をアイデンティティーに書き込めないとき。	詳細な情報が必要な場合は、データストアのログを調べてください。
201	INFO	すべてのグローバルサービスのデフォルト属性値を読み取ろうとしています	サービスの名前	サービスのグローバル設定ビューを表示したとき。	
202	INFO	すべてのグローバルサービスのデフォルト属性値の読み取りに成功しました	サービスの名前	サービスのグローバル設定ビューを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
203	INFO	グローバルサービスのデフォルト属性値を読み取ろうとしています	サービスの名前属性の名前	サービスのグローバル設定ビューを表示したとき。	
204	INFO	グローバルサービスのデフォルト属性値の読み取りに成功しました	サービスの名前属性の名前	サービスのグローバル設定ビューを表示したとき。	
205	INFO	グローバルサービスのデフォルト属性値の読み取りに失敗しました	サービスの名前属性の名前	サービスのグローバル設定ビューを表示したとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
211	INFO	グローバルサービスのデフォルト属性値の書き込もうとしています	サービスの名前属性の名前	サービスのグローバル設定ビューの「保存」ボタンをクリックしたとき。	
212	INFO	グローバルサービスのデフォルト属性値の書き込みに成功しました	サービスの名前属性の名前	サービスのグローバル設定ビューの「保存」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
213	SEVERE	グローバルサービスのデフォルト属性値の書き込みに失敗しました	サービスの名前属性の名前エラーメッセージ	グローバルサービスのデフォルト属性値を書き込めないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
214	SEVERE	グローバルサービスのデフォルト属性値の書き込みに失敗しました	サービスの名前属性の名前エラーメッセージ	サービス管理エラーが原因で、サービスのデフォルト属性値を書き込めないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
221	INFO	サブ設定名を取得しようとしています	サービスの名前基本グローバルサブ設定の名前	サブスキーマを持つサービスのグローバルサービスビューを表示したとき。	
222	INFO	グローバルサブ設定名の読み取りに成功しました	サービスの名前基本グローバルサブ設定の名前	サブスキーマを持つサービスのグローバルサービスビューを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
223	SEVERE	グローバルサブ設定名の読み取りに失敗しました。	サービスの名前基本グローバルサブ設定の名前 エラーメッセージ	グローバルサブ設定名を取得できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
224	SEVERE	グローバルサブ設定名の読み取りに失敗しました。	サービスの名前 基本グローバルサブ設定の名前 エラーメッセージ	サービス管理エラーが原因で、グローバルサブ設定名を取得できないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
231	INFO	サブ設定を削除しようとしています	サービスの名前 基本グローバルサブ設定の名前 削除されるサブ設定の名前	グローバルサービスプロファイルビューの「選択を削除」ボタンをクリックしたとき。	
232	INFO	サブ設定の削除に成功しました	サービスの名前 基本グローバルサブ設定の名前 削除されるサブ設定の名前	グローバルサービスプロファイルビューの「選択を削除」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
233	SEVERE	サブ設定の削除に失敗しました	サービスの名前 基本グローバルサブ設定の名前 削除されるサブ設定の名前 エラーメッセージ	サブ設定を削除できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
234	SEVERE	サブ設定の削除に失敗しました	サービスの名前 基本グローバルサブ設定の名前 削除されるサブ設定の名前 エラーメッセージ	サービス管理エラーが原因で、サブ設定を削除できないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
241	INFO	サブ設定を作成しようとしています	サービスの名前 基本グローバルサブ設定の名前 作成されるサブ設定の名前 作成されるサブスキーマの名前	サブ設定の作成ビューの「追加」ボタンをクリックしたとき。	
242	INFO	サブ設定の作成に成功しました	サービスの名前 基本グローバルサブ設定の名前 作成されるサブ設定の名前 作成されるサブスキーマの名前	サブ設定の作成ビューの「追加」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
243	SEVERE	サブ設定の作成に失敗しました。	サービスの名前 基本グローバルサブ設定の名前 作成されるサブ設定の名前 作成されるサブスキーマの名前 エラーメッセージ	サブ設定を作成できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
244	SEVERE	サブ設定の作成に失敗しました。	サービスの名前 基本グローバルサブ設定の名前 作成されるサブ設定の名前 作成されるサブスキーマの名前 エラーメッセージ	サービス管理エラーが原因で、サブ設定を作成できないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
251	INFO	サブ設定の属性値の読み取りに成功しました	サービスの名前サブ設定の名前	サブ設定プロファイルビューを表示したとき。	
261	INFO	サブ設定の属性値を書き込もうとしています	サービスの名前サブ設定の名前	サブ設定プロファイルビューの「保存」ボタンをクリックしたとき。	
262	INFO	サブ設定の属性値の書き込みに成功しました	サービスの名前サブ設定の名前	サブ設定プロファイルビューの「保存」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
263	SEVERE	サブ設定の属性値の書き込みに失敗しました。	サービスの名前サブ設定の名前 エラーメッセージ	サブ設定の属性値を書き込めないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
264	SEVERE	サブ設定の属性値の書き込みに失敗しました。	サービスの名前サブ設定の名前 エラーメッセージ	サービス管理エラーが原因で、サブ設定の属性値を書き込めないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
301	INFO	レルムのポリシー名を取得しようとしています。	レルムの名前	ポリシーメインページを表示したとき。	
302	INFO	レルムのポリシー名の取得に成功しました	レルムの名前	ポリシーメインページを表示したとき。	
303	SEVERE	レルムのポリシー名の取得に失敗しました。	レルムの名前 エラーメッセージ	レルムのポリシー名を取得できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、ポリシーのログを調べてください。

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
304	SEVERE	レルムのポリシー名の取得に失敗しました。	レルムの名前 エラーメッセージ	ポリシー SDK に関連するエラーが原因で、レルムのポリシー名を取得できないとき。	詳細な情報が必要な場合は、ポリシーのログを調べてください。
311	INFO	レルムにポリシーを作成しようとしています。	レルムの名前 ポリシーの名前	ポリシー作成ページの「新規」ボタンをクリックしたとき。	
312	INFO	ポリシーの作成に成功しました	レルムの名前 ポリシーの名前	ポリシー作成ページの「新規」ボタンをクリックしたとき。	
313	SEVERE	ポリシーの作成に失敗しました。	レルムの名前 ポリシーの名前エラーメッセージ	レルムにポリシーを作成できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、ポリシーのログを調べてください。
314	SEVERE	ポリシーの作成に失敗しました。	レルムの名前 ポリシーの名前エラーメッセージ	ポリシー SDK に関連するエラーが原因で、レルムにポリシーを作成できないとき。	詳細な情報が必要な場合は、ポリシーのログを調べてください。

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
321	INFO	ポリシーを変更しようとしています。	レルムの名前 ポリシーの名前	ポリシープロファイルページの「保存」ボタンをクリックしたとき。	
322	INFO	ポリシーの変更に成功しました	レルムの名前 ポリシーの名前	ポリシープロファイルページの「保存」ボタンをクリックしたとき。	
323	SEVERE	ポリシーの変更に失敗しました。	レルムの名前 ポリシーの名前エラーメッセージ	レルムのポリシーを変更できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、ポリシーのログを調べてください。
324	SEVERE	ポリシーの変更に失敗しました。	レルムの名前 ポリシーの名前エラーメッセージ	ポリシー SDK に関連するエラーが原因で、ポリシーを変更できないとき。	詳細な情報が必要な場合は、ポリシーのログを調べてください。
331	INFO	ポリシーを削除しようとしています。	レルムの名前 ポリシーの名前	ポリシーメインページの「削除」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
332	INFO	ポリシーの削除に成功しました	レルムの名前 ポリシーの名前	ポリシーメインページの「削除」ボタンをクリックしたとき。	
333	SEVERE	ポリシーの削除に失敗しました。	レルムの名前 ポリシーの名前エラーメッセージ	ポリシーを削除できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、ポリシーのログを調べてください。
334	SEVERE	ポリシーの削除に失敗しました。	レルムの名前 ポリシーの名前エラーメッセージ	ポリシー SDK に関連するエラーが原因で、ポリシーを削除できないとき。	詳細な情報が必要な場合は、ポリシーのログを調べてください。
401	INFO	レルム名を取得しようとしています	親レルムの名前	レルムメインページを表示したとき。	
402	INFO	レルム名の取得に成功しました。	親レルムの名前	レルムメインページを表示したとき。	
403	SEVERE	レルム名の取得に失敗しました。	親レルムの名前エラーメッセージ	サービス管理 SDK の例外が原因で、レルム名を取得できないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
411	INFO	レルムを作成しようとしています	親レルムの名前新しいレルムの名前	レルム作成ページの「新規」ボタンをクリックしたとき。	
412	INFO	レルムの作成に成功しました。	親レルムの名前新しいレルムの名前	レルム作成ページの「新規」ボタンをクリックしたとき。	
413	SEVERE	レルムの作成に失敗しました。	親レルムの名前新しいレルムの名前エラーメッセージ	サービス管理 SDK の例外が原因で、新しいレルムを作成できないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
421	INFO	レルムを削除しようとしています	親レルムの名前削除するレルムの名前	レルムメインページの「削除」ボタンをクリックしたとき。	
422	INFO	レルムの削除に成功しました。	親レルムの名前削除するレルムの名前	レルムメインページの「削除」ボタンをクリックしたとき。	
423	SEVERE	レルムの削除に失敗しました。	親レルムの名前削除するレルムの名前エラーメッセージ	サービス管理 SDK の例外が原因で、レルムを削除できないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
431	INFO	レルムの属性値を取得しようとしています	レルムの名前	レルムプロファイルページを表示したとき。	
432	INFO	レルムの属性値の取得に成功しました。	レルムの名前	レルムプロファイルページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
433	SEVERE	レルムの属性値の取得に失敗しました。	レルムの名前 エラーメッセージ	サービス管理の SDK の例外が原因で、レルム内の属性値を取得できないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
441	INFO	レルムのプロファイルを変更しようとしています	レルムの名前	レルムプロファイルページの「保存」ボタンをクリックしたとき。	
442	INFO	レルムのプロファイルの変更に成功しました。	レルムの名前	レルムプロファイルページの「保存」ボタンをクリックしたとき。	
443	SEVERE	レルムのプロファイルの変更に失敗しました。	レルムの名前 エラーメッセージ	サービス管理 SDK の例外が原因で、レルムのプロファイルを変更できないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
501	INFO	レルムの委譲対象を取得しようとしています	レルムの名前 検索パターン	委譲メインページを表示したとき。	
502	INFO	レルムの委譲対象の取得に成功しました。	レルムの名前 検索パターン	委譲メインページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
503	SEVERE	レルムの委譲対象の取得に失敗しました。	レルムの名前 検索パターン エラーメッセージ	委譲対象を取得できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、委譲管理のログを調べてください。
504	SEVERE	レルムの委譲対象の取得に失敗しました。	レルムの名前 検索パターン エラーメッセージ	委譲管理 SDK に関連するエラーが原因で、委譲対象を取得できないとき。	詳細な情報が必要な場合は、委譲管理のログを調べてください。
511	INFO	委譲対象の権限を取得しようとしています	レルムの名前 委譲対象の *ID*	委譲対象プロファイルページを表示したとき。	
512	INFO	委譲対象の権限の取得に成功しました。	レルムの名前 委譲対象の *ID*	委譲対象プロファイルページを表示したとき。	
513	SEVERE	委譲対象の権限の取得に失敗しました。	レルムの名前 委譲対象の *ID*エラーメッセージ	委譲対象の権限を取得できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、委譲管理のログを調べてください。

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
514	SEVERE	委譲対象の権限の取得に失敗しました。	レルムの名前 委譲対象の *ID*エラーメッセージ	委譲管理 SDK に関連するエラーが原因で、委譲対象の権限を取得できないとき。	詳細な情報が必要な場合は、委譲管理のログを調べてください。
521	INFO	委譲権限を変更しようとしています	レルムの名前 委譲権限の *ID*対象の *ID*	委譲対象プロファイルページの「保存」ボタンをクリックしたとき。	
522	INFO	委譲権限の変更に成功しました。	レルムの名前 委譲権限の *ID*対象の *ID*	委譲対象プロファイルページの「保存」ボタンをクリックしたとき。	
523	SEVERE	委譲権限の変更に失敗しました。	レルムの名前 委譲権限の *ID*対象の *ID*エラーメッセージ	委譲権限を変更できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、委譲管理のログを調べてください。
524	SEVERE	委譲権限の変更に失敗しました。	レルムの名前 委譲権限の *ID*対象の *ID*エラーメッセージ	委譲管理 SDK に関連するエラーが原因で、委譲権限を変更できないとき。	詳細な情報が必要な場合は、委譲管理のログを調べてください。
601	INFO	データストア名を取得しようとしています	レルムの名前	データストアメインページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
602	INFO	データストア名の取得に成功しました。	レルムの名前	データストアメインページを表示したとき。	
603	SEVERE	データストア名の取得に失敗しました。	レルムの名前 エラーメッセージ	データストア名を取得できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
604	SEVERE	データストア名の取得に失敗しました。	レルムの名前 エラーメッセージ	サービス管理SDK の例外が原因で、データストア名を取得できないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
611	INFO	アイデンティティーリポジトリの属性値を取得しようとしています。	レルムの名前 アイデンティティーリポジトリの名前	データストアプロファイルページを表示したとき。	
612	INFO	データストアの属性値の取得に成功しました。	レルムの名前 アイデンティティーリポジトリの名前	データストアプロファイルページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
613	SEVERE	データストアの属性値の取得に失敗しました。	レルムの名前 アイデンティティーリポジトリの名前 エラーメッセージ	アイデンティティーリポジトリの属性値を取得できないとき。 ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
614	SEVERE	データストアの属性値の取得に失敗しました。	レルムの名前 アイデンティティーリポジトリの名前 エラーメッセージ	サービス管理SDK の例外が原因で、データストアの属性値を取得できないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
621	INFO	アイデンティティーリポジトリを作成しようとしています。	レルムの名前 アイデンティティーリポジトリの名前 アイデンティティーリポジトリのタイプ	データストア作成ページの「新規」ボタンをクリックしたとき。	
622	INFO	データストアの作成に成功しました。	レルムの名前 アイデンティティーリポジトリの名前 アイデンティティーリポジトリのタイプ	データストア作成ページの「新規」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
623	SEVERE	データストアの作成に失敗しました。	レルムの名前 アイデンティティーリポジトリの名前 アイデンティティーリポジトリのタイプ エラーメッセージ	アイデンティティーリポジトリを作成できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
624	SEVERE	データストアの作成に失敗しました。	レルムの名前 アイデンティティーリポジトリの名前 アイデンティティーリポジトリのタイプ エラーメッセージ	サービス管理SDK の例外が原因で、データストアを作成できないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
631	INFO	アイデンティティーリポジトリを削除しようとしています	レルムの名前 アイデンティティーリポジトリの名前	データストアメインページの「削除」ボタンをクリックしたとき。	
632	INFO	データストアの削除に成功しました。	レルムの名前 アイデンティティーリポジトリの名前	データストアメインページの「削除」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
633	SEVERE	データストアの削除に失敗しました。	レルムの名前 アイデンティティーリポジトリの名前エラーメッセージ	アイデンティティーリポジトリを削除できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
634	SEVERE	データストアの削除に失敗しました。	レルムの名前 アイデンティティーリポジトリの名前エラーメッセージ	サービス管理SDK の例外が原因で、データストアを削除できないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
641	INFO	アイデンティティーリポジトリを変更しようとしています	レルムの名前 アイデンティティーリポジトリの名前	データストアプロファイルページの「保存」ボタンをクリックしたとき。	
642	INFO	データストアの変更に成功しました。	レルムの名前 アイデンティティーリポジトリの名前	データストアプロファイルページの「保存」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
643	SEVERE	データストアの変更に失敗しました。	レルムの名前 アイデンティティーリポジトリの名前エラーメッセージ	アイデンティティーリポジトリを変更できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
644	SEVERE	データストアの変更に失敗しました。	レルムの名前 アイデンティティーリポジトリの名前エラーメッセージ	サービス管理SDK の例外が原因で、データストアを変更できないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
701	INFO	レルムに割り当てられたサービスを取得しようとしています。	レルムの名前	レルムのサービスメインページを表示したとき。	
702	INFO	レルムに割り当てられたサービスの取得に成功しました。	レルムの名前	レルムのサービスメインページを表示したとき。	
703	SEVERE	レルムに割り当てられたサービスの取得に失敗しました。	レルムの名前 エラーメッセージ	認証設定の例外が原因で、レルムに割り当てられたサービスを取得できないとき。	詳細な情報が必要な場合は、認証のログを調べてください。

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
704	SEVERE	レルムに割り当てられたサービスの取得に失敗しました。	レルムの名前 エラーメッセージ	サービス管理SDK の例外が原因で、レルムに割り当てられたサービスを取得できないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
705	SEVERE	レルムに割り当てられたサービスの取得に失敗しました。	レルムの名前 エラーメッセージ	データストア SDK の例外が原因で、レルムに割り当てられたサービスを取得できないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
706	SEVERE	レルムに割り当てられたサービスの取得に失敗しました。	レルムの名前 エラーメッセージ	レルムに割り当てられたサービスを取得できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
711	INFO	レルムに割り当て可能なサービスを取得しようとしています	レルムの名前	レルムのサービスメインページを表示したとき。	
712	INFO	レルムに割り当て可能なサービスの取得に成功しました。	レルムの名前	レルムのサービスメインページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
713	SEVERE	レルムに割り当て可能なサービスの取得に失敗しました。	レルムの名前 エラーメッセージ	認証設定の例外が原因で、レルムに割り当て可能なサービスを取得できないとき。	詳細な情報が必要な場合は、認証のログを調べてください。
714	SEVERE	レルムに割り当て可能なサービスの取得に失敗しました。	レルムの名前 エラーメッセージ	サービス管理SDK の例外が原因で、レルムに割り当て可能なサービスを取得できないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
715	SEVERE	レルムに割り当て可能なサービスの取得に失敗しました。	レルムの名前 エラーメッセージ	ID リポジトリ管理SDK の例外が原因で、レルムに割り当て可能なサービスを取得できないとき。	詳細な情報が必要な場合は、ID リポジトリ管理のログを調べてください。
716	SEVERE	レルムに割り当て可能なサービスの取得に失敗しました。	レルムの名前 エラーメッセージ	レルムに割り当て可能なサービスを取得できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、サービス管理のログを調べてください。

