管理ガイド

Sun™ ONE Identity Server

Version 6.1

817-4407-10
2003 年 12 月

目 次

本書について

『Sun™ ONE Identity Server 管理ガイド』では、Sun ONE Identity Server をカスタマイズし、その機能を組織に既存の技術インフラストラクチャに統合する方法について説明します。また、製品とその API のプログラムに関連する情報も含まれています。ここでは、次の項目について説明します。

対象読者

この『管理ガイド』は、IT 管理者、および Sun ONE のサーバーおよびソフトウェアを使用した統合アイデンティティ管理および Web アクセスプラットフォームを実装するソフトウェア開発者向けに書かれています。管理者は次の技術に精通していることが推奨されます。

- Lightweight Directory Access Protocol (LDAP)
- Java™
- JavaServer Pages™ (JSP)
- HyperText Transfer Protocol (HTTP)
- HTML (HyperText Markup Language)
- XML (eXtensible Markup Language)

Sun ONE Directory Server は Identity Server の配備ではデータストアとして使用するため、管理者は、この製品に付属のマニュアルも目を通しておく必要があります。Directory Server の最新のマニュアルは、次の Web サイトからオンラインでアクセスできます。

Identity Server 6.1 のマニュアルセット

Identity Server のマニュアルセットは、2 つに分かれています。Sun ONE Identity Server 6.1 の主要アプリケーションのマニュアルセットと、Sun ONE Identity Server ポリシーエージェントのマニュアルセットです。

Identity Server の主要マニュアル

Identity Server のマニュアルセットには、次のマニュアルが含まれています。

- 『Product Brief』: Identity Server アプリケーションの概要と機能について説明します。
- 『Migration Guide』: 既存のデータおよび Sun ONE 製品の配備を、最新バージョンの Identity Server に移行する方法の詳細について説明します。Identity Server のインストール手順については、『Sun Java Enterprise System 2003Q4 インストールガイド』を参照してください。
- 『管理ガイド』: Identity Server コンソールの使用方法と、コマンド行によるユーザー管理およびデータサービスの方法について説明します。
- 『Customization and API Guide』: Identity Server インストールのカスタマイズ方法について説明します。また、公共の API を使ってアプリケーションに新しいサービスを付加する方法についても説明します。
- 『Deployment Guide』: 既存の情報技術インフラストラクチャ内に Identity Server を配備する方法について説明します。
- 『リリースノート』は、製品のリリース後、オンラインでご利用になれます。このリリースの最新情報、既知の問題、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の各種情報を提供します。

『リリースノート』の更新および主要マニュアルの変更については、Sun ONE のマニュアルの Web サイトにある Identity Server のページで確認できます。更新されたマニュアルには改訂日を記してあります。

Identity Server ポリシーエージェントのマニュアルセット

Identity Server のポリシーエージェントは、サーバー製品自体とは異なるスケジュールで提供されます。したがって、ポリシーエージェントのマニュアルは、Identity Server の主要マニュアルセットとは別に提供されます。このセットには、次のマニュアルが含まれています。

- 『Web Policy Agents Guide』: 各種の Web サーバーやプロキシサーバーに Identity Server ポリシーエージェントをインストールし、設定する方法について説明します。また、トラブルシューティングや、各エージェントに固有の情報についても説明します。
- 『J2EE Policy Agents Guide』: ホストされている J2EE アプリケーションを保護する Identity Server ポリシーエージェントをインストールし、設定する方法について説明します。また、トラブルシューティングや、各エージェントに固有の情報についても説明します。
- 『リリースノート』は、エージェントセットのリリース後、オンラインでご利用になれます。通常、エージェントタイプのリリースごとに『リリースノート』ファイルが 1 つ用意されます。『リリースノート』は、このリリースの最新情報、既知の問題、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の各種情報を提供します。

『リリースノート』の更新およびポリシーエージェントのマニュアルの変更については、Sun ONE のマニュアルの Web サイトにあるポリシーエージェントのページで確認できます。更新されたマニュアルには改訂日を記してあります。

マニュアルに関するフィードバック

米国 Sun Microsystems, Inc. および Identity Server のマニュアル執筆陣は、マニュアルをより良いものにするために、ご意見やご提案をお待ちしております。ご意見は `docfeedback@sun.com` まで電子メールをお送りください。

表記上の規則

Identity Server のマニュアルでは、特定の表記および用語を使用します。これらの規則について、以降の節で説明します。

表記上の規則

このマニュアルでは、次の表記規則を適用します。

- *イタリック体*は、新出用語、強調語句、および文字どおりの意味で使われている語句を示すときに使用します。
- モノスペース（等倍）フォントは、サンプルコードとコードのリスト、API およびプログラミング言語の要素 (関数名、クラス名など)、ファイル名、パス名、ディレクトリ名、HTML タグ、および画面に入力する必要のあるテキストを示すときに使用します。
- *イタリック体セリフ系フォント*は、コード内の可変部分を示すときに使用します。たとえば、次のコマンドの場合、*filename* の位置には `gunzip` コマンドの引数が入ります。

  `gunzip -d` *`filename`*`.tar.gz`

用語

Identity Server マニュアルセットで共通に使用する用語を次に示します。

- Identity Server は、Identity Server および Identity Server ソフトウェアのインストール済みのインスタンスを示します。
- ポリシーおよび管理サービスは、Web サーバーなど専用の配備コンテナで実行される、インストール済みの Identity Server コンポーネントおよびソフトウェアの集合的なセットを示します。
- Directory Server は、Sun ONE Directory Server のインストール済みのインスタンスを示します。
- Application Server は、Sun ONE Application Server のインストール済みのインスタンスを示します。
- Web Server は、Sun ONE Web Server のインストール済みのインスタンスを示します。
- *IdentityServer_base* という変数は、Identity Server のインストール先であるホームディレクトリを示します。

- *DirectoryServer_base* という変数は、Sun ONE Directory Server のインストール先であるホームディレクトリを示します。
- *ApplicationServer_base* という変数は、Sun ONE Application Server のインストール先であるホームディレクトリを示します。
- *WebServer_base* という変数は、Sun ONE Web Server のインストール先であるホームディレクトリを示します。
- Identity Server を実行する Web コンテナは、ポリシーおよび管理サービスがインストールされた専用の J2EE コンテナ (Web Server や Application Server など) を示します。

関連情報

Identity Server のマニュアルのほかにも、参考になるマニュアルがあります。これらのマニュアルの入手先と関連情報を表 0-1 に示します。

表 0-1　Sun ONE 関連情報と入手先

情報	インターネット URL
Directory Server のマニュアルセット	http://docs.sun.com/coll/S1_DirectoryServer_52
Web Server のマニュアルセット	http://docs.sun.com/coll/S1_websvr61_en
Web Proxy Server のマニュアルセット	http://docs.sun.com/prod/s1.webproxys#hic
Sun ONE ダウンロードセンター	http://wwws.sun.com/software/download/
Sun ONE テクニカルサポート	http://www.sun.com/service/sunone/software/index.html
Sun ONE プロフェッショナルサービス	http://www.sun.com/service/sunps/sunone/index.html
Sun エンタープライズサービスによる Solaris のパッチとサポート	http://sunsolve.sun.com/
開発者用情報	http://developers.sun.com/prodtech/index.html

このマニュアルに記載されたサードパーティの 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、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。

第 1 部

Identity Server コンソールガイド

この「Identity Server コンソールガイド」は『Sun™ ONE Identity Server 管理ガイド』の第 1 部です。Identity Server のグラフィカルユーザーインタフェースと、その使用方法について説明しています。次の章で構成されています。

- 製品の概要
- アイデンティティ (識別情報) 管理
- サービス設定
- 現在のセッション
- 連携管理
- ポリシー管理
- 認証オプション
- パスワードリセットサービス

第 1 章

製品の概要

この章では、Sun™ ONE Identity Server の機能の概要を説明します。この章は、次の節で構成されています。

Sun ONE Identity Server

Sun ONE Identity Server テクノロジーは、Sun Open Net Environment (Sun ONE) Platform for Network Identity の一部です。Identity Server は、Lightweight Directory Access Protocol (LDAP) ベースのデータストアである、Sun ONE Directory Server の管理およびセキュリティ保護機能を利用するためのツール群です。Identity Server では、ユーザー認証およびシングルサインオン機能を Directory Server に統合し、データのセキュリティ機能を高めています。また、管理者は、ロールに基づいてユーザーエントリの管理を行うこともできます。ロールとは、ユーザーエントリの属性として現れる、エントリのグループ化メカニズムです。さらに、開発者は、数多くのデフォルトおよびカスタムのサービスで、設定パラメータの定義また管理が可能です。これら 3 つの機能はすべて、カスタマイズ可能なグラフィカルユーザーインタフェースである、ブラウザベースの Identity Server コンソールからアクセスできます。

Identity Server の機能

Identity Server は Directory Server をインストールしたその上に構築されます。このことによって、ディレクトリ管理者は、Directory Server の能力を拡張する機能に加え、より一貫した直感的なインタフェースの利用が可能になります。

サービス設定

デフォルトおよびカスタムのビジネスサービスの設定パラメータは、Identity Server サービス管理コンポーネントで指定します。Identity Server フレームワークで定義された XML および DTD を使用することで、開発者は企業サービス (メールサービス、課金サービス、ログサービスなど) のパラメータを定義し、サービスのパラメータ、つまり属性を管理できます。さらに、Identity Server ではサービス管理者がこれらの属性の値を定義することもできます。

ポリシー管理

Identity Server では、ビジネスリソースへのアクセスを制御するルールを定義、修正、または削除するための方法を用意しています。これらのルールは、まとめてポリシーと呼ばれます。

SAML

Identity Server では、セキュリティ情報の交換に SAML (Security Assertion Markup Language) を使用します。SAML では XML (eXtensible Markup Language) フレームワークを定義して、セキュリティ情報を提供するさまざまなベンダープラットフォーム間の相互運用を実現します。SAML フレームワークについては、『Sun ONE Identity Server Customization and API Guide』を参照してください。

連携管理

Identity Server では、Liberty Alliance Project で策定した連携ネットワークアイデンティティのオープンスタンダードを利用できるように、連携管理モジュールを統合しました。

認証

Identity Server では、ユーザー認証にプラグイン可能なソリューションを用意しています。あるユーザーを認証するために必要な基準は、Identity Server を使用する企業内の各組織に設置された認証サービスによって異なります。Identity Server セッションへのアクセスが許可される前に、ユーザーは認証に成功しなければなりません。

シングルサインオン

ユーザーが認証されると、Identity Server のシングルサインオン (SSO) 用 API が後を引き継ぎます。認証済みのユーザーが保護されたページにアクセスしようとするたびに、SSO API ではそのユーザーの認証資格情報を基に、必要なアクセス権があるかどうかを判断します。ユーザーが有効である場合は、追加で認証を受けることなくページへのアクセスが行われます。そうでない場合、ユーザーはもう一度認証を求められます。

ポリシーエージェント

ポリシーエージェントは、Web コンテナ (Sun ONE Web Server または Sun ONE Application Server) 上にインストールされます。このエージェントは、Identity Server ポリシーコンポーネントの特化したインスタンスです。ユーザーが保護された Web サーバー上の Web リソースに対する要求を送信すると、認証ステップを実行します。この認証は、そのリソースが実行しなければならないユーザー認証チェックに追加されるものです。このエージェントは Web サーバーを保護し、リソースは認証プラグインによって保護されます。

アイデンティティ管理

アイデンティティ管理コンポーネントでは、アイデンティティ関連のオブジェクトを作成および管理することができます。Identity Server 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、ポリシー、組織、サブ組織、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。コンソールにはデフォルト管理者がいます。組織、グループ、コンテナ、ユーザー、サービス、ポリシーを作成し管理するための権限は、管理者によって異なります。ロールに基づいて、管理者を追加作成できます。管理者は Identity Server とインストールするときに、Directory Server 内に定義されます。次の管理者がいます。

- 最上位レベル管理者。Identity Server 企業内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つ

- 最上位ヘルプデスク管理者。Identity Server 企業内のすべてのエントリに対する読み取りアクセス権と、ユーザーパスワードの属性に対する書き込みアクセス権を持つ
- 組織管理者。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つ
- 組織のヘルプデスク管理者。組織のすべてのエントリに対する読み取りアクセス権を持つ
- コンテナ管理者。グループ内のすべてのメンバ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つ、グループ管理者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つ

Identity Server コンソール

Identity Server コンソールはロケーションフレーム、ナビゲーションフレーム、およびデータフレームの 3 つの部分で構成されます。これら 3 つのフレームをすべて活用することで、管理者はディレクトリを移動したり、ユーザーおよびサービスを設定したり、ポリシーを作成したりすることができます。

図 1-1 Identity Server コンソール

ヘッダーフレーム

ヘッダーフレームはコンソールの上部にあります。ヘッダーフレームにあるタブを使用すると、さまざまな管理モジュールの表示に切り換えることができます。

- 「アイデンティティ管理」モジュール - アイデンティティ関連のオブジェクトを作成および管理することができる
- 「サービス設定」モジュール - Identity Server のデフォルトサービスを設定できる
- 「現在のセッション」モジュール - 管理者は、現在のセッション情報を参照したり、任意のセッションを終了したりすることができる
- 「連携管理」モジュール - Liberty Alliance Project で策定した連携ネットワークアイデンティティのオープンスタンダードを利用できる

「場所」フィールドは、ディレクトリツリー内の管理者の位置までの経路です。このパスはナビゲーションのために使用します。

「ようこそ」フィールドは、現在コンソールを実行しているユーザーの名前を、ユーザープロファイルへのリンク付きで表示します。

「検索」リンクは、特定の Identity Server オブジェクトタイプのエントリを検索できるインタフェースを表示します。プルダウンメニューを使用してオブジェクトタイプを選択し、検索文字列を入力します。結果は検索テーブルに表示されます。ワイルドカードも使用できます。

「ヘルプ」リンクは、ブラウザのウィンドウを開きます。このウィンドウにはアイデンティティ管理、現在のセッション、連携管理、およびこのマニュアルの第 3 部である「属性リファレンスガイド」についての情報があります。

「ログアウト」リンクは、ユーザーが Identity Server からログアウトできます。

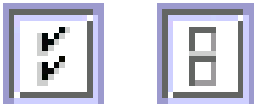
ナビゲーションフレーム

ナビゲーションフレームは、Identity Server コンソールの左部分のフレームです。ディレクトリオブジェクト部分 (グレーのボックス内) には、現在開かれているディレクトリオブジェクトの名前と、そのプロパティへのリンクが表示されます。ナビゲーションフレームに表示されるオブジェクトのほとんどには、対応するプロパティのリンクがあります。このリンクを選択すると、右側のデータフレームにそのエントリの属性が表示されます。「表示」メニューでは、選択したディレクトリオブジェクト配下のディレクトリが一覧表示されます。サブディレクトリ数によっては、ページ移動のメカニズムが用意されます。

データフレーム

データフレームは、コンソールの右部分のフレームです。すべてのオブジェクト属性とその値を表示および設定できるほか、それぞれのグループ、ロール、組織に対してエントリを選択できる場所です。

ヒント　「すべて選択」または「すべてを選択解除」アイコンをクリックすると、リスト内のすべての項目を選択または選択解除できます。



第 2 章

アイデンティティ (識別情報) 管理

この章では、Sun™ ONE Identity Server のアイデンティティ管理機能について説明します。アイデンティティ管理モジュールインタフェースでは、すべての Identity Server オブジェクトおよびアイデンティティを表示、管理、および設定する方法を提供します。この章は、次の節で構成されています。

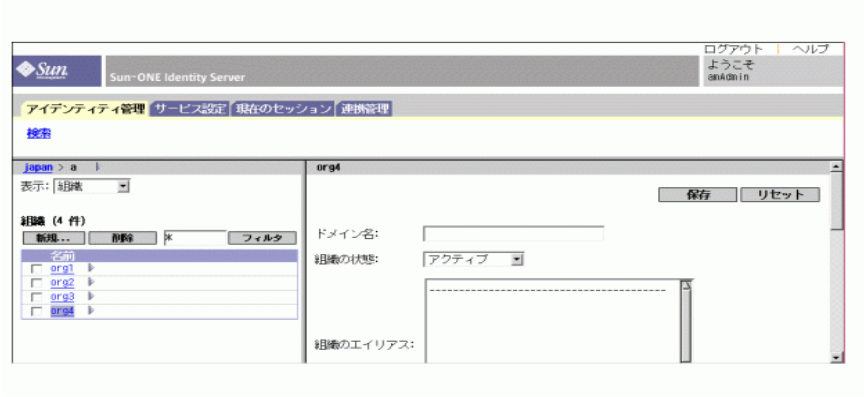
アイデンティティ管理インタフェース

Identity Server グラフィカルユーザーインタフェースには、基本的なビューが 2 つあります。ログインしているユーザーのロールによって、アイデンティティ管理ビューまたはユーザープロファイルビューにアクセスできます。

アイデンティティ管理ビュー

管理者のロールを持つユーザーが Identity Server に認証されると、デフォルトのビューはアイデンティティ管理ビューになります。このビューでは、管理者は管理タスクを実行できます。管理者のロールに応じて実行できる管理タスクには、オブジェクト (ユーザー、組織、ポリシーなど) の作成、削除、管理、およびサービスの設定が含まれます。

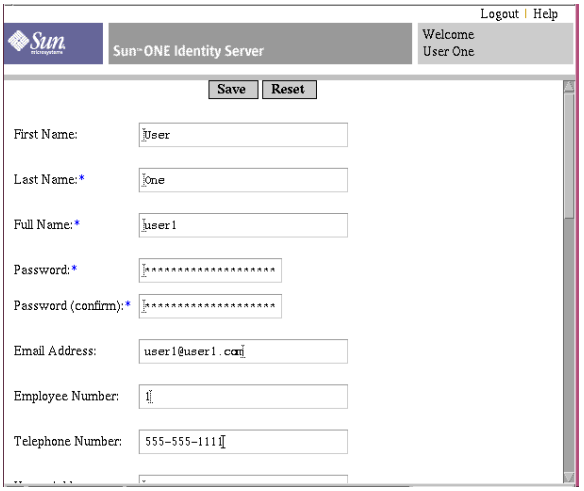
図 2-1　組織プロパティの表示されたアイデンティティ管理ビュー



ユーザープロファイルビュー

管理者のロールを割り当てられていないユーザーが Identity Server に認証されると、デフォルトのビューは各自のユーザープロファイルになります。このビューでは、各自の個人プロファイルに固有の属性値を修正できます。これには名前、ホームアドレス、パスワード以外にも、さまざまな属性が含まれます。ユーザープロファイルビューに表示される属性は拡張できます。オブジェクトおよびアイデンティティのカスタマイズした属性を追加するには、『Sun ONE Identity Server Customization and API Guide』を参照してください。

図 2-2　ユーザープロファイルビュー



Identity Server オブジェクトの管理

ユーザー管理インタフェースには、Identity Server オブジェクト (組織、グループ、ユーザー、サービス、ロール、ポリシー) 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。

プロパティ機能

エントリのプロパティを表示または修正するには、オブジェクト名の隣にある「プロパティ」の矢印をクリックします。属性とその値がデータフレームに表示されます。オブジェクトが異なると表示されるプロパティも異なります。

エントリのプロパティを拡張する詳細については、『Sun ONE Identity Server Customization and API Guide』を参照してください。

組織

このオブジェクトは、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、Identity Server は最上位レベルの組織 (インストール時に定義) をダイナミックに作成して、Identity Server 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。

組織の作成

1. アイデンティティ (識別情報) 管理モジュールの「表示」メニューから、「組織」を選択します。
2. ナビゲーションフレームで「新規」をクリックします。

   「新規組織」テンプレートがデータフレームに表示されます。
3. 「新規組織」テンプレートに組織の名前の値を入力します。
4. 「有効」または「無効」の状態を選択します。

   デフォルトは「有効」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」アイコンを選択して変更できます。「無効」を選択すると、その組織へのログイン中にユーザーアクセスが無効になります。
5. 必要に応じて、オプションのフィールドに値を入力します。オプションのフィールドは次のとおりです。

   「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/UI/Login?org=exampleorg
   ```

   ```
   http://machine.example.com/UI/Login?org=abc
   ```

   ```
   http://machine.example.com/UI/Login?org=123
   ```

   「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、DNS の完全な名前を入力します。

   「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/UI/Login?org=exampleorg
   ```

   ```
   http://machine.example1.com/UI/Login?=org=exampleorg
   ```

   ```
   http://machine.example2.com/UI/Login?org=exampleorg
   ```

「一意の属性リスト」: 組織内のユーザー用の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指定する一意の属性名を追加した場合、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、カ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、カ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。

すべてのサブ組織で一意性が要求されます。

6. 「作成」をクリックします。

   新しい組織がナビゲーションフレームに表示されます。

組織の削除

1. アイデンティティ管理で、「表示」メニューから「組織」を選択します。

   作成されたすべての組織が表示されます。特定の組織を表示するには、検索文字列を入力して「フィルタ」をクリックします。

2. 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。
3. 「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。

ポリシーへの組織の追加

Identity Server オブジェクトは、ポリシーのサブジェクト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「サブジェクト」ページで、組織、ロール、グループ、ユーザーをサブジェクトとして定義できます。サブジェクトを定義すると、ポリシーがオブジェクトに適用されます。詳細は、84 ページの「ポリシーの修正」を参照してください。

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、およびサブグループとして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。スタティックまたはダイナミックに (フィルタを適用して) 管理されているグループに、ユーザーを追加できます。

加入によるメンバーシップ

加入によるグループメンバーシップを指定すると、指定した管理されているグループタイプを基に、スタティックなグループが作成されます。管理されているグループタイプの値が `static` (スタティック) の場合は、`groupOfNames` または `groupOfUniqueNames` オブジェクトクラスを使用して、グループメンバーがグループエントリに追加されます。管理されているグループタイプの値が `dynamic` (ダイナミック) の場合は、LDAP フィルタを使用して、`memberof` 属性を含むユーザーエントリだけを検索して返します。詳細は、165 ページの「管理されているグループタイプ」を参照してください。

フィルタによるメンバーシップ

フィルタを適用したグループは、LDAP フィルタを使用して作成したダイナミックグループです。エントリはすべてフィルタを通してまとめられ、グループにダイナミック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一覧を返します。

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。

管理グループの作成

1. 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. 「表示」メニューから「グループ」を選択します。
3. 「新規」をクリックします。
4. データフレーム内からグループタイプを選択します。

   スタティックな加入グループを作成する場合は、「加入によるメンバーシップ」を選択します。

   a. 「名前」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。

   b. 「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。

c. 「メンバーリスト」で「追加」を選択して、ユーザーをグループに追加します。

d. 検索条件を入力し、「フィルタ」をクリックします。ユーザーの一覧が返ってきたら、追加したいユーザーを選択して「送信」をクリックします。グループへのユーザーの追加は必要に応じて行います。ユーザーはグループの作成後に追加できます。

e. 「作成」をクリックします。

ダイナミックな (LDAP フィルタを適用した) グループを作成する場合は、「フィルタによるメンバーシップ」を選択します。

a. 「名前」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。

b. LDAP 検索フィルタを作成します。

c. フィルタの作成に使用するフィールドでは、OR または AND 演算子を使用します。UI にあるすべてのフィールドを使用します。フィールドを空白のままにすると、そのフィールドはその特定の属性に対して可能なすべてのエントリと一致します。

d. 「作成」をクリックします。

管理グループの削除

1. グループが存在する組織に移動します。
2. 「表示」メニューから「グループ」を選択します。
3. 削除するグループ名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。

注 Identity Server と Directory Server は、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、削除や名前の変更を行った直後に、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 ONE Identity Server Migration Guide』を参照してください。

ポリシーへのグループの追加

Identity Server オブジェクトは、ポリシーのサブジェクト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「サブジェクト」ページで、組織、ロール、グループ、ユーザーをサブジェクトとして定義できます。サブジェクトを定義すると、ポリシーがオブジェクトに適用されます。詳細は、84 ページの「ポリシーの修正」を参照してください。

ユーザー

ユーザーは、個人のアイデンティティを表します。Identity Server のアイデンティティ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、およびユーザーへのサービスの割り当てが可能です。

ユーザーの作成

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。または、ユーザー作成ページからピープルコンテナを選択します。
2. 「表示」メニューから「ユーザー」を選択します。
3. 「新規」をクリックします。

   「新規ユーザー」ページがデータフレームに表示されます。
4. 必要な属性とオプションフィールドの値を入力します。

   ユーザープロファイルの属性については、289 ページの「ユーザー属性」を参照してください。
5. 「作成」をクリックします。

ロールおよびグループへのユーザーの追加

1. ユーザーを修正する組織に移動します。
2. 「表示」メニューから「ユーザー」を選択します。
3. ナビゲーションフレームで、修正するユーザーを選択し、「プロパティ」の矢印をクリックします。
4. データフレームの「表示」メニューから、「ロール」または「グループ」を選択します。

   「ユーザー」表示では、ユーザーサービスを定義した属性をどれでも修正できます。
5. ユーザーを追加するロールまたはグループを選択し、「保存」をクリックします。フィルタを適用したロールやグループは表示されません。

ユーザーへのサービスの追加

1. ユーザーを修正する組織に移動します。
2. 「表示」メニューから「ユーザー」を選択します。
3. ナビゲーションフレームで、修正するユーザーを選択し、「プロパティ」の矢印をクリックします。
4. データフレームの「表示」メニューから「サービス」を選択します。
5. 「追加」をクリックし、ユーザーに割り当てるサービスを選択します。
6. 「保存」をクリックします。

ユーザーの削除

1. ユーザーの存在する組織に移動します。
2. 「表示」メニューから「ユーザー」を選択します。
3. 削除するユーザー名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。

ポリシーへのユーザーの追加

Identity Server オブジェクトは、ポリシーのサブジェクト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「サブジェクト」ページで、組織、ロール、グループ、ユーザーをサブジェクトとして定義できます。サブジェクトを定義すると、ポリシーがオブジェクトに適用されます。詳細は、84 ページの「ポリシーの修正」を参照してください。

サービス

組織またはコンテナのサービスを有効にするには、2 つの手順の処理が必要です。コンテナは組織と同様の振る舞いをします。最初の手順で、サービスを組織に登録する必要があります。サービスの登録後に、その組織用に特別に構成したテンプレートを作成する必要があります。詳細は、第 3 章「サービス設定」を参照してください。

注 新しいサービスは、まずコマンド行の `amadmin` を使用して Identity Server にインポートする必要があります。サービスの XML スキーマのインポートについては、『Sun ONE Identity Server Customization and API Guide』を参照してください。

サービスの登録

1. サービスを追加する組織に移動します。

   アイデンティティ管理モジュールで「表示」メニューから「組織」を選択し、ナビゲーションフレームから組織を選択します。デフォルトの最上位組織と選択した組織がロケーションパスに表示されます。

2. 「表示」メニューから「サービス」を選択します。

3. 「登録」をクリックします。

   この組織に登録可能なサービスのリストがデータフレームに表示されます。

4. 追加するサービスの横にあるチェックボックスを選択します。

5. 「登録」をクリックします。登録済みのサービスがナビゲーションフレームに表示されます。

注 最上位組織に登録されているサービスだけがロールレベルで表示されます。

サービス用のテンプレートの作成

1. 登録したサービスがある組織またはロールに移動します。

   アイデンティティ管理モジュールで「表示」メニューから「組織」を選択し、ナビゲーションフレームから組織を選択します。

2. 「表示」メニューから「サービス」を選択します。

3. 有効にするサービス名の横にあるプロパティアイコンをクリックします。

   データフレームに、「このサービスに利用可能なテンプレートはありません。新規に作成しますか ?」というメッセージが表示されます。

4. 「作成」をクリックします。

   このサービス用のテンプレートが親の組織またはロール用に作成されます。このサービスのデフォルト属性と値がデータフレームに表示されます。デフォルトサービスの属性については、161 ページの「属性リファレンスガイド」で説明しています。

5. デフォルト値を受け入れるか、または変更して、「保存」をクリックします。

サービスの登録の解除

1. サービスを削除する組織に移動します。

   アイデンティティ管理モジュールで「表示」メニューから「組織」を選択し、ナビゲーションフレームから組織を選択します。

2. 「表示」メニューから「サービス」を選択します。

3. 削除するサービスのチェックボックスを選択します。

4. 「登録解除」をクリックします。

注 サービスがサブ組織のレベルで登録されている場合は、親組織のレベルでそのサービスの登録を解除することはできません。

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、LDAP エントリの属性で定義されます。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、Identity Server 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、Identity Server コンソールで管理することはできません。ポリシーのサブジェクト定義に他の Directory Server タイプを使用することもできます。ポリシーサブジェクトについての詳細は、81 ページの「ポリシー管理」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 URL ポリシーエージェントサービスの属性を持つコントラクタロールを作成できます。管理者はコントラクタエントリの別の属性を設定しなくても、新しいコントラクタが開始すると、コントラクタにこのロールを割り当てることができます。コントラクタがフルタイムの従業員になると、管理者はこのユーザーに別のロールを割り当て直すことになります。

Identity Server 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。Identity Server を初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限が定義されます。

ユーザーは、管理サービスで「ユーザーのロールを表示」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。詳細は、174 ページの「ユーザーのロールを表示」を参照してください。

グループ同様に、ロールもフィルタで作成することも、スタティックに作成することもできます。

「フィルタされたロール」：フィルタを適用したロールは、LDAP フィルタを使用して作成したダイナミックロールです。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。

「スタティックロール」：フィルタされたロールとは対照的に、スタティックロールはユーザーをロールの作成時に追加しなくても作成できます。これにより、特定のユーザーを指定されたロールに追加するときの制御がより細かくできます。

フィルタされたロールの作成

1. ナビゲーションフレームで、ロールを作成する組織に移動します。
2. 「表示」メニューから「ロール」を選択します。

   組織の構成時にデフォルトのロールが作成され、ナビゲーションフレームに表示されます。

   これらのロールについては、「属性リファレンス」の節の169 ページの「ダイナミック管理者ロール ACI」を参照してください。
3. ナビゲーションフレームで「新規」をクリックします。「新規ロール」テンプレートがデータフレームに表示されます。
4. 「フィルタされたロール」を選択し、名前を入力します。「次へ」をクリックします。
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、DIT でどこからユーザーを開始するかをコンソールが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。166 ページの「デフォルトロールアクセス権 (ACI)」の節を参照してください。ここで示すデフォルトの権限は順不同です。

   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。

   「論理演算子」: 演算子を含めたい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。AND 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。OR 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。

   「ユーザー ID」: ユーザー ID でユーザーを検索します。

   「ファーストネーム」: 名 (ファーストネーム) でユーザーを検索します。

   「ラストネーム」: 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 (有効または無効) でユーザーを検索します。

   「高度」ボタンを選択すると、フィルタ属性自体を定義できます。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 (デフォルト)、次のロールが作成されます。

   ```
   (objectclass = inetorgperson)
   ```

   「リセット」をクリックするとフィルタのプロパティを消去できます。また「キャンセル」をクリックすると、ロールの作成処理をキャンセルできます。

9. 「作成」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。

スタティックロールの作成

1. ナビゲーションフレームで、ロールを作成する組織に移動します。
2. 「表示」メニューから「ロール」を選択します。

組織の構成時にデフォルトのロールが作成され、ナビゲーションフレームに表示されます。

これらのロールについては、「属性リファレンス」の節の169 ページの「ダイナミック管理者ロール ACI」を参照してください。

3. ナビゲーションフレームで「新規」をクリックします。「新規ロール」テンプレートがデータフレームに表示されます。
4. 「スタティックロール」を選択し、名前を入力します。「次へ」をクリックします。
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、DIT でどこからユーザーを開始するかをコンソールが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。166 ページの「デフォルトロールアクセス権 (ACI)」の節を参照してください。ここで示すデフォルトの権限は順不同です。

   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. 「作成」をクリックします。

   作成されたロールがナビゲーションフレームに表示され、ロールのステータス情報がデータフレームに表示されます。

   ロールで利用可能なサービスは、そのロールの親組織から継承されます。ロールのサービステンプレートが存在しない場合は、「編集」リンクをクリックして作成できます。サービステンプレートが存在する場合は、サービスのプロパティが表示され、設定できます。詳細は、48 ページの「ロールへのサービスのカスタマイズ」を参照してください。

スタティックロールへのユーザーの追加

1. 修正するロールを選択し、「プロパティ」の矢印をクリックします。
2. データフレームの「表示」メニューから「ユーザー」を選択します。
3. 「追加」をクリックします。
4. 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。

「論理演算子」: 演算子を含めたい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。AND 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。OR 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。

「ユーザー ID」: ユーザー ID でユーザーを検索します。

「ファーストネーム」: 名 (ファーストネーム) でユーザーを検索します。

「ラストネーム」: 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 (有効または無効) でユーザーを検索します。

「ユーザー検索属性」: 検索で返される値を指定できます。

5. 「フィルタ」をクリックすると、検索が始まります。
6. 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。
7. 「保存」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。

注 ロールプロファイルページやユーザープロファイルページを使用して、ユーザーをロールに追加することもできます。

ロールからのユーザーの削除

1. 変更するロールを含む組織に移動します。

   アイデンティティ管理モジュールで「表示」メニューから「組織」を選択し、ナビゲーションフレームから組織を選択します。
2. 「表示」メニューから「ロール」を選択します。
3. 変更するロールを選択します。
4. 「表示」メニューから「ユーザー」を選択します。
5. 削除するユーザーのチェックボックスを選択します。
6. 「削除」をクリックします。

   これで、ロールからユーザーが削除されます。

注	Identity Server と Directory Server は、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 ONE Identity Server Migration Guide』を参照してください。

ポリシーへのロールの追加

Identity Server オブジェクトは、ポリシーのサブジェクト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「サブジェクト」ページで、組織、ロール、グループ、ユーザーをサブジェクトとして定義できます。サブジェクトを定義すると、ポリシーがオブジェクトに適用されます。詳細は、84 ページの「ポリシーの修正」を参照してください。

ロールへのサービスのカスタマイズ

ロールで利用可能なサービス、およびそのサービス属性に対するアクセスレベルをロール単位でカスタマイズできます。「一般」表示を使用すると、管理者はサービスおよびユーザーページをカスタマイズし、特定のサービスへのアクセスだけが可能なサービス管理者を作成できます。たとえば、管理者は指定されたロールで、ユーザーサービスの 1 つ以上の属性に対して書き込みアクセスを拒否することができます。そして、このロールを持つユーザーは、そのような属性を変更することができなくなります。ポリシー管理者ロールを作成するには、すべてのポリシーサービスへのアクセスを付与し、その他のサービスへのアクセスを拒否します。すると、ポリシー管理者ロールを持つ管理者は、ポリシーを作成および割り当てできるようになりますが、ユーザー管理タスクを実行することは拒否されます。

サービスを表示するには、サービスを組織レベルで登録する必要があります。ロールに追加されたユーザーは、ロールのサービス属性を継承します。

サービスアクセスのカスタマイズ

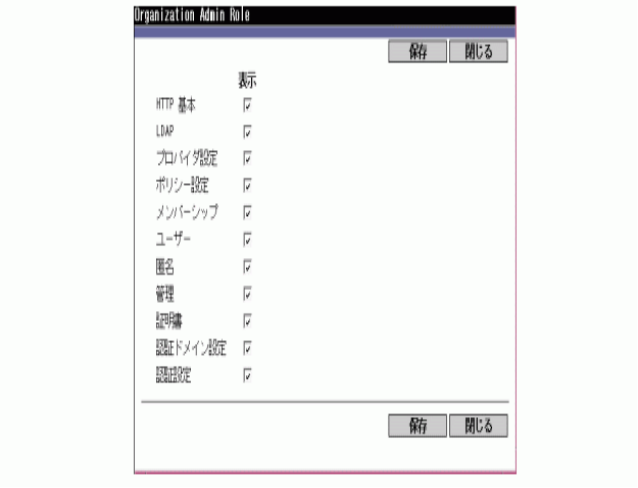
1. 変更するロールの「プロパティ」の矢印をクリックします。
2. 「表示」メニューから「一般」を選択します。
3. 「ロールプロパティ」ページで、「サービス」のリストで「編集」をクリックします。

   図 2-3 に示すようなサービスアクセスページが表示されます。
4. 「表示」列でサービス名をクリックすることで、ロールに付与するサービスを選択します。デフォルトで、ロールはすべてのサービスへアクセスできます。

5. 「保存」をクリックします。

注 サービスへのアクセスを拒否すると (選択されていない場合)、サービスはこのロールを持つユーザーの Identity Server コンソールに表示されません。さらに、ユーザーの登録または登録解除、ユーザーへのサービスの割り当て、またはサービステンプレートの作成、削除、表示、修正ができなくなります。

図 2-3 サービスアクセスページ

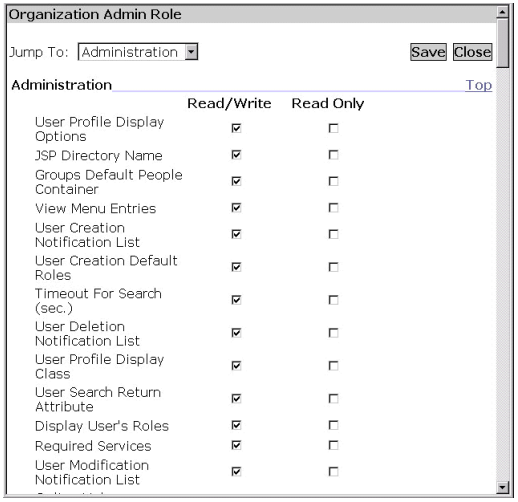


属性アクセスのカスタマイズ

1. 「ロールプロパティ」ページで、「サービス属性」のリストの「編集」をクリックします。図 2-4 に示すような属性アクセスページが表示されます。
2. 「ジャンプ先」メニューを使用して、特定のサービスの属性を表示します。
3. 「読み取り／書き込み」または「読み取り専用」チェックボックスを選択し、その属性へのアクセスレベルを割り当てます。
4. 「保存」をクリックします。

注 属性に「読み取り / 書き込み」または「読み取り専用」オプションのどちらも選択されていない場合、その属性に対する読み取りおよび書き込みのアクセスは拒否されます。

図 2-4 属性アクセスページ



特定のサービスの属性の詳細については、このマニュアルの第 3 部「属性リファレンスガイド」を参照してください。

ロールの削除

1. 削除するロールを含む組織に移動します。

   アイデンティティ管理で「表示」メニューから「組織」を選択し、ナビゲーションフレームから組織を選択します。デフォルトの最上位組織と選択した組織がロケーションパスに表示されます。

2. 「表示」メニューから「ロール」を選択します。
3. ロール名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。

ポリシー

ポリシーでは、組織の Web リソースを保護するためのルールを定義します。ポリシーの作成、修正、削除はアイデンティティ管理モジュールを使用して実行しますが、81 ページの「ポリシー管理」で説明しています。

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、組織エントリが使用できない場合に使用します。Identity Server コンテナエントリと Identity Server 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、Identity Server 管理サービスで「メニューにコンテナを表示」を選択します。詳細は、165 ページの「メニューにコンテナを表示」を参照してください。

コンテナの作成

1. コンテナを作成する組織またはコンテナに移動します。

   「表示」メニューから「コンテナ」を選択します。

2. 「新規」をクリックします。

   コンテナのテンプレートがデータフレームに表示されます。

3. 作成するコンテナの名前を入力します。
4. 「作成」をクリックします。

コンテナの削除

1. 削除対象のコンテナを含む組織またはコンテナに移動します。
2. 「表示」メニューから「コンテナ」を選択します。
3. 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。
4. 「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。

