インストールおよび設定ガイド

Sun™ ONE Identity Server

Version 6.0

817-1573-10
2002 年 12 月

目 次

本書について

『インストールおよび設定ガイド』では、Sun™ Open Network Environment (Sun ONE) Identity Server の概要、および Identity Server を使用する場合の計画とインストールの方法について説明します。

ここでは、次の項目について説明します。

- お読みになる前に
- Sun ONE Identity Server のマニュアルセット
- 表記上の規則

お読みになる前に

本書は、Sun ONE Identity Server に付属する一連のマニュアルの中で、「最初」にお読みいただきたいマニュアルです。このマニュアルでは、ディレクトリテクノロジについて理解し、Java および XML プログラミング言語の使用経験があることを前提にしています。ディレクトリサーバや LDAP (Lightweight Directory Access Protocol) に精通していれば、このマニュアルを最大限に活用できます。Sun ONE Directory Server のマニュアルを精読して、製品の使用方法に慣れておくことをお勧めします。

このマニュアルは、Sun ONE のサーバおよびサービスを介したネットワークアクセスを管理する IT 技術者向けに書かれています。Identity Server に含まれる機能を利用すれば、全社的にユーザデータを管理し、アクセスポリシーを施行できます。

このマニュアルで説明する概念を理解すれば、『Sun ONE Identity Server Administration Guide』および『Sun ONE Identity Server Programmer's Guide』に記載されているように、Sun ONE Identity Server の管理およびカスタマイズを行えるようになります。

Sun ONE Identity Server のマニュアルセット

Sun ONE 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。

- 『インストールガイド』: Identity Server を使用する場合の計画とインストールの方法について詳しく説明します。
- 『Administration Guide』: Sun ONE Identity Server システムのインストール後、ユーザおよびサービスデータを管理する方法について説明します。
- 『Programmer's Guide』: Identity Server インタフェースのカスタマイズ方法について説明します。
- 『ポリシーエージェントガイド』: Web、Proxy、Application サーバに Sun ONE Identity Server ポリシーエージェントをインストールし、配備する方法について説明します。
- 『リリースノート』: このリリースの最新情報、インストールに関する最新の注意事項、既知の問題、制限事項、問題の報告方法などの各種情報を提供します。

注 リリースノートの更新およびマニュアルの改訂については、Identity Server マニュアルの Web サイトを確認してください。

`http://docs.sun.com/db/prod/s1idsrv`

表記上の規則

このマニュアルを含む Sun ONE Identity Server のマニュアルでは、説明を簡潔にし、内容をより理解しやすくするために、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次に説明します。

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、および文字通りの意味の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、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。
- Serif フォントは、コードおよびコードフラグメント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

Sun ONE 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、Sun ONE Identity Server および Sun ONE 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、専用 Web Server で実行される、インストール済みの Sun ONE 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。専用 Web Server は、ポリシーおよび管理サービスをインストールすると自動的にインストールされます。
- *Identity Server* を実行する Web Server 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 Web Server を示します。
- ディレクトリサーバは、Sun ONE Directory Server または Netscape™ Directory Server のインストール済みのインスタンスを示します。
- *IS_root* は、Sun ONE Identity Server をインストールしたホームディレクトリの可変部分を示します。
- *Directory_Server_root* は、Sun ONE Directory Server をインストールしたホームディレクトリの可変部分を示します。
- *Web_Server_root* は、Sun ONE Web Server をインストールしたホームディレクトリの可変部分を示します。

第 1 章

Sun ONE Identity Server の紹介

Sun ONE Identity Server は、企業向けインフラストラクチャソリューションです。Sun ONE Identity Server は、すべてのビジネス関係、サービス、データ、およびアクセス許可の設定の鍵です。Identity Server によって、顧客、社員、提携業者、および供給業者を 1 つのオンラインディレクトリに統合することができます。また、企業内のどの情報にだれがアクセスできるかに関するポリシーと権限を確立する手段を提供します。Identity Server は、急速に拡大するエクストラネットやホスティングサービスの要求に対応できるように設計されています。この章では、Identity Server ソリューションについて紹介します。

この章には次のトピックがあります。

- Identity Server ソリューション
- 主な機能と利点
- Identity Server 6.0 の新機能

Identity Server ソリューション

Identity Server は Sun ONE サーバ、サービス、およびエージェントで構成されています。Identity Server は、Sun ONE Directory Server の基本的な機能を拡張し、ユーザデータ、サービスデータ、およびアクセスポリシーを統合して、1 つのコンソールでこれらすべてを効率的に管理できるようにします。Identity Server を使用して、企業内の Web リソースへのアクセスを制御するロールとポリシーを定義し、適用することができます。また、これらのロールとポリシーによって、ユーザアカウントの管理を管理者だけでなく、管理者でない人にも委託することが可能になります。Identity Server のプラグイン可能なアーキテクチャにより、比較的簡単に新しいサービスを追加してその構成をユーザおよびポリシーに合わせてカスタマイズできます。

Identity Server を購入すると、Identity Server ソリューションを構成する Sun ONE サーバおよびサービスをすべて受け取ることができます。

- Sun ONE Directory Server 5.1
- Identity Server ポリシーサービスおよび管理サービス
- Identity Server コンソール
- Identity Server スキーマ
- ドメイン間シングルサインオン (CDSSO) コンポーネント
- 共通ドメインサービス

Identity Server と連携する Web エージェントは、別個のコンポーネントとして使用できます。Identity Server Web エージェントの詳細は、29 ページの「ポリシーエージェント」を参照してください。

Sun ONE Directory Server

Sun ONE Directory Server は、業界標準の Lightweight Directory Access Protocol (LDAP) に基づいた強力でスケーラブルな分散ディレクトリサーバです。Identity Server の導入では、Directory Server はユーザデータ、サービスデータ、およびアクセスポリシーの中央リポジトリになります。これにより、さまざまなサーバやアプリケーションが一貫性のあるデータを共有できます。

Identity Server ポリシーサービス

ポリシーサービスは、細分化され特化された 4 つのサービスで構成されています。認証、シングルサインオン、ログ、およびセッションです。これらのサービスが連携して、アクセスルールの適用を可能にします。アクセスルールは、アプリケーションへのログインをユーザに許可または拒否するポリシーを構成します。

認証

認証サービスは、アプリケーションにアクセスを試みるユーザのアイデンティティ (識別情報) を検証します。認証は、ログイン時にユーザの資格を検証するプラグイン可能ないくつかのモジュールによって実装されます。

シングルサインオン

シングルサインオン (SSO) サービスでは、アプリケーション間でユーザ情報を保存および転送するためのトークンを使用します。これにより、ユーザは企業に一度ログインすると、アプリケーションごとに認証をやり直さなくても複数の Web ベースアプリケーションにアクセスできます。サービスによって提供される Java API は、SSO トークンとエージェントを検証して、サーバに格納されている特定のページのアクセスルールとポリシーを適用します。

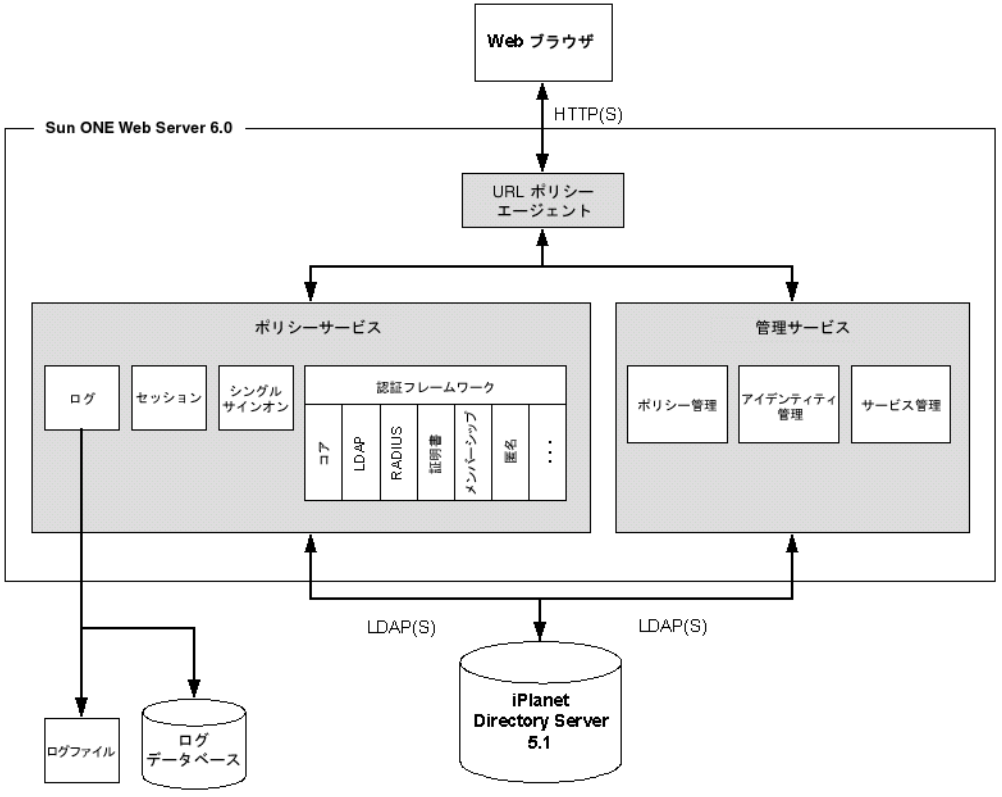
ログ

ログサービスは、ログ情報をログファイルまたはログデータベースに書き込みます。ログデータは、認証モジュールおよび Identity Server コンソールが使用します。

セッション

セッションサービスは、ユーザセッション情報と有効期間の情報を保持します。セッション情報は、シングルサインオンのトークンの検証に使用されます。

図 1-1　Identity Server アーキテクチャ



Identity Server 管理サービス

管理サービスは、細分化された 3 つのサービスで構成されています。ポリシー管理、アイデンティティ管理、およびサービス管理です。これらの 3 つのサービスは、Identity Server コンソールに統合され、1 箇所で企業管理を行うことができます。管理サービスを使って変更を行うと、Directory Server で自動的にそれらの変更が行われます。

ポリシー管理

ポリシー管理サービスは、組織およびサブ組織のアクセスルールとポリシーの作成、変更、および削除の手段を提供します。

アイデンティティの管理

アイデンティティ管理サービスは、ユーザ管理サービスとも呼ばれます。アイデンティティ管理は、ユーザ、ロール、グループ、ピープルコンテナ、組織、組織単位、およびサブ組織の作成および管理の手段を提供します。

サービス管理

サービス管理サービスは、サービスの登録と登録解除、およびディレクトリ内のオブジェクトに割り当てられたサービス属性の管理の手段を提供します。

Identity Server コンソール

Identity Server コンソールは、アイデンティティ、サービス、およびポリシーの管理を統合するグラフィカルインタフェースです。Identity Server コンソールを使用すると、ユーザ (管理者および非管理者のいずれの場合も) は、LDAP に関する知識がなくても、1 つのインタフェースを使って Directory Server でユーザアカウント、サービス属性、およびアクセスルールを作成および管理できます。

ドメイン間シングルサインオン

ドメイン間シングルサインオン (SSO) 機能により、ユーザは企業内の DNS ドメインで 1 回認証を行えば、別のドメインで実行中の Identity Server サービスにアクセスできます。このサービスは、ドメインにインストールしたコントローラとドメイン間シングルサインオン (CDSSO) コンポーネントを使って実装します。

ドメイン間コントローラ

ドメイン間コントローラ (CDC) コンポーネントは、アイデンティティ情報サービスのインストール時に自動的にインストールされます。このコントローラは、認証要求を適切に転送します。要求にシングルサインオン (SSO) 情報が含まれていない場合、コントローラはその要求を認証サービスに転送します。SSO 情報を含む要求は、照会文字列に付加された SSO 情報により、適切な CDSSO コンポーネントに送信されます。

ドメイン間のシングルサインオンコンポーネント

ドメイン間のシングルサインオン (CDSSO) コンポーネントは、主に、このコンポーネントが配備されたドメインの cookie の設定に使用されます。CDSSO コンポーネントは、関連 DNS ドメインとは別にインストールされます。

Web Server

Sun ONE Web Server は、製品 CD にスタンドアロン製品として含まれてはいませんが、Identity Server ソリューションの重要部分です。Sun ONE Web Server は、ポリシーサービスと管理サービスのインストール時に自動的にインストールされ設定されます。バックグラウンドで動作するこの専用 Web Server インスタンスは、ポリシーの適用、アイデンティティの管理、およびサービス管理のためのエンジンを提供します。また、グラフィカルユーザインタフェースも提供します。

共通ドメインサービス

共通ドメインサービスにより、共通ドメインをホスティングするマシンは、リダイレクト URL に渡されたパラメータに基づいて Cookie の読み取りと書き込みを行うことができます。IDP (Identity Service Provider) でユーザが認証されると、IDP はユーザがその IDP を使っていることを示すパラメータを使用して、共通ドメインにユーザのブラウザをリダイレクトします。共通ドメインのサーバは、この IDP を使用している IDP として識別する Cookie を書き込み、ユーザのブラウザを IDP にリダイレクトして戻します。

主な機能と利点

ビジネスが成長するにつれて、ネットワークのニーズも変わります。サービスの効率性、拡張性、迅速な導入、およびセキュリティの確保が、企業活動を円滑に継続し、システムの停止時間を最小限にとどめるための重要な要素になります。Identity Server では、拡大する企業の必要に応えるため、次の機能を提供します。

管理コンソール

アイデンティティ、サービス、およびポリシーの管理を統合するグラフィカルインタフェース。管理コンソールは、ユーザ (管理者および非管理者のいずれの場合も) が、LDAP に関する知識がなくても、1 つのインタフェースを使って Directory Server でユーザアカウント、サービス属性、およびアクセスルールを作成および管理できるようにします。

ポリシー管理

アクセスルールを作成および適用する手段。ユーザの資格、およびアクセスルールとポリシーに基づいて、ユーザにリソースへのアクセスを許可または拒否します。

サービス管理

サービスおよびサービス属性を登録する手段。ユーザを管理するために使うのと同じコンソールから、組織、グループ、または個々のユーザにサービス属性を割り当てることができます。

アイデンティティの管理

事前定義されたいくつかの管理者ロールをサポートするフレームワーク。組織、グループ、およびユーザを作成、変更、または削除するための手段を提供します。新しい組織または管理グループを作成するたびに、適切な管理者エントリ、ロール、およびアクセス制御命令 (ACI) を自動的に作成します。

認証

ユーザのアイデンティティを検証するための 1 つのフレームワークといくつかのモジュール。企業内のアプリケーションにログインするために資格情報を提示するようユーザに要求することにより、セキュリティを確保します。プラグインアーキテクチャにより、Sun ONE のユーザは Identity Server で独自のモジュールを作成して使用することができます。Identity Server には、次の認証モジュールが付属しています。

- LDAP
- RADIUS
- メンバーシップ

- 匿名
- 証明書に基づく認証モジュール
- Unix
- SafeWord

注	UNIX 認証モジュールは、Solaris バージョンにのみ付属しています。

Web ベースのシングルサインオン

アプリケーション間でユーザ情報を保存および転送するためにトークンを使うメカニズム。1 つのセッションの間、アプリケーションごとに認証をやり直さなくても、ユーザが複数の Web ベースアプリケーションにアクセスできるようにします。

ポリシーエージェント

Web リソースを保護するアクセスルールとポリシーを適用するメカニズム。Web サーバにある保護されたファイルやページへのアクセスを試みるユーザにさらにアイデンティティを要求することにより、セキュリティを確保します。

SSL (Secure Socket Layer)

暗号化によりネットワークを介した通信を保護する転送プロトコル。SSL により、権限がない場合にはネットワークを介した通信を傍受できないようにします。

ディレクトリレプリケーションのサポート

Identity Server は、Directory Server のマルチマスターレプリケーション機能と連携して、読み取りと書き込みの両方の操作に対して可用性の高いディレクトリサービスを提供します。

サービスのロールとクラスのサポート

Identity Server は、Directory Server と連携して、エントリ間で属性をグループ化および共有するための柔軟なメカニズムを提供します。ロールまたは属性を 1 回変更するだけで、多数のユーザ、グループ、または組織のエントリをダイナミックに変更できるようにします。

負荷均衡アプリケーションのサポート

Identity Server は、Sun ONE Directory Access Router などの負荷均衡アプリケーションと連携して、高可用性とファイアウォールに似たセキュリティを実現します。

Identity Server 6.0 の新機能

Identity Server 6.0 には、次の新しい機能が組み込まれています。

- Liberty 仕様のサポート
- SAML のサポート

Liberty 仕様のサポート

私たちの個人情報は断片的に、銀行、クレジットカード会社、証券仲買会社、自動車関連部門、保険会社、社会保険庁、百貨店、ガソリンスタンド、電話会社などによって際限なく拡散しています。今日、私たちが仕事や地域社会を通じ、さらには個人的にやりとりを行うための主要なコミュニケーション手段であるインターネットによって、私たちの個人情報はなお一層断片的に広がっています。私たちの情報は、雇用者、ISP、電子掲示板、インスタントメッセージングシステム、オンラインビジネスなどによって使用される多くのコンピュータシステムやネットワーク全体に断片的に提供されています。これらすべてのシステムやネットワークは、私たちの側で調整、操作、あるいは管理することはほとんどできません。

個人情報の総合的な管理インフラストラクチャの構築は、このような状況を改善する鍵となっています。このようなインフラストラクチャの構築によって、ビジネスコストの低下およびインターネットや電子商取引の拡大の促進など、経済的利益の提供をもたらす新しいビジネスチャンスが生まれます。消費者にとっては、個人情報に関する新しいレベルのパーソナライズ、セキュリティ、および管理が約束されます。Liberty Alliance Project は、このようなすべてのインフラストラクチャを構築します。

SAML のサポート

SAML (Security Assertion Markup Language) 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 XML 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ベンダープラットフォーム間の相互運用性を実現することを主な目的としています。

次に、SAML によって実行される使用シナリオの一部を示します。

- 信頼関係にある提携業者間のシングルサインオンを有効にします。ユーザがソース Web サイトに認証されると、認証をやり直さなくても、異なるベンダーが管理する Web リソースにアクセスできます。
- ユーザの認証基準に基づくアプリケーションのアクセス許可を有効にします。
- 異なるセキュリティドメインにある 2 当事者の相互検証を有効にして、2 当事者間の商取引が続行されるようにします。

- 2 つのアプリケーション間のユーザセッションの共有を有効にします。

SAML の詳細情報と Identity Server での使用方法については、『Programmer's Guide』の第 8 章「Using SAML」を参照してください。

第 2 章

導入に関する検討事項

この章では、Identity Server の導入を計画する際に念頭に置いておく必要のある情報を提供します。

この章には次のトピックがあります。

- ディレクトリに関する問題
- ポリシー管理に関する問題
- アイデンティティ管理サービスを使用するための製品のインストール
- ハードウェア要件
- ソフトウェア要件

ディレクトリに関する問題

Identity Server をインストールして設定する方法は、会社の現在のディレクトリ環境とディレクトリに関する長期的なニーズによって異なります。Identity Server をインストールする前に、最善の性能と拡張性が得られるように、新しいディレクトリの作成を計画するか、既存のディレクトリを最適化する必要があります。以降の節では、Identity Server に付属のディレクトリ情報ツリー (DIT) を最大限に活用する方法について説明します。

Directory Server の一般的な計画と実装については、次の URL から入手可能な『Directory Server 導入ガイド』を参照してください。

`http://docs.sun.com/db/doc/816-5609-10`

既存のディレクトリへのインストール

ユーザデータがすでに存在する既存の Sun ONE Directory Server に対して Identity Server をインストールできます。ただし、Identity Server インストールプログラムの実行直後に、既存のディレクトリと Identity Server の設定の両方を変更して両方が連携するようにする必要があります。変更内容は DIT 構造によって異なりますが、次の処理が必要になることがあります。

- Identity Server オブジェクトクラスを既存のディレクトリエントリに追加する (これは必須です。)
- カスタムオブジェクトクラスを Identity Server XML ファイルに追加する
- 属性のネーミング方式を変更する

これらのトピックについては、第 5 章「既存の Directory Server を使用する Identity Server のインストール」で詳しく説明します。

注 既存の Directory Server に Identity Server をインストールする場合は、複雑なディレクトリ変更が必要です。変更には LDAP の計画と実装に関する高度な専門知識が必要であり、また XML に精通している必要があります。この手続きは複雑であり、時間がかかることがあります。配備に関してはこの問題を考慮して計画を立てるようにしてください。

Identity Server スキーマ

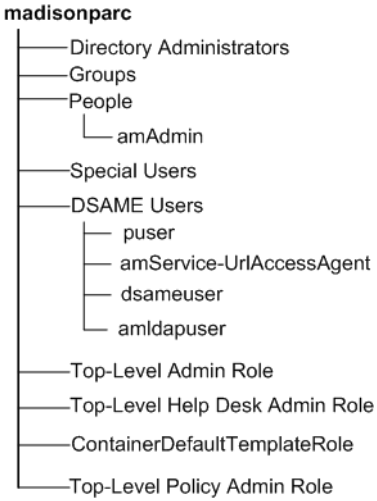
インストールプログラムの実行時に、「既存の Directory Server を設定する」オプションを選択して、Identity Server スキーマをインストールすることができます。Identity Server スキーマは、Directory Server がインストールされているサーバにインストールされます。スキーマファイル `ds_remote_schema.ldif` は、Directory Server のスキーマディレクトリにロードされます。

ディレクトリにユーザがすでに存在するかどうかにかかわらず、次の Identity Server オブジェクトが作成され、ディレクトリに保存されます。

- 特別なオブジェクトクラス
- 1 つの組織
- 管理者のロール
- Identity Server サービス属性と関連するポリシー
- 最上位管理者

インストール時に作成される Identity Server のベース接尾辞は、ユーザデータの保存と管理のために設計されています。特別なオブジェクトクラスは、Identity Server が管理するディレクトリ内のユーザおよびグループのエントリを識別します。このオブジェクトクラスにより、Identity Server は選択したデータ、つまりユーザデータだけを管理し、サーバやハードウェアなど、ツリーのほかの部分には干渉しないようにできます。

図 2-1　デフォルト DIT



サポートされていない DIT

データが存在するほとんどの DIT は Identity Server とともに使えるように設定し直すことができますが、設定し直さないほうがよい場合もあります。一般に、既存の DIT が複数の種類のディレクトリエントリ (たとえば、dc、o、ou) を使って組織を定義している場合は、ユーザデータは特定の条件下でだけ Identity Server に認識されます。詳細は、『Programmer's Guide』を参照してください。

ディレクトリのレプリケーション

レプリケートされたディレクトリを Identity Server とともに使う予定の場合は、Identity Server インストールプログラムを実行する前に、データベースレプリケーションアグリーメントを定義する必要があります。詳細は、このマニュアルの 175 ページの「ディレクトリレプリケーションと高可用性のサポート」を参照してください。

ポリシー管理に関する問題

Identity Server の委託管理と Web アクセス管理は、特殊なロールとポリシーを使って実装されます。ロールおよびポリシーはインストール時に作成され、Identity Server のグラフィカルユーザインタフェースで表示および管理できます。ディレクトリ構造を計画するときは、自社のニーズを満たすために、これらの事前定義された Identity Server オブジェクトを最大限に活用する方法を検討してください。

ロール

Identity Server のロールは、Directory Server のロール機能の拡張です。Directory Server では、ロールはエントリのグループ化メカニズムです。このグループ化メカニズムは、スタティックグループよりも柔軟性を高め、ダイナミックグループのように維持を容易にするために設計されています。

Identity Server では、ロールの概念は Directory Server の場合と同じですが、抽象化のレベルが高くなっています。Identity Server をインストールすると、いくつかの管理者ロールが自動的に作成されます。各管理者ロールは、範囲の異なるアクセス制御を指定し、ユーザアカウント管理の委託の手段を提供します。ロールは、ACI (アクセス制御命令)、ポリシールール、またはサービス属性の任意の組み合わせを含むように設定できます。ロールは管理コンソールの「ロール」ページで設定します。特定のアクセス権を持ったロールを作成して、顧客委譲モデルを提供することもできます。

次の表は、Identity Server の管理者ロールとそれぞれのロールに対応する書き込み権限の範囲を要約したものです。

表 2-1 管理者ロールと権限

管理者ロール	ツリーのこのレベルのディレクトリエントリを変更する権限がある					
	ベース接尾辞	ロールの定義	組織	グループ	ユーザ	個人のエントリ
最上位管理者	X	X	X	X	X	X
最上位レベルのヘルプデスク *			X*			
組織			X	X	X	X
組織のヘルプデスク *			X*			
コンテナ				X	X	X
コンテナのヘルプデスク *			X*			
グループ				X	X	X

表 2-1 管理者ロールと権限 (続き)

管理者ロール	ツリーのこのレベルのディレクトリエントリを変更する権限がある					
	ベース接尾辞	ロールの定義	組織	グループ	ユーザ	個人のエントリ
ピープルコンテナ					X	X
ユーザ (自己管理)						X
* ヘルプデスク管理者は、ツリーの自分の分岐内にあるユーザのパスワードだけを変更できます。						

ディレクトリエントリを作成すると、適切な管理者ロールと ACI が作成され、ディレクトリエントリに割り当てられます。その後、個々のユーザにロールを割り当てることができます。

たとえば、Identity Server を使って新しい組織を作成すると、自動的に次の 2 つのロールが作成されてディレクトリに保存されます。

- 組織の管理者ロール
- 組織のヘルプデスク管理者

組織内で組織の管理者ロールをユーザ `mikeb` に割り当てると、`mikeb` は組織管理者に付与されたすべての権限を継承します。ヘルプデスクの管理者ロールをユーザ `ginac` に割り当てると、`ginac` は限定されたヘルプデスク管理者の権限を継承します。最終的には、グループに基づく ACI の代わりにロールを使うほうが、効率が良く維持の手間も少なくてすみます。

ポリシーとポリシーエージェント

ロールおよび組織にポリシーを適用して、自社の Web リソースへのアクセスを制御できます。ポリシーはルールで設定されます。ルールは、サーバに格納されているサービスやコンテンツページなど、指定したリソースへのユーザアクセスを許可または拒否します。自社の Web Server にインストールするポリシーエージェントは、定義したポリシーを評価および適用します。

ユーザが会社のサーバに格納されている Web ページなどの保護されたリソースへのアクセスを試みると、Identity Server ポリシーサービスは、ユーザの組織、ロール、またはユーザ ID に適用されているルールを評価します。ユーザに割り当てられたルールとポリシーを組み合わせた結果に基づいて、個々のユーザは Web ページへのアクセスを許可または拒否されます。ルールおよびポリシーは、Identity Server 管理コンソールで設定できます。ポリシーの設定に関する詳細は、『Sun ONE Identity Server

Administration Guide』を参照してください。Identity Server ポリシーエージェントとポリシーエージェントのインストールおよび設定方法に関する総合的な情報については、http://docs.sun.com/db/prod/s1.ipdirsame にある『Sun ONE ポリシーエージェントガイド』を参照してください。

サービス属性

サービス属性を使って、サービスを Identity Server と連携させる方法を定義できます。サービス属性には、グローバルレベルで設定されて DIT 全体に影響するもの、個々のユーザにだけ影響するもの、複数のレベルで設定可能なものなどがあります。属性の値を指定するには、属性の効果の範囲を理解することが重要です。この理解を容易にするために、サービス属性は、グローバル、ダイナミック、ポリシー、およびユーザの各カテゴリに分かれています。

グローバル：グローバル属性は、DIT 全体に適用されます。グローバル属性の値は、サービス管理表示で設定できます。

ダイナミック：ダイナミック属性は、組織またはロールの、グローバルレベルのサービス管理、またはユーザ管理表示で設定できます。ポリシー属性の値は、親オブジェクトから継承することもできます。

ポリシー：ポリシー属性は、ポリシー管理表示で設定できます。定義されたポリシーは、1 つ以上のロールや組織に適用できます。ポリシー属性の値は、親オブジェクトから継承することもできます。

ユーザ：ユーザ属性は、個々のユーザエントリに適用されます。ユーザ属性の値は、組織管理表示で設定できます。

管理コンソールを使って、サービスのポリシーを設定できます。詳細は、http://docs.sun.com/db/prod/s1.ipdirsame にある『Sun ONE Identity Server Administration Guide』を参照してください。

アイデンティティ管理サービスを使用するための製品のインストール

Identity Server は、リモート Web Server、Sun ONE Directory Access Router などの LDAP 負荷均衡アプリケーションとともに、またはマルチマスターレプリケーションで配備できます。Identity Server インストールプログラムを実行する前に、それらの製品が配備条件にどのように適合するかを検討してください。多くの場合、Identity Server をインストールする前に、それらの製品をインストールして設定しておく必要があります。

リモート Web Server

このマニュアルでは、Identity Server のポリシーサービスおよび管理サービスを実行する Web Server からみて離れたところにある Web Server を「リモート」と呼んでいます。会社のコンテンツページを提供するために、すでにリモート Web Server が導入されている場合があります。追加の Web Server をインストールできます。リモートサーバにポリシーエージェントをインストールした場合だけ、そのリモートサーバは Identity Server と統合されます。詳細は、29 ページの「ポリシーエージェント」を参照してください。

Web Server のインストールと管理の詳細については、サーバに付属のマニュアルを参照するか、あるいはインターネット上の `http://docs.sun.com/db/prod/s1websrv` にあるマニュアルにアクセスしてください。

ポリシーエージェント

Identity Server ポリシーエージェントは、企業に導入されているさまざまな Web サーバにインストールできます。このエージェントは、サーバに格納されている特定のページに設定されたアクセスルールとポリシーを適用します。このエージェントは、設定された Web Server が受け取る要求を傍受し、ポリシーサービスと通信します。ポリシーサービスはユーザの資格を認証し、ユーザのロールとポリシーを調べます。ユーザの資格と割り当てられているポリシーが正当な場合、エージェントはユーザに HTTP を介して URL にアクセスすることを許可します。

Identity Server ポリシーエージェントは個別に入手する製品であり、次の URL でダウンロードできます。

`http://wwws.sun.com/software/download/developer/5256.html`

ポリシーエージェントをインストールするには、製品に付属の説明書を参照してください。

複数の Directory Server によるフェイルオーバと高可用性

アップグレード、フェイルオーバディレクトリのセットアップ、またはマルチマスターレプリケーションのセットアップのために、Identity Server インストールプログラムを使って Directory Server をインストールできます。Identity Server を使用するには、Directory Server を適切にインストールして、設定し、導入する必要があります。詳細は、175 ページの「ディレクトリレプリケーションと高可用性のサポート」を参照してください。

Directory Server の導入とインストールの詳細については、サーバに付属のマニュアルを参照するか、あるいはインターネット上の `http://docs.sun.com/prod/s1dirsrv` にあるマニュアルにアクセスしてください。

LDAP 負荷均衡アプリケーション

Sun ONE Directory Access Router などの負荷均衡アプリケーションと連携するように Identity Server を設定できます。このように設定すると、ディレクトリの高可用性を正確に管理したい場合に役に立つことがあります。詳細は、175 ページの「ディレクトリレプリケーションと高可用性のサポート」を参照してください。

Sun ONE Directory Access Router のインストールと管理の詳細については、インターネット上の `http://docs.sun.com/db/prod/s1.ipdirar` にあるマニュアルにアクセスしてください。

その他の負荷均衡アプリケーションについては、製品に付属のマニュアルを参照してください。

ハードウェア要件

Identity Server をインストールする予定のシステムが、最小ハードウェア要件を満たしていることを確認する必要があります。理論上は、すべての Identity Server コンポーネントを 1 台のサーバマシンにインストールできますが、そうすることはあまりないでしょう。Identity Server の導入を設計する前に、各コンポーネントのマニュアルでインストールと導入に関する情報を確認してください。Sun ONE Identity Server のインストールを設計および導入する前に、Sun ONE プロフェッショナルサービスまたは Sun ONE 認定システムインテグレータに相談することをお勧めします。

最適なハードウェア要件

最善の性能とスケーラビリティを得るためのハードウェア要件を次に示します。

- Directory Server 用に、512M バイト～ 2G バイトの RAM を搭載したコンピュータシステム
- Sun ONE Identity Server 用に、512M バイト～ 1G バイトの RAM を備えたコンピュータシステム
- 保護する必要のある既存の Web サーバがある場合は、ポリシー適用ポイントエージェントまたはポリシーエージェントを各 Web サーバにインストールする必要がある。このためには 10M バイトの空きディスク容量が必要

一般に、ディレクトリリソース要件は高くなります。実際の要件は、顧客固有の条件、データ、用途によって決定されるため、上記とは異なります。

推奨ハードウェア構成

一般的なインストールのハードウェア構成を次に示します。

- Directory Server 用に、512M バイト～ 1G バイトのメモリと、Directory Server 内の最小限のデータ用に約 300M バイトの空きディスク容量を持つコンピュータシステム
- Identity Server (および Sun ONE Web Server)、および場合によっては Sun ONE Application Server およびポリシーエージェント用に、512M バイト～ 1G バイトのメモリと、25M バイト～ 100M バイトの空きディスク容量を持つコンピュータシステム。後で、ログファイルやデバッグファイル用に追加の空きディスク容量 (G バイト単位) が必要な場合がある
- 大規模なインストールの場合は、製品バイナリ、データベース、およびログファイル (ログファイルにはデフォルトで 1G バイトが必要) をサポートするために最小 2G バイトの空きディスク容量を確保する必要があり、非常に大きなディレクトリの場合は 4G バイト以上が必要になる場合もある