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
721	INFO	サービスの割り当てをレルムから解除しようとしています	レルムの名前 サービスの名前	レルムのサービスページの「割り当て解除」ボタンをクリックしたとき。	
722	INFO	サービスの割り当てをレルムから解除することに成功しました。	レルムの名前 サービスの名前	レルムのサービスページの「割り当て解除」ボタンをクリックしたとき。	
723	SEVERE	サービスの割り当てをレルムから解除することに失敗しました。	レルムの名前 サービスの名前エラーメッセージ	サービス管理SDK の例外が原因で、サービスの割り当てをレルムから解除できないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
725	SEVERE	サービスの割り当てをレルムから解除することに失敗しました。	レルムの名前 サービスの名前エラーメッセージ	サービスの割り当てをレルムから解除できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、データストア管理のログを調べてください。
724	SEVERE	サービスの割り当てをレルムから解除することに失敗しました。	レルムの名前 サービスの名前エラーメッセージ	データストア管理SDK の例外が原因で、サービスの割り当てをレルムから解除できないとき。	詳細な情報が必要な場合は、データストア管理のログを調べてください。

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
731	INFO	サービスをレルムに割り当てようとしています	レルムの名前 サービスの名前	レルムのサービスページの「割り当て」ボタンをクリックしたとき。	
732	INFO	レルムへのサービスの割り当てに成功しました。	レルムの名前 サービスの名前	レルムのサービスページの「割り当て」ボタンをクリックしたとき。	
733	SEVERE	レルムへのサービスの割り当てに失敗しました。	レルムの名前 サービスの名前エラーメッセージ	サービス管理SDK の例外が原因で、レルムにサービスを割り当てることができないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
734	SEVERE	レルムへのサービスの割り当てに失敗しました。	レルムの名前 サービスの名前エラーメッセージ	レルムにサービスを割り当てることができないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
735	SEVERE	レルムへのサービスの割り当てに失敗しました。	レルムの名前 サービスの名前エラーメッセージ	データストア SDK の例外が原因で、レルムにサービスを割り当てることができないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
741	INFO	レルム内のサービスの属性値を取得しようとしています	レルムの名前 サービスの名前属性スキーマの名前	レルムのサービスプロファイルページを表示したとき。	
742	INFO	レルム内のサービスの属性値の取得に成功しました。	レルムの名前 サービスの名前属性スキーマの名前	レルムのサービスプロファイルページを表示したとき。	
743	SEVERE	レルム内のサービスの属性値の取得に失敗しました。	レルムの名前 サービスの名前属性スキーマの名前エラーメッセージ	サービス管理SDK の例外が原因で、サービスの属性値を取得できないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
744	INFO	レルム内のサービスの属性値の取得に失敗しました。	レルムの名前 サービスの名前属性スキーマの名前エラーメッセージ	データストア SDK の例外が原因で、サービスの属性値を取得できないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
745	SEVERE	レルム内のサービスの属性値の取得に失敗しました。	レルムの名前 サービスの名前属性スキーマの名前エラーメッセージ	サービスの属性値を取得できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
751	INFO	レルム内のサービスの属性値を変更しようとしています	レルムの名前 サービスの名前	レルムのサービスプロファイルページの「保存」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
752	INFO	レルム内のサービスの属性値の変更に成功しました。	レルムの名前 サービスの名前	レルムのサービスプロファイルページの「保存」ボタンをクリックしたとき。	
753	SEVERE	レルム内のサービスの属性値の変更に失敗しました。	レルムの名前 サービスの名前エラーメッセージ	サービス管理SDK の例外が原因で、サービスの属性値を変更できないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
754	SEVERE	レルム内のサービスの属性値の変更に失敗しました。	レルムの名前 サービスの名前エラーメッセージ	データストアエラーが原因で、サービスの属性値を変更できないとき。	詳細な情報が必要な場合は、データストアのログを調べてください。
755	SEVERE	レルム内のサービスの属性値の変更に失敗しました。	レルムの名前 サービスの名前エラーメッセージ	サービスの属性値を変更できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、データストアのログを調べてください。
801	INFO	認証タイプを取得しようとしています		認証プロファイルページを表示したとき。	
802	INFO	認証タイプの取得に成功しました。		認証プロファイルページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
803	SEVERE	認証タイプの取得に失敗しました。	エラーメッセージ	認証設定 SDK の例外が原因で、認証タイプを取得できないとき。	詳細な情報が必要な場合は、認証管理のログを調べてください。
811	INFO	レルム内の認証インスタンスを取得しようとしています	レルムの名前	認証プロファイルページを表示したとき。	
812	INFO	レルム内の認証インスタンスの取得に成功しました。	レルムの名前	認証プロファイルページを表示したとき。	
813	SEVERE	レルム内の認証インスタンスの取得に失敗しました。	レルムの名前エラーメッセージ	認証設定 SDK の例外が原因で、認証インスタンスを取得できないとき。	詳細な情報が必要な場合は、認証管理のログを調べてください。
821	INFO	レルム内の認証インスタンスを消去しようとしています	レルムの名前認証インスタンスの名前	認証プロファイルページを表示したとき。	
822	INFO	レルム内の認証インスタンスの消去に成功しました。	レルムの名前認証インスタンスの名前	認証プロファイルページを表示したとき。	
823	SEVERE	レルム内の認証インスタンスの消去に失敗しました。	レルムの名前認証インスタンスの名前エラーメッセージ	認証設定 SDK の例外が原因で、認証インスタンスを消去できないとき。	詳細な情報が必要な場合は、認証管理のログを調べてください。
831	INFO	レルムに認証インスタンスを作成しようとしています	レルムの名前認証インスタンスの名前認証インスタンスのタイプ	認証作成ページの「新規」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
832	INFO	レルムへの認証インスタンスの作成に成功しました。	レルムの名前 認証インスタンスの名前認証インスタンスのタイプ	認証作成ページの「新規」ボタンをクリックしたとき。	
833	SEVERE	レルムへの認証インスタンスの作成に失敗しました。	レルムの名前 認証インスタンスの名前認証インスタンスのタイプエラーメッセージ	認証設定 SDK の例外が原因で、認証インスタンスを作成できないとき。	詳細な情報が必要な場合は、認証設定のログを調べてください。
841	INFO	認証インスタンスを変更しようとしています	レルムの名前 認証サービスの名前	認証プロファイルページの「保存」ボタンをクリックしたとき。	
842	INFO	認証インスタンスの変更に成功しました。	レルムの名前 認証サービスの名前	認証プロファイルページの「保存」ボタンをクリックしたとき。	
843	SEVERE	認証インスタンスの変更に失敗しました。	レルムの名前 認証サービスの名前エラーメッセージ	サービス管理 SDK の例外が原因で、認証インスタンスを変更できないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
844	SEVERE	認証インスタンスの変更に失敗しました。	レルムの名前 認証サービスの名前エラーメッセージ	認証インスタンスを変更できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
851	INFO	認証インスタンスのプロファイルを取得しようとしています	レルムの名前 認証インスタンスの名前	認証インスタンスプロファイルページを表示したとき。	
852	INFO	認証インスタンスのプロファイルの取得に成功しました。	レルムの名前 認証インスタンスの名前	認証インスタンスプロファイルページを表示したとき。	
853	SEVERE	認証インスタンスのプロファイルの取得に失敗しました。	レルムの名前 認証インスタンスの名前エラーメッセージ	認証設定 SDK の例外が原因で、認証インスタンスのプロファイルを取得できないとき。	詳細な情報が必要な場合は、認証管理のログを調べてください。
861	INFO	認証インスタンスのプロファイルを変更しようとしています	レルムの名前 認証インスタンスの名前	認証インスタンスプロファイルページの「保存」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
862	INFO	認証インスタンスのプロファイルの変更に成功しました。	レルムの名前 認証インスタンスの名前	認証インスタンスプロファイルページの「保存」ボタンをクリックしたとき。	
863	SEVERE	認証インスタンスのプロファイルの変更に失敗しました。	レルムの名前 認証インスタンスの名前エラーメッセージ	認証設定 SDK の例外が原因で、認証インスタンスのプロファイルを変更できないとき。	詳細な情報が必要な場合は、認証管理のログを調べてください。
864	SEVERE	認証インスタンスのプロファイルの変更に失敗しました。	レルムの名前 認証インスタンスの名前エラーメッセージ	サービス管理 SDK の例外が原因で、認証インスタンスのプロファイルを変更できないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
864	SEVERE	認証インスタンスのプロファイルの変更に失敗しました。	レルムの名前 認証インスタンスの名前エラーメッセージ	認証インスタンスのプロファイルを変更できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
871	INFO	レルム内の認証プロファイルを取得しようとしています	レルムの名前	レルムの認証プロファイルのページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
872	INFO	レルム内の認証プロファイルの取得に成功しました。	レルムの名前	レルムの認証プロファイルのページを表示したとき。	
873	SEVERE	レルム内の認証プロファイルの取得に失敗しました。	レルムの名前 エラーメッセージ	サービス管理 SDK の例外が原因で、レルム内の認証プロファイルを取得できないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
881	INFO	認証設定プロファイルを取得しようとしています	レルムの名前 認証設定の名前	認証設定プロファイルページを表示したとき。	
882	INFO	認証設定プロファイルの取得に成功しました。	レルムの名前 認証設定の名前	認証設定プロファイルページを表示したとき。	
883	SEVERE	認証設定プロファイルの取得に失敗しました。	レルムの名前 認証設定の名前 エラーメッセージ	認証設定プロファイルを取得できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
884	SEVERE	認証設定プロファイルの取得に失敗しました。	レルムの名前 認証設定の名前 エラーメッセージ	サービス管理 SDK の例外が原因で、認証設定プロファイルを取得できないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
885	SEVERE	認証設定プロファイルの取得に失敗しました。	レルムの名前 認証設定の名前 エラーメッセージ	認証設定 SDK の例外が原因で、認証設定プロファイルを取得できないとき。	詳細な情報が必要な場合は、認証設定のログを調べてください。
891	INFO	認証設定プロファイルを変更しようとしています	レルムの名前 認証設定の名前	認証設定プロファイルページの「保存」ボタンをクリックしたとき。	
892	INFO	認証設定プロファイルの変更に成功しました。	レルムの名前 認証設定の名前	認証設定プロファイルページの「保存」ボタンをクリックしたとき。	
893	SEVERE	認証設定プロファイルの変更に失敗しました。	レルムの名前 認証設定の名前 エラーメッセージ	認証設定プロファイルを変更できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
894	SEVERE	認証設定プロファイルの変更に失敗しました。	レルムの名前 認証設定の名前 エラーメッセージ	サービス管理 SDK の例外が原因で、認証設定プロファイルを変更できないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
895	SEVERE	認証設定プロファイルの変更に失敗しました。	レルムの名前 認証設定の名前 エラーメッセージ	認証設定 SDK の例外が原因で、認証設定プロファイルを変更できないとき。	詳細な情報が必要な場合は、認証設定のログを調べてください。
901	INFO	認証設定を作成しようとしています	レルムの名前 認証設定の名前	認証設定作成ページの「新規」ボタンをクリックしたとき。	
902	INFO	認証設定の作成に成功しました。	レルムの名前 認証設定の名前	認証設定作成ページの「新規」ボタンをクリックしたとき。	
903	SEVERE	認証設定の作成に失敗しました。	レルムの名前 認証設定の名前 エラーメッセージ	認証設定を作成できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
904	SEVERE	認証設定の作成に失敗しました。	レルムの名前 認証設定の名前 エラーメッセージ	サービス管理 SDK の例外が原因で、認証設定を作成できないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
905	SEVERE	認証設定の作成に失敗しました。	レルムの名前 認証設定の名前 エラーメッセージ	認証設定 SDK の例外が原因で、認証設定を作成できないとき。	詳細な情報が必要な場合は、認証設定のログを調べてください。

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
1001	INFO	エンティティー記述子名を取得しようとしています。	検索パターン	エンティティー記述子メインページを表示したとき。	
1002	INFO	エンティティー記述子名の取得に成功しました。	検索パターン	エンティティー記述子メインページを表示したとき。	
1003	SEVERE	エンティティー記述子名の取得に失敗しました。	検索パターン エラーメッセージ	連携 SDK に関連するエラーが原因で、エンティティー記述子名を取得できないとき。	詳細な情報が必要な場合は、連携のログを調べてください。
1011	INFO	エンティティー記述子を作成しようとしています。	記述子名記述子タイプ	エンティティー記述子作成ページの「新規」ボタンをクリックしたとき。	
1012	INFO	エンティティー記述子の作成に成功しました。	記述子名記述子タイプ	エンティティー記述子作成ページの「新規」ボタンをクリックしたとき。	
1013	SEVERE	エンティティー記述子の作成に失敗しました。	記述子名記述子タイプエラーメッセージ	連携 SDK に関連するエラーが原因で、エンティティー記述子を作成できないとき。	詳細な情報が必要な場合は、連携のログを調べてください。

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
1021	INFO	エンティティー記述子を削除しようとしています。	記述子名	エンティティー記述子メインページの「削除」ボタンをクリックしたとき。	
1022	INFO	エンティティー記述子の削除に成功しました	記述子名	エンティティー記述子メインページの「削除」ボタンをクリックしたとき。	
1023	SEVERE	エンティティー記述子の削除に失敗しました。	記述子名エラーメッセージ	連携 SDK に関連するエラーが原因で、エンティティー記述子を削除できないとき。	詳細な情報が必要な場合は、連携のログを調べてください。
1031	INFO	アフィリエイトエンティティー記述子の属性値を取得しようとしています。	記述子名	アフィリエイトエンティティー記述子プロファイルページを表示したとき。	
1032	INFO	アフィリエイトエンティティー記述子の属性値の取得に成功しました。	記述子名	アフィリエイトエンティティー記述子プロファイルページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
1033	SEVERE	アフィリエイトエンティティー記述子の属性値の取得に失敗しました。	記述子名エラーメッセージ	連携 SDK に関連するエラーが原因で、アフィリエイトエンティティー記述子の属性値を取得できないとき。	詳細な情報が必要な場合は、連携のログを調べてください。
1041	INFO	アフィリエイトエンティティー記述子を変更しようとしています。	記述子名	アフィリエイトエンティティー記述子プロファイルページの「保存」ボタンをクリックしたとき。	
1042	INFO	アフィリエイトエンティティー記述子の変更に成功しました。	記述子名	アフィリエイトエンティティー記述子プロファイルページの「保存」ボタンをクリックしたとき。	
1043	SEVERE	アフィリエイトエンティティー記述子の変更に失敗しました。	記述子名エラーメッセージ	連携 SDK に関連するエラーが原因で、アフィリエイトエンティティー記述子を変更できないとき。	詳細な情報が必要な場合は、連携のログを調べてください。

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
1044	SEVERE	アフィリエイトエンティティー記述子の変更に失敗しました。	記述子名エラーメッセージ	1 つ以上の属性値の番号形式が正しくないことが原因で、アフィリエイトエンティティー記述子を変更できないとき。	詳細な情報が必要な場合は、連携のログを調べてください。
1051	INFO	エンティティー記述子の属性値を取得しようとしています。	記述子名	エンティティー記述子プロファイルページを表示したとき。	
1052	INFO	エンティティー記述子の属性値の取得に成功しました。	記述子名	エンティティー記述子プロファイルページを表示したとき。	
1053	SEVERE	エンティティー記述子の属性値の取得に失敗しました。	記述子名エラーメッセージ	連携 SDK に関連するエラーが原因で、エンティティー記述子の属性値を取得できないとき。	詳細な情報が必要な場合は、連携のログを調べてください。
1061	INFO	エンティティー記述子を変更しようとしています。	記述子名	エンティティー記述子プロファイルページの「保存」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
1062	INFO	エンティティー記述子の変更に成功しました。	記述子名	エンティティー記述子プロファイルページの「保存」ボタンをクリックしたとき。	
1063	SEVERE	エンティティー記述子の変更に失敗しました。	記述子名エラーメッセージ	連携 SDK に関連するエラーが原因で、エンティティー記述子を変更できないとき。	詳細な情報が必要な場合は、連携のログを調べてください。
1101	INFO	認証ドメイン名を取得しようとしています。	検索パターン	認証ドメインメインページを表示したとき。	
1102	INFO	認証ドメイン名の取得に成功しました。	検索パターン	認証ドメインメインページを表示したとき。	
1103	SEVERE	認証ドメイン名の取得に失敗しました。	検索パターンエラーメッセージ	連携 SDK に関連するエラーが原因で、認証ドメイン名を取得できないとき。	詳細な情報が必要な場合は、連携のログを調べてください。
1111	INFO	認証ドメインを作成しようとしています	認証ドメインの名前	認証ドメイン作成ページの「新規」ボタンをクリックしたとき。	
1112	INFO	認証ドメインの作成に成功しました。	認証ドメインの名前	認証ドメイン作成ページの「新規」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
1113	SEVERE	認証ドメインの作成に失敗しました。	認証ドメインの名前エラーメッセージ	連携 SDK に関連するエラーが原因で、認証ドメインを作成できないとき。	詳細な情報が必要な場合は、連携のログを調べてください。
1121	INFO	認証ドメインを削除しようとしています	認証ドメインの名前	認証ドメインメインページの「削除」ボタンをクリックしたとき。	
1122	INFO	認証ドメインの削除に成功しました。	認証ドメインの名前	認証ドメインメインページの「削除」ボタンをクリックしたとき。	
1123	SEVERE	認証ドメインの削除に失敗しました。	認証ドメインの名前エラーメッセージ	連携 SDK に関連するエラーが原因で、認証ドメインを削除できないとき。	詳細な情報が必要な場合は、連携のログを調べてください。
1131	INFO	認証ドメインの属性値を取得しようとしています	認証ドメインの名前	認証ドメインプロファイルページを表示したとき。	
1132	INFO	認証ドメインの属性値の取得に成功しました。	認証ドメインの名前	認証ドメインプロファイルページを表示したとき。	
1133	SEVERE	認証ドメインの属性値の取得に失敗しました。	認証ドメインの名前エラーメッセージ	連携 SDK に関連するエラーが原因で、認証ドメインの属性値を取得できないとき。	詳細な情報が必要な場合は、連携のログを調べてください。