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にあり、サブピープルコンテナとしてピープルコンテナレベルにあります。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、Identity Server 管理サービスで「ピープルコンテナを表示」を選択します。詳細は、164 ページの「ピープルコンテナを表示」を参照してください。

ピープルコンテナの作成

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。

   「表示」メニューから「ピープルコンテナ」を選択します。

2. 「新規」をクリックします。

   ピープルコンテナのテンプレートがデータフレームに表示されます。

3. 作成するピープルコンテナの名前を入力します。
4. 「作成」をクリックします。

ピープルコンテナの削除

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. 「表示」メニューから「ピープルコンテナ」を選択します。
3. 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。
4. 「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。

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ダイナミック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、Identity Server 管理サービスで「グループコンテナを表示」を選択します。詳細は、165 ページの「グループコンテナを表示」を参照してください。

グループコンテナの作成

1. 作成対象のグループコンテナを含む組織またはグループコンテナに移動します。
2. 「表示」メニューから「グループコンテナ」を選択します。

   デフォルトの「グループ」は組織の作成時に作成されています。
3. 「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、「作成」をクリックします。

   新しいグループコンテナがナビゲーションフレームに表示されます。

グループコンテナの削除

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. 「表示」メニューから「グループコンテナ」を選択します。

   デフォルトの「グループ」と、作成したすべてのグループコンテナがナビゲーションフレームに表示されます。
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. 選択した項目の「削除」をクリックします。

第 3 章

サービス設定

この章では、Sun™ ONE Identity Server のサービス管理機能について説明します。サービス設定インタフェースでは、Identity Server サービスおよびその値 (デフォルトとカスタムの両方) を表示、管理、および設定する方法を備えるほかに、Identity Server コンソールの表示設定を行う方法を備えています。この章は、次の節で構成されています。

サービスの定義

サービスとは、共通名のもとに定義された属性のグループです。属性では、サービスが組織に提供するパラメータを定義します。たとえば、給与情報サービスの開発では、開発者は従業員名、時給、税の控除などを定義する属性を含めるかどうかを決める場合があります。このサービスが組織に登録されると、その組織ではこれらの属性をエントリの設定で使用できます。

Identity Server では XML (Extensible Markup Language) を使用してサービスを定義します。サービス管理サービスのドキュメントタイプ定義 (`sms.dtd`) では、サービスの XML ファイルの構造を定義します。このファイルは、次のディレクトリにあります。

IdentityServer_base`/SUNWam/dtd/`

Identity Server サービスの定義の詳細は、『Sun ONE Identity Server Customization and API Guide』を参照してください。

Identity Server のサービス

Identity Server に付属するデフォルトのサービスは、次のディレクトリにある XML ファイルで定義されています。

IdentityServer_base/SUNWamconfig/xml

または

/etc/opt/SUNWam/config/xml

一部のサービスでは、サービス設定インタフェースで設定するときに、Identity Server アプリケーション用に値を定義します。ほかのサービスは、Identity Server 内で設定された特定の組織に登録され、その組織用にデフォルト値を定義するために使用されます。

管理サービス

管理サービスでは、アプリケーションレベル (Identity Server アプリケーションの「プリファレンス」または「オプション」メニューに似たもの) と設定済みの組織レベル (設定済み組織に固有の「プリファレンス」または「オプション」メニュー) の両方で、コンソールを設定できます。

認証サービス

基本モジュールを含めて、10 種類の認証モジュールがあります。管理者は定義済み組織のそれぞれで、ユーザーの認証を検証するための方法を選択できます。

匿名

ユーザー名とパスワードを指定せずにログインできます。匿名接続ではサーバーへのアクセスに制限があり、管理者がカスタマイズできます。

証明書に基づく認証モジュール

個人用デジタル証明書 (PDC) を使用してログインできます。

注	6.1 リリースでは、Application Server 配備用の証明書認証サービスはサポートされていません。

コア

このモジュールは、Identity Server 認証サービスの一般設定の基本となります。どのサービスを使用する場合も、登録し、設定する必要があります。管理者は、匿名、証明書に基づく、HTTP 基本、LDAP、メンバーシップ、NT、RADIUS、SafeWord、SecurID、および UNIX の各認証サービスで、値が特に設定されない場合に使用されるデフォルト値を定義できます。

HTTP 基本

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。

LDAP

LDAP バインドを使用して認証できるようにします。LDAP バインドとは、パスワードを特定の LDAP エントリに関連付ける操作です。

メンバーシップ (自己登録)

ログインおよびパスワードを使用した認証を受けるために、新しいユーザーは自己登録できます。

NT

Windows NT™/2000™ サーバーを使用してユーザーを認証できます。NT 認証モジュールを実際に使用するには、Samba Client (smbclient) 2.2.2 をダウンロードしてインストールする必要があります。

RADIUS

外部 RADIUS (Remote Authentication Dial-In User Service) サーバーを使用して、ユーザーを認証できます。

Sun ONE Application Server で RADUIS 認証サービスを正常に機能させるには、Application Server の `service.policy` ファイルを設定する必要があります。手順については、93 ページの「認証オプション」を参照してください。

SafeWord

Secure Computing の SafeWord™ または SafeWord PremierAccess™ 認証サーバーを使用して、ユーザーを認証できます。

Sun ONE Application Server で SafeWord 認証サービスを正常に機能させるには、Application Server の `service.policy` ファイルを設定する必要があります。手順については、93 ページの「認証オプション」を参照してください。

SecurID

RSA ACE/ServerÆ 認証ソフトウェアと SecurIDÆ 認証を使用して、ユーザーを認証できます。このサービスは、Solaris x86 ではサポートされていません。

UNIX

UNIX サーバーを使用して、ユーザーを UNIX ID とパスワードで認証できます。

注	UNIX 認証サービスは、Windows 2000 プラットフォームではサポートされていません。

認証設定サービス

認証設定サービスでは、ロール、ユーザー、およびサービスに対する認証を設定したり、認証モジュールの優先順位を決めるためのルールを決めるために、組織を設定することができます。

クライアントディテクションサービス

クライアントディテクションサービスを使用すると、アクセス中のブラウザのクライアントタイプを Identity Server で検出でき、それに基づいて管理者はデバイスの追加や設定を行うことができます。

グローバル化設定のサービス

グローバル化設定に含まれているプロパティを使用すると、さまざまな文字セットに対応するように Identity Server を設定できます。

ログサービス

ログサービスでは、管理者は Identity Server アプリケーションのログ機能を設定します。例には、ログファイルのサイズやログファイルの場所が含まれます。

ネーミングサービス

ネーミングサービスは、URL、プラグイン、および設定を、取得したり設定するために使用します。また、セッション、認証、ログなど、さまざまなその他の Identity Server サービスの通知を要求するために使用します。

パスワードリセットサービス

パスワードリセットサービスでは、Identity Server 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したり、忘れた場合に取得できます。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によって定義され、ユーザー検証の資格情報を「秘密の質問」形式で制御し、新規または既存のパスワード通知のメカニズムを制御します。また、ユーザー検証が失敗した場合のロックアウト間隔も設定できます。

プラットフォームサービス

プラットフォームサービスは、Identity Server アプリケーションの最上位で適用された Identity Server 設定やその他のオプションに、サーバーを追加できます。

ポリシー設定サービス

ポリシー設定サービスは、ポリシー管理やポリシー評価の際にポリシーフレームワークで使用する値を定義します。

SAML サービス

SAML (Security Assertion Markup Language) サービスは、セキュリティ当局間でセキュリティアサーションを交換するためのフレームワークを定義します。これは、認証および承認サービスを提供するさまざまなプラットフォーム間の相互運用性を実現することを目的としています。

セッションサービス

セッションサービスでは、最大セッション時間、最大アイドル時間など、認証済みのユーザーセッションでの値を定義します。

ユーザーサービス

ユーザーサービスを使用して、デフォルトのユーザー設定を定義します。タイムゾーン、ロケール、および DN 開始表示などが含まれます。

属性のタイプ

Identity Server サービスを構成する属性は、ダイナミック、ポリシー、ユーザー、組織、グローバルのいずれかのタイプに分類されます。サービスの属性を細分するのにこれらのタイプを使用すると、サービススキーマの内容をより一貫したものにしたり、サービスパラメータの管理をさらに容易にしたりすることができます。

ダイナミック属性

ダイナミック属性は、Identity Server の設定済みロールまたは組織に割り当てることができます。ロールがユーザーに割り当てられるか、ユーザーが組織で作成される場合は、ダイナミック属性がそのユーザーの特性になります。たとえば、ロールを組織の従業員用に作成します。このロールには組織の住所とファックス番号という、全従業員において不変の 2 つの項目が含まれているとします。このロールが各従業員に割り当てられると、これらのダイナミック属性は各従業員に継承されます。

ユーザー属性

ユーザー属性は各ユーザーに直接割り当てられます。ロールまたは組織から継承されず、また、通常はユーザーごとに異なります。ユーザー属性の例としては、ユーザー ID、社員番号、およびパスワードなどが挙げられます。`amUser.xml` ファイルを修正することで、ユーザー属性をユーザーサービスに対して追加または削除できます。詳細は、『Sun ONE Identity Server Customization and API Guide』を参照してください。

組織属性

組織属性は組織にだけ割り当てられます。この点からはダイナミック属性のように機能しますが、ダイナミック属性と異なるのは、サブツリー内のエントリに継承されないという点です。さらに、組織属性に割り当てられるオブジェクトクラスはありません。認証サービスにリストされる属性は、組織属性として定義されます。それは、サブツリーまたはユーザーのレベルではなく、組織レベルで認証が行われるためです。

グローバル属性

グローバル属性は、Identity Server 設定に対して適用されます。グローバル属性の目的は Identity Server アプリケーションをカスタマイズすることであるため、ユーザー、ロール、または組織に適用することはできません。Identity Server 設定ではグローバル属性のインスタンスは 1 つしかありません。また、グローバル属性に割り当てられるオブジェクトクラスはありません。グローバル属性の例としては、ログファイルのサイズ、ログファイルの場所、データにアクセスするために Identity Server で使用するポート番号やサーバー URL などがあります。

ポリシー属性

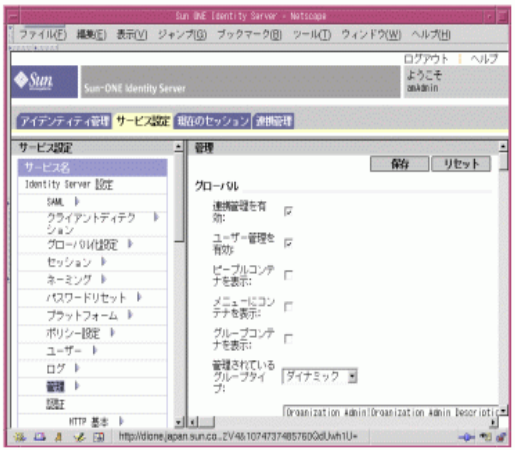
ポリシー属性は、サービスに関連するアクセス制御アクション (権限) を指定します。ポリシーにルールを追加するとき、これらの属性がルールの一部になります。

サービス設定インタフェース

サービスはサービス設定モジュールで設定され、管理されます。Identity Server のデフォルトサービスパッケージで対応できない組織固有のサービスは、Identity Server サービス DTD (ドキュメントタイプ定義) を基に XML を使用して記述し、「その他の設定」見出し下のインタフェースに追加することができます。この手順については、第 3 部「属性リファレンスガイド」を参照してください。デフォルトサービス、および対応する属性の定義について説明しています。

サービス設定モジュールは、グローバルレベルでサービス設定を表示するために使用します。つまり、登録しているかどうかにかかわらず、Identity Server で利用可能なすべてのサービスのデフォルト設定を表示します。サービスが組織で登録され有効にされると、サービスのサービス設定ページには、サービスに割り当てられた初期のデフォルトデータが表示されます。図 3-1 はグラフィカルユーザーインタフェースのスクリーンショットです。

図 3-1　サービス設定の表示



サービス設定表示にアクセスするには、サービス設定モジュールを選択します。ナビゲーションフレームに、すべての定義済みの Identity Server サービスのリストが表示されます。サービスのグローバルなデフォルト値を設定するには、サービス名の隣にある「プロパティ」の矢印を選択します。そのサービスの属性がデータフレームに表示されます。

第 4 章

現在のセッション

この章では、Sun™ ONE Identity Server 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。

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、Identity Server 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。

図 4-1　現在のセッションのインタフェース

セッション管理フレーム

セッション管理フレームには、現在管理されている Identity Server の名前が表示されます。

セッション情報ウィンドウ

セッション情報ウィンドウには、Identity Server 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」：ユーザーの再認証までの、セッション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。詳細は、285 ページの「セッションサービス属性」を参照してください。

「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や特定の範囲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。そのためには、次の手順を実行します。

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 5 章

連携管理

この章では、Sun™ ONE Identity Server の連携管理インタフェース機能について説明します。連携管理インタフェースでは、認証ドメインおよびプロバイダに関するメタデータを表示、管理、および設定する方法を備えています。

Liberty Alliance Project の仕様 1.0 に記述されている機能はサポートされなくなりました。実質的には 1.0 による配備はないため、深刻な影響はありません。

この章は、次の節で構成されています。

注 この章で説明する属性フィールドで例示するデータは、デフォルトでは次の場所にあります。

IdentityServer_base/SUNWam/samples/liberty

認証ドメインおよびプロバイダの概要

連携管理モジュールでは、認証ドメイン、リモートプロバイダ、およびホストプロバイダを作成、修正、および削除するインタフェースを備えています。次の手順は、連携管理の基本モデルを示しています。

1. 認証ドメインを作成します。
2. 作成した認証ドメインに属するホストプロバイダを 1 つ以上作成します。
3. 作成した認証ドメインに属するリモートプロバイダを 1 つ以上作成します。リモートプロバイダのメタデータも含める必要があります。

4. プロバイダ間の信頼関係を確立します。ホストプロバイダでは、同じ認証ドメインに属するホストまたはリモートプロバイダのサブセットを信頼することもできます。

次の節では、認証ドメイン、リモートプロバイダ、およびホストプロバイダを作成し、設定する方法について説明します。

認証ドメイン

ここでは、認証ドメインの作成、修正、および削除方法を説明します。

認証ドメインの作成

1. 連携管理モジュールの「表示」メニューから「認証ドメイン」を選択します。
2. ナビゲーションフレームで「新規」をクリックします。

   「新規認証ドメイン」テンプレートがデータフレームに表示されます。
3. 「新規認証ドメイン」ウィンドウで、認証ドメインの名前を入力します。
4. 認証ドメインの説明に値を入力します。
5. 「ライタサービス URL」の値を入力します。

   「ライタサービス URL」は、共通ドメインからの cookie を書き込むサービスが行われる場所を指定します。たとえば example.com が共通ドメインの場合、URL は次のようになります。

   ```
   http://example.com:8080/liberty/WriterServlet
   ```
6. 「リーダサービス URL」の値を入力します。

   「リーダサービス URL」は、共通ドメインからの cookie を読み込むサービスの場所を指定します。
7. 「有効」または「無効」の状態を選択します。

   デフォルトは「有効」です。これは、その認証ドメインの存続期間中であればいつでも、「プロパティ」アイコンを選択して変更できます。「無効」を選択すると、現在の Identity Server インストールに関して、認証ドメイン内での Liberty 通信が無効になります。
8. 「作成」をクリックします。

   新しい認証ドメインがナビゲーションフレームに表示されます。

認証ドメインの修正

1. 修正したい認証ドメインの横にあるプロパティの矢印をクリックします。

   認証ドメインのプロパティがデータフレームに表示されます。

2. 認証ドメインのプロパティを修正します。
3. 「保存」をクリックします。

認証ドメインの削除

認証ドメインを削除しても、そのドメインに属するプロバイダは削除されません。削除された認証ドメインにプロバイダが属している場合、そのプロバイダ自体を削除しないかぎり、プロバイダは認証ドメインに属したままとなります。削除された認証ドメインにプロバイダを追加することはできません。

1. 連携管理モジュールの「表示」メニューから「認証ドメイン」を選択します。

   作成されたすべての認証ドメインがナビゲーションフレームに表示されます。

2. 削除する認証ドメイン名の横にあるチェックボックスを選択します。
3. 選択した項目の「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。

プロバイダ

ここでは、リモートおよびホストプロバイダの作成、修正、および削除方法を説明します。

リモートプロバイダの作成

リモートプロバイダとは、主体からのメタデータを受信するエンティティのことです。主体とは、システムとやりとりする組織や個人を指します。リモートプロバイダを作成するには、次の手順に従ってください。

1. 連携管理モジュールの「表示」メニューから「リモートプロバイダ」を選択します。

   プロバイダを作成すると、デフォルトではサービスプロバイダとなります。手順 15 の説明にあるオプションを選択すれば、リモートプロバイダをアイデンティティプロバイダとして作成することもできます。

2. 「新規」をクリックします。「リモートプロバイダの作成」ウィンドウが表示されます。
3. 「プロバイダ ID」の値を入力します。

   「プロバイダ ID」には、プロバイダの URL 識別子を指定する必要があります。リモートプロバイダおよびホストプロバイダすべてに対して重複しない値にする必要があります。
4. リモートプロバイダの詳細を入力します。
5. 「セキュリティキー」を入力します。

   「セキュリティキー」は、セキュリティ証明エイリアスを定義します。証明書はすべて、エイリアスに対する JKS キーストアに格納されています。このエイリアス (セキュリティキー) は、必要な証明書を取得するために使用します。
6. 「SOAP エンドポイント URL」を入力します。

   このフィールドは、SOAP 要求の受信者の場所を指定します。SOAP 経由のバックチャネルの通信 (ブラウザを使用しない通信) に使用されます。
7. 「シングルログアウトサービス URL」を入力します。

   「シングルログアウトサービス URL」は、サービスプロバイダまたはアイデンティティプロバイダがログアウト要求を送受信するために使用されます。
8. 「シングルログアウトの返信 URL」を入力します。

   この値は、ログアウト要求処理後に要求がリダイレクトされる URL を指定します。
9. 「連携終了サービス URL」を入力します。

   このフィールドは、連携の終了要求をどの URL に通知するかを指定します。
10. 「連携終了の返信 URL」の値を入力します。

    この値は、連携の終了要求処理後に要求がリダイレクトされる URL を指定します。
11. 「シングルサインオンサービス URL」を定義します。

    このフィールドは、連携と SSO の期間中にサービスプロバイダが要求を送信する、アイデンティティプロバイダの URL を定義します。このフィールドは、「アイデンティティプロバイダ」オプションが有効になっている場合のみ定義する必要があります。
12. 「名前登録サービス URL」を入力します。

このフィールドは、サービスプロバイダがアイデンティティプロバイダと通信する間に、専用の名前識別子を登録するために用いる、名前登録プロトコルを使用します。連携セッションが確立した後でのみ、登録が行われます。このフィールドは、サービスプロバイダが名前識別子をアイデンティティプロバイダに登録するために使用するサービス URL を定義します。

13. 「名前登録の返信 URL」を入力します。

    このフィールドは、サービスプロバイダがアイデンティティプロバイダと通信する間に、専用の名前識別子を登録するために用いる、名前登録プロトコルを使用します。連携セッションが確立した後でのみ、登録が行われます。「名前登録の返信 URL」は、アイデンティティプロバイダが登録の状況を返信する URL です。

14. 「アサーションコンシューマ URL」を入力します。

    このフィールドは、アイデンティティプロバイダが SAML アサーションを送信するサービスプロバイダの終端点を定義します。

15. リモートプロバイダをアイデンティティプロバイダとして定義するかどうかを決定します。デフォルトでは、すべてのプロバイダがサービスプロバイダとなります。「アイデンティティプロバイダ」オプションを選択すると、リモートプロバイダがアイデンティティプロバイダとしても定義されます。

16. 「作成」をクリックします。

    新しいプロバイダがナビゲーションフレームに表示されます。

リモートプロバイダの修正

リモートホストは、作成後いつでも修正できます。そのためには、次の手順を実行します。

1. ナビゲーションフレームの「表示」メニューから「リモートプロバイダ」を選択します。
2. 修正したいプロバイダのプロファイルを選択し、「編集」の矢印をクリックします。

   デフォルトでは、ナビゲーションフレームは「一般」表示となっています。「一般」表示内のほとんどのフィールドには、リモートプロバイダの作成時に入力されたデータが入っています。次の追加フィールドを修正できます。

   「プロバイダの簡潔な ID」: アイデンティティプロバイダに対してサービスプロバイダを一意に特定します。

   「プロバイダの簡潔な ID」は、SHA1 で符号化された文字列にする必要があります。プロバイダ ID の文字列は、符号化する値として使用してください。こうすれば、重複を確実に避けられます。SHA1 符号化を生成するには、OpenSSL コマンド行ツールの構文を使用します。

```
$ echo プロバイダ ID | openssl sha1
```

フィールドを修正した場合、「保存」をクリックして変更を保存します。

「状態」: 有効状態にすると、リモートプロバイダが連携と SSO で使用できます。無効状態にすると、リモートプロバイダは使用不能となり、要求に応答しなくなります。

3. 「サービスプロバイダ」フィールドを変更するには、「表示」メニューで「サービスプロバイダ」を選択します。

   「アサーションコンシューマ URL」フィールドには、リモートプロバイダの作成時に入力されたデータが入っています。なお、次のフィールドも修正可能です。

   「連携後の名前登録」: このオプションを有効にすると、サービスプロバイダでは連携後に名前登録に参加できます。名前登録とは、サービスプロバイダが主体の名前識別子を指定するためのプロファイルです。名前識別子は、アイデンティティプロバイダがサービスプロバイダと通信する際に使用します。

   「署名済みの認証要求」: このオプションが有効になっている場合、署名済みの認証および連携の要求をリモートプロバイダが送信するように指定します。アイデンティティプロバイダは、サービスプロバイダから署名のない要求を受け取っても処理しません。

   「アサーションコンシューマ URL」: このフィールドは、アイデンティティプロバイダが SAML アサーションを送信するプロバイダの終端点を定義します。

   「連携終了のプロファイル」: SOAP または HTTP リダイレクトを選択できます。このフィールドは、連携終了の通知に SOAP または HTTP リダイレクトプロファイルを使用するかどうかを指定します。対象プロバイダの存続期間中であればいつでも変更できます。

   「シングルログアウトのプロファイル」: SOAP または HTTP リダイレクトを選択できます。このフィールドは、ログアウトイベントの通知に SOAP または HTTP リダイレクトを使用するかどうかを指定します。対象プロバイダの存続期間中であればいつでも変更できます。

   「名前登録のプロファイル」: SOAP または HTTP リダイレクトを選択できます。このフィールドは、名前登録に SOAP または HTTP リダイレクトプロファイルを使用するかどうかを指定します。対象プロバイダの存続期間中であればいつでも変更できます。

4. 「保存」をクリックします。

5. 作成時にリモートプロバイダをアイデンティティプロバイダとして定義した場合、「表示」メニューの「アイデンティティプロバイダ」を選択して、フィールドを変更することができます。

「アイデンティティプロバイダ」：このフィールドは、リモートプロバイダをアイデンティティプロバイダとして定義するかどうかを指定します。デフォルトでは、すべてのプロバイダがサービスプロバイダとなります。「アイデンティティプロバイダ」オプションを選択すると、リモートプロバイダがアイデンティティプロバイダとしても定義されます。

「SSO 時の名前登録」：このオプションを有効にすると、アイデンティティプロバイダでは SSO 中に名前登録に参加できます。名前登録とは、サービスプロバイダが主体の名前識別子を指定するためのプロファイルです。名前識別子は、アイデンティティプロバイダがサービスプロバイダと通信する際に使用します。

「シングルサインオンサービス URL」：このフィールドは、連携と SSO の期間中にサービスプロバイダが要求を送信する、アイデンティティプロバイダの URL を定義します。このフィールドは、「アイデンティティプロバイダ」オプションが有効になっている場合のみ定義する必要があります。

6. 「表示」メニューの認証ドメインを選択し、リモートプロバイダを所属させる認証ドメインを編集します。

   矢印を使用して、選択した認証ドメインを「利用可能」リストに移動します。「保存」をクリックします。これによって、プロバイダが認証ドメインに割り当てられます。プロバイダは 1 つまたは複数の認証ドメインに属することができます。指定されたどの認証ドメインにも属さないプロバイダは、Liberty 通信を行うことができません。「保存」をクリックします。

ホストプロバイダの作成

ホストプロバイダとは、主体についてのアイデンティティを作成、維持、および管理し、認証ドメイン内のほかのサービスプロバイダに対して主体の認証を実行するエンティティのことです。ホストプロバイダを作成するには、次の手順に従ってください。

1. 連携管理モジュールの「表示」メニューから「ホストプロバイダ」を選択します。

   プロバイダを作成すると、デフォルトではサービスプロバイダとなります。手順 6 の説明にあるオプションを選択すれば、リモートプロバイダをアイデンティティプロバイダとして作成することもできます。

2. 「新規」をクリックします。「ホストプロバイダの作成」ウィンドウが表示されます。

3. 「プロバイダ ID」の値を入力します。

   「プロバイダ ID」は、プロバイダの URL 識別子を指定します。リモートプロバイダおよびホストプロバイダすべてに対して重複しない値にする必要があります。

4. ホストプロバイダの詳細を入力します。

5. プロバイダの「エイリアス」を入力します。

それぞれのホストプロバイダに対して、このフィールドに入力されたエイリアスが、メタエイリアスと呼ばれる文字列に追加されます。続いてこの文字列は、ホストプロバイダに対して自動生成された URL に追加されます。この URL はメタデータ URL と呼ばれます。次の例では、sunAlias はプロバイダのエイリアスです。

連携終了サービス URL

```
http://www.example.com:58080/amserver/ProcessTermination/metaAlias/sunAlias
```

SOAP エンドポイント URL

```
http://www.example.com:58080/amserver/SOAPReceiver/metaAlias/sunAlias
```

6. リモートプロバイダをアイデンティティプロバイダとして定義するかどうかを決定します。デフォルトでは、すべてのプロバイダがサービスプロバイダとなります。「アイデンティティプロバイダ」オプションを選択すると、リモートプロバイダがアイデンティティプロバイダとしても定義されます。

7. 「セキュリティキー」を入力します。

   「セキュリティキー」は、セキュリティ証明エイリアスを定義します。証明書はすべて、エイリアスに対する JKS キーストアに格納されています。このエイリアス (セキュリティキー) は、必要な証明書を取得するために使用します。

8. 「プロバイダ URL」を入力します。

   このフィールドは、メタデータを送信する URL を指定します。

9. ホストプロバイダをアイデンティティプロバイダとして定義するかどうかを決定します。デフォルトでは、すべてのプロバイダがサービスプロバイダとなります。「アイデンティティプロバイダ」オプションを選択すると、ホストプロバイダがアイデンティティプロバイダとしても定義されます。

10. 「作成」をクリックします。

    新しいプロバイダがナビゲーションフレームに表示されます。

ホストプロバイダの修正

1. 修正したいプロバイダのプロファイルを選択し、「編集」の矢印をクリックします。

   デフォルトでは、ナビゲーションフレームは「一般」表示となっています。「一般」表示内のほとんどのフィールドには、ホストプロバイダの作成時に入力されたデータが入っています。次の追加フィールドを修正できます。

   「SOAP エンドポイント URL」：このフィールドは、SOAP 要求の受信者の場所を指定します。SOAP 経由のバックチャネルの通信 (ブラウザを使用しない通信) に使用されます。

   「シングルログアウトサービス URL」：「シングルログアウトサービス URL」は、サービスプロバイダまたはアイデンティティプロバイダがログアウト要求を送受信するために使用されます。

   「シングルログアウトの返信 URL」：この値は、ログアウト要求処理後に要求がリダイレクトされる URL を指定します。

   「連携終了サービス URL」：このフィールドは、連携の終了要求をどの URL に通知するかを指定します。

   「連携終了の返信 URL」：この値は、連携の終了要求処理後に要求がリダイレクトされる URL を指定します。

   「名前登録サービス URL」：このフィールドは、サービスプロバイダがアイデンティティプロバイダと通信する間に、専用の名前識別子を登録するために用いる、名前登録プロトコルを使用します。連携セッションが確立した後でのみ、登録が行われます。このフィールドは、サービスプロバイダが名前識別子をアイデンティティプロバイダに登録するために使用するサービス URL を定義します。

   「名前登録の返信 URL」：このフィールドは、サービスプロバイダがアイデンティティプロバイダと通信する間に、専用の名前識別子を登録するために用いる、名前登録プロトコルを使用します。連携セッションが確立した後でのみ、登録が行われます。「名前登録の返信 URL」は、アイデンティティプロバイダが登録の状況を返信する URL です。

   フィールドを修正した場合、「保存」をクリックします。

2. 「サービスプロバイダ」フィールドを変更するには、「表示」メニューで「サービスプロバイダ」を選択します。

   「アサーションコンシューマ URL」フィールドには、リモートプロバイダの作成時に入力されたデータが入っています。次の追加フィールドを修正できます。

   「連携後の名前登録」：このオプションを有効にすると、サービスプロバイダでは連携後に名前登録に参加できます。名前登録とは、サービスプロバイダが主体の名前識別子を指定するためのプロファイルです。名前識別子は、アイデンティティプロバイダがサービスプロバイダと通信する際に使用します。

「署名済みの認証要求」：このオプションが有効になっている場合、署名済みの認証および連携の要求をホストプロバイダが送信するように指定します。アイデンティティプロバイダは、サービスプロバイダから署名のない要求を受け取っても処理しません。

「連携終了のプロファイル」：SOAP または HTTP リダイレクトを選択できます。このフィールドは、連携終了の通知に SOAP または HTTP リダイレクトプロファイルを使用するかどうかを指定します。対象プロバイダの存続期間中であればいつでも変更できます。

「シングルログアウトのプロファイル」：SOAP または HTTP リダイレクトを選択できます。このフィールドは、ログアウトイベントの通知に SOAP または HTTP リダイレクトを使用するかどうかを指定します。対象プロバイダの存続期間中であればいつでも変更できます。

「名前登録のプロファイル」：SOAP または HTTP リダイレクトを選択できます。このフィールドは、名前登録に SOAP または HTTP リダイレクトプロファイルを使用するかどうかを指定します。対象プロバイダの存続期間中であればいつでも変更できます。

「認証コンテキスト」：使用される認証コンテキストの認証レベルを指定します。

フィールドを修正した場合、「保存」をクリックします。

3. 作成時にホストプロバイダをアイデンティティプロバイダとして定義した場合、「表示」メニューの「アイデンティティプロバイダ」を選択して、フィールドを変更することができます。このフィールドの値のほとんどは、作成時に入力されたものです。次のフィールドを修正できます。

   「アイデンティティプロバイダ」：このフィールドは、リモートプロバイダをアイデンティティプロバイダとして定義するかどうかを指定します。デフォルトでは、すべてのプロバイダがサービスプロバイダとなります。「アイデンティティプロバイダ」オプションを選択すると、リモートプロバイダがアイデンティティプロバイダとしても定義されます。

   「SSO 時の名前登録」：このオプションを有効にすると、アイデンティティプロバイダでは SSO 中に名前登録に参加できます。名前登録とは、サービスプロバイダが主体の名前識別子を指定するためのプロファイルです。名前識別子は、アイデンティティプロバイダがサービスプロバイダと通信する際に使用します。

   「シングルサインオンサービス URL」：このフィールドは、連携と SSO の期間中にサービスプロバイダが要求を送信する、アイデンティティプロバイダの URL を定義します。このフィールドは、「アイデンティティプロバイダ」オプションが有効になっている場合のみ定義する必要があります。

   「サポート」：アイデンティティプロバイダがその認証コンテキストをサポートするかどうかを指定します。アイデンティティプロバイダは、少なくとも 1 つの認証コンテキストをサポートしている必要があります。

「コンテキスト参照」：認証コンテキストの名前を定義します。Liberty プロトコルには 10 個のコンテキストが定義されています。

「キー」：/UI/Login (Identity Server 認証サーブレット) に送信されたクエリ文字列には、使用される認証メカニズムを識別するキーと値のペアが含まれます。次の値が使用できます。

- モジュール
- レベル
- ロール
- サービス
- ユーザー

「値」：認証メカニズム用のキーと値のペアの値を定義します。

「優先順位」：アイデンティティプロバイダによって決定される、Liberty 定義の認証コンテキストの順番を示します。認証要求中にサービスプロバイダから要求される認証コンテキストをアイデンティティプロバイダがサポートしていない場合、アイデンティティプロバイダは同じ優先順位レベル以上のほかの認証コンテキストをどれでも使用できます。

「保存」をクリックして変更を保存します。

4. 「表示」メニューの認証ドメインを選択し、リモートプロバイダを所属させる認証ドメインを編集します。

   矢印を使用して、選択した認証ドメインを「利用可能」リストに移動します。「保存」をクリックします。これによって、プロバイダが認証ドメインに割り当てられます。プロバイダは 1 つまたは複数の認証ドメインに属することができます。指定されたどの認証ドメインにも属さないプロバイダは、Liberty 通信を行うことができません。

5. 「表示」メニューから「信頼プロバイダ」を選択します。

   リモートプロバイダは、ここで選択されたプロバイダからの要求だけを受け付けます。その他のプロバイダからの要求は無視されます。信頼できるプロバイダのリストを作成するには、「利用可能」フィールドでプロバイダを選択し、「追加」ボタンを使用して「選択」フィールドに追加します。プロバイダを削除するには「削除」ボタンを使用します。「保存」をクリックします。

6. Identity Server の設定属性を選択します。

   フィールドは次のとおりです。

   「認証タイプ」：リモートとローカルがあります。リモートでは、認証要求を受け取った場合に、ホストプロバイダが認証のためにアイデンティティプロバイダと通信する必要があるか指定します。また、ローカルでは、認証がホストプロバイダ自身によって行われる必要があるか指定します。

「シングルサインオン / 連携のプロファイル」: ホストプロバイダが認証要求送信のために使用するプロファイルを指定します。Identity Server では次のプロトコルが使用できます。

- ブラウザ POST - フロントチャネル (HTTP POST ベース) プロトコルを指定
- ブラウザアーティファクト - バックチャネル (ブラウザを使用しない) SOAP ベースのプロトコル

「デフォルト認証コンテキスト」: アイデンティティプロバイダがサービスプロバイダの要求の一部として認証コンテキストを受け取らないようになっている場合、使用する認証コンテキストを指定します。また、保護されたリソースに未知のユーザーがアクセスしようとした場合にサービスプロバイダが使用する、認証コンテキストも指定します。デフォルト値は次のとおりです。

- 以前のセッション
- 時間同期トークン
- スマートカード
- モバイル機器が未登録
- スマートカード PKI
- モバイル機器の契約
- パスワード
- パスワードで保護されたトランスポート
- モバイル機器のデジタル ID
- ソフトウェア PKI

「アイデンティティプロバイダでの強制認証」: 認証要求を受信した場合に、アイデンティティプロバイダが (セッション継続中でも) 再認証する必要があるかどうかを示します。

「アイデンティティプロバイダをパッシブにするように要求」: 選択された場合、アイデンティティプロバイダが主体ではなくユーザーとやりとりする必要があることを指定します。

「組織 DN」: 各ホストプロバイダが、ホスティングされたモデルまで別々の組織にわたってユーザーを管理する場合、組織の DN の格納場所を指定します。

「Liberty バージョン URI」: Liberty 仕様のバージョンを指定します。

「名前 ID の実装」：サービスプロバイダが名前登録を行えるようにします。名前登録とは、サービスプロバイダが主体の名前識別子を指定するためのプロファイルです。名前識別子は、アイデンティティプロバイダがサービスプロバイダと通信する際に使用します。

「プロバイダホームページ URL」：プロバイダのホームページを指定します。

「シングルサインオンエラー時のリダイレクト URL」：SSO がエラーになった場合のリダイレクト URL を指定します。

「アサーション間隔」：アイデンティティプロバイダが発行するアサーションの間隔の有効期限を指定します。アサーションが期限切れになるまで、主体の認証はアイデンティティプロバイダによって維持されます。

「クリーンアップ間隔」：アイデンティティプロバイダに格納されているアサーションをクリアする時間間隔を指定します。

「アーティファクトのタイムアウト」：アサーションアーティファクトに対するアイデンティティプロバイダのタイムアウト時間を指定します。

「アサーション限界」：アイデンティティプロバイダが発行または格納できるアサーション数を指定します。

7. 「保存」をクリックします。

プロバイダの削除

1. 連携管理で、「表示」メニューから「プロバイダ」を選択します。

   作成済みのプロバイダがすべてナビゲーションフレームに表示されます。

2. 削除したいプロバイダのチェックボックスを選択します。
3. 選択した項目の「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。

第 6 章

ポリシー管理

この章では、Sun™ ONE Identity Server のポリシーサービスの管理機能について説明します。ポリシー管理では、すべての Identity Server ポリシーを表示、管理、および設定する方法を提供します。

この章は、次の節で構成されています。

ポリシータイプ

Identity Server を使用して設定可能なポリシーには、標準ポリシーと、参照ポリシーの 2 タイプがあります。標準ポリシーは、複数のルール、サブジェクト、および条件から構成されます。参照ポリシーは、複数のルール、および組織への参照から構成されます。

標準ポリシー

Identity Server では、アクセス許可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、複数のルール、サブジェクト、および条件から構成されます。

ルールは、1 つのリソースと、1 つ以上のアクションと値の組で構成されます。リソースは保護しているオブジェクトを定義します。またアクションは、リソースで実行している操作の名前、値はアクセス権を定義します。

注　リソースなしでアクションを定義することも可能です。

ポリシーはアイデンティティに割り当てられていません。その代わりに、サブジェクトがポリシーに割り当てられています。サブジェクトとは、ポリシーが割り当てられ、適用されているアイデンティティオブジェクトのことです。

条件は、ポリシーが適用可能な状況を定義します。たとえばポリシーで午前 7 時～ 10 時という時間条件は、そのポリシーが午前 7 時～ 10 時までの間で適用可能であることを意味します。

注　参照、ルール、リソース、サブジェクト、条件、アクション、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。詳細については、『Sun ONE Identity Server Customization and API Guide』で説明しています。

参照ポリシー

管理者は、通常、ある組織のポリシーの定義や判断を、別の組織に委任します。または、あるリソースに対するポリシーの判断を、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。参照は、ポリシーの定義と評価をどの組織に対して参照するかを定義します。

注　参照先の組織では、その組織をすでに参照済みのリソース (またはサブリソース) のポリシーを定義または評価できます。ただし、この制約はルート組織には適用されません。

Identity Server に付属する参照には、ピア組織とサブ組織の 2 タイプがあります。それぞれ、同じレベルの組織、下位レベルの組織を表します。詳細は、91 ページの「ピア組織およびサブ組織のポリシーの作成」を参照してください。

ポリシー管理

ポリシーの作成、削除、修正には、ポリシー API を使う方法、amadmin コマンド行ツールを使う方法、そして Identity Server コンソールを使う方法があります。