- 保護する必要のある既存の Web サーバがある場合は、各 Web サーバにポリシーエージェントをインストールする必要がある。このエージェントには、10M バイトの空きディスク容量が必要
- 表 2-2 に、Directory Server が管理するエントリ数に応じたディスク容量とメモリの要件に関するガイドラインの一部を示す

表 2-2　Directory Server のディスク容量に関するガイドライン

エントリの数	必要なディスク容量とメモリ
10,000 ～ 250,000 のエントリ	空きディスク容量 : 2G バイト、空きメモリ : 256M バイト
250,000 ～ 1,000,000 のエントリ	空きディスク容量 : 4G バイト、空きメモリ : 512M バイト
1,000,000 を超えるエントリ	空きディスク容量 : 8G バイト、空きメモリ : 1G バイト

ソフトウェア要件

システムが、次のソフトウェアおよびオペレーティングシステムの要件を満たしていることを確認してください。

オペレーティングシステム要件

Identity Server は次のプラットフォームでサポートされています。

- Solaris 8 (32 ビットおよび 64 ビット)
- Solaris 9 (32 ビットおよび 64 ビット)
- Microsoft Windows 2000 Server SP 2
- Microsoft Windows 2000 Advanced Server

Solaris 用パッチクラスタ

Sun ONE Directory Server を Solaris 8 オペレーティングシステム上で実行する場合は、推奨パッチクラスタがインストールされていることを確認する必要があります。Solaris のパッチは、たとえば 108827-15 のように、2 つの番号で識別されます。最初の番号 (108827) は、パッチ自体を示します。2 番目の番号は、パッチのバージョン (15) を示します。最新の修正内容が適用されるように、最新バージョンのパッチをインストールすることをお勧めします。

showrev -p コマンドを使って、現在マシンにインストールされているパッチを一覧表示できます。すべてのパッチは、http://sunsolve.sun.com からダウンロードできます。この Web サイトで、「Patches」>「Recommended & Security Patches」に移動すると、「Recommended & Security Patch Clusters for Solaris」のリストを参照することができます。

前述したリストにないパッチの場合は、http://sunsolve.sun.com で「Patches」>「Patchfinder」に移動してください。

Sun ONE Certificate Server 4.7 用パッチのインストール

Identity Server セキュリティサービスを設定するには、Sun ONE Certificate Server バージョン 4.7 のパッチをインストールする必要があります。このパッチをインストールする前に、システムに Certificate Server をインストールする必要があります。

Certificate Server のインストール手順については、次の Web サイトにある『Sun ONE Certificate Server Installation and Setup Guide』を参照してください。

http://docs.sun.com/prod/s1certsrv

Certificate Server 4.7 パッチのインストール

1. CMS47sp1.jar ファイルを次の場所にコピーします。

   Windows 2000 の場合 :

   CMS_Root¥bin¥cert

   Solaris 8 の場合 :

   CMS_Root/bin/cert

2. 次のコマンドを実行して jar ファイルの内容を展開します。

   ```
   jar xvf CMS47sp1.jar
   ```

3. SSOBasedAuthentication インスタンスを作成するか、すでにある場合は再設定します。

4. Certificate Server を再起動します。

パッチをインストールしたら、Identity Server コンソールで Identity Server セキュリティサービスを設定します。

Java の要件

Identity Server インストールプログラムには Java バージョン 1.3.1_06 が必要です。

リモート Web Server の要件

Identity Server の Web エージェントは、約 10M バイトのディスク容量を使用します。Identity Server Web エージェントの Web Server の要件に関する詳細は、次の URL にある『Sun ONE ポリシーエージェントガイド』を参照してください。

`http://docs.sun.com/prod/s1.ipdirsame`

Web ブラウザの要件

管理者とエンドユーザは、Web ブラウザを使ってユーザ管理タスクを実行します。Identity Server は、次の Web ブラウザをサポートしています。

- Solaris 8、Windows NT 4.0 SP6a および 98SE 上の Netscape Communicator 4.79
- Windows 2000 Professional、NT 4.0 SP 6a および 98 SE 上の Microsoft Internet Explorer 5.5 SP2
- Windows 2000 Professional、XP Professional、XP Home、NT 4.0 Sp6a 上の Microsoft Internet Explorer 6.0

第 3 章

Identity Server インストールプログラム

この章では、インストールプログラムで提示されるオプションの概要、および実行する必要のあるインストール作業を決定する際のいくつかの指針を説明します。この章および以降の章で提供される手順は、Solaris および Windows プラットフォーム上での Sun ONE Identity Server のインストールを前提としています。

この章には次のトピックがあります。

- 始める前に
- インストール方法
- インストールプログラムのオプション
- ドメイン名の設定
- Windows 上のインストール手順

始める前に

インストールプログラムを開始する前に次の事項を確認してください。

- インスロールプログラムを実行するには、Solaris の場合は root で、Windows 2000 の場合は管理者としてログインする必要があります。
- ホストマシンのドメイン名の設定が必要です。ドメイン名が設定されていない場合は、38 ページの「ドメイン名の設定」の手順に従ってください。
- Identity Server またはそのコンポーネントをインストールできるのはローカルマシンだけです。ネットワーク上のリモートマシンにインストールすることはできません。

インストール方法

Identity Server の使用およびインストールの必要性に応じて、最適なインストール方法を選択します。これらの方法を使用する手順は、以降の章で説明します。

インストール方法は次のとおりです。

- `setup` プログラムを GUI モードで使用します。この方法は、最も簡単な推奨インストール方法です。
- `setup` プログラムを `no display` モードで使用します。
- サイレントインストール

インストールプログラムのオプション

インストールプログラムを実行すると、多数のオプションが表示されます。まず自分のインストールシナリオを表 3-1 で確認し、次にそのシナリオに対応する詳細なインストール手順に従って、どのインストールオプションを選択するかを決定します。

表 3-1 特定のシナリオに対応する Identity Server のインストール手順の参照先

一般的なインストールシナリオ	詳しいインストール手順の参照先
1. 本稼働のために初めて Identity Server と Directory Server をインストールおよび導入する。処理する既存のユーザデータはない	第 4 章「新しい Directory Server を使用するインストール」
2. 既存の Directory Server 5.1 で動作する Identity Server をインストールする	第 5 章「既存の Directory Server を使用する Identity Server のインストール」
3. エージェントのフェイルオーバのために、1 つの Directory Server に対して複数の Identity Server インスタンスをイントールする。Identity Server とマスター Directory Server がすでにインストールされている。ディレクトリにはユーザがすでに存在する場合も存在しない場合もある	173 ページの「同じ Directory Server に対する複数の Identity Server インスタンスのインストール」
4. Identity Server で使用する既存の Directory Server 5.1 を設定する	69 ページの「既存の Directory Server を使用する Identity Server のインストール」
5. ドメイン間シングルサインオン (CDSSO) コンポーネントをインストールおよび設定する	161 ページの「ドメイン間のシングルサインオンコンポーネント」
6. 共通ドメインサービスをインストールする	151 ページの「共通ドメインサービスのインストール」
7. Identity Server をアンインストールする	197 ページの「Solaris 上の Identity Server のアンインストール」

次に、主な各インストールオプションを選択するとどのようになるかを簡単に示します。

オプション 1) Sun ONE Identity Server 管理およびポリシーサービス

このオプションを選択すると、次のコンポーネントがインストールされます。

- Identity Server 管理およびポリシーサービス
- Sun ONE Web Server
- Sun ONE Directory Server (オプション)
- Sun ONE Identity Server コンソール (オプション)
- 共通ドメインサービス
- JDK 1.3.1_06 (オプション)

上に示したオプションのコンポーネントは、インストールの際の確認項目に対する応答に従ってインストールされます。インストールプログラムが完了すると、製品全体がインストールされ、すぐに Identity Server にログインできます。ユーザデータはディレクトリに存在しません。

オプション 2) Sun ONE Identity Server 管理コンソール

アイデンティティ、サービスおよびポリシー管理、Identity Server コンソールを統合するグラフィカルユーザインタフェース (GUI) により、ユーザ (管理者または非管理者を問わず) は LDAP に関する知識がなくても、1 つのユーザインタフェースを使用して、Directory Server のユーザアカウント、サービス属性、およびアクセスルールを作成し管理することができます。

オプション 3) 既存の Directory Server を設定する

このオプションを選択すると、既存の Directory Server のホストおよびポート番号の入力を要求されます。Directory Server のインストール先に Identity Server スキーマだけがインストールされます。スキーマファイル `ds_remote_schema.ldif` は、Directory Server のスキーマディレクトリにロードされます。新しい Directory Server はインストールされないので、既存のデータは上書きされません。ユーザデータがすでに存在している既存の Directory Server 5.1 インスタンスとともに Identity Server を使う場合だけ、このオプションを選択します。

オプション 4) Sun ONE Identity Server ドメイン間シングルサインオン

ドメイン間のシングルサインオン機能により、あるドメインで 1 回認証されたら、再認証なしでその他のドメインでアプリケーションを使用できます。このオプションを選択した場合、ドメイン間シングルサインオン (CDSSO) コンポーネントだけがインストールされます。このコンポーネントは、既存の Identity Server の一部として Web Server にインストールできます。また、Web Server のインストール時に自動的にインストールすることもできます。詳細は、17 ページの「Identity Server コンソール」を参照してください。

オプション 5) 連合用共通ドメインサービス

共通ドメインサービスにより、共通ドメインをホスティングするマシンは、リダイレクト URL に渡されたパラメータに基づいて Cookie の読み取りと書き込みを行うことができます。IDP でユーザが認証されると、IDP はユーザがその IDP を使っていることを示すパラメータを使用して、共通ドメインにユーザのブラウザをリダイレクトします。共通ドメインのサーバは、この IDP を使用している IDP として識別する Cookie を書き込み、ユーザのブラウザを IDP にリダイレクトして戻します。

ドメイン名の設定

Identity Server をインストールする前に、Identity Server をインストールするマシンのドメイン名が設定されていることを確認します。ドメイン名が設定されていない場合は、次の手順に従って設定します。

Solaris の場合

1. 次のコマンドを実行してホスト名の設定を確認します。

   ```
   uname -n
   ```

   ホスト名、たとえば *nila* がマシンに表示されます。

2. ドメイン名を確認します。`/etc/resolv.conf` ファイルがマシンで定義されている場合は、テキストエディタを使ってこのファイルを開き、設定エントリのドメインに対するドメイン名を入力します。たとえば、ドメインは *eng.siroe.com* になります。

3. このファイルが定義されていない場合は、プロンプトから、コマンド `domainname` を入力して、ドメイン名が設定されているかどうかを確認します。設定されている場合は、ドメイン名が表示されます。たとえば、*eng.siroe.com* が表示されます。

4. ドメイン名が設定されていない場合は、次のコマンドを実行してドメイン名を設定します。

   `domainname` *nila.eng.siroe*`.com`

   この場合、*nila.eng.siroe.com* はマシンのドメイン名です。

5. コマンド `ping` *nila.eng.siroe.com* を実行して、ホストが有効であるかどうか確認します。ホストが有効でない場合は、このコマンドが期待通りに動作するまで DNS またはホストエントリを変更します。

Windows 2000 の場合

1. デスクトップに移動します。
2. 「マイコンピュータ」を右クリックし、「プロパティ」をクリックします。または、「コントロールパネル」に移動して、「システム」をクリックします。このいずれかの操作によって、「システムのプロパティ」ウィンドウが開きます。
3. 「システムのプロパティ」ウィンドウで、「ネットワーク ID」タブをクリックします。
4. 「プロパティ」ボタンをクリックして、「識別の変更」ウィンドウを開きます。
5. マシンの名前が設定されていない場合は、「コンピュータ名」フィールドに入力します。
6. 「詳細」をクリックします。このコンピュータフィールドの「プライマリ DNS サフィックス」で、コンピュータが属するドメイン名を入力します。コンピュータ名とプライマリ DNS サフィックスを組み合わせて、このコンピュータの FQDN が設定されます。

Windows 上のインストール手順

Identity Server のインストール手順は、Solaris の場合と Windows の場合で同じです。したがって、Windows 上でインストールする場合、Solaris 用マニュアルで提供される手順を使用することができます。プラットフォーム固有のパスの入力に関連する相違だけを念頭に置いてください。次の節では、Solaris の場合と異なるインストールプログラムを起動するまでの手順を具体的に説明します。

GUI インストール

1. 製品 CD から Sun ONE Identity Server をインストールする場合は、ソフトウェアをインストールするシステムのドライブに製品 CD を挿入します。製品をダウンロードした場合は、製品バイナリファイルを解凍します。
2. `setup.exe` を実行します。インストールプログラムは、CD-ROM のルートディレクトリにあります。製品バイナリをダウンロードした場合、プログラムはバイナリファイルを解凍したディレクトリにあります。

   `setup.exe` をダブルクリックします。

   インストールプログラムが起動し、開始パネルが開きます。

コマンド行からのインストール

1. 製品 CD から Identity Server をインストールする場合は、ソフトウェアをインストールするシステムのドライブに製品 CD を挿入します。

   製品をダウンロードした場合は、製品バイナリを解凍します。
2. バイナリを解凍したディレクトリに移動して、プロンプトから次のコマンドを入力し Enter を押します。

   ```
   java am -nodisplay
   ```
3. 画面に表示される手順を確認します。インストーラが示すさまざまなプロンプトに対する応答方法の説明が表示されます。手順を確認したら、Enter を押してソフトウェアライセンス契約を確認します。インストールのどの段階でも、< を入力して前のプロンプトに戻ることができます。また、! を入力してインストールプログラムを終了することができます。

第 4 章

新しい Directory Server を使用するインストール

この章では、Sun ONE Identity Server の一般的なインストール手順について説明します。これらの手順では、対象となるコンピュータシステムに Sun ONE Directory Server がまだインストールされていないことを前提としています。すでに Sun ONE Directory Server がインストールされている場合は、第 5 章「既存の Directory Server を使用する Identity Server のインストール」の手順に従ってください。

この章には次のトピックがあります。

- GUI を使用した Identity Server のインストール
- コマンド行からの Identity Server のインストール

GUI を使用した Identity Server のインストール

Identity Server インストールプログラムは、Identity Server のインストール用に、グラフィカルユーザインタフェース (GUI)、コマンド行、サイレントインストールの 3 種類のモードを提供します。GUI モードを使用して Identity Server をインストールするには、後述の手順に従います。Solaris のコマンド行からインストールするには、56 ページの「コマンド行からの Identity Server のインストール」の節を参照してください。

始める前に

インストール手順を開始する前に、次の事項を確認してください。

- Identity Server をインストールする場合、そのマシンの root 権限が必要です。このマシンをホストマシンと呼びます。

- ホストマシンのドメイン名の設定が必要です。ドメイン名が設定されていない場合は、38 ページの「ドメイン名の設定」の手順に従ってください。

注 Identity Server またはそのコンポーネントをインストールできるのはローカルマシンだけです。ネットワーク上のリモートマシンにインストールすることはできません。

Identity Server サービスを新しい Directory Server とともにインストールするには

1. 製品 CD から Identity Server をインストールする場合は、ソフトウェアをインストールするシステムのドライブに製品 CD を挿入します。

   製品をダウンロードした場合は、次のコマンドを使って製品バイナリファイルを解凍します。

   `gunzip -dc` *`binaryfile`*`.tar.gz | tar -xvof -`

   この場合、*binaryfile* をダウンロードした製品バイナリの名前に置き換える必要があります。

2. 別の端末ウィンドウを開き、`xhost +` と入力してマシンのアクセス制御を無効にします。

3. アプリケーションウィンドウで、次のコマンドのどちらかを使用して DISPLAY 変数を設定します。

   - csh または tcsh を使用している場合、次のように入力します。

     `setenv DISPLAY` *`host.siroe.COM:0.0`*

   - sh、ksh、または bash を使用している場合、次のように入力します。

     `export DISPLAY=`*`host.siroe.COM:0.0`*

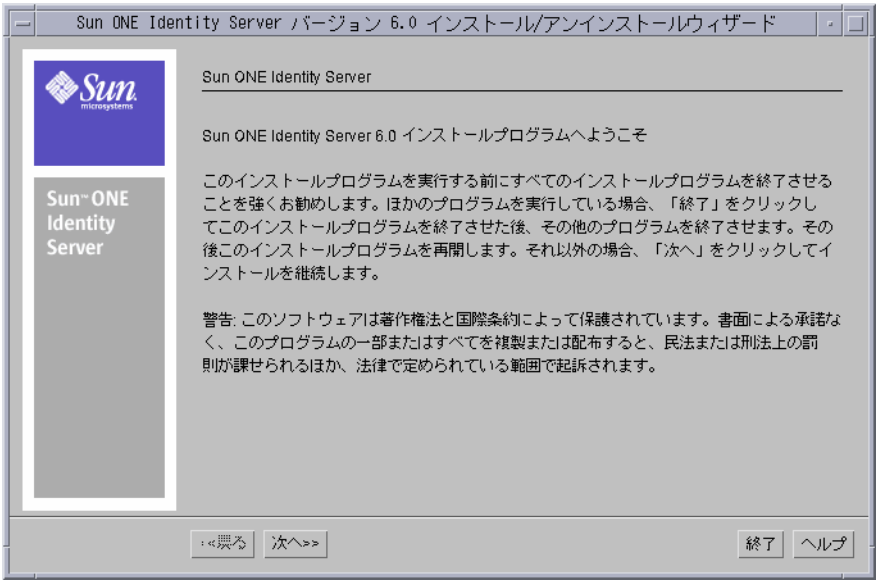
   この場合、`host` はインストールプログラムを実行しているマシンです。

4. 次のコマンドを使用して、`setup` プログラムを起動します。

   `./setup`

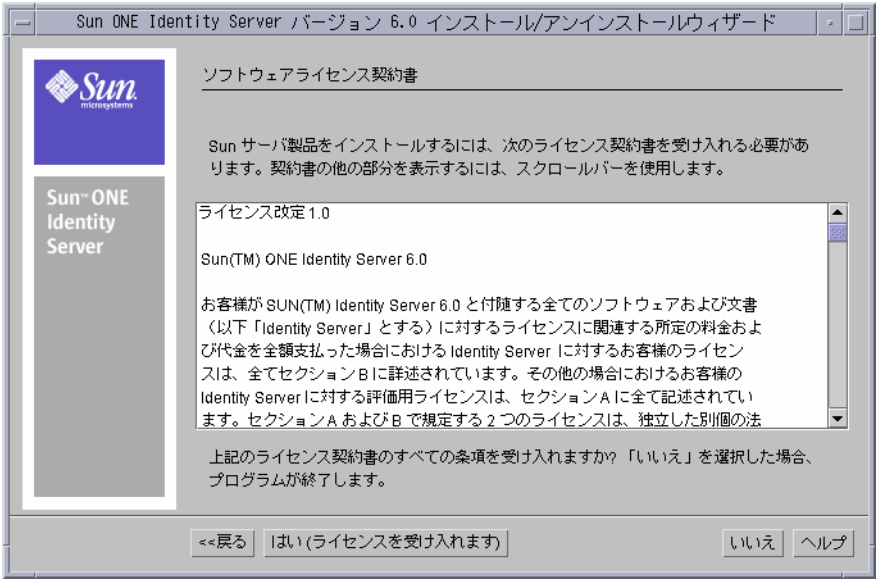
   インストールプログラムが起動し、開始パネルが開きます。

図 4-1　開始パネル



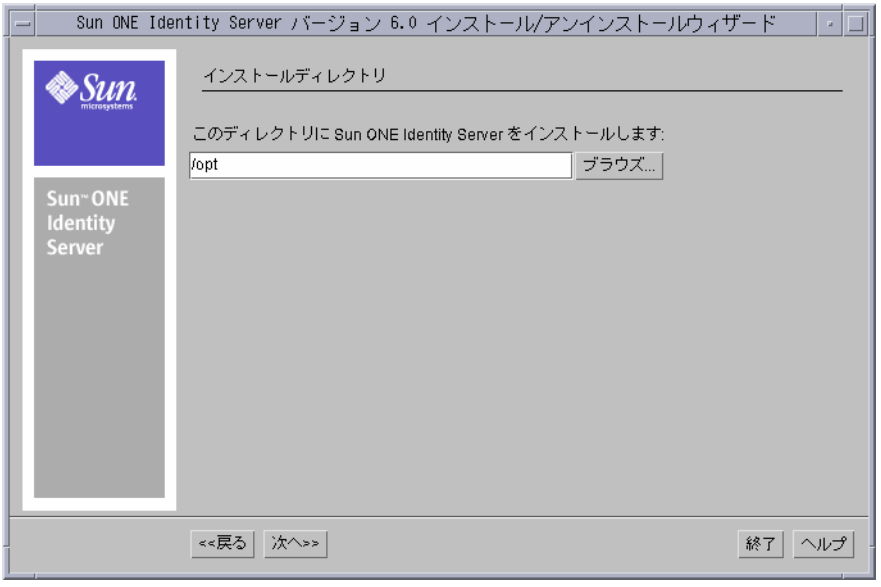
5. 「次へ」をクリックして、ソフトウェアライセンス契約に同意します。

図 4-2　「ソフトウェアライセンス契約書」パネル



6. 「インストールディレクトリ」パネルで、製品をインストールするディレクトリを指定します。このディレクトリに対する書き込み権限と実行権限が必要なことに注意してください。

図 4-3 「インストールディレクトリ」パネル

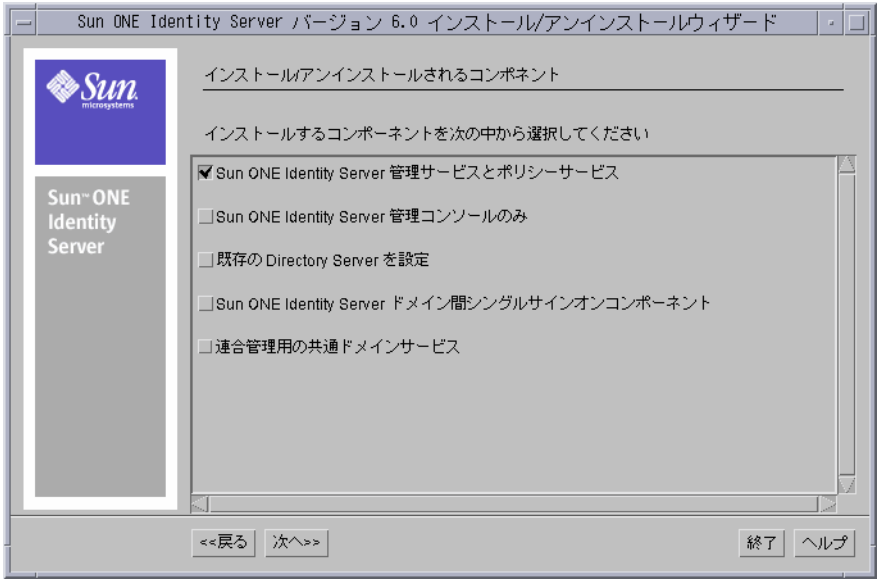


このディレクトリに Sun ONE Identity Server をインストールします : Identity Server サービスをインストールするディレクトリのパスを入力します。デフォルトディレクトリは、Solaris の場合 `/opt`、Windows 2000 の場合 `c:\SunONE\SunONEIS` です。必要に応じて、別のディレクトリを指定できます。

7. 「次へ」をクリックし、「インストール / アンインストールされるコンポーネント」パネルで、「Sun ONE Identity Server 管理サービスとポリシーサービス」を選択します。

   これらのサービスのほかに、インストールプログラムは Sun ONE Web Server、Sun ONE Directory Server、Sun ONE Identity Server コンソール、共通ドメインサービス、Sun ONE Identity Server 管理およびポリシーサービス、および Java SDK 1.3.1_06 もインストールします。

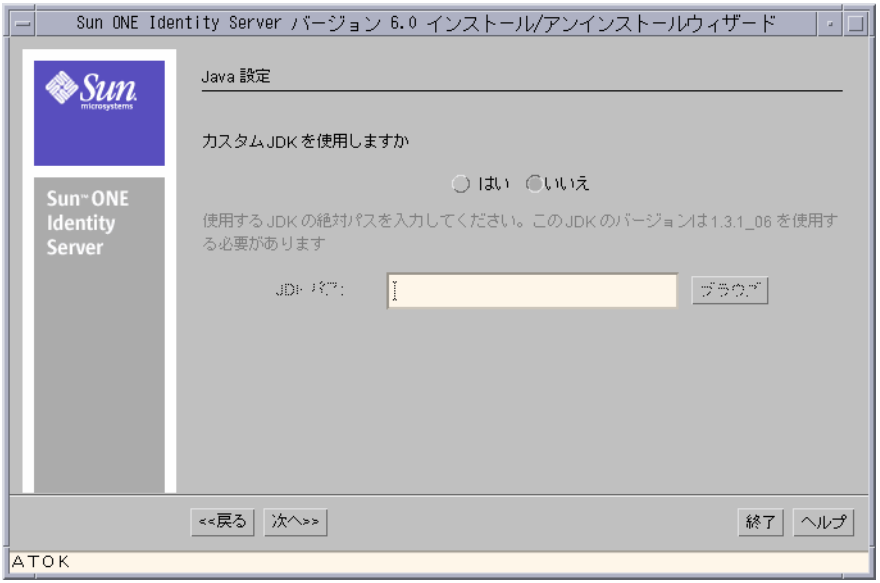
図 4-4　「インストール / アンインストールされるコンポーネント」パネル



これらのサービスのコンポーネントの詳細については、第 1 章「Identity Server ソリューション」の節と「Sun ONE Identity Server の紹介」を参照してください。

8. 「次へ」をクリックし、「Java 設定」パネルで次の情報を入力します。

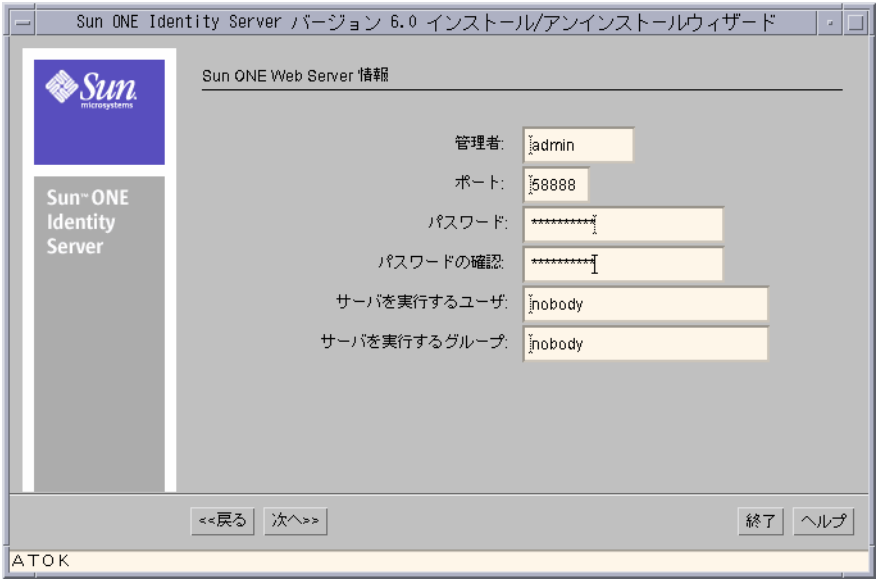
図 4-5　「Java 設定」パネル



カスタム JDK を使用しますか : Web Server で Java をサポートするには、Java SDK バージョン 1.3.1_06 が必要です。この Java SDK は Identity Server 6.0 に付属しています。Identity Server に付属の Java SDK をインストールする場合は、「いいえ」を選択します。ただし、既存の JDK (バージョン 1.3.1_06) を使用する場合は、「はい」を選択し、そのファイルの場所への絶対パスを入力します。

9. 「次へ」をクリックし、「Sun ONE Web Server 情報」パネルで、Identity Server サービスを実行する Web Server に関する次の情報を入力します。

図 4-6　「Sun ONE Web Server 情報」パネル



管理者 : Web Server にアクセスし、Web Server を管理する管理者としてのユーザ名を入力します。

ポート : ポート番号を入力します。通常、デフォルトは 58888 です。

パスワード : 管理者のパスワードを入力します。パスワードの指定には 8 文字以上必要です。

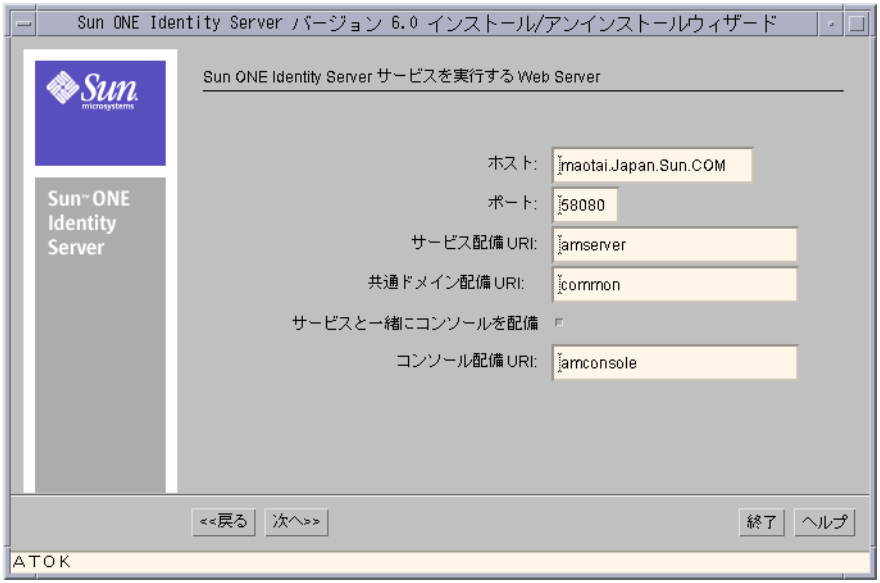
パスワードの確認 : 管理者パスワードを確認するために、もう一度入力します。

サーバを実行するユーザ : Web Server を実行する UNIX ユーザアカウントを入力します。デフォルトは nobody です。

サーバを実行するグループ : 上述のユーザが属する UNIX グループを入力します。デフォルトは、nobody です。

10. 「次へ」をクリックし、「Sun ONE Identity Server サービスを実行する Web Server」パネルで次の情報を入力します。

図 4-7　「Sun ONE Identity Server サービスを実行する Web Server」パネル



ホスト: このフィールドでは、Identity Server コンポーネントと専用 Web Server の両方をインストールするコンピュータの完全指定のドメイン名が表示されます。

ポート: Identity Server サービスを実行する Web Server のポート番号を入力します。デフォルトのポート番号は `58080` です。

サービス配備 URI: Web Server は、URI (Universal Resource Identifier) 接頭辞の指定に従って、サービスに関連付けられた HTML ページや Web アプリケーション固有の情報 (クラス、jar などに関する情報) を検索します。

デフォルトの URI 接頭辞は `amserver` です。別の名前を入力することもできます。

共通ドメイン配備 URI: Web Server の共通ドメインサービスにアクセスする URI。デフォルトの URI は `common` です。必要に応じて変更可能です。

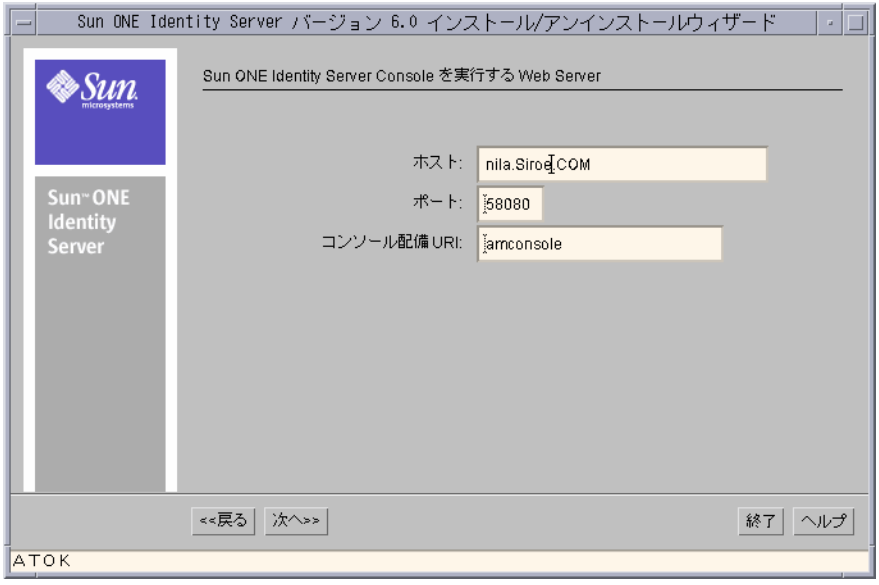
サービスと一緒にコンソールを配備: デフォルトでは、このチェックボックスをオンにすると、Identity Server サービスにより Identity Server コンソールがインストールされます。ただし、既存のコンソールを使用しているため、ここでコンソールを配置する必要がない場合は、チェックボックスをオフにして選択を取消します。この場合、インストールプログラムにより、既存のコンソールに関する追加情報を要求する別のパネルが表示されます。詳細は、次の手順を参照してください。