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
1141	INFO	認証ドメインを変更しようとしています	認証ドメインの名前	認証ドメインプロファイルページの「保存」ボタンをクリックしたとき。	
1142	INFO	認証ドメインの変更に成功しました。	認証ドメインの名前	認証ドメインプロファイルページの「保存」ボタンをクリックしたとき。	
1143	SEVERE	認証ドメインの変更に失敗しました。	認証ドメインの名前エラーメッセージ	連携 SDK に関連するエラーが原因で、認証ドメインを変更できないとき。	詳細な情報が必要な場合は、連携のログを調べてください。
1151	INFO	すべてのプロバイダ名を取得しようとしています		認証ドメインプロファイルページを表示したとき。	
1152	INFO	すべてのプロバイダ名の取得に成功しました。		認証ドメインプロファイルページを表示したとき。	
1153	SEVERE	すべてのプロバイダ名の取得に失敗しました。	エラーメッセージ	連携 SDK に関連するエラーが原因で、すべてのプロバイダ名を取得できないとき。	詳細な情報が必要な場合は、連携のログを調べてください。
1161	INFO	認証ドメイン内のプロバイダ名を取得しようとしています。	認証ドメインの名前	認証ドメインプロファイルページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
1162	INFO	認証ドメイン内のプロバイダ名の取得に成功しました。	認証ドメインの名前	認証ドメインプロファイルページを表示したとき。	
1163	SEVERE	認証ドメイン内のプロバイダ名の取得に失敗しました。	認証ドメインの名前エラーメッセージ	連携 SDK に関連するエラーが原因で、認証ドメイン内のプロバイダ名を取得できないとき。	詳細な情報が必要な場合は、連携のログを調べてください。
1171	INFO	認証ドメインにプロバイダを追加しようとしています	認証ドメインの名前プロバイダの名前	プロバイダ割り当てページの「保存」ボタンをクリックしたとき。	
1172	INFO	認証ドメインへのプロバイダの追加に成功しました。	認証ドメインの名前プロバイダの名前	プロバイダ割り当てページの「保存」ボタンをクリックしたとき。	
1173	SEVERE	認証ドメインへのプロバイダの追加に失敗しました。	認証ドメインの名前プロバイダの名前エラーメッセージ	連携 SDK に関連するエラーが原因で、認証ドメインにプロバイダを追加できないとき。	詳細な情報が必要な場合は、連携のログを調べてください。
1181	INFO	認証ドメインからプロバイダを消去しようとしています	認証ドメインの名前プロバイダの名前	プロバイダ割り当てページの「保存」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
1182	INFO	認証ドメインからのプロバイダの削除に成功しました。	認証ドメインの名前プロバイダの名前	プロバイダ割り当てページの「保存」ボタンをクリックしたとき。	
1183	SEVERE	認証ドメインからのプロバイダの削除に失敗しました。	認証ドメインの名前プロバイダの名前エラーメッセージ	連携 SDK に関連するエラーが原因で、認証ドメインからプロバイダを消去できないとき。	詳細な情報が必要な場合は、連携のログを調べてください。
1301	INFO	プロバイダを作成しようとしています	プロバイダの名前プロバイダのロールプロバイダのタイプ	プロバイダ割り当てページの「保存」ボタンをクリックしたとき。	
1302	INFO	プロバイダの作成に成功しました。	プロバイダの名前プロバイダのロールプロバイダのタイプ	プロバイダ割り当てページの「保存」ボタンをクリックしたとき。	
1303	SEVERE	プロバイダの作成に失敗しました。	プロバイダの名前プロバイダのロールプロバイダのタイプエラーメッセージ	連携 SDK に関連するエラーが原因で、プロバイダを作成できないとき。	詳細な情報が必要な場合は、連携のログを調べてください。
1303	SEVERE	プロバイダの作成に失敗しました。	プロバイダの名前プロバイダのロールプロバイダのタイプエラーメッセージ	連携 SDK に関連するエラーが原因で、プロバイダを作成できないとき。	詳細な情報が必要な場合は、連携のログを調べてください。

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
1304	SEVERE	プロバイダの作成に失敗しました。	プロバイダの名前プロバイダのロールプロバイダのタイプエラーメッセージ	管理コンソールがこのプロバイダの値を設定する方法を見つけることができないために、プロバイダを作成できないとき。	Web アプリケーションエラーです。Sun のサポートに連絡してください。
1311	INFO	プロバイダの属性値を取得しようとしています	プロバイダの名前プロバイダのロールプロバイダのタイプ	プロバイダプロファイルページを表示したとき。	
1312	INFO	プロバイダの属性値の取得に成功しました。	プロバイダの名前プロバイダのロールプロバイダのタイプ	プロバイダプロファイルページを表示したとき。	
1321	INFO	プロバイダへのハンドラを取得しようとしています	プロバイダの名前プロバイダのロール	プロバイダプロファイルページを表示したとき。	
1322	INFO	プロバイダへのハンドラの取得に成功しました。	プロバイダの名前プロバイダのロール	プロバイダプロファイルページを表示したとき。	
1323	SEVERE	プロバイダへのハンドラの取得に失敗しました。	プロバイダの名前プロバイダのロールエラーメッセージ	連携 SDK に関連するエラーが原因で、プロバイダへのハンドラを取得できないとき。	詳細な情報が必要な場合は、連携のログを調べてください。
1331	INFO	プロバイダを変更しようとしています	プロバイダの名前プロバイダのロール	プロバイダプロファイルページの「保存」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
1332	INFO	プロバイダの変更に成功しました。	プロバイダの名前プロバイダのロール	プロバイダプロファイルページの「保存」ボタンをクリックしたとき。	
1333	SEVERE	プロバイダの変更に失敗しました。	プロバイダの名前プロバイダのロールエラーメッセージ	連携 SDK に関連するエラーが原因で、プロバイダを変更できないとき。	詳細な情報が必要な場合は、連携のログを調べてください。
1334	SEVERE	プロバイダの変更に失敗しました。	プロバイダの名前プロバイダのロールエラーメッセージ	管理コンソールがこのプロバイダの値を設定する方法を見つけることができないために、プロバイダを変更できないとき。	Web アプリケーションエラーです。Sun のサポートに連絡してください。
1341	INFO	プロバイダを削除しようとしています	プロバイダの名前プロバイダのロール	プロバイダプロファイルページの「プロバイダの削除」ボタンをクリックしたとき。	
1342	INFO	プロバイダの削除に成功しました。	プロバイダの名前プロバイダのロール	プロバイダプロファイルページの「プロバイダの削除」ボタンをクリックしたとき。	
1343	SEVERE	プロバイダの削除に失敗しました。	プロバイダの名前プロバイダのロールエラーメッセージ	連携 SDK に関連するエラーが原因で、プロバイダを削除できないとき。	詳細な情報が必要な場合は、連携のログを調べてください。