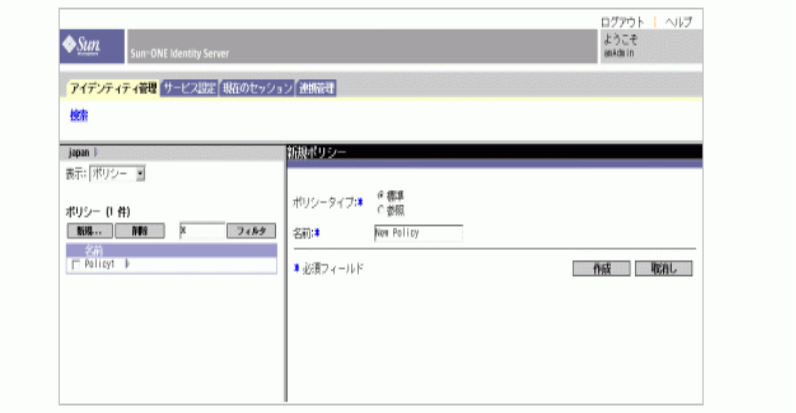
この章では、コンソールを使用したポリシーの作成について説明します。amadmin の詳細については、133 ページの「amadmin コマンド行ツール」を参照してください。ポリシー API の詳細については、『Sun ONE Identity Server Customization and API Guide』の「ポリシーサービス」の章を参照してください。

ポリシーはアイデンティティ管理インタフェースを使用して設定します。このインタフェースを使用すると、次の作業ができます。

- 最上位管理者が、すべての組織で使用できる特定のサービスに対するポリシーを表示、作成、削除、修正する
- 組織管理者またはサブ組織管理者が、その組織で特定の目的に使用するポリシーを表示、作成、削除、修正する

一般に、ポリシーは組織ツリー全体で使用するために、組織またはサブ組織レベルで作成します。

図 6-1　ポリシーの表示



ポリシー設定サービスの登録

ポリシー設定サービスの登録はサービスのタイプの登録と同じで、アイデンティティ管理インタフェース内で行います。デフォルトでは、ポリシー設定サービスは自動的に最上位の組織に登録されます。作成するポリシーサービスは、すべての組織に登録する必要があります。ポリシー設定サービスを登録するときは常に、組織で適用されるすべてのポリシーのテンプレートに、LDAP バインドパスワードを入力する必要があります。

1. アイデンティティ管理インタフェースに移動します。

   コンソールが開くときのデフォルトのインタフェースはアイデンティティ管理です。

2. ポリシーを作成する組織を選択します。

   最上位レベル管理者としてログインした場合は、アイデンティティ管理モジュールがすべての設定済み組織が表示される最上位レベルの組織であることを確認します。デフォルトの最上位レベル組織は、インストール時に定義されます。

3. 「表示」メニューから「サービス」を選択します。

   その組織にすでにサービスが登録されている場合は、ナビゲーションフレームにそのサービスが表示されます。

4. ナビゲーションフレームで「登録」をクリックします。

   この組織にまだ登録されていないサービスのリストが、データフレームに表示されます。

5. データフレームで開かれた「サービスを登録」ウィンドウから、「ポリシー設定」を選択して「登録」をクリックします。

   ポリシー設定サービスがナビゲーションフレームのサービス一覧に追加されます。

6. 「プロパティ」の矢印をクリックして、ポリシーサービスを設定します。ポリシーテンプレートが設定されていない場合、新しく登録されたポリシーサービス用にサービステンプレートを作成する必要があります。

   ポリシーサービスを設定するには、「作成」をクリックします。ポリシー設定属性を修正します。これらの属性については、267 ページの「ポリシー設定サービス属性」を参照してください。「保存」をクリックします。

   これで、選択した組織にポリシー設定サービスが登録されます。

注 サブ組織は、その親組織とは別にポリシーサービスを登録する必要があります。それは、サブ組織 `o=suborg,dc=sun,dc=com` は親の `dc=sun,dc=com` からポリシー設定サービスを継承しないためです。

ポリシーの作成

ポリシーはアイデンティティ管理インタフェースを使用して作成します。

1. アイデンティティ管理インタフェースに移動します。
2. ポリシーを作成する組織を選択します。

   組織のポリシー管理ウィンドウの位置が正しいことを確認します。
3. 「表示」メニューから「ポリシー」を選択します。

   デフォルトでは、組織は「表示」メニューに表示されます。サブ組織がある場合は、すべてその下に表示されます。サブ組織のポリシーを作成する場合は、サブ組織を選択して、「表示」メニューから「ポリシー」を選択します。
4. ナビゲーションフレームで「新規」をクリックします。「ポリシーの作成」ウィンドウを開きます。
5. 作成するポリシーのタイプを、標準ポリシーまたは参照ポリシーのどちらかから選択します。

   サブ組織を参照する参照ポリシーが存在しない場合、そのサブ組織のポリシーを作成することはできません。詳細は、91 ページの「ピア組織およびサブ組織のポリシーの作成」を参照してください。

   この時点では、標準また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。ポリシー作成後、ルール、サブジェクト、参照などを追加できます。標準ポリシーや参照ポリシーの設定の詳細については、84 ページの「ポリシーの修正」を参照してください。
6. ポリシーの名前を入力して、「作成」をクリックします。

   作成したポリシー名の下に、新しいポリシールールのウィンドウが開きます。
7. デフォルトでは、「一般」表示となっています。

   「一般」にはポリシー名が表示され、作成するポリシーの説明を入力できます。
8. 「保存」をクリックして、ポリシーの設定を完了します。

ポリシーの修正

標準または参照ポリシーの作成後、ルール、サブジェクト、条件、および参照を変更できます。

1. アイデンティティ管理インタフェースで、「表示」メニューから「ポリシー」を選択します。

   その組織用に作成されたポリシーが表示されます。

2. 修正したいポリシーを選択し、「プロパティ」の矢印をクリックします。データフレームでポリシーの「編集」ウィンドウが開きます。

   デフォルトでは、「一般」表示となっています。

標準ポリシーの修正

アイデンティティ管理インタフェースでは、アクセス許可を定義するポリシーを作成できます。このようなポリシーを標準ポリシーと呼びます。標準ポリシーは、複数のルール、サブジェクト、および条件から構成できます。ここでは、標準ポリシー作成時に指定できるデフォルトのフィールドについて説明します。

ルールの追加

ルールは、ポリシーのリソース、アクション、およびアクション値を定義します。

1. アイデンティティ管理インタフェースで、「表示」メニューから「ポリシー」を選択します。

   その組織用に作成されたポリシーが表示されます。

2. 修正したいポリシーを選択し、「プロパティ」の矢印をクリックします。データフレームでポリシーの「編集」ウィンドウが開きます。

   デフォルトでは、「一般」表示となっています。

3. ポリシーのルールを定義するには、「表示」メニューから「ルール」を選択し「追加」をクリックします。

   複数のポリシーサービスが存在する場合は、データフレームに一覧表示されます。ポリシーを作成したいサービスを選択して、「次へ」をクリックします。「ルールの追加」ウィンドウが表示されます。

4. 「ルール」フィールドに、ポリシーのリソース、アクション、およびアクション値を定義します。

   フィールドは次のとおりです。

   「サービス」：ポリシーを作成するサービスが表示されます。デフォルトは URL ポリシーエージェントです。

   「ルール名」：ルール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。次に例を示します。

```
http://www.sunone.com
```

現在のところ、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。

「選択、アクション」: URL ポリシーエージェントサービスでは、デフォルトとして次のアクションの両方または一方を選択できます。

- `GET`
- `POST`

「値」: URL ポリシーエージェントサービスでは、次のアクション値の 1 つを選択できます。

- 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

ポリシーでは、拒否ルールが許可ルールよりも優先されます。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。通常は、ポリシー定義プロセスでは許可ルールだけを使用し、拒否の場合を実現するのに適用するポリシーがない場合にデフォルトの拒否を使用してください。

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、異なるサブジェクト (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は、ポリシーの判断によってアクセスを拒否されます。

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。詳細は、87 ページの「条件の追加」を参照してください。

注 アクションにリソース定義が不要となるようサービスが定義されている場合、リソースフィールドは表示されません。リソースを要求するアクションと要求しないアクションの両方がサービスに含まれている場合、選択肢が表示され、リソースを要求しないアクションを伴うルールまたはリソースを要求するアクションを伴うルールのどちらかを選択できます。

5. 「作成」をクリックしてルールを保存します。
6. 手順 1 から 5 を繰り返して、追加のルールを作成します。
7. ポリシーに対して作成されたすべてのルールが、「ルール」の表に表示されます。「保存」をクリックしてポリシーにルールを追加します。

   ポリシーからルールを削除するには、ルールを選択して「削除」をクリックします。

   ルール名の横にある「編集」リンクをクリックすれば、ルールの定義を編集できます。

サブジェクトの追加

サブジェクトは、ポリシーを適用するサブジェクトを定義します。

1. ポリシーのサブジェクトを定義するには、「表示」メニューから「サブジェクト」を選択し「追加」をクリックします。
2. デフォルトのサブジェクトタイプを次の中から選択します。
   - Identity Server ロール
   - LDAP グループ
   - LDAP ロール
   - LDAP ユーザー
   - 組織

   「次へ」をクリックして先に進みます。
3. サブジェクトの名前を入力します。
4. 「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、サブジェクトのメンバーであるアイデンティティに適用されます。このフィールドが選択されていると、ポリシーは、サブジェクトのメンバーではないアイデンティティに適用されます。

ポリシーに複数のサブジェクトが存在するときは、指定されたアイデンティティにポリシーが適用されていることが少なくとも 1 つのサブジェクトで示されている場合に、そのポリシーがアイデンティティに適用されます。「排他的」フィールドが選択されているかどうかにかかわらず、ポリシーに定義された条件がすべて満たされている場合は、そのポリシーがアイデンティティに適用されます。

5. 検索を実行して、サブジェクトに追加するアイデンティティを表示します。

   デフォルト (*) の検索パターンでは、該当するすべてのエントリが表示されます。

6. サブジェクトに追加するアイデンティティを選択し、「追加」をクリックして「選択」リストボックスに移動します。または「すべて追加」を選択して、すべてのアイデンティティを追加します。

7. 「作成」をクリックします。

8. サブジェクトの名前、タイプ、および排他の状況が、「サブジェクト」の表に表示されます。「保存」をクリックします。

   ポリシーからサブジェクトを削除するには、サブジェクトを選択して「削除」をクリックし、「保存」をクリックします。

   サブジェクト名の横にある「編集」リンクをクリックすれば、サブジェクトの定義を編集できます。

条件の追加

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、補助的に使用されます。たとえば、`http://org.example.com/hr/*jsp` は `org.example.net` で午前 9 時～午後 5 時だけアクセスできますが、`http://org.example.com/finance/*.jsp` は `org.example2.net` で午前 5 時～午後 11 時にアクセスできます。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。

標準ポリシーに条件を追加するには、次の手順に従ってください。

1. ポリシーの条件を定義します。「表示」メニューから「条件」を選択します。「追加」をクリックして新しい条件を追加するか、または「編集」リンクをクリックして既存の条件を編集します。
2. デフォルトの条件を次の中から選択します。
   - 認証レベル
   - 認証方式
   - IP アドレス
   - セッション
   - 時間

   「次へ」をクリックします。
3. 「ルール」フィールドに、所定の条件の値を定義します。フィールドは次のとおりです。

   「名前」: 条件の名前を入力します。

   認証レベル

   「認証レベル」: 認証の信頼レベルを指定します。利用可能な認証レベルの一覧は、認証レベルと認証モジュールの表に表示されます。

   認証方式

   「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、組織認証モジュールのコア認証サービステンプレートから取得されます。

   IP アドレス

   「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。

   時間

   「日付 開始 / 終了」: 日付の範囲を指定します。

   「時間」: 1 日での時間の範囲を指定します。

   「日」: 日数を指定します。

   「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)。

   セッション

   「最大セッション時間」: 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の終了が設定されます。

4. 条件を定義したら、「作成」をクリックします。
5. ポリシーに対して作成されたすべての条件が、「条件」の表に表示されます。「保存」をクリックします。

   ポリシーから条件を削除するには、条件を選択して「削除」をクリックします。

   条件名の横にある「編集」リンクをクリックすれば、条件の定義を編集できます。

参照ポリシーの修正

アイデンティティ管理インタフェースでは、ある組織のポリシーの定義や判断を、別の組織に委任できます。また、あるリソースに対するポリシーの判断を、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。参照ポリシーは、ルールおよび参照自体から構成されます。リソースを要求しないアクションがポリシーサービスに含まれている場合、サブ組織に対して参照ポリシーを作成することはできません。

ルールの追加

ルールは、ポリシーのリソースを定義します。

1. ポリシーのルールを定義するには、「表示」メニューから「ルール」を選択します。「追加」をクリックして新しいルールを追加するか、または「編集」リンクをクリックして既存のルールを編集します。
2. 「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。

   「サービス」：ポリシーを作成するポリシーサービスが表示されます。

   「名前」：ルール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。次に例を示します。

   ```
   http://www.sunone.com
   ```

   現在のところ、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。

   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。
3. 「作成」をクリックしてルールを保存します。
4. 手順 1 から 3 を繰り返して、追加のルールを作成します。

5. ポリシーに対して作成されたすべてのルールが、「ルール」の表に表示されます。「保存」をクリックします。

   ポリシーからルールを削除するには、ルールを選択して「削除」をクリックします。

   ルール名の横にある「編集」リンクをクリックすれば、ルールの定義を編集できます。

参照の追加

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。ピア組織とサブ組織です。それぞれ、同じレベルの組織、下位レベルの組織を表します。

1. ポリシーの参照を定義するには、「表示」メニューから「参照」を選択します。「追加」をクリックして新しい参照を追加するか、または「編集」リンクをクリックして既存の参照を編集します。
2. 「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」: 現在の参照を表示します。

   「名前」: 参照の名前を入力します。

   「含む」: 「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」: 参照の組織名を入力します。
3. 「作成」をクリックし、「保存」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。

ピア組織およびサブ組織のポリシーの作成

ピア組織またはサブ組織のポリシーを作成するには、まず親組織または別のピア組織で参照ポリシーを作成する必要があります。サブ組織でポリシー設定サービスを登録し、テンプレートを作成することも必要です。参照ポリシーのルールの定義には、サブ組織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。親組織または別のピア組織で参照ポリシーを作成すれば、サブ組織またはピア組織で標準ポリシーを作成できます。

Identity Server ポリシーフレームワークでは、アクション名にリソース名が含まれない場合は、参照ポリシーの作成を許可していません。つまり、アクションにリソース名が含まれていない場合、ポリシーはルート組織の下にのみ作成できます。サブ組織の下には作成できません。

この例では、o=isp が親組織、o=sun.com はサブ組織で http://www.example.com のリソースおよびサブリソースを管理しています。このサブ組織のポリシーを作成するには、次の手順に従ってください。

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、89 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.sun.com をリソースとしてルールに定義し、参照内で sun.com を SubOrgReferral の値として持つ必要があります。

2. 「組織」表示で sun.com というサブ組織に移動します。

3. ポリシー設定サービスが sun.com というサブ組織レベルに登録されていることを確認します。詳細は、82 ページの「ポリシー設定サービスの登録」を参照してください。

4. これでリソースが isp によって sun.com に参照されるようになったので、http://www.sun.com というリソース、または http://www.sun.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。

   標準ポリシーの作成については、84 ページの「標準ポリシーの修正」の手順を参照してください。

   sun.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。

第 7 章

認証オプション

Sun™ ONE Identity Server では、認証のフレームワークを備えています。認証とは、エンタープライズ内のアプリケーションにアクセスするユーザーのアイデンティティを確認するためのプロセスです。ユーザーは、Identity Server コンソールまたは Identity Server で保護されたリソースにアクセスする前に、認証プロセスにパスする必要があります。認証は、ユーザーのアイデンティティを検証するプラグインによって実装されます。このプラグインアーキテクチャの詳細については、『Sun ONE Identity Server Customization and API Guide』で説明します。

Identity Server コンソールは、デフォルト値の設定、認証サービスの登録、認証テンプレートの作成、およびサービスの有効化のために使用されます。この章では、認証サービスの概要と登録手順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。

コア認証

Identity Server では、デフォルトで 10 種類の認証サービスと、コア認証サービスを提供しています。コア認証サービスでは、認証サービスに対する全体的な設定を行います。匿名、証明書に基づく、HTTP 基本、LDAP、メンバーシップ、NT、RADIUS、SafeWord、SecurID、および UNIX 認証を登録し、有効にする前に、コア認証サービスを登録し、有効にする必要があります。第 19 章「コア認証属性」に、コア属性の詳細な一覧を示します。

コアサービスを登録し、有効にする

1. コアサービスを登録する組織のナビゲーションフレームに移動します。
2. 「表示」メニューから「サービス」を選択します。
3. ナビゲーションフレームで「登録」をクリックします。

   利用可能なサービスの一覧がデータフレームに表示されます。
4. 「認証」「コア」のチェックボックスを選択し、「追加」をクリックします。

   コア認証サービスがナビゲーションフレームに表示され、登録されたことが管理者に示されます。
5. 「認証」「コア」の矢印をクリックします。

   「現在このサービスにはテンプレートが存在しません。新規に作成しますか ?」というメッセージがデータフレームに表示されます。
6. 「作成」をクリックします。

   コア属性がデータフレームに表示されます。必要に応じて属性を修正します。コア属性の説明については、第 19 章「コア認証属性」を参照するか、またはコンソール右上の「ヘルプ」リンクをクリックしてください。

匿名認証

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 *anonymous* ユーザーとして Identity Server にログインできるようになります。有効な匿名ユーザーリスト属性 (187 ページ参照) を設定して、このモジュールに匿名ユーザーの一覧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。

匿名認証を登録し、有効にする

組織管理者または最上位管理者として、Identity Server にログインする必要があります。

1. 匿名認証を登録する組織のナビゲーションフレームに移動します。
2. 「表示」メニューから「サービス」を選択します。

   コアサービスが登録済みの場合は、ナビゲーションフレームに表示されます。登録済みでない場合は、匿名認証サービスとともに登録されます。
3. ナビゲーションフレームで「追加」をクリックします。

   利用可能なサービスの一覧がデータフレームに表示されます。
4. 「匿名認証」のチェックボックスを選択し、「追加」をクリックします。

   匿名認証サービスがナビゲーションフレームに表示され、登録されたことが管理者に示されます。
5. 「認証」「匿名」の矢印をクリックします。

   「現在このサービスにはテンプレートが存在しません。新規に作成しますか ?」というメッセージがデータフレームに表示されます。
6. 「作成」をクリックします。

   匿名認証属性がデータフレームに表示されます。必要に応じて属性を修正します。これらの属性の説明については、第 17 章「匿名認証属性」を参照するか、またはコンソール右上の「ヘルプ」リンクをクリックしてください。
7. 「保存」をクリックします。

   匿名認証サービスが有効になります。

匿名認証を使用してログインする

匿名認証を使用してログインするには、198 ページの「組織認証モジュール」というコア認証サービス属性で、匿名認証を定義するように修正する必要があります。そうすると、ユーザーが `http(s)://` ホスト名 : ポート / 配備 *URI*`/Login?module=Anonymous&org=` 組織名を使用してログインするときに、匿名認証のログインウィンドウが表示されます。匿名認証のログインウィンドウを表示せずにログインするには、次の構文を使用します。

`http(s)://` ホスト名 : ポート / 配備 *URI*`/Login?module=Anonymous&org=` 組織名 `&IDTolken1=user_id`

使用している認証タイプ (サービス、ロール、ユーザー、組織など) によっては、認証モジュールをデフォルトとして設定する場合に、URL でモジュール名を指定する必要がありません。

注　匿名認証サービスのデフォルトの匿名ユーザー名属性値は `anonymous` です。ユーザーがログインするときは、この名前が使用されます。デフォルトの匿名ユーザーを組織内に作成する必要があります。そのユーザー ID は、匿名認証属性で指定されているユーザー名と同一にする必要があります。

証明書に基づく認証

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、また証明書の取り消しリスト (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サービスを組織に登録する前に、行う必要のある作業があります。まず、Identity Server 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。証明書に基づくサービスを有効にする前に、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
```

注	証明書に基づくサービス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。

証明書に基づく認証を登録し、有効にする

組織管理者として、Identity Server にログインする必要があります。

1. 証明書に基づく認証を登録する組織のナビゲーションフレームに移動します。
2. 「表示」メニューから「サービス」を選択します。

   コアサービスが登録済みの場合は、ナビゲーションフレームに表示されます。登録済みでない場合は、証明書に基づく認証サービスとともに登録されます。
3. ナビゲーションフレームで「追加」をクリックします。

   利用可能なサービスの一覧がデータフレームに表示されます。
4. 「証明書」のチェックボックスを選択し、「追加」をクリックします。

   証明書に基づく認証サービスがナビゲーションフレームに表示され、登録されたことが管理者に示されます。
5. 「認証」「証明書」の矢印をクリックします。

   「現在このサービスにはテンプレートが存在しません。新規に作成しますか?」というメッセージがデータフレームに表示されます。
6. 「作成」をクリックします。

   証明書に基づく認証属性がデータフレームに表示されます。必要に応じて属性を修正します。これらの属性の説明については、第 18 章「証明書認証属性」を参照するか、またはコンソール右上の「ヘルプ」リンクをクリックしてください。
7. 「保存」をクリックします。

証明書に基づく認証のプラットフォームサーバーリストを追加する

組織管理者として Identity Server にログインする必要があります。

1. サービス設定モジュールを選択します。
2. 利用可能なサービスの一覧から、「プラットフォーム」サービスを選択します。
3. サーバーリスト属性にサーバー情報を追加します。追加のサーバー属性についての詳細は、第 34 章「プラットフォームサービス属性」を参照してください。

証明書に基づく認証を使用してログインする

証明書に基づく認証をデフォルトの認証方法として設定するには、コア認証サービス属性である組織認証モジュール (198 ページ参照) を修正する必要があります。そうすると、ユーザーが `https://` ホスト名 : ポート / 配備 *URI*`/UI/Login?module=Cert` を使用してログインするときに、証明書に基づく認証のログインウィンドウが表示されます。使用している認証タイプ (ロール、ユーザー、組織など) によっては、認証モジュールをデフォルトとして設定する場合に、URL でモジュール名を指定する必要がありません。

HTTP 基本認証

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。Identity Server ではユーザー名とパスワードを受信し、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 認証モジュールを登録する必要があります (HTTP 基本モジュールを単独で登録しても機能しません)。詳細は、100 ページの「LDAP 認証を登録し、有効にする」を参照してください。いったん認証に成功したユーザーには、以降の認証でユーザー名とパスワードの入力は要求されません。

HTTP 基本認証を登録し、有効にする

組織管理者または最上位管理者として、Identity Server にログインする必要があります。

1. HTTP 基本認証を登録する組織のナビゲーションフレームに移動します。
2. 「表示」メニューから「サービス」を選択します。

   コアサービスが登録済みの場合は、ナビゲーションフレームに表示されます。登録済みでない場合は、HTTP 基本認証サービスとともに登録されます。
3. ナビゲーションフレームで「追加」をクリックします。

   利用可能なサービスの一覧がデータフレームに表示されます。
4. 「HTTP 基本」のチェックボックスを選択し、「追加」をクリックします。

   HTTP 基本認証サービスがナビゲーションフレームに表示され、登録されたことが管理者に示されます。
5. 「認証」「HTTP 基本」の矢印をクリックします。

   「現在このサービスにはテンプレートが存在しません。新規に作成しますか?」というメッセージがデータフレームに表示されます。
6. 「作成」をクリックします。

   HTTP 基本認証属性がデータフレームに表示されます。必要に応じて属性を修正します。これらの属性の説明については、第 20 章「HTTP 基本認証属性」を参照するか、またはコンソール右上の「ヘルプ」リンクをクリックしてください。
7. 「保存」をクリックします。

   HTTP 基本認証サービスが有効になります。

HTTP 基本認証を使用してログインする

LDAP 認証を使用してログインするには、コア認証サービス属性である 198 ページの「組織認証モジュール」で、HTTP 基本認証を定義するように修正する必要があります。そうすると、ユーザーが `http://` ホスト名 : ポート / 配備 *URI*`/UI/Login?module=HTTPBasic` を使用してログインするときに、HTTP 基本認証のログインウィンドウが表示されます。使用している認証タイプ (サービス、ロール、ユーザー、組織など) によっては、認証モジュールをデフォルトとして設定する場合に、URL でモジュール名を指定する必要がありません。認証に失敗した場合、ユーザーは新しいインスタンスを開いてログインし直す必要があります。

LDAP ディレクトリ認証

LDAP 認証サービスを使用すると、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。すべての組織ベースの認証では、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 Identity Server 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。LDAP 認証は、Identity Server のインストール時にデフォルトで有効になっています。このサービスが無効である場合の手順を次に示します。

LDAP 認証を登録し、有効にする

組織管理者または最上位管理者として、Identity Server にログインする必要があります。

1. LDAP 認証を登録する組織のナビゲーションフレームに移動します。
2. 「表示」メニューから「サービス」を選択します。

   コアサービスが登録済みの場合は、ナビゲーションフレームに表示されます。登録済みでない場合は、LDAP 認証サービスとともに登録されます。
3. ナビゲーションフレームで「追加」をクリックします。

   利用可能なサービスの一覧がデータフレームに表示されます。
4. 「LDAP 認証」のチェックボックスを選択し、「追加」をクリックします。

   LDAP 認証サービスがナビゲーションフレームに表示され、登録されたことが管理者に示されます。
5. 「認証」「LDAP」の矢印をクリックします。

   「現在このサービスにはテンプレートが存在しません。新規に作成しますか ?」というメッセージがデータフレームに表示されます。
6. 「作成」をクリックします。

   LDAP 認証属性がデータフレームに表示されます。必要に応じて属性を修正します。これらの属性の説明については、第 21 章「LDAP 認証属性」を参照するか、またはコンソール右上の「ヘルプ」リンクをクリックしてください。
7. パスワードを「root ユーザーバインドパスワード」に入力します。デフォルトで、インストール中に入力した `amldapuser` パスワードが、バインドユーザーとして使用されます。

   別のバインドユーザーを使用するには、「root ユーザーバインド DN」でユーザーの DN を変更し、そのユーザーのパスワードを「root ユーザーバインドパスワード」に入力します。

8. 「保存」をクリックします。

   LDAP 認証サービスが有効になります。

LDAP 認証を使用してログインする

LDAP 認証を使用してログインするには、コア認証サービス属性である 198 ページの「組織認証モジュール」で、LDAP 認証を定義するように修正する必要があります。そうすると、ユーザーが `http://` ホスト名 : ポート / 配備 *`URI`*`/UI/Login?module=LDAP` を使用してログインするときに、LDAP 認証のログインウィンドウが表示されます。使用している認証タイプ (サービス、ロール、ユーザー、組織など) によっては、認証モジュールをデフォルトとして設定する場合に、URL でモジュール名を指定する必要がありません。

LDAP 認証のフェイルオーバーを有効にする

LDAP 認証属性には、プライマリとセカンダリ両方の Directory Server の値フィールドがあります。プライマリサーバーが利用できなくなると、Identity Server では、認証を行うために、セカンダリサーバーを使用します。詳細は、210 ページの「プライマリ LDAP サーバーとポート」および 210 ページの「セカンダリ LDAP サーバーとポート」の LDAP 属性を参照してください。

複数の LDAP 設定

フェイルオーバーの形式として、あるいは、Identity Server 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 つの組織に複数の LDAP 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。複数の LDAP 設定については、『Sun ONE Identity Server Customization and API Guide』の「Multi LDAP Configuration」を参照してください。

メンバーシップ認証

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。サービスが有効なときに、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、登録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。

メンバーシップ認証を登録し、有効にする

組織管理者または最上位管理者として、Identity Server にログインする必要があります。

1. メンバーシップ認証を登録する組織のナビゲーションフレームに移動します。
2. 「表示」メニューから「サービス」を選択します。

   コアサービスが登録済みの場合は、ナビゲーションフレームに表示されます。登録済みでない場合は、メンバーシップ認証サービスとともに登録されます。
3. ナビゲーションフレームで「追加」をクリックします。

   利用可能なサービスの一覧がデータフレームに表示されます。
4. 「メンバーシップ認証」のチェックボックスを選択し、「追加」をクリックします。

   メンバーシップ認証サービスがナビゲーションフレームに表示され、登録されたことが管理者に示されます。
5. 「認証」「メンバーシップ」の矢印をクリックします。

   「現在このサービスにはテンプレートが存在しません。新規に作成しますか ?」というメッセージがデータフレームに表示されます。
6. 「作成」をクリックします。

   メンバーシップ認証属性がデータフレームに表示されます。必要に応じて属性を修正します。これらの属性の説明については、第 22 章「メンバーシップ認証属性」を参照するか、またはコンソール右上の「ヘルプ」リンクを選択してください。
7. パスワードを「root ユーザーバインドパスワード」に入力します。デフォルトで、インストール中に入力した amldapuser パスワードが、バインドユーザーとして使用されます。

別のバインドユーザーを使用するには、「root ユーザーバインド DN」でユーザーの DN を変更し、そのユーザーのパスワードを「root ユーザーバインドパスワード」に入力します。

8. 「保存」をクリックします。

   メンバーシップ認証サービスが有効になります。

メンバーシップ認証を使用してログインする

メンバーシップ認証を使用してログインするには、コア認証サービス属性である 198 ページの「組織認証モジュール」で、メンバーシップ認証を定義するように修正する必要があります。そうすると、ユーザーが `http://` ホスト名 : ポート / 配備 *`URI`*`/UI/Login?module=Membership` を使用してログインするときに (大文字と小文字の区別に注意)、メンバーシップ認証のログインウィンドウが表示されます。使用している認証タイプ (サービス、ロール、ユーザー、組織など) によっては、認証モジュールをデフォルトとして設定する場合に、URL でモジュール名を指定する必要がありません。

NT 認証

Identity Server は、すでにインストールされている NT または Windows 2000 サーバーで使用できるように設定できます。Identity Server では、NT 認証のクライアント部分を担当します。NT 認証サービスは、Solaris プラットフォームでのみサポートされています。

1. NT サーバーを設定します。

   詳しい手順については、NT サーバーのマニュアルを参照してください。

2. NT 認証サービスを登録し、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 Identity Server と通信できるようにする必要があります。詳細は、221 ページの「NT 認証属性」を参照してください。

3. NT 認証サービスを登録し、有効にします。

NT 認証を登録し、有効にする

組織管理者または最上位管理者として、Identity Server にログインする必要があります。

1. NT 認証を登録する組織のナビゲーションフレームに移動します。
2. 「表示」メニューから「サービス」を選択します。

   コアサービスが登録済みの場合は、ナビゲーションフレームに表示されます。登録済みでない場合は、NT 認証サービスとともに登録されます。
3. ナビゲーションフレームで「追加」をクリックします。

   利用可能なサービスの一覧がデータフレームに表示されます。
4. 「NT 認証」のチェックボックスを選択し、「追加」をクリックします。

   NT 認証サービスがナビゲーションフレームに表示され、登録されたことが管理者に示されます。
5. 「認証」「NT」の矢印をクリックします。

   「現在このサービスにはテンプレートが存在しません。新規に作成しますか ?」というメッセージがデータフレームに表示されます。
6. 「作成」をクリックします。

   NT 認証属性がデータフレームに表示されます。必要に応じて属性を修正します。これらの属性の説明については、第 23 章「NT 認証属性」を参照するか、またはコンソール右上の「ヘルプ」リンクをクリックしてください。
7. 「保存」をクリックします。

   NT 認証サービスが有効になります。

NT 認証を使用してログインする

NT 認証を使用してログインするには、コア認証サービス属性である 198 ページの「組織認証モジュール」で、NT 認証を定義するように修正する必要があります。そうすると、ユーザーが `http://` ホスト名 : ポート / 配備 *`URI`*`/UI/Login?module=NT` を使用してログインするときに、NT 認証のログインウィンドウが表示されます。使用している認証タイプ (サービス、ロール、ユーザー、組織など) によっては、認証モジュールをデフォルトとして設定する場合に、URL でモジュール名を指定する必要がありません。

RADIUS サーバー認証

Identity Server は、すでにインストールされている RADIUS サーバーで使用でき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レガシーの RADIUS サーバーを使用している場合に便利です。RADIUS 認証サービスを有効にするには、次の 2 つのプロセスを行います。

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 認証サービスを登録し、有効にします。

RADIUS 認証を登録し、有効にする

組織管理者として、Identity Server にログインする必要があります。

1. RADIUS 認証を登録する組織のナビゲーションフレームに移動します。
2. 「表示」メニューから「サービス」を選択します。

   コアサービスが登録済みの場合は、ナビゲーションフレームに表示されます。登録済みでない場合は、RADIUS 認証サービスとともに登録されます。

3. ナビゲーションフレームで「追加」をクリックします。

   利用可能なサービスの一覧がデータフレームに表示されます。

4. 「RADIUS 認証」のチェックボックスを選択し、「追加」をクリックします。

   RADIUS 認証サービスがナビゲーションフレームに表示され、登録されたことが管理者に示されます。

5. 「認証」「RADIUS」の矢印をクリックします。

   「現在このサービスにはテンプレートが存在しません。新規に作成しますか ?」というメッセージがデータフレームに表示されます。

6. 「作成」をクリックします。

   RADIUS 認証属性がデータフレームに表示されます。必要に応じて属性を修正します。これらの属性の説明については、第 24 章「RADIUS 認証属性」を参照するか、またはコンソール右上の「ヘルプ」リンクをクリックしてください。

7. 「保存」をクリックします。

   RADIUS 認証サービスが有効になります。

RADIUS 認証を使用してログインする

RADIUS 認証を使用してログインするには、コア認証サービス属性である 198 ページの「組織認証モジュール」 で、RADIUS 認証を定義するように修正する必要があります。そうすると、ユーザーが `http://` ホスト名 : ポート / 配備 *`URI`*`/UI/Login?module=RADIUS` を使用してログインするときに、RADIUS 認証のログインウィンドウが表示されます。使用している認証タイプ (サービス、ロール、ユーザー、組織など) によっては、認証モジュールをデフォルトとして設定する場合に、URL でモジュール名を指定する必要がありません。

Sun ONE Application Server で RADUIS 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 (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、他のアクションで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 に接続することと、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 認証

Secure Computing の SafeWord™ または SafeWord PremierAccess™ 認証サーバーで SafeWord 認証要求を処理するように、Identity Server を設定できます。Identity Server では、SafeWord 認証のクライアント部分を担当します。SafeWord サーバーは、Identity Server 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。

SafeWord 認証を登録し、有効にする

組織管理者または最上位管理者として、Identity Server にログインする必要があります。

1. SafeWord 認証を登録する組織のナビゲーションフレームに移動します。
2. 「表示」メニューから「サービス」を選択します。

   コアサービスが登録済みの場合は、ナビゲーションフレームに表示されます。登録済みでない場合は、SafeWord 認証サービスとともに登録されます。
3. ナビゲーションフレームで「追加」をクリックします。

   利用可能なサービスの一覧がデータフレームに表示されます。
4. 「SafeWord 認証」のチェックボックスを選択し、「追加」をクリックします。

   SafeWord 認証サービスがナビゲーションフレームに表示され、登録されたことが管理者に示されます。
5. 「認証」「SafeWord」の矢印をクリックします。

   「現在このサービスにはテンプレートが存在しません。新規に作成しますか ?」というメッセージがデータフレームに表示されます。
6. 「作成」をクリックします。

   SafeWord 認証属性がデータフレームに表示されます。必要に応じて属性を修正します。これらの属性の説明については、第 25 章「SafeWord 認証属性」を参照するか、またはコンソール右上の「ヘルプ」リンクをクリックしてください。
7. 「保存」をクリックします。

   SafeWord 認証サービスが有効になります。

SafeWord 認証を使用してログインする

SafeWord 認証を使用してログインするには、コア認証サービス属性である 198 ページの「組織認証モジュール」で、SafeWord 認証を定義するように修正する必要があります。そうすると、ユーザーが `http://` ホスト名 : ポート / 配備 *`URI`*`/UI/Login?module=SAFEWORD` を使用してログインするときに、SafeWord 認証のログインウィンドウが表示されます。使用している認証タイプ (ロール、ユーザー、組織など) によっては、認証モジュールをデフォルトとして設定する場合に、URL でモジュール名を指定する必要がありません。

Sun ONE 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、他のアクションで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` に接続することと、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。

SecurID 認証

RSA の ACE/Server 認証サーバーで SecureID 認証要求を処理するように、Identity Server を設定できます。Identity Server では、SecurID 認証のクライアント部分を担当します。ACE/Server は、Identity Server 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、ルートユーザーでアクセスする必要があります。

SecurID 認証では、認証ヘルパ `amsecuridd` を使用します。認証ヘルパはメイン Identity Server プロセスとは独立したプロセスです。このヘルパは起動時に、設定情報を得るためにポートで待機します。Identity Server が `nobody`、またはルート以外のユーザー ID で実行するようにインストールされている場合でも、*`IdentityServer_base`*`/SUNWam/share/bin/amsecuridd` プロセスはルートユーザーとして実行する必要があります。`amsecuridd` ヘルパについての詳細は、157 ページの「amsecuridd ヘルパ」を参照してください。

SecurID 認証を登録し、有効にする

組織管理者または最上位管理者として、Identity Server にログインする必要があります。

1. SecurID 認証を登録する組織のナビゲーションフレームに移動します。
2. 「表示」メニューから「サービス」を選択します。

   コアサービスが登録済みの場合は、ナビゲーションフレームに表示されます。登録済みでない場合は、SecurID 認証サービスとともに登録されます。
3. ナビゲーションフレームで「追加」をクリックします。

利用可能なサービスの一覧がデータフレームに表示されます。

4. 「SecurID 認証」のチェックボックスを選択し、「追加」をクリックします。

   SecurID 認証サービスがナビゲーションフレームに表示され、登録されたことが管理者に示されます。

5. 「認証」「SecurID」の矢印をクリックします。

   「現在このサービスにはテンプレートが存在しません。新規に作成しますか?」というメッセージがデータフレームに表示されます。

6. 「作成」をクリックします。

   SecurID 認証属性がデータフレームに表示されます。必要に応じて属性を修正します。これらの属性の説明については、第 26 章「SecurID 認証属性」を参照するか、またはコンソール右上の「ヘルプ」リンクをクリックしてください。

7. 「保存」をクリックします。

   SecurID 認証サービスが有効になります。

SecurID 認証を使用してログインする

SecurID 認証を使用してログインするには、コア認証サービス属性である 198 ページの「組織認証モジュール」で、SecurID 認証を定義するように修正する必要があります。そうすると、ユーザーが `http://` ホスト名 : ポート / 配備 *URI*`/UI/Login?module=SecurID` を使用してログインするときに、SecurID 認証のログインウィンドウが表示されます。使用している認証タイプ (ロール、ユーザー、組織など) によっては、認証モジュールをデフォルトとして設定する場合に、URL でモジュール名を指定する必要がありません。

UNIX 認証

Identity Server がインストールされている Solaris 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、Identity Server を設定できます。UNIX 認証では組織属性は 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 `amunixd` を使用します。認証ヘルパはメイン Identity Server プロセスとは独立したプロセスです。このヘルパが起動すると、設定情報を元に 1 つのポートで待機します。UNIX ヘルパは Identity Server ごとに 1 つだけあり、そのすべての組織で使用されます。

Identity Server が `nobody`、またはルートユーザー以外のユーザー ID で実行するようにインストールされている場合でも、*`IdentityServer_base`*`/SUNWam/share/bin/amunixd` プロセスはルート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` ヘルパを実行するには、次のコマンドを入力します。