コンソール配備 URI: Web Server は、URI (Universal Resource Identifier) 接頭辞の指定に従って、Identity Server コンソールに関連付けられた HTML ページや、その他の Web アプリケーション固有の情報 (クラス、jar などに関する情報) を検索します。デフォルトの URI 接頭辞は `amconsole` です。別の名前を入力すること

もできます。「サービスと一緒にコンソールを配備」チェックボックスをオフにした場合、このフィールドは使用できません。

11. 前のパネルで、このサービスでコンソールを配備するように選択しなかった場合は、「Sun ONE Identity Server Console を実行する Web Server」パネルで、既存のコンソールに関する次の情報を入力する必要があります。

図 4-8 「Sun ONE Identity Server Console を実行する Web Server」パネル



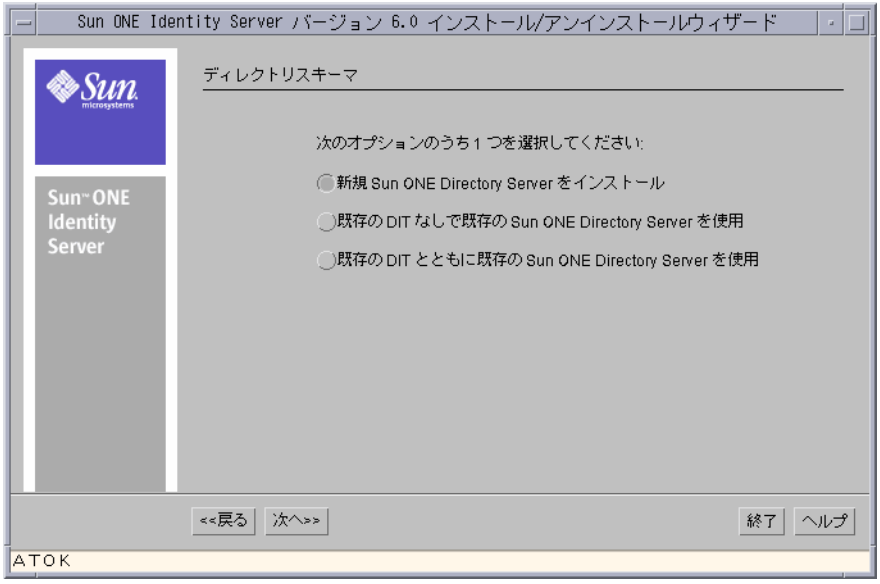
ホスト: Identity Server コンポーネントと専用 Web Server の両方をインストールするコンピュータの完全指定のドメイン名を入力します。コンピュータのドメイン名が設定され、フィールドに正しく入力されていることを確認します。ドメイン名の設定方法に関する手順については、38 ページの「ドメイン名の設定」の節を参照してください。

ポート: Identity Server サービスを実行する Web Server のポート番号を入力します。デフォルトのポート番号は `58080` です。

コンソール配備 URI: Web Server は、URI (Universal Resource Identifier) 接頭辞の指定に従って、Identity Server コンソールに関連付けられた HTML ページや、その他の Web アプリケーション固有の情報 (クラス、jar などに関する情報) を検索します。デフォルトの URI 接頭辞は `amconsole` です。別の名前を入力することもできます。

12. 「次へ」をクリックし、「ディレクトリスキーマ」パネルで、次のオプションを選択します。

図 4-9　「ディレクトリスキーマ」パネル

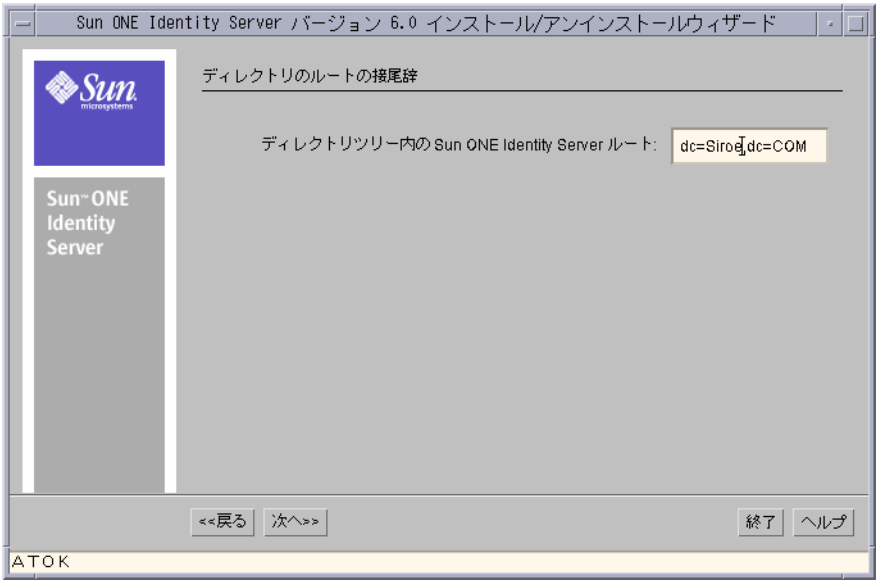


新規 Sun ONE Directory Server をインストール: クリックして、Identity Server に付属の Sun ONE Directory Server 5.1 をインストールします。

13. 「次へ」をクリックし、「ディレクトリのルートの接尾辞」パネルで次の情報を入力します。

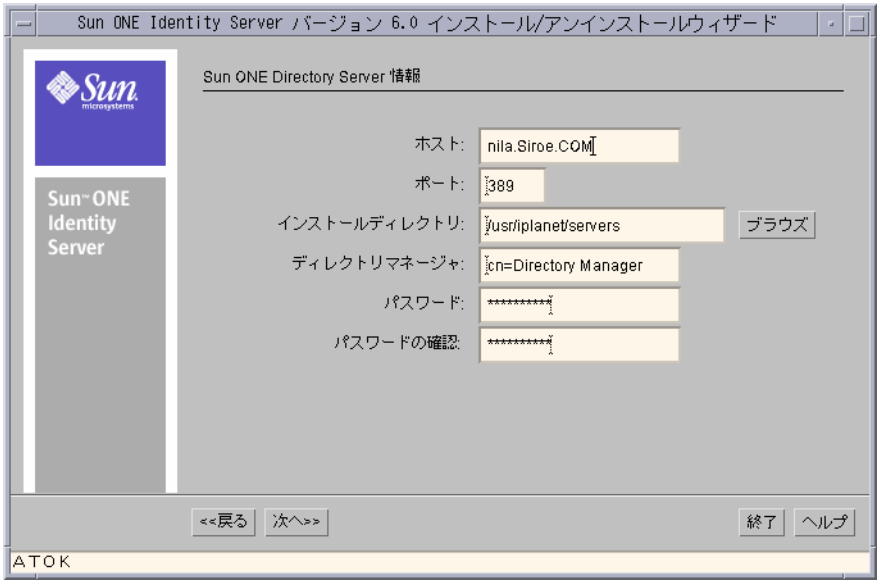
    ディレクトリツリー内の Sun ONE Identity Server ルート: ルート接尾辞として設定する識別名 (DN) を入力します。識別名 (DN) には、最低 1 個の type=value ペアが必要です。たとえば、`o=isp,o=madisonparc,dc=Siroe,dc=COM` のようになります。

図 4-10　「ディレクトリのルートの接尾辞」パネル



14. 「次へ」をクリックし、「Sun ONE Directory Server 情報」パネルで次の情報を入力します。

図 4-11　「Sun ONE Directory Server 情報」パネル



ホスト：Directory Server をインストールするコンピュータの完全指定のドメイン名を入力します。

ポート：Directory Server のポート番号を入力します。デフォルトのポート番号は 389 です。ポートがすでに使用されている場合、インストールプログラムから別のポート番号を入力するよう要求されます。1 ～ 65535 までの未使用の別の番号を入力できます。

インストールディレクトリ：Directory Server をインストールするディレクトリの絶対パスを入力します。デフォルトディレクトリ /usr/iplanet/servers が空であることを確認するか、さもなければ新しいインストールディレクトリを指定することをお勧めします。これは、アンインストールが必要になった場合に、アンインストールプログラムにより、このディレクトリが内容を含めて削除されてしまい、以前にそのディレクトリにあったすべてのデータが消失することがあるためです。

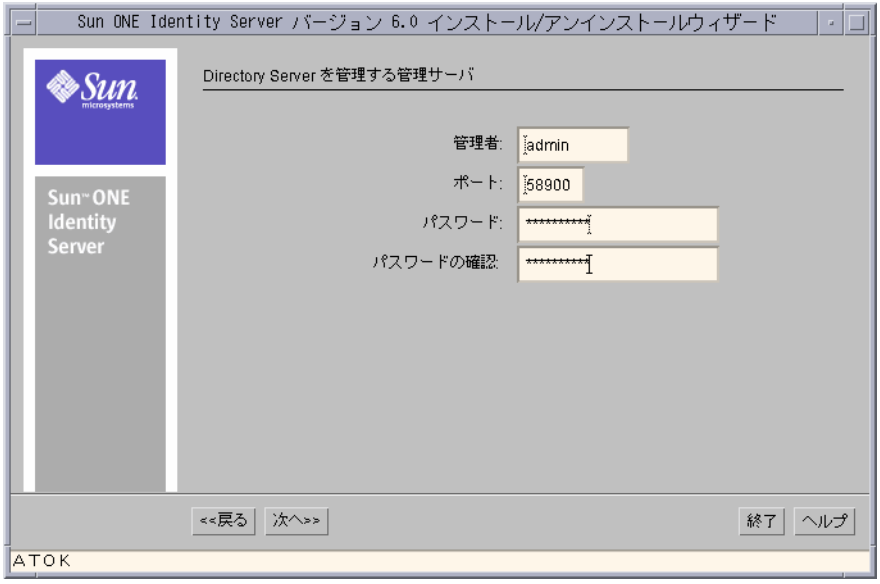
ディレクトリマネージャ：Directory Server へのアクセスを制限されたユーザの DN を入力します。例：cn=Directory Manager など。

パスワード：ディレクトリマネージャのパスワードを入力します。パスワードの指定には 8 文字以上必要です。

パスワードの確認：ディレクトリマネージャのパスワードを確認するために、もう一度入力します。

15. 「次へ」をクリックし、「Directory Server を管理する管理サーバ」パネルで次の情報を入力します。

図 4-12 「Directory Server を管理する管理サーバ」パネル



管理者 : Sun ONE Directory Server を管理する管理サーバにアクセスできる管理者のユーザ名を入力します。デフォルトユーザ名は `admin` です。変更可能です。

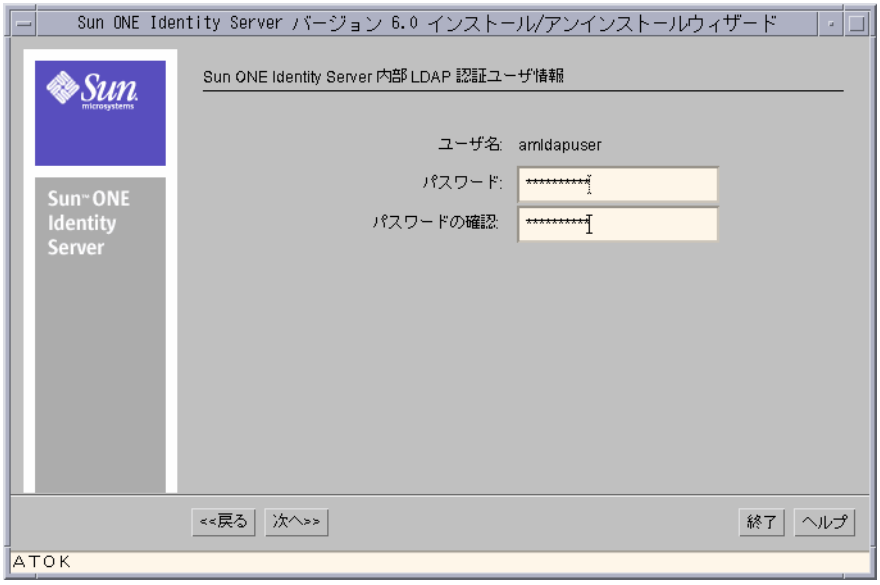
ポート : Directory Server を管理する管理サーバ用のポート番号を入力します。デフォルトでは、このポート番号は `58900` に設定されます。

パスワード : ユーザ `amAdmin` のパスワードを入力します。パスワードの指定には 8 文字以上必要です。

パスワードの確認 : パスワードを確認するために、もう一度入力します。

16. 「次へ」をクリックし、「Sun ONE Identity Server 内部 LDAP 認証ユーザ情報」パネルで、次の情報を入力して amldap ユーザを作成します。

図 4-13　「内部 LDAP 認証ユーザ情報」パネル



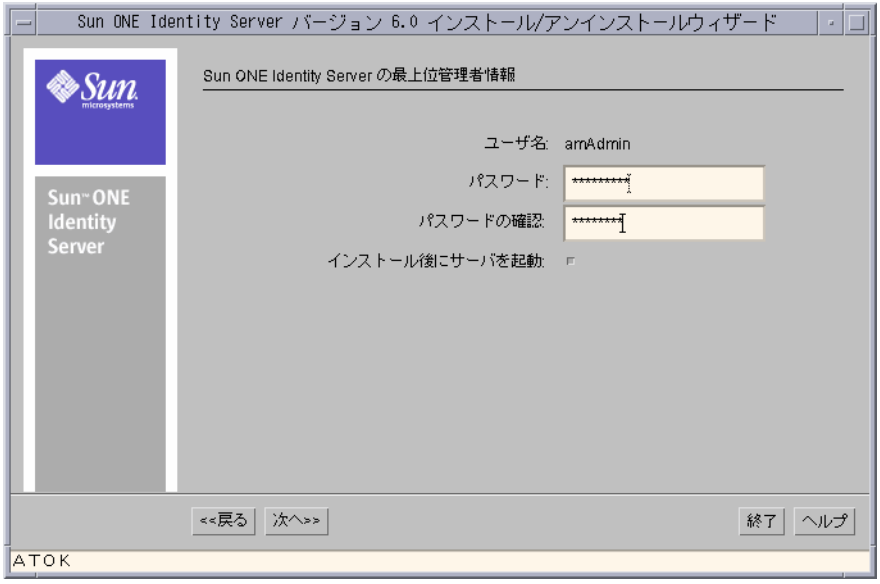
ユーザ名 : これは、LDAP/ メンバーシップ / ポリシーサービスのバインド DN ユーザです。ユーザ名は、*amldapuser* としてハードコードされ変更できません。このユーザは、読み取り権を持ち、Directory Server エントリの検索を行えます。

パスワード : *amldap* ユーザのパスワードを入力します。このパスワードは一意のもので、次のパネルで入力する最上位管理者のパスワードとは異なっている必要があります。このパスワードは、Identity Server とエージェント間の共有シークレットになります。

パスワードの確認 : 確認のためにもう一度パスワードを入力します。

17. 「次へ」をクリックし、「Sun ONE Identity Server の最上位管理者情報」パネルで次の情報を入力します。

図 4-14　「Sun ONE Identity Server の最上位管理者情報」パネル



ユーザ名：最上位管理者のユーザ名は amAdmin です。この名前は設定し直すことはできません。

パスワード：ユーザ amAdmin のパスワードを入力します。パスワードの指定には 8 文字以上必要です。このパスワードは、前のパネルで設定した amldapuser パスワードとは異なっている必要があります。

パスワードの確認：確認のため、amAdmin パスワードを再度入力します。

インストール後にサーバを起動：インストール後に Identity Server を自動的に起動する場合は、このオプションをクリックします。このオプションを選択しない場合は、インストール後に手動でサーバを起動できます。実行手順については、195 ページの「Identity Server サービスの起動」を参照してください。

18. 「次へ」をクリックして、「現在選択されている設定」パネルで、入力した設定情報を確認します。変更が必要な場合は、「戻る」をクリックし、必要なパネルに移動して変更を行います。変更の必要がない場合は、「次へ」をクリックして処理を続行します。

19. 「インストールの準備完了」パネルで、インストール情報を確認します。変更が必要な場合は、「戻る」をクリックして、前の任意のパネルに移動します。それ以外の場合は、「今すぐインストール」をクリックしてインストールを開始します。

20. 「インストールの要約」パネルで、「詳細」をクリックして、インストール中に処理された設定情報の詳細を確認します。「終了」をクリックしてプログラムを終了します。

    Identity Server のインストールが完了し、Identity Server コンソールにログインできます。実行手順については、195 ページの「インストール後のタスク」を参照してください。

コマンド行からの Identity Server のインストール

UNIX のコマンド行から `nodisplay` オプションを使用して、インストールプログラムを実行することもできます。

始める前に

最初に、次の事項を確認してください。

- Identity Server をインストールするコンピュータに、root (Solaris の場合) または管理者 (Windows 2000 の場合) としてログインします。このマシンをホストマシンと呼びます。
- ホストマシンのドメイン名の設定が必要です。ドメイン名が設定されていない場合は、38 ページの「ドメイン名の設定」の手順に従ってください。

コマンド行から Identity Server サービスをインストールするには

1. 製品 CD から Identity Server をインストールする場合は、ソフトウェアをインストールするシステムのドライブに製品 CD を挿入します。

   製品をダウンロードした場合は、次のコマンドを使って製品バイナリファイルを解凍します。

   ```
   gunzip -dc binaryfile.tar.gz | tar -xvof -
   ```

   この場合、*binaryfile* はダウンロードした製品バイナリです。

2. バイナリファイルを解凍したディレクトリに移動して、プロンプトから次のコマンドを入力し Enter を押します。

   ```
   # ./setup -nodisplay
   ```

   Windows 上でインストールする場合は、次のコマンドを使用します。

```
java am -nodisplay
```

インストールスクリプトにより、次のメッセージが表示されます。

```
SunONE Identity Server のインストール / アンインストールプログラムを実行しています。このプログラムでは、サーバをインストール / アンインストールするために、ユーザによる設定が必要です。

インストール / アンインストールプログラムは、ユーザに情報を提供する 1 つまたは複数の選択肢があり、ユーザは SunONE Identity Server のインストール / アンインストール方法を決定する設定を入力します。

次の質問が表示されると、インストール / アンインストールプロセスが中断され、ユーザは提示された情報を読むことができます。準備が整ったら、Enter キーを押してインストール / アンインストールを継続します。
< 継続するには ENTER キーを押します >

一部の質問では、詳細な情報を入力する必要があります。そのような質問では、カッコ [] にデフォルト値が表示されていることがあります。たとえば、次の質問のデフォルトの応答は yes です :

Are you sure? [yes]
デフォルトの応答を受け入れる場合、Enter キーを押すだけです ( 一部のキーボードでは Return となっています )。
別の応答をする場合、コマンドプロンプトに応答を入力し、Enter キーを押します。

< 継続するには ENTER キーを押します >
```

3. 画面に表示される手順を確認します。インストーラが示すさまざまなプロンプトに対する応答方法の説明が表示されます。手順を確認したら、Enter を押してソフトウェアライセンス契約を確認します。インストールのどの段階でも、< を入力して前のプロンプトに戻ることができます。また、! を入力してインストールプログラムを終了することができます。
4. ライセンス契約を確認し、yes と入力してライセンス契約に同意します。
5. 次のプロンプトで、Identity Server をインストールするディレクトリを指定します。

```
SunONE Identity Server コンポーネントは、次のディレクトリにインストールされます。そのディレクトリは、" インストールディレクトリ " と呼ばれます。このディレクトリを使用するには、Enter キーだけを押します。別のディレクトリを使用するには、そのディレクトリの完全パスを入力した後に Enter キーを押します。

SunONE Identity Server コンポーネントをインストールするディレクトリ
[/opt] {"<" 戻る , "!" 終了 }:
```

6. 次のオプションから、Sun ONE Identity Server 管理およびポリシーサービスを選択します。オプション番号 1 を入力して選択します。

```
インストールするコンポーネントを次の中から選択してください。インストールするコンポーネントの番号を入力し、ENTER キーを押してください
1. Sun ONE Identity Server 管理サービスとポリシーサービス
2. Sun ONE Identity Server 管理コンソールのみ
3. 既存の Directory Server を設定
4. Sun ONE Identity Server ドメイン間シングルサインオンコンポーネント
5. 連合管理用の共通ドメインサービス
コンポーネントを選択し ENTER キーを押します [1] {"<" 戻る , "!" 終了 }
```

7. 次のプロンプトで、カスタム Java SDK を使用するかどうかを指定します。Identity Server がサポートする Java には、Java SDK バージョン 1.3.1_06 が必要です。デフォルトの Java SDK が提供されていますが、ユーザ独自の JDK (バージョン 1.3.1_06) を使用できます。

```
Java 設定

Sun ONE Identity Server が使用する JDK について次の情報を提供してくだ
さい。

カスタム JDK を使用しますか :
すでにマシンに JDK がインストールされていて、JDK のバージョンが 1.3.1_06
の場合は、yes を選択してください
JDK がまだインストールされていない場合、または JDK のバージョンが
1.3.1_06 でない場合は、no を選択してください

JDK パス :
既存の JDK の完全なパスを入力してください。

   カスタム JDK を使用しますか [n] {"<" 戻る , "!" 終了 }
```

8. 既存の JDK 1.3.1_06 がある場合は、y を入力して JDK への絶対パスを入力します。それ以外の場合は、n を入力してインストールプログラムに付属する JDK を使用します。
9. 次の情報を入力して、Sun ONE Web Server をインストールし、設定します。

```
Sun ONE Web Server 情報
   管理者 [admin] {"<" 戻る , "!" 終了 }:
   ポート [58888] {"<" 戻る , "!" 終了 }:
   パスワード :
   パスワードの確認 :
   サーバを実行するユーザ [nobody] {"<" 戻る , "!" 終了 }:
   サーバを実行するグループ [nobody] {"<" 戻る , "!" 終了 }:
```

管理者 [admin]: Sun ONE Web Server のサーバ管理者としてのユーザ名を入力します。Enter を押して、デフォルトのユーザ ID (admin) を選択します。

ポート [58888]: Identity Server サービスを実行する Web Server のポート番号を入力します。デフォルトのポート番号は 58088 です。デフォルトのポート番号を選択する場合は Enter を押します。

パスワード : Web Server 管理者のパスワードを入力します。パスワードの指定には 8 文字以上必要です。

パスワードの確認 : 確認のためにもう一度 Web Server 管理者パスワードを入力します。

サーバを実行するユーザ [nobody]: Web Server を実行するユーザアカウントを入力します。Enter を押して、デフォルトユーザ nobody を選択します。Windows でのインストール時に、このプロンプトは使用できません。

サーバを実行するグループ [nobody]: 上述のユーザが属するグループを入力します。例 : nobody など。Windows でのインストール時に、このプロンプトは使用できません。

10. 次の情報を指定して、Sun ONE Identity Server サービスを実行する Web Server をインストールし、設定します。

```
Sun ONE Identity Server サービスを実行する Web Server
   ホスト [nila.Siroe.COM] {"<" 戻る , "!" 終了 }:
   ポート [58080] {"<" 戻る , "!" 終了 }:
   サービス配備 URI [amserver] {"<" 戻る , "!" 終了 }:
   共通ドメイン配備 URI [common] {"<" 戻る , "!" 終了 }:
   サービスと一緒にコンソールをインストールする [yes] {"<" 戻る , "!" 終了 } no
```

ホスト [nila.Siroe.COM]: Web Server を実行するコンピュータの完全指定のドメイン名を入力します。デフォルトの名前を使用するには、Enter を押します。

ポート [58080]: Web Server が使用するポート番号を入力します。

サービス配備 URI [/amserver]: Web Server は、URI (Universal Resource Identifier) 接頭辞の指定に従って、サービスに関連付けられた HTML ページや Web アプリケーション固有の情報 (クラス、jar などに関する情報) を検索します。

デフォルトの URI 接頭辞は `amserver` です。Enter を押してデフォルトの接頭辞を受け入れるか、あるいは別の名前を入力できます。

共通ドメイン配備 URI: Web Server の共通ドメインサービスにアクセスする URI。デフォルトの URI は `common` です。必要に応じて変更可能です。

サービスと一緒にコンソールをインストールする [yes]: サービスとともにコンソールを導入する場合は、Enter を押します。既存のコンソールを使用しており、インストールプログラムに付属のコンソールをインストールしない場合は no を入力します。no を入力した場合は、次のプロンプトで既存のコンソールに関する情報を入力する必要があります。

11. 次のプロンプトで、既存のコンソールに関する次の詳細情報を入力します。

```
Sun ONE Identity Server Console を実行する Web Server
   ホスト [nila.Siroe.COM] {"<" 戻る , "!" 終了 }:
   ポート [58080] {"<" 戻る , "!" 終了 }:
   コンソール配備 URI [amconsole] {"<" 戻る , "!" 終了 }:
```

ホスト [nila.Siroe.COM]: Web Server を実行するコンピュータの名前を入力します。デフォルトの名前を使用するには、Enter を押します。

ポート [58080]: Web Server が使用するポート番号を入力します。

コンソール配備 URI [amconsole]: Web Server は、URI (Universal Resource Identifier) 接頭辞の指定に従って、Identity Server コンソールに関連付けられた HTML ページや、その他の Web アプリケーション固有の情報 (クラス、jar などに関する情報) を検索します。デフォルトの URI 接頭辞は `amconsole` です。別の名前を入力することもできます。

12. 次のプロンプトで、1 を入力するか、または Enter を押して、Identity Server 6.0 に付属の Sun ONE Directory Server をインストールします。

```
ディレクトリのルートの接尾辞
1. 新規 Sun ONE Directory Server をインストール
2. 既存の DIT なしで既存の Sun ONE Directory Server を使用
3. 既存の DIT とともに既存の Sun ONE Directory Server を使用
上のオプションの 1 つを選択してください [1] {"<" 戻る , "!" 終了 }
```

既存の Directory Server で Identity Server を使用する場合は、2 または 3 を入力します。既存の Directory Server 上に Identity Server をインストールする手順については、第 5 章「既存の Directory Server を使用する Identity Server のインストール」を参照してください。

13. 次のプロンプトで、情報を入力して DIT を設定します。

```
ディレクトリのルートの接尾辞
   ディレクトリツリー内の Sun ONE Identity Server ルート [dc=siroe,dc=COM] {"<"
   戻る , "!" 終了 }:
```

ディレクトリツリー内の Sun ONE Identity Server ルート [dc=siroe,dc=COM]:
ルート接尾辞として設定する識別名 (DN) を入力します。識別名 (DN) には、最低 1 個の type=value ペアが必要です。たとえば、
`o=isp;o=madisonparc;dc=Siroe,dc=COM` のようになります。

14. 次のプロンプトで、情報を入力して Sun ONE Directory Server をインストールし、設定します。

```
Sun ONE Directory Server 情報
   ホスト [nila.Siroe.COM] {"<" 戻る , "!" 終了 }:
   ポート [389] {"<" 戻る , "!" 終了 }:
   インストールディレクトリ [/usr/iplanet/servers] {"<" 戻る , "!" 終了
}:
ディレクトリが存在しません。ディレクトリを作成しますか ?
   作成 [yes] {"<" 戻る , "!" 終了 } yes
   ディレクトリマネージャ [cn=Directory Manager] {"<" 戻る , "!" 終了
}:
   パスワード :
   パスワードの確認 :
```

ホスト [nila.Siroe.COM]: Directory Server をインストールするコンピュータのドメイン名を入力します。デフォルトの名前を使用するには、Enter を押します。

ポート [389]: Directory Server が使用するポート番号を入力します。デフォルトのポート番号を使用するには、Enter を押します。ポートがすでに使用されている場合、インストールプログラムから別のポート番号を入力するよう要求されます。1 ～ 65535 までの別の番号を入力できます。

インストールディレクトリ [/usr/iplanet/servers]: Directory Server をインストールするディレクトリ。デフォルトディレクトリ `/usr/iplanet/servers` が空であることを確認するか、さもなければ新しいインストールディレクトリを指定することをお勧めします。これは、アンインストールが必要になった場合に、アンインストールプログラムにより、このディレクトリが内容を含めて削除されてしまい、以前にそのディレクトリにあったすべてのデータが消失することがあるためです。

ディレクトリマネージャ [cn=Directory Manager]: Directory Server 管理ユーザ、つまりディレクトリマネージャは、Directory Server のデータおよび設定に対して無制限のアクセス権を持つ管理者です。ディレクトリマネージャのデフォルト DN は、`cn=Directory Manager` です。

パスワード : Directory Server 管理者のパスワードを入力します。パスワードの指定には 8 文字以上必要です。

パスワードの確認 : パスワードを確認するために、もう一度入力します。

15. 次のプロンプトで、情報を入力して Directory Server を管理する管理サーバを設定します。

```
Directory Server を管理する管理サーバ
   管理者 [admin] {"<" 戻る , "!" 終了 }:
   ポート [58900] {"<" 戻る , "!" 終了 }:
   パスワード :
   パスワードの確認 :
```

管理者 [admin]: Sun ONE Directory Server を管理する管理サーバにアクセスできる管理者のユーザ名を入力します。デフォルトのユーザ名は `admin` です。

ポート [58900]: 管理サーバのポート番号を入力します。デフォルトでは、このポート番号は `58900` に設定されます。

パスワード : ユーザ `amAdmin` のパスワードを入力します。パスワードの指定には 8 文字以上必要です。

パスワードの確認 : 入力したパスワードを確認するために、もう一度入力します。

16. 次のプロンプトで、Sun ONE Identity Server 内部 LDAP 認証ユーザのインストールおよび設定に関する情報を入力します。

```
Sun ONE Identity Server 内部 LDAP 認証ユーザ情報
ユーザ名 : amldapuser
パスワード :
パスワードの確認 :
```

ユーザ名 : これは、LDAP/ メンバーシップ / ポリシーサービスのバインド DN ユーザです。ユーザ名は、*amldapuser* としてハードコードされ変更できません。このユーザは、読み取り権を持ち、Directory Server エントリを検索できます。

パスワード : *amldap* ユーザのパスワードを入力します。このパスワードは一意のもので、次のパネルで入力する最上位管理者のパスワードとは異なっている必要があります。このパスワードは、Identity Server とエージェント間の共有シークレットになります。

パスワードの確認 : 確認のためにもう一度パスワードを入力します。

17. 次のプロンプトで、Sun ONE Identity Server 最上位管理者に関する情報を入力します。

```
Sun ONE Identity Server の最上位管理者情報
ユーザ名
    パスワード :
    パスワードの確認 :
    インストール後にサーバを起動 [yes] {"<" 戻る , "!" 終了 }:
```

ユーザ名 : これは、Identity Server が管理するすべてのエントリに対して無制限のアクセス権を持つ管理者です。最上位管理者のユーザ ID は、`amAdmin` としてハードコードされています。これにより、Identity Server 管理者ロールとその権限が作成されて適切に Directory Server に割り当てられるので、インストール直後に Identity Server 製品にログインできます。これは管理者ロールなので、インストール後にほかのユーザをこのロールに追加できます。

パスワード : 管理者のパスワードを入力します。このパスワードは、前のプロンプトで設定した amldapuser パスワードとは異なっている必要があります。

パスワードの確認 : 入力したパスワードを確認するために、もう一度入力します。

インストール後にサーバを起動 [yes]: Enter を押すと、インストール後 Identity Server サーバは自動的に起動します。インストール後、手動でサーバを起動する場合は *no* を入力します。

選択した設定が、インストールプログラムにより表示されます。

```
現在選択されている設定
Sun ONE Identity Server コンソール : http://nila.Siroe.COM:58080
コンソール配備 URI:/amconsole
Sun ONE Identity Server サービス : http://nila.Siroe.COM:58080
サービス配備 URI:/amserver
Sun ONE Identity Server インストールディレクトリ : /opt
管理者 : admin
ポート : 58888
ディレクトリサーバ : nila.Siroe.COM:389
ディレクトリマネージャ :cn=Directory Manager
DS インストールディレクトリ : /usr/iplanet/servers
ディレクトリ管理者 : admin
ディレクトリ管理者ポート : 58900
既存の DIT を使用 :  false
Sun ONE Identity Server ルート : dc=Siroe,dc=COM
```

また、コンピュータの使用可能な空きディスク容量が検出され、インストールするコンポーネントの一覧が表示されます。

```
次のコンポーネントがインストールされます :

プロダクト : Sun ONE Identity Server
場所 : /opt
サイズ :197.94MB
---------------------------------
JDK
Sun ONE Directory Server
Sun ONE Web Server
その他のパッケージ
Sun ONE Identity Server 管理サービスとポリシーサービス
Sun ONE Identity Server 管理コンソール
連合管理用の共通ドメインサービス
リソースパッケージ

インストールの準備完了
1. 今すぐインストール
2. 開始
3. 終了
上のオプションを 1 つ選択してください [1] {"<" 戻る , "!" 終了 }
```

18. 1 を入力し、Enter を押して選択したコンポーネントをインストールします。

    選択した設定を変更する場合は、2 を入力します。インストールプログラムにより、最初のプロンプトが表示されます。Identity Server をインストールしない場合は、3 を入力してプログラムを終了します。