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
1351	INFO	見込み信頼プロバイダを取得しようとしています	プロバイダの名前プロバイダのロール	信頼プロバイダを追加するページを表示したとき。	
1352	INFO	見込み信頼プロバイダの取得に成功しました。	プロバイダの名前プロバイダのロール	信頼プロバイダを追加するページを表示したとき。	
1353	SEVERE	見込み信頼プロバイダの取得に失敗しました。	プロバイダの名前プロバイダのロールエラーメッセージ	連携 SDK に関連するエラーが原因で、見込み信頼プロバイダを取得できないとき。	詳細な情報が必要な場合は、連携のログを調べてください。
2001	INFO	サービススキーマのスキーマタイプの属性値を取得しようとしています	サービスの名前スキーマタイプの名前属性スキーマの名前	サービスプロファイルページを表示したとき。	
2002	INFO	サービススキーマのスキーマタイプの属性値の取得に成功しました。	サービスの名前スキーマタイプの名前属性スキーマの名前	サービスプロファイルページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
2003	SEVERE	サービススキーマのスキーマタイプの属性値の取得に失敗しました。	サービスの名前スキーマタイプの名前属性スキーマの名前エラーメッセージ	サービススキーマのスキーマタイプの属性値を取得できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
2004	SEVERE	サービススキーマのスキーマタイプの属性値の取得に失敗しました。	サービスの名前スキーマタイプの名前属性スキーマの名前エラーメッセージ	サービス管理 SDK に関連するエラーが原因で、サービススキーマのスキーマタイプの属性値を取得できないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
2005	INFO	サービススキーマのスキーマタイプの属性値の取得に失敗しました。	サービスの名前スキーマタイプの名前属性スキーマの名前	サービスプロファイルページを表示したとき。	このイベントに対する対処は必要ありません。コンソールがサービスから取得しようとしたスキーマがありません。
2011	INFO	サービススキーマのスキーマタイプの属性スキーマの属性値を取得しようとしています	サービスの名前スキーマタイプの名前属性スキーマの名前	サービスプロファイルページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
2012	INFO	サービススキーマのスキーマタイプの属性スキーマの属性値の取得に成功しました。	サービスの名前スキーマタイプの名前属性スキーマの名前	サービスプロファイルページを表示したとき。	
2013	SEVERE	サービススキーマのスキーマタイプの属性スキーマの属性値の取得に失敗しました。	サービスの名前スキーマタイプの名前属性スキーマの名前エラーメッセージ	サービススキーマのスキーマタイプの属性値を取得できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
2014	SEVERE	サービススキーマのスキーマタイプの属性スキーマの属性値の取得に失敗しました。	サービスの名前スキーマタイプの名前属性スキーマの名前エラーメッセージ	サービス管理 SDK に関連するエラーが原因で、サービススキーマのスキーマタイプの属性値を取得できないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
2021	INFO	サービススキーマのスキーマタイプの属性スキーマの属性値を変更しようとしています。	サービスの名前スキーマタイプの名前属性スキーマの名前	サービスプロファイルページの「保存」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
2022	INFO	サービススキーマのスキーマタイプの属性スキーマの属性値の変更に成功しました。	サービスの名前スキーマタイプの名前属性スキーマの名前	サービスプロファイルページの「保存」ボタンをクリックしたとき。	
2023	SEVERE	サービススキーマのスキーマタイプの属性スキーマの属性値の変更に失敗しました。	サービスの名前スキーマタイプの名前属性スキーマの名前エラーメッセージ	サービススキーマのスキーマタイプの属性値を変更できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
2024	SEVERE	サービススキーマのスキーマタイプの属性スキーマの属性値の変更に失敗しました。	サービスの名前スキーマタイプの名前属性スキーマの名前エラーメッセージ	サービス管理 SDK に関連するエラーが原因で、サービススキーマのスキーマタイプの属性値を変更できないとき。	詳細な情報が必要な場合は、サービス管理のログを調べてください。
2501	INFO	クライアントディテクションサービスのデバイス名を取得しようとしています	プロファイルの名前スタイルの名前検索パターン	クライアントプロファイルページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
2502	INFO	クライアントディテクションサービスのデバイス名の取得に成功しました。	プロファイルの名前スタイルの名前検索パターン	クライアントプロファイルページを表示したとき。	
2511	INFO	クライアントディテクションサービスでクライアントを削除しようとしています。	クライアントのタイプ	クライアントタイプを削除するハイパーリンクページをクリックしたとき。	
2512	INFO	クライアントディテクションサービスでクライアントの削除に成功しました。	クライアントのタイプ	クライアントタイプを削除するハイパーリンクページをクリックしたとき。	
2513	SEVERE	クライアントディテクションサービスでクライアントの削除に失敗しました。	クライアントのタイプエラーメッセージ	クライアントディテクション SDK に関連するエラーが原因で、クライアントを削除できないとき。	詳細な情報が必要な場合は、クライアントディテクション管理のログを調べてください。
2521	INFO	クライアントディテクションサービスでクライアントを作成しようとしています	クライアントのタイプ	クライアント作成ページの「新規」ボタンをクリックしたとき。	
2522	INFO	クライアントディテクションサービスでクライアントの作成に成功しました。	クライアントのタイプ	クライアント作成ページの「新規」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
2523	SEVERE	クライアントディテクションサービスでクライアントの作成に失敗しました。	クライアントのタイプエラーメッセージ	クライアントディテクション SDK に関連するエラーが原因で、クライアントを作成できないとき。	詳細な情報が必要な場合は、クライアントディテクション管理のログを調べてください。
2524	INFO	クライアントディテクションサービスでクライアントの作成に失敗しました。	クライアントのタイプエラーメッセージ	クライアントタイプが無効なために、クライアントを作成できないとき。	もう一度クライアントタイプを確認してから作成してください。
2531	INFO	クライアントディテクションサービスでクライアントプロファイルを取得しようとしています	クライアントのタイプ分類	クライアントプロファイルページを表示したとき。	
2532	INFO	クライアントディテクションサービスでクライアントプロファイルの取得に成功しました。	クライアントのタイプ分類	クライアントプロファイルページを表示したとき。	
2541	INFO	クライアントディテクションサービスでクライアントプロファイルを変更しようとしています。	クライアントのタイプ	クライアントプロファイルページの「保存」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
2542	INFO	クライアントディテクションサービスでクライアントプロファイルの変更に成功しました。	クライアントのタイプ	クライアントプロファイルページの「保存」ボタンをクリックしたとき。	
2543	SEVERE	クライアントディテクションサービスでクライアントプロファイルの変更に失敗しました。	クライアントのタイプエラーメッセージ	クライアントディテクション SDK に関連するエラーが原因で、クライアントプロファイルを変更できないとき。	詳細な情報が必要な場合は、クライアントディテクション管理のログを調べてください。
3001	INFO	現在のセッションを取得しようとしています	サーバーの名前検索パターン	セッションメインページを表示したとき。	
3002	INFO	現在のセッションの取得に成功しました。	サーバーの名前検索パターン	セッションメインページを表示したとき。	
3003	SEVERE	現在のセッションの取得に失敗しました。	サーバーの名前レルムの名前エラーメッセージ	セッション SDK の例外が原因で、現在のセッションを取得できないとき。	詳細な情報が必要な場合は、セッション管理のログを調べてください。
3011	INFO	セッションを無効にしようとしています	サーバーの名前セッションの *ID*	セッションメインページの「無効にする」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
3012	INFO	セッションを無効することに成功しました。	サーバーの名前セッションの *ID*	セッションメインページの「無効にする」ボタンをクリックしたとき。	
3013	SEVERE	セッションを無効にすることに失敗しました。	サーバーの名前セッションの *ID*エラーメッセージ	セッション SDK の例外が原因で、セッションを無効にできないとき。	詳細な情報が必要な場合は、セッション管理のログを調べてください。
10001	INFO	組織内のコンテナを検索しようとしています	組織の DN 検索パターン	組織のコンテナページの「検索」ボタンをクリックしたとき。	
10002	INFO	組織内のコンテナの検索に成功しました。	組織の DN 検索パターン	組織のコンテナページの「検索」ボタンをクリックしたとき。	
10003	SEVERE	組織内のコンテナの検索に失敗しました。	組織の DN 検索パターンエラーメッセージ	コンテナを検索できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10004	SEVERE	組織内のコンテナの検索に失敗しました。	組織の DN 検索パターン エラーメッセージ	アクセス管理 SDK の例外が原因で、コンテナを検索できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10011	INFO	コンテナ内のコンテナを検索しようとしています	コンテナの DN検索パターン	コンテナのサブコンテナページの「検索」ボタンをクリックしたとき。	
10012	INFO	コンテナ内のコンテナの検索に成功しました。	コンテナの DN検索パターン	コンテナのサブコンテナページの「検索」ボタンをクリックしたとき。	
10013	SEVERE	コンテナ内のコンテナの検索に失敗しました。	コンテナの DN検索パターンエラーメッセージ	コンテナを検索できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10014	SEVERE	コンテナ内のコンテナの検索に失敗しました。	コンテナの DN検索パターンエラーメッセージ	アクセス管理 SDK の例外が原因で、コンテナを検索できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10021	INFO	組織内にコンテナを作成しようとしています	組織の DN コンテナの名前	コンテナ作成ページの「新規」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10022	INFO	組織内のコンテナの作成に成功しました。	組織の DN コンテナの名前	コンテナ作成ページの「新規」ボタンをクリックしたとき。	
10023	SEVERE	組織内のコンテナの作成に失敗しました。	組織の DN コンテナの名前 エラーメッセージ	コンテナを作成できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10024	SEVERE	組織内のコンテナの作成に失敗しました。	組織の DN コンテナの名前 エラーメッセージ	アクセス管理 SDK の例外が原因で、コンテナを作成できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10031	INFO	コンテナ内のコンテナを作成しようとしています	コンテナの DNコンテナの名前	コンテナ作成ページの「新規」ボタンをクリックしたとき。	
10032	INFO	コンテナ内のコンテナの作成に成功しました。	コンテナの DNコンテナの名前	コンテナ作成ページの「新規」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10033	SEVERE	コンテナ内のコンテナの作成に失敗しました。	コンテナのDNコンテナの名前エラーメッセージ	コンテナを作成できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10034	SEVERE	コンテナ内のコンテナの作成に失敗しました。	コンテナのDNコンテナの名前エラーメッセージ	アクセス管理 SDK の例外が原因で、コンテナを作成できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10041	INFO	コンテナに割り当てられたサービスを取得しようとしています	コンテナの DN	コンテナのサービスプロファイルページを表示したとき。	
10042	INFO	コンテナに割り当てられたサービスの取得に成功しました。	コンテナの DN	コンテナのサービスプロファイルページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10043	SEVERE	コンテナに割り当てられたサービスの取得に失敗しました。	コンテナのDNエラーメッセージ	コンテナに割り当てられたサービスを取得できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10044	SEVERE	コンテナに割り当てられたサービスの取得に失敗しました。	コンテナのDNエラーメッセージ	アクセス管理 SDK の例外が原因で、コンテナに割り当てられたサービスを取得できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10101	INFO	組織のサービステンプレートを取得しようとしています。	組織の DN サービスの名前 テンプレートのタイプ	組織のサービスプロファイルページを表示したとき。	
10102	INFO	組織のサービステンプレートの取得に成功しました。	組織の DN サービスの名前 テンプレートのタイプ	組織のサービスプロファイルページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10103	SEVERE	組織のサービステンプレートの取得に失敗しました。	組織の DN サービスの名前 テンプレートのタイプ エラーメッセージ	サービステンプレートを取得できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10104	SEVERE	組織のサービステンプレートの取得に失敗しました。	組織の DN サービスの名前 テンプレートのタイプ エラーメッセージ	アクセス管理 SDK の例外が原因で、サービステンプレートを取得できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10111	INFO	コンテナのサービステンプレートを取得しようとしています。	コンテナの DNサービスの名前テンプレートのタイプ	コンテナのサービスプロファイルページを表示したとき。	
10112	INFO	コンテナのサービステンプレートの取得に成功しました。	コンテナの DNサービスの名前テンプレートのタイプ	コンテナのサービスプロファイルページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10113	SEVERE	コンテナのサービステンプレートの取得に失敗しました。	コンテナのDNサービスの名前テンプレートのタイプエラーメッセージ	サービステンプレートを取得できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10114	SEVERE	コンテナのサービステンプレートの取得に失敗しました。	コンテナのDNサービスの名前テンプレートのタイプエラーメッセージ	アクセス管理 SDK の例外が原因で、サービステンプレートを取得できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10121	INFO	ディレクトリオブジェクトを削除しようとしています	オブジェクトの名前	オブジェクトメインページの「削除」ボタンをクリックしたとき。	
10122	INFO	ディレクトリオブジェクトの削除に成功しました。	オブジェクトの名前	オブジェクトメインページの「削除」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10123	SEVERE	ディレクトリオブジェクトの削除に失敗しました。	オブジェクトの名前エラーメッセージ	ディレクトリオブジェクトを削除できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10124	SEVERE	ディレクトリオブジェクトの削除に失敗しました。	オブジェクトの名前エラーメッセージ	アクセス管理 SDK の例外が原因で、ディレクトリオブジェクトを削除できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10131	INFO	ディレクトリオブジェクトを変更しようとしています	オブジェクトの DN	オブジェクトプロファイルページをクリックしたとき。	
10132	INFO	ディレクトリオブジェクトの変更に成功しました。	オブジェクトの DN	オブジェクトプロファイルページをクリックしたとき。	
10133	SEVERE	ディレクトリオブジェクトの変更に失敗しました。	オブジェクトの DNエラーメッセージ	アクセス管理 SDK の例外が原因で、ディレクトリオブジェクトを変更できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10141	INFO	組織からサービスを削除しようとしています	組織の DN サービスの名前	組織のサービスページの「割り当て解除」ボタンをクリックしたとき。	
10142	INFO	組織からサービスを削除することに成功しました。	組織の DN サービスの名前	組織のサービスページの「割り当て解除」ボタンをクリックしたとき。	
10143	SEVERE	組織からサービスを削除することに失敗しました。	組織の DN サービスの名前エラーメッセージ	サービスを削除できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10144	SEVERE	組織からサービスを削除することに失敗しました。	組織の DN サービスの名前 エラーメッセージ	アクセス管理 SDK の例外が原因で、サービスを削除できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10151	INFO	コンテナからサービスを削除しようとしています	コンテナの DNサービスの名前	コンテナのサービスページの「割り当て解除」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10152	INFO	コンテナからサービスを削除することに成功しました。	コンテナのDNサービスの名前	コンテナのサービスページの「割り当て解除」ボタンをクリックしたとき。	
10153	SEVERE	コンテナからサービスを削除することに失敗しました。	コンテナのDNサービスの名前エラーメッセージ	サービスを削除できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10154	SEVERE	コンテナからサービスを削除することに失敗しました。	コンテナのDNサービスの名前エラーメッセージ	アクセス管理 SDK の例外が原因で、サービスを削除できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10201	INFO	組織内のグループコンテナを検索しようとしています	組織の DN 検索パターン	組織のグループコンテナページの「検索」ボタンをクリックしたとき。	
10202	INFO	組織内のグループコンテナの検索に成功しました。	組織の DN 検索パターン	組織のグループコンテナページの「検索」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10203	SEVERE	組織内のグループコンテナの検索に失敗しました。	組織の DN 検索パターン エラーメッセージ	グループコンテナを検索できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10204	SEVERE	組織内のグループコンテナの検索に失敗しました。	組織の DN 検索パターン エラーメッセージ	アクセス管理 SDK の例外が原因で、グループコンテナを検索できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10211	INFO	コンテナ内のグループコンテナを検索しようとしています	コンテナの DN検索パターン	コンテナのグループコンテナページの「検索」ボタンをクリックしたとき。	
10212	INFO	コンテナ内のグループコンテナの検索に成功しました。	コンテナの DN検索パターン	コンテナのグループコンテナページの「検索」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10213	SEVERE	コンテナ内のグループコンテナの検索に失敗しました。	コンテナのDN検索パターンエラーメッセージ	グループコンテナを検索できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10214	SEVERE	コンテナ内のグループコンテナの検索に失敗しました。	コンテナのDN検索パターンエラーメッセージ	アクセス管理 SDK の例外が原因で、グループコンテナを検索できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10221	INFO	グループコンテナ内のグループコンテナを検索しようとしています	グループコンテナの DN検索パターン	グループコンテナのグループコンテナページの「検索」ボタンをクリックしたとき。	
10222	INFO	グループコンテナ内のグループコンテナの検索に成功しました。	グループコンテナの DN検索パターン	グループコンテナのグループコンテナページの「検索」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10223	SEVERE	グループコンテナ内のグループコンテナの検索に失敗しました。	グループコンテナの DN検索パターンエラーメッセージ	グループコンテナを検索できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10224	SEVERE	グループコンテナ内のグループコンテナの検索に失敗しました。	グループコンテナの DN検索パターンエラーメッセージ	アクセス管理 SDK の例外が原因で、グループコンテナを検索できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10231	INFO	組織内にグループコンテナを作成しようとしています	組織の DN グループコンテナの名前	グループコンテナ作成ページの「新規」ボタンをクリックしたとき。	
10232	INFO	組織内のグループコンテナの作成に成功しました。	組織の DNグループコンテナの名前	グループコンテナ作成ページの「新規」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10233	SEVERE	組織内のグループコンテナの作成に失敗しました。	組織の DN グループコンテナの名前 エラーメッセージ	グループコンテナを作成できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10234	SEVERE	組織内のグループコンテナの作成に失敗しました。	組織の DN グループコンテナの名前 エラーメッセージ	アクセス管理 SDK の例外が原因で、グループコンテナを作成できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10241	INFO	コンテナ内にグループコンテナを作成しようとしています	コンテナの DNグループコンテナの名前	グループコンテナ作成ページの「新規」ボタンをクリックしたとき。	
10242	INFO	コンテナ内のグループコンテナの作成に成功しました。	コンテナの DNグループコンテナの名前	グループコンテナ作成ページの「新規」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10243	SEVERE	コンテナ内のグループコンテナの作成に失敗しました。	コンテナのDNグループコンテナの名前エラーメッセージ	グループコンテナを作成できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10244	SEVERE	コンテナ内のグループコンテナの作成に失敗しました。	コンテナのDNグループコンテナの名前エラーメッセージ	アクセス管理 SDK の例外が原因で、グループコンテナを作成できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10251	INFO	グループコンテナ内にグループコンテナを作成しようとしています。	グループコンテナの DNグループコンテナの名前	グループコンテナ作成ページの「新規」ボタンをクリックしたとき。	
10252	INFO	グループコンテナ内のグループコンテナの作成に成功しました。	グループコンテナの DNグループコンテナの名前	グループコンテナ作成ページの「新規」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10253	SEVERE	グループコンテナ内のグループコンテナの作成に失敗しました。	グループコンテナの DNグループコンテナの名前エラーメッセージ	グループコンテナを作成できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10254	SEVERE	グループコンテナ内のグループコンテナの作成に失敗しました。	グループコンテナの DNグループコンテナの名前エラーメッセージ	アクセス管理 SDK の例外が原因で、グループコンテナを作成できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10301	INFO	組織内のグループを検索しようとしています	組織の DN 検索パターン	組織のグループページの「検索」ボタンをクリックしたとき。	
10302	INFO	組織内のグループの検索に成功しました。	組織の DN 検索パターン	組織のグループページの「検索」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10303	SEVERE	組織内のグループの検索に失敗しました。	組織の DN 検索パターン エラーメッセージ	グループを検索できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10304	SEVERE	組織内のグループの検索に失敗しました。	組織の DN 検索パターン エラーメッセージ	アクセス管理 SDK の例外が原因で、グループを検索できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10311	INFO	コンテナ内のグループを検索しようとしています	コンテナの DN検索パターン	コンテナのグループページの「検索」ボタンをクリックしたとき。	
10312	INFO	コンテナ内のグループの検索に成功しました。	コンテナの DN検索パターン	コンテナのグループページの「検索」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10313	SEVERE	コンテナ内のグループの検索に失敗しました。	コンテナのDN検索パターンエラーメッセージ	グループを検索できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10314	SEVERE	コンテナ内のグループの検索に失敗しました。	コンテナのDN検索パターンエラーメッセージ	アクセス管理 SDK の例外が原因で、グループを検索できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10321	INFO	静的グループ内のグループを検索しようとしています。	静的グループの DN検索パターン	静的グループのグループページの「検索」ボタンをクリックしたとき。	
10322	INFO	静的グループ内のグループの検索に成功しました。	静的グループの DN検索パターン	静的グループのグループページの「検索」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10323	SEVERE	静的グループ内のグループの検索に失敗しました。	静的グループの DN検索パターンエラーメッセージ	グループを検索できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10324	SEVERE	静的グループ内のグループの検索に失敗しました。	静的グループの DN検索パターンエラーメッセージ	アクセス管理 SDK の例外が原因で、グループを検索できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10331	INFO	動的グループ内のグループを検索しようとしています。	動的グループの DN検索パターン	動的グループのグループページの「検索」ボタンをクリックしたとき。	
10332	INFO	動的グループ内のグループの検索に成功しました。	動的グループの DN検索パターン	動的グループのグループページの「検索」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10333	SEVERE	動的グループ内のグループの検索に失敗しました。	動的グループの DN検索パターンエラーメッセージ	グループを検索できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10334	SEVERE	動的グループ内のグループの検索に失敗しました。	動的グループの DN検索パターンエラーメッセージ	アクセス管理 SDK の例外が原因で、グループを検索できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10341	INFO	割り当て可能な動的グループ内のグループを検索しようとしています。	割り当て可能な動的グループの DN検索パターン	割り当て可能な動的グループのグループページの「検索」ボタンをクリックしたとき。	
10342	INFO	割り当て可能な動的グループ内のグループの検索に成功しました。	割り当て可能な動的グループの DN検索パターン	割り当て可能な動的グループのグループページの「検索」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10343	SEVERE	割り当て可能な動的グループ内のグループの検索に失敗しました。	割り当て可能な動的グループの DN検索パターンエラーメッセージ	グループを検索できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10344	SEVERE	割り当て可能な動的グループ内のグループの検索に失敗しました。	割り当て可能な動的グループの DN検索パターンエラーメッセージ	アクセス管理 SDK の例外が原因で、グループを検索できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10351	INFO	組織内にグループを作成しようとしています	組織の DN グループの名前	グループ作成ページの「新規」ボタンをクリックしたとき。	
10352	INFO	組織内のグループの作成に成功しました。	組織の DN グループの名前	グループ作成ページの「新規」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10353	SEVERE	組織内のグループの作成に失敗しました。	組織の DN グループの名前 エラーメッセージ	グループを作成できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10354	SEVERE	組織内のグループの作成に失敗しました。	組織の DN グループの名前 エラーメッセージ	アクセス管理 SDK の例外が原因で、グループを作成できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10361	INFO	コンテナ内にグループを作成しようとしています。	コンテナの DNグループの名前	グループ作成ページの「新規」ボタンをクリックしたとき。	
10362	INFO	コンテナ内のグループの作成に成功しました。	コンテナの DNグループの名前	グループ作成ページの「新規」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10363	SEVERE	コンテナ内のグループの作成に失敗しました。	コンテナのDNグループの名前エラーメッセージ	グループを作成できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10364	SEVERE	コンテナ内のグループの作成に失敗しました。	コンテナのDNグループの名前エラーメッセージ	アクセス管理 SDK の例外が原因で、グループを作成できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10371	INFO	グループコンテナ内にグループを作成しようとしています	グループコンテナの DNグループの名前	グループ作成ページの「新規」ボタンをクリックしたとき。	
10372	INFO	グループコンテナ内のグループの作成に成功しました。	グループコンテナの DNグループの名前	グループ作成ページの「新規」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10373	SEVERE	グループコンテナ内のグループの作成に失敗しました。	グループコンテナの DNグループの名前エラーメッセージ	グループを作成できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10374	SEVERE	グループコンテナ内のグループの作成に失敗しました。	グループコンテナの DNグループの名前エラーメッセージ	アクセス管理 SDK の例外が原因で、グループを作成できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10381	INFO	動的グループ内にグループを作成しようとしています	動的グループの DNグループの名前	グループ作成ページの「新規」ボタンをクリックしたとき。	
10382	INFO	動的グループ内のグループの作成に成功しました。	動的グループの DNグループの名前	グループ作成ページの「新規」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10383	SEVERE	動的グループ内のグループの作成に失敗しました。	動的グループの DNグループの名前エラーメッセージ	グループを作成できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10384	SEVERE	動的グループ内のグループの作成に失敗しました。	動的グループの DNグループの名前エラーメッセージ	アクセス管理 SDK の例外が原因で、グループを作成できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10391	INFO	静的グループ内にグループを作成しようとしています	静的グループの DNグループの名前	グループ作成ページの「新規」ボタンをクリックしたとき。	
10392	INFO	静的グループ内のグループの作成に成功しました。	静的グループの DNグループの名前	グループ作成ページの「新規」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10393	SEVERE	静的グループ内のグループの作成に失敗しました。	静的グループの DNグループの名前エラーメッセージ	グループを作成できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10394	SEVERE	静的グループ内のグループの作成に失敗しました。	静的グループの DNグループの名前エラーメッセージ	アクセス管理 SDK の例外が原因で、グループを作成できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10401	INFO	割り当て可能な動的グループ内にグループを作成しようとしています	割り当て可能な動的グループの DNグループの名前	グループ作成ページの「新規」ボタンをクリックしたとき。	
10402	INFO	割り当て可能な動的グループ内のグループの作成に成功しました。	割り当て可能な動的グループの DNグループの名前	グループ作成ページの「新規」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10403	SEVERE	割り当て可能な動的グループ内のグループの作成に失敗しました。	割り当て可能な動的グループの DNグループの名前エラーメッセージ	グループを作成できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10404	SEVERE	割り当て可能な動的グループ内のグループの作成に失敗しました。	割り当て可能な動的グループの DNグループの名前エラーメッセージ	アクセス管理 SDK の例外が原因で、グループを作成できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10411	INFO	グループを変更しようとしています	グループの DN	グループプロファイルページの「保存」ボタンをクリックしたとき。	
10412	INFO	グループの変更に成功しました。	グループの DN	グループプロファイルページの「保存」ボタンをクリックしたとき。	