```
./amunixd [-c ポート番号 ] [IP アドレス ]
```

IP アドレスとポート番号は、`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。

UNIX 認証サービスは、Windows プラットフォームでは利用できません。

UNIX 認証を登録し、有効にする

以下の手順では、最上位管理者として、Identity Server にログインする必要があります。

1. サービス設定モジュールを選択します。
2. 「サービス名」リストで、「認証」「UNIX」の矢印をクリックします。

   グローバル属性および組織属性が表示されます。1 つの UNIX ヘルパで Identity Server サーバーの組織をすべて提供するため、UNIX 属性のほとんどはグローバルです。これらの属性の説明については、第 27 章「UNIX 認証属性」を参照するか、またはコンソール右上の「ヘルプ」リンクをクリックしてください。
3. 「保存」をクリックして、属性の新しい値を保存します。

   組織管理者として Identity Server にログインすると、組織に対する UNIX 認証を有効にできます。
4. UNIX 認証を登録する組織のナビゲーションフレームに移動します。
5. 「表示」メニューから「サービス」を選択します。

   コアサービスが登録済みの場合は、ナビゲーションフレームに表示されます。登録済みでない場合は、UNIX 認証サービスとともに登録されます。
6. ナビゲーションフレームで「追加」をクリックします。

   利用可能なサービスの一覧がデータフレームに表示されます。
7. 「UNIX 認証」のチェックボックスを選択し、「追加」をクリックします。

   UNIX 認証サービスがナビゲーションフレームに表示され、登録されたことが管理者に示されます。
8. 「認証」「UNIX」の矢印をクリックします。

   「現在このサービスにはテンプレートが存在しません。新規に作成しますか?」というメッセージがデータフレームに表示されます。
9. 「作成」をクリックします。

   UNIX 認証の組織属性がデータフレームに表示されます。必要に応じて認証レベル属性を修正します。この属性の説明については、第 27 章「UNIX 認証属性」を参照するか、またはコンソール右上の「ヘルプ」リンクをクリックしてください。
10. 「保存」をクリックします。

    UNIX 認証サービスが有効になります。

UNIX 認証を使用してログインする

UNIX 認証を使用してログインするには、コア認証サービス属性である 198 ページの「組織認証モジュール」 で、UNIX 認証を定義するように修正する必要があります。そうすると、ユーザーが `http://` ホスト名 : ポート / 配備 *`URI`*`/UI/Login?module=Unix` を使用してログインするときに、UNIX 認証のログインウィンドウが表示されます。使用している認証タイプ (サービス、ロール、ユーザー、組織など) によっては、認証モジュールをデフォルトとして設定する場合に、URL でモジュール名を指定する必要がありません。

認証設定

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。

- 組織
- ロール
- サービス
- ユーザー

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

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組織認証モジュールを修正する必要があります。

認証設定のユーザーインタフェース

認証設定サービスでは、ユーザーがコンソール、または Identity Server 内でセキュリティ保護されたリソースにアクセスできるようになる前にパスしなければならない 1 つ以上の認証サービス (モジュール) を定義できます。組織、ロール、サービス、およびユーザーを基にした認証では、共通のユーザーインタフェースを使用して、認証モジュールを定義します。特定のオブジェクトタイプの認証設定インタフェースにアクセスする手順は、後続の節で説明します。

1. オブジェクトの認証設定属性の隣にある「編集」リンクをクリックして、「モジュールリスト」ウィンドウを表示します。

2. このウィンドウには、そのオブジェクトに割り当ててある認証モジュールの一覧が表示されます。モジュールが存在しない場合は、「追加」をクリックして「モジュールを追加」ウィンドウを表示します。

   「モジュールを追加」ウィンドウには、定義するファイルが 3 つあります。

「モジュール名」：このプルダウンリストでは、Identity Server で利用可能な認証モジュールを選択できます (追加されたカスタムモジュールを含む)。デフォルトでは、次のモジュールがあります。

- LDAP
- 証明書
- 匿名
- SafeWord
- SecurID
- HTTPBasic
- メンバーシップ
- NT
- RADIUS
- UNIX

「フラグ」：プルダウンメニューで認証モジュールの要件を次のいずれかに指定できます。

- REQUIRED - 認証には認証モジュールが必要です。認証に成功または失敗すると、認証モジュール一覧の次のモジュールへと認証が進行します。
- REQUISITE - 認証には認証モジュールが必要です。認証に成功すると、認証モジュール一覧の次のモジュールへと認証が進行します。認証に失敗すると、制御がアプリケーションに返されます。認証モジュール一覧の次のモジュールには認証が進行しません。
- SUFFICIENT - 認証に認証モジュールは不要です。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、認証モジュール一覧の次のモジュールには認証が進行しません。認証に失敗すると、一覧の次のモジュールへと認証が進行します。
- OPTIONAL - 認証に認証モジュールは不要です。認証に成功または失敗しても、認証モジュール一覧の次のモジュールへと認証が進行します。

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。適用条件には上下関係があり、「REQUIRED」が最も高く、「OPTIONAL」が最も低くなります。

たとえば、管理者が LDAP モジュールに「REQUIRED」フラグを設定している場合、ユーザーが特定のリソースにアクセスするためには、ユーザーの資格情報が LDAP の認証条件にパスすることが必要です。

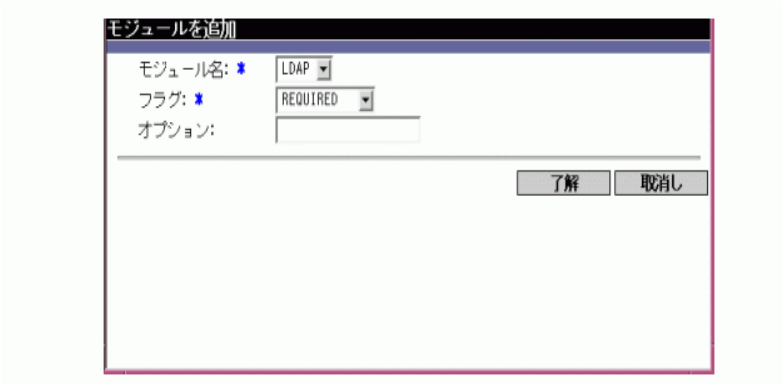
複数の認証モジュールを追加して各モジュールのフラグを「REQUIRED」に設定した場合、ユーザーがアクセスするためにはすべての認証条件にパスする必要があります。

フラグの定義の詳細については、次のサイトの JAAS (Java Authentication and Authorization Service) を参照してください。

```
http://java.sun.com/security/jaas/doc/module.html
```

「オプション」：モジュールの追加オプションをキー = 値のペアとして指定できます。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。

図 7-1　ユーザー用の「モジュールを追加」ウィンドウ



3. フィールドを選択したら、「OK」をクリックして「モジュールリスト」ウィンドウに戻ります。定義した認証モジュールがこのウィンドウに表示されます。「保存」をクリックします。

   このリストには必要なだけ多くの認証モジュールを追加できます。複数の認証モジュールを追加することを連鎖と言います。認証モジュールを連鎖している場合は、一覧に表示される順番で、適用される階層の順序が決まります。

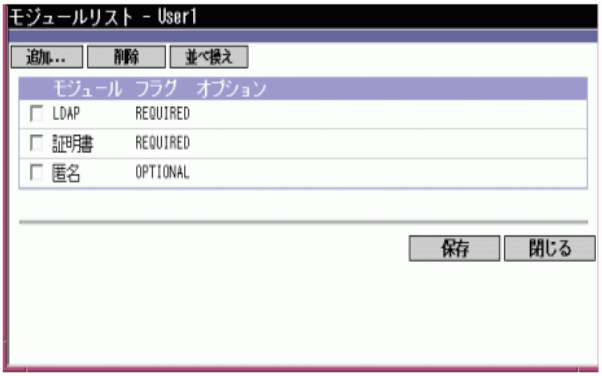
   認証モジュールの順番を変更するには、次の手順を実行します。

   a. 「並べ換え」ボタンをクリックします。

   b. 並べ換えるモジュールを選択します。

   c. 「上」および「下」のボタンを使用して、希望する位置に移動します。

図 7-2　ユーザー用の「モジュールリスト」ウィンドウ



4. リストから認証モジュールを削除するには、認証モジュールの隣にあるチェックボックスを選択して「削除」をクリックします。

注　連鎖内の任意のモジュールで amadmin 資格情報を入力した場合は、amadmin プロファイルを受信します。この場合は、認証でエイリアスのマッピングや連鎖内のモジュールは確認されません。

組織用の認証設定

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

組織の認証属性を設定するには、次の手順を実行します。

1. 認証属性を設定する組織に移動します。
2. 「表示」メニューから「サービス」を選択します。
3. サービスのリスト表示で、「コア」をクリックします。

   コア認証属性がデータフレームに表示されます。
4. 管理者認証属性の隣にある「編集」リンクをクリックします。これにより、管理者専用に認証サービスを定義できます。管理者とは、Identity Server コンソールにアクセスする必要があるユーザーのことです。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。

   認証サービスを定義したら、「保存」をクリックして変更内容を保存します。次に「閉じる」をクリックし、組織のコア認証属性に戻ります。

5. 組織認証設定属性の隣にある「編集」リンクをクリックします。これにより、組織内の全ユーザー用に認証モジュールを定義できます。デフォルトの認証モジュールは LDAP です。
6. 認証サービスを定義したら、「保存」をクリックして変更内容を保存します。次に「閉じる」をクリックし、組織のコア認証属性に戻ります。

ロール用の認証設定

認証モジュールは、認証設定サービスをロールレベルで登録すると、ロール用に設定されます。

1. 認証属性を設定する組織に移動します。
2. 「表示」メニューから「ロール」を選択します。
3. 認証設定を設定するロールを選択し、「プロパティ」の矢印をクリックします。

   ロールのプロパティがデータフレームに表示されます。
4. データフレームの「表示」メニューから「サービス」を選択します。
5. 必要に応じて認証設定属性を修正します。これらの属性の説明については、第 28 章「認証設定サービス属性」を参照するか、またはコンソール右上の「ヘルプ」リンクをクリックしてください。
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。

ロールベースの認証を有効にするときは、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。

サービス用の認証設定

認証モジュールは、認証設定サービスを登録すると、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. アイデンティティ (識別情報) 管理モジュールの「表示」メニューから、「サービス」を選択します。

   登録済みのサービスの一覧が表示されます。認証設定サービスを登録していない場合は、次の手順に進みます。サービスを登録済みの場合は、手順 4 にスキップします。

2. ナビゲーションフレームで「追加」をクリックします。

   利用可能なサービスの一覧がデータフレームに表示されます。

3. 「認証設定」のチェックボックスを選択し、「追加」をクリックします。

   認証設定サービスがナビゲーションフレームに表示され、登録されたことが管理者に示されます。

4. 「認証設定」の矢印をクリックします。

   「サービスインスタンスリスト」がデータフレームに表示されます。

5. 認証モジュールを設定するサービスインスタンスをクリックします。

6. 認証設定属性を修正し、「保存」をクリックします。これらの属性の説明については、第 28 章「認証設定サービス属性」を参照するか、またはコンソール右上の「ヘルプ」リンクをクリックしてください。

ユーザー用の認証設定

1. アイデンティティ (識別情報) 管理モジュールの「表示」メニューから、「ユーザー」を選択します。

   ユーザーの一覧がナビゲーションフレームに表示されます。

2. 修正したいユーザーを選択し、「プロパティ」の矢印をクリックします。

   ユーザープロファイルがデータフレームに表示されます。

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、ユーザー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。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。

3. 認証設定サービスがユーザーに割り当てられていることを確認するには、「表示」メニューで「サービス」を選択します。割り当てられている場合は、認証設定サービスが割り当て済みサービスとして表示されます。
4. データフレームの「表示」メニューから「ユーザー」を選択します。
5. ユーザー認証設定属性の隣にある「編集」リンクをクリックして、ユーザー用の認証モジュールを定義します。
6. 「保存」をクリックします。

認証レベルによる認証

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」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、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:// ホスト名 : ポート / 配備 URI/UI/Login?authlevel= 認証レベル値
```

認証レベルが認証レベル値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。

モジュールによる認証

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://` ホスト名 `:` ポート `/` 配備 *`URI`*`/UI/Login?module=` モジュール名

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組織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。詳細は、198 ページの「組織認証モジュール」を参照してください。

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」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、組織、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組織に追加し、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 REQUIRED、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。アイデンティティオブジェクトの認証設定サービスを登録する方法については、114 ページの「認証設定」を参照してください。

第 8 章

パスワードリセットサービス

Sun™ ONE Identity Server では、Identity Server 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によって定義され、ユーザー検証の資格情報を「秘密の質問」形式で制御し、新規または既存のパスワード通知のメカニズムを制御します。また、ユーザー検証が失敗した場合のロックアウト間隔も設定できます。

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

ユーザーの属している組織に対しては、パスワードリセットサービスを登録する必要はありません。ユーザーの属し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、このサービスについてサービス設定モジュールで定義されている値が継承されます。

異なる組織のユーザーのパスワードリセットサービスを登録するには、次の手順を実行します。

1. アイデンティティ管理モジュールで、「組織」を選択し、サービスを登録する組織を選択します。
2. ナビゲーションフレームで「登録」をクリックします。

   利用可能なサービスの一覧がデータフレームに表示されます。
3. 「パスワードリセット」のチェックボックスを選択し、「登録」をクリックします。

パスワードリセットサービスがナビゲーションフレームに表示され、登録されたことが管理者に示されます。

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には、次の手順を実行します。

1. パスワードリセットサービスが登録されている組織を選択します。
2. 「パスワードリセット」の矢印をクリックします。

   「このサービスに利用可能なテンプレートはありません。」というメッセージがデータフレームに表示されます。「作成」をクリックします。
3. パスワードリセット属性がデータフレームに表示され、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になっています)。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。

   これら以外の属性は省略可能です。パスワードリセット属性の説明については、257 ページの「パスワードリセットサービス属性」を参照するか、またはコンソール右上の「ヘルプ」リンクをクリックしてください。

注

Identity Server 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:

```
IdentityServer_base/SUNWam/samples/console/PasswordGenerator
```

NotifyPassword:

```
IdentityServer_base/SUNWam/samples/console/NotifyPassword
```

4. ユーザー自身が独自の質問を定義できるようにするには、「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ロックアウト機能があり、ユーザーが秘密の質問に回答できる回数を制限します。ロックアウト機能を設定するには、パスワードリセットサービス属性を使用します。これらの属性については、257 ページの「パスワードリセットサービス属性」を参照してください。パスワードリセットでは、メモリロックアウトと物理ロックアウトの 2 種類がサポートされています。

メモリロックアウト

これは一時的なロックアウトであり、「パスワードリセット失敗のロックアウト持続時間 (分)」属性の値が 0 より大きく、かつ、「パスワードリセット失敗のロックアウトモード」属性が有効になっている場合にのみ機能します。これで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通してパスワードをリセットすることができなくなります。「パスワードリセット失敗のロックアウト持続時間」で指定された時間が経過するまで、あるいはサーバーが再起動されるまで、このロックアウトは持続します。

物理ロックアウト

これは、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、かつ、「パスワードリセット失敗のロックアウトモード」属性が有効になっている場合に、ユーザーが秘密の質問に対して回答を誤ると、ユーザーのアカウント状態は無効に変更されます。

エンドユーザーから見たパスワードリセット

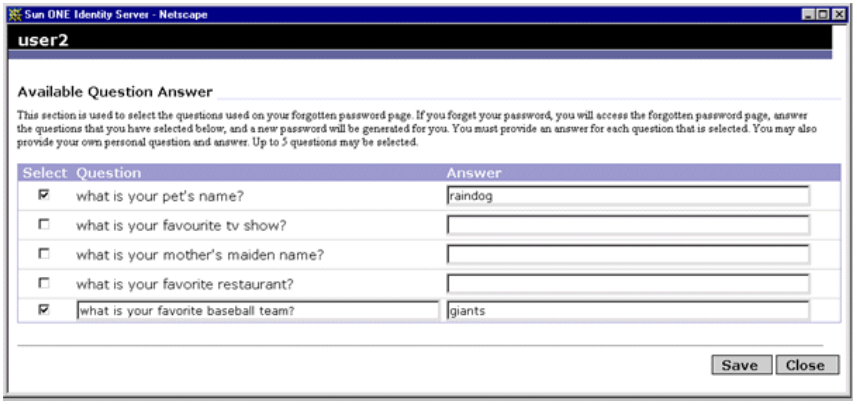
以降の節では、ユーザーの観点からパスワードリセットサービスについて説明します。

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 Identity Server 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。次に例を示します。

1. ユーザーはユーザー名とパスワードを入力して認証を受け、Identity Server 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. このサービスに対して管理者が定義した、利用可能な質問がユーザーに提示されます。次に例を示します。
   - ペットの名前
   - 好きなテレビ番組
   - 母親の旧姓
   - よく行くレストランの名前
4. 秘密の質問を選択します。管理者が組織に対して定義した最大数 (最大数はパスワードリセットサービスで定義されます) まで選択できます。選択した質問に対して回答を指定します。これらの質問と回答は、ユーザーのパスワードをリセットするための基準になります (次の節を参照)。管理者が「個人的な質問を有効」属性を選択した場合は、ユーザーが独自の秘密の質問と回答を指定できるように、テキストフィールドが表示されます。

図 8-1　個人的な質問を有効にした場合の「質問と回答」の画面



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

ユーザーがパスワードを忘れた場合、Identity Server はパスワードリセット Web アプリケーションを使って新しいパスワードをランダムに生成し、それをユーザーに通知します。パスワードを忘れた場合の典型的なシナリオを次に示します。

1. ユーザーは管理者から与えられた 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://` ホスト名 : ポート `/ampassword` (デフォルトの組織の場合)

   または

   `http://` ホスト名 : ポート / 配備
   URI`/ui/PWResetUserValidation?org=`*orgname* (*orgname* は組織の名前)

注　パスワードリセットサービスがサブ組織で有効になっていても、親組織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。

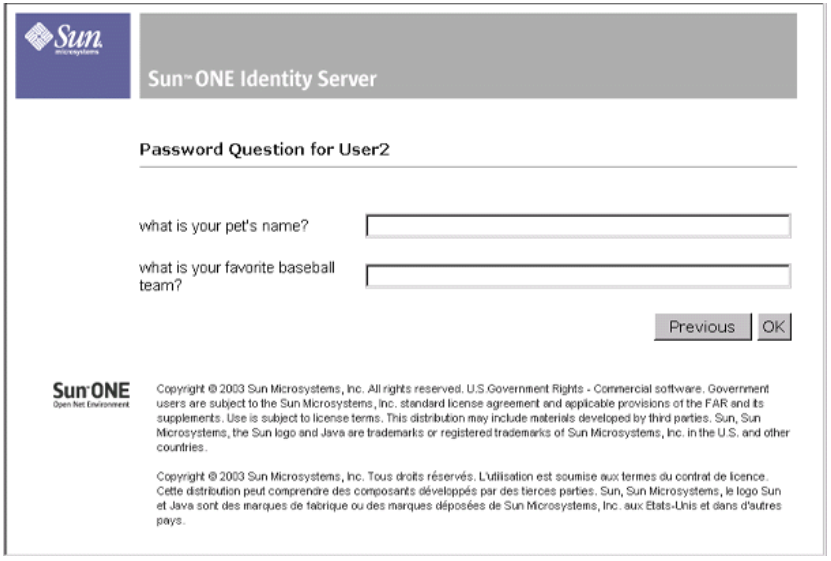
`http://` ホスト名 : ポート / 配備
URI`/ui/PWResetUserValidation?org=` 組織名

---

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で定義されている質問のうち、ユーザーがカスタマイズで選択したものが提示されます。あらかじめ「ユーザープロファイル」ページにログインして質問をカスタマイズしておかないと、パスワードは生成されません。

図 8-2　パスワードの質問画面



質問に対して正しく回答すると、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。回答が正しいかどうかにかかわらず、パスワードリセットが試みられたという通知が送信されます。新しいパスワードやパスワードリセット試行通知を受け取るには、「ユーザープロファイル」ページで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

次のような条件を適用した安全なパスワードポリシーによって、推測されやすいパスワードに関連するリスクを最小限に抑えることができます。

- ユーザーはスケジュールに従ってパスワードを変更しなければならない
- ユーザーは、自明ではないパスワードを指定しなければならない
- パスワードを一定回数誤ると、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で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 2 部

コマンド行リファレンスガイド

この「コマンド行リファレンスガイド」は、『Sun™ ONE Identity Server 管理者ガイド』の第 2 部です。次の章で構成されています。

- amadmin コマンド行ツール
- amserver コマンド行ツール
- ampassword コマンド行ツール
- am2bak コマンド行ツール
- bak2am コマンド行ツール
- VerifyArchive コマンド行ツール
- amsecuridd ヘルパ

この節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。

```
IdentityServer_base/SUNWam/bin
```

第 9 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。この章は、次の節で構成されています。

- amadmin コマンド行実行可能ファイル
- amadmin でのポリシーの作成

amadmin コマンド行実行可能ファイル

コマンド行ツール amadmin の第一の目的は、XML サービスファイルを Directory Server にロードして、DIT で管理タスクのバッチ処理を実行することです。amadmin は、IdentityServer_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を使用するサービスを Identity Server 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が、Identity Server 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、Identity Server で参照される XML データの静的なかたまりとして Directory Server に格納されます。この情報は、LDAP だけを使用できる 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、ユーザーを 1000、およびグループを 100 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。詳細については、『Sun ONE Identity Server Programmer's Guide』の「Service Management」の章を参照してください。

注 amadmin は、Identity Server 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規則があります。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 | --password file 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 [XML 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を説明します。

--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) の値です。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、ドメイン要素間にスペースを挿入し、DN 全体を二重引用符で囲むこともできます。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 のパスワードの値になります。

--locale (-l)

--locale は、ロケール名の値になります。メッセージ言語をカスタマイズするために使用できます。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。

--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 ユーザー名
```

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入力します。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入力します。

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、*IdentityServer_base*/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、i18n 互換ではありません。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、i18n 互換です。

--data (-t)

--data は、インポートされるバッチ処理用 XML ファイルの名前の値です。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。このオプションに渡される XML ファイルの種類の詳細については、『Sun ONE Identity Server Programmer's Guide』の「Service Management」の章を参照してください。

--schema (-s)

--schema は、Identity Server 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 137 ページのコード例 9-1 に示します。

コード例 9-1 `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 でのポリシーの作成

ポリシーは amadmin を介して管理できますが、amadmin を直接使用して修正することはできません。ポリシーを修正するには、そのポリシーを削除してから、修正したポリシーを amadmin を使用して追加します。

amadmin を使用してポリシーを追加するには、ポリシーの XML ファイルを policy.dtd に従って作成します。(policy.dtd については、『Sun ONE Identity Server Customization and API Guide』を参照してください。ポリシーの XML ファイルを作成すると、次のコマンドを使用してロードできます。

IdentityServer_base/SUNWam/bin/amadmin

--runasdn "uid=amAdmin,ou=People,*default_org*, ルートサフィックス "

--password パスワード

--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組織に認証モジュールを登録すること、組織、LDAP グループ、LDAP ロール、および LDAP ユーザーのサブジェクトを作成中に対応する LDAP オブジェクト (組織、グループ、ロール、およびユーザー) が存在すること、IdentityServerRoles サブジェクトを作成中に Identity Server ロールが存在すること、そしてサブ組織またはピア組織の参照を作成中に関連がある組織が存在することを確認してください。

SubOrgReferral、PeerOrgReferral、Organization サブジェクト、IdentityServerRoles サブジェクト、LDAPGroups サブジェクト、LDAPRoles サブジェクト、および LDAPUsers サブジェクトの 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。

第 10 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
- マルチサーバーのインストール管理での amserver の使用 (Web Server インスタンスのみ)

amserver コマンド行実行可能ファイル

amserver コマンド行ツールは、Solaris プラットフォームでは、Identity Server インスタンスの作成、開始、終了のほか、追加インスタンスの削除ができます。ただし、Windows 2000 プラットフォーム上の amserver では、Identity Server の開始と終了だけができます。

amserver の構文

amserver ツールの一般的な構文は次のとおりです。

```
./amserver { create | delete [インスタンス名] | startall | start |
stop | stopall | version }
```

amserver コマンド (Solaris)

create

`create` は、Identity Server の新しいインスタンスを作成するコマンドです。amserver スクリプトはルートユーザーとして実行する必要があります。インスタンスを作成するときは、amserver スクリプト `./amserver create` を実行します。複数のサーバーインスタンスを作成する詳細な手順については、141 ページの「マルチサーバーのインストール管理での amserver の使用 (Web Server インスタンスのみ)」で説明します。このコマンドは、Web Server インスタンスにのみ適用可能です。

startall

`startall` は、Identity Server のすべてのインスタンスを開始するコマンドです。インスタンスを個別に開始するには、次のコマンド行を実行します。

```
IdentityServer_base/SUNWam/bin/amserver. インスタンス名 start
```

stopall

`stopall` は、Identity Server のすべてのインスタンスを停止するコマンドです。インスタンスを個別に停止するには、次のコマンド行を実行します。

```
/opt/SUNWam/bin/amserver. インスタンス名 stop
```

delete

`delete` は、`create` オプションで作成されたインスタンスを削除するコマンドです。

amserver コマンド (Windows 2000)

Windows 2000 プラットフォームでの amserver では、次のコマンドだけを使用できます。

start

`start` は、Identity Server を開始するコマンドです。

stop

`stop` は、Identity Server を停止するコマンドです。

注 `stop` および `start` は、新しいコンテナ非依存の配備では、正しく機能しない場合があります。正しく動作させるには、コンテナで `stop` および `start` を使用してください。

---

restart

`restart` は、Identity Server を再起動するコマンドです。

`amserver` では、Directory Server の起動や停止ができません。Directory Server は別に再起動する必要があります。このコマンドから再起動できるのは、Web Server のインスタンスに限られます。他の Web コンテナに対しては、このコマンドは認証ヘルパだけを再起動します。

マルチサーバーのインストール管理での amserver の使用 (Web Server インスタンスのみ)

複数の Identity Server インスタンスをインストールおよび管理するために、`amserver` コマンド行ユーティリティーを使用できます。複数の Identity Server インスタンスをインストールする前に、ルートユーザーでログインする必要があります。これから説明する手順で使用するスクリプトは、`IdentityServer_base/SUNWam/bin` にあります。

複数のインスタンスをインストールするには、次の手順を実行します。

1. amServer を使用して `./amserver create` と入力し、新しいサーバーインスタンスを作成します。

   たとえば `port 81:` を待機するインスタンス `instance1` を作成する場合、スクリプトの出力は次のようになります。

```
#####################################################################
##
Please enter the name of the server instance:instance1
Please enter the port number: 81
Do you want to create more server instances? y/[n]
Installing... please wait....
#####################################################################
```

a. それぞれの Web サーバーインスタンスに対してディレクトリが作成されます。次に例を示します。

   IdentityServer_base/SUNWam/servers/https- インスタンス名

b. Identity Server アプリケーションが、次の場所に配備されます。

   IdentityServer_base/SUNWam/servers/web-apps- インスタンス名

c. IdentityServer_base/SUNWam/bin ディレクトリには、インスタンス固有のバージョンの amServer が保持されます。次に例を示します。

   amserver. インスタンス名

d. Identity Server 設定ファイルのコピーが IdentityServer_base/SUNWam/lib/AMConfig- インスタンス名 .properties に作成されます。

e. ファイル /etc/rc3.d には、インスタンス固有のバージョンの初期化ファイルが保持されます。

   S55amserver. インスタンス名

   K55amserver. インスタンス名

注 インスタンス名には「_」(アンダースコア) または「.」(ピリオド) を使用しないでください。

2. 元のサーバーインスタンスを含むすべての Identity Server インスタンスを開始するには、次のコマンド行を入力します。

   ./amserver startall

   代わりに、次のコマンドを使用し、サーバーを個別に開始することもできます。

   IdentityServer_base/SUNWam/bin/amserver. インスタンス名 start

   これで、ブラウザを使用して、すべてのインスタンスに対する Identity Server ログイン画面を呼び出すことができるようになりました。

3. 元のサーバーインスタンスを含むすべての Identity Server インスタンスを停止するには、次のコマンド行を入力します。

   ./amserver stopall

   代わりに、次のコマンドを使用し、サーバーを個別に停止することもできます。

   IdentityServer_base/SUNWam/bin/amserver. インスタンス名 stop

4. delete コマンドオプションを呼び出すには、次のコマンド行を入力します。

   ./amserver delete

create コマンドで作成されたファイルがすべて削除されます。Identity Server のアンインストールユーティリティを使用する場合、スクリプトで生成されたファイルは削除されません。

5. デバッグファイル用のディレクトリを指定するには、次のコマンド行を入力します。

   ```
   Edit IdentityServer_base/SUNWam/lib/AMConfig- インスタンス名
   .properties
   ```

   com.iplanet.services.debug.directory プロパティを、あらかじめ指定したディレクトリに変更しておいてください。

6. ammultiserverinstall ユーティリティを呼び出すには、次の構文を使用します。

   ```
   ammultiserverinstall [ サーバーインスタンス名 ] [ ポート ]
   ```

   複数の Identity Server インスタンスをインストールする必要があるが、対話的でないインタフェースを使用するアプリケーションでは、ammultiserverinstall ユーティリティを使用してください。ammultiserverinstall がエラーになると、値 1 で終了します。

7. amserver は、サーバーインスタンスをプラットフォームサーバーリストに自動的に追加します。

8. SSL モードで実行するように Identity Server を設定します。手順については、このマニュアルの付録 B「Identity Server を SSL モードに設定する」を参照してください。

9. 次のコマンドを入力し、Identity Server インスタンスをすべて開始します。

   ```
   ./amserver startall
   ```

   代わりに、次のコマンドを使用し、Identity Server インスタンスを個別に開始することもできます。

   ```
   ./amserver- インスタンス start
   ```

第 11 章

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。この章は、次の節で構成されています。

- am2bak コマンド行実行可能ファイル

am2bak コマンド行実行可能ファイル

am2bak ユーティリティは IdentityServer_base/SUNWam/bin にあります。am2bak ユーティリティは、Identity Server 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
```

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 IdentityServer_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、Identity Server 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

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™ Operating Environment 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
     - *IdentityServer_base*/SUNWam/config/
     - *IdentityServer_base*/SUNWam/locale/
     - *IdentityServer_base*/SUNWam/servers/httpacl
     - *IdentityServer_base*/SUNWam/lib/*.properties (Java プロパティファイル)
     - *IdentityServer_base*/SUNWam/bin/amserver. インスタンス名
     - *IdentityServer_base*/SUNWam/servers/https- すべてのインスタンス
     - *IdentityServer_base*/SUNWam/servers/web-apps- すべてのインスタンス
     - *IdentityServer_base*/SUNWam/web-apps/services/WEB-INF/config
     - *IdentityServer_base*/SUNWam/web-apps/services/config
     - *IdentityServer_base*/SUNWam/web-apps/applications/WEB-INF/classes
     - *IdentityServer_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- ホスト /config/schema/

- *DirectoryServer_base*/slapd- ホスト /config/slapd-collations.conf
- *DirectoryServer_base*/slapd- ホスト /config/dse.ldif

- ログファイルおよびデバッグファイル
  - var/opt/SUNWam/logs (Identity Server ログファイル)
  - var/opt/SUNWam/install (Identity Server インストールログファイル)
  - var/opt/SUNWam/debug (Identity Server デバッグファイル)
- 証明書
  - *IdentityServer_base*/SUNWam/servers/alias
  - *DirectoryServer_base*/alias

このスクリプトでは、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します。

- 設定ファイルおよびカスタマイズファイル
  - *IdentityServer_base*/web-apps/services/WEB-INF/config/*
  - *IdentityServer_base*/locale/*
  - *IdentityServer_base*/web-apps/applications/WEB-INF/classes/*.properties (Java プロパティファイル)
  - *IdentityServer_base*/servers/https-ホスト/config/jvm12.conf
  - *IdentityServer_base*/servers/https- ホスト /config/magnus.conf
  - *IdentityServer_base*/servers/https- ホスト /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 (Identity Server ログファイル)
  - var/opt/debug (Identity Server デバッグファイル)
- 証明書
  - *IdentityServer_base*/servers/alias
  - *IdentityServer_base*/alias

第 12 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

bak2am コマンド行実行可能ファイル

bak2am ユーティリティは IdentityServer_base/SUNWam/bin にあります。bak2am ユーティリティでは、am2back ユーティリティでバックアップした Identity Server 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の bak2am ツール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
```

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 `IdentityServer_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 `IdentityServer_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 `IdentityServer_base/backup` です。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。

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. 入力 tar ファイルを解凍します。

   入力 tar ファイルは、バックアップスクリプトの実行時に作成されています。

第 13 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
- SSL での ampassword の実行

ampassword コマンド行実行可能ファイル

ampassword ユーティリティは $installroot/SUNWam/bin にあります。ampassword ユーティリティは、管理者またはユーザーの Identity Server パスワードを変更します。

ampassword の構文

ampassword ツールの一般的な構文は次のとおりです。

```
ampassword -a | --admin [ -o | --old 旧パスワード -n | --new 新パスワード ]
```

```
ampassword -p | --proxy [ -o | --old 旧パスワード -n | --new 新パスワード ]
```

```
ampassword -e | --encrypt [ password ]
```

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。

ampassword のオプション

--admin (-a)

--admin は、管理者のパスワードを変更します。

--proxy (-p)

`--proxy` は、プロキシパスワードを変更します。プロキシユーザー (`serverconfig.xml` でユーザータイプ `proxy`) に対応しています。

--encrypt (-e)

`--encrypt` は、パスワードを暗号化します。コマンド行に出力されます。

SSL での ampassword の実行

SSL (Secure-Socket Layer) モードで実行中の Identity Server で ampassword を実行するには、次の手順を実行します。

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。

   `IdentityServer_base/SUNWam/config/ums`

2. サーバー属性 `port` を Identity Server 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。Identity Server 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 14 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。

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。

```
VerifyArchive -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。その代わりに、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、Identity Server 管理者のユーザー ID です。

password

password は、Identity Server 管理者のパスワードです。

第 15 章

amsecuridd ヘルパ

この章では、amsecuridd ヘルパ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 ヘルパコマンド行実行可能ファイル
- amsecuridd ヘルパの実行

amsecuridd ヘルパコマンド行実行可能ファイル

Identity Server の SecurID 認証モジュールは、Security Dynamic ACE/Client C API と amsecuridd ヘルパを使って実装されます。このヘルパは、Identity Server 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、SecurID 認証要求を待機するために localhost:57943 へのソケットを開くことで、amsecuridd デーモンを呼び出します。

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 からのクリアテキストなので、ローカルホスト接続だけが許可されています。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、デフォルトでは IdentityServer_base/SUNWam/lib/ にあります。securidHelp.ports 属性には、amsecuridd ヘルパ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、Identity Sever を再起動してください。

注	別の ACE/Server (別の sdconf.rec ファイルを持つ) 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

verbose (-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。

configure portnumber (-c portnm)

待機ポート番号を設定します。デフォルトは 58943 です。

amsecuridd ヘルパの実行

amsecuridd は、デフォルトでは *IdentityServer_base*/SUNWam/share/bin にあります。デフォルトのポートでヘルパを実行するには、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 *IdentityServer_base*/Sunwam/lib/ に設定します。

第 3 部

属性リファレンスガイド

この「属性リファレンスガイド」は、『Sun ONE Identity Server 管理ガイド』の第 3 部です。Identity Server のデフォルトサービス内で設定済みの属性について説明します。次の章で構成されています。

- ポリシー設定サービス属性
- SAML サービス属性
- セッションサービス属性
- ユーザー属性

第 16 章

管理サービス属性

管理サービスにはグローバル属性と組織属性があります。グローバル属性に適用される値は Sun ONE Identity Server 設定全体に適用され、設定済みのすべての組織に継承されます。グローバル属性の目的は Identity Server アプリケーションをカスタマイズすることであるため、ロールまたは組織に直接適用することはできません。組織属性に適用される値は設定済みの各組織のデフォルト値で、サービスを組織に登録するときに変更できます。組織属性は組織のエントリに継承されません。管理属性は次のように分けられます。

- グローバル属性
- 組織属性

グローバル属性

管理サービスのグローバル属性は次のとおりです。

- 連携管理を有効
- ユーザー管理を有効
- ピープルコンテナを表示
- メニューにコンテナを表示
- グループコンテナを表示
- 管理されているグループタイプ
- デフォルトロールアクセス権 (ACI)
- ドメインコンポーネントツリーを有効
- 管理グループを有効
- ユーザー削除を有効
- ダイナミック管理者ロール ACI

- ユーザープロファイルサービスクラス
- DC ノードの属性リスト
- 削除したオブジェクトの検索フィルタ

連携管理を有効

このフィールドを選択すると、連携管理が有効になります。デフォルトは有効です。この機能を無効にするには、フィールドの選択を解除します。「連携管理サービス」タブはコンソールに表示されなくなります。

ユーザー管理を有効

このフィールドが true (チェックボックスを選択) の場合、ユーザー管理が有効になります。デフォルトでは、有効になっています。

ピープルコンテナを表示

この属性は、Identity Server コンソールにピープルコンテナを表示するかどうかを指定します。このオプションを選択すると、組織、コンテナ、およびグループコンテナの「表示」メニューに「ピープルコンテナ」メニュー項目が表示されます。「ピープルコンテナ」はフラット DIT の最上位レベルにのみ表示されます。

ピープルコンテナは、ユーザープロファイルを含む組織単位です。DIT で 1 つのピープルコンテナを使用し、ロールの柔軟性を利用してアクセスおよびサービスを管理することをお勧めします。Identity Server コンソールのデフォルトの動作では、ピープルコンテナは非表示です。ただし、DIT に複数のピープルコンテナがある場合は、「ピープルコンテナを表示」を選択して、ピープルコンテナを Identity Server コンソールの管理オブジェクトとして表示します。

メニューにコンテナを表示

この属性は、Identity Server コンソールの「表示」メニューにコンテナを表示するかどうかを指定します。デフォルト値は `false` です。管理者は必要に応じてどちらかを選択できます。

- `false` (チェックボックスを選択しない) - コンテナは組織およびほかのコンテナの最上位レベルの「表示」メニューの項目に含まれません。
- `true` (チェックボックスを選択する) - コンテナは組織およびほかのコンテナの最上位レベルの「表示」メニューの項目に含まれます。

グループコンテナを表示

この属性は、Identity Server コンソールにグループコンテナを表示するかどうかを指定します。このオプションを選択すると、組織、コンテナ、およびグループコンテナの「表示」メニューに「グループコンテナ」メニュー項目が表示されます。グループコンテナはグループの組織単位です。

管理されているグループタイプ

このオプションは、コンソールで作成した加入グループがスタティックかダイナミックかを指定します。コンソールは、スタティックでありかつダイナミックである加入グループではなく、スタティックまたはダイナミックのどちらかである加入グループを作成および表示します。フィルタを適用したグループは、この属性に指定された値には関係なく常にサポートされます。デフォルト値はダイナミックです。