19. Identity Server が正常にインストールされたら、次のプロンプトで Enter を押してプログラムを終了します。

```
インストール中 Sun ONE Identity Server
|-1%
--------------25%-----------------50%-----------------75%-------
-------100%|
インストールの要約
プロダクト            要約の結果   詳細
1.  Sun ONE Identity Server インストールされました       ログを表示する
には 1、終了するには 2 を入力してください。

終了
オプションを 1 つ選択してください [2] {"!" 終了 }
```

Identity Server のインストールが完了し、Identity Server コンソールにログインできます。実行手順については、195 ページの「インストール後のタスク」を参照してください。

第 5 章

既存の Directory Server を使用する Identity Server のインストール

ユーザデータが存在する既存の Directory Server を使う場合、Sun ONE Identity Server がユーザデータを認識できるように、ディレクトリ情報ツリー (DIT) に対していくつかの変更を行う必要があります。必要な変更の数や範囲は、既存の DIT の構造、および Identity Server の使用方法によって異なります。

この章では、ユーザデータが存在する既存のディレクトリに対して Identity Server サービスをインストールするための手順について説明します。また、DIT と連携させるための Identity Server の設定方法、および既存のディレクトリエントリに必要な変更を加える方法についても説明します。

アイデンティティ管理のサポートなしで、ポリシー管理用の Identity Server をセットアップすることができます。ポリシー管理のためだけに設定を行うには、インストール時に「既存の DIT とともに既存の Sun ONE Directory Server を使用」オプションを選択して、Identity Server の管理およびポリシーサービスをインストールします。「はい」を選択して、インストール時に Identity Service Management エントリを自動的にロードします。インストール後、Identity Server コンソールからポリシー管理を実行できるようになります。インストール後にアイデンティティ管理を有効にする場合は、*IS_root*/SUNWam/migration/README を参照して実行手順の詳細を確認してください。

この章には次のトピックがあります。

- 始める前に
- インストールの方法
- 既存の Directory Server の設定
- 既存の Directory Server を使用する Identity Server のインストール
- カスタムのオブジェクトクラスの Identity Server スキーマへの追加 (オプション)
- 代替ネーミング属性の設定 (オプション)

- Identity Server LDIF のディレクトリへの読み込み
- Identity Server サービス属性のディレクトリへの読み込み
- Identity Server ACI のデフォルト組織への追加 (オプション)
- Identity Server の起動
- Identity Server のオブジェクトクラスと属性の既存のディレクトリエントリへの追加
- 変更された LDIF ファイルの読み込み

始める前に

必要なディレクトリ変更は複雑です。変更には LDAP の計画と実装に関する高度な専門知識が必要であり、また XML に関する知識も必要です。この手続きは複雑であり、時間がかかることがあります。配備の際にはこの問題を考慮して計画を立てるようにしてください。

注 ユーザデータが存在する既存のディレクトリがない場合は、この章で説明されている手順を実行する必要はありません。第 4 章「新しい Directory Server を使用するインストール」を参照してください。

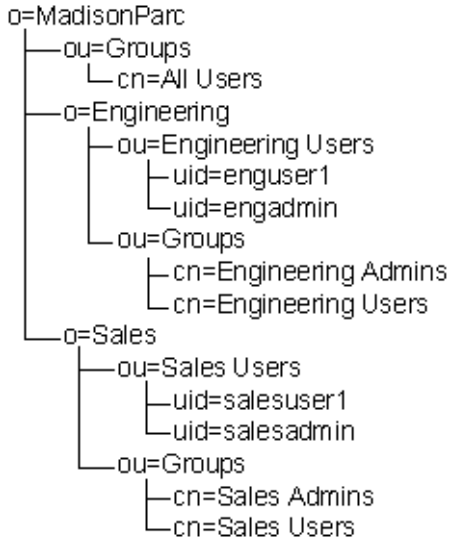
この章で使っている例に関する基本情報

ディレクトリに対して行う必要のある変更のタイプを例示するために、架空の会社の単純な DIT を使用します。*o=madisonparc* で表されるこの会社のディレクトリエントリには、2 つのカスタムオブジェクトクラスが含まれています。それらは、Identity Server スキーマでまだ定義されていないオブジェクトクラスです。使用している DIT にカスタムオブジェクトクラスが含まれている場合は、Identity Server の XML ファイルも変更する必要があります。

基本的な DIT の構造

この章で使っている例は、架空の会社の単純な DIT に基づいています。71 ページの図 5-1 では、ルートの下に 2 つの組織、*Engineering* と *Sales* があります。この例の中のグループはすべてスタティックグループです。これは、これらのグループのエントリが、グループのメンバーを命名する値を含む `groupOfUniqueNames` オブジェクトクラスを使うことを意味します。

図 5-1　この章の例で使われるディレクトリ情報ツリー (DIT)



この DIT の例にあるグループの使用法について次に要約します。

- Engineering の管理者を含むグループが 1 つ、Sales の管理者から成るグループが 1 つあります。
- これらのグループのメンバーがそれぞれの組織を管理できるように、Engineering グループと Sales グループには単純な ACI が設定されています。
- 各組織には、管理者でないユーザを含むグループが 1 つあります。
- ルートレベル、つまり最上位レベルにもう一つ別のグループがあります。このグループには、ディレクトリ内のすべてのユーザが含まれます。

カスタムオブジェクトクラス

この例に出てくる架空の会社では、Identity Server スキーマにも Directory Server 5.1 スキーマにも含まれていない 2 つのオブジェクトクラスを使用します。AUXILIARY オブジェクトクラス `madisonparc-org` はすべての組織エントリに存在し、AUXILIARY オブジェクトクラス `madisonparc-user` はすべてのユーザエントリに存在します。これらの拡張を管理するには、次の 3 つのファイルを変更する必要があります。

- `amEntrySpecific.xml`
  (ユーザエントリだけを変更する場合、変更は不要)
- `amUser.xml`
- `ums.xml`

これらの変更の詳しい説明は、100 ページの「カスタムのオブジェクトクラスの Identity Server スキーマへの追加 (オプション)」の節にあります。カスタムオブジェクトクラスを既存のディレクトリで使う場合は、同様の変更が必要です。

インストールの方法

既存のセットアップに基づくインストール方法を次の表で説明します。

表 5-1 インストールシナリオ

シナリオ	方法
Directory Server をまったく使用していない場合	Identity Server 6.0 のすべてのコンポーネントをインストールします。手順については、第 4 章「新しい Directory Server を使用するインストール」を参照してください。
5.1 より前の Directory Server を使用している場合	次の手順どおりに実行します。 1. Directory Server のデータを Directory Server 5.1 に移行します。データ移行の手順は、73 ページの「既存のデータの Directory Server 5.1 への移行」の節にあります。 2. インストールプログラムのオプション「既存の Directory Server を設定する」を使って、この Directory Server を設定します。 3. Identity Server 6.0 管理およびポリシーサービスをインストールします。 この手順を実行するには、第 4 章で説明するインストール手順に従ってください。ただし、「Sun ONE Directory Server 情報」パネルで、デフォルトのインストールディレクトリ `/usr/iplanet/servers` を、既存の Directory Server の場所に置き換える必要があります。
DSAME 5.1 を使用している場合	データを Identity Server 6.0 に移行します。この手順は、製品バイナリに付属のファイル `migration.html` にあります。
Identity Server と連携するよう設定されていない Directory Server 5.1 を使用している場合	Identity Server 6.0 と連携するよう設定します。実行手順の詳細は、「既存の Directory Server の設定」の節を参照してください。
Identity Server と連携するよう設定されている Directory Server 5.1 を使用している場合	インストールプログラムの「既存の DIT とともに既存の Sun ONE Directory Server を使用」オプションを選択して、Identity Server 6.0 管理およびポリシーサービスをインストールします。手順については、80 ページの「既存の Directory Server を使用する Identity Server のインストール」を参照してください。

表 5-1　インストールシナリオ (続き)

シナリオ	方法
既存の DIT のない Directory Server 5.1 を使用している場合	インストールプログラムの「既存の DIT なしで既存の Sun ONE Directory Server を使用」オプションを選択して、Identity Server 6.0 管理およびポリシーサービスをインストールします。手順については、80 ページの「既存の Directory Server を使用する Identity Server のインストール」を参照してください。
既存の DIT のある Directory Server 5.1 を使用している場合	インストールプログラムの「既存の DIT とともに既存の Sun ONE Directory Server を使用」オプションを選択して、Identity Server 6.0 管理およびポリシーサービスをインストールします。手順については、80 ページの「既存の Directory Server を使用する Identity Server のインストール」を参照してください。

既存のデータの Directory Server 5.1 への移行

Identity Server 6.0 をインストールする前に、既存のユーザデータを Directory Server 5.1 に移行する必要があります。そうしないと、Identity Server は既存のユーザデータを認識できません。

この手順では、5.1 より前のデータを Directory Server 5.1 で使用できるように更新します。この処理は、Directory Server に付属の `migrateInstance5` スクリプトを実行して行います。移行スクリプトにより、次のタスクが順に実行されます。

- スキーマ設定ファイルを調べて、標準の設定ファイルとシステムに存在する設定ファイルの違いを通知します。
- レガシー Directory Server に格納されている接尾辞ごとにデータベースを作成します。(Directory Server 5.0 では、複数のデータベースが可能ですが、データベース当たり 1 つの接尾辞です。)
- サーバパラメータとデータベースパラメータを移行します。(Directory Server 5.0 では、これらは `dse.ldif` ファイルの LDAP エントリとして格納されています。)
- ユーザ定義のスキーマオブジェクトを移行します。
- インデックスを移行します。
- 標準のサーバプラグインを移行します。
- 証明書データベース、および SSL パラメータを移行します。

既存の Directory Server がインストールされているシステムでスクリプトを実行する必要があります。移行スクリプトを実行する前に、ディレクトリサービスを停止しておく必要があります。移行手順については、次の『Sun ONE Directory Server インストールガイド』を参照してください。

```
http://docs.sun.com/db/doc/816-5602-10
```

データを Directory Server 5.1 に移行してある場合は、74 ページの「ディレクトリデータのバックアップ」に進んでください。

注 インストール後、適切な LDIF または XML ファイルをロードするまで、管理コンソールにはログインできません。手順については、この章の後述の節を参照してください。

ディレクトリデータのバックアップ

ディレクトリのバックアップについては、次の『Sun ONE Directory Server インストールガイド』を参照してください。

```
http://docs.sun.com/db/doc/816-5602-10
```

既存の Directory Server の設定

Identity Server と連携するように設定されていない Sun ONE Directory Server 5.1 を使用している場合は、最初に Identity Server スキーマをインストールして設定を行い、次に Identity Server 管理およびポリシーサービスをインストールします。Sun ONE Identity Server インストールプログラムを使って、Directory Server を設定する必要があります。

注 コンピュータの別のディレクトリに、Identity Server スキーマがインストール済みでないことを確認します。次のコマンドを使用して、既存のインスタンスを確認できます。

```
pkginfo | grep SUNWamdsc.
```

GUI を使用した設定

1. 製品 CD から Identity Server スキーマをインストールする場合は、ソフトウェアをインストールするシステムのドライブに製品 CD を挿入します。

   製品をダウンロードした場合は、次のコマンドを使って製品バイナリファイルを解凍します。

   `gunzip -dc` *`binaryfile`*`.tar.gz | tar -xvof -`

   この場合、*binaryfile* をダウンロードした製品バイナリの名前に置き換える必要があります。

2. 別の端末ウィンドウを開き、`xhost +` と入力してマシンのアクセス制御を無効にします。

3. アプリケーションウィンドウで、次のコマンドのどちらかを使用して DISPLAY 変数を設定します。

   - csh、または tcsh を使用している場合、次のように入力します。

     `setenv DISPLAY` *`host.domain.com`*`:0.0`

   - sh、ksh、または bash を使用している場合、次のように入力します。

     `export DISPLAY=`*`host.domain.com`*`:0.0`

4. コマンド `./setup` を使用して、`installation` プログラムを実行します。開始パネルが開きます。「次へ」をクリックします。

5. ライセンス契約を確認して同意します。

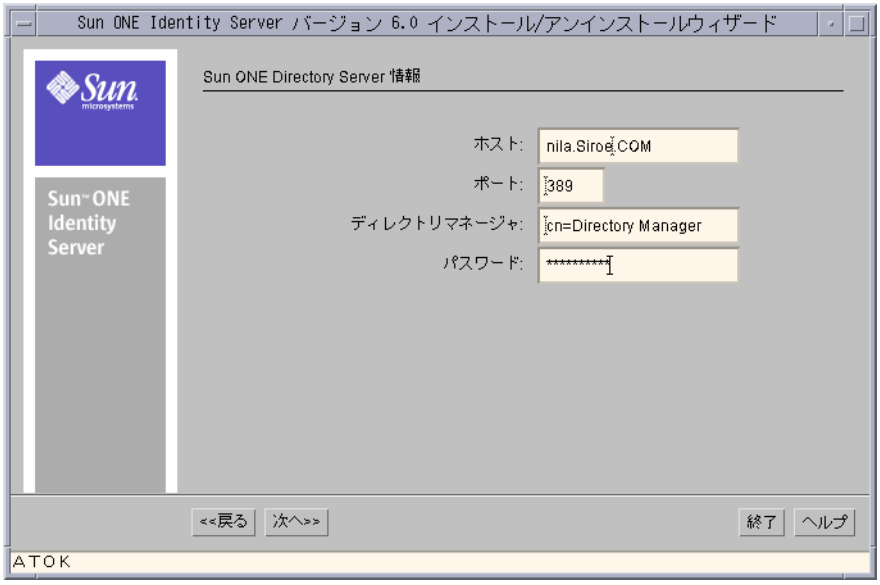
6. 「インストールディレクトリ」パネルで、Identity Server スキーマをインストールするディレクトリのパスを指定します。

7. 「次へ」をクリックし、「インストール / アンインストールされるコンポーネント」パネルで、「既存の Directory Server を設定」をクリックします。

図 5-2　「インストール / アンインストールされるコンポーネント」パネル

8. 「次へ」をクリックし、「Sun ONE Directory Server 情報」パネルで、既存の Directory Server の詳細を入力します。

図 5-3　「Sun ONE Directory Server 情報」パネル



ホスト : Directory Server がインストールされるコンピュータの完全指定のドメイン名を入力します。

ポート : Directory Server のポート番号を入力します。デフォルトのポート番号は 389 です。

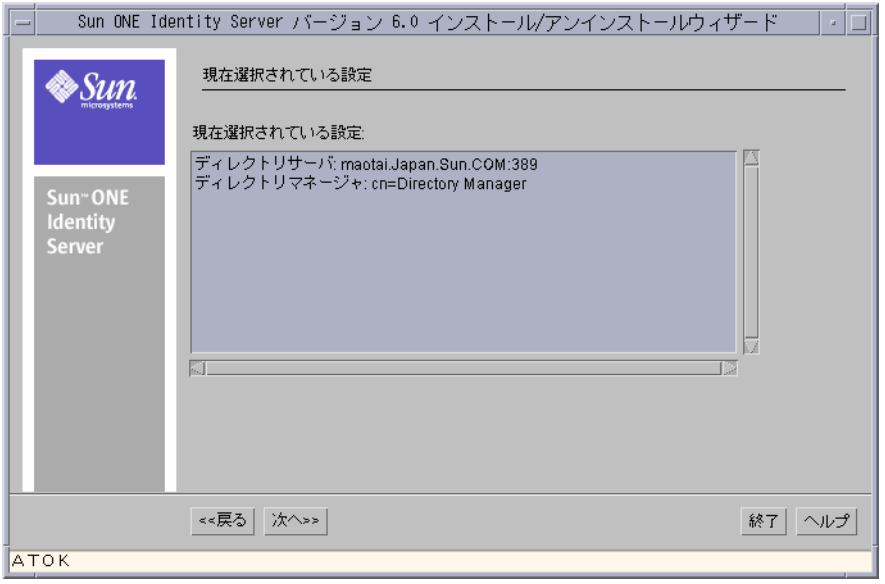
ディレクトリマネージャ : Directory Server へのアクセスを制限されたユーザの DN を入力します。例 : cn=Directory Manager など。

パスワード : ディレクトリマネージャのパスワードを入力します。パスワードの指定には 8 文字以上必要です。

これらのフィールドに入力する情報が不正確であると、インストールプログラムによりエラーメッセージが表示されます。入力した値を確認し、訂正してから次の手順に進んでください。

9. 「次へ」をクリックし、「現在選択されている設定」パネルで選択した設定を表示します。

図 5-4 「現在選択されている設定」パネル



10. 「次へ」をクリックして、「インストールの準備完了」パネルを開きます。
11. 「今すぐインストール」をクリックして、Directory Server を設定します。

コマンド行からの設定

1. バイナリファイルを解凍したディレクトリに移動して、プロンプトから次のコマンドを入力し Enter を押します。

   ```
   # ./setup -nodisplay
   ```

   Windows の場合は、次のコマンドを使用します。

   ```
   java am -nodisplay
   ```

2. 画面に表示される手順を確認します。インストーラが示すさまざまなプロンプトに対する応答方法の説明が表示されます。手順を確認したら、Enter を押してソフトウェアライセンス契約を確認します。インストールのどの段階でも、< を入力して前のプロンプトに戻ることができます。また、! を入力してインストールプログラムを終了することができます。
3. ライセンス契約を確認し、yes と入力してライセンス契約に同意します。
4. 次のプロンプトで、ldif ファイルおよびユーティリティなどの設定ファイルをインストールするディレクトリを指定します。

```
Sun ONE Identity Server コンポーネントは、次のディレクトリにインストール
されます。そのディレクトリは、" インストールディレクトリ " と呼ばれます。この
ディレクトリを使用するには、Enter キーだけを押します。別のディレクトリを使用
するには、そのディレクトリの完全パスを入力した後に Enter キーを押します。Sun
ONE Identity Server コンポーネントをインストールするディレクトリ [/opt]
{"<" 戻る , "!" 終了 }:
```

5. 次のプロンプトで、3 を入力して既存の Directory Server を設定します。

```
インストールするコンポーネントを次の中から選択してください。インストールする
コンポーネントの番号を入力し、ENTER キーを押してください

1. Sun ONE Identity Server 管理サービスとポリシーサービス
2. Sun ONE Identity Server 管理コンソールのみ
3. 既存の Directory Server を設定
4. Sun ONE Identity Server ドメイン間シングルサインオンコンポーネント
5. 連合管理用の共通ドメインサービス

   コンポーネントを選択し ENTER キーを押します [1] {"<" 戻る , "!" 終了 }
```

6. 次のプロンプトで、設定する Directory Server に関する情報を入力します。

```
Sun ONE Directory Server 情報
ホスト [nila.Siroe.COM] {"<" 戻る , "!" 終了 }:
ポート [389] {"<" 戻る , "!" 終了 }:
ディレクトリマネージャ [cn=Directory Manager] {"<" 戻る , "!" 終了 }:
パスワード :
```

7. 次のプロンプトで、1 を入力して設定を開始します。

```
次のコンポーネントがインストールされます :
プロダクト : Sun ONE Identity Server
場所 : /opt
サイズ : 0 bytes
---------------------------------
既存の Directory Server を設定
リソースパッケージ
インストールの準備完了
1. 今すぐインストール
2. 開始
3. 終了
上のオプションを 1 つ選択してください [1] {"<" 戻る , "!" 終了 }
```

セットアッププログラムにより、Directory Server が設定されます。

8. プロンプトで、Enter を押してインストールプログラムを終了します。

既存の Directory Server を使用する Identity Server のインストール

Identity Server と連携するように設定された既存の Directory Server を使用している場合は、次の手順に従って Identity Server 6.0 をインストールする必要があります。

始める前に

最初に、次の事項を確認してください。

- Identity Server をインストールするマシンに、ルート (Windows 2000 の場合は管理者として) でログインします。このマシンをホストマシンと呼びます。
- ホストマシンのドメイン名の設定が必要です。ドメイン名が設定されていない場合は、「ホストコンピュータのドメイン名の設定」の手順に従ってください。

ホストコンピュータのドメイン名の設定

Identity Server をインストールする前に、Identity Server をインストールするマシンにドメイン名が設定されていることを確認します。実行手順の詳細については、38 ページの「ドメイン名の設定」を参照してください。

GUI を使用したインストール

1. 製品 CD から Identity Server をインストールする場合は、ソフトウェアをインストールするシステムのドライブに製品 CD を挿入します。

   製品をダウンロードした場合は、次のコマンドを使って製品バイナリファイルを解凍します。

   ```
   gunzip -dc binaryfile.tar.gz | tar -xvof -
   ```

   この場合、*binaryfile* は製品バイナリファイルの名前です。

2. 別の端末ウィンドウを開き、`xhost +` と入力してマシンのアクセス制御を無効にします。

3. アプリケーションウィンドウで、次のコマンドのどちらかを使用して DISPLAY 変数を設定します。

   csh または tcsh を使用している場合、次のように入力します。

   `setenv DISPLAY` *host.domain.COM:0.0*

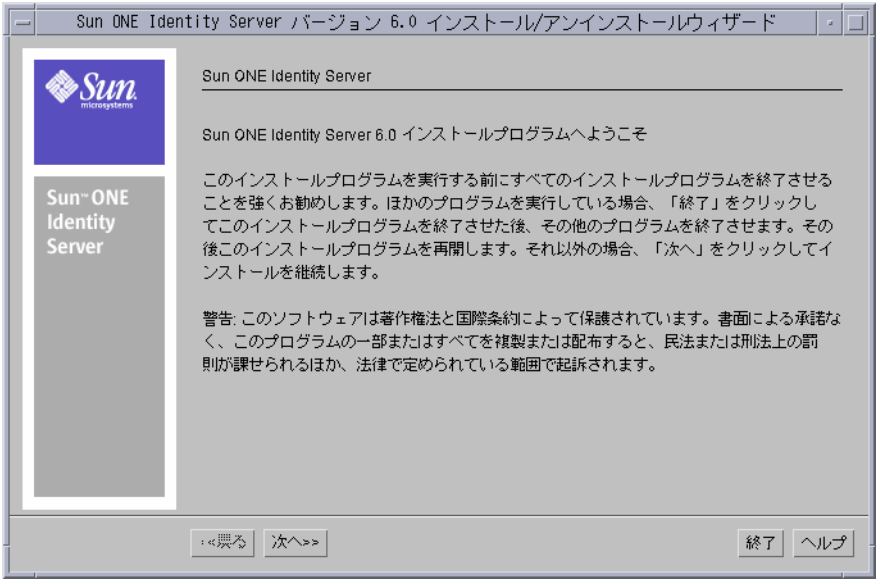
   sh、ksh、または bash を使用している場合、次のように入力します。

   `export DISPLAY=`*host.domain.COM:0.0*

   この場合、`nila` はインストールプログラムを実行しているマシンです。

4. `setup` プログラムを実行します。
5. コマンド行から `./setup` と入力します。インストールプログラムが起動し、開始パネルが開きます。

図 5-5　開始パネル



6. 「次へ」をクリックして、ソフトウェアライセンス契約に同意します。

7. 「インストールディレクトリ」パネルで、Directory Server をインストールするディレクトリを指定します。このディレクトリに対する書き込み権限と実行権限が必要なことに注意してください。

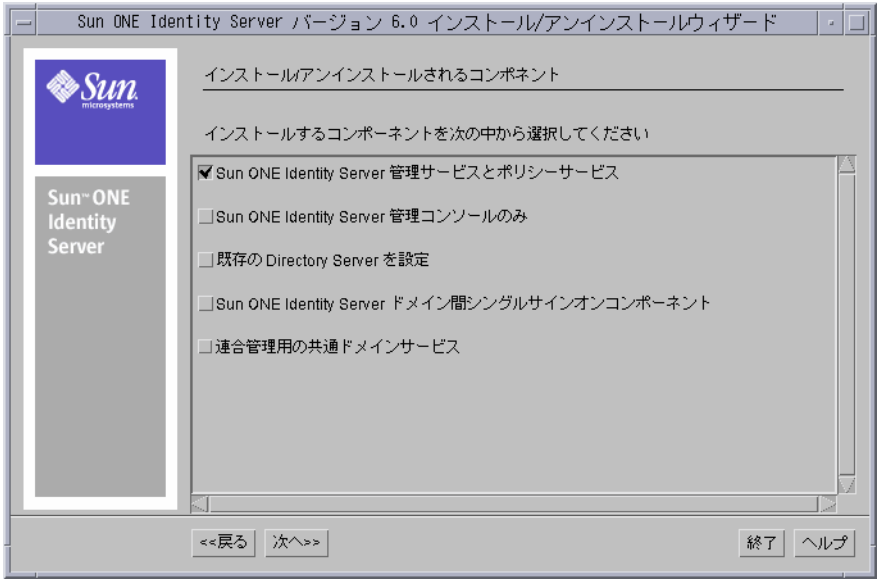
   このディレクトリに Sun ONE Identity Server をインストールします : Identity Server サービスをインストールするディレクトリのパスを入力します。

注　Identity Server サービスと Directory Server を別々のディレクトリにインストールするようにします。Identity Server サービスと Directory Server を別々のコンピュータシステムにインストールするのが理想的です。

8. 「次へ」をクリックし、「インストール / アンインストールされるコンポーネント」パネルで、「Sun ONE Identity Server 管理サービスとポリシーサービス」を選択します。

   インストールプログラムは、これらのサービスと一緒に Sun ONE Web Server、Sun ONE Directory Server、Sun ONE Identity Server コンソール、共通ドメインサービス、Identity Server 管理およびポリシーサービス、および JDK もインストールします。

図 5-6　「インストール / アンインストールされるコンポーネント」パネル

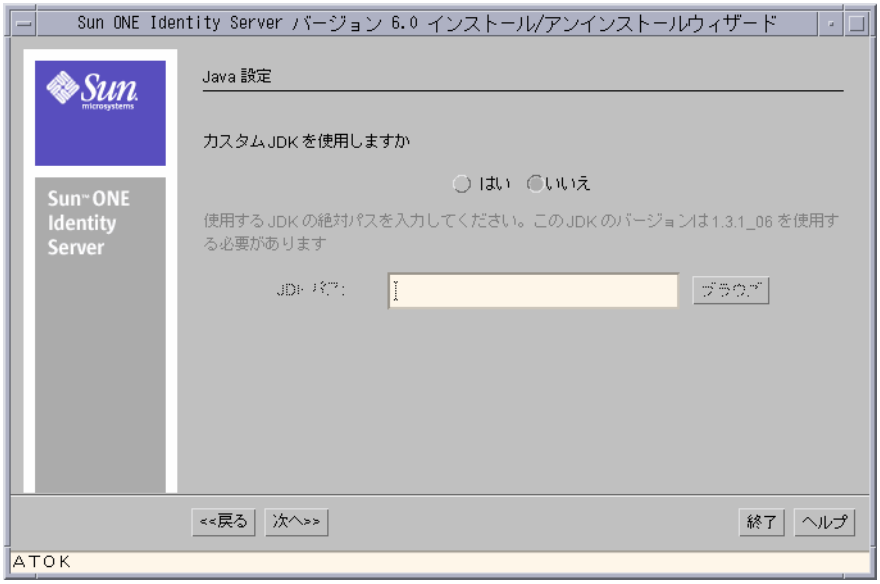


これらのサービスのコンポーネントの詳細については、第 1 章「Identity Server ソリューション」の節と「Sun ONE Identity Server の紹介」を参照してください。

9. 「次へ」をクリックし、「Java の設定」パネルで次の情報を入力します。

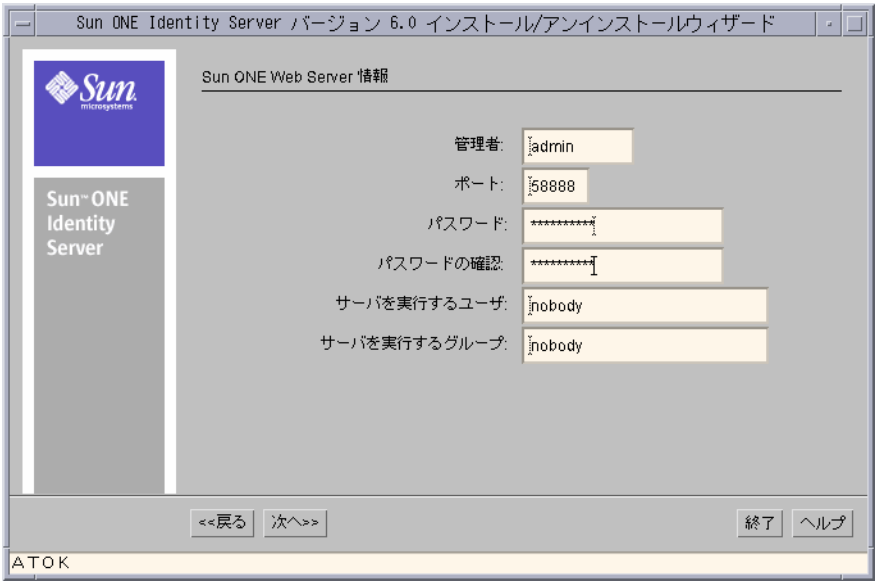
   カスタム JDK を使用しますか : Web Server で Java をサポートするには、Java SDK バージョン 1.3.1_06 が必要です。この Java SDK は Identity Server 6.0 に付属しています。Identity Server に付属の Java SDK をインストールする場合は、「いいえ」を選択します。ただし、既存の JDK (バージョン 1.3.1_06) を使用する場合は、「はい」を選択し、そのファイルの場所への絶対パスを入力します。

図 5-7 「Java 設定」パネル



10. 「次へ」をクリックし、「Sun ONE Web Server 情報」パネルで、Identity Server サービスを実行する Web Server に関する次の情報を入力します。

図 5-8　「Sun ONE Web Server 情報」パネル



管理者 : Web Server にアクセスし、Web Server を管理する管理者としてのユーザ名を入力します。

ポート : ポート番号を入力します。通常、デフォルトは 58888 です。

パスワード : 管理者のパスワードを入力します。パスワードの指定には 8 文字以上必要です。

パスワードの確認 : 管理者パスワードを確認するために、もう一度入力します。

サーバを実行するユーザ : Web Server を実行するユーザアカウントを入力します。例 : nobody など。

サーバを実行するグループ : 上述したユーザが属するグループを入力します。例 : nobody など。

11. 「次へ」をクリックし、「Sun ONE Identity Server サービスを実行する Web Server」パネルで次の情報を入力します。

    ホスト : Identity Server コンポーネントと専用 Web Server の両方をインストールするコンピュータの完全指定のホスト名を入力します。コンピュータのドメイン名が設定され、フィールドに正しく入力されていることを確認します。ドメイン名の設定方法に関する手順については、「ホストコンピュータのドメイン名の設定」の節を参照してください。

    ポート : Identity Server サービスを実行する Web Server のポート番号を入力します。デフォルトのポート番号は 58080 です。

サービス配備 URI: Web Server は、URI (Universal Resource Identifier) 接頭辞の指定に従って、サービスに関連付けられた HTML ページや Web アプリケーション固有の情報 (クラス、jar などに関する情報) を検索します。

デフォルトの URI 接頭辞は `amserver` です。別の名前を入力することもできます。

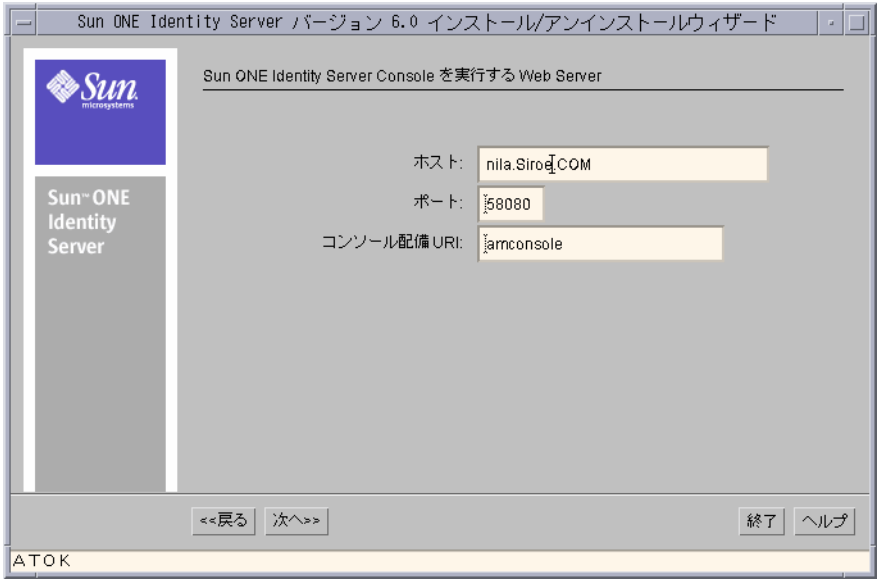
共通ドメイン配備 URI: Web Server の共通ドメインサービスにアクセスする URI です。デフォルトの URI は `common` です。必要に応じて変更可能です。

サービスと一緒にコンソールを配備 : デフォルトでは、このチェックボックスをオンにすると、Identity Server サービスによりコンソールがインストールされます。ただし、既存のコンソールを使用しているため、ここでコンソールを配備する必要がない場合は、チェックボックスをオフにして選択を取り消します。この場合、インストールプログラムにより、既存のコンソールに関する追加情報を要求する別のパネルが表示されます。詳細は、次の手順を参照してください。