10414	SEVERE	グループの変更に失敗しました。	割り当て可能な動的グループの DNグループの名前エラーメッセージ	アクセス管理 SDK の例外が原因で、グループを変更できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10421	INFO	グループのユーザーを検索しようとしています	グループの DN検索パターン	グループのユーザーページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10422	INFO	グループのユーザーの検索に成功しました。	グループのDN検索パターン	グループのユーザーページを表示したとき。	
10423	SEVERE	グループのユーザーの検索に失敗しました。	グループのDN検索パターンエラーメッセージ	ユーザーを検索できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10424	SEVERE	グループのユーザーの検索に失敗しました。	グループのDN検索パターンエラーメッセージ	アクセス管理 SDK の例外が原因で、ユーザーを検索できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10431	INFO	入れ子グループを取得しようとしています	グループの DN	グループのメンバーページを表示したとき。	
10432	INFO	入れ子グループの取得に成功しました。	グループの DN	グループのメンバーページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10433	SEVERE	入れ子グループの取得に失敗しました。	グループのDNエラーメッセージ	入れ子グループを取得できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10434	SEVERE	入れ子グループの取得に失敗しました。	グループのDNエラーメッセージ	アクセス管理 SDK の例外が原因で、入れ子グループを取得できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10441	INFO	入れ子グループを消去しようとしています	グループのDN入れ子グループの *DN*	グループのメンバーページの「消去」ボタンをクリックしたとき。	
10442	INFO	入れ子グループの消去に成功しました。	グループのDN入れ子グループの *DN*	グループのメンバーページの「消去」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10443	SEVERE	入れ子グループの消去に失敗しました。	グループのDN入れ子グループの *DN*エラーメッセージ	入れ子グループを消去できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10444	SEVERE	入れ子グループの消去に失敗しました。	グループのDN入れ子グループの *DN*エラーメッセージ	アクセス管理 SDK の例外が原因で、入れ子グループを消去できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10451	INFO	グループからユーザーを消去しようとしています	グループのDNユーザーの *DN*	グループのメンバーページの「消去」ボタンをクリックしたとき。	
10452	INFO	グループからのユーザーの消去に成功しました。	グループのDNユーザーの *DN*	グループのメンバーページの「消去」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10453	SEVERE	グループからのユーザーの消去に失敗しました。	グループのDNユーザーの*DN*エラーメッセージ	ユーザーを消去できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10454	SEVERE	グループからのユーザーの消去に失敗しました。	グループのDNユーザーの*DN*エラーメッセージ	アクセス管理 SDK の例外が原因で、ユーザーを消去できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10501	INFO	組織内のピープルコンテナを検索しようとしています	組織の DN検索パターン	組織のピープルコンテナページを表示したとき。	
10502	INFO	組織内のピープルコンテナの検索に成功しました。	組織の DN検索パターン	組織のピープルコンテナページを表示したとき。	
10503	SEVERE	組織内のピープルコンテナの検索に失敗しました。	組織の DN検索パターンエラーメッセージ	ピープルコンテナを検索できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10504	SEVERE	組織内のピープルコンテナの検索に失敗しました。	組織の DN 検索パターン エラーメッセージ	アクセス管理 SDK の例外が原因で、ピープルコンテナを検索できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10511	INFO	コンテナ内のピープルコンテナを検索しようとしています	コンテナの DN 検索パターン	コンテナのピープルコンテナページを表示したとき。	
10512	INFO	コンテナ内のピープルコンテナの検索に成功しました。	コンテナの DN 検索パターン	コンテナのピープルコンテナページを表示したとき。	
10513	SEVERE	コンテナ内のピープルコンテナの検索に失敗しました。	コンテナの DN 検索パターン エラーメッセージ	ピープルコンテナを検索できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10514	SEVERE	コンテナ内のピープルコンテナの検索に失敗しました。	コンテナの DN 検索パターン エラーメッセージ	アクセス管理 SDK の例外が原因で、ピープルコンテナを検索できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10521	INFO	ピープルコンテナ内のピープルコンテナを検索しようとしています	ピープルコンテナの DN 検索パターン	ピープルコンテナのピープルコンテナページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10522	INFO	ピープルコンテナ内のピープルコンテナの検索に成功しました。	ピープルコンテナの DN 検索パターン	ピープルコンテナのピープルコンテナページを表示したとき。	
10523	SEVERE	ピープルコンテナ内のピープルコンテナの検索に失敗しました。	ピープルコンテナの DN検索パターンエラーメッセージ	ピープルコンテナを検索できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10524	SEVERE	ピープルコンテナ内のピープルコンテナの検索に失敗しました。	ピープルコンテナの DN検索パターンエラーメッセージ	アクセス管理 SDK の例外が原因で、ピープルコンテナを検索できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10531	INFO	組織内にピープルコンテナを作成しようとしています	組織の DN ピープルコンテナの名前	ピープルコンテナ作成ページの「新規」ボタンをクリックしたとき。	
10532	INFO	組織内のピープルコンテナの作成に成功しました。	組織の DN ピープルコンテナの名前	ピープルコンテナ作成ページの「新規」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10533	SEVERE	組織内のピープルコンテナの作成に失敗しました。	組織の DN ピープルコンテナの名前 エラーメッセージ	ピープルコンテナを作成できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10534	SEVERE	組織内のピープルコンテナの作成に失敗しました。	組織の DN ピープルコンテナの名前 エラーメッセージ	アクセス管理 SDK の例外が原因で、ピープルコンテナを作成できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10541	INFO	コンテナ内にピープルコンテナを作成しようとしています	コンテナの DN ピープルコンテナの名前	ピープルコンテナ作成ページの「新規」ボタンをクリックしたとき。	
10542	INFO	コンテナ内のピープルコンテナの作成に成功しました。	コンテナの DNピープルコンテナの名前	ピープルコンテナ作成ページの「新規」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10543	SEVERE	コンテナ内のピープルコンテナの作成に失敗しました。	コンテナのDNピープルコンテナの名前エラーメッセージ	ピープルコンテナを作成できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10544	SEVERE	コンテナ内のピープルコンテナの作成に失敗しました。	コンテナのDNピープルコンテナの名前エラーメッセージ	アクセス管理 SDK の例外が原因で、ピープルコンテナを作成できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10551	INFO	ピープルコンテナ内にピープルコンテナを作成しようとしています	ピープルコンテナの DNピープルコンテナの名前	ピープルコンテナ作成ページの「新規」ボタンをクリックしたとき。	
10552	INFO	ピープルコンテナ内のピープルコンテナの作成に成功しました。	ピープルコンテナの DNピープルコンテナの名前	ピープルコンテナ作成ページの「新規」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10553	SEVERE	ピープルコンテナ内のピープルコンテナの作成に失敗しました。	ピープルコンテナの DN ピープルコンテナの名前エラーメッセージ	ピープルコンテナを作成できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10554	SEVERE	ピープルコンテナ内のピープルコンテナの作成に失敗しました。	ピープルコンテナの DN ピープルコンテナの名前エラーメッセージ	アクセス管理 SDK の例外が原因で、ピープルコンテナを作成できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10601	INFO	組織に割り当てられたサービスを取得しようとしています	組織の DN	組織のサービスプロファイルページを表示したとき。	
10602	INFO	組織に割り当てられたサービスの取得に成功しました。	組織の DN	組織のサービスプロファイルページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10603	SEVERE	組織に割り当てられたサービスの取得に失敗しました。	組織の DN エラーメッセージ	割り当てられたサービスを取得できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10604	SEVERE	組織に割り当てられたサービスの取得に失敗しました。	組織の DN エラーメッセージ	アクセス管理 SDK の例外が原因で、割り当てられたサービスを取得できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10611	INFO	組織からサービスを消去しようとしています	組織の DN サービスの名前	組織のサービスプロファイルページの「割り当て解除」ボタンをクリックしたとき。	
10612	INFO	組織からのサービスの消去に成功しました。	組織の DN サービスの名前	組織のサービスプロファイルページの「割り当て解除」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10613	SEVERE	組織からのサービスの消去に失敗しました。	組織の DN サービスの名前 エラーメッセージ	サービスを消去できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10614	SEVERE	組織からのサービスの消去に失敗しました。	組織の DN サービスの名前 エラーメッセージ	アクセス管理 SDK の例外が原因で、サービスを消去できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10621	INFO	組織内の組織を検索しようとしています	組織の DN 検索パターン	組織のサブ組織ページを表示したとき。	
10622	INFO	組織内の組織の検索に成功しました。	組織の DN 検索パターン	組織のサブ組織ページを表示したとき。	
10623	SEVERE	組織内の組織の検索に失敗しました。	組織の DN 検索パターン エラーメッセージ	組織を検索できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10624	SEVERE	組織内の組織の検索に失敗しました。	組織の DN 検索パターン エラーメッセージ	アクセス管理 SDK の例外が原因で、組織を検索できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10631	INFO	組織を変更しようとしています	組織の DN	組織プロファイルページの「保存」ボタンをクリックしたとき。	
10632	INFO	組織の変更に成功しました。	組織の DN	組織プロファイルページの「保存」ボタンをクリックしたとき。	
10633	SEVERE	組織の変更に失敗しました。	組織の DN エラーメッセージ	組織を変更できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10634	SEVERE	組織の変更に失敗しました。	組織の DN エラーメッセージ	アクセス管理 SDK の例外が原因で、組織を変更できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10641	INFO	組織内に組織を作成しようとしています	組織の DN 新しい組織の名前	組織作成ページの「新規」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10642	INFO	組織内の組織の作成に成功しました。	組織の DN 新しい組織の名前	組織作成ページの「新規」ボタンをクリックしたとき。	
10643	SEVERE	組織内の組織の作成に失敗しました。	組織の DN 新しい組織の名前 エラーメッセージ	組織を作成できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10644	SEVERE	組織内の組織の作成に失敗しました。	組織の DN 新しい組織の名前 エラーメッセージ	アクセス管理 SDK の例外が原因で、組織を作成できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10651	INFO	組織の属性値を取得しようとしています	組織の DN	組織プロファイルページを表示したとき。	
10652	INFO	組織の属性値の取得に成功しました。	組織の DN	組織プロファイルページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10653	SEVERE	組織の属性値の取得に失敗しました。	組織の DN エラーメッセージ	組織の属性値を取得できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10654	SEVERE	組織の属性値の取得に失敗しました。	組織の DN エラーメッセージ	アクセス管理 SDK の例外が原因で、組織の属性値を取得できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10661	INFO	組織にサービスを追加しようとしています	組織の DN サービスの名前	組織のサービスページの「割り当て」ボタンをクリックしたとき。	
10662	INFO	組織へのサービスの追加に成功しました。	組織の DN サービスの名前	組織のサービスページの「割り当て」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10663	SEVERE	組織へのサービスの追加に失敗しました。	組織の DN サービスの名前 エラーメッセージ	組織にサービスを追加できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10664	SEVERE	組織へのサービスの追加に失敗しました。	組織の DN サービスの名前 エラーメッセージ	アクセス管理 SDK の例外が原因で、組織にサービスを追加できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10701	INFO	ロールからユーザーを消去しようとしています	ロールの DNユーザーの名前	ロールのユーザーページの「消去」ボタンをクリックしたとき。	
10702	INFO	ロールからのユーザーの消去に成功しました。	ロールの DNユーザーの名前	ロールのユーザーページの「消去」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10703	SEVERE	ロールからのユーザーの消去に失敗しました。	ロールのDNユーザーの名前エラーメッセージ	ユーザーを消去できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10704	SEVERE	ロールからのユーザーの消去に失敗しました。	ロールのDNユーザーの名前エラーメッセージ	アクセス管理 SDK の例外が原因で、ユーザーを消去できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10711	INFO	ロールの属性値を取得しようとしています	ロールの DN	ロールプロファイルページを表示したとき。	
10712	INFO	ロールの属性値の取得に成功しました。	ロールの DN	ロールプロファイルページを表示したとき。	
10713	SEVERE	ロールの属性値の取得に失敗しました。	ロールの DNエラーメッセージ	属性値を取得できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10714	SEVERE	ロールの属性値の取得に失敗しました。	ロールの DNエラーメッセージ	アクセス管理 SDK の例外が原因で、属性値を取得できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10721	INFO	ロールを変更しようとしています	ロールの DN	ロールプロファイルページの「保存」ボタンをクリックしたとき。	
10722	INFO	ロールの変更に成功しました。	ロールの DN	ロールプロファイルページの「保存」ボタンをクリックしたとき。	
10723	SEVERE	ロールの変更に失敗しました。	ロールの DNエラーメッセージ	ロールを変更できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10724	SEVERE	ロールの変更に失敗しました。	ロールの DNエラーメッセージ	アクセス管理 SDK の例外が原因で、ロールを変更できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10731	INFO	ロール内のメンバーを取得しようとしています	ロールの DN検索パターン	ロールのメンバーページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10732	INFO	ロール内のメンバーの取得に成功しました。	ロールの DN検索パターン	ロールのメンバーページを表示したとき。	
10733	SEVERE	ロール内のメンバーの取得に失敗しました。	ロールの DN検索パターンエラーメッセージ	メンバーを取得できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10734	SEVERE	ロール内のメンバーの取得に失敗しました。	ロールの DN検索パターンエラーメッセージ	アクセス管理 SDK の例外が原因で、メンバーを取得できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10741	INFO	組織内のロールを取得しようとしています	ロールの DN検索パターン	組織のロールページを表示したとき。	
10742	INFO	組織内のロールの取得に成功しました。	ロールの DN検索パターン ロールのメンバーのページを表示したとき。	組織のロールページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10743	SEVERE	組織内のロールの取得に失敗しました。	ロールの DN検索パターンエラーメッセージ	ロールを取得できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10744	SEVERE	組織内のロールの取得に失敗しました。	ロールの DN検索パターンエラーメッセージ	アクセス管理 SDK の例外が原因で、ロールを取得できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10751	INFO	コンテナ内のロールを取得しようとしています	ロールの DN検索パターン	コンテナのロールページを表示したとき。	
10752	INFO	コンテナ内のロールの取得に成功しました。	ロールの DN検索パターン ロールのメンバーのページを表示したとき。	コンテナのロールページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10753	SEVERE	コンテナ内のロールの取得に失敗しました。	ロールの DN検索パターンエラーメッセージ	ロールを取得できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10754	SEVERE	コンテナ内のロールの取得に失敗しました。	ロールの DN検索パターンエラーメッセージ	アクセス管理 SDK の例外が原因で、ロールを取得できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10761	INFO	コンテナ内にロールを作成しようとしています	コンテナの DNロールの名前	ロール作成ページの「新規」ボタンをクリックしたとき。	
10762	INFO	コンテナ内のロールの作成に成功しました。	コンテナの DNロールの名前	ロール作成ページの「新規」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10763	SEVERE	コンテナ内のロールの作成に失敗しました。	コンテナのDNロールの名前	ロールを作成できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10764	SEVERE	コンテナ内のロールの作成に失敗しました。	コンテナのDNロールの名前エラーメッセージ	アクセス管理 SDK の例外が原因で、ロールを作成できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10771	INFO	組織内にロールを作成しようとしています	組織の DN ロールの名前	ロール作成ページの「新規」ボタンをクリックしたとき。	
10772	INFO	組織内のロールの作成に成功しました。	組織の DN ロールの名前	ロール作成ページの「新規」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10773	SEVERE	組織内のロールの作成に失敗しました。	組織の DN ロールの名前	ロールを作成できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10774	SEVERE	組織内のロールの作成に失敗しました。	組織の DN ロールの名前 エラーメッセージ	アクセス管理 SDK の例外が原因で、ロールを作成できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10781	INFO	ロールに割り当てられたサービスを取得しようとしています	ロールの DN	ロールのサービスページを表示したとき。	
10782	INFO	ロールに割り当てられたサービスの取得に成功しました。	ロールの DN	ロールのサービスページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10783	SEVERE	ロールに割り当てられたサービスの取得に失敗しました。	ロールの DNエラーメッセージ	ロールのサービスを取得できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10784	SEVERE	ロールに割り当てられたサービスの取得に失敗しました。	ロールの DNエラーメッセージ	アクセス管理 SDK の例外が原因で、ロールのサービスを取得できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10791	INFO	ロールからサービスを消去しようとしています	ロールの DNサービスの名前	ロールのサービスページの「割り当て解除」ボタンをクリックしたとき。	
10792	INFO	ロールからのサービスの消去に成功しました。	ロールの DNサービスの名前	ロールのサービスページの「割り当て解除」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10793	SEVERE	ロールからのサービスの消去に失敗しました。	ロールのDNサービスの名前エラーメッセージ	ロールからサービスを消去できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10794	SEVERE	ロールからのサービスの消去に失敗しました。	ロールのDNサービスの名前エラーメッセージ	アクセス管理 SDK の例外が原因で、ロールからサービスを消去できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10801	INFO	ロールにサービスを追加しようとしています	ロールのDNサービスの名前	ロールのサービスページの「割り当て」ボタンをクリックしたとき。	
10802	INFO	ロールへのサービスの追加に成功しました。	ロールのDNサービスの名前	ロールのサービスページの「割り当て」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10803	SEVERE	ロールへのサービスの追加に失敗しました。	ロールのDNサービスの名前エラーメッセージ	ロールにサービスを追加できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10804	SEVERE	ロールへのサービスの追加に失敗しました。	ロールのDNサービスの名前エラーメッセージ	アクセス管理 SDK の例外が原因で、ロールにサービスを追加できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10901	INFO	ユーザーに割り当てられたロールを取得しようとしています	ユーザーの DN	ユーザーのロールページを表示したとき。	
10902	INFO	ユーザーに割り当てられたロールの取得に成功しました。	ユーザーの DN	ユーザーのロールページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10903	SEVERE	ユーザーに割り当てられたロールの取得に失敗しました。	ユーザーのDNエラーメッセージ	割り当てられたロールを取得できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10904	SEVERE	ユーザーに割り当てられたロールの取得に失敗しました。	ユーザーのDNサービスの名前エラーメッセージ	アクセス管理 SDK の例外が原因で、割り当てられたロールを取得できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10911	INFO	ユーザーからロールを消去しようとしています	ユーザーのDNロールの *DN*	ユーザーのロールページの「削除」ボタンをクリックしたとき。	
10912	INFO	ユーザーからのロールの消去に成功しました。	ユーザーのDNロールの *DN*	ユーザーのロールページの「削除」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10913	SEVERE	ユーザーからのロールの消去に失敗しました。	ユーザーのDNロールの*DN*エラーメッセージ	ロールを消去できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10914	SEVERE	ユーザーからのロールの消去に失敗しました。	ユーザーのDNロールの*DN*サービスの名前エラーメッセージ	アクセス管理 SDK の例外が原因で、ロールを消去できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10921	INFO	ユーザーにロールを追加しようとしています	ユーザーのDNロールの*DN*	ユーザーのロールページの「追加」ボタンをクリックしたとき。	
10922	INFO	ユーザーへのロールの追加に成功しました。	ユーザーのDNロールの*DN*	ユーザーのロールページの「追加」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10923	SEVERE	ユーザーへのロールの追加に失敗しました。	ユーザーのDNロールの*DN*エラーメッセージ	ロールを追加できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10924	SEVERE	ユーザーへのロールの追加に失敗しました。	ユーザーのDNロールの*DN*サービスの名前エラーメッセージ	アクセス管理 SDK の例外が原因で、ロールを追加できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10931	INFO	ユーザーに割り当てられたサービスを取得しようとしています	ユーザーの DN	ユーザーのサービスページを表示したとき。	
10932	INFO	ユーザーに割り当てられたサービスの取得に成功しました。	ユーザーの DN	ユーザーのサービスページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10933	SEVERE	ユーザーに割り当てられたサービスの取得に失敗しました。	ユーザーのDNエラーメッセージ	サービスを取得できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10934	SEVERE	ユーザーに割り当てられたサービスの取得に失敗しました。	ユーザーのDNエラーメッセージ	アクセス管理 SDK の例外が原因で、サービスを取得できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10941	INFO	ユーザーからサービスを消去しようとしています。	ユーザーのDNサービスの名前	ユーザーのサービスページの「消去」ボタンをクリックしたとき。	
10942	INFO	ユーザーからのサービスの消去に成功しました。	ユーザーのDNサービスの名前	ユーザーのサービスページの「消去」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10943	SEVERE	ユーザーからのサービスの消去に失敗しました。	ユーザーのDNサービスの名前エラーメッセージ	サービスを消去できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10944	SEVERE	ユーザーからのサービスの消去に失敗しました。	ユーザーのDNサービスの名前エラーメッセージ	アクセス管理 SDK の例外が原因で、サービスを消去できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10951	INFO	組織内のユーザーを検索しようとしています	組織の DN 検索パターン	組織のユーザーページを表示したとき。	
10952	INFO	組織内のユーザーの検索に成功しました。	組織の DN 検索パターン	組織のユーザーページを表示したとき。	
10953	SEVERE	組織内のユーザーの検索に失敗しました。	組織の DN 検索パターンエラーメッセージ	ユーザーを検索できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10954	SEVERE	組織内のユーザーの検索に失敗しました。	組織の DN 検索パターン エラーメッセージ	アクセス管理 SDK の例外が原因で、ユーザーを検索できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10961	INFO	ユーザーを変更しようとしています	ユーザーの DN	ユーザープロファイルページの「保存」ボタンをクリックしたとき。	
10962	INFO	ユーザープロファイルの変更に成功しました。	ユーザーの DN	ユーザープロファイルページの「保存」ボタンをクリックしたとき。	
10963	SEVERE	ユーザープロファイルの変更に失敗しました。	ユーザーの DNエラーメッセージ	ユーザーを変更できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10964	SEVERE	ユーザープロファイルの変更に失敗しました。	ユーザーの DNエラーメッセージ	アクセス管理 SDK の例外が原因で、ユーザーを変更できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10971	INFO	ユーザーを作成しようとしています	ピープルコンテナの DNユーザーの名前	ユーザー作成ページの「追加」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10972	INFO	ユーザーの作成に成功しました。	ピープルコンテナの DNユーザーの名前	ユーザー作成ページの「追加」ボタンをクリックしたとき。	
10973	SEVERE	ユーザーの作成に失敗しました。	ピープルコンテナの DNユーザーの名前エラーメッセージ	ユーザーを作成できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10974	SEVERE	ユーザーの作成に失敗しました。	ピープルコンテナの DNユーザーの名前エラーメッセージ	アクセス管理 SDK の例外が原因で、ユーザーを作成できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10981	INFO	ユーザーの属性値を取得しようとしています	ユーザーの DN	ユーザープロファイルページを表示したとき。	
10982	INFO	ユーザーの属性値の取得に成功しました。	ユーザーの DN	ユーザープロファイルページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10983	SEVERE	ユーザーの属性値の取得に失敗しました。	ユーザーのDNエラーメッセージ	属性値を取得できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10984	SEVERE	ユーザーの属性値の取得に失敗しました。	ユーザーのDNエラーメッセージ	アクセス管理 SDK の例外が原因で、属性値を取得できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10991	INFO	ユーザーにサービスを追加しようとしています	ユーザーのDNサービスの名前	ユーザーのサービスページの「追加」ボタンをクリックしたとき。	
10992	INFO	ユーザーへのサービスの追加に成功しました。	ユーザーのDNサービスの名前	ユーザーのサービスページの「追加」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10993	SEVERE	ユーザーへのサービスの追加に失敗しました。	ユーザーのDNサービスの名前エラーメッセージ	サービスを追加できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
10994	SEVERE	ユーザーへのサービスの追加に失敗しました。	ユーザーのDNサービスの名前エラーメッセージ	アクセス管理 SDK の例外が原因で、サービスを追加できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
11001	INFO	ユーザーに割り当てられたグループを取得しようとしています	ユーザーの DN	ユーザーのグループページを表示したとき。	
11002	INFO	ユーザーに割り当てられたグループの取得に成功しました。	ユーザーの DN	ユーザーのグループページを表示したとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
11003	SEVERE	ユーザーに割り当てられたグループの取得に失敗しました。	ユーザーのDNエラーメッセージ	割り当てられたグループを取得できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
11004	SEVERE	ユーザーに割り当てられたグループの取得に失敗しました。	ユーザーのDNエラーメッセージ	アクセス管理 SDK の例外が原因で、割り当てられたグループを取得できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
11011	INFO	ユーザーからグループを消去しようとしています	ユーザーのDNグループの *DN*	ユーザーのグループページの「消去」ボタンをクリックしたとき。	
11012	INFO	ユーザーからのグループの消去に成功しました。	ユーザーのDNグループの *DN*	ユーザーのグループページの「消去」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
11013	SEVERE	ユーザーからのグループの消去に失敗しました。	ユーザーのDNグループの*DN*エラーメッセージ	グループを消去できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
11014	SEVERE	ユーザーからのグループの消去に失敗しました。	ユーザーのDNグループの*DN*エラーメッセージ	アクセス管理 SDK の例外が原因で、グループを消去できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
11021	INFO	ユーザーにグループを追加しようとしています	ユーザーのDNグループの*DN*	ユーザーのグループページの「追加」ボタンをクリックしたとき。	
11022	INFO	ユーザーへのグループの追加に成功しました。	ユーザーのDNグループの*DN*	ユーザーのグループページの「追加」ボタンをクリックしたとき。	