- スタティックグループは、`groupOfNames` または `groupOfUniqueNames` オブジェクトクラスを使って、各グループメンバーを明示的に一覧表示します。グループエントリには、グループの各メンバーの `uniqueMember` 属性が含まれます。スタティックグループのメンバーは手動で追加しますが、ユーザーエントリ自体は変更されません。スタティックグループはメンバーの少ないグループに適しています。
- ダイナミックグループは、各グループメンバーのエントリの `memberOf` 属性を使用します。ダイナミックグループのメンバーは、`memberOf` 属性を含むすべてのエントリを検索して返す LDAP フィルタを使って生成されます。ダイナミックグループは、メンバーが非常に多いグループに適しています。

- フィルタを適用したグループは、LDAP を使用して、フィルタの要件を満たすメンバーを検索して返します。たとえば、フィルタは、特定の uid (`uid=g*`) または電子メールアドレス (`mail=*@sun.com`) を持つメンバーを生成できます。これらの例では、LDAP フィルタはそれぞれ、uid が `g` で始まる、または電子メールアドレスが `sun.com` で終わるすべてのユーザーを返します。フィルタを適用したグループは、「フィルタによるメンバーシップ」を選択して、ユーザー管理ビュー内でのみ作成できます。

管理者は次の中から 1 つ選択できます。

- ダイナミック - 加入によるメンバーシップのオプションを使って作成されたグループはダイナミックになります。
- スタティック - 加入によるメンバーシップのオプションを使って作成されたグループはスタティックになります。

デフォルトロールアクセス権 (ACI)

この属性は、新しいロールの作成時に管理者権限の認可に使うデフォルト ACI (アクセス制御命令) または権限のリストを定義します。必要な権限のレベルに応じて、これらの ACI の 1 つを選択します。Identity Server にはデフォルトロール権限が 4 つあります。

アクセス権なし (No permission)

ロールにアクセス権が設定されません。

組織管理者 (Organization Admin)

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。

組織のヘルプデスク管理者 (Organization Help Desk Admin)

組織の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 (Organization Policy Admin)

組織のポリシー管理者は、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。組織のポリシー管理者は、ピア組織に対する参照ポリシーを作成できません。

注

ロールは、`aci_name | aci_desc | dn:aci ## dn:aci ## dn:aci` という形式で定義します。

- *aci_name* は ACI の名前です。
- *aci_desc* はこれらの ACI が許可するアクセスの説明です。使いやすくするため、対象読者は ACI やその他のディレクトリの概念に関する知識がないものと仮定します。

aci_name および *aci_desc* は、`amAdminUserMsgs.properties` ファイルに含まれる国際化 (i18n) キーです。コンソールに表示される値は、`.properties` ファイルから取得され、これらのキーを使用して値を検索します。

- *dn:aci* は DN と ACI のペアを表し、## で区切ります。Identity Server は関連付けられた DN エントリの各 ACI を設定します。この形式では、ACI の値に、特定の名前の代わりに次のタグを指定できます。ROLENAME、ORGANIZATION、GROUPNAME および PCNAME です。これらのタグを使用することによって、デフォルトとして使用するのに十分に柔軟なロールを定義できます。デフォルトのロールの 1 つに基づいてロールを作成すると、ACI のタグはその新しいロールの DN から取得した値になります。

ドメインコンポーネントツリーを有効

ドメインコンポーネントツリー (DC ツリー) は固有の DIT 構造で、多くの Sun ONE コンポーネントがこれを使用して、DNS 名と組織のエントリ間のマッピングをします。

このオプションを有効にすると、組織が作成されたときに組織の DNS 名が入力されていれば、組織の DC ツリーエントリが作成されます。DNS 名フィールドは、組織作成ページに表示されます。このオプションは最上位レベルの組織にだけ適用され、サブ組織には表示されません。

組織ツリーで、Identity Server SDK を使用して `inetdomainstatus` 属性の状態を変更すると、対応する DC ツリーエントリの状態が更新されます。Identity Server SDK を使用せずに状態を更新した場合、その内容は同期しません。たとえば、新しい組織 `sun` を sun.com という DNS 名属性で作成すると、DC ツリーに次のエントリが作成されます。

`dc=sun,dc=com,o=internet,`*root suffix*

AMConfig.properties で com.iplanet.am.domaincomponent を設定することによって、この DC ツリーに独自のルートサフィックスを設定することもできます。デフォルトでは、これは Identity Server root に設定されています。異なるサフィックスが望ましい場合は、LDAP コマンドを使ってこのサフィックスを作成する必要があります。組織を作成する管理者の ACI は、新しい DC ツリーのルートに無制限のアクセス権を持つように、修正する必要があります。

管理グループを有効

このオプションは、DomainAdministrators および DomainHelpDeskAdministrators グループを作成するかどうかを指定します。選択すると (true)、これらのグループが作成され、それぞれ組織管理者ロールおよび組織ヘルプデスク管理者ロールと関連付けられます。このグループが作成されると、これらの関連するロールの 1 つにユーザーを追加したり削除したりしたときに、対応するグループへのユーザーの追加や、グループからのユーザーの削除が自動的に行われます。ただし、逆の処理は行われません。これらのグループの 1 つでユーザーの追加や削除をしても、関連するロールではユーザーの追加や削除は行われません。

DomainAdministrators および DomainHelpDeskAdministrators グループは、このオプションを有効にした後に作成された組織でのみ作成されます。

注 このオプションはサブ組織には適用されません。ただし、root org は例外です。root org には、ServiceAdministrators および ServiceHelpDesk 管理者グループが作成され、それぞれ最上位レベル管理者および最上位レベルヘルプデスク管理者のロールと関連付けられます。同じ動作が適用されます。

ユーザー削除を有効

このオプションは、ディレクトリからユーザーのエントリを削除するか、それとも削除マークを付けるだけかを指定します。ユーザーのエントリが削除され、このオプションが選択されている場合 (true)、ユーザーのエントリはまだディレクトリに存在していますが、削除マークは付けられています。削除マークを付けられたユーザーエントリは、ディレクトリサーバーの検索時に返されることはありません。このオプションが選択されていない場合は、ユーザーのエントリはディレクトリから削除されます。

ダイナミック管理者ロール ACI

この属性は、Identity Server を使ってグループまたは組織を構成するときにダイナミックに作成される管理者ロールのアクセス制御命令を定義します。これらのロールは、作成したエントリの特定のグループに管理権限を与えるのに使用します。デフォルトの ACI はこの属性リストの下でのみ変更できます。

警告 組織レベルの管理者は、グループ管理者よりも広範なアクセス権を持っています。ただし、デフォルトでは、ユーザーをグループ管理者ロールに追加すると、そのユーザーはグループのすべてのユーザーのパスワードを変更できます。これには、そのグループのメンバーである組織管理者も含まれます。

コンテナヘルプデスク管理者 (Container Help Desk Admin)

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。

組織のヘルプデスク管理者 (Organization Help Desk Admin)

組織の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 (Container Admin)

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。Identity Server 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 (Organization Policy Admin)

組織のポリシー管理者は、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。

ピープルコンテナ管理者 (People Container Admin)

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ピープルコンテナのメンバーです。ピープルコンテナ管理者は、組織のピープルコンテナ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削除したりすることができません。

注 ほかのコンテナは、Identity Server 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。組織を構成した後で、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 (Group Admin)

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 (Top-level Admin)

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、Identity Server 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 (Organization Admin)

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。

ユーザープロファイルサービスクラス

この属性は、ユーザープロファイルページでカスタム表示を持つサービスをリストします。サービスによっては、コンソールによって生成されるデフォルト表示では不十分な場合があります。この属性は、どんなサービスでもカスタム表示を作成し、表示するサービス情報の内容や、表示の方法をすべてコントロールすることができます。構文は次のとおりです。

service name | *relative url*

注 この属性でリストされるサービスは、ユーザー作成ページには表示されません。カスタムサービス表示のデータ設定は、ユーザープロファイルページで行う必要があります。

DC ノードの属性リスト

オブジェクトが作成されるときに、DC ツリーエントリ内に設定される属性のセットを定義します。デフォルトのパラメータは次のとおりです。

- maildomainwelcomemessage
- preferredmailhost
- mailclientattachmentquota
- mailroutingsmarthost
- mailroutingsmarthost
- mailroutingsmarthost
- mailaccessproxyreplay
- preferredlanguage
- domainuidseparator
- maildomainmsgquota
- maildomainallowedserviceaccess
- preferredmailmessagestore
- maildomaindiskquota
- maildomaindiskquota
- objectclass=maildomain
- mailroutinghosts

削除したオブジェクトの検索フィルタ

このフィールドは、「ユーザー削除を有効」モードが有効であるときに削除される、オブジェクトの検索フィルタを定義します。

組織属性

管理サービスの組織属性は次のとおりです。

- グループのデフォルトピープルコンテナ
- グループのピープルコンテナリスト
- ユーザープロファイル表示クラス
- ユーザーのロールを表示
- ユーザーのグループを表示
- ユーザーのグループへの自己加入
- ユーザープロファイル表示オプション
- ユーザー作成のデフォルトロール
- 表示メニューエントリ
- 検索で返される結果の最大数
- 検索のタイムアウト (秒)
- JSP ディレクトリ名
- オンラインヘルプドキュメント
- 必要なサービス
- ユーザー検索キー
- ユーザー検索により返される属性
- ユーザー作成通知リスト
- ユーザー削除通知リスト
- ユーザー修正通知リスト
- ページごとの最大エントリ数
- 表示オプション
- イベントリスナークラス
- プレおよびポストプロセスクラス

- 外部属性のフェッチを有効

グループのデフォルトピープルコンテナ

このフィールドは、デフォルトのピープルコンテナを指定します。ユーザーは作成時にこのコンテナに配置されます。デフォルト値はありません。有効な値は、ピープルコンテナの DN です。ピープルコンテナの代替順位については、グループのピープルコンテナリスト属性の下にある注を参照してください。

グループのピープルコンテナリスト

このフィールドは、ピープルコンテナのリストを指定します。グループ管理者は、新しいユーザーを作成するときに、このリストから選択できます。ディレクトリツリー内に複数のピープルコンテナがある場合に、このリストを使用できます。このリスト、または「グループのデフォルトピープルコンテナ」フィールドにピープルコンテナが指定されていない場合、ユーザーはデフォルトの Identity Server ピープルコンテナ `ou=people` に作成されます。このフィールドのデフォルト値はありません。この属性の構文は次のとおりです。

group name|*dn of people container*

注	ユーザーの作成時に、エントリを入れるコンテナのこの属性がチェックされます。この属性が空の場合、コンテナの「グループのデフォルトピープルコンテナ」属性がチェックされます。後者の属性が空の場合、エントリは `ou=people` の下に作成されます。

ユーザープロファイル表示クラス

この属性は、Identity Server コンソールがユーザープロファイルページを表示するときに使用する Java のクラスを指定します。

ユーザーのロールを表示

このオプションは、ユーザーに割り当てられているロールのリストを、ユーザーのユーザープロファイルページの一部として表示するかどうかを指定します。この値が `false` (選択されていない) の場合、ユーザープロファイルページは管理者のみにユーザーのロールを表示します。デフォルト値は `false` です。

ユーザーのグループを表示

このオプションは、ユーザーに割り当てられているグループのリストを、ユーザーのユーザープロファイルページの一部として表示するかどうかを指定します。この値が `false` (選択されていない) の場合、ユーザープロファイルページは管理者のみにユーザーのグループを表示します。デフォルト値は `false` です。

ユーザーのグループへの自己加入

このオプションは、加入可能なグループにユーザーが自分自身を追加できるかどうかを指定します。この値が false の場合、ユーザーのグループメンバーシップを変更できるのは管理者のみです。デフォルト値は `false` です。

注	このオプションは、「ユーザーのグループを表示」オプションが選択されている場合だけ適用されます。

ユーザープロファイル表示オプション

このメニューは、どのサービス属性がユーザープロファイルページに表示されるかを指定します。管理者は次の中から選択できます。

- `UserOnly` - そのユーザーに割り当てられたサービスの、表示可能なユーザースキーマ属性を表示します。

  属性にキーワード「表示」が含まれている場合、ユーザーはユーザーサービス属性の値を見ることができます。詳細は、『Sun ONE Identity Server Customization and API Guide』を参照してください。

- `Combined` - そのユーザーに割り当てられたサービスの、表示可能なユーザーおよびダイナミックスキーマ属性を表示します。

ユーザー作成のデフォルトロール

このリストは、新規に作成されたユーザーに自動的に割り当てるロールを定義します。デフォルト値はありません。管理者は 1 つまたは複数のロールの DN を入力できます。

注 このフィールドに指定できるのは、完全識別名のアドレスのみです。ロール名は指定できません。

表示メニューエントリ

このフィールドは、コンソールの上部にある「表示」メニューに表示されるサービスの Java クラスを一覧表示します。構文は、`i18N キー | Java クラス名`です。i18N キーは、「表示」メニューのエントリのローカル名に使用します。

検索で返される結果の最大数

このフィールドは検索で返される結果の最大数を定義します。デフォルト値は 100 です。

警告 この属性に大きな値を設定するときは注意してください。サイズの制限については、次の場所にある『Sun ONE Directory Server インストールおよびチューニングガイド』を参照してください。

`http://docs.sun.com/db/doc/816-6697-10`

検索のタイムアウト (秒)

このフィールドは検索を開始してからタイムアウトするまでの時間 (秒数) を定義します。これは長くかかる可能性のある検索を停止するために使用します。最大検索時間に達すると、エラーが返されます。デフォルト値は 5 秒です。

JSP ディレクトリ名

このフィールドは、コンソールを構築するのに使用する .jsp ファイルを含むディレクトリの名前を指定し、組織に異なった外観を与えます (カスタマイズ)。.jsp ファイルは、このフィールドで指定されたディレクトリにコピーする必要があります。

オンラインヘルプドキュメント

このフィールドは、Identity Server ヘルプのメインページ上に作成されるオンラインヘルプリンクをリスト表示します。これにより、ほかのアプリケーションは、そのオンラインヘルプリンクを Identity Server ページに追加できます。この属性の形式は次のとおりです。

linki18nkey | クリックしたときにロードする html ページ | i18n プロパティファイル

次に例を示します。

IdentityServer Help | /AMAdminHelp.html | amAdminModuleMsgs

必要なサービス

このフィールドは、ユーザーが作成されたときにダイナミックにユーザーのエントリに追加されるサービスをリスト表示します。管理者は、作成時にどのサービスを追加するかを選択できます。

この属性は、コンソールではなく、Identity Server SDK によって使用されます。ダイナミックに作成されるユーザーと、amadmin コマンド行ユーティリティーで作成されるユーザーには、この属性に含まれているサービスが割り当てられます。

ユーザー検索キー

この属性は、ナビゲーションページで単純検索を実行するときに検索対象となる属性の名前を定義します。この属性のデフォルト値は cn です。たとえば、この属性がデフォルト値を使用している場合は、次のようになります。

ナビゲーションフレームの「名前」フィールドに j* を入力すると、「j」または「J」で始まる名前が表示されます。

ユーザー検索により返される属性

このフィールドは、単純検索から返されるユーザーを表示するときに使用する属性名を定義します。この属性のデフォルトは uid cn です。ユーザー ID とユーザーのフルネームが表示されます。

先頭に表示される属性名は、返されるユーザーのセットをソートするためのキーとしても使用されます。パフォーマンスが低下しないようにするには、ユーザーのエントリに値が設定されている属性を使用します。

ユーザー作成通知リスト

このフィールドは、新しいユーザーが作成されたときに通知を送る電子メールアドレスのリストを定義します。次の構文で示されているように、複数の電子メールアドレスを指定できます。

電子メール | ロケール | *Charset*

電子メール | ロケール | *Charset*

電子メール | ロケール | *Charset*

通知リストには、|locale オプションを使って異なるロケールを指定することもできます。たとえばフランスにいる管理者に通知を送信するには、次のようにします。

```
someuser@example.com|fr|fr
```

ロケールの一覧については、201 ページの表 19-1 を参照してください。

注 amProfile.properties のプロパティ 497 を修正することで、送信元の電子メール ID を変更できます。このファイルは、デフォルトで IdentityServer_base/Identity-Server/SUNWam/locale にあります。

ユーザー削除通知リスト

このフィールドは、ユーザーが削除されたときに通知を送る電子メールアドレスのリストを定義します。次の構文で示されているように、複数の電子メールアドレスを指定できます。

電子メール | ロケール | *Charset*

電子メール | ロケール | *Charset*

電子メール | ロケール | *Charset*

通知リストには、|locale オプションを使って異なるロケールを指定することもできます。たとえばフランスにいる管理者に通知を送信するには、次のようにします。

```
someuser@example.com|fr|fr
```

ロケールの一覧については、201 ページの表 19-1 を参照してください。

注 amProfile.properties のプロパティ 497 を修正することで、送信元の電子メール ID を変更できます。このファイルは、デフォルトで IdentityServer_base/Identity-Server/SUNWam/locale にあります。デフォルトの送信元 ID は DSAME です。

ユーザー修正通知リスト

このフィールドは、属性および属性に関連する電子メールアドレスのリストを定義します。リストに定義された属性でユーザーの修正が発生すると、その属性に関連する電子メールアドレスに通知が送信されます。各属性は、それぞれ異なるセットの関連アドレスを持つことができます。次の構文で示されているように、複数の電子メールアドレスを指定できます。

属性名 電子メール | ロケール | *Charset* 電子メール | ロケール | *Charset* .....

属性名 電子メール | ロケール | *Charset* 電子メール | ロケール | *Charset* .....

アドレスのいずれか 1 つに self キーワードを使用することもできます。このキーワードを使用すると、プロファイルが修正されたユーザーにメールが送信されます。

次に例を示します。

```
manager someuser@sun.com|self|admin@sun.com
```

この場合、manager 属性で指定されたアドレス、someuser@sun.com、admin@sun.com およびユーザーを修正した人 (self) にメールが送信されます。

通知リストには、|locale オプションを使って異なるロケールを指定することもできます。たとえばフランスにいる管理者に通知を送信するには、次のようにします。

```
manager someuser@sun.com|self|admin@sun.com|fr
```

ロケールの一覧については、201 ページの表 19-1 を参照してください。

注 属性名は Directory Server スキーマに表示されるのと同じものですが、コンソールの表示名とは違います。

ページごとの最大エントリ数

この属性を使用して、ページあたりに表示できる最大行数を定義することができます。デフォルトは 25 です。たとえばユーザー検索結果が 100 行の場合、1 ページあたり 25 行のページが 4 ページ表示されます。

表示オプション

この属性では、Identity Server コンソールの表示オプションを設定するための値を追加できます。値を入力し、「追加」をクリックして、表示オプションを設定します。使用できる値は次のとおりです。

表 16-1 表示オプションの値

パラメータ	説明と構文
generateUserCN	true に設定すると、ユーザーの作成時にダイナミックにユーザー CN を生成する。デフォルトは false 構文 `generateUserCN=[false|true]`
userAttributeNameForProfileTitle	ユーザープロファイルページのタイトルに表示されるユーザー属性の値を指定する。デフォルトは uid 構文 `userAttributeNameForProflleTitle=[uid| ユーザー属性 ]`

表 16-1　表示オプションの値 (続き)

パラメータ	説明と構文
autoSelect	true (デフォルト) に設定すると、Identity Server では、ナビゲーション表示内の、指定されたアイデンティティオブジェクトの最初の項目を自動的に選択する 構文 `autoselect=[true|false]`
disableIntitialSearch	1 つまたは複数のアイデンティティオブジェクトタイプに対する Identity Server の初期検索を無効にする。初期検索を無効にすると、Identity Server コンソールを表示する時間が短くなる。この指示に対応するコンソールのサービス属性は、管理サービスの組織属性である「表示オプション」。このコンソールオプションは、`com.iplanet.am.console.display.off` に定義されたどの値よりも優先する。このプロパティを `AMConfig.properties` で設定する場合は、コンソールを使用して設定しないこと。逆も同様 構文 (複数の値はカンマで区切る) `disableInitialSearch=[users|organizaitons|peopleContainers|organizationalUnits|roles|groups|policies]`
defaultUserView	ユーザープロファイルページの「表示」メニューでのデフォルトの表示を設定する。デフォルトですべての値が設定されている 構文 `defaultUserView=[roles|groups|services|IplanetAMUserService|` サービス名 `]`
defaultGroupView	グループプロファイルページの「表示」メニューでのデフォルトの表示を設定する。デフォルトですべての値が設定されている 構文 `defaultGroupView=[general|users]`

表 16-1　表示オプションの値 (続き)

パラメータ	説明と構文
defaultRoleView	ロールプロファイルページの「表示」メニューでのデフォルトの表示を設定する。デフォルトですべての値が設定されている 構文 `defaultRoleView=[general|users|services]`
defaultPolicyView	ポリシープロファイルページの「表示」メニューでのデフォルトの表示を設定する。デフォルトですべての値が設定されている 構文 `defaultPolicyView=[general|rules|subjects|referrals|conditions]`
defaultFederationHostedProviderView	連携管理モジュールのホストプロバイダプロファイルページの「表示」メニューでのデフォルトの表示を設定する。デフォルトですべての値が設定されている 構文 `defaultFederationHostedProviderView=[general|serviceProvider|identityProvider|authenticaionDomain|trustedProviders|identityServerConfiguration]`
defaultFederationRemoteProviderView	連携管理モジュールのリモートプロバイダプロファイルページの「表示」メニューでのデフォルトの表示を設定する。デフォルトですべての値が設定されている 構文 `defaultFederationRemoteProviderView=[general|serviceProvider|identityProvider|authenticaionDomain]`

表 16-1　表示オプションの値 (続き)

パラメータ	説明と構文
rootNavMenu	ルートサフィックスのナビゲーション表示に対するアイデンティティオブジェクトのデフォルトの表示を設定する。デフォルトですべての値が設定されている 構文 `rootNavMenu=[organizations|organizationalUnits|groupContainers|peopleContainers|roles|groups|users|policies]`
organizationNavMenu	組織のナビゲーション表示に対するアイデンティティオブジェクトのデフォルトの表示を設定する。デフォルトですべての値が設定されている 構文 `organizationNavMenu=[organizations|organizationalUnits|groupContainers|peopleContainers|roles|groups|users|policies]`
groupContainerNavMenu	グループコンテナのナビゲーション表示に対するアイデンティティオブジェクトのデフォルトの表示を設定する。デフォルトですべての値が設定されている 構文 `groupContainerNavMenu=[groupContainers|groups]`
peopleContainerNavMenu	ピープルコンテナのナビゲーション表示に対するアイデンティティオブジェクトのデフォルトの表示を設定する。デフォルトですべての値が設定されている 構文 `peopleContainerNavMenu=[peopleContainers|users]`

表 16-1　表示オプションの値 (続き)

パラメータ	説明と構文
federationNavMenu	連携管理モジュールのナビゲーション表示に対するアイデンティティオブジェクトのデフォルトの表示を設定する。デフォルトですべての値が設定されている 構文 `federationNavMenu=[authenticationDomains|hostedProviders|remoteProviders]`
userProfileMenu	ユーザープロファイルページの表示メニューのサブエントリに対するデフォルトの表示を設定する。デフォルトですべての値が設定されている 構文 `userProfileMenu=[roles|groups|services|iPlanetAMUserService|`*service name]*
groupProfileMenu	グループプロファイルページの表示メニューのサブエントリに対するデフォルトの表示を設定する。デフォルトですべての値が設定されている 構文 `groupProfileMenu=[general|users]`
roleProfileMenu	ロールプロファイルページの表示メニューのサブエントリに対するデフォルトの表示を設定する。デフォルトですべての値が設定されている 構文 `roleProfileMenu=[general|users|services]`
policyProfileMenu	ポリシープロファイルページの表示メニューのサブエントリに対するデフォルトの表示を設定する。デフォルトですべての値が設定されている 構文 `policyProfileMenu=[general|rules|subjects|referrals|conditions]`

表 16-1　表示オプションの値 (続き)

パラメータ	説明と構文
federationRemoteProviderProfileMenu	連携リモートプロバイダプロファイルページの表示メニューのサブエントリに対するデフォルトの表示を設定する。デフォルトですべての値が設定されている 構文 `federationRemoteProviderProfileMenu=[general|serviceProvider|identityProvider|authenticationDomain]`
FederationHostedProviderProfileMenu	連携ホストプロバイダプロファイルページの表示メニューのサブエントリに対するデフォルトの表示を設定する。デフォルトですべての値が設定されている 構文 `federationHostedProviderProfileMenu=[general|serviceProvider|identityProvider|authenticationDomain|trustedProviders|identityServerConfiguration]`

イベントリスナークラス

この属性には、作成、修正、および削除の各イベントを Identity Server コンソールから受け取るリスナーの一覧が格納されています。

プレおよびポストプロセスクラス

このフィールドは、ユーザー、組織、ロール、およびグループに対するプレおよびポストプロセス操作中にコールバックを受け取るように、`com.iplanet.am.sdk.AMCallBack` クラスを拡張する実装クラスの一覧を、プラグインを通じて定義します。操作は次のとおりです。

- 作成
- 削除
- 修正
- ユーザーをロールまたはグループに追加
- ユーザーをロールまたはグループから削除

プラグインの完全なクラス名を入力する必要があります。次に例を示します。

```
com.iplanet.am.sdk.AMCallbacSample
```

そして、プラグインクラスの場所へのフルパスを含むように、Web コンテナのクラスパスを変更する必要があります。これは Identity Server のインストール単位で行います。

外部属性のフェッチを有効

このオプションは、プラグインで外部属性を受け取れるように、コールバックを有効にします。外部属性とは、外部アプリケーション固有の属性のことです。外部属性は Identity Server SDK ではキャッシュされません。そのためこの属性を使用すると、組織単位のレベルで属性を受け取ることができるようになります。このオプションは、デフォルトでは無効になっています。

第 17 章

匿名認証属性

匿名認証属性は組織属性です。サービス設定の下で組織属性に適用される値は、匿名認証テンプレートのデフォルト値になります。組織にサービスを登録した後、サービステンプレートを作成する必要があります。デフォルト値は組織の管理者が登録後に変更できます。組織属性は組織のサブツリーのエントリに継承されません。匿名認証属性は次のとおりです。

- 有効な匿名ユーザーリスト
- 大文字と小文字を区別するユーザー名
- デフォルトの匿名ユーザー名
- 認証レベル

有効な匿名ユーザーリスト

このフィールドには、資格を指定しないでログインする権限のあるユーザー ID のリストが含まれています。ユーザーのログイン名がこのリストのユーザー ID と一致すれば、アクセスが許可され、指定したユーザー ID にセッションが割り当てられます。

このリストが空の場合、ユーザーは次のデフォルトモジュールログイン URL にアクセスすると、デフォルトの匿名ユーザー名として認証を受けます。

```
protocol://server_host.server_domain:server_port/server_deploy_uri/
UI/Login?module=Anonymous&org=org_name
```

このリストが空でない場合、ユーザーはデフォルトモジュールログイン URL (上記と同じ) にアクセスすると、有効な匿名ユーザー名を入力するよう求められます。

このリストが空でない場合、ユーザーは次の URL にアクセスすると、ログインページを表示せずにログインできます。

```
protocol://server_host.server_domain:server_port/server_deploy_uri/
UI/Login?module=Anonymous&org=org_name&IDToken1=<有効な匿名ユーザー名>
```

大文字と小文字を区別するユーザー名

有効にすると、ユーザー ID の大文字小文字を区別するようになります。デフォルトでは、無効になっています。

デフォルトの匿名ユーザー名

このフィールドは、有効な匿名ユーザーリストが空の場合で、次のデフォルトモジュールログイン URL がアクセスされたときに、セッションを割り当てるユーザー ID を定義します。

```
protocol://server_host.server_domain:server_port/server_deploy_uri/UI/Login?module=Anonymous&org=org_name
```

デフォルト値は anonymous です。匿名ユーザーは組織にも作成する必要があります。

注　有効な匿名ユーザーリストが空でない場合、デフォルトの匿名ユーザー名に定義されたユーザーを使用すると、ログインページにアクセスせずにログインできます。そのためには、次の URL にアクセスします。

```
protocol://server_host.server_domain:server_port/server_deploy_uri/UI/Login?module=Anonymous&org=org_name&IDToken1=< デフォルトの匿名ユーザー名 >
```

認証レベル

認証レベルは認証方法ごとに個別に設定します。この値は、認証の信頼度を示します。ユーザーが認証を受けると、この値がセッションの SSO トークンに格納されます。ユーザーがアクセスしたいアプリケーションに SSO トークンが提供されると、そのアプリケーションは格納されている値を使用して、ユーザーにアクセスを許可するのに十分なレベルかどうかを判別します。SSO トークンに格納されている認証レベルが必要な最小値に満たない場合、アプリケーションはユーザーにより高い認証レベルのサービスで認証を再度受けるよう要求することがあります。デフォルト値は 0 です。

注　認証レベルの指定がない場合、SSO トークンはコア認証属性のデフォルト認証レベルで指定した値を格納します。詳細は、206 ページの「デフォルト認証レベル」を参照してください。

第 18 章

証明書認証属性

証明書認証属性は組織属性です。サービス設定の下で組織属性に適用される値は、証明書認証テンプレートのデフォルト値になります。組織にサービスを登録した後、サービステンプレートを作成する必要があります。デフォルト値は組織の管理者が登録後に変更できます。組織属性は組織のサブツリーのエントリに継承されません。証明書認証属性は次のとおりです。

- LDAP での証明書のマッチング
- LDAP 検索で使用するサブジェクト DN の属性
- CRL に対する証明書のマッチング
- CRL 検索で使用する発行者 DN の属性
- OCSP 検証を有効
- LDAP サーバーとポート
- LDAP 検索の開始 DN
- LDAP サーバーの主体ユーザー
- LDAP サーバーの主体パスワード
- プロファイル ID のための LDAP 属性
- LDAP アクセスで SSL を有効
- ユーザープロファイルへのアクセスに使用する証明書のフィールド
- ユーザープロファイルへのアクセスに使用する証明書のほかのフィールド
- 信頼できるリモートホスト
- SSL ポート番号
- 認証レベル

LDAP での証明書のマッチング

このオプションは、ログイン時に提出されたユーザー証明書が LDAP サーバに格納されているかをチェックするかどうかを指定します。一致する証明書がない場合、ユーザーはアクセスを拒否されます。一致する証明書があり、かつほかの検証が必要ない場合、ユーザーはアクセスを許可されます。デフォルトでは、証明書認証サービスはユーザー証明書をチェックしません。

注	Directory Server に格納されている証明書は必ずしも有効とはかぎりません。190 ページの「CRL に対する証明書のマッチング」を参照してください。ただし、ログイン時に提出されたユーザー証明書が有効かどうかを Web コンテナでチェックすることはできます。

LDAP 検索で使用するサブジェクト DN の属性

このフィールドは、LDAP で証明書を検索するのに使用する証明書の `SubjectDN` 値の属性を指定します。ユーザーエントリを一意に特定する属性でなければなりません。検索には実際の値を使用します。デフォルト値は `CN` です。

CRL に対する証明書のマッチング

このオプションは、ユーザー証明書と LDAP サーバの証明書の取り消しリスト (CRL) を比較するかどうかを指定します。CRL は、発行者の `SubjectDN` に含まれている属性名のいずれかによって特定されます。証明書が CRL に載っている場合ユーザーはアクセスを拒否され、載っていない場合は許可されます。デフォルトでは、この属性は無効になっています。

注	証明書の所有者の状態が変わってその証明書を使う権利がなくなった場合、または証明書の所有者の秘密鍵が漏洩した場合は、証明書を取り消す必要があります。

CRL 検索で使用する発行者 DN の属性

このフィールドは、LDAP で CRL を検索するのに使用する、受信した証明書の発行者 SubjectDN 値の属性を指定します。このフィールドは、CRL に対する証明書のマッチング属性が有効になっているときだけ使用されます。検索には実際の値を使用します。デフォルト値は CN です。

OCSP 検証を有効

このパラメータは、対応する OCSP レスポンダと連絡することによって実行される OCSP 検証を有効にします。OCSP レスポンダは、実行時に次のように決定されます。

- com.sun.identity.authentication.ocspCheck が true の場合で、OCSP レスポンダが com.sun.identity.authentication.ocsp.repsonder.url 属性で設定されているときは、この属性の値が OCSP レスポンダとして使用されます。
- com.sun.identity.authentication.ocspCheck が true に設定されている場合で、この属性の値が AMConfig.properties ファイルで設定されていないときは、クライアント証明書に示されている OCSP レスポンダが OCSP レスポンダとして使用されます。

com.sun.identity.authentication.ocspCheck が false に設定されている場合や、com.sum.identity.authentication.ocspCheck が true に設定されているが OCSP レスポンダが見つからない場合は、OCSP 検証は実行されません。

注　OCSP 検証を有効にする前に、Identity Server マシンと OCSP レスポンダマシンの時刻ができるかぎり一致するようにしてください。また、Identity Server マシンの時刻が OCSP レスポンダの時刻より遅れないようにすることが必要です。次に例を示します。

OCSP レスポンダマシン - 12:00:00 pm

Identity Server マシン - 12:00:30 pm

LDAP サーバーとポート

このフィールドは証明書を格納する LDAP サーバーの名前とポート番号を指定します。デフォルト値は、Identity Server のインストール時に指定したホスト名とポートです。証明書が格納されている LDAP サーバーのホスト名とポートを使用できます。形式は *hostname:port* です。

LDAP 検索の開始 DN

このフィールドは、ユーザーの証明書に対する検索を開始するノードの DN を指定します。デフォルト値はありません。このフィールドは有効な DN をすべて認識します。複数のエントリの場合は、ローカルサーバー名をプレフィックスとして付ける必要があります。

LDAP サーバーの主体ユーザー

このフィールドは、証明書が格納されている LDAP サーバーの主体ユーザー (通常はディレクトリマネージャ) の DN を受け入れます。このフィールドにデフォルト値はありません。有効な DN をすべて認識します。主体ユーザーは読み取り権限を持ち、Directory Server に格納されている証明書情報を検索する必要があります。

LDAP サーバーの主体パスワード

このフィールドは、LDAP サーバーの主体ユーザーフィールドで指定されるユーザーに関連付けられた LDAP パスワードを保持します。このフィールドにデフォルト値はありません。指定した主体ユーザーの有効な LDAP パスワードを認識します。

注	この値は読み取り可能テキストとしてディレクトリに格納されます。

プロファイル ID のための LDAP 属性

このフィールドは、証明書と一致する Directory Server エントリの属性を指定します。この証明書の値は、正しいユーザープロファイルの識別に使用します。このフィールドにデフォルト値はありません。ユーザー ID として使用できるユーザーエントリ (cn、sn など) の有効な属性をすべて認識します。

LDAP アクセスで SSL を有効

このオプションは LDAP サーバーへのアクセスに SSL を使用するかどうかを指定します。デフォルトでは、証明書認証サービスは LDAP アクセスに SSL を使用しません。

ユーザープロファイルへのアクセスに使用する証明書のフィールド

このメニューでは、一致するユーザープロファイルの検索に使用する証明書のフィールドを指定します。たとえば、`email address` を選択すると、証明書認証サービスはユーザー証明書の属性 `emailAddr` に一致するユーザープロファイルを検索します。その後、ログインするユーザーは一致したプロファイルを使用します。デフォルトのフィールドは `subject CN` です。リストは次のとおりです。

- email address
- subject CN
- subject DN
- subject UID
- other

ユーザープロファイルへのアクセスに使用する証明書のほかのフィールド

ユーザープロファイルへのアクセスに使用する証明書のフィールド属性の値が `other` に設定されている場合は、このフィールドは、受信した証明書の `subjectDN` 値から選択する属性を指定します。認証サービスは、その属性の値に一致するユーザープロファイルを検索します。

信頼できるリモートホスト

この属性では、証明書を Identity Server に送信できると信頼されている、信頼できるホストの一覧を定義します。Identity Server では、証明書がこれらのホストの 1 つから送信されているかどうかを確認する必要があります。この設定は Sun ONE Portal Server でのみ使用されます。

SSL ポート番号

この属性は、SSL (Secure Socket Layer) 用のポート番号を指定します。現在、この属性は Gateway サーブレットでのみ使用されます。SSL ポート番号の追加や変更を行う前に、『Sun ONE Identity Server Customization and API Guide』の第 7 章の「Policy-Based Resource Management」を参照してください。

認証レベル

認証レベルは認証方法ごとに個別に設定します。この値は、認証の信頼度を示します。ユーザーが認証を受けると、この値がセッションの SSO トークンに格納されます。ユーザーがアクセスしたいアプリケーションに SSO トークンが提供されると、そのアプリケーションは格納されている値を使用して、ユーザーにアクセスを許可するのに十分なレベルかどうかを判別します。SSO トークンに格納されている認証レベルが必要な最小値に満たない場合、アプリケーションはユーザーにより高い認証レベルのサービスで認証を再度受けるよう要求することがあります。デフォルト値は `0` です。

注　認証レベルの指定がない場合、SSO トークンはコア認証属性のデフォルト認証レベルで指定した値を格納します。詳細は、206 ページの「デフォルト認証レベル」を参照してください。

第 19 章

コア認証属性

コア認証サービスは、デフォルトの認証サービス、および認証 SPI で作成するカスタム認証サービスのための基本サービスです。コア認証は、どの形式であれ認証を使用する組織ごとのサービスとして設定する必要があります。コア認証属性はグローバルおよび組織属性から構成されます。グローバル属性に適用される値は Sun ONE Identity Server 設定全体に適用され、設定済みのすべての組織に継承されます。グローバル属性の目的は Identity Server アプリケーションのカスタマイズであるため、ロールまたは組織に直接適用することはできません。サービス設定の下で組織属性に適用される値が、コア認証テンプレートのデフォルト値になります。組織にサービスを登録した後、サービステンプレートを作成する必要があります。デフォルト値は組織の管理者が登録後に変更できます。組織属性は組織のエントリに継承されません。コア認証属性は次のように分けられます。

- グローバル属性
- 組織属性

グローバル属性

コア認証サービスのグローバル属性には、次のものがあります。

- プラグイン可能な認証モジュールクラス
- クライアント用にサポートされている認証モジュール
- LDAP 接続のプールサイズ
- LDAP 接続のデフォルトプールサイズ

プラグイン可能な認証モジュールクラス

このフィールドは、Identity Server プラットフォーム内で設定されるどの組織でも利用できる認証モジュールの Java クラスを指定します。デフォルトでは、LDAP、Safeword、SecurID、Application、Anonymous、HTTP Basic、Membership、UNIX、Certificate、NT、および RADIUS があります。Identity Server には、ほかの認証サービスを追加するのに使用できる公開 SPI も含まれています。新しいサービスを定義するには、新しい各認証サービスの完全クラス名 (パッケージ名を含む) を取得するテキスト文字列をこのフィールドに入力する必要があります。

クライアント用にサポートされている認証モジュール

この属性は、特定のクライアント用にサポートされている認証モジュールのリストを指定します。形式は次のとおりです。

```
clientType | module1,module2,module3
```

この属性は、クライアントディテクションが有効になっているときに機能します。

LDAP 接続のプールサイズ

この属性は、特定のサーバーおよびポートで使用される最大および最小の接続プールを指定します。この属性は、LDAP およびメンバーシップ認証サービス専用です。形式は次のとおりです。

```
host:port:min:max
```

注	この接続プールは、`serverconfig.xml` で構成される SDK 接続プールとは異なります。

LDAP 接続のデフォルトプールサイズ

この属性は、すべての LDAP 認証モジュール設定で使用されるデフォルトの最小および最大接続プールを指定します。ホストおよびポートのエントリが LDAP 接続のプールサイズ属性に存在する場合、LDAP 接続のデフォルトプールサイズから最小および最大設定を使用しません。