コンソール配備 URI: Web Server は、URI (Universal Resource Identifier) 接頭辞の指定に従って、Identity Server コンソールに関連付けられた HTML ページや、その他の Web アプリケーション固有の情報 (クラス、jar などに関する情報) を検索します。デフォルトの URI 接頭辞は `amconsole` です。別の名前を入力することもできます。「サービスと一緒にコンソールを配備」チェックボックスをオフにした場合、このフィールドは使用できません。

12. 前のパネルで、このサービスでコンソールを配備しないように選択した場合は、「Sun ONE Identity Server Console を実行する Web Server」パネルで、既存のコンソールに関する次の情報を入力する必要があります。

図 5-9　「Sun ONE Identity Server Console を実行する Web Server」パネル



ホスト : Identity Server コンソールがインストールされるコンピュータの完全指定のドメイン名を入力します。

ポート : Identity Server サービスを実行する Web Server のポート番号を入力します。デフォルトのポート番号は `58080` です。

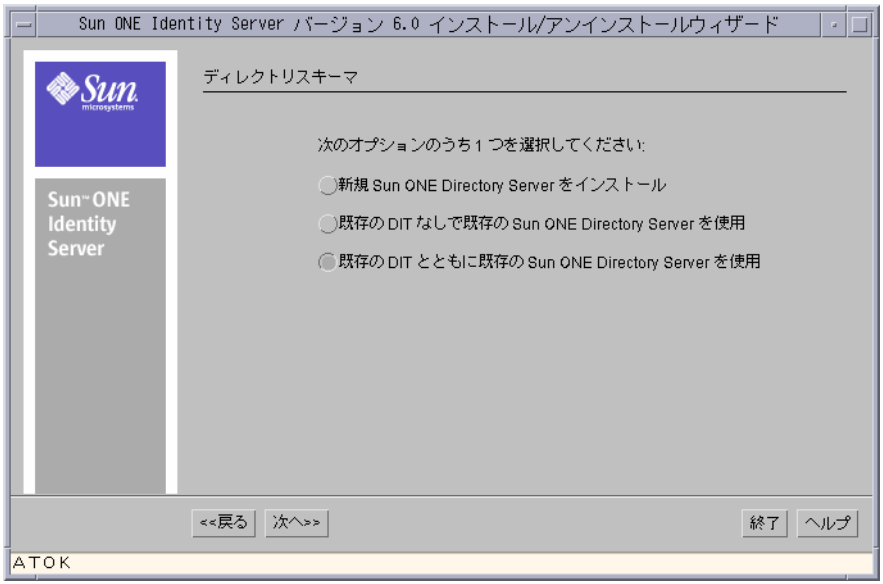
コンソール配備 URI: Web Server は、URI (Universal Resource Identifier) 接頭辞の指定に従って、Identity Server コンソールに関連付けられた HTML ページや、その他の Web アプリケーション固有の情報 (クラス、jar などに関する情報) を検索します。デフォルトの URI 接頭辞は `amconsole` です。別の名前を入力することもできます。

13. 「次へ」をクリックし、「ディレクトリスキーマ」パネルで、次のオプションのどちらか 1 つを選択します。

    既存の DIT なしで既存の Sun ONE Directory Server を使用 : Sun ONE Directory Server 5.1 の既存のインスタンスを使用している場合は、このオプションをクリックします。

    既存の DIT とともに既存の Sun ONE Directory Server を使用: Sun ONE Directory Server 5.1 の既存のインスタンスと既存の DIT を使用している場合は、このオプションをクリックします。

図 5-10　「ディレクトリスキーマ」パネル

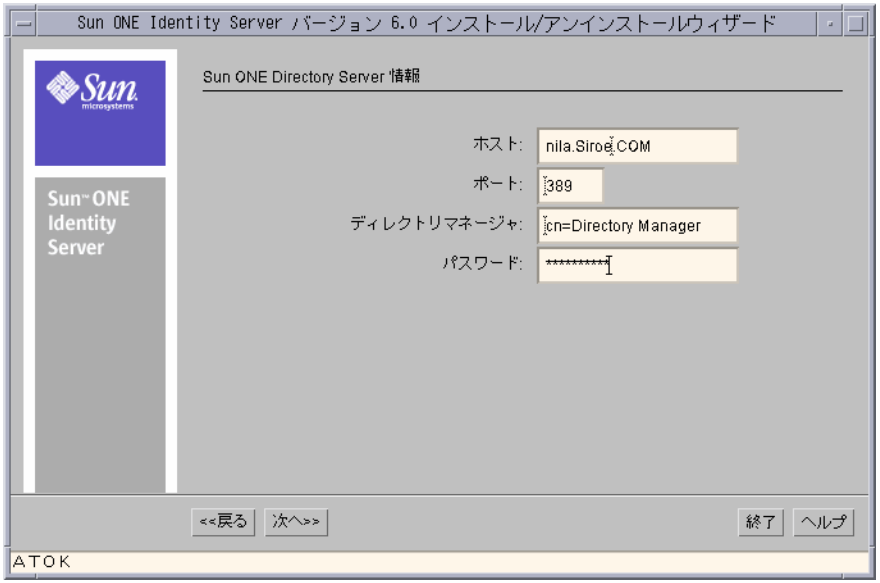


14. 「次へ」をクリックし、「ディレクトリのルートの接尾辞」パネルで次の情報を入力します。

    ディレクトリツリー内の Sun ONE Identity Server ルート : ルート接尾辞として設定する識別名 (DN) を入力します。識別名 (DN) には、最低 1 個の type=value ペアが必要です。たとえば、`o=isp,o=madisonparc,dc=siroe,dc=COM` のようになります。

15. 「次へ」をクリックし、「Sun ONE Directory Server 情報」パネルで次の情報を入力します。

図 5-11 「Sun ONE Directory Server 情報」パネル



ホスト: Directory Server がインストールされるコンピュータの完全指定のドメイン名を入力します。

ポート: Directory Server のポート番号を入力します。デフォルトのポート番号は `389` です。

ディレクトリマネージャ: Directory Server へのアクセスを制限されたユーザの DN を入力します。例: `cn=Directory Manager` など。

パスワード: ディレクトリマネージャのパスワードを入力します。パスワードの指定には 8 文字以上必要です。

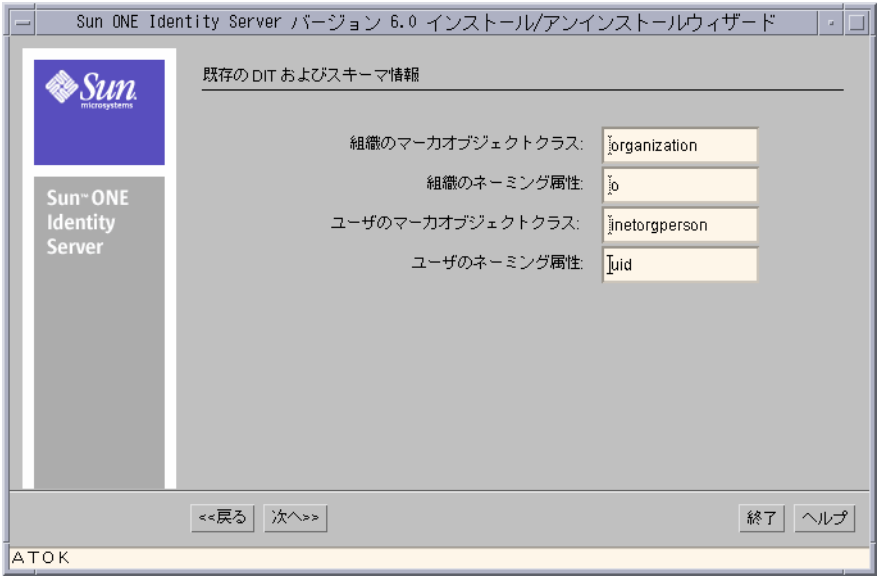
これらのフィールドに入力する情報が不正確であると、インストールプログラムによりエラーメッセージが表示されます。入力した値を確認し、訂正してから次の手順に進んでください。

16. 「次へ」をクリックします。インストールプログラムにより、次のメッセージが表示されます。

    この Directory Server には 6.0 準拠の DIT がありません。インストーラで DIT を Directory Server 内にロードしますか ?: 「はい」をクリックすると、Directory Server に 6.0 準拠 DIT およびスキーマ (`ldif` と `xml`) ファイルが自動的にロードされます。「いいえ」をクリックした場合は、インストール後に手動でファイルをロードできます。

17. 「既存の DIT およびスキーマ情報」パネルで、次の情報を入力します。

図 5-12　「既存の DIT およびスキーマ情報」パネル



組織のマーカオブジェクトクラス : 既存の DIT の組織用に定義されたオブジェクトクラスを入力します。

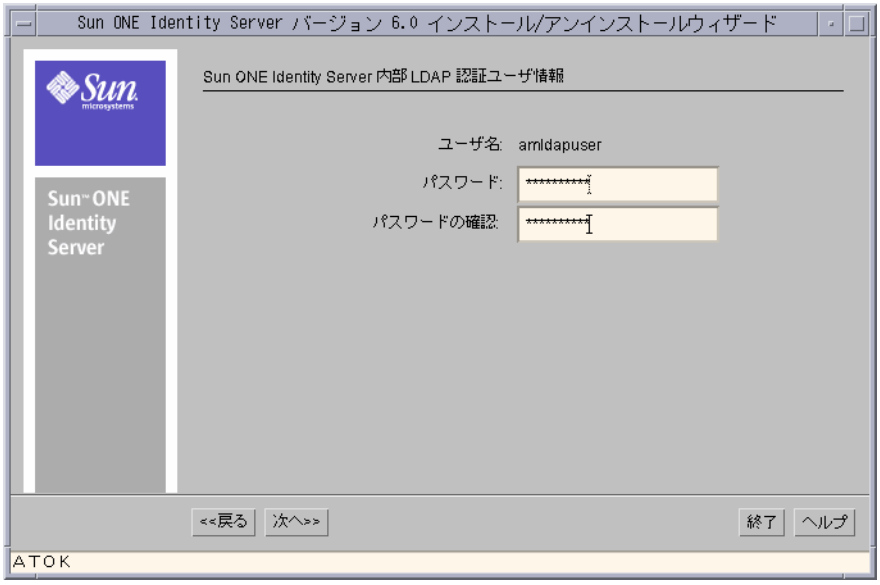
組織のネーミング属性 : 既存の DIT の組織を定義するために使用するネーミング属性を入力します。DIT が `o=organization` を使用している場合は、フィールドに表示されるデフォルトの値を使用することができます。

ユーザのマーカオブジェクトクラス : DIT のユーザ用に定義されたオブジェクトクラスを入力します。

ユーザのネーミング属性 : 既存の DIT のユーザを定義するために使用するネーミング属性を入力します。DIT が `uid` を使用していない場合は、フィールドに表示されるデフォルト値を上書きできます。

18. 「次へ」をクリックし、「Sun ONE Identity Server 内部 LDAP 認証ユーザ情報」パネルで、次の情報を入力して amldap ユーザを作成します。

図 5-13 「Sun ONE Identity Server 内部 LDAP 認証ユーザ情報」パネル



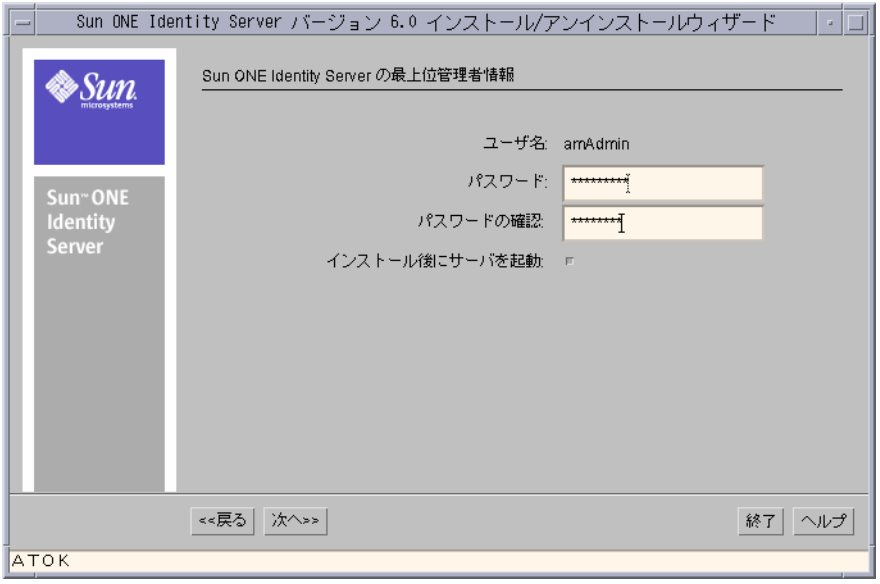
ユーザ名 : これは、LDAP、メンバーシップ、およびポリシーサービスのバインド DN ユーザです。ユーザ名は、*amldapuser* としてハードコードされ変更できません。このユーザは、読み取り権を持ち、Directory Server エントリを検索できます。

パスワード : *amldap* ユーザのパスワードを入力します。このパスワードは一意のもので、次のパネルで入力する最上位管理者のパスワードとは異なっている必要があります。このパスワードは、Identity Server とエージェント間の共有シークレットになります。

パスワードの確認 : 確認のためにもう一度パスワードを入力します。

19. 「次へ」をクリックし、「Sun ONE Identity Server の最上位管理者」パネルで次の情報を入力します。

図 5-14　「Sun ONE Identity Server の最上位管理者」パネル



ユーザ名：スーパー管理者のユーザ名は amAdmin です。最上位管理者には、Identity Server が管理するすべてのエントリに対して無制限のアクセス権があります。ユーザ名は、amAdmin としてハードコードされています。これにより、Identity Server 管理者ロールとその権限が作成され、適切に Directory Server に割り当てられるので、インストール直後に Identity Server にログインできます。これは管理者ロールなので、インストール後にほかのユーザをこのロールに追加できます。

パスワード：amAdmin ユーザのパスワードを入力します。パスワードの指定には 8 文字以上必要です。

パスワードの確認：確認のため、amAdmin パスワードを再度入力します。

インストール後にサーバを起動：インストール後に Identity Server を自動的に起動する場合は、このオプションをクリックします。このオプションを選択しない場合は、インストール後に手動でサーバを起動できます。この実行手順については、118 ページの「Identity Server の起動」を参照してください。

20. 「次へ」をクリックし、「現在選択されている設定」パネルで、これまでのパネルで選択した項目を確認します。任意のパネルを再表示するには、「戻る」をクリックして必要なパネルに移動します。

21. 「次へ」をクリックし、「インストールの準備完了」パネルで、Identity Server を使用してインストールしたコンポーネントを表示します。

22. 「今すぐインストール」をクリックしてインストールを開始します。インストールの終了時に、「インストールの要約」パネルで、製品が正常にインストールされたかどうかが表示されます。このパネルで、「取消し」ボタンをクリックして、製品がインストールされた場所を確認します。詳細を確認したら、「インストールの要約」パネルで「閉じる」をクリックして、インストールプログラムを終了します。

コマンド行からのインストール

1. 製品 CD から Identity Server をインストールする場合は、ソフトウェアをインストールするシステムのドライブに製品 CD を挿入します。

   製品をダウンロードした場合は、次のコマンドを使って製品バイナリファイルを解凍します。

   ```
   gunzip -dc binaryfile.tar.gz | tar -xvof -
   ```

2. `setup` プログラムを実行します。このプログラムは、製品 CD の `/cdrom/Identity Server_60` ディレクトリにあります。製品バイナリをダウンロードした場合、このプログラムはバイナリファイルを展開したディレクトリにあります。

   コマンド行から `./setup -nodisplay` と入力します。

   Windows の場合は、次のコマンドを使用します。

   ```
   java am -nodisplay
   ```

3. 画面に表示される手順を確認します。インストーラが示すさまざまなプロンプトに対する応答方法の説明が表示されます。手順を確認したら、Enter を押してソフトウェアライセンス契約を確認します。インストールのどの段階でも、`<` を入力して前のプロンプトに戻ることができます。また、`!` を入力してインストールプログラムを終了することができます。

4. ライセンス契約を確認し、`yes` と入力してライセンス契約に同意します。

5. 次のプロンプトで、1 を入力し Enter を押して、「Sun ONE Identity Server 管理サービスとポリシーサービス」を選択します。

```
インストールするコンポーネントを次の中から選択してください。インストールする
コンポーネントの番号を入力し、ENTER キーを押してください
1. Sun ONE Identity Server 管理サービスとポリシーサービス
2. Sun ONE Identity Server 管理コンソールのみ
3. Sun ONE Identity Server ドメイン間シングルサインオン
4. 連合管理用の共通ドメインサービス
コンポーネントを選択し ENTER キーを押します [1] {"<" 戻る , "!" 終了 }
```

6. 次のプロンプトで、使用する Java SDK を指定します。Identity Server がサポートする Java には、JDK バージョン 1.3.1_06 が必要です。

```
Java 設定
Sun ONE Identity Server が使用する JDK について次の情報を提供してください。
カスタム JDK を使用しますか：
すでにマシンに JDK がインストールされていて､JDK のバージョンが 1.3.1_06 の場合は、yes を選択してください
JDK がまだインストールされていない場合、または JDK のバージョンが 1.3.1_06 でない場合は、no を選択してください
JDK パス：
既存の JDK の完全なパスを入力してください。
カスタム JDK を使用しますか [n] {"<" 戻る , "!" 終了 }
```

7. このインストールプログラムに付属する JDK 1.3.1_06 を使用する場合は、Enter を押します。ただし、既存の JDK (バージョン 1.3.1_06) を使用することもできます。この場合は、y を入力し、その JDK へのパスを入力します。
8. 次のプロンプトの情報を入力して Sun ONE Web Server をインストールし、設定します。

```
Sun ONE Web Server 情報
管理者 [admin] {"<" 戻る , "!" 終了 }:
ポート [58888] {"<" 戻る , "!" 終了 }:
パスワード：
パスワードの確認：
サーバを実行するユーザ [nobody] {"<" 戻る , "!" 終了 }:
サーバを実行するグループ [nobody] {"<" 戻る , "!" 終了 }:
```

管理者 [admin]: Sun ONE Web Server のサーバ管理者としてのユーザ名を入力します。Enter を押して、デフォルトのユーザ ID (admin) を選択します。

ポート [58888]: Identity Server サービスを実行する Web Server のポート番号を入力します。デフォルトのポート番号は 58088 です。デフォルトのポート番号を選択する場合は Enter を押します。

パスワード : Web Server 管理者のパスワードを入力します。パスワードの指定には 8 文字以上必要です。

パスワードの確認 : 確認のためにもう一度パスワードを入力します。

サーバを実行するユーザ [nobody]: Web Server を実行するユーザアカウントを入力します。Enter を押して、デフォルトユーザ nobody を選択します。Windows 2000 にインストールする場合、このプロンプトは表示されません。

サーバを実行するグループ [nobody]: 上述したユーザが属するグループを入力します。例 : nobody など。Windows 2000 にインストールする場合、このプロンプトは表示されません。

9. 次の情報を指定して、Sun ONE Identity Server サービスを実行する Web Server をインストールし、設定します。

```
Sun ONE Identity Server サービスを実行する Web Server
ホスト [nila.Siroe.COM] {"<" 戻る , "!" 終了 }:
ポート [58080] {"<" 戻る , "!" 終了 }:
サービス配備 URI [amserver] {"<" 戻る , "!" 終了 }:
共通ドメイン配備 URI [common] {"<" 戻る , "!" 終了 }:
サービスと一緒にコンソールをインストールする [yes] {"<" 戻る , "!" 終了 }
コンソール配備 URI [amconsole] {"<" 戻る , "!" 終了 }:
```

ホスト [nila.Siroe.COM]: Web Server を実行するコンピュータの完全指定のドメイン名を入力します。デフォルトの名前を使用するには、Enter を押します。

ポート [58080]: Web Server が使用するポート番号を入力します。

サービス配備 URI [/amserver]: Web Server は、URI (Universal Resource Identifier) 接頭辞の指定に従って、サービスに関連付けられた HTML ページや Web アプリケーション固有の情報 (クラス、jar などに関する情報) を検索します。

デフォルトの URI 接頭辞は amserver です。Enter を押してデフォルトの接頭辞を受け入れるか、あるいは別の名前を入力できます。

共通ドメイン配備 URI: Web Server の共通ドメインサービスにアクセスする URI です。デフォルトの URI は common です。必要に応じて変更可能です。

サービスと一緒にコンソールをインストールする [yes]: サービスとともにコンソールを配備する場合は、Enter を押します。既存の Identity Server コンソールを使用している場合は、「いいえ」を入力します。この場合、次のプロンプトで Identity Server コンソールに関する情報を入力する必要があります。

コンソール配備 URI [amconsole]: Web Server は、URI (Universal Resource Identifier) 接頭辞の指定に従って、Identity Server 管理コンソールに関連付けられた HTML ページや、その他の Web アプリケーション固有の情報 (クラス、jar などに関する情報) を検索します。デフォルトの URI 接頭辞は amconsole です。別の名前を入力することもできます。Identity Server コンソールを配備しないよう選択した場合、このフィールドは使用できません。

10. 前のプロンプトで、Identity Server コンソールを配備しないよう選択した場合は、次のプロンプトで既存の Identity Server コンソールの詳細を指定する必要があります。

```
Sun ONE Identity Server Console を実行する Web Server
   ホスト [nila.Siroe.COM] {"<" 戻る , "!" 終了 }:
   ポート [58080] {"<" 戻る , "!" 終了 }:
   コンソール配備 URI [amconsole] {"<" 戻る , "!" 終了 }:
```

コンソール配備 URI [amconsole]: Web Server は、URI (Universal Resource Identifier) 接頭辞の指定に従って、Identity Server 管理コンソールに関連付けられた HTML ページや、その他の Web アプリケーション固有の情報 (クラス、jar などに関する情報) を検索します。デフォルトの URI 接頭辞は `amconsole` です。別の名前を入力することもできます。

11. 次のプロンプトで、インストールプログラムに付属する Sun ONE Directory Server 5.1 をインストールするか、または Identity Server が既存のバージョンの Directory Server を使用するかを指定します。

```
ディレクトリスキーマ
1. 新規 Sun ONE Directory Server をインストール
2. 既存の DIT なしで既存の Sun ONE Directory Server を使用
3. 既存の DIT とともに既存の Sun ONE Directory Server を使用
上のオプションの 1 つを選択してください [1] {"<" 戻る , "!" 終了 }
```

12. DIT を使用しない既存のサーバを使用する場合、2 を入力します。DIT を使用する既存の Directory Server を選択するには、3 を入力します。

13. 次のプロンプトで、情報を入力して DIT 設定します。

```
ディレクトリのルートの接尾辞
ディレクトリツリー内の Sun ONE Identity Server ルート
[dc=Siroe,dc=COM] {"<" 戻る , "!" 終了 }:
```

ディレクトリツリー内の Sun ONE Identity Server ルート [dc=Siroe,dc=COM]: ルート接尾辞として設定する識別名 (DN) を入力します。識別名 (DN) には、最低 1 個の type=value ペアが必要です。たとえば、`o=isp;o=madisonparc;dc=Siroe,dc=COM` のようになります。

14. 次のプロンプトで、Sun ONE Directory Server の情報を入力します。

```
Sun ONE Directory Server 情報
ホスト [nila.Siroe.COM] {"<" 戻る , "!" 終了 }:
ポート [389] {"<" 戻る , "!" 終了 }:
ディレクトリマネージャ [cn=Directory Manager] {"<" 戻る , "!" 終了}:
パスワード :
```

ホスト [nila.Siroe.COM]: Directory Server をインストールしたコンピュータの完全指定のドメイン名を入力します。通常、Directory Server は Identity Server とは異なるホストにインストールされます。

ポート [389]: Directory Server が使用しているポート番号です。

ディレクトリマネージャ [cn=Directory Manager]: Directory Server 管理ユーザ、つまりディレクトリマネージャは、Directory Server のデータおよび設定に対して無制限のアクセス権を持つ管理者です。ディレクトリマネージャのデフォルト DN は、`cn=Directory Manager` です。

パスワード : Directory Server 管理者のパスワードを入力します。パスワードの指定には 8 文字以上必要です。

15. 次のプロンプトで、Identity Server 6.0 に準拠する DIT をインストールするかどうかを指定します。

```
この Directory Server には 6.0 準拠の DIT がありません。インストーラ
で DIT を Directory Server 内にロードしますか ?
1. はい
2. いいえ
   該当する番号を入力してください  [1] {"<" 戻る , "!" 終了 }
```

この Directory Server には 6.0 準拠の DIT がありません。インストーラで、Directory Server に DIT をロードしますか ?:「はい」を選択すると、Directory Server に 6.0 準拠 DIT およびスキーマ (`ldif` と `xml`) ファイルが自動的にロードされます。「いいえ」を選択すると、インストール後に手動でファイルをロードすることができます。

16. 次のプロンプトで、既存の DIT およびスキーマの情報を入力します。

```
既存の DIT およびスキーマ情報
組織のマーカオブジェクトクラス [organization] {"<" 戻る , "!" 終了 }:
組織のネーミング属性 [o] {"<" 戻る , "!" 終了 }:
ユーザのマーカオブジェクトクラス [inetorgperson] {"<" 戻る , "!" 終了 }:
ユーザのネーミング属性 [uid] {"<" 戻る , "!" 終了 }:
```

組織のマーカオブジェクトクラス : 既存の DIT の組織用に定義されたオブジェクトクラスを入力します。

組織のネーミング属性 : 既存の DIT の組織を定義するために使用するネーミング属性を入力します。DIT が o=*organization* を使用している場合は、フィールドに表示されるデフォルトの値を使用することができます。

ユーザのマーカオブジェクトクラス : DIT のユーザ用に定義されたオブジェクトクラスを入力します。

ユーザのネーミング属性 : 既存の DIT のユーザを定義するために使用するネーミング属性を入力します。DIT が `uid` を使用していない場合は、フィールドに表示されるデフォルト値を上書きできます。

17. 次のプロンプトで、Sun ONE Identity Server 内部 LDAP 認証ユーザのインストールおよび設定に関する情報を入力します。

```
Sun ONE Identity Server 内部 LDAP 認証ユーザ情報
ユーザ名 : amldapuser
パスワード :
パスワードの確認 :
```

ユーザ名 : これは、LDAP、メンバーシップ、およびポリシーサービスのバインド DN ユーザです。ユーザ名は、*amldapuser* としてハードコードされ変更できません。このユーザは、読み取り権を持ち、Directory Server エントリを検索できます。

パスワード : *amldap* ユーザのパスワードを入力します。このパスワードは一意のもので、次のパネルで入力する最上位管理者のパスワードとは異なっている必要があります。このパスワードは、Identity Server とエージェント間の共有シークレットになります。

パスワードの確認 : 確認のためにもう一度パスワードを入力します。

18. 次のプロンプトで、Sun ONE Identity Server 最上位管理者に関する詳細情報を入力します。

```
Sun ONE Identity Server の最上位管理者情報
ユーザ名 :amAdmin
    パスワード :
    パスワードの確認 :
    インストール後にサーバを起動 [yes] {"<" 戻る , "!" 終了 }:
```

ユーザ名：スーパー管理者のユーザ名は amAdmin です。最上位管理者には、Identity Server が管理するすべてのエントリに対して無制限のアクセス権があります。ユーザ名は、amAdmin としてハードコードされています。これにより、Identity Server 管理者ロールとその権限が作成され、適切に Directory Server に割り当てられるので、インストール直後に Identity Server にログインできます。これは管理者ロールなので、インストール後にほかのユーザをこのロールに追加できます。

パスワード：amAdmin ユーザのパスワードを入力します。パスワードの指定には 8 文字以上必要です。

パスワードの確認：確認のため、amAdmin パスワードを再度入力します。

インストール後にサーバを起動：インストール後 Identity Server サーバを自動的に起動するには、Enter を押します。あるいは、no を入力し、後でサーバを手動で起動することができます。手順については、118 ページの「Identity Server の起動」を参照してください。

インストールプログラムは、これまでのプロンプトで選択した設定を表示し、次に Identity Server でインストールするコンポーネントの一覧を表示します。

```
現在選択されている設定
Sun ONE Identity Server コンソール : http://nila.Siroe.COM:58080
コンソール配備 URI:/amconsole
Sun ONE Identity Server サービス : http://nila.Siroe.COM:58080
サービス配備 URI:/amserver
共通ドメイン配備 URI:/common
Sun ONE Identity Server インストールディレクトリ :
/is6install/dsame-20020925.2/opt
管理者 : admin
ポート : 58888
ディレクトリサーバ : nila.Siroe.COM:389
ディレクトリマネージャ :cn=Directory Manager
既存の DIT を使用 :  true
組織のネーミング属性 :o
組織のマーカオブジェクトクラス :organization
ユーザのネーミング属性 :uid
ユーザのマーカオブジェクトクラス :inetorgperson
Sun ONE Identity Server ルート : dc=siroe,dc=COM
```

19. 次のプロンプトで、1 を入力してインストールを開始します。

```
次のコンポーネントがインストールされます :
プロダクト : Sun ONE Identity Server
場所 : /opt
サイズ :139.22MB
---------------------------------
JDK
Sun ONE Web Server
その他のパッケージ
Sun ONE Identity Server 管理サービスとポリシーサービス
Sun ONE Identity Server 管理コンソール
共通ドメインサービス
インストールの準備完了
1. 今すぐインストール
2. 開始
3. 終了
   上のオプションを 1 つ選択してください [1] {"<" 戻る , "!" 終了 }
```

20. コピーしたファイルなどインストールの詳細を表示するには、次のプロンプトで 1 を入力します。

```
インストール中 Sun ONE Identity Server
|-1%--------------25%-----------------50%-----------------75%---
-----------100%|

インストールの要約
インストールの要約      要約の結果   詳細
1.  Sun ONE Identity Server インストールされました        ログを表示する
には 1、終了するには 2 を入力してください。
終了
オプションを 1 つ選択してください [2] {"!" 終了 }
```

21. 2 を入力してインストールプログラムを終了します。

カスタムのオブジェクトクラスの Identity Server スキーマへの追加 (オプション)

ユーザが作成した、Directory Server に付属していないオブジェクトクラスが既存の DIT にある場合は、それらのオブジェクトクラスおよび属性を Identity Server スキーマに追加する必要があります。基本情報については、『Programmer's Guide』の「Identity Server XMLs and DTDs」を参照してください。

DIT でカスタムのオブジェクトクラスを使わない場合は、この手順は不要です。114 ページの「Identity Server LDIF のディレクトリへの読み込み」に進んでください。

この節の例では、Madison Park という会社が Identity Server スキーマに付属していない 2 つのオブジェクトクラスを使用します。AUXILIARY オブジェクトクラス `madisonparc-org` はすべての組織エントリに存在し、AUXILIARY オブジェクトクラス `madisonparc-user` はすべてのユーザエントリに存在します。

コード例 5-1 madisonparc のカスタマイズされたスキーマ

```
dn:cn=schema
attributeTypes:( madisonparc-org-description-oid NAME
'madisonparc-org-description' DESC 'org description'
SYNTAX 1.3.6.1.1466.115.121.1.15
SINGLE-VALUE X-ORIGIN 'madisonparc'
attributeTypes:( madisonparc-org-city-oid NAME
'madisonparc-org-city' DESC 'org city location'
SYNTAX 1.3.6.1.4.1.1666.115.121.1.15
SINGLE-VALUE X-ORIGIN 'madisonparc' )
attributeTypes:( madisonparc-user-id-oid NAME
'madisonparc-user-id' DESC 'user madisonparc id'
SYNTAX 1.3.6.1.4.1.1666.115.121.1.15
SINGLE-VALUE X-ORIGIN 'madisonparc' )
attributeTypes:( madisonparc-user-building-oid NAME
'madisonparc-user-building' DESC 'priority of a service
with respect to its siblings'
SYNTAX 1.3.6.1.4.1.1666.115.121.1.15
SINGLE-VALUE X-ORIGIN 'madisonparc' )
objectClasses:( madisonparc-org-oid NAME
'madisonparc-org' DESC 'custom attributes
for madisonparc org' SUP top MUST
(madisonparc-org-description $ madisonparc-org-city )
X-ORIGIN 'madisonparc' )
objectClasses:( madisonparc-user-oid NAME
'madisonparc-user' DESC 'custom attributes
for madisonparc user' SUP top MUST
( madisonparc-user-id $ madisonparc-user-building )
X-ORIGIN 'madisonparc' )
```

これらの拡張を管理するには、次の 3 つのファイルを変更する必要があります。

- `amEntrySpecific.xml` (組織データ用)
- `amUser.xml` (ユーザデータ用)
- `ums.xml`

組織スキーマへの属性の追加

組織スキーマに属性を追加するには、2 つのサービスファイルを変更する必要があります。

- `amEntrySpecific.xml`
- `amEntrySpecific.properties`

Identity Server コンソールは、表示のために `amEntrySpecific.xml` 内の情報を使用します。各 Identity Server 抽象エントリは、この XML ファイル内にサブスキーマを持つことがあります。次の例では、2 つの属性を `madisonparc-org` オブジェクトクラスから組織サブスキーマに追加します。カスタマイズされた組織単位、グループ、またはピープルコンテナが DIT に含まれる場合は、同じ XML ファイルのそれらのサブスキーマを追加または変更します。