表 C–3 Access Manager コンソールのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
11023	SEVERE	ユーザーへのグループの追加に失敗しました。	ユーザーのDNグループの*DN*エラーメッセージ	グループを追加できないとき。ユーザーのシングルサインオントークンが期限切れになっているか、ユーザーにこの操作を実行するためのアクセス権がない可能性があります。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。
11024	SEVERE	ユーザーへのグループの追加に失敗しました。	ユーザーのDNグループの*DN*エラーメッセージ	アクセス管理 SDK の例外が原因で、グループを追加できないとき。	詳細な情報が必要な場合は、アクセス管理 SDK のログを調べてください。

表 C–4 連携のログリファレンス

ID	ログレベル	説明	データ	発生原因	対処方法
1	INFO	認証ドメインの作成	認証ドメイン名	作成された認証ドメイン	
2	INFO	認証ドメインの削除	認証ドメイン名	削除された認証ドメイン	
3	INFO	認証ドメインの変更	認証ドメイン名	変更された認証ドメイン	
4	INFO	リモートプロバイダの作成	プロバイダ ID	作成されたリモートプロバイダ	
5	INFO	ホストプロバイダの作成	プロバイダ ID	作成されたホストプロバイダ	
6	INFO	削除されたアフィリエイト	アフィリエイト ID	削除されたアフィリエイト	

表C–4連携のログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
7	INFO	エンティティーの削除	エンティティーID	削除されたエンティティー	
8	INFO	削除されたプロバイダ	プロバイダID	削除されたプロバイダ	
9	INFO	エンティティーの変更	エンティティーID	変更されたエンティティー	
10	INFO	アフィリエイトの変更	アフィリエイトID	変更されたアフィリエイト	
11	INFO	プロバイダの変更	プロバイダID	変更されたプロバイダ	
12	INFO	エンティティーの作成	エンティティーID	作成されたエンティティー	
13	INFO	アフィリエイトの作成	アフィリエイトID	作成されたアフィリエイト	
14	INFO	アカウント連携情報の書き込み	ユーザーDN連携情報キー連携情報値	キーを持つアカウント連携情報がユーザーに追加されたとき。	
15	INFO	アカウント連携情報の消去	ユーザーDNプロバイダ*ID*既存の連携情報キー	キーとプロバイダIDを持つアカウント連携情報がユーザーから消去されたとき。	
16	FINER	表明の作成	表明のIDまたは文字列	作成された表明	
17	INFO	Libertyが有効になっていません。	メッセージ	Libertyが有効になっていません。要求を処理できないとき。	管理コンソールにログインし、管理コンソールサービスの「連携管理」を有効にしてください。

表C–4連携のログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
18	INFO	ログアウト要求の処理に失敗しました。	メッセージ	ログアウト要求の処理に失敗したとき	
19	INFO	終了要求の処理に失敗しました	メッセージ	終了要求の処理に失敗しました	
20	INFO	SOAP URL エンドポイントの作成に失敗しました。	SOAP エンドポイント URL	SOAP URL エンドポイントの作成に失敗したとき	
21	INFO	認証タイプとプロトコル (SOAPUrl に基づいた) が一致しません。	プロトコル 認証タイプ	認証タイプとプロトコル (SOAPUrl に基づいた) が一致しないとき。	
22	INFO	認証タイプが間違っています	認証タイプ	認証タイプが間違っています	
23	FINER	SAML SOAP 受信者の URL	SOAP URL	SAML SOAP 受信者の URL	
24	INFO	SOAP 応答が無効です	メッセージ	SOAP 応答が無効なとき。	
25	INFO	表明が無効です	メッセージ	この表明が無効なとき。	
26	INFO	シングルサインオンに失敗しました	メッセージ	シングルサインオンに失敗しました	
27	INFO	アクセスを許可したあとに URL にリダイレクトします。	リダイレクト URL	アクセスを許可したあとに URL にリダイレクトしたとき。	
28	INFO	認証応答が見つかりません	メッセージ	認証応答が見つからないとき	
29	INFO	アカウント連携が失敗しました	メッセージ	アカウント連携が失敗しました	

表C–4連携のログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
30	INFO	SSOTokenの生成が失敗しました	メッセージ	SSOTokenの生成に失敗したとき	
31	INFO	認証応答が無効です	無効な認証応答	認証応答が無効です	
32	INFO	認証要求の処理に失敗しました	メッセージ	認証要求の処理に失敗したとき。	
33	INFO	署名の検証に失敗しました。	メッセージ	署名の検証に失敗しました。	
34	FINER	SAML応答を作成しました	SAML応答	SAML応答を作成しました	
35	FINER	リダイレクトURL	リダイレクトURL	リダイレクト先:	
36	INFO	共通ドメインサービス情報が見つかりません	メッセージ	共通ドメインサービス情報が見つからないとき。	
37	INFO	プロバイダが信頼されていません	プロバイダID	プロバイダが信頼されていないとき。	
38	INFO	認証要求が無効です	メッセージ	認証要求が無効です	
39	INFO	ユーザーのアカウント連携情報が見つかりません	ユーザー名	ユーザーのアカウント連携情報が見つからないとき:	
40	INFO	ユーザーが見つかりません。	ユーザー名	ユーザーが見つかりません。	
41	INFO	ログアウトプロファイルがサポートされていません。	ログアウトプロファイル	ログアウトプロファイルがサポートされていません。	メタデータが正しいことを確認してください。
42	INFO	正常にログアウトしました。	ユーザー名	正常にログアウトしました。	

表C–4 連携のログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
43	INFO	URLが正しくないため、ログアウトのリダイレクトに失敗しました。	メッセージ	URLが正しくないため、ログアウトのリダイレクトに失敗しました。	
44	INFO	ログアウト要求の形式が正しくありません。	ユーザー名	ログアウト要求の形式が正しくありません。	
45	INFO	Pre/Logoutハンドラの取得に失敗しました。	ログアウトURL	Pre/Logoutハンドラの取得に失敗しました。	
46	INFO	シングルログアウトに失敗しました。	ユーザー名	シングルログアウトに失敗しました。	
47	INFO	SPProvidedNameIdentifierの作成に失敗しました。	メッセージ	SPProvidedNameIdentifierの作成に失敗しました。	
48	INFO	署名が無効です。	メッセージ	署名が無効です。	
49	INFO	連携終了に失敗しました。	ユーザー名	連携終了に失敗しました。アカウントを更新できないとき。	
50	FINER	連携終了に成功しました。	ユーザーDN	連携終了に成功しました。ユーザーアカウントが更新されたとき。	
51	INFO	応答が無効です	SAML応答	SAML応答が無効なとき。	
52	INFO	プロバイダ登録が無効です。	プロバイダID	プロバイダが無効なとき。	

表 C–5 Libertyのログリファレンス

ID	ログレベル	説明	データ	発生原因	対処方法
1	INFO	SASL要求を処理できません	メッセージID 認証メカニズム 認証*ID* アドバイザリ認証*ID*	SASL要求を処理できないとき。	
2	INFO	SASL応答は正常です	メッセージID 認証メカニズム 認証*ID* アドバイザリ認証*ID*	SASL応答が正常のとき。	
3	INFO	SASL認証応答を返します	メッセージID 認証メカニズム 認証*ID* アドバイザリ認証*ID*	SASL応答を返し、認証を続行するとき。	
4	INFO	ユーザーがデータストアに見つかりません	ユーザー名	ユーザーがデータストアに見つかりません	
5	INFO	ユーザーがデータストアに見つかりました	ユーザー名	ユーザーがデータストアに見つかりました	
6	INFO	リソースIDからユーザーを検索できません	リソースID	リソースIDからユーザーを検索できません	
7	INFO	ユーザープロファイルの更新に成功しました	ユーザー名	ユーザープロファイルの更新に成功しました	
8	INFO	承認されていません。個人プロファイルサービスのクエリーに失敗しました	リソースID	個人プロファイルサービスのクエリーに失敗しました	

表 C–5 Liberty のログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
9	INFO	対話に失敗しました	リソース ID	個人プロファイルサービスとの対話に失敗したとき	
10	INFO	PP サービスのクエリーに成功しました	リソース ID	個人プロファイルサービスのクエリーに成功したとき	
11	INFO	変更に失敗しました	リソース ID	個人プロファイルサービスの変更に失敗したとき	
12	INFO	変更に成功しました	リソース ID	個人プロファイルサービスの変更に成功したとき。	
13	INFO	対話に成功しました	成功した対話のメッセージ	個人プロファイルサービスとの対話に成功したとき	
14	INFO	メッセージを送信しています	要求メッセージ ID	SOAP 要求メッセージを WSP に送信しているとき。	
15	INFO	応答メッセージを返しています	応答メッセージ ID要求メッセージ *ID*	SOAP 要求の応答メッセージを返しているとき。	
16	INFO	メッセージを再送信しています	メッセージ ID	SOAP 要求メッセージを WSP に再送信しているとき	

表 C–5 Libertyのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
17	INFO	Interaction Managerが対話サービスにユーザーエージェントをリダイレクトしています	要求メッセージID	Interaction Managerが対話サービスにユーザーエージェントをリダイレクトしています	
18	INFO	Interaction Managerが応答要素を返信しています	メッセージID参照 メッセージ*ID*キャッシュエントリの状態	Interaction Managerが応答要素を返信しています	
19	INFO	対話クエリーがユーザーエージェントに表示されました	メッセージID	対話クエリーがユーザーエージェントに表示されました	
20	INFO	ユーザーエージェントが対話クエリーに応答しました	メッセージID	ユーザーエージェントが対話クエリーに応答しました	
21	INFO	ユーザーエージェントがSPにリダイレクトされました	メッセージID	ユーザーエージェントがSPにリダイレクトされました	
22	INFO	Webサービスが成功しました	メッセージIDハンドラキー	Webサービスが成功したとき。	
23	INFO	Webサービスが失敗しました	エラーメッセージ	Webサービスが失敗したとき	

表C–6 ポリシーのログリファレンス

ID	ログレベル	説明	データ	発生原因	対処方法
1	INFO	ポリシーの評価に成功しました	ポリシー名レルム名サービスタイプ名リソース名アクション名ポリシー決定	ポリシーを評価しているとき。	
2	INFO	保護されたポリシーリソースの取得に成功しました	主体名リソース名保護しているポリシー	保護されたポリシーリソースを取得しているとき。	
3	INFO	レルム内のポリシーの作成に成功しました	ポリシー名レルム名	レルム内にポリシーを作成しているとき。	
4	INFO	レルム内のポリシーの変更に成功しました	ポリシー名レルム名	レルム内のポリシーを変更しているとき。	
5	INFO	レルムからのポリシーの消去に成功しました	ポリシー名レルム名	レルムからポリシーを消去しているとき。	
6	INFO	ポリシーはレルムにすでに存在します	ポリシー名レルム名	レルムにポリシーを作成しているとき。	
7	INFO	レルム内のポリシーの作成に失敗しました	ポリシー名レルム名	レルム内にポリシーを作成しているとき。	ユーザーがこのレルムにポリシーを作成する権限を持っているかどうかを確認してください。