組織属性

コア認証サービスの組織属性は次のとおりです。

- 組織認証モジュール
- ユーザープロファイル
- 管理者認証
- ダイナミックユーザープロファイル作成のデフォルトロール
- 持続 Cookie モード
- Cookie の最大持続時間 (秒)
- すべてのユーザーのピープルコンテナ
- エイリアス検索属性名
- デフォルト認証レベル
- ユーザーネーミング属性
- デフォルト認証ロケール
- 組織認証設定
- ログイン失敗のロックアウトモード
- ログイン失敗のロックアウト回数
- ログイン失敗のロックアウト間隔 (分)
- ロックアウト通知を送信するための電子メールアドレス
- ユーザーに警告する失敗回数
- ログイン失敗のロックアウト持続時間 (分)
- ロックアウト属性名
- ロックアウト属性値
- デフォルト成功ログイン URL
- デフォルト失敗ログイン URL
- 認証ポストプロセスクラス
- ユーザー名ジェネレータモード
- プラグイン可能なユーザー名ジェネレータクラス

組織認証モジュール

このリストは組織で利用できる認証モジュールを指定します。管理者は組織ごとに固有の認証タイプを選ぶことができます。複数の認証モジュールには柔軟性がありますが、ユーザーはログイン設定が選択した認証モジュールに適合することを確認する必要があります。デフォルトの認証は LDAP です。Identity Server に含まれている認証サービスは次のとおりです。

- LDAP
- 証明書
- 匿名
- HTTP 基本
- メンバーシップ
- NT
- SafeWord
- RADIUS
- SecurID
- UNIX

注 管理者は作成済み組織にコアおよび認証モジュールのテンプレートを作成、通知して、その組織が正しく機能するようにする必要があります。

ユーザープロファイル

このオプションを使用すると、ユーザープロファイルのオプションを指定することができます。

- 必須 - 認証が成功した場合に認証サービスで SSOToken を発行するには、Identity Server とともにインストールされたローカル Directory Server 内にユーザーのプロファイルが存在している必要があることを指定します。
- ダイナミックに作成 - 認証が成功した場合で、ユーザープロファイルがまだ存在していないときに、認証サービスによってユーザープロファイルを作成することを指定します。作成後、SSOToken が発行されます。ユーザープロファイルは、Identity Server とともにインストールされたローカル Directory Server 内に作成されます。
- 無視 - 認証が成功した場合に SSOToken を発行する認証サービスに対して、ユーザープロファイルが不要であることを指定します。

管理者認証

編集リンクをクリックすることで、管理者専用の認証サービスを定義することができます。管理者とは、Identity Server コンソールにアクセスする必要があるユーザーのことです。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。Identity Server コンソールにアクセスするときは、この属性で設定されているモジュールが使用されます。

ダイナミックユーザープロファイル作成のデフォルトロール

このフィールドは、ダイナミック作成が選択されている場合に、プロファイルが 198 ページの「ユーザープロファイル」機能で作成された新しいユーザーに割り当てるロールを指定します。デフォルト値はありません。管理者は、新しいユーザーに割り当てられるロールの DN を指定する必要があります。

注	指定するロールは、認証を構成する組織の下にあることが必要です。

持続 Cookie モード

このオプションは、ユーザーがブラウザを再起動したときに認証セッションに戻れるかどうかを指定します。ユーザーセッションは持続 Cookie モードを有効にすれば保持できます。持続 Cookie モードを有効にすると、ユーザーセッションは持続 Cookie の期限が切れるか、ユーザーが意図的にログアウトするまで期限切れにはなりません。期限は Cookie の最大持続時間 (秒) で指定します。デフォルトでは、持続 Cookie モードが無効になっており、認証サービスはメモリの Cookie だけを使用します。

注	持続 Cookie は、クライアントがログイン URL の `iPSPCookie=yes` パラメータを使用して明示的に要求する必要があります。

Cookie の最大持続時間 (秒)

このフィールドは、持続 Cookie の期限が切れるまでの間隔を指定します。チェックボックスを選択して持続 Cookie モードを有効にする必要があります。この間隔は、ユーザーのセッションの認証が成功したときに始まります。デフォルト値は 2147483 (秒) です。このフィールドは、0 から 2147483 までの任意の整数値を取得できます。

すべてのユーザーのピープルコンテナ

ユーザー認証が成功したあと、ユーザーのプロファイルを検索します。このフィールドの値は、プロファイルの検索先を指定します。一般に、この値はデフォルトのピープルコンテナの DN です。組織に追加されるすべてのユーザーエントリは、自動的にその組織のデフォルトピープルコンテナに追加されます。デフォルト値は ou=People です。一般に、組織名とルートサフィックスで構成されます。このフィールドは組織単位の有効な DN を取得します。

注

認証では、次の方法でユーザープロファイルを検索します。

- デフォルトのピープルコンテナの下を検索し、次に
- デフォルトの組織の下を検索し、さらに
- エイリアス検索属性名の属性を使用して、デフォルトの組織内でユーザーを検索します。

最後に SSO を検索しますが、その場合認証に使用するユーザー名がプロファイルのネーミング属性でないことがあります。たとえば、uid=jamie というプロファイルを持つユーザーが、jn10191 という SafeWord ID を使用して認証を受ける場合などです。

エイリアス検索属性名

ユーザー認証が成功したあと、ユーザーのプロファイルを検索します。このフィールドは、201 ページの「ユーザーネーミング属性」で指定する最初の LDAP 属性に対する検索で一致するユーザープロファイルを見つけられなかった場合に、次に検索する LDAP 属性を指定します。この属性は主に、認証モジュールから返されたユーザーアイデンティティがユーザーネーミング属性で指定したものと異なる場合に使用します。たとえば、RADIUS サーバーが abc1234 を返しても、ユーザー名は abc という可能性があります。この属性のデフォルト値はありません。このフィールドは有効な LDAP 属性をすべて取得します (たとえば、cn)。

ユーザーネーミング属性

ユーザー認証が成功したあと、ユーザーのプロファイルを検索します。この属性の値は、検索に使用する LDAP 属性を指定します。デフォルトでは、Identity Server はユーザーエントリが `uid` 属性によって識別されるものと想定します。Directory Server で異なる属性 (`givenname` など) を使用している場合は、このフィールドにその属性名を指定します。

デフォルト認証ロケール

このフィールドは、認証サービスが使用するデフォルトの言語サブタイプを指定します。デフォルト値は `en_US` です。有効な言語サブタイプの一覧を表 19-1 に示します。

別のロケールを使用するには、最初にそのロケールのすべての認証テンプレートを作成する必要があります。次に、それらのテンプレートの新しいディレクトリを作成する必要があります。詳細は、『Sun ONE Identity Server Customization and API Guide』の第 3 章「認証サービス」を参照してください。

表 19-1 サポートされている言語ロケール

言語タグ	言語
af	アフリカーンス語
be	ベラルーシ語
bg	ブルガリア語
ca	カタロニア語
cs	チェコ語
da	デンマーク語
de	ドイツ語
el	ギリシャ語
en	英語
es	スペイン語
eu	バスク語
fi	フィンランド語
fo	フェロー語

表 19-1　サポートされている言語ロケール (続き)

言語タグ	言語
fr	フランス語
ga	アイルランド語
gl	ガリシア語
hr	クロアチア語
hu	ハンガリー語
id	インドネシア語
is	アイスランド語
it	イタリア語
ja	日本語
ko	韓国語
nl	オランダ語
no	ノルウェー語
pl	ポーランド語
pt	ポルトガル語
ro	ルーマニア語
ru	ロシア語
sk	スロバキア語
sl	スロベニア語
sq	アルバニア語
sr	セルビア語
sv	スウェーデン語
tr	トルコ語
uk	ウクライナ語
zh	中国語

組織認証設定

この属性は、組織の認証モジュールを設定します。デフォルトの認証モジュールは LDAP です。編集リンクをクリックすると、1 つまたは複数の認証モジュールを選択できます。複数のモジュールが選択された場合、ユーザーはそれらのモジュールの連鎖に沿ってすべての認証に成功する必要があります。

ユーザーが `/server_deploy_uri/UL/Login` 形式を使って認証モジュールにアクセスするとき、この属性に設定されたモジュールが認証に使用されます。詳細は、『Sun ONE Identity Server Customization and API Guide』を参照してください。

ログイン失敗のロックアウトモード

この機能は、最初の認証に失敗した場合に再試行を許可するかどうかを指定します。この属性を選択すると、ロックアウトが有効になります。その場合、ユーザーには 1 回だけ認証を受ける機会が与えられます。デフォルトでは、ロックアウト機能は無効になっています。この属性は、ロックアウト関連および通知関連の属性とともに機能します。

ログイン失敗のロックアウト回数

この属性は、ログイン失敗のロックアウト間隔 (分) で定義された時間内に、ユーザーが認証を試みることができる回数を定義します。この回数を超えると、ユーザーはロックアウトされます。

ログイン失敗のロックアウト間隔 (分)

この属性は、ログインが失敗した場合の、次の再試行までの時間を分単位で定義します。ログイン失敗の後、ロックアウト間隔以内にもう一度ログインが失敗すると、ロックアウト回数が増分されます。それ以外の場合は、ロックアウト回数がリセットされます。

ロックアウト通知を送信するための電子メールアドレス

この属性は、ユーザーのロックアウトが発生した場合に通知を受け取る電子メールアドレスを指定します。電子メール通知を複数のアドレスに送信する場合は、電子メールアドレスをスペースで区切ります。

ユーザーに警告する失敗回数

この属性は、認証に失敗した場合、Identity Server がそのユーザーにロックアウトされるという警告を送信するまでに許可される認証失敗の回数を指定します。

ログイン失敗のロックアウト持続時間 (分)

この属性を選択すると、メモリロックが有効になります。デフォルトでは、このロックアウトメカニズムにより、ロックアウト属性名で定義されているユーザープロファイルが無効になります (ログイン失敗後)。ログイン失敗のロックアウト持続時間 が 0 より大きい値に設定されている場合は、その時間だけメモリとユーザーアカウントがロックされます。

ロックアウト属性名

この属性は、ロックアウトする LDAP 属性を指定します。この属性名のロックアウトを有効にするには、ロックアウト属性値の値も変更する必要があります。デフォルトでは、Identity Server コンソールで「ロックアウト属性名」は空になっています。デフォルトの実装値は、`inetuserstatus` (LDAP 属性) と `inactive` です。ログイン失敗のロックアウト持続時間が 0 に設定されている場合で、ユーザーがロックアウトされたときに適用されます。

ロックアウト属性値

この属性は、ロックアウト属性名で指定されている属性について、ロックアウトを有効にするかどうかを指定します。デフォルトでは、`inetuserstatus` に対して、この値は 0 に設定されています。

デフォルト成功ログイン URL

このフィールドは、認証の成功後にユーザーをリダイレクトする URL を指定します。このフィールドは有効な URL を取得できます。成功ログイン URL は、`remote-auth.dtd` 内の `LoginStatus` 要素で設定されます。詳細は、『Sun ONE Identity Server Customization and API Guide』を参照してください。

デフォルト失敗ログイン URL

このフィールドは、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。このフィールドは有効な URL を取得できます。失敗ログイン URL は、`remote-auth.dtd` 内の `LoginStatus` 要素で設定されます。詳細は、『Sun ONE Identity Server Customization and API Guide』を参照してください。

認証ポストプロセスクラス

このフィールドは、ログインの成功または失敗後に実行する、認証後プロセスをカスタマイズするための Java クラス名を指定します。次に例を示します。

```
com.abc.authentication.PostProcessClass
```

この Java クラスでは、次の Java インタフェースを実装する必要があります。

```
com.sun.identity.authentication.spi.AMPostAuthProcessInterface
```

また、このクラスが置かれている場所へのパスを、Web Server の Java Classpath 属性に追加する必要があります。

ユーザー名ジェネレータモード

この属性は、メンバーシップ認証モジュールによって使用されます。この属性フィールドが有効になっている場合、すでにユーザー ID が存在していれば、自己登録プロセス中にメンバーシップモジュールによって特定ユーザーのユーザー ID が生成可能です。このユーザー ID は、プラグイン可能なユーザー名ジェネレータクラスで指定された Java クラスから生成されます。

プラグイン可能なユーザー名ジェネレータクラス

このフィールドは、ユーザー名ジェネレータモードが有効になっている場合にユーザー ID を生成するための Java クラス名を指定します。

デフォルト認証レベル

認証レベルの値は、認証の信頼度を示します。ユーザーが認証を受けると、この値がセッションの SSO トークンに格納されます。ユーザーがアクセスしたいアプリケーションに SSO トークンが提供されると、そのアプリケーションは格納されている値を使用してユーザーにアクセスを許可するのに十分なレベルかどうかを判別できます。SSO トークンに格納されている認証レベルが必要な最小値に満たない場合、アプリケーションはユーザーにより高い認証レベルのサービスで認証を再度受けるよう要求することがあります。

認証レベルは、組織の特定の認証テンプレート内で設定する必要があります。ここで説明するデフォルト認証レベルの値は、特定の組織の、認証テンプレートの認証レベルフィールドに認証レベルが指定されていない場合だけ適用されます。デフォルト認証レベルのデフォルト値は 0 です。この属性の値は Identity Server が使用するものではなく、どの外部アプリケーションでもその値の使用を選択すれば使用できます。

第 20 章

HTTP 基本認証属性

HTTP 基本認証属性は組織属性です。サービス設定の下で組織属性に適用される値は、HTTP 基本認証テンプレートのデフォルト値になります。組織にサービスを登録した後、サービステンプレートを作成する必要があります。デフォルト値は組織の管理者が登録後に変更できます。組織属性は組織のエントリに継承されません。

HTTP 基本認証属性は次のとおりです。

認証レベル

認証レベルは認証方法ごとに個別に設定します。この値は、認証の信頼度を示します。ユーザーが認証を受けると、この値がセッションの SSO トークンに格納されます。ユーザーがアクセスしたいアプリケーションに SSO トークンが提供されると、そのアプリケーションは格納されている値を使用して、ユーザーにアクセスを許可するのに十分なレベルかどうかを判別します。SSO トークンに格納されている認証レベルが必要な最小値に満たない場合、アプリケーションはユーザーにより高い認証レベルのサービスで認証を再度受けるよう要求することがあります。デフォルト値は 0 です。

注 認証レベルの指定がない場合、SSO トークンはコア認証属性のデフォルト認証レベルで指定した値を格納します。詳細は、206 ページの「デフォルト認証レベル」を参照してください。

第 21 章

LDAP 認証属性

LDAP 認証属性は組織属性です。サービス設定の下で組織属性に適用される値は、LDAP 認証テンプレートのデフォルト値になります。組織にサービスを登録した後、サービステンプレートを作成する必要があります。デフォルト値は組織の管理者が登録後に変更できます。組織属性は組織のエントリに継承されません。LDAP 認証属性は次のとおりです。

- プライマリ LDAP サーバーとポート
- セカンダリ LDAP サーバーとポート
- ユーザー検索の開始 DN
- root ユーザーバインド DN
- root ユーザーバインドパスワード
- root ユーザーバインドパスワード (確認)
- ユーザーネーミング属性
- ユーザーエントリ検索属性
- ユーザー検索フィルタ
- 検索範囲
- LDAP サーバーに対する SSL を有効
- 認証においてユーザー DN を返す
- LDAP サーバーのチェック間隔
- ユーザー作成の属性リスト
- 認証レベル

プライマリ LDAP サーバーとポート

このフィールドは、Identity Server のインストール時に指定するプライマリ LDAP サーバーのホスト名およびポート番号を指定します。これは、LDAP 認証で最初に通信するサーバーです。形式は `hostname:port` です。ポート番号がないときは、`389` と想定します。

複数のドメインに Identity Server が配備されている場合は、Identity Server および Directory Server の個々のインスタンス間の通信リンクを、次の形式で指定できます。複数のエントリを指定する場合は、エントリにローカルサーバー名をプレフィックスとして付ける必要があります。

```
local_servername|server:port local_servername2|server:port ...
```

たとえば、異なる場所に配備された 2 つの Identity Server (`L1-machine1-IS` および `L2- machine2-IS`) が、それぞれ別の Identity Server インスタンス (`L1-machine1-DS` および `L2-machine2-DS`) と通信する場合は、次のように指定できます。

```
L1-machine1-IS.example.com|L1-machine1-DS.example.com:389
L2-machine2-IS.example.com|L2-machine2-DS.example.com:389
```

セカンダリ LDAP サーバーとポート

このフィールドは、Identity Server プラットフォームが利用できるセカンダリ LDAP サーバーのホスト名およびポート番号を指定します。プライマリ LDAP サーバーが認証要求に応答しない場合は、このサーバーと通信します。プライマリサーバーが起動すると、Identity Server はプライマリサーバーに戻ります。この形式も `hostname:port` です。複数のエントリの場合は、ローカルサーバー名をプレフィックスとして付ける必要があります。

警告 Identity Server を使用する企業から遠隔地にある Directory Server からユーザーを認証する場合は、プライマリとセカンダリ両方の LDAP サーバーポートに値があることが重要です。1 つの Directory Server の場所の値を両方のフィールドに使用できます。

ユーザー検索の開始 DN

このフィールドは、ユーザーの検索を開始するノードの DN を指定します。性能を確保するため、この DN はできる限り固有のものにすることが必要です。デフォルト値は、ディレクトリツリーのルートです。有効な DN はすべて認識されます。複数のエントリの場合は、ローカルサーバー名をプレフィックスとして付ける必要があります。形式は次のとおりです。

`servername|search dn`

複数のエントリを指定する場合は、次のようになります。

`servername1|search dn servername2|search dn servername3|search dn...`

同一の検索で複数のユーザーが見つかった場合、認証は失敗します。

root ユーザーバインド DN

このフィールドは、「プライマリ LDAP サーバーとポート」フィールドで指定した Directory Server に管理者としてバインドするのに使用するユーザーの DN を指定します。ユーザーログイン ID に基づく、一致するユーザー DN を検索するためには、認証サービスをこの DN にバインドする必要があります。デフォルト値は `amldapuser` です。有効な DN はすべて認識されます。

パスワードが間違っているとロックアウトされるので、ログアウトする前にパスワードが正しいことを確認してください。ロックアウトされた場合は、`AMConfig.Properties` ファイル内の `com.iplanet.authentication.super.user` プロパティで指定されているスーパーユーザー DN を使ってログインできます。デフォルトでは、これはログインに通常使用する amAdmin アカウントですが、完全な DN を使用する必要があります。次に例を示します。

`uid_amAdmin,ou=People,`IdentityServer_base

root ユーザーバインドパスワード

このフィールドは、「root ユーザーバインド DN」フィールドで指定される管理者プロファイルのパスワードを指定します。デフォルト値はありません。管理者の有効な LDAP パスワードだけが認識されます。

root ユーザーバインドパスワード (確認)

パスワードの確認。

ユーザーネーミング属性

ユーザー認証が成功したあと、ユーザーのプロファイルを検索します。この属性の値を使用して検索を実行します。このフィールドは、使用する LDAP 属性を指定します。デフォルトでは、Identity Server はユーザーエントリが `uid` 属性によって識別されるものと想定します。Directory Server で異なる属性 (`givenname` など) を使用している場合は、このフィールドにその属性名を指定します。

注 ユーザー検索フィルタは、検索フィルタ属性とユーザーエントリネーミング属性の組み合わせです。

ユーザーエントリ検索属性

このフィールドは、認証を受けるユーザーの検索フィルタを設定するのに使用する属性をリストします。そのため、ユーザーはそのエントリで、複数の属性で認証を受けることができます。たとえば、このフィールドが `uid`、`employeenumber` および `mail` に設定されている場合、ユーザーはこれらの名前のどれを使用しても認証を受けることができます。

ユーザー検索フィルタ

このフィールドは、「ユーザー検索の開始 DN」フィールドの下でユーザーの検索に使用する属性を指定します。これはユーザーエントリネーミング属性とともに機能します。デフォルト値はありません。有効なユーザーエントリ属性はすべて認識されます。

検索範囲

このメニューは、一致するユーザープロファイルの検索対象となる、Directory Server 内の階層の数を示します。検索は、211 ページの「ユーザー検索の開始 DN」属性で指定されるノードから開始します。デフォルト値は `SUBTREE` です。次のリスト項目から 1 つ選択できます。

- OBJECT - 指定したノードだけを検索します。
- ONELEVEL - 指定したノードのレベルとその 1 つ下のレベルで検索します。
- SUBTREE - 指定したノードとその下のノードのエントリすべてを検索します。

警告 サブ組織のユーザーは、サブ組織の状態が非アクティブであってもログインする可能性があります。これを防ぐには、ユーザーの所属する特定の組織を指定するように検索範囲とベース DN が設定されていることを確認してください。

LDAP サーバーに対する SSL を有効

このオプションは、プライマリおよびセカンダリ LDAP サーバーとポートのフィールドで指定される Directory Server への SSL アクセスを有効にします。デフォルトでは、これは無効になっているので、Directory Server へのアクセスに SSL プロトコルは使用されません。ただし、この属性が有効になっている場合は、非 SSL サーバーにバインドできます。

認証においてユーザー DN を返す

Identity Server ディレクトリが LDAP 用に設定されたディレクトリと同じ場合、このオプションを有効にすることができます。オプションを有効にすると、このオプションによって LDAP 認証モジュールが `userId` ではなく DN を返すことができるため、検索が不要になります。通常、認証モジュールは `userId` のみを返すため、認証サービスはローカルの Identity Server LDAP でユーザー ID を検索します。外部の LDAP ディレクトリが使用された場合、通常このオプションは有効になりません。

LDAP サーバーのチェック間隔

この属性は LDAP サーバーのフェイルバックに使用します。LDAP プライマリサーバーが実行中であることを確認する前にスレッドが「スリープ」するまでの秒数を定義します。

ユーザー作成の属性リスト

この属性は、外部 LDAP サーバーとして LDAP サーバーが設定されているときに、LDAP 認証モジュールで使用されます。ローカルと外部の Directory Server との間の属性のマッピングが含まれます。この属性は次の形式です。

```
attr1|externalattr1
attr2|externalattr2
```

この属性に値が指定されると、外部属性の値が外部 Directory Server から読み込まれ、内部 Directory Server 属性に対して設定されます。コア認証モジュールのユーザープロファイル属性が「ダイナミックに作成」であり、かつユーザーがローカル Directory Server インスタンスに存在しない場合だけ、外部属性の値が内部属性に設定されます。新しく作成されるユーザーには、ユーザー作成の属性リストで指定した内部属性の値と、その値にマッピングされた外部属性の値が含まれます。

認証レベル

認証レベルは認証方法ごとに個別に設定します。この値は、認証の信頼度を示します。ユーザーが認証を受けると、この値がセッションの SSO トークンに格納されます。ユーザーがアクセスしたいアプリケーションに SSO トークンが提供されると、そのアプリケーションは格納されている値を使用して、ユーザーにアクセスを許可するのに十分なレベルかどうかを判別します。SSO トークンに格納されている認証レベルが必要な最小値に満たない場合、アプリケーションはユーザーにより高い認証レベルのサービスで認証を再度受けるよう要求することがあります。デフォルト値は `0` です。

注 認証レベルの指定がない場合、SSO トークンはコア認証属性のデフォルト認証レベルで指定した値を格納します。詳細は、206 ページの「デフォルト認証レベル」を参照してください。

第 22 章

メンバーシップ認証属性

メンバーシップ認証属性は組織属性です。サービス設定の下で組織属性に適用される値は、メンバーシップ認証属性テンプレートのデフォルト値になります。組織にサービスを登録した後、サービステンプレートを作成する必要があります。デフォルト値は組織の管理者が登録後に変更できます。組織属性は組織のサブツリーのエントリに継承されません。メンバーシップ認証属性は次のとおりです。

- パスワードの最少文字数
- デフォルトユーザーロール
- 登録後のユーザー状態
- プライマリ LDAP サーバーとポート
- セカンダリ LDAP サーバーとポート
- ユーザー検索の開始 DN
- root ユーザーバインド DN
- root ユーザーバインドパスワード
- root ユーザーバインドパスワード (確認)
- ユーザーネーミング属性
- ユーザーエントリ検索属性
- ユーザー検索フィルタ
- 検索範囲
- LDAP サーバーに対する SSL を有効
- 認証においてユーザー DN を返す
- 認証レベル

パスワードの最少文字数

このフィールドは、自己登録時に設定するパスワードに必要な最少文字数を指定します。デフォルト値は 8 です。

この値を変更すると、次のファイルの登録およびエラーテキストでも値が変更されます。

IdentitySever_base/locale/amAuthMembership.properties (PasswdMinChars *entry*)

デフォルトユーザーロール

このフィールドは、自己登録で作成されたプロファイルを持つ新しいユーザーに割り当てるロールを指定します。デフォルト値はありません。管理者は、新しいユーザーに割り当てられるロールの DN を指定する必要があります。

注	指定するロールは、認証を構成する組織の下にあることが必要です。自己登録時には、そのユーザーに割り当て可能なロールだけが追加されます。他の DN はすべて無視されます。

登録後のユーザー状態

このメニューは、自己登録したユーザーにサービスをすぐに利用できるようにするかどうかを指定します。デフォルト値は「有効」なので、新しいユーザーはサービスを利用できます。管理者が「無効」を選択すると、新しいユーザーはサービスを利用できません。

プライマリ LDAP サーバーとポート

このフィールドは、Identity Server のインストール時に指定するプライマリ LDAP サーバーのホスト名およびポート番号を指定します。これは、LDAP 認証で最初に通信するサーバーです。形式は hostname:port です。ポート番号がないときは、389 と想定します。

複数のドメインに Identity Server が配備されている場合は、Identity Server および Directory Server の個々のインスタンス間の通信リンクを、次の形式で指定できます。複数のエントリを指定する場合は、エントリにローカルサーバー名をプレフィックスとして付ける必要があります。

```
local_servername|server:port local_servername2|server:port ...
```

たとえば、異なる場所に配備された 2 つの Identity Server (`L1-machine1-IS` および `L2- machine2-IS`) が、それぞれ別の Identity Server インスタンス (`L1-machine1-DS` および `L2-machine2-DS`) と通信する場合は、次のように指定できます。

```
L1-machine1-IS.example.com|L1-machine1-DS.example.com:389
L2-machine2-IS.example.com|L2-machine2-DS.example.com:389
```

セカンダリ LDAP サーバーとポート

このフィールドは、Identity Server プラットフォームが利用できるセカンダリ LDAP サーバーのホスト名およびポート番号を指定します。プライマリ LDAP サーバーが認証要求に応答しない場合は、このサーバーと通信します。プライマリサーバーが起動すると、Identity Server はプライマリサーバーに戻ります。この形式も `hostname:port` です。複数のエントリの場合は、ローカルサーバー名をプレフィックスとして付ける必要があります。

警告 Identity Server を使用する企業から遠隔地にある Directory Server からユーザーを認証する場合は、プライマリとセカンダリ両方の LDAP サーバーポートに値があることが重要です。1 つの Directory Server の場所の値を両方のフィールドに使用できます。

ユーザー検索の開始 DN

このフィールドは、ユーザーの検索を開始するノードの DN を指定します。性能上の理由から、この DN はできるだけ特定のものにしてください。デフォルト値は、ディレクトリツリーのルートです。有効な DN はすべて認識されます。複数のエントリを使用する場合は、エントリにローカルサーバー名をプレフィックスとして付ける必要があります。

注 同一の検索で複数のユーザーが一致した場合、認証は失敗します。

root ユーザーバインド DN

このフィールドは、「プライマリ LDAP サーバーとポート」フィールドで指定した Directory Server に管理者としてバインドするのに使用するユーザーの DN を指定します。ユーザーログイン ID に基づく、一致するユーザー DN を検索するためには、認証サービスをこの DN にバインドする必要があります。デフォルト値は `amldapuser` です。有効な DN はすべて認識されます。

root ユーザーバインドパスワード

このフィールドは、「root ユーザーバインド DN」フィールドで指定される管理者プロファイルのパスワードを指定します。デフォルト値はありません。管理者の有効な LDAP パスワードだけが認識されます。

root ユーザーバインドパスワード (確認)

パスワードの確認。

ユーザーネーミング属性

このフィールドは、ユーザーエントリのネーミング規則に使用する属性を指定します。デフォルトでは、Identity Server はユーザーエントリが `uid` 属性によって識別されるものと想定します。Directory Server で異なる属性 (`givenname` など) を使用している場合は、このフィールドにその属性名を指定します。

ユーザーエントリ検索属性

このフィールドは、認証を受けるユーザーの検索フィルタを設定するのに使用する属性をリストします。そのため、ユーザーはそのエントリで、複数の属性で認証を受けることができます。たとえば、このフィールドが `uid`、`employeenumber` および `mail` に設定されている場合、ユーザーはこれらの名前のどれを使用しても認証を受けることができます。

ユーザー検索フィルタ

このフィールドは、「ユーザー検索の開始 DN」フィールドの下でユーザーの検索に使用する属性を指定します。これはユーザーネーミング属性とともに機能します。デフォルト値はありません。有効なユーザーエントリ属性はすべて認識されます。

検索範囲

このメニューは、一致するユーザープロファイルの検索対象となる、Directory Server 内の階層の数を示します。検索は、217 ページの「ユーザー検索の開始 DN」属性で指定されるノードから開始します。デフォルト値は `SUBTREE` です。次のリスト項目から 1 つ選択できます。

- OBJECT - 指定したノードだけを検索します。
- ONELEVEL - 指定したノードのレベルとその 1 つ下のレベルで検索します。
- SUBTREE - 指定したノードとその下のノードのエントリすべてを検索します。

LDAP サーバーに対する SSL を有効

このオプションは、プライマリおよびセカンダリ LDAP サーバーとポートのフィールドで指定される Directory Server への SSL アクセスを有効にします。デフォルトでは、このチェックボックスは選択されていないので、Directory Server へのアクセスに SSL プロトコルは使用されません。

認証においてユーザー DN を返す

Identity Server ディレクトリが LDAP 用に設定されたディレクトリと同じ場合、このオプションを有効にすることができます。オプションを有効にすると、このオプションによって LDAP 認証モジュールが `userId` ではなく DN を返すことができるため、検索が不要になります。通常、認証モジュールは `userId` のみを返すため、認証サービスはローカルの Identity Server LDAP でユーザー ID を検索します。外部の LDAP ディレクトリが使用された場合、通常このオプションは有効になりません。

認証レベル

認証レベルは認証方法ごとに個別に設定します。この値は、認証の信頼度を示します。ユーザーが認証を受けると、この値がセッションの SSO トークンに格納されます。ユーザーがアクセスしたいアプリケーションに SSO トークンが提供されると、そのアプリケーションは格納されている値を使用して、ユーザーにアクセスを許可するのに十分なレベルかどうかを判別します。SSO トークンに格納されている認証レベルが必要な最小値に満たない場合、アプリケーションはユーザーにより高い認証レベルのサービスで認証を再度受けるよう要求することがあります。デフォルト値は 0 です。

注 認証レベルの指定がない場合、SSO トークンはコア認証属性のデフォルト認証レベルで指定した値を格納します。詳細は、206 ページの「デフォルト認証レベル」を参照してください。

第 23 章

NT 認証属性

NT 認証属性は組織属性です。サービス設定の下で組織属性に適用される値は、NT 認証テンプレートのデフォルト値になります。組織にサービスを登録した後、サービステンプレートを作成する必要があります。デフォルト値は組織の管理者が登録後に変更できます。組織属性は組織のサブツリーのエントリに継承されません。

NT 認証は、Solaris 版の Identity Server でのみサポートされています。NT 認証モジュールを実際に使用するには、Samba Client 2.2.2 をダウンロードしてインストールする必要があります。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。

NT 認証属性は次のとおりです。

- NT 認証ドメイン
- NT 認証ホスト
- 認証レベル

NT 認証ドメイン

この属性は、ユーザーが属するドメイン名を定義します。

NT 認証ホスト

この属性は、NT 認証のホスト名を定義します。ホスト名は、完全指定のドメイン名 (FQDN) ではなく、NetBIOS 名にする必要があります。デフォルトでは、FQDN の先頭部は NetBIOS 名です。

DHCP (ダイナミックホスト構成プロトコル) を使用している場合、Windows 2000 マシンの HOSTS ファイルに適切なエントリを設定します。

名前解決は、NetBIOS 名に基づいて行われます。サブネット上で NetBIOS 名の名前解決をするサーバーがない場合、マッピングはハードコードされている必要があります。

たとえば、ホスト名は `example1.company1.com` ではなく `example1` とする必要があります。

認証レベル

認証レベルは認証方法ごとに個別に設定します。この値は、認証の信頼度を示します。ユーザーが認証を受けると、この値がセッションの SSO トークンに格納されます。ユーザーがアクセスしたいアプリケーションに SSO トークンが提供されると、そのアプリケーションは格納されている値を使用して、ユーザーにアクセスを許可するのに十分なレベルかどうかを判別します。SSO トークンに格納されている認証レベルが必要な最小値に満たない場合、アプリケーションはユーザーにより高い認証レベルのサービスで認証を再度受けるよう要求することがあります。デフォルト値は `0` です。

注 認証レベルの指定がない場合、SSO トークンはコア認証属性のデフォルト認証レベルで指定した値を格納します。詳細は、206 ページの「デフォルト認証レベル」を参照してください。

第 24 章

RADIUS 認証属性

RADIUS 認証属性は組織属性です。サービス設定の下で組織属性に適用される値は、RADIUS 認証テンプレートのデフォルト値になります。組織にサービスを登録した後、サービステンプレートを作成する必要があります。デフォルト値は組織の管理者が登録後に変更できます。組織属性は組織のエントリに継承されません。RADIUS 認証属性は次のとおりです。

- RADIUS サーバー 1
- RADIUS サーバー 2
- RADIUS 共有シークレット
- RADIUS 共有シークレット (確認)
- RADIUS サーバーのポート
- タイムアウト (秒)
- 認証レベル

RADIUS サーバー 1

このフィールドは、プライマリ RADIUS サーバーの IP アドレスまたは完全修飾ホスト名を表示します。デフォルト IP アドレスは `127.0.0.1` です。このフィールドは有効な IP アドレスまたはホスト名をすべて認識します。複数のエントリの場合は、ローカルサーバー名をプレフィックスとして付ける必要があります。次の構文を使用します。

```
local_servername|ip_address local_servername2|ip_adress ...
```

RADIUS サーバー 2

このフィールドは、セカンダリ RADIUS サーバーの IP アドレスまたは完全修飾ドメイン名 (FQDN) を表示します。これはフェイルオーバーサーバーで、プライマリサーバーが通信できない場合に通信するサーバーです。デフォルト IP アドレスは `127.0.0.1` です。複数のエントリの場合は、ローカルサーバー名をプレフィックスとして付ける必要があります。次の構文を使用します。

local_servername | ip_address local_servername2 | ip_adress ...