組織単位のサブスキーマ名は `OrganizationalUnit` です。ピープルコンテナのサブスキーマ名は `PeopleContainer` です。

注 User サブスキーマは、`amEntrySpecific.xml` ファイルではなく、`amuser.xml` ファイル (106 ページの「ユーザスキーマへの属性の追加」を参照) で設定されます。どのサービス XML ファイルでもユーザ専用の属性を記述できますが、`amentryspecific.xml` ファイルは、特定のサービスに結び付けられていないユーザ属性のデフォルトの可変部分として機能します。

属性をカスタムの組織から Organization サブスキーマに追加するには

注 XML では、属性名はすべて小文字にする必要があります。Identity Server では、属性名を Directory Server から取得するときに、すべての名前を小文字に変換します。

1. 次のファイルで、属性をカスタムのオブジェクトクラスからサブスキーマ Organization に追加します。

   `IS_root/SUNWam/config/xml/amEntrySpecific.xml`

   Windows の場合、このファイルへのパスは次のとおりです。

   `IS_root¥config¥xml¥amEntrySpecific.xml`

   たとえば、次の 2 つの属性がカスタムのオブジェクトクラス `madisonparc-org` からファイルに追加されています。

```
<AttributeSchema name="madisonparc-org-description"
    type="single"
    syntax="string"
    any="required"
/>
<AttributeSchema name="madisonparc-org-city"
    type="single"
    syntax="string"
    any="required|filter"
/>
```

2. また、amEntrySpecific.xml ファイルで、各属性に対して国際化 (i18n) キー (インデックスキーまたは地域対応化キーとも呼ばれる) を作成します。組織内のすべての i18n キーは、一意の文字列で構成する必要があります。Identity Server 管理コンソールでは、このキーを使って属性の表示名を検索します。

```
<AttributeSchema name="madisonparc-org-description"
    type="single"
    syntax="string"
    any="required"
    i18nKey="o3"
/>
<AttributeSchema name="madisonparc-org-city"
    type="single"
    syntax="string"
    any="required|filter"
    i18nKey="o4"
/>
```

3. 次のファイルでは、手順 2 で作成した i18n キーの値を追加します。

   IS_root/SUNWam/locale/amEntrySpecific.properties

   Windows の場合、このファイルの場所は次のとおりです。

   IS_root¥locale¥amEntrySpecific.properties

```
iplanet-am-entry-specific-service-description=Identity Server
Entry Specific
g1=Member List
g2=Users Can Subscribe to this Group
dg1=Membership Filter
r1=Membership Filter
o1=Full DNS name
o2=Organization Status
o3=Org Description
o4=Organization Location
```

組織が表示されるときに、サブスキーマに含まれているすべての属性が管理コンソールに表示されます。サブスキーマに含まれていない属性は管理コンソールに表示されません。

ヒント 属性に i18n キーがない場合、その属性は管理コンソールに表示されません。属性を追加してもその属性が管理コンソールに表示されない場合は、i18n キーおよびプロパティを確認してください。

any 属性

XML 記述内の any 属性は、`filter`、`display`、`adminDisplay`、`userReadOnly`、`required`、`optional` の 5 つの値のいずれかをとることができます。これらの値は、この属性を GUI に表示する必要があるかどうかを管理コンソールに指示します。通常、`required` と `optional` の両方が同時に表示されることはありません。この 2 つは相互に排他的です。

filter: この属性は、「検索」ページに表示されます。

display: この属性は、管理者と一般ユーザに対して読み取りと書き込みを許可します。

adminDisplay: この属性は、管理者の読み取り / 書き込み用であり、通常のユーザ用には表示されません。

userReadOnly: この属性は、管理者の読み取り / 書き込み用ですが、通常のユーザには読み取り専用です。この属性は、編集できないように、通常のユーザにはラベルとして表示されます。たとえば、`display`、`adminDisplay`、`userReadOnly` の設定は、ユーザプロファイルページを表示するときに使用され、ページをカスタマイズするために使用できます。

required: この属性は作成ページに表示されます。エントリの作成時に値を必要とします。any=required の場合、この属性には値が必要です。値がないと、コンソールが作成処理を許可しません。空白文字列 (" ") を使って、何も表示しないよう管理コンソールに指示できます。

optional: この属性は作成ページに表示されますが、エントリの作成時に値は不要です。any=optional の場合、属性はアスタリスクなしで「作成」ページに表示されます。これは、エントリを作成するのに値を指定する必要がないことを示します。「Create User (新規ユーザ)」ページでは、UserID (ユーザ ID) は必須属性ですが First Name (名前) はオプションです。

次の例では、両方の属性が「組織」ページに表示され、両方とも作成に必要です。このことは、required 値の使用によって示されています。filter 値の使用が示すように、Identity Server コンソールの「検索」ページでは madisonparc-org-city 属性だけが使用されます。

```
<AttributeSchema name="madisonparc-org-description"
    type="single"
    syntax="string"
    any="required"
    i18nKey="o3"
/>
<AttributeSchema name="madisonparc-org-city"
    type="single"
    syntax="string"
    any=required|filter
    i18nKey="o4"
/>
```

type 属性

type 属性には、文字列、文字列リスト、単一選択肢、複数選択肢、またはブール値を使用できます。たとえば、madisonparc-org-city 属性に Concord、San Francisco、または Palo Alto のどれか 1 つの都市だけを有効な値として指定できる場合は、この属性を単一選択肢にすることができ、各都市は選択肢の 1 つになります。Identity Server コンソールには、それらの都市だけを含む一覧が表示されます。複数の都市が許可される場合、属性は複数選択肢になります。

ユーザスキーマへの属性の追加

この手順では、サービス用に次の 2 つのファイルを変更します。

- `amUser.xml`
- `amUser.properties`

組織およびグループのスキーマが `amEntrySpecific.xml` に記述されているように、`amUser.xml` ファイルにはユーザ属性が記述されています (手順 2 を参照)。ファイル `amUser.xml` には、Identity Server のユーザサービスが記述されています。どのサービスでも、ユーザ専用の属性を記述できます。このファイルは、特定のサービスに結び付けられていない `user` 属性のためのデフォルトの可変部分です。

ユーザの属性を表示するときは、Identity Server 管理コンソールはサブスキーマタイプが `User` であるすべてのサービスからすべての属性を取得し、`amEntrySpecific.xml` ファイルで使われているのと同じ値を使ってそれらの属性を表示します (104 ページの「any 属性」および 105 ページの「type 属性」を参照)。次の例では、いくつかの属性が `madisonparc-user` オブジェクトクラスからファイルに追加されるので、新しいサービスを作成する必要はありません。`iplanetamuserservice` サービスを変更または拡張するだけですみます。

amUser.xml ファイルに関する追加情報

ファイル `amUser.xml` には、特別な属性が含まれています。`any=display` 属性は、この属性をユーザプロファイルページに表示するかどうかを Identity Server に指示します。これは、アクセス制御を暗に示すので、誤解を与えやすい名前です。これは表示だけに使用されます。この属性が `no` に設定されている場合、コンソールにはこの属性は表示されません。

また、属性は、サブスキーマ `Dynamic` ではなく `User` の下に定義されます。`User` の下に定義される属性は、物理的にユーザエントリの属性です。属性をロールベースまたは組織ベースの属性にする場合は、属性を `Dynamic` サブスキーマの下に定義します。基本情報については、『Programmer's Guide』の「Identity Server XMLs and DTDs」を参照してください。

たとえば、`madison-user-building` 属性を Dynamic にして、Identity Server でこの属性を使ってロールを作成することができます。このようにすると、ある部門のすべての社員が別の建物に移動した場合、すべての個々のユーザエントリを変更する必要はなく、そのロール属性を変更するだけですみます。

属性をカスタムの組織から User サブスキーマに追加するには

1. 次のファイルでは、カスタムのオブジェクトクラスから User サブスキーマに属性を追加します。

   IS_root/SUNWam/config/xml/amUser.xml

   Windows の場合、このファイルは次の場所にあります。

   IS_root¥config¥xml¥amUser.xml

2. たとえば、次の 2 つの属性がカスタムのオブジェクトクラス madisonparc-user からファイルに追加されています。

```
<AttributeSchema name="madisonparc-user_id"
    type=single
    syntax=string
    any=required|display
    i18nKey=u13
/>
<AttributeSchema name="madisonparc-user-building"
    type=single
    syntax=string
    any=required|filter|display
    i18nKey=u14
```

3. amUser.xml ファイルで、各属性に対して i18n キー (インデックスキーまたは地域対応化キーとも呼ばれる) を作成します。組織内のすべての i18n キーは、一意の文字列で構成する必要があります。Identity Server コンソールでは、このキーを使って属性の表示名を検索します。上述した例を参照してください。

4. 前の手順で作成した i18n キーの値を次のファイルに追加します。
   IS_root/SUNWam/locale/amUser.properties

   Windows の場合、このファイルは次の場所にあります。

   IS_root¥locale¥amUser.properties

   次に例を示します。

```
iplanet-am-user-service-description=Identity Server User
iwtUser-desc=Default User Profile
u1=User Name
u2=First Name
u3=Last Name
u4=Full Name
u5=Password
u6=Email Address
u7=Employee Number
u8=Telephone Number
u9=Manager
u10=Home Address
u11=User Status
u12=User Auth Modules
u13=User Id
u14=Employee Building
```

この値は、管理コンソールページに表示されるフィールドそのものです。このキーは、ロケールに応じてローカライズされます。この例では、管理コンソールには、テキストフィールド「User Id」と「Employee Building」が表示されます。

作成テンプレートの変更

この手順では、ums.xml ファイルを変更します。

120 ページの図 5-16 の DIT の例では、ユーザと組織の両方に新しいオブジェクトクラスがあります。UI にそれらの新しいオブジェクトクラスを表示するには、ums.xml ファイル内のユーザと組織の両方の作成テンプレートを変更します。作成テンプレートは、エントリの作成時に特定のオブジェクトクラスを追加または許可するように Identity Server を設定します。

作成テンプレートを変更するには

1. ファイル IS_root/SUNWam/config/ums/ums.xml で次の変更を行います。

   Windows の場合、このファイルは次の場所にあります。

   IS_root¥config¥ums¥ums.xml

2. <SubConfiguration name="BasicOrganization" id="CreationUmsObjects"> の下の <AttributeValuePair> <Attribute name="required" /> 要素に、次の行を追加します。

   <Value>objectClass=madisonparc-org</Value>

   次に例を示します。

```
<SubConfiguration name="BasicOrganization" id="CreationUmsObjects">

<AttributeValuePair> <Attribute name="name" />
<Value>BasicOrganization</Value>
</AttributeValuePair>
<AttributeValuePair> <Attribute name="javaclass" />
<Value>com.iplanet.ums.Organization</Value>
</AttributeValuePair>
<AttributeValuePair> <Attribute name="required" />
<Value>objectClass=top</Value>
<Value>objectClass=organization</Value>
<Value>objectClass=nsManagedDomain</Value>
<Value>objectClass=inetDomain</Value>
<Value>objectClass=iplanet-am-managed-org</Value>
<Value>objectClass=madisonparc-org</Value>
<Value>o</Value>
<Value>inetdomainstatus=Active</Value>
</AttributeValuePair>
```

3. <SubConfiguration name="BasicUser" id="CreationUmsObjects"> の下の <AttributeValuePair><Attribute name="optional" /> 要素に、次の行を追加します。

   <Value>objectClass=madisonparc-user</Value>

次に例を示します。(続き)

```
<SubConfiguration name="CreationTemplates" >
<SubConfiguration name="BasicUser" id="CreationUmsObjects">
<AttributeValuePair> <Attribute name="name" />
<Value>BasicUser</Value>
</AttributeValuePair>
<AttributeValuePair> <Attribute name="javaclass" />
<Value>com.iplanet.ums.User</Value>
</AttributeValuePair>
<AttributeValuePair> <Attribute name="required" />
<Value>objectClass=top</Value>
<Value>objectClass=person</Value>
<Value>objectClass=organizationalPerson</Value>
<Value>objectClass=inetOrgPerson</Value>
<Value>objectClass=iPlanetPreferences</Value>
<Value>objectClass=iplanet-am-user-service</Value>
<Value>objectClass=inetuser</Value>
<Value>objectClass=iplanet-am-managed-person</Value>
<Value>objectClass=madisonparc-user</Value>
<Value>cn=default</Value>
<Value>sn=default</Value>
<Value>uid</Value>
<Value>inetuserstatus=Active</Value>
</AttributeValuePair>
```

4. `<SubConfiguration name="BasicOrganization" id="CreationUmsObjects">` の下の `<AttributeValuePair> <Attribute name="optional" />` 要素に、次の行を追加します。

   ```
   <Value>madisonparc-org-description</Value>
   ```

   ```
   <Value>madisonparc-org-city</Value>
   ```

   次に例を示します。

```
<SubConfiguration name="BasicOrganization" id="CreationUmsObjects">
<AttributeValuePair> <Attribute name="name" />
<Value>BasicOrganization</Value>
</AttributeValuePair>
<AttributeValuePair> <Attribute name="javaclass" />
<Value>com.iplanet.ums.Organization</Value>
</AttributeValuePair>
<AttributeValuePair> <Attribute name="required" />
<Value>objectClass=top</Value>
<Value>objectClass=organization</Value>
<Value>objectClass=nsManagedDomain</Value>
<Value>objectClass=inetDomain</Value>
<Value>objectClass=iplanet-am-managed-org</Value>
<Value>objectClass=madisonparc-org</Value>
<Value>o</Value>
<Value>inetdomainstatus=Active</Value>
</AttributeValuePair>
<AttributeValuePair> <Attribute name="namingattribute" />
<Value>o</Value>
</AttributeValuePair>
<AttributeValuePair> <Attribute name="optional" />
<Value>*</Value>
<Value>madisonparc-org-description</Value>
<Value>madisonparc-org-city</Value>
</AttributeValuePair>
```

5. `<SubConfiguration name="BasicUser" id="CreationUmsObjects">` の下の `<AttributeValuePair> <Attribute name="optional" />` 要素に、次の行を追加します。

   ```
   <Value>madisonparc-user-id</Value>
   ```

   ```
   <Value>madisonparc-user-building</Value>
   ```

```
<SubConfiguration name="CreationTemplates" >
<SubConfiguration name="BasicUser" id="CreationUmsObjects">
<AttributeValuePair> <Attribute name="name" />
<Value>BasicUser</Value>
</AttributeValuePair>
<AttributeValuePair> <Attribute name="javaclass" />
<Value>com.iplanet.ums.User</Value>
</AttributeValuePair>
<AttributeValuePair> <Attribute name="required" />
<Value>objectClass=top</Value>
<Value>objectClass=person</Value>
<Value>objectClass=organizationalPerson</Value>
<Value>objectClass=inetOrgPerson</Value>
<Value>objectClass=iPlanetPreferences</Value>
<Value>objectClass=iplanet-am-user-service</Value>
<Value>objectClass=inetuser</Value>
<Value>objectClass=iplanet-am-managed-person</Value>
<Value>objectClass=madisonparc-user</Value>
<Value>cn=default</Value>
<Value>sn=default</Value>
<Value>uid</Value>
<Value>inetuserstatus=Active</Value>
</AttributeValuePair>
<AttributeValuePair> <Attribute name="optional" />
<Value>nsroledn</Value>
<Value>madisonparc-user-id</Value>
<Value>madisonparc-user-building</Value>
<Value>*</Value>
```

代替ネーミング属性の設定 (オプション)

o=*organization* 以外のネーミング属性を使って DIT で組織を定義した場合は、ums.xml ファイルを変更して標準でないネーミング属性に対応させる必要があります。uid=*username* 以外のネーミング属性を使って DIT でユーザを定義した場合は、ums.xml ファイルで同様の変更を行う必要があります。

組織の代替ネーミング属性を設定するには

次の手順では、組織に使用するネーミング属性が dc であることを前提としています。次のファイルで変更を行ないます。

IS_root/SUNWam/config/ums/ums.xml

Windows の場合、このファイルは次の場所にあります。

IS_root¥config¥ums¥ums.xml

1. o=org を dc=org に置き換えます。
2. BasicOrganization セクションで、o の値を dc に置き換えます。
3. BasicOrganizationSearch SubConfiguration セクションで、o の値を dc に置き換えます。
4. BasicOrganization セクションで、organization のオブジェクトクラスを domain に変更します。組織に ou を使う場合は、organizationalUnit に変更する必要があります。

ユーザの代替ネーミング属性を設定するには

次の手順では、ユーザに使用するネーミング属性が cn であることを前提としています。

1. 次のディレクトリで、次のように変更を行います。

   IS_root/SUNWam/config/ums

   IS_root/SUNWam/config/xml

2. Windows の場合は、次のディレクトリで変更を行います。

   IS_root¥config¥ums

   IS_root¥config¥xml

3. ファイル ldif/installExisting.ldif で、2 つの例外を除いて、uid を cn に置き換えます。例外は次のとおりです。

- ACI の下で使う場合
- amAdmin エントリ内の uid: amAdmin 属性

4. xml/amAuth.xml で、uid をユーザネーミング属性の cn に置き換えます。
5. xml/amMembership.xml で、uid をユーザネーミング属性の cn に置き換えます。
6. xml/amAuthLDAP.xml で、uid をユーザネーミング属性の cn に置き換えます。
7. AMConfig.properties で、uid=amAdmin を cn=amAdmin に置き換えます。
8. ums/ums.xml の BasicUser subconfiguration で、uid を namingattribute の cn に置き換えます。
9. ums/ums.xml の BasicUser 必須値で、cn=default を cn に、uid を uid=default に変更します。

Identity Server LDIF のディレクトリへの読み込み

installExisting.ldif ファイルには、インストール時に Directory Server に読み込まれる Identity Server 固有のエントリが含まれています。通常、インストール処理時に読み込む前にこのファイルを変更する必要はありません。

Directory Server に付属の ldapmodify ユーティリティを使用して、installExisting.ldif を読み込むことができます。MadisonParc の例では、LDIF の読み込み時に、次のように行われます。

- Identity Server に必要なユーザおよびマーカーオブジェクトクラスは、o=madisonparc および o=Engineering、o=madisonparc に追加される
- 組織およびヘルプデスク管理者用のデフォルトのロールが作成される
- それらの管理者エントリ用のデフォルトアクセス制御命令 (ACI) が設定される

始める前に

1. 適切なバージョンの ldapmodify を使っていることを確認してください。次の手順に従います。
   - Sun ONE Directory Server 5.1 に付属の ldapmodify コマンドを使うようにパスが設定されていることを確認します。/bin または /usr/bin にある、Solaris に付属のバージョンは使用しないでください。
   - また、Directory Server ライブラリを取り込むために、/usr/iplanet/servers/lib を LD_LIBRARY_PATH に追加する必要があります。コマンド行に次のように入力します。

```
which ldapmodify
```

`Directory_Server_root/shared/bin/ldapmodify` が表示されます。

Windows の場合、`ldapmodify` は Identity Server をインストールした次のディレクトリにあります。

```
IS_root¥tools
```

DOS プロンプトウィンドウを開き、`ldapmodify` ツールのパスを入力します。たとえば次のようになります。

```
set PATH=IS_root¥tools;%PATH%
```

2. Identity Server は、必要な変更を加えるのに役立つ 2 つの異なる LDIF ファイルを提供します。使用するファイルと手順を決めます。
   - Identity Server のデフォルト組織がディレクトリツリーのルート接尾辞の下のレベルにある場合は、「`installExisting.ldif` ファイルを読み込むには」の節の手順を使用します。
   - Identity Server のデフォルト組織のルート接尾辞がピリオド (.) として入力されている場合は、「`install.ldif` ファイルを読み込むには」の節の手順を使用します。

installExisting.ldif ファイルを読み込むには

1. 次のディレクトリに移動します。

   ```
   cd IS_root/SUNWam/web-apps/services/WEB-INF/config/ldif
   ```

   Windows の場合は、次のディレクトリに移動します。

   ```
   cd IS_root¥web-apps¥services¥WEB-INF¥config¥ldif
   ```

2. コマンド行に次のコマンドを入力します。

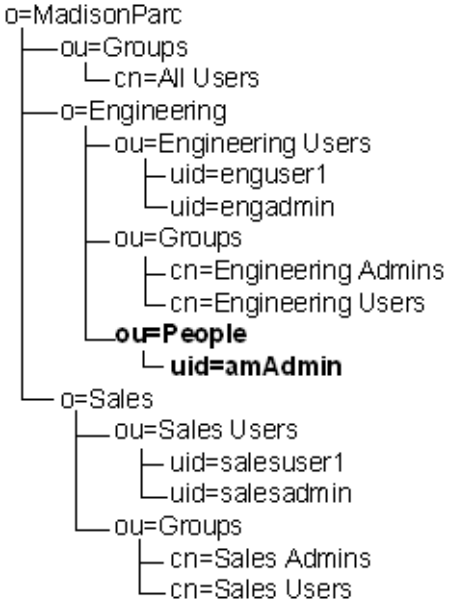
   ```
   ldapmodify -v -c -D "cn=Directory manager" -w password -a -f
   installExisting.ldif
   ```

注 `-c` オプションを指定する必要があります。`installExisting.ldif` だけをインストールし、他のどのファイルも同じディレクトリにインストールしないでください。

デフォルトの組織の「すでに存在している」エントリまたは値に関するエラーメッセージが表示される場合は、118 ページの「Identity Server ACI のデフォルト組織への追加 (オプション)」を参照してください。

Identity Server の管理ユーザ amAdmin が、ou=People,o=Engineering,o=madisonparc ピープルコンテナの下に作成されます。これは、Identity Server の最上位レベルの管理者です。この管理者は、o=madisonparc のサブツリー全体に対する読み取りおよび書き込みアクセス権を持ちます。Identity Server コンソールの起動後に、ユーザの 1 人をこの最上位レベルの管理者ロールに追加できます。

図 5-15　この章の例で使われているディレクトリ情報ツリー (DIT)



install.ldif ファイルを読み込むには

1. 次のディレクトリに移動します。

   ```
   cd IS_root/SUNWam/web-apps/services/WEB-INF/config/ldif
   ```

   Windows の場合は、次のディレクトリに移動します。

   ```
   cd IS_root¥web-apps¥services¥WEB-INF¥config¥ldif
   ```

2. コマンド行に次のコマンドを入力します。

   ```
   ldapmodify -v -c -D "cn=Directory manager" -w password -a -f
   install.ldif
   ```

注 -c オプションを指定する必要があります。install.ldif だけをインストールし、他のどのファイルも同じディレクトリにインストールしないでください。

Identity Server サービス属性のディレクトリへの読み込み

同じコマンドを使って ums.xml ファイルとすべてのサービスファイルを読み込むことができます。

1. 次のディレクトリに移動します。

   cd IS_root/SUNWam/config/ums

   Windows の場合は、次のディレクトリに移動します。

   cd IS_root¥config¥ums

2. 次のコマンドを実行します。

   amadmin *amAdmin_DN password ums.xml*

構文解析エラーが発生した場合は、前の手順で行なった変更をもう一度確認する必要があります。また、amUser.xml ファイルと amEntrySpecific.xml ファイルの構文を調べて、正しい構文を使っていることを確認します。構文の例を参照する場合は、次のディレクトリにあるほかのサービス XML ファイルを参照してください。

IS_root/SUNWam/config/xml （Solaris の場合）

IS_root¥config¥xml （Windows の場合）

Identity Server ACI のデフォルト組織への追加 (オプション)

インストール時に既存の組織をデフォルトの組織として指定した場合だけ、この手順を実行する必要があります。デフォルトでは、Identity Server は DN `o=iplanet` を使って新しい組織を 1 つ作成します。デフォルトの RDN を受け入れた場合は、「Identity Server の起動」の節に進みます。

この手順では、Identity Server のデフォルト ACI をデフォルトの組織、つまり最初の組織として指定した組織に手動で追加します。

1. Identity Server のデフォルト組織の ACI をコピーします。
   - ファイル `installExisting.ldif` を読み込んだ場合は、次のファイルから ACI をコピーします。

     `IS_root/SUNWam/web-apps/services/WEB-INF/config/ldif`
   - ファイル `install.ldif` を読み込んだ場合は、次のファイルから ACI をコピーします。

     `IS_root/SUNWam/web-apps/services/WEB-INF/config/ldif`
2. `ldapmodify` ユーティリティがあるディレクトリで、次のコマンドを入力します。

   `ldapmodify -D bind_DN -w` *password* `-p` *port_number* `-h` *hostname* `-a -f` *textfile_name*

Identity Server の起動

この時点で、Identity Server サーバを起動し、`amAdmin` ユーザとして Identity Server コンソールにログインできます。インストール時に指定したルート接尾辞と組織が表示されます。MadisonParc の例では、`o=madisonparc` と `o=Engineering` が表示されます。残りのエントリにはまだ Identity Server マーカーオブジェクトクラスが含まれていないので、それらのエントリは表示されません。

Solaris で Identity Server を起動するには

Identity Server を手動で起動するには、コマンド行に次のコマンドを入力します。

```
/IS_root/SUNWam/bin/amserver start
```

Windows で Identity Server を起動するには

次の方法のいずれかを使って、Identity Server を起動できます。

1. 「コマンドプロンプト」ウィドウに次のコマンドを入力します。

   ```
   cd Is_root¥bin
   amserver start
   ```

2. 「スタート」メニューから、「設定」>「コントロールパネル」>「管理ツール」>「サービス」を選択します。
3. 「サービス」ウィンドウで、「SunONEIS-*hostname*」を右クリックし、「開始」をクリックします。

Identity Server コンソールにログインするには

1. 次の形式でログインのための URL を入力します。

   ```
   http://host.domain:port/amconsole
   ```

   この場合、*host* はシステムのホスト名、*domain* は Identity Server サービスを実行するサーバのドメイン名、*port* は Identity Server サービスのポート番号です。

   例 : `http://nila.eng.siroe.com:58080/amconsole`

2. 「ログイン」ページで、インストール時に指定した最上位管理者のユーザ ID とパスワードを入力します。

Identity Server のオブジェクトクラスと属性の既存のディレクトリエントリへの追加

この手順では、既存のディレクトリエントリを変更して、必要な Identity Server のオブジェクトクラスと属性を含めます。Identity Server オブジェクトクラスは、Identity Server によって管理するディレクトリエントリを示す *marker* とみなすことができます。この marker により、Identity Server はディレクトリ内のエントリを認識できます。オブジェクトクラスには、委託管理に必要な特別な属性が含まれています。

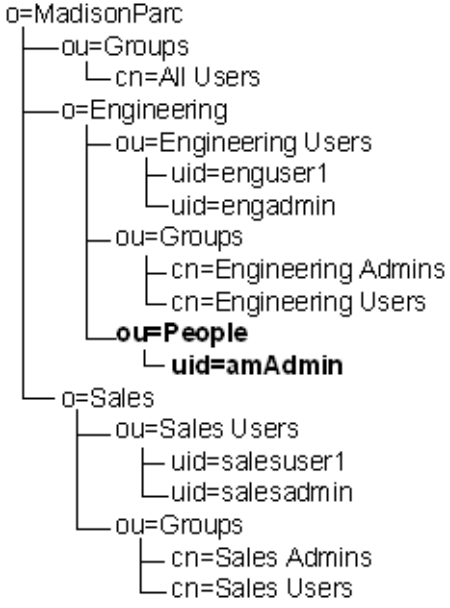
始める前に

既存のディレクトリを使うための残りの手順を容易にするために利用できるリソースがいくつかあります。

この節で使われている例

この章で使っている例は、MadisonParc の DIT に基づいています。図 5-16 では、ルートの下に 2 つの組織、`Engineering` と `Sales` があります。この例の中のグループはすべてスタティックグループです。

図 5-16 MadisonParc ディレクトリ情報ツリー (DIT)



利用できるユーティリティとスクリプト

Sun ONE Directory Server コンソールを使って、または Directory Server に付属の `ldapmodify` または `db2ldif` ユーティリティを使って、これらの変更を行うことができます。Sun ONE Directory Server コンソールを使って、またはこれらのユーティリティを使ってディレクトリを変更する方法については、次の Sun ONE Directory Server のマニュアルを参照してください。

```
http://docs.sun.com/db/prod/s1dirsrv
```

また、この製品に含まれるサンプルスクリプトを使うこともできます。サンプルスクリプトには、Perl 5.x 以降が必要です。サンプルスクリプトは、次の場所にあります。

IS_root`/SUNWam/migration` (`Solaris` の場合)

IS_root`/migration` (`Windows` の場合)

これらのサンプルスクリプトは役に立ちますが、DIT やその他のデータを適切にフォーマットするのを支援するツールにすぎません。各スクリプトには、スクリプトを実行する前に編集する必要がある 1 つ以上の変数がファイルの一番上にあります。各スクリプトを実行すると、LDIF (LDAP Data Interchange Format) ファイルが生成されます。

「すでに存在している」エントリまたは値に関するエラーメッセージが表示される場合は、オブジェクトクラスまたは属性を手動で追加する必要があります。詳細は、Sun ONE Directory Server のマニュアルを参照してください。

各サンプルスクリプトを使うための手順は、この章の各オブジェクトクラスにマークを付ける手順の中に記述されています。

注 サンプルスクリプトを使うための手順を実行する前に、次のサンプルスクリプトを IS_root/SUNWam/migration からディレクトリ Directory_Server_root/shared/bin にコピーする必要があります。

- update-users.pl
- update-static-groups.pl
- update-assignable-dynamic-groups.pl
- update-filtered-groups.pl
- update-people.pl
- update-ou.pl
- update-o.pl
- update-groups.pl

これらのスクリプトを使って行う変更は、自動的に元に戻すことができないことに注意してください。必ずデータをバックアップしてからスクリプトを実行してください。

既存の DIT を変更する 2 つの方法

DIT を変更する 2 つの方法のいずれかを利用できます。1 つの方法では、Identity Server の LDIF および XML の設定ファイルを読み込む前に、必要なすべての変更を DIT に加えます。この方法は間違いが起きやすい方法ですが、LDAP を使った経験があれば速い方法です。

もう 1 つの方法では、LDIF および XML ファイルでいくつかの変更を行なってから、Identity Server を起動して変更が正しく行われたかどうかを確認します。この 2 番目の方法をお勧めします。たとえば、各組織の Identity Server オブジェクトクラスを追加し、Identity Server を再起動して、Identity Server 管理コンソールに組織が表示されることを確認することができます。次に、グループの marker クラスを追加して、確認その他の作業を行うことができます。

組織のマーク付け

インストール時に既存の組織をデフォルトの組織として使った場合は、これらの変更を行う必要はありません。これらのオブジェクトクラスおよび属性は、インストールプログラムによって自動的に追加されています。124 ページの「ピープルコンテナのマーク付け」に進んでください。

この手順では、次の操作を実行します。

1. 次のオブジェクトクラスを各組織エントリに追加します。
   - iplanet-am-managed-org
   - inetDomain
2. 次の属性を各組織エントリに追加します。
   - inetDomainStatus

MadisonParc の例では、これらのオブジェクトクラスと属性は、『インストールおよび設定ガイド』のインストール時に指定および作成されたデフォルトの組織 o=Engineering に自動的に追加されています。オブジェクトクラスと属性は、手動で o=Sales 組織に追加されています。

次に例を示します。

```
dn:o=Engineering,o=madisonparc
objectClass:top
objectClass:organization
objectClass:madisonparc-org
madisonparc-org-description:Engineering Organization
madisonparc-org-city:Santa Clara
aci:(targetattr = "*")(version 3.0; acl "madisonparc Org admin";
allow (all) groupdn="ldap:///cn=Engineering
Admins,o=Engineering,o=madisonparc";)
objectclass:iplanet-am-managed-org
objectlcass:inetDomain
inetDomainStatus:Active
dn:o=Sales,o=madisonparc
objectClass:top

objectClass:organization
objectClass:madisonparc-org
madisonparc-org-description:Sales Organization
madisonparc-org-city:Menlo Park
aci:(targetattr = "*")(version 3.0; acl "madisonparc Org admin";
allow (all) groupdn="ldap:///cn=Sales
Admins,o=Sales,o=madisonparc";)
objectclass:iplanet-am-managed-org
objectlcass:inetDomain
inetDomainStatus:Active
```

サンプルスクリプトを使って組織にマークを付けるには

1. `update-o.pl` を次のディレクトリにコピーします。

   `Directory_Server_root/shared/bin`

2. `$base` 変数を Identity Server が管理する DIT のベース接尾辞に設定します。例 : `o=madisonparc` など。
3. スクリプトがあるディレクトリで、次のコマンドを入力します。

   `perl update-o.pl`

4. プロンプトが表示されたら、次の情報を入力します。

   ホスト名を入力 : Directory Server がインストールされているコンピュータシステムの名前を入力します。

   バインドユーザ名を入力 : ディレクトリ全体にアクセスする十分な権限を持つユーザ名を入力します。例 : `cn=Directory Manager` など。

   バインドパスワードを入力 : 上で指定したユーザのパスワードを入力します。

   ポート番号を入力 : Directory Server のポート番号を入力します。例 : `389` など。

5. 結果を確認するには、作成された `ldif` ファイル (たとえば、`o-update.ldif`) を開いて、適切な変更が行われたことを確認します。

ピープルコンテナのマーク付け

各ピープルコンテナに `iplanet-am-managed-people-container` オブジェクトクラスを追加します。

次に例を示します。

```
dn:ou=Engineering Users,o=Engineering,o=madisonparc
objectClass:top
objectClass:organizationalunit
objectclass:iplanet-am-managed-people-container

...

dn:ou=Sales Users,o=Sales,o=madisonparc
objectClass:top
objectClass:organizationalunit
objectclass:iplanet-am-managed-people-container

...
```