表C–6ポリシーのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
8	INFO	レルム内のポリシーの置き換えに失敗しました	ポリシー名レルム名	レルム内のポリシーを置き換えているとき。	ユーザーがこのレルムのポリシーを置き換える権限を持っているかどうかを確認してください。
81	INFO	ポリシーを置き換えませんでした - 新しい名前を持つ別のポリシーがレルムにすでに存在しています	新しいポリシー名レルム名	レルム内のポリシーを置き換えているとき	
9	INFO	レルムからのポリシーの消去に失敗しました。	ポリシー名レルム名	レルムからポリシーを消去しているとき。	ユーザーがこのレルムからポリシーを消去する権限を持っているかどうかを確認してください。
10	INFO	管理者によるポリシー決定の計算が成功しました	管理者名主体名リソース名ポリシー決定	管理者がポリシー決定を計算しているとき。	
11	INFO	管理者による対象を無視したポリシー決定の計算が成功しました	管理者名リソース名ポリシー決定	管理者が対象を無視してポリシー決定を計算しているとき。	

表 C–7 SAMLのログリファレンス

ID	ログレベル	説明	データ	発生原因	対処方法
1	INFO	新しい表明を作成しました	メッセージID表明 *ID* またはログレベルが *LL_FINER* の場合は表明	ブラウザアーティファクトプロファイルブラウザ *POST* プロファイル表明アーティファクトを作成するとき認証クエリー属性クエリー認証決定クエリー	
2	INFO	新しい表明アーティファクトを作成しました	メッセージID表明アーティファクトアーティファクトに対応する表明の *ID*	ブラウザアーティファクトプロファイル表明アーティファクトを作成しているとき	
3	FINE	表明アーティファクトがマップから消去されました	メッセージID表明アーティファクト	SAMLアーティファクトクエリー表明アーティファクトが期限切れのとき	
4	FINE	表明がマップから消去されました	メッセージID表明 *ID*	SAMLアーティファクトクエリー表明が期限切れのとき	
5	INFO	表明アーティファクトによってアクセス権が検証されました	メッセージID表明アーティファクト	SAMLアーティファクトクエリー	

表 C–7 SAMLのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
6	INFO	設定されている認証タイプと実際のSOAPプロトコルが一致しません。	メッセージID	SAML SOAPクエリー	コンソールにログインし、「連携」、「SAML」の順に移動し、「信頼パートナ」設定を編集し、選択されている「認証タイプ」フィールドを確認し、認証タイプが「SOAP URL」フィールドに指定されているプロトコルと一致することを確認してください。
7	INFO	認証タイプが無効です	メッセージID	SAML SOAPクエリー	コンソールにログインし、「連携」、「SAML」の順に移動し、「信頼パートナ」設定を編集し、「認証タイプ」フィールドの値の1つを選択して、保存してください。
8	FINE	リモートSOAP受信者URL	メッセージID*SOAP*受信者*URL*	SAML SOAPクエリー	
9	INFO	SAML応答に表明がありません。	メッセージID*SAML*応答	SAMLアーティファクトクエリー	リモートパートナに問題点を連絡してください

表 C–7 SAMLのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
10	INFO	SAML応答の表明の数とSAML要求のアーティファクトの数が一致していません	メッセージID*SAML*応答	SAMLアーティファクトクエリー	リモートパートナに問題点を連絡してください
11	INFO	リモートパートナに送信されるアーティファクト	メッセージID*SAML*アーティファクト	SAMLアーティファクトクエリー	
12	INFO	信頼パートナ設定のSOAP URLが間違っています	メッセージID	SAMLアーティファクトクエリー	コンソールにログインし、「連携」、「SAML」の順に移動し、「信頼パートナ」設定を編集し、「SOAP URL」フィールドの値を入力して、保存します。
13	FINE	SAMLアーティファクトクエリーSOAP要求	メッセージID*SAML*アーティファクトクエリーメッセージ	SAMLアーティファクトクエリー	
14	INFO	リモートSAML SOAP受信者から返信がありません。	メッセージID	SAMLアーティファクトクエリー	リモートパートナに問題点を確認してください
15	FINE	SAMLアーティファクトクエリー応答	メッセージID*SAML*アーティファクトクエリー応答メッセージ	SAMLアーティファクトクエリー	
16	INFO	SOAP応答の内部にSAML応答がありません	メッセージID	SAMLアーティファクトクエリー	リモートパートナに問題点を確認してください

表 C–7 SAMLのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
17	INFO	SAML応答のXML署名が有効ではありません	メッセージID	SAMLアーティファクトクエリー	リモートパートナにXMLデジタル署名の問題点を確認してください
18	INFO	SAML応答状態コードの取得中にエラーが発生しました	メッセージID	SAMLアーティファクトクエリー	リモートパートナに応答状態コードの問題点を確認してください
19	INFO	この要求にはTARGETパラメータがありません	メッセージID	SAMLアーティファクトプロファイル*SAML POST*プロファイル	「TARGET=target_url」を要求のクエリーパラメータとして追加してください
20	INFO	SAMLアーティファクトソースサイトのリダイレクトURL	メッセージID ターゲットリダイレクト*URL* *POST*プロファイルとログレベルが*LL_FINER*の場合は*SAML*応答メッセージ	SAMLアーティファクトプロファイルソース*SAML POST*プロファイルソース	
21	INFO	指定されたターゲットサイトは禁止されています	メッセージIDターゲット*URL*	SAMLアーティファクトプロファイルソース*SAML POST*プロファイルソース	要求に指定されているTARGET URLが信頼パートナによって処理されません。TARGET URLを確認し、信頼パートナのサイトに設定されているTARGET URLのいずれかと一致することを確認してください

表 C–7 SAMLのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
22	INFO	シングルサインオントークンの作成に失敗しました	メッセージ ID	SAML アーティファクトプロファイル送信先*SAML POST* プロファイル送信先	認証コンポーネントが SSO トークンの作成に失敗しました。認証ログで詳細を確認してデバッグしてください。
23	INFO	シングルサインオンに成功しました。ターゲットへのアクセスが許可されます	メッセージ ID*POST* プロファイルとログレベルが *LL_FINER* 以上の場合は応答メッセージ	SAML アーティファクトプロファイル送信先 *SAML POST* プロファイル送信先	
24	INFO	サーブレットの要求または応答が Null です	メッセージ ID	SAML アーティファクトプロファイル*SAML POST* プロファイル	詳細については、Web コンテナのエラーログを確認してください
25	INFO	POST 本文に SAML 応答がありません	メッセージ ID	SAML POST プロファイル送信先	HTTP POST 本文に SAML 応答オブジェクトがない理由については、リモート SAML パートナに確認してください

表 C–7 SAMLのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
26	INFO	応答メッセージにエラーが発生しました	メッセージ ID	SAML POST プロファイル送信先	エンコードされた POST 本文属性を SAML 応答オブジェクトに変換できません。エンコードエラーや無効な応答サブ要素など、SAML 応答の作成にエラーがないかどうかをリモート SAML パートナーに確認してください
27	INFO	応答が有効ではありません	メッセージ ID	SAML POST プロファイル送信先	SAML 応答の受け側の属性がこのサイトの POST プロファイル URL と一致しません応答状態コードは成功ではありません
28	INFO	メッセージファクトリのインスタンスの取得に失敗しました	メッセージ ID	SAML SOAP 受信者初期化	SOAP ファクトリプロパティー (javax.xml.soap.MessageFactory) を確認して、有効な SOAP ファクトリ実装を使用していることを確認してください

表 C–7 SAMLのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
29	INFO	信頼できないサイトから要求を受信しました	メッセージIDリモートサイトのホスト名または *IP* アドレス	SAML SOAP クエリー	コンソールにログインし、「連携」、「SAML」サービスの順に移動し、「信頼パートナ」設定を編集し、「ホストリスト」フィールドを確認して、リモートホストまたはIP の値があることを確認してください。クライアント認証で SSL を使用する場合は、「ホストリスト」にリモートサイトのクライアント証明書エイリアスが含まれていることを確認してください。
30	INFO	リモートパートナサイトからの要求が無効です	メッセージ ID および要求ホスト名/IP アドレス返信応答	SAML SOAP クエリー	リモートパートナサイトの管理者に確認してください
31	FINE	パートナーサイトからの要求メッセージ	メッセージ ID および要求ホスト名/IP アドレス要求 *XML*	SAML SOAP クエリー	

表 C–7 SAMLのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
32	INFO	内部サーバーエラーが原因で、応答の構築に失敗しました	メッセージ ID	SAML SOAP クエリー	失敗した原因について、デバックメッセージを確認してください。応答状態を作成できなかったり、さまざまなエラーが発生している可能性があります
33	INFO	SAML 応答をパートナサイトに送信しています	メッセージ ID *SAML* 応答または応答 *ID*	SAML SOAP クエリー	
32	INFO	SOAP エラー応答本文の構築に失敗しました	メッセージ ID	SAML SOAP クエリー	失敗した原因について、デバックメッセージを確認してください。SOAP エラーを作成できないなどの問題が発生している可能性があります

表 C–8 セッションのログリファレンス

ID	ログレベル	説明	データ	発生原因	対処方法
1	INFO	セッションが作成されました	ユーザー ID	ユーザーが認証されたとき。	
2	INFO	セッションはアイドルタイムアウトになっています	ユーザー ID	ユーザーセッションが長時間アイドル状態のとき。	

表C–8セッションのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
3	INFO	セッションが期限切れになっています	ユーザー ID	ユーザーセッションが最大セッション時間の上限に到達したとき。	
4	INFO	ユーザーがログアウトしました	ユーザー ID	ユーザーがシステムからログアウトしたとき。	
5	INFO	セッションが再度アクティブになっています	ユーザー ID	ユーザーセッションの状態がアクティブのとき。	
6	INFO	セッションが破棄されています	ユーザー ID	ユーザーセッションが破棄されていて、参照できないとき。	
7	INFO	セッションのプロパティーが変更されています。	ユーザー ID	ユーザーがセッションの保護されていないプロパティーを変更したとき。	
8	INFO	セッションが不明なイベントを受信しました	ユーザー ID	セッションイベントが不明のとき	
9	INFO	保護されたプロパティーを設定しようとしています	ユーザー ID	保護されたプロパティーを設定しようとしています	
10	INFO	ユーザーのセッション制限がいっぱいになりました。	ユーザー ID	セッション制限がいっぱいになったとき	

表C–8セッションのログリファレンス　(続き)

ID	ログレベル	説明	データ	発生原因	対処方法
11	INFO	セッションフェイルオーバーおよびセッション制限に使用されるセッションデータベースが使用できません。	ユーザー ID	セッションデータベースに到達できないとき。	
12	INFO	セッションデータベースがオンラインに戻りました	ユーザー ID	セッションデータベースがオンラインに戻りました	
13	INFO	AM サーバー上で運用される有効なセッションの合計数が上限に到達しました。	ユーザー ID	セッション数の上限に到達したとき。	

◆ ◆ ◆ 付 録 D

エラーコード

この付録では、Access Manager によって生成されるエラーメッセージのリストを示します。このリストにすべてが網羅されているわけではありませんが、この章の情報は一般的な問題に対処するための開始点として役立ちます。この付録の各表には、エラーコードそのもの、エラーの説明や考えられる原因、および発生した問題を解決するための対処方法が示されています。

この付録では、次の機能分野に関連するエラーコードのリストを示します。

エラー診断に支援が必要な場合は、次の Web サイトから Sun テクニカルサポートに連絡してください。

http://www.sun.com/service/sunone/software/index.html

Access Manager コンソールのエラー

次の表は、Access Manager コンソールによって生成され表示されるエラーコードのリストです。

表 D–1 Access Manager コンソールのエラー

エラーメッセージ	説明/考えられる原因	対処方法
次のものを削除中にエラーが発生しました。	現在のユーザーが削除を行う前に、そのオブジェクトはほかのユーザーによって削除された可能性があります。	削除しようとしているオブジェクトを再表示し、操作をやり直します。
入力した URL が無効です。	Access Manager コンソールウィンドウに URL を正しく入力しなかった場合に発生します。	
検索条件と一致するエントリがありません。	検索ウィンドウまたはフィルタフィールドに入力されたパラメータが、ディレクトリ内のどのオブジェクトにも一致しませんでした。	パラメータを変更して検索をやり直します。
表示する属性がありません。	選択されたオブジェクトのスキーマには、編集可能な属性が定義されていません。	
このサービスのために表示する情報がありません。	サービス設定モジュールから表示するサービスに、グローバル属性または組織ベースの属性がありません。	
検索サイズの上限を超えました。検索を絞り込んでください。	指定されたパラメータによる検索で、許容数を超えるエントリが返されました。	管理サービスの「検索で返される結果の最大数」属性を、より大きな値に修正します。検索パラメータをより厳しい条件に修正することもできます。
検索時間が指定された時間を過ぎました。検索を絞り込んでください。	指定されたパラメータによる検索に、許容値より長い検索時間がかかりました。	管理サービスの「検索のタイムアウト」属性を、より大きな値に修正します。より多数の値を取得するために、検索パラメータをより緩やかな条件に修正することもできます。

表 D–1 Access Manager コンソールのエラー　(続き)

エラーメッセージ	説明/考えられる原因	対処方法
ユーザーの開始位置が無効です。管理者に連絡してください。	ユーザーエントリの開始位置 DN が無効です。	ユーザープロファイルページで、開始 DN の値を有効な DN に変更します。
アイデンティティーオブジェクトを作成できませんでした。ユーザーに適切なアクセス権がありません。	必要なアクセス権を持っていないユーザーが操作を実行しました。ユーザーが実行できる操作は、持っているアクセス権によって決定します。	

認証エラーコード

次の表は、認証サービスによって生成されるエラーコードのリストです。これらのエラーは、認証モジュールでユーザーや管理者に表示されます。

表 D–2 認証エラーコード

エラーメッセージ	説明/考えられる原因	対処方法
すでにログインしています	ユーザーはすでにログインし、有効なセッションを持っていますが、成功リダイレクト URL が定義されていません。	ログアウトするか、Access Manager コンソールを使ってログイン成功リダイレクト URL をセットアップします。管理コンソール URL として、この値に ”goto’ クエリーパラメータを使用します。
ログアウトに失敗しました。	ユーザーが Access Manager からログアウトできません。	サーバーを再起動します。
不正なハンドラによる認証の例外	不正なハンドラが原因で、認証の例外がスローされました。	ログイン URL に無効な文字や特殊文字が含まれていないかどうかをチェックします。
デフォルトページにリダイレクトできません。	Access Manager で成功 URL または失敗 URL にリダイレクトできません。	Web コンテナのエラーログをチェックして、エラーがないかどうかを確認します。
ログインページに戻る	このリンクは、ほとんどのエラー発生時に生成されます。ユーザーはこのリンクをクリックして、元のログイン URL ページに戻ります。	

表D–2認証エラーコード　(続き)

エラーメッセージ	説明/考えられる原因	対処方法
入力したパスワードが無効です。	入力したパスワードが無効です。	パスワードは8文字以上である必要があります。パスワードに適切な文字数が含まれていることと、パスワードの有効期限が切れていないことを確認します。
認証に失敗しました。	認証に失敗しました。これは汎用のエラーメッセージであり、デフォルトのログイン失敗テンプレートで表示されます。もっとも一般的な原因は、資格が無効または不正であることです。	有効なユーザー名とパスワード(呼び出される認証モジュールに対して必要な資格)を正しく入力します。
ユーザー名と一致するユーザープロファイルが見つかりませんでした	その組織には、入力されたユーザー名に一致するユーザープロファイルが見つかりませんでした。このエラーは、メンバーシップ(自己登録)認証モジュールにログインするときに表示されます。	ログイン情報を入力し直します。はじめてログインする場合は、ログイン画面で「新規ユーザー」を選択します。
入力したパスワードの文字が足りません。	入力されたパスワードの文字数が不足しています。このエラーは、メンバーシップ(自己登録)認証モジュールにログインするときに表示されます。	デフォルトでは、ログインパスワードは8文字以上である必要があります。この値は、メンバーシップ認証モジュールを通して設定できます。
この名前を持つユーザーがすでに存在しています。	その組織には、この名前を持つユーザーがすでに存在しています。このエラーは、メンバーシップ(自己登録)認証モジュールにログインするときに表示されます。	ユーザーIDは組織内で一意にする必要があります。
「ユーザー名」と「パスワード」のフィールドは同じ値にすることはできません。	「ユーザー名」と「パスワード」のフィールドは同じ値にすることはできません。このエラーは、メンバーシップ(自己登録)認証モジュールにログインするときに表示されます。	ユーザー名とパスワードは必ず異なる値にします。
ユーザー名が入力されていません。	ユーザー名が入力されていません。このエラーは、メンバーシップ(自己登録)認証モジュールにログインするときに表示されます。	必ずユーザー名を入力します。
パスワードが入力されていません。	パスワードが入力されていません。このエラーは、メンバーシップ(自己登録)認証モジュールにログインするときに表示されます。	必ずパスワードを入力します。

表 D–2 認証エラーコード　(続き)