RADIUS 共有シークレット

このフィールドは RADIUS 認証の共有シークレットを保持します。共有シークレットは、注意深く選んだパスワードと同じレベルにする必要があります。このフィールドのデフォルト値はありません。

RADIUS 共有シークレット (確認)

RADIUS 認証の共有シークレットの確認。

RADIUS サーバーのポート

このフィールドは、RADIUS サーバーが待機するポートを指定します。デフォルト値は `1645` です。

注 認証レベルの指定がない場合、SSO トークンはコア認証属性のデフォルト認証レベルで指定した値を格納します。詳細は、206 ページの「デフォルト認証レベル」を参照してください。

タイムアウト (秒)

このフィールドは、RADIUS サーバーがタイムアウトするまで応答を待つ時間間隔を秒単位で指定します。デフォルト値は 3 秒です。どんな秒数のタイムアウトを指定しても認識されます。

認証レベル

認証レベルは認証方法ごとに個別に設定します。この値は、認証の信頼度を示します。ユーザーが認証を受けると、この値がセッションの SSO トークンに格納されます。ユーザーがアクセスしたいアプリケーションに SSO トークンが提供されると、そのアプリケーションは格納されている値を使用して、ユーザーにアクセスを許可するのに十分なレベルかどうかを判別します。SSO トークンに格納されている認証レベルが必要な最小値に満たない場合、アプリケーションはユーザーにより高い認証レベルのサービスで認証を再度受けるよう要求することがあります。デフォルト値は 0 です。

注 認証レベルの指定がない場合、SSO トークンはコア認証属性のデフォルト認証レベルで指定した値を格納します。詳細は、206 ページの「デフォルト認証レベル」を参照してください。

第 25 章

SafeWord 認証属性

SafeWord 認証属性は組織属性です。サービス設定の下で組織属性に適用される値は、SafeWord 認証テンプレートのデフォルト値になります。組織にサービスを登録した後、サービステンプレートを作成する必要があります。デフォルト値は組織の管理者が登録後に変更できます。組織属性は組織のサブツリーのエントリに継承されません。

このサービスでは、Secure Computing の SafeWord または SafeWord PremierAccess 認証サーバーを使用して、ユーザーを認証できます。SafeWord 認証属性は次のとおりです。

- SafeWord サーバー仕様
- SafeWord システム名
- SafeWord サーバー検証ファイルパス
- SafeWord ログレベル
- SafeWord ログのパス
- 認証レベル

SafeWord サーバー仕様

このフィールドは、SafeWord または SafeWord PremierAccess サーバー名とポートを指定します。SafeWord サーバーのデフォルトとしてポート 7482 が設定されます。SafeWord PremierAccess サーバーのデフォルトのポート番号は 5030 です。

SafeWord システム名

このフィールドは、SafeWord サーバーで構成されるシステム名を指定します。デフォルトのシステム名は STANDARD です。

SafeWord サーバー検証ファイルパス

このフィールドは、SafeWord クライアントライブラリがその検証ファイルを置くディレクトリを指定します。デフォルトは次のとおりです。

```
/var/opt/SUNWam/auth/safeword/serverVerification
```

このフィールドに異なるディレクトリを指定する場合は、SafeWord 認証を試みる前にそのディレクトリが存在する必要があります。

SafeWord ログレベル

この属性は使用されません。

SafeWord ログのパス

この属性は、SafeWord クライアントログのディレクトリパスとログファイル名を指定します。デフォルトのパスは次のとおりです。

```
/var/opt/SUNWam/auth/safeword/safe.log
```

異なるパスまたはファイル名を指定する場合は、SafeWord 認証を試みる前にそれらが存在している必要があります。

SafeWord 認証に複数の組織が構成され別々の SafeWord サーバーが使用されている場合、別々のパスを指定する必要があります。そうしないと、SafeWord 認証が行われる最初の組織だけが認証されます。同様に、組織が SafeWord サーバーを変更した場合、新しく構成された SafeWord サーバーの認証が行われる前に、指定されたディレクトリの swec.dat を削除する必要があります。

認証レベル

認証レベルは認証方法ごとに個別に設定します。この値は、認証の信頼度を示します。ユーザーが認証を受けると、この値がセッションの SSO トークンに格納されます。ユーザーがアクセスしたいアプリケーションに SSO トークンが提供されると、そのアプリケーションは格納されている値を使用して、ユーザーにアクセスを許可するのに十分なレベルかどうかを判別します。SSO トークンに格納されている認証レベルが必要な最小値に満たない場合、アプリケーションはユーザーにより高い認証レベルのサービスで認証を再度受けるよう要求することがあります。デフォルト値は 0 です。

注 認証レベルの指定がない場合、SSO トークンはコア認証属性のデフォルト認証レベルで指定した値を格納します。詳細は、206 ページの「デフォルト認証レベル」を参照してください。

第 26 章

SecurID 認証属性

SecurID 認証属性は組織属性です。サービス設定の下で組織属性に適用される値は、SecurID 認証テンプレートのデフォルト値になります。組織にサービスを登録した後、サービステンプレートを作成する必要があります。デフォルト値は組織の管理者が登録後に変更できます。組織属性は組織のサブツリーのエントリに継承されません。

このサービスでは、RSA の ACE/Server 認証サーバーを使用して、ユーザーを認証できます。SecurID 認証属性は次のとおりです。

- SecurID ACE/ サーバー設定パス
- SecurID ヘルパ設定ポート
- SecurID ヘルパ認証ポート
- 認証レベル

注 Identity Server 6.1 では、x86 オペレーティングシステムでの SecurID 認証サービスはサポートされていません。

SecurID ACE/ サーバー設定パス

このフィールドは、SecurID ACE/Server `sdconf.rec` ファイルの存在するディレクトリを指定します。デフォルトは次のとおりです。

```
/opt/ace/data
```

このフィールドに異なるディレクトリを指定する場合は、SecurID 認証を試みる前にそのディレクトリが存在する必要があります。

SecurID ヘルパ設定ポート

この属性は、起動時に SecurID ヘルパ認証ポート属性に含まれる設定情報について、SecurID ヘルパがどのポート上で待機するかを指定します。デフォルトは 58943 です。

この属性を変更した場合、`AMConfig.properties` ファイルの `securidHelper.ports` エントリも変更して、Identity Server を再起動することが必要です。`AMConfig.properties` ファイル内のエントリは、SecurID ヘルパのインスタンスのポートをスペースで区切ったリストです。別の ACE/Server (別の `sdconf.rec` ファイルを持つ) と通信する組織ごとに、別々の SecurID ヘルパを用意する必要があります。

SecurID ヘルパ認証ポート

この属性は、SecurID ヘルパインスタンスが認証要求を待機するように、組織の SecurID 認証モジュールで設定するためのポートを指定します。ポート番号は、SecurID または UNIX 認証を使用するすべての組織で一意でなければなりません。デフォルトのポート番号は、57943 です。

認証レベル

認証レベルは認証方法ごとに個別に設定します。この値は、認証の信頼度を示します。ユーザーが認証を受けると、この値がセッションの SSO トークンに格納されます。ユーザーがアクセスしたいアプリケーションに SSO トークンが提供されると、そのアプリケーションは格納されている値を使用して、ユーザーにアクセスを許可するのに十分なレベルかどうかを判別します。SSO トークンに格納されている認証レベルが必要な最小値に満たない場合、アプリケーションはユーザーにより高い認証レベルのサービスで認証を再度受けるよう要求することがあります。デフォルト値は `0` です。

注 認証レベルの指定がない場合、SSO トークンはコア認証属性のデフォルト認証レベルで指定した値を格納します。詳細は、206 ページの「デフォルト認証レベル」を参照してください。

第 27 章

UNIX 認証属性

UNIX 認証サービスにはグローバル属性と組織属性があります。グローバル属性に適用される値は Sun ONE Identity Server 設定全体に適用され、設定済みのすべての組織に継承されます。グローバル属性の目的は Identity Server アプリケーションのカスタマイズであるため、ロールまたは組織に直接適用することはできません。組織属性に適用される値は設定済みの各組織のデフォルト値で、サービスを組織に登録するときに変更できます。組織属性は組織のエントリに継承されません。UNIX 認証属性は次のように分類できます。

- グローバル属性
- 組織属性

注 UNIX 認証サービスは、Windows 2000 プラットフォームではサポートされていません。

グローバル属性

UNIX 認証サービスのグローバル属性には、次のものがあります。

- UNIX ヘルパ設定ポート
- UNIX ヘルパ認証ポート
- UNIX ヘルパのタイムアウト (分)
- UNIX ヘルパスレッド

UNIX ヘルパ設定ポート

この属性は、起動時に、UNIX ヘルパ認証ポート、UNIX ヘルパのタイムアウト (分)、および UNIX ヘルパスレッド属性に含まれる設定情報について、UNIX ヘルパがどのポート上で待機するかを指定します。デフォルトは 58946 です。

この属性を変更した場合、`AMConfig.properties` ファイルの `unixHelper.ports` エントリも変更して、Identity Server を再起動することが必要です。

UNIX ヘルパ認証ポート

この属性は、構成後に UNIX ヘルパがどのポート上で認証要求を待機するかを指定します。デフォルトのポート番号は、57946 です。

UNIX ヘルパのタイムアウト (分)

この属性は、認証の制限時間を分単位で指定します。指定された時間を超えると、認証は自動的に失敗します。デフォルトでは 3 分に設定されています。

UNIX ヘルパスレッド

この属性は、同時に可能な UNIX 認証セッションの最大数を指定します。所定の時間にこの最大数に達すると、いずれかのセッションが解放されるまで、認証を試みても認証は行われません。デフォルトは 5 に設定されています。

組織属性

UNIX 認証サービスの組織属性には、次のものがあります。

認証レベル

認証レベルは認証方法ごとに個別に設定します。この値は、認証の信頼度を示します。ユーザーが認証を受けると、この値がセッションの SSO トークンに格納されます。ユーザーがアクセスしたいアプリケーションに SSO トークンが提供されると、そのアプリケーションは格納されている値を使用して、ユーザーにアクセスを許可するのに十分なレベルかどうかを判別します。SSO トークンに格納されている認証レベルが必要な最小値に満たない場合、アプリケーションはユーザーにより高い認証レベルのサービスで認証を再度受けるよう要求することがあります。デフォルト値は 0 です。

注 認証レベルの指定がない場合、SSO トークンはコア認証属性のデフォルト認証レベルで指定した値を格納します。詳細は、206 ページの「デフォルト認証レベル」を参照してください。

第 28 章

認証設定サービス属性

認証設定サービス属性はダイナミックな組織属性です。この属性は、組織、サービス、またはロールに対して定義できます。組織属性はコア認証モジュールで定義されます。

ロールがユーザーに適用されると、またはユーザーが組織に割り当てられると、これらの属性はデフォルトでユーザーに継承されます。認証設定属性は次のとおりです。

- 認証設定
- ログイン成功 URL
- ログイン失敗 URL
- 認証ポストプロセスクラス

認証設定

「編集」リンクをクリックすると、認証設定インタフェースが表示されます。これにより、ロールベースまたは組織ベースの認証の認証モジュールを設定することができます。

次の表に、認証モジュールの設定オプションの一覧を示します。

モジュール名	Identity Server に使用できるデフォルトの認証モジュールのリストから選択できます。

フラグ

プルダウンメニューで認証モジュールの要件を次のいずれかに指定できます。

- REQUIRED - 認証には認証モジュールが必要です。認証に成功または失敗すると、認証モジュール一覧の次のモジュールへと認証が進行します。
- REQUISITE - 認証には認証モジュールが必要です。認証に成功すると、認証モジュール一覧の次のモジュールへと認証が進行します。認証に失敗すると、制御がアプリケーションに返されます。認証モジュール一覧の次のモジュールには認証が進行しません。
- SUFFICIENT - 認証に認証モジュールは不要です。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、認証モジュール一覧の次のモジュールには認証が進行しません。認証に失敗すると、一覧の次のモジュールへと認証が進行します。
- OPTIONAL - 認証に認証モジュールは不要です。認証に成功または失敗しても、認証モジュール一覧の次のモジュールへと認証が進行します。

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。適用条件には上下関係があり、「REQUIRED」が最も高く、「OPTIONAL」が最も低くなります。

たとえば、管理者が LDAP モジュールに「REQUIRED」フラグを設定している場合、ユーザーが特定のリソースにアクセスするためには、ユーザーの資格情報が LDAP の認証条件にパスすることが必要です。

複数の認証モジュールを追加して各モジュールのフラグを「REQUIRED」に設定した場合、ユーザーがアクセスするためにはすべての認証条件にパスする必要があります。

フラグの定義の詳細については、次のサイトの JAAS (Java Authentication and Authorization Service) を参照してください。

`http://java.sun.com/security/jaas/doc/module.html`

オプション

モジュールの追加オプションをキー = 値のペアとして指定できます。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。

ログイン成功 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。

ログイン失敗 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。

認証ポストプロセスクラス

この属性は、ログインの成功または失敗後に実行する、認証後プロセスをカスタマイズするための Java クラス名を定義します。

競合の解決レベル

この属性は、ロールにだけ適用されます。競合解決レベルは、ロールの認証設定属性の優先順位を設定します。ロールには同一のユーザーが含まれる場合もあります。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 の優先順位が最も高くなるように設定することができます。

第 29 章

クライアントディテクションサービス属性

クライアントディテクションサービス属性はグローバル属性です。この属性に適用される値は Identity Server 設定全体に適用され、設定済みのすべての組織に継承されます。グローバル属性の目的は Identity Server アプリケーションのカスタマイズなので、ロールまたは組織に直接適用することはできません。クライアントディテクション属性は次のとおりです。

クライアントタイプ

クライアントタイプを検出するには、Identity Server でクライアントの特性を認識する必要があります。これらの特性は、サポートされているすべてのタイプのプロパティをクライアントデータの形式で識別します。この属性を使って、クライアントマネージャインタフェースを通してクライアントデータを変更できます。クライアントマネージャにアクセスするには、「編集」リンクをクリックします。

何も変更を加えない状態では、HTML ベースのブラウザで利用できる設定済みの Identity Server クライアントデータは 1 つだけで、全体的なスキーマのサブ設定として定義されています。genericHTML とその親である HTML です。

クライアントマネージャ

クライアントマネージャは、基本クライアント、スタイル、および関連プロパティを一覧表示するインタフェースです。また、デバイスの追加や設定を行うことができます。

基本クライアントタイプ

基本クライアントタイプは、クライアントマネージャの上部に一覧表示されます。基本クライアントタイプにはデフォルトのプロパティがあり、そのクライアントタイプに属するすべてのデバイスは、これらのプロパティを継承できます。

スタイルプロファイル

クライアントマネージャでは、基本クライアントタイプも含め、利用可能なクライアントがすべて「スタイル」プルダウンメニューにまとめられます。選択したスタイル (親プロファイル) によって、設定済みの子デバイスに共通するプロパティが定義されます。デバイスには、親プロファイルのプロパティがダイナミックに継承されます。

「現在のスタイルのプロパティ」リンクをクリックすると、読み取り専用のクライアントエディタウィンドウが開き、スタイルのプロパティが表示されます。

デバイスプロファイル

スタイルを選択すると、そのスタイルに対して設定されているデバイスプロファイルがクライアントマネージャに表示されます。デバイスはユーザーエージェント (デバイス名) に基づいてソートされます。デバイスをフィルタリングするには、「フィルタ」フィールドにユーザーエージェント文字列を入力します (ワイルドカードも使用可)。

各デバイスのクライアントプロパティを修正するには、そのデバイス名の横にある「編集」リンクをクリックします。クライアントエディタウィンドウにプロパティが表示されます。プロパティを編集するには、プルダウンリストから以下の分類を選択します。

ハードウェアプラットフォーム : ディスプレイサイズ、サポートされている文字セットなど、デバイスのハードウェアのプロパティが含まれています。

ソフトウェアプラットフォーム : デバイスのアプリケーション環境、オペレーティングシステム、およびインストール済みソフトウェアのプロパティが含まれています。

ネットワーク特性 : サポートされているベアラなど、ネットワーク環境を記述するプロパティが含まれています。

BrowserUA: デバイス上で実行中のブラウザユーザーエージェントに関連する属性が含まれています。

WapCharacteristics: デバイスでサポートされている WAP (Wireless Application Protocol) 環境のプロパティが含まれています。

PushCharacteristicsNames: デバイスでサポートされている WAP 環境のプロパティが含まれています。

追加プロパティ : デバイスのプロパティを追加できます。

具体的なプロパティの定義については、次の場所にある Open Mobile Alliance Ltd. (OMA) の『Wireless Application Protocol, Version 20-Oct-2001』を参照してください。

http://www1.wapforum.org/tech/terms.asp?doc=WAP-248-UAProf-20011020-a.pdf

プロパティの修正が完了したら、「保存」をクリックします。デバイスには、カスタマイズされたことを示す「**」という文字が表示されます。「デフォルト」リンクを使用すると、カスタマイズしたプロパティを削除し、デバイスをデフォルト設定に戻すことができます。

スタイルに新しいデバイスを追加するには、「新規デバイス」ボタンをクリックします。次のフィールドを持つ「新規デバイスを作成」ウィンドウが表示されます。

スタイル : デバイスの基本スタイルを表示します。たとえば、`HTML` などです。

デバイスユーザーエージェント : デバイスの名前を指定します。

「次へ」をクリックして、次のフィールドを表示します。

クライアントタイプ名 : クライアントタイプを表示します。たとえば、HTML などです。クライアントタイプ名は、すべてのデバイスで一意でなければなりません。

このデバイスの直接の親 : デバイスの親 (基本) クライアントタイプを指定します。たとえば、HTML などです。

HTTP ユーザーエージェント文字列 : HTTP 要求ヘッダー内のユーザーエージェントを定義します。たとえば、Mozilla/4.0 などです。

「OK」をクリックし、デバイスのプロパティをカスタマイズします。具体的なプロパティの定義については、次の場所にある Open Mobile Alliance Ltd. (OMA) の『Wireless Application Protocol, Version 20-Oct-2001』を参照してください。

http://www1.wapforum.org/tech/terms.asp?doc=WAP-248-UAProf-20011020-a.pdf

デバイスとそのプロパティを複製するには、「複製」リンクをクリックします。デバイス名は一意でなければなりません。Identity Server では、デフォルトで `copy_of_` デバイス名というデバイス名に変更されます。

デバイスを削除するには、そのデバイスに表示されている「削除」リンクをクリックします。

デフォルトクライアントタイプ

この属性は、クライアントタイプ属性のクライアントタイプのリストの中からデフォルトクライアントタイプを定義します。デフォルトは genericHTML です。

クライアントディテクションクラス

この属性は、クライアントディテクション要求のすべてが送信されるクライアントディテクションクラスを定義します。この属性によって返される文字列は、クライアントタイプ属性に指定されているクライアントタイプのいずれかと一致します。デフォルトのクライアントディテクションクラスは、com.iplanet.services.cdm.ClientDetectionDefaultImpl です。

クライアントディテクションを有効

この属性で、クライアントディテクションを有効にすることができます。クライアントディテクションが有効になっている (選択されている) 場合、すべての要求はクライアントディテクションクラス属性で指定されているクラスを使って送信されます。

デフォルトでは、genericHTML 以外のクライアントタイプに対しては、クライアントディテクション機能は無効になっています。この属性が選択されていない場合、Identity Server では、そのクライアントは genericHTML であり、HTML ブラウザからアクセスされると見なされます。

第 30 章

グローバル化設定のサービス属性

グローバル化設定のサービス属性はグローバル属性です。この属性に適用される値は Identity Server 設定全体に適用され、設定済みのすべての組織に継承されます。グローバル属性の目的は Identity Server アプリケーションのカスタマイズなので、ロールまたは組織に直接適用することはできません。グローバル化設定の属性は次のとおりです。

- 各ロケールでサポートされる Charset
- Charset のエイリアス
- 自動生成される共通名の形式

各ロケールでサポートされる Charset

この属性では、各ロケールでサポートされる Charset をリストします。このリストでは、ロケールと Charset とのマッピングを示します。形式は次のとおりです。

`locale=`*ロケール名*`|charset=charset1;charset2;charset3;...;charsetn`

属性の下にあるボタンを使用すると、Charset を追加、編集、複製、および削除できます。

Charset のエイリアス

この属性では、応答を送信するために使用するコードセット名をリストします。コードセット名は IANA 名にマップしています。Java コードセット名に一致する必要はありません。現在は、Java 文字セットと IANA Charset との間のマップにはハッシュテーブルが使われます。エイリアスの形式は次のとおりです。

`mimeName=`*Charset*`|javaName=`*Charset*

次に例を示します。

```
mimeName=Shift_JIS|javaName=SJIS
```

これはどちらも同じ文字セットを示しています。

属性の下にあるボタンを使用すると、文字セットのエイリアスを追加、編集、複製、および削除できます。

自動生成される共通名の形式

この表示オプションではさまざまなロケールおよび文字セットに名前の形式を適応するように、名前を自動生成する方法を定義します。デフォルトの構文は次のとおりです。定義中のカンマやスペースは名前の形式で表示されることに注意してください。

```
en_us = {givenname} {initials} {sn}
```

たとえば中国語の文字セットで、uid (11111) のユーザー (User One) に対して新しい名前の形式で表示するには、次の表現を使用します。

```
zh = {sn}{givenname}({uid})
```

これにより、次のように表示されます。

```
OneUser 11111
```

第 31 章

ログサービス属性

ログサービス属性はグローバル属性です。これらの属性に適用される値は Sun ONE Identity Server 設定全体に適用され、設定済みのすべての組織に継承されます。グローバル属性の目的は Identity Server アプリケーションのカスタマイズであるため、ロールまたは組織に直接適用することはできません。ログ属性は次のとおりです。

- 最大ログサイズ
- 履歴ファイルの数
- ログの場所
- ログタイプ
- データベースユーザー名
- データベースユーザーパスワード
- データベースユーザーパスワード (確認)
- データベースドライバ名
- 設定可能なログフィールド
- ログ検証時間
- ログ署名時間
- セキュリティ保護されたログ
- レコードの最大数
- アーカイブごとのファイル数
- バッファサイズ
- バッファ時間
- 時間バッファリング

最大ログサイズ

この属性は、Identity Server ログファイルの最大サイズ (バイト単位) の値を指定します。デフォルト値は 1000000 です。

履歴ファイルの数

この属性は、履歴解析のために保持するバックアップログファイルの数に等しい値を持ちます。入力できる整数値は、ローカルシステムのパーティションサイズと利用可能なディスク容量で決まります。デフォルト値は 3 です。

ログの場所

ファイルベースのログ機能には、ログファイルを格納する場所が必要です。このフィールドは、その場所の完全なディレクトリパスを指定します。デフォルトの場所は次に示すとおりです。

```
/var/opt/SUNWam/logs
```

デフォルト以外のディレクトリを使う場合、そのディレクトリには Identity Server を実行しているユーザーに対する書き込み権限が必要です。

Oracle や MySQL などの DB (データベース) ログ用にログの場所を設定するとき、ログの場所の記述部分では大文字と小文字が区別されます。

たとえば、Oracle データベースにログを書き込む場合、ログの場所は次のようになります。

```
jdbc:oracle:thin:@machine.domain:port:DBName
```

`jdbc:oracle:thin` は小文字で記述する必要があります。

注 ログ属性の値を変更した場合は、変更を有効にするために Identity Server を再起動する必要があります。

ログタイプ

この属性により、フラットファイルログには File、データベースログには DB のいずれかを指定できます。

データベースユーザー名

この属性は、ログタイプ属性が DB に設定されている場合に、データベースに接続するユーザーの名前を指定します。

データベースユーザーパスワード

この属性は、ログタイプ属性が DB に設定されている場合に、データベースユーザーのパスワードを指定します。

データベースユーザーパスワード (確認)

データベースパスワードの確認。

データベースドライバ名

この属性は、ログ実装クラスに使用するドライバを指定します。

設定可能なログフィールド

このパラメータは、記録されるフィールドのリストを表します。デフォルトでは、次のフィールドが記録されます。

- Domain
- Hostname
- IPAddress
- LoggedBy
- Loglevel
- LoginID
- ModuleName

ログ検証時間

この属性は、サーバーがログを検証して改ざんを検出する頻度 (秒単位) を設定します。デフォルトの時間は 3600 秒です。このパラメータは、セキュリティ保護されたログにだけ適用されます。

ログ署名時間

このパラメータは、ログに署名する頻度 (秒単位) を設定します。デフォルトの時間は 900 秒です。このパラメータは、セキュリティ保護されたログにだけ適用されます。

セキュリティ保護されたログ

この属性は、セキュリティ保護されたログを有効にするかどうかを指定します。デフォルトでは、セキュリティ保護されたログはオフです。セキュリティ保護されたログでは、不正な変更またはセキュリティログの改ざんを検出できます。

レコードの最大数

この属性は、読み取り照会と一致するレコードの数に関係なく、Java LogReader インタフェースが返すレコードの最大数を設定します。デフォルトでは 500 に設定されています。この属性は、LogQuery パラメータを使用してログ API を呼び出した場合オーバーライド可能です。

アーカイブごとのファイル数

この属性は、セキュリティ保護されたログにのみ適用可能です。この属性は、セキュリティ保護された後続のログに対して、ログファイルとキーストアをいつアーカイブする必要があるか、およびセキュリティ保護されたキーストアをいつ再生成する必要があるかを指定します。デフォルトでは、各ログで 5 ファイル処理します。

バッファサイズ

この属性は、ログサービスに送られて記録される前にメモリ内のバッファに保存される、ログレコードの最大数を指定します。デフォルトは、1 レコードです。

バッファ時間

この属性は、ログレコードがログサービスに送られて記録される前にメモリ内のバッファに保存される時間を指定します。デフォルト値は 3600 秒です。

時間バッファリング

「オン」にすると、Identity Server では、ログレコードをメモリにバッファする時間の上限を設定します。この時間は、バッファ時間属性に設定します。

第 32 章

ネーミングサービス属性

ネーミングサービス属性はグローバル属性です。これらの属性に適用される値は Sun ONE Identity Server 設定全体に適用され、設定済みのすべての組織に継承されます。グローバル属性の目的は Identity Server アプリケーションのカスタマイズであるため、ロールまたは組織に直接適用することはできません。

ネーミングサービスを使用すると、プラットフォームで複数の Identity Server が動作していても、クライアントは正しいサービス URL を見つけることができます。ネーミング URL が見つかると、ネーミングサービスはユーザーのセッションを復号化して、プロトコル、ホスト、およびポートをセッションのパラメータでダイナミックに置き換えます。これにより、サービスに対して返された URL が、ユーザーセッションの作成されたホストの URL であることが保証されます。ネーミング属性は次のとおりです。

- プロファイルサービス URL
- セッションサービス URL
- ログサービス URL
- ポリシーサービス URL
- 認証サービス URL
- SAML Web プロファイル / アーティファクトサービス URL
- SAML SOAP サービス URL
- SAML Web プロファイル /POST サービス URL
- SAML アサーションマネージャサービス URL
- 連携アサーションマネージャサービス URL
- Identity SDK サービス URL

プロファイルサービス URL

このフィールドは、次の構文を使用して値を取得します。

`%protocol://%host:%port/` サーバー配備 *URI*`/profileservice`

この構文により、特定のセッションパラメータに基づくプロファイル URL をダイナミックに置き換えることができます。

セッションサービス URL

このフィールドは、次の構文を使用して値を取得します。

`%protocol://%host:%port/` サーバー配備 *URI*`/sessionservice`

この構文により、特定のセッションパラメータに基づくセッション URL をダイナミックに置き換えることができます。

ログサービス URL

このフィールドは、次の構文を使用して値を取得します。

`%protocol://%host:%port/` サーバー配備 *URI*`/loggingservice`

この構文により、特定のセッションパラメータに基づくログ URL をダイナミックに置き換えることができます。

ポリシーサービス URL

このフィールドは、次の構文を使用して値を取得します。

`%protocol://%host:%port/` サーバー配備 *URI*`/policyservice`

この構文により、特定のセッションパラメータに基づくポリシー URL をダイナミックに置き換えることができます。

認証サービス URL

このフィールドは、次の構文を使用して値を取得します。

`%protocol://%host:%port/` サーバー配備 *URI*`/authservice`

この構文により、特定のセッションパラメータに基づく認証 URL をダイナミックに置き換えることができます。

SAML Web プロファイル / アーティファクトサービス URL

このフィールドは、次の構文を使用して値を取得します。

`%protocol://%host:%port/` サーバー配備 *URI*`/SAMLAwareServlet`

この構文により、特定のセッションパラメータに基づく SAML Web プロファイル / アーティファクト URL をダイナミックに置き換えることができます。

SAML SOAP サービス URL

このフィールドは、次の構文を使用して値を取得します。

`%protocol://%host:%port/` サーバー配備 *URI*`/SAMLSOAPReceiver`

この構文により、特定のセッションパラメータに基づく SAML SOAP URL をダイナミックに置き換えることができます。

SAML Web プロファイル /POST サービス URL

このフィールドは、次の構文を使用して値を取得します。

`%protocol://%host:%port/` サーバー配備 *URI*`/SAMLPOSTProfileServlet`

この構文により、特定のセッションパラメータに基づく SAML Web プロファイル /POST URL をダイナミックに置き換えることができます。

SAML アサーションマネージャサービス URL

このフィールドは、次の構文を使用して値を取得します。

`%protocol://%host:%port/` サーバー配備
URI`/AssertionManagerServlet/AssertionManagerIF`

この構文により、特定のセッションパラメータに基づく SAML アサーションマネージャサービス URL をダイナミックに置き換えることができます。

連携アサーションマネージャサービス URL

このフィールドは、次の構文を使用して値を取得します。

```
%protocol://%host:%port/amserver/FSAssertionManagerServlet/FSAssert
ionManagerIF
```

この構文により、特定のセッションパラメータに基づく連携アサーションマネージャサービス URL をダイナミックに置き換えることができます。

Identity SDK サービス URL

このフィールドは、次の構文を使用して値を取得します。

```
%protocol://%host:%port/amserver/UserManagementServlet/
```

この構文により、特定のセッションパラメータに基づく Identity SDK サービス URL をダイナミックに置き換えることができます。

第 33 章

パスワードリセットサービス属性

パスワードリセットサービス属性は組織属性です。サービス設定の下で組織属性に適用される値は、指定された組織でのパスワードリセットサービスのデフォルト値になります。組織属性は組織のサブツリーのエントリに継承されません。

パスワードリセット属性は次のとおりです。

- ユーザー検証
- 秘密の質問
- 検索フィルタ
- ベース DN
- バインド DN
- バインドパスワード
- パスワードリセットのオプション
- パスワードの変更通知のオプション
- パスワードリセットを有効
- 個人的な質問を有効
- 質問の数
- パスワードリセット失敗のロックアウトカウント
- パスワードリセット失敗のロックアウト間隔 (分)
- ロックアウト通知を送信するための電子メールアドレス
- ユーザーに警告する失敗回数
- パスワードリセット失敗のロックアウト持続時間 (分)
- パスワードリセット失敗のロックアウトモード
- パスワードリセットのロックアウト属性名

- パスワードリセットのロックアウト属性値

ユーザー検証

この属性では、パスワードをリセットするユーザーを検索するための値を指定します。

秘密の質問

このフィールドでは、ユーザーが自分のパスワードをリセットするために使用できる質問のリストを追加できます。質問を追加するには、「秘密の質問」フィールドに質問を入力し、「追加」をクリックします。選択した質問は、ユーザーの「ユーザープロファイル」ページに表示されます。すると、パスワードをリセットするために、ユーザーは質問を選択できるようになります。

「個人的な質問を有効」属性を選択している場合は、ユーザーが独自の質問を作成できます。

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。

ベース DN

この属性は、ユーザーの検索をどの DN から開始するかを指定します。DN が指定されていない場合は、組織 DN から検索が始まります。プロキシ認証の競合の原因となるので、ベース DN として `cn=directorymanager` は使用しないでください。

バインド DN

この属性は、バインドパスワードとともに、ユーザーのパスワードをリセットするために使用します。

バインドパスワード

この属性は、バインド DN とともに、ユーザーのパスワードをリセットするために使用します。

パスワードリセットのオプション

この属性は、パスワードをリセットするためのクラス名を指定します。デフォルトのクラス名は次のとおりです。

```
com.sun.identity.password.RandomPasswordGenerator
```

パスワードリセットクラスは、プラグインを使用してカスタマイズできます。このクラスは、`PasswordGenerator` インタフェースで実装する必要があります。詳細は、『Sun ONE Identity Server Customization and API Guide』を参照してください。

パスワードの変更通知のオプション

この属性は、パスワードをリセットするときのユーザーへの通知方法を指定します。デフォルトのクラス名は次のとおりです。

```
com.sun.identity.password.EmailPassword
```

パスワード通知クラスは、プラグインを使用してカスタマイズできます。このクラスは、`NotifyPassword` インタフェースで実装する必要があります。詳細は、『Sun ONE Identity Server Customization and API Guide』を参照してください。

パスワードリセットを有効

この属性を選択すると、パスワードリセット機能が有効になります。

個人的な質問を有効

この属性を選択すると、ユーザーはパスワードをリセットするための独自の質問を作成できます。

質問の数

この値は、パスワードリセットページで確認される質問の最大数を指定します。

パスワードリセット失敗のロックアウトカウント

この属性は、パスワードリセット失敗のロックアウト間隔で定義された時間内に、ユーザーがパスワードのリセットを試みることができる回数を定義します。この回数を超えると、ユーザーはロックアウトされます。

たとえば、パスワードリセット失敗のロックアウトカウントが 5 に設定されていて、ログイン失敗のロックアウト間隔が 5 分に設定されている場合、ユーザーは、ロックアウトになる前の 5 分以内に 5 回パスワードリセットのチャンスがあります。

パスワードリセット失敗のロックアウト間隔 (分)

この属性は、パスワードのリセットを試みる回数 (パスワードリセット失敗のロックアウトカウントで定義される) を完了するまでの時間を分単位で定義します。これを超えるとロックアウトされます。

ロックアウト通知を送信するための電子メールアドレス

この属性は、ユーザーがパスワードリセットサービスからロックアウトされた場合に通知を受け取る電子メールアドレスを指定します。スペース区切りのリストで複数の電子メールアドレスを指定できます。

ユーザーに警告する失敗回数

この属性は、Identity Server がそのユーザーにロックアウトされるという警告を送信するまでに許可されるパスワードリセット失敗の回数を指定します。

パスワードリセット失敗のロックアウト持続時間 (分)

この属性は、ロックアウトが発生した際に、ユーザーがパスワードリセットを試みることが許可されない期間を、分単位で定義します。

パスワードリセット失敗のロックアウトモード

この属性は、パスワードリセットアプリケーションを使用してユーザーが最初にパスワードリセットに失敗したときに、ユーザーにパスワードリセットを禁止するかどうかを指定します。デフォルトでは、無効になっています。

パスワードリセットのロックアウト属性名

この属性には、パスワードリセットのロックアウト属性値で設定する inetuserstatus 値が含まれています。ユーザーがパスワードリセットでロックアウトされて、パスワードリセット失敗のロックアウト持続時間 (分) 変数が 0 に設定されている場合、inetuserstatus が無効に設定され、ユーザーはパスワードのリセットを試みることができません。

パスワードリセットのロックアウト属性値

この属性は、ユーザー状態の inetuserstatus 値 (パスワードリセットロックアウト属性名に含まれる) を有効と無効のいずれかに指定します。ユーザーがパスワードリセットでロックアウトされて、パスワードリセット失敗のロックアウト持続時間 (分) 変数が 0 に設定されている場合、inetuserstatus が無効に設定され、ユーザーはパスワードのリセットを試みることができません。

第 34 章

プラットフォームサービス属性

プラットフォームサービス属性はグローバル属性です。これらの属性に適用される値は Sun ONE Identity Server 設定全体に適用され、設定済みのすべての組織に継承されます。グローバル属性の目的は Identity Server アプリケーションのカスタマイズであるため、ロールまたは組織に直接適用することはできません。プラットフォーム属性は次のとおりです。

- サーバーリスト
- プラットフォームロケール
- Cookie ドメイン
- ログインサービス URL
- ログアウトサービス URL
- 使用可能なロケール
- クライアント文字セット

サーバーリスト

ネーミングサービスは初期化時にこの属性を読み取ります。このリストには、1 つの Identity Server 構成内の Identity Server セッションサーバーが含まれます。たとえば、2 つの Identity Server をインストールして 1 つのサーバーとして動作させる場合は、両方ともこのリストに入れる必要があります。サービス URL の要求で指定したホストがこのリストにない場合、ネーミングサービスは要求を拒否します。このリストの最初の値は、インストール時に指定したサーバーのホスト名およびポートを指定します。最後の値は、サーバーを一意に特定する 2 バイトの値です。ロードバランスに参加するサーバーには、それぞれに固有の識別子が必要です。これはまた、サーバー URL をサーバー ID にマッピングして Cookie の長さを短くするためにも使用されます。次に例を示します。

```
protocol:// サーバードメイン : ポート |01
```

protocol:// サーバードメイン : ポート |01| インスタンス名の形式を使用して、サーバーを追加できます。

プラットフォームロケール

プラットフォームロケールの値は、Identity Server とともにインストールしたデフォルトの言語サブタイプです。認証サービス、ログサービス、および管理サービスは、この値の言語で管理されます。デフォルトは en_US です。サポートされている言語サブタイプの全リストについては、201 ページの表 19-1 を参照してください。

Cookie ドメイン

これはドメインのリストで、認証中にユーザーのブラウザに Cookie を設定するときに Cookie ヘッダーで返されます。空の場合、Cookie ドメインは設定されません。言い換えると、Identity Server セッション Cookie は Identity Server 自体にだけ転送され、ドメインのほかのサーバーには転送されません。ドメインのほかのサーバーで SSO が必要な場合は、Cookie ドメインでこの属性を設定する必要があります。1 つの Identity Server 上で異なるドメインに 2 つのインタフェースがある場合、両方の Cookie ドメインをこの属性に設定する必要があります。ロードバランサを使用する場合、Cookie ドメインは、ロードバランサの背後にあるサーバーではなく、ロードバランサのドメインのものであることが必要です。このフィールドのデフォルト値はインストールされている Identity Server のドメインです。

ログインサービス URL

このフィールドはログインページの URL を指定します。この属性のデフォルト値は / サービス配備 *URI*/UI/Login です。

ログアウトサービス URL

このフィールドはログアウトページの URL を指定します。この属性のデフォルト値は / サービス配備 *URI*/UI/Logout です。

使用可能なロケール

この属性は、プラットフォーム用に設定したすべての使用可能なロケールを格納します。たとえば、ユーザーにロケールを選択させるアプリケーションを考えます。このアプリケーションは、プラットフォームのプロファイルからこの属性を取得して、ロケールのリストをユーザーに提示します。ユーザーがロケールを選択すると、アプリケーションがそれをユーザーエントリ `preferredLocale` に設定します。

クライアント文字セット

この属性は、プラットフォームレベルのさまざまなクライアント用の文字セットを指定します。これには、クライアントタイプのリスト、および対応する文字セットも含まれます。形式は次のとおりです。

```
clientType|charset

clientType2|charset
```

次に例を示します。

```
genericHTML|UTF-8
```

第 35 章

ポリシー設定サービス属性

ポリシー設定サービス属性には、グローバル属性と組織属性とがあります。グローバル属性に適用される値は Sun ONE Identity Server 設定全体に適用され、設定済みのすべての組織に継承されます。グローバル属性の目的は Identity Server アプリケーションのカスタマイズであるため、ロールまたは組織に直接適用することはできません。サービス管理の下で組織属性に適用される値が、ポリシー設定のデフォルト値になります。組織にサービスを登録した後、サービステンプレートを作成する必要があります。デフォルト値は組織の管理者が登録後に変更できます。組織属性は組織のエントリに継承されません。ポリシー設定属性は次のように分けられます。

グローバル属性

ポリシー設定サービスのグローバル属性には、次のものがあります。

リソースコンパレータ

この属性はリソースコンパレータ情報を指定します。リソースコンパレータは、「ポリシー」ルール定義で指定されたリソースの比較に使用されます。リソースの比較は、ポリシーの作成と評価の両方に使用します。この属性には次の値があります。

`serviceType`	コンパレータを使用するサービスを指定します。
`class`	リソース比較アルゴリズムを実装する Java クラスを定義します。

wildcard	リソース名に使用可能なワイルドカードを指定します。
delimiter	リソース名に使用する区切り記号を指定します。
caseSensitivity	リソースを比較する際に、大文字と小文字を区別するかどうかを指定します。False の場合は区別せず、True の場合は区別します。

組織属性

ポリシー設定サービスの組織属性は次のとおりです。

- LDAP サーバーとポート
- LDAP ベース DN
- LDAP ユーザーベース DN
- Identity Server ロールベース DN
- LDAP バインド DN
- LDAP バインドパスワード
- LDAP バインドパスワード (確認)
- LDAP 組織検索フィルタ
- LDAP 組織検索範囲
- LDAP グループ検索フィルタ
- LDAP グループ検索範囲
- LDAP ユーザー検索フィルタ
- LDAP ユーザー検索範囲
- LDAP ロール検索フィルタ
- LDAP ロール検索範囲
- Identity Server ロール検索範囲
- LDAP 組織検索属性
- LDAP グループ検索属性
- LDAP ユーザー検索属性
- LDAP ロール検索属性
- 検索で返される結果の最大数

- 検索のタイムアウト (秒)
- LDAP SSL を有効
- LDAP 接続プールの最小サイズ
- LDAP 接続プールの最大サイズ
- 選択したポリシーサブジェクト
- 選択したポリシー条件
- 選択したポリシー参照
- サブジェクト結果の有効時間
- ユーザーエイリアスを有効

LDAP サーバーとポート

このフィールドは、Identity Server インストール時に指定されるプライマリ LDAP サーバーのホスト名とポート番号を指定します。このホスト名とポート番号は、LDAP ユーザー、LDAP ロール、LDAP グループなどのポリシーサブジェクトを検索する際に使用します。形式は *hostname:port* です。次に例を示します。

```
machine1.example.com:389
```

複数の LDAP サーバーホストに対するフェイルオーバー設定の場合は、この値にスペース区切りのリストで複数のホストを指定できます。形式は hostname1:port1 hostname2:port2... です。

次に例を示します。

```
machine1.example1.com:389 machine2.example1.com:389
```

複数のエントリの場合は、ローカルサーバー名をプレフィックスとして付ける必要があります。これにより、特定の Identity Server が特定の Directory Server と通信するように設定できます。

形式は `servername|hostname:port` です。

次に例を示します。

```
machine1.example1.com|machine1.example1.com:389
machine1.example2.com|machine1.example2.com:389
```

フェイルオーバー設定の場合は次のようになります。

```
machine1.example1.com|machine1.example1.com:389 machine2.example.com1:389
machine1.example2.com|machine1.example2.com:389 machine2.example2.com:389
```

注

この属性は、複数のサーバーをサポートする値のリストを使用できるように変更されました。6.0 SP1 リリースでは、単一の値しか使用できませんでした。

この変更により、6.0 SP1 および 6.1 を単一の配備環境に共存させようとすると、Identity Server 6.0 SP1 インスタンスが 6.1 の DIT を指している場合は特に、問題が起こるおそれがあります。

共存できるようにするには、この属性に単一 LDAP サーバーだけを指定するようにしてください。

LDAP ベース DN

このフィールドは、検索を開始する LDAP サーバー内のベース DN を指定します。デフォルトでは、Identity Server インストールの最上位組織です。

LDAP ユーザーベース DN

この属性は、検索を開始する LDAP サーバー内の LDAP ユーザーサブジェクトで使用するベース DN を指定します。デフォルトでは、Identity Server インストールベースの最上位組織です。

Identity Server ロールベース DN

この属性は、検索を開始する LDAP サーバー内の Identity Server ロールサブジェクトで使用するベース DN を指定します。デフォルトでは、Identity Server インストールベースの最上位組織です。