サンプルスクリプトを使ってピープルコンテナにマークを付けるには

1. `update-people.pl` を次のディレクトリにコピーします。

   `Directory_Server_root/shared/bin`

2. `$base` 変数を Identity Server が管理する DIT のベース接尾辞に設定します。例 : `o=madisonparc` など。

3. スクリプトがあるディレクトリに移動して、コマンド行に次のコマンドを入力します。

   ```
   perl update-people.pl
   ```

4. プロンプトが表示されたら、次の情報を入力します。

   ホスト名を入力 : Directory Server がインストールされているコンピュータシステムの名前を入力します。

   バインドユーザ名を入力 : ディレクトリ全体にアクセスする十分な権限を持つユーザ名を入力します。例 : `cn=Directory Manager` など。

   バインドパスワードを入力 : 上で指定したユーザのパスワードを入力します。

   ポート番号を入力 : Directory Server のポート番号を入力します。例 : `389` など。

   ピープルコンテナを入力 : 変更対象の uid が含まれているピープルコンテナの名前を入力します。例 : `People` など。

5. 結果を確認するには、作成された LDIF ファイル (たとえば、`people-update.ldif`) を開いて、適切な変更が行われたことを確認します。

組織単位のマーク付け

組織単位である各コンテナに、次のオブジェクトクラスを追加します。

`iplanet-am-managed-org-unit`

次に例を示します。

```
dn:ou=Groups,o=Engineering, o=madisonparc

objectClass:top
objectClass:organizationalunit
objectClass:inetAdmin
objectclass:iplanet-am-managed-org-unit
dn:cn=Engineering Admins,o=Engineering,o=madisonparc
objectClass:top
objectClass:groupofuniquenames
uniquemember:uid=engadmin,ou=Engineering
Users,o=Engineering,o=madisonparc
dn:cn=Engineering Users,o=Engineering,o=madisonparc
objectClass:top
objectClass:groupofuniquenames
uniquemember:uid=enguser1,ou=Engineering
Users,o=eng,o=madisonparc
uniquemember:uid=enguser2,ou=Engineering
Users,o=eng,o=madisonparc

uniquemember:uid=enguser3,ou=Engineering
Users,o=eng,o=madisonparc
uniquemember:uid=enguser4,ou=Engineering
Users,o=eng,o=madisonparc
dn:ou=Groups,o=Sales, o=madisonparc
objectClass:top
objectClass:organizationalunit
objectClass:inetAdmin
objectclass:iplanet-am-managed-org-unit
```

サンプルスクリプトを使って組織単位にマークを付けるには

1. `update-ou.pl` を次のディレクトリにコピーします。

   ```
   Directory_Server_root/shared/bin
   ```

2. `$base` 変数を Identity Server が管理する DIT のベース接尾辞に設定します。例 : `o=madisonparc` など。

3. スクリプトがあるディレクトリに移動して、コマンド行に次のコマンドを入力します。

   ```
   perl update-ou.pl
   ```

4. プロンプトが表示されたら、次の情報を入力します。

   ホスト名を入力 : Directory Server がインストールされているコンピュータシステムの名前を入力します。

   バインドユーザ名を入力 : ディレクトリ全体にアクセスする十分な権限を持つユーザ名を入力します。例 : `cn=Directory Manager` など。

   バインドパスワードを入力 : 上で指定したユーザのパスワードを入力します。

   ポート番号を入力 : Directory Server のポート番号を入力します。例 : `389` など。

5. 結果を確認するには、作成された LDIF ファイル (たとえば、`ou-update.ldif`) を開いて、適切な変更が行われたことを確認します。

ユーザのマーク付け

各ユーザエントリに、次のオブジェクトクラスを追加します。

- `iplanet-am-web-agent-service`
- `iplanet-am-managed-person`
- `iplanet-am-user-service`
- `inetuser`
- `iPlanetPreferences`
- `inetOrgPerson`

次に例を示します。

```
dn:ou=Engineering Users,o=Engineering,o=madisonparc
objectClass:top
objectClass:organizationalunit

dn:uid=engadmin,ou=Engineering Users,o=Engineering,o=madisonparc
objectClass:inetorgperson
objectClass:organizationalperson
objectClass:person
objectClass:top
objectClass:iplanet-am-web-agent-service
objectClass:iplanet-am-managed-person
objectClass:iplanet-am-user-service
objectClass:inetuser
objectClass:iPlanetPreferences
objectClass:inetOrgPerson
inetuserstatus:active
cn:engadmin
sn:engadmin
userPassword:engadmin
```

```
dn:ou=Engineering Users,o=Engineering,o=madisonparc
dn:uid=enguser1,ou=Engineering Users,o=Engineering,o=madisonparc
objectClass:inetorgperson
objectClass:organizationalperson
objectClass:person
objectClass:top
objectClass:madisonparc-user
objectClass:iplanet-am-web-agent-service
objectClass:iplanet-am-managed-person
objectClass:iplanet-am-user-service
objectClass:inetuser
objectClass:iPlanetPreferences
objectClass:inetOrgPerson
inetuserstatus:active
madisonparc-user-id: 11111
madisonparc-user-building:SCA16
cn:enguser1
sn:enguser1
userPassword:enguser1
```

サンプルスクリプトを使ってユーザにマークを付けるには

1. udpate-users.pl を次のディレクトリにコピーします。

   Directory_Server_root/shared/bin

2. $base 変数を Identity Server が管理する DIT のベース接尾辞に設定します。
   例 : o=madisonparc など。

3. $base-component 変数を DIT のベース接尾辞に設定します。
   例 : o=madisonparc など。

4. スクリプトがあるディレクトリに移動して、コマンド行に次のコマンドを入力します。

   perl udpate-users.pl

5. プロンプトが表示されたら、次の情報を入力します。

   ホスト名を入力 : Directory Server がインストールされているコンピュータシステムの名前を入力します。

   バインドユーザ名を入力 : ディレクトリ全体にアクセスする十分な権限を持つユーザ名を入力します。例 : cn=Directory Manager など。

   バインドパスワードを入力 : 上で指定したユーザのパスワードを入力します。

   ポート番号を入力 : Directory Server のポート番号を入力します。例 : 389 など。

6. 結果を確認するには、作成された LDIF ファイル (たとえば、users-update.ldif) を開いて、適切な変更が行われたことを確認します。

スタティックグループのマーク付け

uniquemember 属性の値を含む各グループエントリに、次のオブジェクトクラスを追加します。

- iplanet-am-managed-static-group
- iplanet-am-managed-group

次に例を示します。

```
dn:cn=Engineering Users,o=Engineering,o=madisonparc
objectClass:top
objectClass:groupofuniquenames
objecClass:iplanet-am-managed-static-group
objecClass:ipanet-am-managed-group
uniquemember:uid=enguser1,ou=Engineering
Users,o=eng,o=madisonparc
uniquemember:uid=enguser2,ou=Engineering
Users,o=eng,o=madisonparc
uniquemember:uid=enguser3,ou=Engineering
Users,o=eng,o=madisonparc
uniquemember:uid=enguser4,ou=Engineering
Users,o=eng,o=madisonparc

dn:ou=Groups,o=Sales, o=madisonparc
objectClass:top
objectClass:organizationalunit

dn:cn=Sales Admins,o=Sales,o=madisonparc
objectClass:top
objectClass:groupofuniquenames
objecClass:iplanet-am-managed-static-group
objecClass:ipanet-am-managed-group
uniquemember:uid=salesadmin,ou=Sales Users,o=Sales,o=madisonparc

dn:cn=Sales Users,o=Sales,o=madisonparc
objectClass:top
objectClass:groupofuniquenames
objecClass:iplanet-am-managed-static-group
objecClass:ipanet-am-managed-group
uniquemember:uid=salesuser1,ou=Sales Users,o=sales,o=madisonparc
uniquemember:uid=salesuser2,ou=Sales Users,o=sales,o=madisonparc
uniquemember:uid=salesuser3,ou=Sales Users,o=sales,o=madisonparc
uniquemember:uid=salesuser4,ou=Sales Users,o=sales,o=madisonparc
```

サンプルスクリプトを使ってスタティックグループにマークを付けるには

1. `update-static-groups.pl` を次のディレクトリにコピーします。

   `Directory_Server_root/shared/bin`

2. `$base` 変数を Identity Server が管理する DIT のベース接尾辞に設定します。例 : `o=madisonparc` など。

3. スクリプトがあるディレクトリに移動して、コマンド行に次のコマンドを入力します。

   ```
   perl update-static-groups.pl
   ```

   プロンプトが表示されたら、次の情報を入力します。

   ホスト名を入力 : Directory Server がインストールされているコンピュータシステムの名前を入力します。

   バインドユーザ名を入力 : ディレクトリ全体にアクセスする十分な権限を持つユーザ名を入力します。例 : `cn=Directory Manager` など。

   バインドパスワードを入力 : 上で指定したユーザのパスワードを入力します。

   ポート番号を入力 : Directory Server のポート番号を入力します。例 : `389` など。

4. 結果を確認するには、作成された LDIF ファイル (たとえば、`static-groups-update.ldif`) を開いて、適切な変更が行われたことを確認します。

フィルタが適用された (ダイナミック) グループへのマーク付け

フィルタが適用されたグループでは、ユーザは DN に基づいて 1 つのグループに入れられます。

次のオブジェクトクラス (属性なし) をフィルタが適用された各グループに追加します。

- `iplanet-am-managed-group`
- `iplanet-am-managed-filtered-group`

サンプルスクリプトを使ってフィルタが適用されたグループにマークを付けるには

1. `update-filtered-groups.pl` を次のディレクトリにコピーします。

   `Directory_Server_root/shared/bin`

2. $base 変数を Identity Server が管理する DIT のベース接尾辞に設定します。例 : o=madisonparc など。
3. スクリプトがあるディレクトリに移動して、コマンド行に次のコマンドを入力します。

   ```
   perl update-filtered-groups.pl
   ```

4. プロンプトが表示されたら、次の情報を入力します。

   ホスト名を入力 : Directory Server がインストールされているコンピュータシステムの名前を入力します。

   バインドユーザ名を入力 : ディレクトリ全体にアクセスする十分な権限を持つユーザ名を入力します。例 : cn=Directory Manager など。

   バインドパスワードを入力 : 上で指定したユーザのパスワードを入力します。

   ポート番号を入力 : Directory Server のポート番号を入力します。例 : 389 など。

5. 結果を確認するには、作成された LDIF ファイル (たとえば、update-filtered-groups-update.ldif) を開いて、適切な変更が行われたことを確認します。

割り当て可能なダイナミックグループへのマーク付け

割り当て可能なダイナミックグループは、フィルタが適用されたグループに似ていますが、ユーザエントリの DN を使ってグループを指定します。

割り当て可能な各ダイナミックグループに次のオブジェクトクラスを追加します。

- iplanet-am-managed-group
- iplanet-am-managed-assignable-group

サンプルスクリプトを使って割り当て可能なダイナミックグループにマークを付けるには

1. update-assignable-dynamic-groups.pl を次のディレクトリにコピーします。

   ```
   Directory_Server_root/shared/bin
   ```

2. $base 変数を Identity Server が管理する DIT のベース接尾辞に設定します。例 : o=madisonparc など。
3. スクリプトがあるディレクトリに移動して、コマンド行に次のコマンドを入力します。

   ```
   perl update-assignable-dynamic-groups.pl
   ```

4. プロンプトが表示されたら、次の情報を入力します。

   ホスト名を入力 : Directory Server がインストールされているコンピュータシステムの名前を入力します。

   バインドユーザ名を入力 : ディレクトリ全体にアクセスする十分な権限を持つユーザ名を入力します。例 : `cn=Directory Manager` など。

   バインドパスワードを入力 : 上で指定したユーザのパスワードを入力します。

   ポート番号を入力 : Directory Server のポート番号を入力します。例 : `389` など。

5. 結果を確認するには、作成された LDIF ファイル (たとえば、`assignable-dynamic-groups-update.ldif`) を開いて、適切な変更が行われたことを確認します。

グループコンテナへのマーク付け

グループコンテナは、グループを含む組織単位 (ou) です。各グループコンテナに、次のオブジェクトクラスを追加します。

```
iplanet-am-managed-group-container
```

サンプルスクリプトを使ってグループコンテナにマークを付けるには

1. `update-groups.pl` を次のディレクトリにコピーします。

   ```
   Directory_Server_root/shared/bin
   ```

2. `$base` 変数を Identity Server が管理する DIT のベース接尾辞に設定します。例 : `o=madisonparc` など。

3. スクリプトがあるディレクトリに移動して、コマンド行に次のコマンドを入力します。

   ```
   perl update-groups.pl
   ```

4. プロンプトが表示されたら、次の情報を入力します。

   ホスト名を入力 : Directory Server がインストールされているコンピュータシステムの名前を入力します。

   バインドユーザ名を入力 : ディレクトリ全体にアクセスする十分な権限を持つユーザ名を入力します。例 : `cn=Directory Manager` など。

   バインドパスワードを入力 : 上で指定したユーザのパスワードを入力します。

   ポート番号を入力 : Directory Server のポート番号を入力します。例 : `389` など。

5. 結果を確認するには、作成された LDIF ファイル (たとえば、`groups-update.ldif`) を開いて、適切な変更が行われたことを確認します。

変更された LDIF ファイルの読み込み

ここまでの手順でスクリプトを実行した後には、さまざまな LDIF ファイルが Perl スクリプトを実行した同じディレクトリに作成されます。実際にはこれまで、ディレクトリではなんの変更も行われていません。変更されたファイルをディレクトリに読み込む前に、ファイルを調べて、すべての Identity Server オブジェクトクラスおよび属性が既存のディレクトリエントリに正しく追加されたことを確認するようお勧めします。正しく変更されたことを確認したら、次の `ldapmodify` コマンドを使って各ファイルを読み込みます。

`ldapmodify -h` *hostname* `-p` *port* `-D` *bind_user*`, -w` *password* `-a -c -f` *filename*`.ldif`

Identity Server とディレクトリの変更の結果

ここまでの手順を実行して変更が完了すると、DIT 内のすべてのエントリを Identity Server で管理できるようになります。組織管理者の既存の ACI を変更する必要はありません。Identity Server はデフォルトでロールと ACI を使いますが、既存のグループと ACI はまだ有効です。

グループベースの DIT は、ロールおよび ACI を活用する DIT に変換できます。これを選択する場合は、Identity Server の組織管理者ロールを使って、そのロールを既存の `organizationList` 管理者に割り当てることができます。

第 6 章

Identity Server コンソールのインストール

この章では、Sun ONE Identity Server コンソールのインストール手順を具体的に説明します。この章は、次の項目から構成されています。

- 始める前に
- GUI を使用したインストール
- コマンド行からの Identity Server コンソールのインストール

始める前に

Sun ONE Identity Server 管理およびポリシーサービスをインストールすると、デフォルトで Identity Server コンソールもインストールされます。同じホストに、もう一度インストールする必要はありません。ただし、別のホストに単独でインストールすることができます。

インストールを開始する前に、次の事項を確認してください。

- Sun ONE Identity Server コンソールをインストールする場合、そのマシンの root 権限が必要です。このマシンをホストマシンと呼びます。
- ホストマシンのドメイン名の設定が必要です。ドメイン名が設定されていない場合は、38 ページの「ドメイン名の設定」の手順に従ってください。
- インストールの実行中は、すべての Web ブラウザを終了します。

注 Identity Server またはそのコンポーネントをインストールできるのはローカルマシンだけです。ネットワーク上のリモートマシンにインストールすることはできません。

GUI を使用したインストール

1. 製品 CD から Sun ONE Identity Server コンソールをインストールする場合は、ソフトウェアをインストールするシステムのドライブに製品 CD を挿入します。

   製品をダウンロードした場合は、次のコマンドを使って製品バイナリファイルを解凍します。

   `gunzip -dc` *`binaryfile`*`.tar.gz | tar -xvof -`

   この場合、*binaryfile* をダウンロードした製品バイナリの名前に置き換える必要があります。

2. 別の端末ウィンドウを開き、`xhost +` と入力してマシンのアクセス制御を無効にします。

3. アプリケーションウィンドウで、次のコマンドのどちらかを使用して DISPLAY 変数を設定します。

   csh または tcsh を使用している場合、次のように入力します。

   `setenv DISPLAY` *`myserver.Siroe.COM:0.0`*

   sh、ksh、または bash を使用している場合、次のように入力します。

   `export DISPLAY=`*`myserver.Siroe.COM:0.0`*

   この場合、`nila` はインストールプログラムを実行しているマシンです。

4. `setup` プログラムを実行します。このプログラムは、製品 CD の `/cdrom/idserv_60` ディレクトリにあります。製品バイナリをダウンロードした場合は、バイナリファイルを展開したディレクトリにこのプログラムがあります。

5. コマンド行に `./setup` と入力します。インストールプログラムが起動し、開始パネルが開きます。

6. 「次へ」をクリックして、ソフトウェアライセンス契約に同意します。

7. 「インストールディレクトリ」パネルで、Directory Server をインストールするディレクトリを指定します。このディレクトリに対する書き込み権限と実行権限が必要なことに注意してください。

   このディレクトリへの Sun ONE Identity Server のインストール : Sun ONE Identity Server サービスをインストールするディレクトリへのパスを入力します。

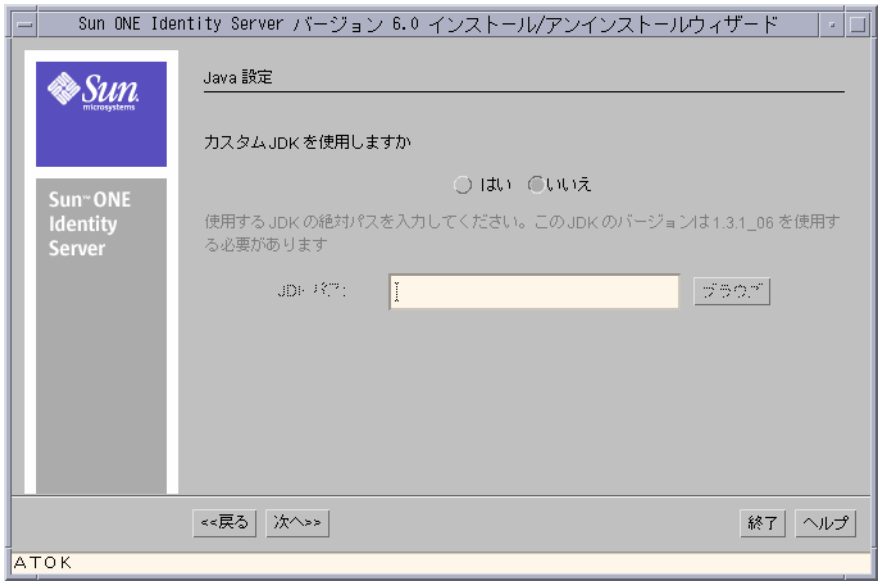
注　Identity Server サービスと Directory Server を別々のディレクトリにインストールするようにします。Identity Server サービスと Directory Server を別々のコンピュータシステムにインストールするのが理想的です。

---

8. 「次へ」をクリックし、「インストール / アンインストールされるコンポーネント」パネルで、「Sun ONE Identity Server 管理コンソールのみ」を選択します。

9. 「次へ」をクリックし、「Java 設定」パネルで次の情報を入力します。

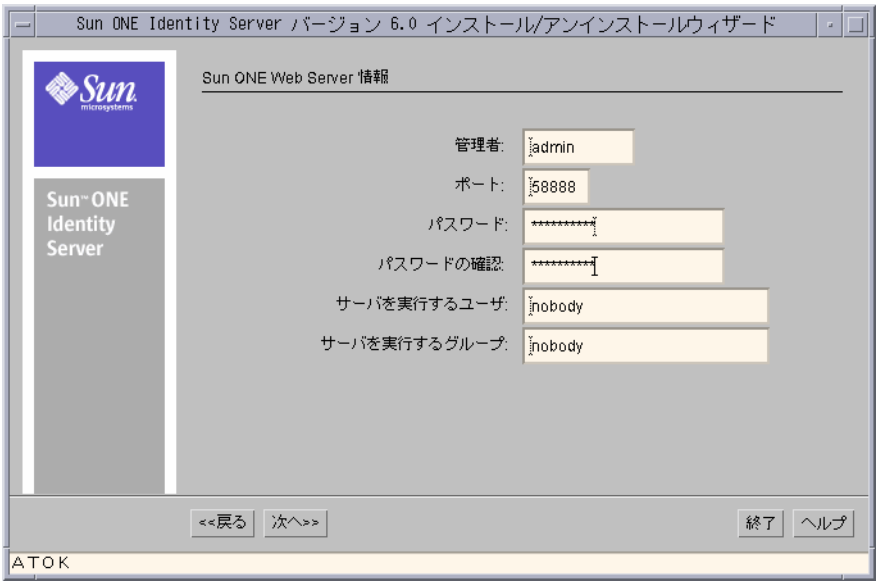
図 6-1 「Java 設定」パネル



カスタム JDK を使用しますか : Web Server で Java をサポートするには、JDK (Java Development Kit) 1.3.1_06 が必要です。この JDK は Identity Server 6.0 に付属しています。Sun ONE Identity Server に付属の JDK をインストールする場合は、「いいえ」を選択します。ただし、既存の JDK (バージョン 1.3.1_06) を使用する場合は、「はい」を選択し、そのファイルの場所への絶対パスを入力します。

10. 「次へ」をクリックし、「Sun ONE Web Server 情報」パネルで、Identity Server サービスを実行する Web Server に関して次の情報を入力します。

図 6-2　「Sun ONE Web Server 情報」パネル



管理者 : Web Server にアクセスし、Web Server を管理する管理者としてのユーザ名を入力します。

ポート : ポート番号を入力します。通常、デフォルトは 58888 です。

パスワード : 管理者のパスワードを入力します。パスワードの指定には 8 文字以上必要です。

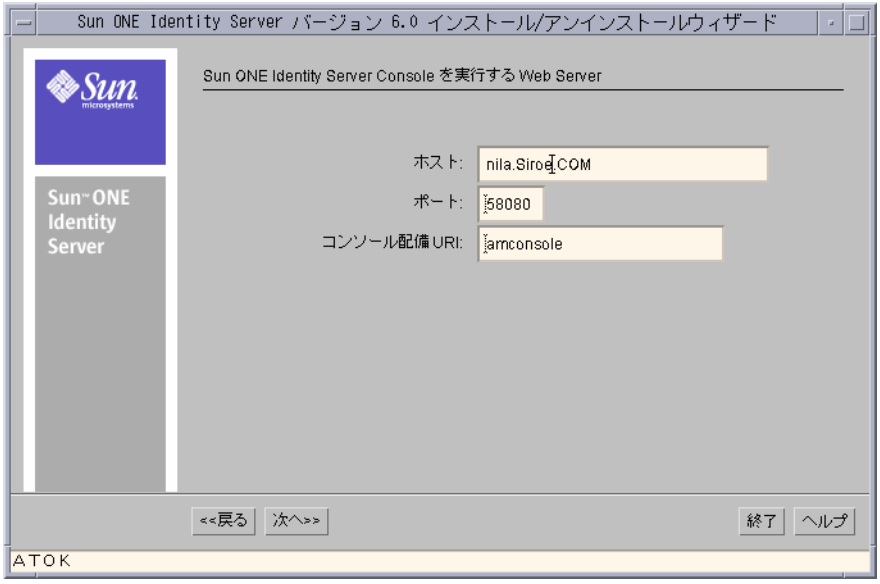
パスワードの確認 : 管理者パスワードを確認するために、もう一度入力します。

サーバを実行するユーザ : Web Server を実行するユーザアカウントを入力します。(例 : nobody)

サーバを実行するグループ : 上述したユーザが属するグループを入力します。(例 : nobody)

11. 「次へ」をクリックし、「Sun ONE Identity Server Console を実行する Web Server」パネルで次の情報を入力します。

図 6-3 「Sun ONE Identity Server Console を実行する Web Server」パネル



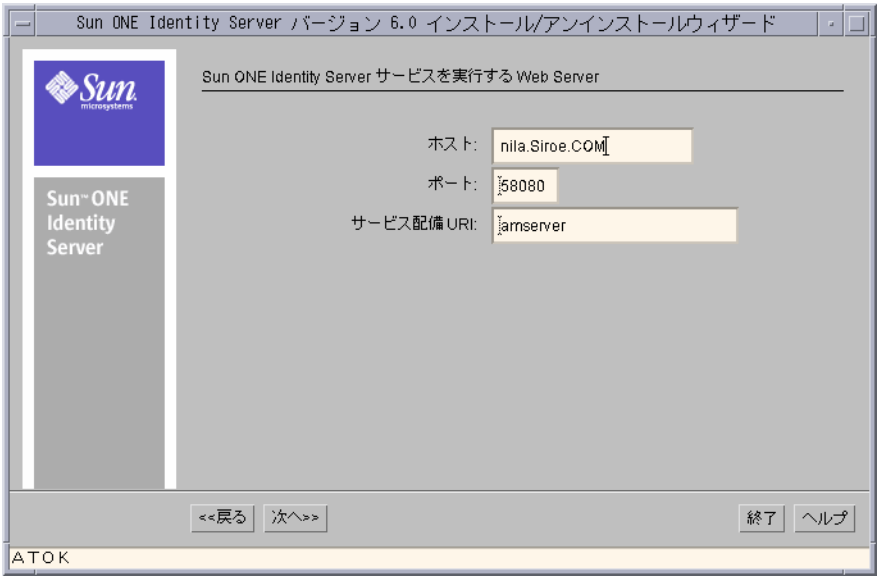
ホスト : Identity Server コンソールをインストールするコンピュータの完全指定のドメイン名を入力します。

ポート : Identity Server コンソールを実行する Web Server のポート番号を入力します。デフォルトのポート番号は `58080` です。

コンソール配備 URI: Web Server は、URI (Universal Resource Identifier) 接頭辞の指定に従って、Sun ONE Identity Server 管理コンソール (関連付けられた HTML ページ) や、その他の Web アプリケーション固有の情報 (クラス、jar などに関する情報) を検索します。デフォルトの URI 接頭辞は `amconsole` です。別の名前を入力することもできます。

12. 次の情報を指定して、Sun ONE Identity Server サービスを実行する Web Server をインストールし、設定します。

図 6-4 「Sun ONE Identity Server サービスを実行する Web Server」パネル



ホスト [nila.Siroe.COM]: Web Server を実行するコンピュータの名前を入力します。

ポート [58080]: Web Server が使用するポート番号を入力します。

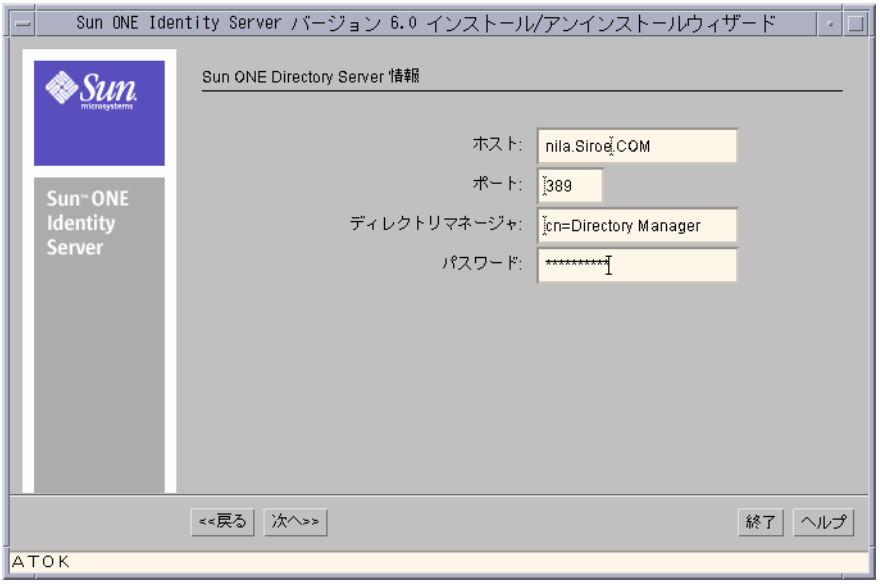
サービス配備 URI [/amserver]: Web Server は、URI (Universal Resource Identifier) 接頭辞の指定に従って、サービスに関連付けられた HTML ページや Web アプリケーション固有の情報 (クラス、jar などに関する情報) を検索します。デフォルトの URI 接頭辞は `amserver` です。

13. 「次へ」をクリックし、「ディレクトリのルートの接尾辞」パネルで次の情報を入力します。

    ディレクトリツリー内の Sun ONE Identity Server ルート : ルート接尾辞として設定する識別名 (DN) を入力します。識別名 (DN) には、最低 1 個の type=value ペアが必要です。たとえば、`o=isp;o=madisonparc;dc=siroe,dc=COM` のようになります。

14. 「次へ」をクリックし、「Sun ONE Directory Server 情報」パネルで次の情報を入力します。

図 6-5　「Sun ONE Directory Server 情報」パネル



ホスト：Directory Server がインストールされるコンピュータの完全指定のドメイン名を入力します。

ポート：Directory Server のポート番号を入力します。デフォルトのポート番号は `389` です。

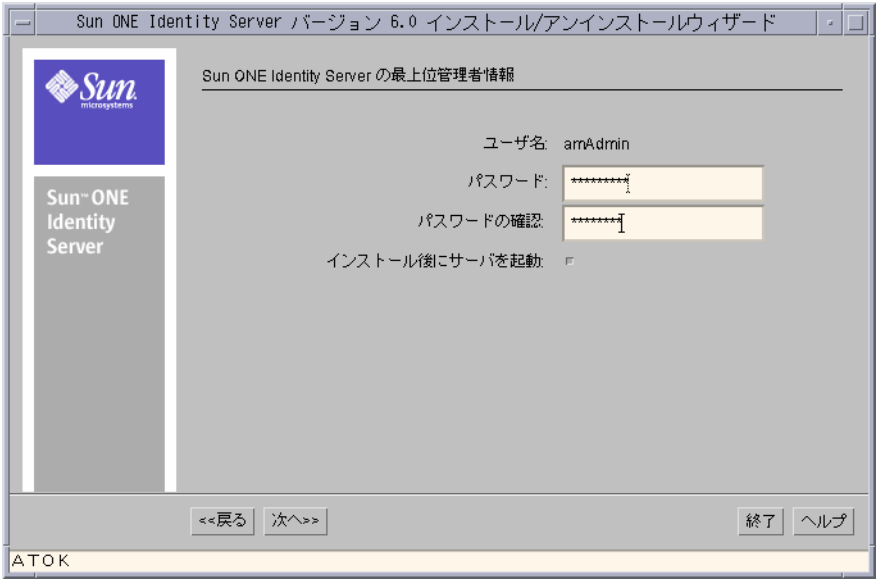
ディレクトリマネージャ：Directory Server へのアクセスを制限されたユーザの DN を入力します。例：`cn=Directory Manager` など。

パスワード：ディレクトリマネージャのパスワードを入力します。パスワードの指定には 8 文字以上必要です。

これらのフィールドに入力する情報が不正確であると、インストールプログラムによりエラーメッセージが表示されます。入力した情報を確認し、訂正してから次の手順に進んでください。

15. 「次へ」をクリックし、「Sun ONE Identity Server の最上位管理者」パネルで次の情報を入力します。

図 6-6　「Sun ONE Identity Server の最上位管理者」パネル



ユーザ名：スーパー管理者のユーザ名は amAdmin です。最上位管理者には、Identity Server が管理するすべてのエントリに対して無制限のアクセス権があります。ユーザ名は、amAdmin としてハードコードされています。これにより、Identity Server 管理者ロールとその権限が作成され、適切に Directory Server に割り当てられるので、インストール直後に Identity Server にログインできます。これは管理者ロールなので、インストール後にほかのユーザをこのロールに追加できます。

パスワード：amAdmin ユーザのパスワードを入力します。パスワードの指定には 8 文字以上必要です。

パスワードの確認：確認のため、amAdmin パスワードを再度入力します。

インストール後にサーバを起動：インストール後に Identity Server を自動的に起動する場合は、このオプションをクリックします。このオプションを選択しない場合は、インストール後に手動でサーバを起動できます。実行手順については、118 ページの「Identity Server の起動」を参照してください。

16. 「次へ」をクリックし、「現在選択されている設定」パネルで、これまでのパネルで選択した項目を確認します。任意のパネルを再表示するには、「戻る」をクリックして必要なパネルに移動します。

17. 「次へ」をクリックし、「インストールの準備完了」パネルで、Sun ONE Identity Server コンソールを使用してインストールしたコンポーネントを表示します。

18. 「今すぐインストール」をクリックしてインストールを開始します。インストールの終了時に、「インストールの要約」パネルで、製品が正常にインストールされたかどうかが表示されます。このパネルで、「取消し」ボタンをクリックして、製品がインストールされた場所を確認します。詳細を確認後、「インストールの要約」パネルで「閉じる」をクリックして、インストールプログラムを終了します。