エラーメッセージ	説明/考えられる原因	対処方法
パスワードの確認フィールドがありません。	パスワードの確認フィールドが入力されていません。このエラーは、メンバーシップ(自己登録)認証モジュールにログインするときに表示されます。	必ず「パスワードの確認」フィールドにパスワードを入力します。
パスワードと確認パスワードの値が一致しません。	パスワードと確認のパスワードが一致しません。このエラーは、メンバーシップ(自己登録)認証モジュールにログインするときに表示されます。	パスワードと確認のパスワードは必ず同じ値にします。
ユーザープロファイルの格納時にエラーが発生しました。	ユーザープロファイルの格納時にエラーが発生しました。このエラーは、メンバーシップ(自己登録)認証モジュールにログインするときに表示されます。	`Membership.xml` ファイル内の「自己登録」の属性と要素が有効で正しいことを確認します。
この組織はアクティブではありません。	この組織はアクティブではありません。	Access Manager コンソールを使って、組織の状態を非アクティブからアクティブに変更します。
内部認証エラーが発生しました。	内部認証エラー。これは汎用の認証エラーであり、さまざまな環境や設定の問題によって発生します。	
このユーザーはアクティブではありません。	ユーザーの状態はアクティブでなくなっています。	管理コンソールを使って、ユーザーの状態を非アクティブからアクティブに変更します。 メモリーロックによってユーザーがロックアウトされている場合は、サーバーを再起動します。
ユーザーはロールに属していません。	ユーザーは、指定されたロールには属していません。このエラーは、ロールベースの認証で表示されます。	ロールベースの認証に指定されているロールに、ログインするユーザーが属していることを確認します。
セッションがタイムアウトしました。	ユーザーのセッションがタイムアウトしました。	ログインし直します。
認証モジュールが拒否されています。	指定された認証モジュールは拒否されています。	要求された認証モジュールが要求された組織で登録されていること、そのモジュールのテンプレートが作成され保存されていること、および、コア認証モジュールの「組織認証モジュール」リストでそのモジュールが選択されていることを確認します。

表 D–2 認証エラーコード　(続き)

エラーメッセージ	説明/考えられる原因	対処方法
設定が見つかりませんでした。	設定が見つかりません。	認証設定サービスをチェックして、必要な認証方法があるかどうかを確認します。
持続 Cookie ユーザー名が、持続 Cookie ドメインに存在しません。	持続 Cookie ユーザー名が、持続 Cookie ドメインに存在しません。	
そのような組織は見つかりません。	その組織が見つかりません。	有効な組織を正しく入力します。
ユーザーにはこの組織におけるプロファイルがありません。	ユーザーには、指定された組織におけるプロファイルがありません。	ローカル Directory Server 内で、指定された組織にそのユーザーが存在し、有効になっていることを確認します。
必須フィールドのどれかが未記入のままです。必ずすべての必須フィールドに入力してください。	必須フィールドのいずれかが未記入のままになっています。必ずすべての必須フィールドに入力します。	必ずすべての必須フィールドに入力します。
最大セッション数の限度に達したか、セッション制限いっぱいになりました。	最大セッション数の限度に達しました。	ログアウトし、ログインし直します。

ポリシーエラーコード

次の表は、ポリシーフレームワークによって生成され、Access Manager コンソールに表示されるエラーコードのリストです。

表 D–3 ポリシーエラーコード

エラーメッセージ	説明/考えられる原因	対処方法
不正な文字 / 名前。	ポリシー名に不正な文字「/」が含まれています。	ポリシー名に「/」という文字が含まれていないことを確認します。
ポリシー A は組織 B 内にすでに存在します。	同じ名前を持つルールがすでに存在しています。	別の名前を使ってポリシーを作成します。
指定した名前のルールがすでに存在します	同じ名前を持つルールがすでに存在しています。	別のルール名を使ってポリシーを作成します。
rule_already_present	同じルール値を持つルールがすでに存在しています。	別のルール値を使用します。

表 D–3 ポリシーエラーコード　(続き)

エラーメッセージ	説明/考えられる原因	対処方法
ポリシーを作成できません。組織 A への参照が存在しません	組織への参照が存在しません。	サブ組織にポリシーを作成するには、その親組織に参照ポリシーを作成して、このサブ組織に対して参照可能なリソースを示す必要があります。
Ldap 検索のサイズの上限を超えています。	LDAP 検索のサイズの上限を超えました。検索で見つかった結果が最大数を超えたのでエラーが発生しました。	検索制御パラメータの組織の検索パターンまたはポリシーの設定を変更します。検索サイズの上限は、ポリシー設定サービスにあります。
指定された Ldap 検索時間を過ぎています。	LDAP 検索の時間の上限を超えました。検索で見つかった結果が最大数を超えたのでエラーが発生しました。	検索制御パラメータの組織の検索パターンまたはポリシーの設定を変更します。検索時間の上限は、ポリシー設定サービスにあります。
無効な LDAP バインドパスワード	無効な LDAP バインドパスワード。	ポリシー設定で定義されている LDAP バインドユーザーのパスワードが間違っています。これが原因で、ポリシー操作を実行するための認証済み LDAP 接続を取得できません。
アプリケーション SSO トークンが無効です	アプリケーション SSO トークンが無効です。	サーバーがアプリケーション SSO トークンを検証できませんでした。SSO トークンの有効期限が切れている可能性があります。
ユーザー SSO トークンが無効です	ユーザー SSO トークンが無効です。	サーバーがユーザー SSO トークンを検証できませんでした。SSO トークンの有効期限が切れている可能性があります。
プロパティー値は整数にしてください。	プロパティー値が整数ではありません。	このプラグインのプロパティー値は整数にする必要があります。
プロパティー値を定義する必要があります。	プロパティー値を定義する必要があります。	そのプロパティーに値を指定します。
開始 IP は終了 IP より大きくすることはできません。	開始 IP が終了 IP より大きくなっています。	IP アドレス条件に、終了 IP アドレスより大きい開始 IP アドレスを設定しようとしました。開始 IP を終了 IP より大きくすることはできません。
開始日は終了日より大きくすることはできません。	開始日が終了日より大きくなっています。	ポリシーの時間条件に、終了日より大きい開始日を設定しようとしました。開始日を終了日より大きくすることはできません。

表 D–3 ポリシーエラーコード　(続き)

エラーメッセージ	説明/考えられる原因	対処方法
組織内にポリシーが見つかりません。	組織内にそのポリシーが見つかりません。組織内に存在していないポリシーを見つけようとしてエラーが発生しました。	指定された組織にそのポリシーが存在していることを確認します。
ユーザーに適切なアクセス権がありません。	ユーザーに適切なアクセス権がありません。ユーザーは、ポリシー操作を実行するために必要なアクセス権を持っていません。	適切なアクセス権を持っているユーザーでポリシー操作を実行します。
無効な LDAP サーバーホスト	無効な LDAP サーバーホスト。	ポリシー設定サービスに入力された無効な LDAP サーバーホストを変更します。

amadmin エラーコード

次の表は、`amadmin` コマンド行ツールによって生成され Access Manager のデバッグファイルに書き込まれるエラーコードのリストです。

表 D–4 amadmin エラーコード

エラーメッセージ	コード	説明/考えられる原因	対処方法
nocomptype	1	引数が足りません。	必須の引数 (`--runasdn`、`--password`、`--passwordfile`、`--schema`、`--data`、および `--addAttributes`) とそれぞれの値がコマンド行で指定されていることを確認します。
入力 XML ファイルが見つかりません。	2	入力 XML ファイルが見つかりませんでした。	構文をチェックし、入力 XML ファイルが有効であることを確認します。
--runasdn または -u 引数の値としてユーザー DN を指定してください	3	`--runasdn` の値としてユーザー DN が指定されていません。	`--runasdn` の値としてユーザー DN を指定します。
--deleteService 引数の値としてサービス名を指定してください。	4	`--deletservice` の値としてサービス名が指定されていません。	`--deleteservice` の値としてサービス名を指定します。
--password または -w の値としてパスワードを入力してください。	5	`--password` の値としてパスワードが指定されていません。	`--password` の値としてパスワードを指定します。

表 D–4 amadmin エラーコード　(続き)

エラーメッセージ	コード	説明/考えられる原因	対処方法
ロケール名が指定されていません。	6	ロケール名が指定されませんでした。ロケールには en_US が指定されます。	ロケールのリストについては、オンラインヘルプを参照してください。
処理する入力 XML ファイル名を少なくとも 1 つ指定してください。	7	入力 XML ファイルが指定されていません。	処理する入力 XML ファイルの名前を少なくとも 1 つ指定します。
無効なオプション。	8	1 つ以上の引数が間違っています。	すべての引数が有効であることを確認します。有効な引数を一覧表示するには、`amadmin --help` と入力します。
操作に失敗しました:	9	操作に失敗しました。	`amadmin` の失敗時には、このエラーを示す詳細なエラーコードが生成されます。これらのエラーコードを参照して問題を評価します。
要求を処理できません:	10	要求を処理できません。	`amadmin` の失敗時には、このエラーを示す詳細なエラーコードが生成されます。これらのエラーコードを参照して問題を評価します。
ポリシーを作成できません:	12	ポリシーを作成できません。	`amadmin` では、このエラーを示す例外メッセージが生成されます。これらのメッセージを参照して問題を評価します。
ポリシーを削除できません:	13	ポリシーを削除できません。	`amadmin` では、このエラーを示す例外メッセージが生成されます。これらのメッセージを参照して問題を評価します。
サービスを削除できません:	14	サービスを削除できません。	`amadmin` では、このエラーを示す例外メッセージが生成されます。これらのメッセージを参照して問題を評価します。
ユーザーを認証できません。	15	ユーザーを認証できません。	ユーザー DN とパスワードが正しいことを確認します。
入力 XML ファイルをパースできません:	16	入力 XML ファイルをパースできません。	XML の形式が正しく、`amAdmin.dtd` に従っていることを確認します。
アプリケーションエラーまたはパーサ初期化エラーのため、パースできません。	17	アプリケーションエラーまたはパーサー初期化エラーのため、パースできません。	XML の形式が正しく、`amAdmin.dtd` に従っていることを確認します。

表 D–4 amadmin エラーコード　(続き)

エラーメッセージ	コード	説明/考えられる原因	対処方法
指定したオプションを持つパーサをビルドできないため、パースできません。	18	指定したオプションを持つパーサーをビルドできないため、パースできません。	amadmin では、このエラーを示す例外メッセージが生成されます。これらのメッセージを参照して問題を評価します。
IOException が発生したため、入力 XML ファイルを読み取ることができません。	19	入力 XML ファイルを読み取ることができません。	amadmin では、このエラーを示す例外メッセージが生成されます。これらのメッセージを参照して問題を評価します。
XML ファイルが有効なファイルではないため、パースできません:	20	XML ファイルが有効なファイルではないため、パースできません。	構文をチェックし、入力 XML ファイルが有効であることを確認します。
XML ファイルが有効なファイルではないため、パースできません:	21	XML ファイルが有効なファイルではないため、パースできません。	amadmin では、このエラーを示す例外メッセージが生成されます。これらのメッセージを参照して問題を評価します。
ファイルに対する XML ファイル検証警告:	22	ファイルに対する XML ファイル検証警告。	amadmin では、このエラーを示す例外メッセージが生成されます。これらのメッセージを参照して問題を評価します。
処理できません。	23	XML ファイルを処理できません。	amadmin では、このエラーを示す例外メッセージが生成されます。これらのメッセージを参照して問題を評価します。
--data または -t、--schema または -s オプションがコマンド行に配置されていません。	24	--data オプションと --schema オプションのどちらもコマンド行に指定されていません。	すべての引数が有効であることを確認します。有効な引数を一覧表示するには、amadmin --help と入力します。
XML ファイルは正しい DTD に従っていません。DOCTYPE の XML ファイルを確認してください。	25	XML ファイルが正しい DTD に従っていません。	XML ファイルの DOCTYPE 要素を確認します。
無効な DN、無効なパスワード、無効なホスト名、または無効なポート番号が原因で LDAP 認証に失敗しました。	26	無効な DN、パスワード、ホスト名、またはポート番号が原因で LDAP 認証に失敗しました。	ユーザー DN とパスワードが正しいことを確認します。
ServiceManager 例外 (SSOException):	28	サービスマネージャー例外 (SSO 例外)。	amadmin では、このエラーを示す例外メッセージが生成されます。これらのメッセージを参照して問題を評価します。

表 D–4 amadmin エラーコード　(続き)

エラーメッセージ	コード	説明/考えられる原因	対処方法
ServiceManager 例外	29	サービスマネージャー例外。	amadmin では、このエラーを示す例外メッセージが生成されます。これらのメッセージを参照して問題を評価します。
スキーマファイルの inputstream 例外:	30	スキーマファイルの入力ストリーム例外。	amadmin では、このエラーを示す例外メッセージが生成されます。これらのメッセージを参照して問題を評価します。
PolicyManager 例外 (SSOException):	31	ポリシーマネージャー例外 (SSO 例外)。	amadmin では、このエラーを示す例外メッセージが生成されます。これらのメッセージを参照して問題を評価します。
PolicyManager 例外:	32	ポリシーマネージャー例外。	amadmin では、このエラーを示す例外メッセージが生成されます。これらのメッセージを参照して問題を評価します。
いずれか 1 つのオプションだけを指定してください:	33	複数のデバッグオプションが指定されています。	デバッグオプションは 1 つだけ指定する必要があります。
ログインに失敗しました	34	ログインに失敗しました。	amadmin では、このエラーを示す例外メッセージが生成されます。これらのメッセージを参照して問題を評価します。
属性値が無効です。	36	属性値が無効です。	LDAP 検索に設定されているレベルを確認します。SCOPE_SUB または SCOPE_ONE である必要があります。
オブジェクトタイプの取得時にエラーが発生しました:	37	オブジェクトタイプの取得時にエラーが発生しました。	XML ファイル内の DN が値であることと、正しいオブジェクトタイプを持っていることを確認します。
無効な組織 DN:	38	無効な組織 DN。	XML ファイル内の DN が有効であることと、組織オブジェクトであることを確認します。
無効なロール DN:	39	無効なロール DN。	XML ファイル内の DN が有効であることと、ロールオブジェクトであることを確認します。
無効な静的グループ DN:	40	無効な静的グループ DN。	XML ファイル内の DN が有効であることと、静的グループオブジェクトであることを確認します。

表 D–4 amadmin エラーコード　(続き)

エラーメッセージ	コード	説明/考えられる原因	対処方法
無効なピープルコンテナ DN:	41	無効なピープルコンテナ DN。	XML ファイル内の DN が有効であることと、ピープルコンテナオブジェクトであることを確認します。
無効な組織単位 DN:	42	無効な組織単位 DN。	XML ファイル内の DN が有効であることと、コンテナオブジェクトであることを確認します。
無効なサービスホスト名	43	無効なサービスホスト名。	有効なセッションを取得するためのホスト名が正しいことを確認します。
サブスキーマはグローバルと組織でのみサポートされています:	44	サブスキーマのエラー。	サブスキーマはグローバル属性と組織属性でのみサポートされています。
スキーマタイプ A のサービスのサービススキーマ B が見つかりません。	45	サービスのサービススキーマを見つけることができません。	XML ファイル内のサブスキーマが有効であることを確認します。
RoleTemplate は、スキーマタイプが動的の場合にのみ true となります	46	ロールテンプレートは、スキーマタイプが動的な場合にのみ true となります。	XML ファイル内のロールテンプレートが有効であることを確認します。
フィルタロールにはユーザーを追加できません。	47	フィルタリングされたロールにはユーザーを追加できません。	XML ファイル内のロール DN が、フィルタリングされたロールでないことを確認します。
テンプレートが存在しません	48	テンプレートが存在しません。	XML ファイル内のサービステンプレートが有効であることを確認します。
動的なグループにはユーザーを追加できません。	49	動的グループにはユーザーを追加できません。	XML ファイル内のグループ DN が動的グループでないことを確認します。
コンテナから派生する組織にポリシーを作成できません。	50	コンテナの子組織である組織にはポリシーを作成できません。	ポリシーの作成先となる組織が、コンテナの子でないことを確認します。
グループコンテナが見つかりません。	51	グループコンテナが見つかりませんでした。	親組織または親コンテナにグループコンテナを作成します。
cannotRemoveUserFromFilteredRole	52	フィルタリングされたロールからはユーザーを削除できません。	XML ファイル内のロール DN が、フィルタリングされたロールでないことを確認します。
動的グループからユーザーを消去できません。	53	動的グループからはユーザーを削除できません。	XML ファイル内のグループ DN が動的グループでないことを確認します。

表 D–4 amadmin エラーコード　(続き)

エラーメッセージ	コード	説明/考えられる原因	対処方法
サブスキーマ文字列が存在しません。	54	サブスキーマ文字列が存在しません。	XML ファイル内にサブスキーマ文字列があることを確認します。
ピープルコンテナが見つかりません。	59	ユーザーを組織またはコンテナに追加しようとしています。しかし、デフォルトのピープルコンテナが、組織およびコンテナには存在しません。	デフォルトのピープルコンテナがあることを確認します。
デフォルトの URL プレフィックスが指定されていません。	60	defaultURLPrefix 引数の URL プレフィックスが見つかりません。	適切なデフォルトの URL プレフィックスを指定します。
メタエイリアスが指定されていません。	61	-metaalias 引数のあとにメタエイリアスが見つかりません。	適切なメタエイリアスを指定します。
エンティティ名が指定されていません。	62	エンティティー名が指定されていません。	エンティティー名を指定します。
メタデータをインポートするためのファイル名がありません。	63	メタデータをインポートするファイル名がありません。	メタデータを含むファイルの名前を指定します。
エクスポートされたメタデータを格納するためのファイル名がありません。	64	エクスポートされたメタデータを格納するためのファイル名がありません。	メタデータを格納するファイルの名前を指定します。
メタ属性にハンドラを取得できません。	65	メタ属性にハンドラを取得できません。指定されたユーザー名とパスワードが誤っている可能性があります。	ユーザー名とパスワードが正しいことを確認します。
リソースバンドル名がありません。	66	ディレクトリサーバーに保存されるリソースバンドルを追加、閲覧、または削除しようとしましたが、リソースバンドル名がありません。	リソースバンドル名を指定します。
リソースファイル名がありません。	67	リソースバンドルをディレクトリサーバーに追加しようとしましたが、リソース文字列を含むファイルの名前がありません。	有効なファイル名を指定します。
ライブラリメタの DS への読み込みに失敗しました。	68	ディレクトリサーバーへの Liberty メタの読み込みに失敗しました。	メタデータをチェックしてから再度読み込みます。

索引

い

え

か

く

け

こ

り

れ

ろ