LDAP バインド DN

このフィールドは、LDAP サーバー内のバインド DN を指定します。

LDAP バインドパスワード

この属性は、LDAP サーバーへのバインドに使用するパスワードを定義します。デフォルトで、インストール中に入力した amldapuser パスワードが、バインドユーザーとして使用されます。

LDAP バインドパスワード (確認)

LDAP バインドパスワードの確認。

LDAP 組織検索フィルタ

組織エントリの検索に使用する検索フィルタを指定します。デフォルトは (objectclass=sunMangagedOrganization) です。

LDAP 組織検索範囲

この属性は、組織エントリの検索範囲を定義します。範囲は次のいずれかにする必要があります。

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB (デフォルト)

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。デフォルトは、(objectclass=groupOfUniqueNames) です。

LDAP グループ検索範囲

この属性は、グループエントリの検索範囲を定義します。範囲は次のいずれかにする必要があります。

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB（デフォルト）

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。デフォルトは、(objectclass=inetorgperson) です。

LDAP ユーザー検索範囲

この属性は、ユーザーエントリの検索範囲を定義します。範囲は次のいずれかにする必要があります。

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB（デフォルト）

LDAP ロール検索フィルタ

ロールのエントリ検索に使用する検索フィルタを指定します。デフォルトは、(&(objectclass=ldapsubentry)(objectclass=nsroledefinitions)) です。

LDAP ロール検索範囲

この属性は、ロールのエントリ検索範囲を定義します。範囲は次のいずれかにする必要があります。

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB（デフォルト）

Identity Server ロール検索範囲

この属性は、Identity Server ロールサブジェクトのエントリ検索範囲を定義します。範囲は次のいずれかにする必要があります。

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB (デフォルト)

LDAP 組織検索属性

このフィールドは、組織に対して検索を行うための属性タイプを定義します。デフォルトは o です。

LDAP グループ検索属性

このフィールドは、グループに対して検索を行うための属性タイプを定義します。デフォルトは cn です。

LDAP ユーザー検索属性

このフィールドは、ユーザーに対して検索を行うための属性タイプを定義します。デフォルトは uid です。

LDAP ロール検索属性

このフィールドは、ロールに対して検索を行うための属性タイプを定義します。デフォルトは cn です。

検索で返される結果の最大数

このフィールドは検索で返される結果の最大数を定義します。デフォルト値は 100 です。指定された最大数を検索結果が上回った場合、その時点までに検索されたエントリが返されます。

検索のタイムアウト (秒)

この属性は、検索のタイムアウトが発生するまでの時間を指定します。指定した時間を過ぎた場合は、その時点までに検索されたエントリが返されます。

LDAP SSL を有効

この属性は、LDAP サーバーが SSL を実行するかどうかを指定します。選択した場合、SSL は有効になり、選択しない場合 (デフォルト)、SSL は無効になります。

LDAP 接続プールの最小サイズ

この属性は、LDAP サーバー属性に指定されたとおり、Directory Server への接続に使用する接続プールの最小サイズを指定します。デフォルトは 1 です。

LDAP 接続プールの最大サイズ

この属性は、LDAP サーバー属性に指定されたとおり、Directory Server への接続に使用する接続プールの最大サイズを指定します。デフォルトは 10 です。

選択したポリシーサブジェクト

この属性を使用すると、組織内のポリシー定義に使用できるサブジェクトタイプのセットを選択できます。

選択したポリシー条件

この属性を使用すると、組織内のポリシー定義に使用できる条件タイプのセットを選択できます。

選択したポリシー参照

この属性を使用すると、組織内のポリシー定義に使用できる参照タイプのセットを選択できます。

サブジェクト結果の有効時間

この属性は、キャッシュされたサブジェクト結果を使用して、シングルサインオントークンに基づく同じポリシー要求を評価できる時間 (分単位) を指定します。

ポリシーが SSO トークンに対して最初に評価される場合に、そのポリシー内のサブジェクトインスタンスが評価され、ポリシーを特定のユーザーに適用できるかどうかが判別されます。サブジェクト結果は SSO トークン ID に合わされ、ポリシーにキャッシュされます。「サブジェクト結果の有効時間」属性で指定された時間内に、同一の SSO トークン ID に対する同一のポリシーで別の評価が発生した場合、ポリシーフレームワークはキャッシュされたサブジェクト結果を検索します。サブジェクトインスタンスは評価しません。これにより、ポリシー評価の時間が大幅に短縮されます。

ユーザーエイリアスを有効

リモート Directory Server でリソースのサブジェクトのメンバーがローカルユーザーをエイリアス化するとき、そのリソースを保護するためのポリシーを作成する場合は、この属性を有効にする必要があります。

リモート Directory Server で `uid=rmuser` を作成し、Identity Server で `rmuser` をエイリアスとしてローカルユーザーに追加する (`uid=luser` など) ような場合、この属性は有効でなければなりません。`rmuser` としてログインすると、ローカルユーザー (`luser`) でセッションが作成され、ポリシーの適用が成功します。

第 36 章

SAML サービス属性

SAML (Security Assertion Markup Language) サービス属性はグローバル属性です。これらの属性に適用される値は Sun ONE Identity Server 設定全体に適用され、設定済みのすべての組織に継承されます。グローバル属性の目的は Identity Server アプリケーションのカスタマイズであるため、ロールまたは組織に直接適用することはできません。

SAML サービスのアーキテクチャの詳細は、『Sun ONE Identity Server Customization and API Guide』を参照してください。

SAML 属性は次のとおりです。

- サイト ID とサイト発行者名
- 署名要求
- 署名応答
- 署名アサーション
- アーティファクト名
- ターゲット指定子
- アーティファクトのタイムアウト (秒)
- notBefore 時間のアサーションスキュー
- アサーションのタイムアウト (秒)
- 信頼パートナーサイト
- ターゲット URL への POST

サイト ID とサイト発行者名

この属性にはエントリの一覧が含まれ、各エントリにはインスタンス ID、サイト ID、およびサイト発行者名が含まれます。インストール時にはデフォルト値が割り当てられます。形式は次のとおりです。

`instanceid=serverprotocol://servername:portnumber|siteid=`*site_id*
`|issuerName=`*site_issuer_name*

ソースサイトと目的サイトの両方で SSL 用にこの属性を設定したら、`instanceid` のプロトコルが `HTTPS//` であることを確認してください。

署名要求

この属性は、配信前にすべての SAML 要求にデジタル署名 (`XML DSIG`) するかどうかを指定します。このオプションをクリックすると、この機能が有効になります。

署名応答

この属性は、配信前にすべての SAML 応答にデジタル署名 (XML DSIG) するかどうかを指定します。このオプションをクリックすると、この機能が有効になります。

このオプションを有効にするかどうかにかかわらず、SAML Web Post プロファイルが使用するすべての SAML 応答にデジタル署名が行われます。

署名アサーション

この属性は、配信前にすべての SAML アサーションにデジタル署名 (`XML DSIG`) するかどうかを指定します。このオプションをクリックすると、この機能が有効になります。

アーティファクト名

この属性は、SAML サービス設定で定義されている SAML アーティファクトに変数名を割り当てます。SAML アーティファクトはサイズ制限付きのデータであり、アサーションとソースサイトを特定します。URL の照会文字列の一部として送られ、目的サイトへのリダイレクトによって転送されます。デフォルト値は SAMLart です。たとえば、デフォルトの SAMLart サービスを使用する場合、リダイレクトの照会文字列は次のようになります。

http:/ ホスト : ポート / 配備
URI/SamlAwareServlet?TARGET=http://*URL*/&SAMLart=artifact123

ターゲット指定子

この属性は、リダイレクトに使用される目的サイトの URL に変数名を割り当てます。デフォルト値は Target です。

アーティファクトのタイムアウト (秒)

この属性は、アーティファクト用に作成したアサーションのタイムアウトを指定します。デフォルトは 400 です。

notBefore 時間のアサーションスキュー

この属性を使用して、アサーションの notBefore 時間を計算します。たとえば、IssueInstant が 2002-09024T21:39:49Z で、「notBefore 時間のアサーションスキュー」の値が 300 秒 (180 秒がデフォルト値) に設定されている場合、アサーションの条件要素の notBefore 属性は 2002-09-24T21:34:49Z になります。

アサーションのタイムアウト (秒)

この属性は、アサーションのタイムアウトが発生するまでの秒数を指定します。デフォルトは 420 です。

注 アサーションの有効な総時間は、notBefore 時間のアサーションスキュー属性、およびアサーションのタイムアウト属性の両方の値に設定された値で決まります。

信頼パートナーサイト

この属性は、あるサイトが別のパートナーサイトと信頼関係を確立して通信できるように、パートナーの情報を保存します。

この属性にはエントリの一覧が含まれ、各エントリにはキーとその値が「|」記号で区切られたペアの形で含まれます。各エントリにはソース ID が必要です。次に例を示します。

`SourceID=siteid|SOAPURL=https://servername:portnumber/amserver/SAMLSOAPReceiver|AuthType=SSL|hostlist=ipaddress` (あるいは、サーバー の DNS 名または証明書エイリアス)

パラメータは次のとおりです。

表 36-1 信頼パートナーサイトのパラメータ

`SourceID`	「サイト ID とサイト発行者名」と同様に定義される 20 バイトのシーケンス

表 36-1　信頼パートナーサイトのパラメータ (続き)

target	このパラメータは、特定のドメインとして定義されます。ポート番号を含む場合と含まない場合とがあります。特定のドメインにホスティングされている Web ページにアクセスしたい場合、target はその後の処理のためパラメータ SAMLUrl または POSTUrl で定義される URL へのリダイレクトを指定します。 「信頼パートナーサイト」属性に指定された同一のドメインを持つエントリで、ポート番号を含むものと含まないものの 2 つのエントリがある場合、ポート番号を含むエントリが優先されます。 たとえば次のように、信頼されたパートナーサイトの定義が 2 つある場合を考えます。 target=sun.com|SAMLUrl=http://machine1.sun.com:8080/amserver/SAMLAwareServlet および target=sun.com:8080|SAMLUrl=httyp://machine2.sun.com:80/amserver/SAMLAwareServlet 両方とも次のページを検索しているものとします。 http://somemachine.sun.com:8080/index.html 上記の場合、一致するドメインとポートの両方が 2 番目の定義の target パラメータ内にあるので、2 番目の定義が SAML サービスプロバイダとして選択されます。
SAMLUrl	SAML サービスを提供する URL を定義します。URL に定義されたサーブレットは、「OASIS-SAML Bindings and Profiles」仕様に定義された「Web-browser SSO with Artifact」プロファイルを実装します
POSTUrl	SAML サービスを提供する URL を定義します。URL に定義されたサーブレットは、「OASIS-SAML Binding and Profiles」仕様に定義された「Web-browser SSO with POST」プロファイルを実装します。
issuer	Identity Server 内で生成されたアサーションの作成者を定義します。構文は hostname:port です。
SOAPUrl	SOAP 受信者サービス URL を指定します。

表 36-1　信頼パートナーサイトのパラメータ (続き)

AuthType	SAML で使用する認証タイプを定義します。次のいずれかになります。 • NOAUTH • BASICAUTH • SSL • SSLWITHBASICAUTH このパラメータは省略可能です。指定しない場合、デフォルトは NOAUTH です。 BASICAUTH または SSLWITHBASICAUTH が指定されている場合、User パラメータは必須で、SOAPUrl には HTTPS を指定する必要があります。
User	パートナーの SOAP 受信者の保護に使用するパートナーの uid を定義します。
hostlist	この属性は、特定のパートナーサイトに対して要求を送信可能なすべてのホストの IP アドレスと certAlias の両方または一方をリストします。これによって、要求の送信者が確実に SAML アーティファクトの本来の受信者であると保証されます。 要求者のホストまたはクライアントの証明書が、受信者のサイトでこのリストに含まれている場合は、サービスが続行されます。ホストまたはクライアントの証明書が、このホストリストに含まれているどのホストや証明書にも一致しない場合、SAML サービスは要求を拒否します。
AccountMapper	アサーションのサブジェクトと目的サイトでの位置付けとを関連付ける方法を定義する、プラグイン可能なクラスを指定します。デフォルトでは、次のようになります。 com.sun.identity.saml.plugins.DefaultAccountMapper
attributeMapper	attributeMapper がある場所へのパスを持つクラスを指定します。アプリケーションは、attributeMapper を展開して、SSOToken ID または AuthenticationStatement を含むアサーションを照会から取得できます。その後、マッパーを使用してサブジェクトの属性を取得します。attributeMapper が指定されていない場合は、DefaultAttributeMapper が使用されます。

表 36-1　信頼パートナーサイトのパラメータ (続き)

actionMapper	actionMapper がある場所へのパスを持つクラスを指定します。アプリケーションは、actionMapper を展開して、SSOToken ID または AuthenticationStatement を含むアサーションを照会から取得できます。その後、マッパーを使用して、照会に定義されているアクションの認証決定を取得します。actionMapper が指定されていない場合は、DefaultActionMapper が使用されます。
siteAttributeMapper	siteAttributeMapper がある場所へのパスを持つクラスを指定します。アプリケーションは、siteAttributeMapper を展開して、SSO 中にアサーションに組み込む属性を取得できます。siteAttributeMapper が見つからない場合、属性は SSO 中にアサーションに組み込まれません。
certAlias=*aliasName*	パートナーがアサーションに署名しているのに、署名されたアサーションの KeyInfo 部分にパートナーの証明書が見つからない場合に、アサーションで署名を検証するために使用する certAlias 名を指定します。

信頼されたパートナーサイトに対する設定例を、以下の表に示します。必ずしもすべてのパラメータを指定する必要はありません。省略可能なパラメータはカギかっこ ([]) で示しています。

	送信者	受信者
アーティファクト	sourceid	sourceid
	target	SOAPUrl
	SAMLUrl	[accountMapper]
	hostlist	[AuthType]
	[siteAttributeMapper]	[User]
		[certAlias]
POST プロファイル	sourceid	sourceid
	target	issuer
	POSTUrl	[accountMapper]

	送信者	受信者
	[siteAttributeMapper]	[certAlias]
SOAP 要求		sourceid hostlist [attributeMapper] [actionMapper] [certAlias] [issuer]

ターゲット URL への POST

アーティファクトプロファイルまたは POST プロファイルの SSO 経由で受信したターゲット URL がこの属性に含まれている場合、SSO から受信したアサーションは http:FORM POST によってターゲット URL に送信されます。POST にテストの URL またはその他の URL は使用しないでください。

第 37 章

セッションサービス属性

セッションサービス属性はグローバルおよびダイナミック属性です。グローバル属性に適用される値は Identity Server 設定全体に適用され、設定済みのすべての組織に継承されます。グローバル属性の目的は Identity Server アプリケーションのカスタマイズなので、ロールまたは組織に直接適用することはできません。

ダイナミック属性に適用される値は、ロールまたは組織に適用されます。ロールがユーザーに適用されると、またはユーザーが組織に割り当てられると、これらの属性はデフォルトでユーザーに継承されます。デフォルトセッションの値は、サービス設定で Identity Server のすべての登録組織に対して設定されます。これらの値は、セッションサービスを特定の組織に登録し、テンプレートを作成して、デフォルト値以外の値を入力することによって、個々の組織に対して異なる設定にすることができます。

グローバル属性

グローバル属性は次のとおりです。

- 検索結果の最大数
- 検索のタイムアウト (秒)

検索結果の最大数

この属性はセッション検索で返される結果の最大数を指定します。デフォルト値は 120 です。

検索のタイムアウト (秒)

この属性はセッション検索を終了するまでの最大時間を定義します。デフォルト値は 5 秒です。

ダイナミック属性

ダイナミック属性は次のとおりです。

- 最大セッション時間 (分)
- 最大アイドル時間 (分)
- 最大キャッシュ時間 (分)

最大セッション時間 (分)

この属性は、セッションが期限切れになるまでの最大時間を分単位で表す値を指定します。期限が切れると、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。有効な値は 1 以上です。デフォルト値は 120 です。セキュリティと利便性の要求のバランスをとるためには、最大セッション時間の間隔にはより大きい値を設定し、最大アイドル時間の間隔には比較的小さい値を設定してください。最大セッション時間では、セッションの有効期限を指定します。設定した値を超えて延長されることはありません。

最大アイドル時間 (分)

この属性は、セッションが期限切れになるまでのアクティビティのない最大時間に等しい値 (分単位) を指定します。期限が切れると、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。有効な値は 1 以上です。デフォルト値は 30 です。セキュリティと利便性の要求のバランスをとるためには、最大セッション時間の間隔にはより大きい値を設定し、最大アイドル時間の間隔には比較的小さい値を設定してください。

最大キャッシュ時間 (分)

この属性は、クライアントが Identity Server と通信してキャッシュされたセッション情報を更新するまでの最大間隔に等しい値 (分単位) を指定します。有効な値は 0 以上です。デフォルト値は 3 です。最大キャッシュ時間は常に最大アイドル時間より小さくなるように設定してください。

第 38 章

ユーザー属性

ユーザー属性を格納する場所は 2 つあります。「サービス設定」ウィンドウと「ユーザー管理」ウィンドウです。「サービス設定」ウィンドウには、登録されている組織のデフォルト属性が含まれます。「ユーザー管理」ウィンドウには、ユーザーエントリ属性が含まれます。

- ユーザーサービス属性
- ユーザープロファイル属性
- ユーザー ID の一意性

ユーザーサービス属性

ユーザーサービス属性はダイナミック属性です。ダイナミック属性に適用される値は、Identity Server で設定されるロールまたは組織に割り当てられます。ロールがユーザーに割り当てられるか、ユーザーが組織に割り当てられる場合は、ダイナミック属性がそのユーザーの特性になります。ユーザー属性は次のように分けられます。

- ユーザー設定言語
- ユーザー設定タイムゾーン
- 継承されたロケール
- 管理者 DN 開始表示
- デフォルトユーザー状態

デフォルトユーザーの値は、Identity Server のすべての登録組織に対して設定されます。これらの値は、ユーザーサービスを特定の組織に登録し、テンプレートを作成して、デフォルト値以外の値を入力することによって、個々の組織に対して異なる設定にすることができます。

ユーザー設定言語

このフィールドは、Identity Server コンソールに表示されるテキスト言語に関するユーザーの選択項目を指定します。デフォルト値は en です。この値によってユーザーセッションへの地域対応化キーのセットがマップされて、画面のテキストがユーザーに合った言語で表示されます。

ユーザー設定タイムゾーン

このフィールドは、ユーザーが Identity Server コンソールにアクセスするタイムゾーンを指定します。デフォルト値はありません。

継承されたロケール

このフィールドは、ユーザーのロケールを指定します。デフォルト値は en_US です。201 ページの表 19-1 のすべての値を使用できます。

管理者 DN 開始表示

このユーザーが Identity Server 管理者の場合、このフィールドはユーザーがログインするときに Identity Server コンソールに表示される開始点となるノードを指定します。デフォルト値はありません。ユーザーが少なくとも読み取りアクセス権を持っている有効な DN を使用することができます。

デフォルトユーザー状態

このオプションは、新しく作成したユーザーのデフォルト状態を示します。ユーザーエントリ状態の方がこの状態よりも優先されます。有効なユーザーだけが Identity Server を使用して認証を受けることができます。デフォルト値は有効です。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。

- 有効 - ユーザーは Identity Server を使用して認証を受けることができます。
- 無効 - ユーザーは Identity Server 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。

個々のユーザー状態は、ユーザーサービスを登録し、値を選択してロールに適用し、そのロールをユーザープロファイルに追加することによって設定します。

ユーザープロファイル属性

ユーザープロファイル属性はユーザープロファイルのデフォルト属性です。この値は、管理者またはユーザーがログイン時にユーザープロファイル表示で設定します。管理者は、自分のユーザー属性をユーザープロファイルに追加したり、新しいサービスを作成したりできます。詳細は、『Sun ONE Identity Server Customization and API Guide』を参照してください。

注 Identity Server ではユーザーエントリ内の属性の一意性は必ずしも必要ではありません。たとえば `userA` と `userB` はどちらも同じ組織で作成されているとします。どちらの場合も、電子メールアドレス属性を `jimb@madisonparc.com` に設定できます。管理者は、Sun ONE Directory Server の属性の一意性プラグインを設定することによって、一意な属性値になるようにすることができます。詳細は、この章の末尾にある「一意なユーザー ID」または『Sun ONE Directory Server 管理者ガイド』を参照してください。

名 (ファーストネーム)

このフィールドはユーザーのファーストネームを取得します。ファーストネーム値とラストネーム値によって、Identity Server コンソールの右上隅にあるログイン名を示すフィールドのユーザーが識別されます。

姓 (ラストネーム)

このフィールドはユーザーのラストネームを取得します。ファーストネーム値とラストネーム値によって、Identity Server コンソールの右上隅にあるログイン名を示すフィールドの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取得します。

パスワード (確認)

パスワードの確認。

電子メールアドレス

このフィールドはユーザーの電子メールアドレスを取得します。

社員番号

このフィールドはユーザーの社員番号を取得します。

電話番号

このフィールドはユーザーの電話番号を取得します。

ホームアドレス

このフィールドはユーザーのホームアドレスを取得します。

ユーザー状態

このオプションは、Identity Server 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。有効なユーザーだけが Identity Server を使用して認証を受けることができます。デフォルト値は有効です。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。

- 有効 - ユーザーは Identity Server を使用して認証を受けることができます。
- 無効 - ユーザーは Identity Server 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「無効」に変えても、Identity Server 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。Identity Server 認証を無効にしたユーザーアカウントでも、Identity Server を必要としないタスクは実行できます。Identity Server 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 true 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 Identity Server ユーザープロファイルのページに追加することを考慮してください。詳細は、『Sun ONE Identity Server Customization and API Guide』を参照してください。

アカウント有効期限

この属性が存在する場合、指定されたアカウント有効期限が現在の日付以前であれば、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、ユーザーの認証方法を設定します。デフォルトの認証方法は LDAP です。1 つまたは複数の認証方法を、「編集」リンクをクリックすることによって選択できます。複数の認証方法を選択した場合、選択した方法すべてに対してユーザーは認証に成功する必要があります。

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。デフォルト値は en_US です。201 ページの表 19-1 のすべての値を使用できます。

プルダウンメニューで次の属性のどれかを選択できます。

- 無視
- カスタマイズ
- 継承

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。

ユーザー ID の一意性

Identity Server アプリケーション内で uid の一意性を実現するには、Directory Server で利用可能なプラグインを次のように設定する必要があります。

```
dn:cn=uid uniqueness,cn=plugins,cn=config
objectClass:top
objectClass:nsSlapdPlugin
objectClass:extensibleObject
cn:uid uniqueness
nsslapd-pluginPath:/ids908/lib/uid-plugin.so
nsslapd-pluginInitfunc:NSUniqueAttr_Init
nsslapd-pluginType:preoperation
nsslapd-pluginEnabled:on
nsslapd-pluginarg0:attribute=uid
nsslapd-pluginarg1:markerObjectClass=nsManagedDomain
```

```
nsslapd-plugin-depends-on-type:database

nsslapd-pluginId:NSUniqueAttr

nsslapd-pluginVersion: 6.1

nsslapd-pluginVendor: Sun | SunONE

nsslapd-pluginDescription:Enforce unique attribute values
```

nsManagedDomain オブジェクトクラスは、uid の一意性を必要とする組織にマークを付けるために使用することをお勧めします。プラグインは、デフォルトでは有効ではありません。

組織ごとに uid の一意性を設定するには、プラグインエントリに各組織の DN を追加するか、またはマーカーオブジェクトクラスオプションを使用して nsManagedDomain を最上位レベルの組織エントリのそれぞれに追加します。

```
nsslapd-pluginEnabled:on

nsslapd-pluginarg0:attribute=uid

nsslapd-pluginarg1:markerObjectClass=nsManagedDomain
```

エラーコード

この付録では、Sun ONE Identity Server によって生成されるエラーメッセージの一覧を示します。この一覧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、エラーの説明や考えられる原因、および、発生した問題を修正する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一覧を示します。

- Identity Server コンソールのエラー
- 認証エラーコード
- ポリシーエラーコード
- amadmin エラーコード

エラー診断に支援が必要な場合は、次の Web サイトから Sun ONE 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

Identity Server コンソールのエラー

次の表は、Identity Server 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一覧です。

表 A-1 Identity Server 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他のユーザーによって削除された可能性がある	削除しようとしているオブジェクトを再表示し、操作をやり直す
入力した URL が無効です。	Identity Server コンソールウィンドウの URL が正しく入力されなかった場合に発生する	
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なかった	パラメータを変更して検索をやり直す
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ない	
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ない	
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は、許容数を超えるエントリが返された	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する。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る
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は、許容値より長い検索時間がかかった	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する。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る
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 が無効になった	ユーザープロファイルページで、開始 DN の値を有効な DN に変更する
アイデンティティ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まる	

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一覧です。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 A-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
ログインしました。	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るが、成功の場合のリダイレクト URL が定義されていない	ログアウトするか、Identity Server コンソールを使ってログイン成功リダイレクト URL をセットアップする。管理コンソール URL として、この値に 'goto' 照会パラメータを使用する
ログアウトに失敗しました。	ユーザーが Identity Server からログアウトできない	サーバーを再起動する
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する
デフォルトページにリダイレクトできません。	Identity Server で成功 URL または失敗 URL にリダイレクトできない	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する
もう一度やり直してください。ログインに進んでください	このリンクは、ほとんどのエラー発生時に生成される。ユーザーはこのリンクをクリックして、元のログイン URL ページに戻る	
入力したパスワードは無効です。	入力したパスワードが無効である	パスワードは 8 文字以上でなければならない。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する
認証に失敗しました。	認証に失敗した。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る。最も一般的な原因は、資格情報が無効または不正であること	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情報) を正しく入力する

表 A-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
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。もう一度ログイン情報を入力してください。初めてシステムに入るのであれば、ログイン画面で「新規ユーザー」を選択してください。	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らなかった。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る	ログイン情報を入力し直す。初めてログインする場合は、ログイン画面で「新規ユーザー」を選択する
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る。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る	デフォルトでは、ログインパスワードは 8 文字以上でなければならない。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る
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る。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る	ユーザー ID は組織内で一意にする必要がある
「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ない。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る	ユーザー名とパスワードは必ず異なる値にする
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なかった。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る	必ずユーザー名を入力する
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なかった。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る	必ずパスワードを入力する
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ない。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る	必ず「パスワードの確認」フィールドにパスワードを入力する

表 A-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
パスワードと確認のパスワードが一致しません。	パスワードと確認のパスワードが一致しない。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る	パスワードと確認のパスワードは必ず同じ値にする
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る	`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する
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ない	Identity Server 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する
内部認証エラー	内部認証エラー。これは一般的な認証エラーであり、さまざまな環境や設定の問題によって発生する	
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る	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する。 メモリ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、サーバーを再起動する
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ない。このエラーは、ロールベースの認証で表示される	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する
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た	ログインし直す
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る	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する

表 A-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。	設定が見つからない	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する
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 ドメインに存在しない	
そのような組織は見つかりません。	その組織は見つからない	有効な組織を正しく入力する
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ない	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する
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。	必須フィールドのどれかが未記入のままになっている。必ずすべての必須フィールドに入力する	必ずすべての必須フィールドに入力する
最大セッション数の限度に到しました。	最大セッション数の限度に達した	ログアウトし、ログインし直す

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、Identity Server コンソールに表示されるエラーコードの一覧です。

表 A-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
名前に不正な文字 / が含まれています。	ポリシー名に不正な文字 "/" が含まれている	ポリシー名に '/' という文字が含まれていないことを確認する
ポリシーは組織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る	別の名前を使ってポリシーを作成する
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る	別のルール名を使ってポリシーを作成する
同じ値を持つルールがすでに存在します。	同じルール値を持つルールがすでに存在している	別のルール値を使用する

表 A-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。組織への参照が存在しません。	組織への参照が存在しない	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る
Ldap 検索のサイズの限界を超えています。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てください。	LDAP 検索のサイズの上限を超えた。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する。検索サイズの上限は、ポリシー設定サービスにある
指定された Ldap 検索時間を過ぎています。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てください。	LDAP 検索の時間の上限を超えた。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する。最大セッション時間は、ポリシー設定サービスにある
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る。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 接続を取得できない
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 トークンが無効である	サーバーがアプリケーション SSO トークンを検証できなかった。SSO トークンの有効期限が切れている可能性が高い
ユーザー SSO トークンが無効です。	ユーザー SSO トークンが無効である	サーバーがユーザー SSO トークンを検証できなかった。SSO トークンの有効期限が切れている可能性が高い
プロパティ値は整数にしてください。	プロパティ値が整数でない	このプラグインのプロパティ値は整数にする必要がある
プロパティ値を定義する必要があります。	プロパティ値を定義する必要がある	そのプロパティに値を指定する
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 より大きい	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た。開始 IP を終了 IP より大きくすることはできない

表 A-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
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い	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た。開始日を終了日より大きくすることはできない
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は見つからない。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する
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ない。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ない	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する
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する

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 Identity Server のデバッグファイルに書き込まれるエラーコードの一覧です。

表 A-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
エラー 1: 引数が足りません。--runasdn または -u 、--password または -w のいずれか、--passwordfile または -f のいずれか、--schema または -s のいずれか、--data または -t のいずれか、および --addAttributes または -a のいずれかは、それぞれ必須の引数であり、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てください。	1	引数が足りない	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する
エラー 2: 入力 XML ファイルが見つかりません。	2	入力 XML ファイルが見つからなかった	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する

表 A-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
エラー 3: --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 が指定されていない	--runasdn の値としてユーザー DN を指定する
エラー 4: --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ない	--deleteservice の値としてサービス名を指定する
エラー 5: --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ない	--password の値としてパスワードを指定する
エラー 6: ロケール名が指定されていません。ロケールには en_US が指定されます。マニュアルを参照してください。	6	ロケール名が指定されなかった。ロケールには en_US が指定される	ロケールの一覧については、「デフォルト認証ロケール」を参照
エラー 7: 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ない	処理する入力 XML ファイルの名前を少なくとも 1 つ指定する
エラー 8: 無効なオプション	8	1 つ以上の引数が間違っている	すべての引数が有効であることを確認する。有効な引数の一覧を表示するには、amadmin --help と入力する
エラー 9: 操作に失敗しました。	9	操作に失敗した	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る。これらのエラーコードを参照して問題を評価する
エラー 10: 要求を処理できません。	10	要求を処理できない	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る。これらのエラーコードを参照して問題を評価する
エラー 12: ポリシーを作成できません。	12	ポリシーを作成できない	amadmin では、このエラーを示す例外メッセージが生成される。これらのメッセージを参照して問題を評価する
エラー 13: ポリシーを削除できません。	13	ポリシーを削除できない	amadmin では、このエラーを示す例外メッセージが生成される。これらのメッセージを参照して問題を評価する

表 A-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
エラー 14: サービスを削除できません。	14	サービスを削除できない	amadmin では、このエラーを示す例外メッセージが生成される。これらのメッセージを参照して問題を評価する
エラー 15: ユーザーを認証できません。	15	ユーザーを認証できない	ユーザー DN とパスワードが正しいことを確認する
エラー 16: 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ない	XML の形式が正しく、amAdmin.dtd に従っていることを確認する
エラー 17: 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初期化エラーのため、パースできない	XML の形式が正しく、amAdmin.dtd に従っていることを確認する
エラー 18: 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をビルドできないため、パースできない	amadmin では、このエラーを示す例外メッセージが生成される。これらのメッセージを参照して問題を評価する
エラー 19: 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ない	amadmin では、このエラーを示す例外メッセージが生成される。これらのメッセージを参照して問題を評価する
エラー 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。	20	XML ファイルが有効なファイルではないため、パースできない	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する
エラー 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。	21	XML ファイルが有効なファイルではないため、パースできない	amadmin では、このエラーを示す例外メッセージが生成される。これらのメッセージを参照して問題を評価する
エラー 22: 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る。これらのメッセージを参照して問題を評価する
エラー 23: 処理できません。	23	XML ファイルを処理できない	amadmin では、このエラーを示す例外メッセージが生成される。これらのメッセージを参照して問題を評価する
エラー 24: --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ない	すべての引数が有効であることを確認する。有効な引数の一覧を表示するには、amadmin --help と入力する

表 A-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
エラー 25: 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 ファイルは正しい DTD に従っていない	XML ファイルの DOCTYPE 要素を確認する
エラー 26: 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 認証に失敗した	ユーザー DN とパスワードが正しいことを確認する
エラー 28: ServiceManager 例外 (SSOException)	28	サービスマネージャ例外 (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る。これらのメッセージを参照して問題を評価する
エラー 29: ServiceManager 例外	29	サービスマネージャ例外	amadmin では、このエラーを示す例外メッセージが生成される。これらのメッセージを参照して問題を評価する
エラー 30: 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る。これらのメッセージを参照して問題を評価する
エラー 31: PolicyManager 例外 (SSOException)	31	ポリシーマネージャ例外 (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る。これらのメッセージを参照して問題を評価する
エラー 32: PolicyManager 例外	32	ポリシーマネージャ例外	amadmin では、このエラーを示す例外メッセージが生成される。これらのメッセージを参照して問題を評価する
エラー 33: 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る	デバッグオプションは 1 つだけ指定する必要がある
エラー 34: ログインに失敗しました !	34	ログインに失敗した	amadmin では、このエラーを示す例外メッセージが生成される。これらのメッセージを参照して問題を評価する
エラー 36: 属性値が無効です。	36	属性値が無効である	LDAP 検索に設定されているレベルを確認する。SCOPE_SUB または SCOPE_ONE でなければならない

表 A-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
エラー 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。	37	オブジェクトタイプの取得時にエラーが発生した	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する
エラー 38: 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する
エラー 39: 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する
エラー 40: 無効なスタティックグループ DN	40	無効なスタティックグループ DN	XML ファイル内の DN が有効であることと、スタティックグループオブジェクトであることを確認する
エラー 41: 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する
エラー 42: 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する
Error 43: Invalid Service Host Name	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する
エラー 44: 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る
エラー 45: サービススキーマはサブスキーマに対して null です。	45	サービスのサービススキーマを見つけることができない	XML ファイル内のサブスキーマが有効であることを確認する
エラー 46: RoleTemplate は、スキーマタイプがダイナミックの場合にのみ true となります。	46	ロールテンプレートは、スキーマタイプがダイナミックの場合にのみ true となる	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する
エラー 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。	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ない	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する

表 A-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
エラー 48: テンプレートが存在しません。	48	テンプレートが存在しない	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する
エラー 49: ダイナミックなグループにはユーザーを追加できません。	49	ダイナミックグループにはユーザーを追加できない	XML ファイル内のグループ DN がダイナミックグループでないことを確認する
エラー 50: 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ない	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する
エラー 51: 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らなかった	親組織または親コンテナにグループコンテナを作成する
エラー 52: フィルタリングされたロールからユーザーを消去できません。	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ない	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する
ダイナミックグループからユーザーを消去できません。	53	ダイナミックグループからはユーザーを削除できない	XML ファイル内のグループ DN がダイナミックグループでないことを確認する
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ない	XML ファイル内にサブスキーマ文字列があることを確認する

Identity Server を SSL モードに設定する

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。

Identity Server では、SSL 通信と非 SSL 通信を同時に使用できます。つまり、SSL 通信と非 SSL 通信とを選択する必要はなく、同時に両方を使用できます。

以降の節では、4 種類の Web コンテナで実行する場合に、Identity Server を SSL モードに設定する手順について説明します。

セキュリティ保護された Sun ONE Web Server で Identity Server を設定する

Sun ONE Web Server で実行する Identity Server 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。

1. Identity Server コンソールで、インストール中に作成される最上位組織の「プロパティ」の矢印をクリックします。

   「組織プロパティ」ウィンドウがデータフレームに表示されます。

2. 「保存」をクリックして変更を保存します。

3. Identity Server 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 4 ～手順 27 は Sun ONE Web Server について説明します。

4. 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、58888 です。
5. Identity Server 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。「OK」をクリックします。
6. 画面の右上部にある「Apply」ボタンをクリックします。
7. 「Apply Settings」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。
8. 選択した Web Server インスタンスを停止します。
9. 「Security」タブをクリックします。
10. 「Create Database」をクリックします。
11. 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。

    後で使用するために、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。
12. 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。
13. 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 11 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。
14. 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--
```

15. 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。

16. 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---
```

17. 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。
18. Web Server コンソールで、「Install Certificate」をクリックします。
19. 「Certificate for this Server」をクリックします。
20. 「Key Pair File Password」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。
21. 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。「Submit」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. 「Install Certificate」をクリックします。
23. 「Certificate for Trusted Certificate Authority」をクリックします。

24. 手順 18 ～手順 23 と同じ方法で、ルート CA 証明書をインストールします。
25. 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。
26. 別のポートで SSL を有効にしたい場合は、「Add Listen Socket」を選択します。次に、「Edit Listen Socket」を選択します。
27. セキュリティ状態を「Disabled」から「Enabled」に変更し、「OK」をクリックして変更を実行します。

手順 28 ～手順 30 は、Identity Server について説明します。

28. `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 `/opt/SUNWam/lib` です。
29. 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。
30. `AMConfig.properties` ファイルを保存します。
31. 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 Identity Server の「オン / オフ」ボタンをクリックします。

    Web Server で「起動 / 停止」ページにテキストボックスが表示されます。
32. 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、「開始」を選択します。

セキュリティ保護された Sun ONE Application Server で Identity Server を設定する

SSL が有効になっている Sun ONE Application Server 上で Identity Server を実行するには、次の 2 つのプロセスでセットアップを行います。まず、インストールされた Identity Server に対して Application Server をセキュリティで保護します。次に、Identity Server 自体を設定します。

Application Server で SSL をセットアップする

Application Server インスタンスをセキュリティで保護するには、次の手順を実行します。

1. ブラウザに次のアドレスを入力して、Sun ONE 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. Identity Server 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」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。後で使用するために、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 の一覧を表示するには、「List of Available Certificate Authorities」をクリックします。

Sun ONE Certificate Server を使用している内部 CA に証明書を要求する場合は、「証明書発行局 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。

「リクエスタ名」: 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 ONE Application Server の完全修飾名。

「電子メールアドレス」: 管理者の電子メールアドレス

「組織名」: 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。

「組織単位名」: 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. Sun ONE 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. 「証明書」の「このサーバー」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。これは、手順 9 で入力したパスワードです。
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. 手順 10 ～手順 22 と同じ方法で、ルート CA 証明書をインストールします。ただし、手順 18 では、「証明書」の「信頼できる証明書発行局 (CA)」を選択します。
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. Sun ONE Identity Server 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。

Identity Server を SSL モードに設定する

Identity Server と WebLogic を連動させて、SSL モードで実行するように設定するには、手順を実行します。

1. Identity Server コンソールで、インストール中に作成される最上位組織の「プロパティ」の矢印をクリックします。「組織プロパティ」ウィンドウがデータフレームに表示されます。
2. 「保存」をクリックして変更を保存します。
3. Identity Server 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。
4. `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。

   `/opt/SUNWam/lib`
5. 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。
6. `AMConfig.properties` ファイルを保存します。
7. Application Server を再起動します。

索引

J

L

N

O

R

S

U

V

あ

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

て

と

に

ね

は

ひ

ふ

へ

ほ

ま

め

ゆ

ら

り

る

れ

ろ