コマンド行からの Identity Server コンソールのインストール

コマンド行からコンソールをインストールするには、次の手順に従います。

1. root でログインします。
2. 開いているすべての Web ブラウザを閉じます。
3. Sun ONE Identity Server インストールファイルを解凍したディレクトリに移動します。
4. 次のコマンドを使用して、インストールプログラムを起動します。

   ```
   # ./setup -nodisplay
   ```

   Windows 上でインストールする場合は、次のコマンドを使用します。

   ```
   java am -nodisplay
   ```

5. 画面に表示される手順を確認します。インストーラが示すさまざまなプロンプトに対する応答方法の説明が表示されます。手順を確認後、Enter を押してソフトウェアライセンス契約を確認します。インストールのどの段階でも、< を入力して前のプロンプトに戻ることができます。また、! を入力してインストールプログラムを終了することができます。
6. ライセンス契約を確認し、yes と入力してライセンス契約に同意します。
7. 次のプロンプトで、共通ドメインサービスをインストールするディレクトリを指定します。

```
Sun ONE Identity Server コンポーネントは、次のディレクトリにインストール
されます。そのディレクトリは、" インストールディレクトリ " と呼ばれます。この
ディレクトリを使用するには、Enter キーだけを押します。別のディレクトリを使用
するには、そのディレクトリの完全パスを入力した後に Enter キーを押します。
   Sun ONE Identity Server コンポーネントをインストールするディレクトリ
[/opt] {"<" 戻る , "!" 終了 }:
```

8. インストールプログラムが指定するデフォルトディレクトリを選択するには、Enter を押します。別のディレクトリにインストールする場合は、そのディレクトリへの絶対パスを入力して Enter を押します。

   指定したディレクトリが存在しない場合、インストールプログラムがディレクトリを作成するか、または別のディレクトリを選択するか聞いてきます。新しいディレクトリを作成する場合は、「作成」を選択します。インストールプログラムには、新しく作成するディレクトリに対する読み取り / 書き込み許可が必要です。または、新しいディレクトリを作成しない場合は、2 を入力して「新規」を選択し、別のディレクトリ名を入力します。

9. 次のプロンプトで、2 を入力して「Identity Server コンソール」を選択します。

```
インストールするコンポーネントを次の中から選択してください。インストールする
コンポーネントの番号を入力し、ENTER キーを押してください

1. Sun ONE Identity Server 管理サービスとポリシーサービス
2. Sun ONE Identity Server 管理コンソールのみ
3. 既存の Directory Server を設定
4. Sun ONE Identity Server ドメイン間シングルサインオン
5. 連合管理用の共通ドメインサービス

コンポーネントを選択し ENTER キーを押します [1] {"<" 戻る , "!" 終了 } 2
```

10. 次のプロンプトで、使用する JDK を指定します。Identity Server がサポートする Java には、JDK バージョン 1.3.1_06 が必要です。デフォルトの JDK が提供されていますが、ユーザ独自の JDK (バージョン 3.1_06) を使用できます。

```
Java 設定

Sun ONE Identity Server が使用する JDK について次の情報を提供してくだ
さい。

カスタム JDK を使用しますか :
すでにマシンに JDK がインストールされていて、JDK のバージョンが 1.3.1_06
の場合は、yes を選択してください
JDK がまだインストールされていない場合、または JDK のバージョンが
1.3.1_06 でない場合は、no を選択してください

JDK パス :
既存の JDK の完全なパスを入力してください。

カスタム JDK を使用しますか [n] {"<" 戻る , "!" 終了 }
```

11. JDK 1.3.1_06 をお持ちの場合は、y を入力して JDK への絶対パスを入力します。それ以外の場合は、n を入力してインストールプログラムに付属する JDK を使用します。
12. 次の情報を入力して、Sun ONE Web Server をインストールし、設定します。

```
Sun ONE Web Server 情報
   管理者 [admin] {"<" 戻る , "!" 終了 }:
   ポート [58888] {"<" 戻る , "!" 終了 }:
   パスワード :
   パスワードの確認 :
   サーバを実行するユーザ [nobody] {"<" 戻る , "!" 終了 }:
   サーバを実行するグループ [nobody] {"<" 戻る , "!" 終了 }:
```

管理者 [admin]: Sun ONE Web Server のサーバ管理者としてのユーザ名を入力します。Enter を押して、デフォルトのユーザ ID (admin) を選択します。

ポート [58888]: Identity Server サービスを実行する Web Server のポート番号を入力します。デフォルトのポート番号は 58088 です。デフォルトのポート番号を選択する場合は Enter を押します。

パスワード : Web Server 管理者のパスワードを入力します。パスワードの指定には 8 文字以上必要です。

パスワードの確認 : 確認のためにもう一度 Web Server 管理者パスワードを入力します。

サーバを実行するユーザ [nobody]: Web Server を実行するユーザアカウントを入力します。Enter を押して、デフォルトユーザ nobody を選択します。

サーバを実行するグループ [nobody]: 上述したユーザが属するグループを入力します。例 : nobody など。

13. 次の情報を指定して、Sun ONE Identity Server コンソールを実行する Web Server をインストールし、設定します。

```
Sun ONE Identity Server Console を実行する Web Serve
   ホスト [nila.Siroe.COM] {"<" 戻る , "!" 終了 }:
   ポート [58080] {"<" 戻る , "!" 終了 }:
   コンソール配備 URI [amconsole] {"<" 戻る , "!" 終了 }:
```

ホスト [nila.Siroe.COM]: Web Server を実行するコンピュータの名前を入力します。デフォルトの名前を使用するには、Enter を押します。

ポート [58080]: Web Server が使用するポート番号を入力します。

コンソール配備 URI: Web Server は、URI (Universal Resource Identifier) 接頭辞の指定に従って、Sun ONE Identity Server 管理コンソール (関連付けられた HTML ページ) や、その他の Web アプリケーション固有の情報 (クラス、jar などに関する情報) を検索します。デフォルトの URI 接頭辞は amconsole です。Enter を押してデフォルトの接頭辞を受け入れるか、または別の名前を入力できます。

14. 次の情報を指定して、Sun ONE Identity Server サービスを実行する Web Server をインストールし、設定します。

```
Sun ONE Identity Server サービスを実行する Web Server
   ホスト [nila.Siroe.COM] {"<" 戻る , "!" 終了 }:
   ポート [58080] {"<" 戻る , "!" 終了 }:
   サービス配備 URI [amserver] {"<" 戻る , "!" 終了 }:
```

ホスト [nila.Siroe.COM]: Web Server を実行するコンピュータの名前を入力します。デフォルトの名前を使用するには、Enter を押します。

ポート [58080]: Web Server が使用するポート番号を入力します。

サービス配備 URI [/amserver]: Web Server は、URI (Universal Resource Identifier) 接頭辞の指定に従って、サービスに関連付けられた HTML ページや Web アプリケーション固有の情報 (クラス、jar などに関する情報) を検索します。

デフォルトの URI 接頭辞は `amserver` です。Enter を押してデフォルトの接頭辞を受け入れるか、あるいは別の名前を入力できます。

15. 次のプロンプトで、情報を入力して DIT を設定します。

```
ディレクトリのルートの接尾辞
   Sun ONE Directory Server 情報 [dc=siroe,dc=COM]
{"<"
   戻る , "!" 終了 }:
```

ディレクトリツリー内の Sun ONE Identity Server ルート [dc=siroe,dc=COM]: ルート接尾辞として設定する識別名 (DN) を入力します。識別名 (DN) には、最低 1 個の type=value ペアが必要です。たとえば、`o=isp;o=madisonparc;dc=siroe,dc=COM` のようになります。

16. 次のプロンプトで、情報を入力して Sun ONE Directory Server をインストールし、構成します。

```
Sun ONE Directory Server 情報
   ホスト [nila.Siroe.COM] {"<" 戻る , "!" 終了 }:
   ポート [389] {"<" 戻る , "!" 終了 }:
   ディレクトリマネージャ [cn=Directory Manager] {"<" 戻る , "!" 終了
}:
   パスワードの確認 :
```

ホスト [nila.Siroe.COM]: Directory Server をインストールするコンピュータのドメイン名を入力します。デフォルトの名前を使用するには、Enter を押します。

ポート [389]: Directory Server が使用するポート番号を入力します。デフォルトのポート番号を使用するには、Enter を押します。ポートがすでに使用されている場合、インストールプログラムから別のポート番号を入力するよう要求されます。1 ～ 65535 までの別の番号を入力できます。

ディレクトリマネージャ [cn=Directory Manager]: Directory Server 管理ユーザ、つまりディレクトリマネージャは、Directory Server のデータおよび設定に対して無制限のアクセス権を持つ管理者です。ディレクトリマネージャのデフォルト DN は、`cn=Directory Manager` です。

パスワードの確認 : Directory Server 管理者のパスワードを入力します。パスワードの指定には 8 文字以上必要です。

17. 次のプロンプトで、Sun ONE Identity Server 最上位管理者に関する情報を入力します。

```
Sun ONE Identity Server の最上位管理者情報
ユーザ名 :amAdmin
   パスワード :
   パスワードの確認 :
   インストール後にサーバを起動 [yes] {"<" 戻る , "!" 終了 }:
```

ユーザ名 : これは、Identity Server が管理するすべてのエントリに対して無制限のアクセス権を持つ管理者です。最上位管理者のユーザ ID は、`amAdmin` としてハードコードされています。これにより、Identity Server 管理者ロールとその権限が作成されて適切に Directory Server に割り当てられるので、インストール直後に Identity Server 製品にログインできます。これは管理者ロールなので、インストール後にほかのユーザをこのロールに追加できます。

パスワード : 管理者のパスワードを入力します。

パスワードの確認 : 入力したパスワードを確認するために、もう一度入力します。

インストール後にサーバを起動 [yes]: Enter を押すと、インストール後 Identity Server は自動的に起動します。手動でサーバを起動する場合は、*no* を入力します。このオプションを選択しない場合は、インストール後に手動でサーバを起動できます。実行手順については、118 ページの「Identity Server の起動」を参照してください。

選択した設定が、インストールプログラムにより表示されます。

```
現在選択されている設定
Sun ONE Identity Server コンソール : http://nila.Siroe.COM:58080
コンソール配備 URI:/amconsole
Sun ONE Identity Server インストールディレクトリ : /opt
管理者 : admin
ポート : 58888
Sun ONE Identity Server サービス : http://nila.Siroe.COM:58080
サービス配備 URI:/amserver
ディレクトリサーバ : nila.Siroe.COM:389
ディレクトリマネージャ :cn=Directory Manager
```

18. 次のプロンプトで、1 を入力して Identity Server コンソールのインストールを開始します。

```
ディスク容量を調べています ....

次のコンポーネントがインストールされます：

プロダクト： Sun ONE Identity Server
場所： /opt
サイズ :133.67MB
--------------------------------
JDK
Sun ONE Web Server
その他のパッケージ
Sun ONE Identity Server 管理コンソール
リソースパッケージ

インストールの準備完了
1．今すぐインストール
2．開始
3．終了

   上のオプションを 1 つ選択してください [1] {"<" 戻る， "!" 終了 }
```

第 7 章

共通ドメインサービスのインストール

この章では、Sun ONE Identity Server のコンポーネントの 1 つである共通ドメインサービスのインストール手順を具体的に説明します。この章は、次の項目から構成されています。

- 始める前に
- GUI を使用したインストール
- コマンド行からの共通ドメインサービスのインストール

始める前に

共通ドメインサービスは、Sun ONE Identity Server のコンポーネントです。そのため、Sun ONE Identity Server 管理およびポリシーサービスをインストールすると、デフォルトで共通ドメインサービスもインストールされます。もう一度インストールする必要はありません。ただし、別のホストに単独でインストールすることができます。

最初に、次の事項を確認してください。

- 共通ドメインサービスをインストールする場合、そのマシンの root 権限が必要です。このマシンをホストマシンと呼びます。
- ホストマシンのドメイン名の設定が必要です。ドメイン名が設定されていない場合は、38 ページの「ドメイン名の設定」の手順に従ってください。
- インストールの実行中は、すべての Web ブラウザを終了します。

注 このコンピュータの別のディレクトリに、共通ドメインサービスがインストール済みでないことを確認します。次のコマンドを使用して、既存のインスタンスを確認できます。`pkginfo | grep SUNWamfcd`

GUI を使用したインストール

GUI を使用した共通ドメインサービスのインストールを開始するには、次の手順に従います。

1. root でログインします。
2. 次のコマンドを使って製品のバイナリファイルを解凍します (実行していない場合)。

   ```
   # gunzip -dc binaryfile.tar.gz | tar -xvof
   ```

   この場合、*binaryfile* をダウンロードした製品バイナリの名前に置き換える必要があります。
3. 別の端末ウィンドウを開き、`xhost +` と入力してマシンのアクセス制御を無効にします。
4. アプリケーションウィンドウで、次のコマンドのどちらかを使用して DISPLAY 変数を設定します。
   - csh または tcsh を使用している場合、次のように入力します。

     ```
     setenv DISPLAY nila.Siroe.COM:0.0
     ```
   - sh、ksh、または bash を使用している場合、次のように入力します。

     ```
     export DISPLAY=nila.Siroe.COM:0.0
     ```

   この場合、`nila` はインストールプログラムを実行しているマシンです。
5. 次のコマンドを使用して、インストールプログラムを起動します。

   ```
   # ./setup
   ```

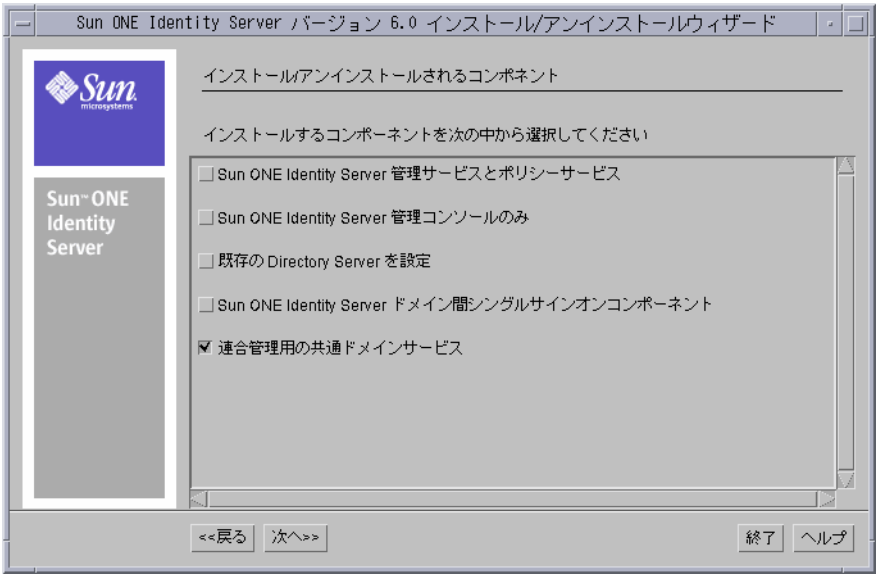
開始パネルが開きます。「次へ」ボタンを使用して、インストールを続行します。どのインストール段階にあっても、必要な場合は「戻る」ボタンを使用して任意のパネルに戻ることができます。

6. 「次へ」をクリックします。
7. ライセンス契約を確認し、「はい」をクリックしてライセンス契約に同意します。
8. 共通ドメインサービスをインストールするディレクトリを指定します。フィールドにインストールするディレクトリの絶対パスを直接入力するか、あるいは「ブラウズ」ボタンを使用してディレクトリを選択することができます。このディレクトリに対する書き込み権限と実行権限が必要なことに注意してください。

   指定したディレクトリが存在しない場合、インストールプログラムがディレクトリを作成するか、または別のディレクトリを選択するか聞いてきます。新しいディレクトリを作成する場合は、「作成」をクリックします。または、新しいディレクトリを作成しない場合は、「新規」をクリックし、既存のディレクトリを選択します。

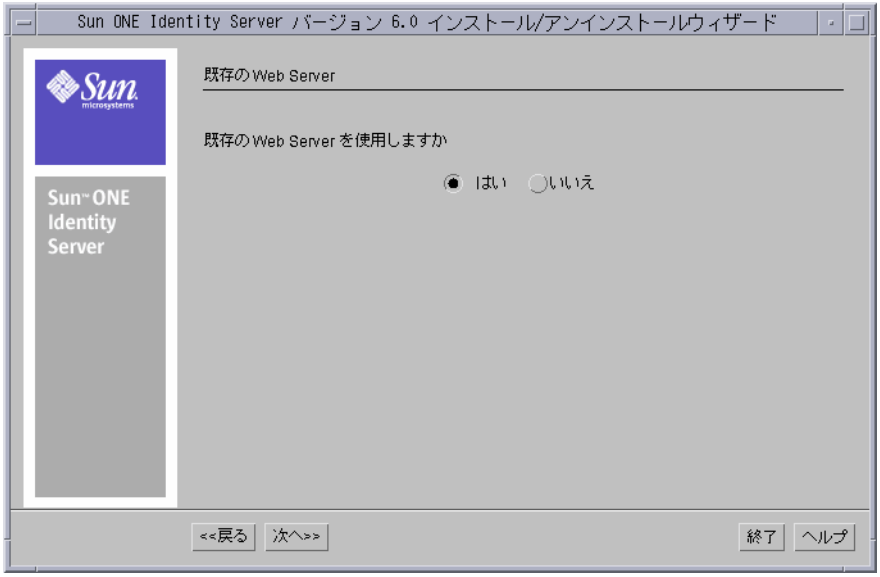
9. 「次へ」をクリックし、「インストール / アンインストールされるコンポーネント」パネルで、「共通ドメインサービス」を選択します。

図 7-1 「インストール / アンインストールされるコンポーネント」パネル



10. 「次へ」をクリックし、「既存の Web Server」パネルで次の情報を入力します。

図 7-2　「既存の Web Server」パネル

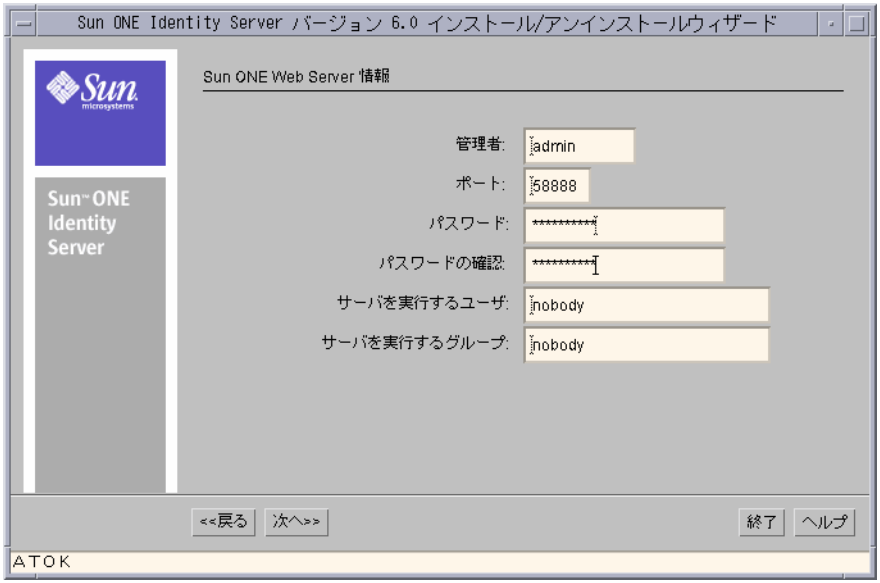


既存の Web Server を使用しますか ?: 既存の Sun ONE Web Server を使用する場合は、「はい」をクリックします。

Identity Server に付属の Sun ONE Web Server をインストールする場合は、「いいえ」をクリックします。

11. 「次へ」をクリックします。上の手順で「いいえ」を選択した場合は、次の情報を入力して、Identity Server 付属の Sun ONE Web Server をインストールし、設定します。「はい」を選択した場合は、この手順を省略して次に進みます。

図 7-3　「Sun ONE Web Server 情報」パネル



管理者 : Web Server を設定する管理者としてのユーザ名を入力します。フィールドに表示されるデフォルト名を上書きすることができます。

ポート : Web Server が使用するポート番号を入力します。フィールドに表示されるデフォルトのポート番号を上書きすることができます。

パスワード : 管理者としてのユーザパスワードを入力します。

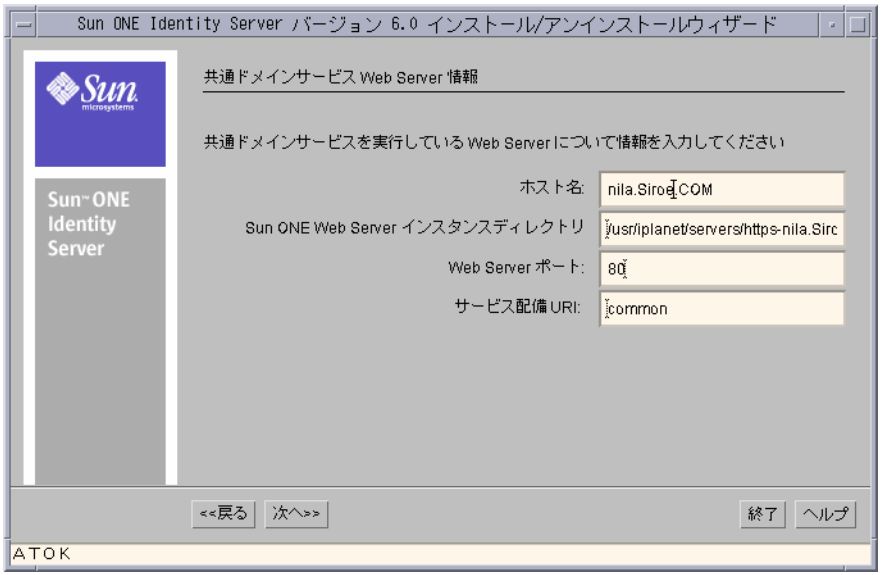
パスワードの確認 : 確認のためにもう一度パスワードを入力します。

サーバを実行するユーザ : Web Server を実行するユーザアカウントを入力します。(例 : nobody)

サーバを実行するグループ : 上述したユーザが属するグループを入力します。(例 : nobody)

12. 「次へ」をクリックし、「共通ドメインサービス Web Server 情報」パネルで次の情報を入力します。

図 7-4　「共通ドメインサービス Web Server 情報」パネル



ホスト名 : 共通ドメインサービスを実行する Web Server の完全指定のドメイン名を入力します。

Sun ONE Web Server インスタンスディレクトリ : Web Server がインストールされているディレクトリの絶対パスおよび Web Server のインスタンス名を入力します。たとえば、`https-nila.Siroe.COM` などです。このパスは、DNS 参加ドメインを管理する Web Server です。このフィールドは、既存の Web Server を使用する場合にのみ有効です。

Web Server ポート : サービスが使用するポート番号を入力します。

サービス配備 URI: 共通ドメインサービスへのアクセスに使用する URI です。デフォルトの URI は `common` です。これは変更可能です。

13. 「次へ」をクリックして、選択した設定を確認します。選択した任意の値を変更する場合は、「戻る」ボタンを使って該当のパネルに移動し、変更します。
14. 「次へ」をクリックします。インストールプログラムは、空きディスク容量をチェックし、インストールするコンポーネントの一覧を表示します。インストールするすべてのコンポーネントの合計ファイルサイズも表示します。
15. 「今すぐインストール」をクリックしてインストールを開始します。

コマンド行からの共通ドメインサービスのインストール

コマンド行から共通ドメインサービスをインストールするには、次の手順に従います。

1. root でログインします。
2. 開いているすべての Web ブラウザを閉じます。
3. インストールファイルを解凍したディレクトリに移動します。
4. 次のコマンドを使用して、インストールプログラムを起動します。

   ```
   # ./setup -nodisplay
   ```

   Windows 上でインストールする場合は、次のコマンドを使用します。

   ```
   java am -nodisplay
   ```

5. 画面に表示される手順を確認します。インストーラが示すさまざまなプロンプトに対する応答方法の説明が表示されます。手順を確認したら、Enter を押してソフトウェアライセンス契約を確認します。インストールのどの段階でも、< を入力して前のプロンプトに戻ることができます。また、! を入力してインストールプログラムを終了することができます。
6. ライセンス契約を確認し、yes と入力してライセンス契約に同意します。
7. 次のプロンプトで、共通ドメインサービスをインストールするディレクトリを指定します。

```
Sun ONE Identity Server コンポーネントは、次のディレクトリにインストール
されます。そのディレクトリは、" インストールディレクトリ " と呼ばれます。この
ディレクトリを使用するには、Enter キーだけを押します。別のディレクトリを使用
するには、そのディレクトリの完全パスを入力した後に Enter キーを押します。
   Sun ONE Identity Server コンポーネントをインストールするディレクトリ
[/opt] {"<" 戻る , "!" 終了 }:
```

8. インストールプログラムが指定するデフォルトディレクトリを選択するには、Enter を押します。別のディレクトリにインストールする場合は、そのディレクトリへの絶対パスを入力して Enter を押します。

   指定したディレクトリが存在しない場合、インストールプログラムがディレクトリを作成するか、または別のディレクトリを選択するか聞いてきます。新しいディレクトリを作成する場合は、「作成」を選択します。インストールプログラムには、新しく作成するディレクトリに対する読み取りおよび書き込み許可が必要です。または、新しいディレクトリを作成しない場合は、2 を入力して「新規」を選択し、別のディレクトリ名を入力します。

9. 次のプロンプトで、5 を入力して「共通ドメインサービス」を選択します。

```
インストールするコンポーネントを次の中から選択してください。インストールする
コンポーネントの番号を入力し、ENTER キーを押してください

1. Sun ONE Identity Server 管理サービスとポリシーサービス
2. Sun ONE Identity Server 管理コンソールのみ
3. 既存の Directory Server を設定
4. Sun ONE Identity Server ドメイン間シングルサインオン
5. C 連合管理用の共通ドメインサービス

コンポーネントを選択し ENTER キーを押します [1] {"<" 戻る , "!" 終了 } 5
```

10. 次のプロンプトで、Sun ONE Web Server を指定します。

```
既存の Web Server
   既存の Web Server を使用しますか [no] {"<" 戻る , "!" 終了 }
```

   既存の Web Server を使用しますか [no]: Sun ONE Identity Server に付属の Sun ONE Web Server をインストールする場合は、Enter を押すかまたは no を入力します。一方、既存の Web Server を使用する場合は、yes を入力して Enter を押します。

11. 上の手順で no を選択した場合、つまり新しい Sun ONE Web Server をインストールし設定する場合は、次の情報を入力します。既存の Web Server を選択した場合は、この手順を省略して次に進みます。

```
Sun ONE Web Server 情報
   管理者 [admin] {"<" 戻る , "!" 終了 }:
   ポート [58888] {"<" 戻る , "!" 終了 }:
   パスワード :
   パスワードの確認 :
   サーバを実行するユーザ [nobody] {"<" 戻る , "!" 終了 }:
   サーバを実行するグループ [nobody] {"<" 戻る , "!" 終了 }:
```

管理者 [admin]: Sun ONE Web Server の管理者としてのユーザ名を入力します。Enter を押して、デフォルトのユーザ ID (admin) を選択します。

ポート [58888]: Identity Server サービスを実行する Web Server のポート番号を入力します。デフォルトのポート番号は 58088 です。デフォルトの名前を使用するには、Enter を押します。

パスワード : Web Server 管理者のパスワードを入力します。パスワードの指定には 8 文字以上必要です。

パスワードの確認 : 確認のためにもう一度 Web Server 管理者パスワードを入力します。

サーバを実行するユーザ [nobody]: Web Server を実行するユーザアカウントを入力します。Enter を押して、デフォルトユーザ nobody を選択します。デフォルト名を使用する場合は、Enter を押します。

サーバを実行するグループ [nobody]: 上述したユーザが属するグループを入力します。例 : nobody など。デフォルト名を使用する場合は、Enter を押します。

12. Common Domain Services Web Server をインストールし設定するには、次の情報を入力します。

```
共通ドメインサービス Web Server 情報
共通ドメインサービスを実行している Web Server について情報を入力してください
   ホスト名 [nila.Siroe.COM] {"<" 戻る , "!" 終了 }:
   Sun ONE Web Server ディレクトリ :
/opt/SUNWam/servers/https-nila.Siroe.COM
   Web Server ポート [80] {"<" 戻る , "!" 終了 }:
   CDS 配備 URI [common] {"<" 戻る , "!" 終了 }:
```

ホスト名 : 共通ドメインサービスを実行する Web Server の名前を入力します。デフォルト名を使用する場合は、Enter を押します。

Sun ONE Web Server ディレクトリ : Web Server がインストールされているディレクトリの完全パスおよび Web Server のインスタンス名を入力します。たとえば、/usr/iplanet/servers/https-nila.Siroe.COM のようになります。既存の Web Server を使用する場合は、インスタンス名の入力が要求されます。

Web Server ポート [80]: サービスが使用するポート番号を入力します。デフォルトのポート番号を使用する場合は、Enter を押します。

CDS 配備 URI [common]: 共通ドメインサービスへのアクセスに使用する URI を入力します。デフォルトの URI は common です。これは変更可能です。デフォルト名を使用する場合は、Enter を押します。

13. 次の画面表示で、今までの選択結果を確認します。

```
次のコンポーネントがインストールされます :
プロダクト : Sun ONE Identity Server
場所 : /opt
サイズ :85.84MB
--------------
Sun ONE Web Server
連合管理用の共通ドメインサービス
リソースパッケージ

インストールの準備完了
1. 今すぐインストール
2. 開始
3. 終了
   上のオプションを 1 つ選択してください [1] {"<" 戻る , "!" 終了 }
```

14. 1 を入力してインストールを開始します。

第 8 章

基本構成

この章では、Identity Server を最初に導入するときに通常実装する構成について説明します。

この章には次のトピックがあります。

- ドメイン間のシングルサインオンコンポーネント
- 同じ Directory Server に対する複数の Identity Server インスタンスのインストール
- ディレクトリレプリケーションと高可用性のサポート

ドメイン間のシングルサインオンコンポーネント

Identity Server の重要な機能であるドメイン間のシングルサインオン (CDSSO) 機能により、あるドメインで 1 回認証されたら、再認証なしでその他のドメインでアプリケーションを使用できます。次の 2 つの主要なコンポーネントが Identity Server に追加されて、ドメイン間のシングルサインオンを実装します。

- **ドメイン間コントローラ** : シングルサインオン (SSO) 情報が存在しない場合、コントローラは認証サービスに要求をリダイレクトします。存在する場合は、照会文字列に SSO 情報を付加して、CDSSO コンポーネントに要求をリダイレクトします。このコントローラは、Identity Server サービスをインストールすると自動的にインストールされます。このコントローラのデフォルト URL は次のとおりです。

  `http://`*`IS_host:IS_port`*`/URI/cdcservlet`

- **CDSSO コンポーネント** : CDSSO コンポーネントは、主に、このコンポーネントが配備されたドメインの cookie の設定に使用されます。CDSSO コンポーネントは、関連 DNS ドメインとは別にインストールされます。

CDSSO のインストール

ドメイン間のシングルサインオンを有効にするには、次の順序に従います。

1. Identity Server 管理およびポリシーサービスをインストールします。

   必要に応じて、第 4 章「新しい Directory Server を使用するインストール」または第 5 章「既存の Directory Server を使用する Identity Server のインストール」に記載されている手順を使用します。

2. すべての関連 DNS ドメインに CDSSO コンポーネントをインストールします。手順については、この章の「GUI を使用した CDSSO コンポーネントのインストール」または「コマンド行からの CDSSO コンポーネントのインストール」を参照してください。

3. 関連 DNS ドメインにインストールされた CDSSO コンポーネントを設定します。

   手順については、172 ページの「CDSSO コンポーネントを設定するには」を参照してください。

4. オプションで、CDSSO コンポーネントと連携して機能するように Identity Server Web エージェントを設定します。

   手順については、「CDSSO コンポーネントと連携するように Identity Server Web エージェントを設定するには」を参照してください。

GUI を使用した CDSSO コンポーネントのインストール

Identity Server インストールプログラムを使用して CDSSO コンポーネントをインストールできます。インストールプログラムを実行するには、root 権限が必要です。

注 このコンピュータの別のディレクトリに CDSSO がインストールされていないことを確認します。次のコマンドを使用して、既存のインスタンスを確認できます。

```
pkginfo | grep SUNWamcds
```

CDSSO コンポーネントをインストールするには、次の手順に従います。

1. 製品 CD から CDSSO をインストールする場合は、ソフトウェアをインストールするシステムのドライブに製品 CD を挿入します。

   製品をダウンロードした場合は、次のコマンドを使って製品バイナリファイルを解凍します。

   ```
   gunzip -dc binaryfile.tar.gz | tar -xvof -
   ```

   この場合、*binaryfile* をダウンロードした製品バイナリの名前に置き換える必要があります。

2. 別の端末ウィンドウを開き、`xhost +` と入力してマシンのアクセス制御を無効にします。

3. アプリケーションウィンドウで、次のコマンドのどちらかを使用して DISPLAY 変数を設定します。

   csh または tcsh を使用している場合、次のように入力します。

   ```
   setenv DISPLAY nila.Siroe.COM:0.0
   ```

   sh、ksh、または bash を使用している場合、次のように入力します。

   ```
   export DISPLAY=nila.Siroe.COM:0.0
   ```

   この場合、`nila` はインストールプログラムを実行しているマシンです。

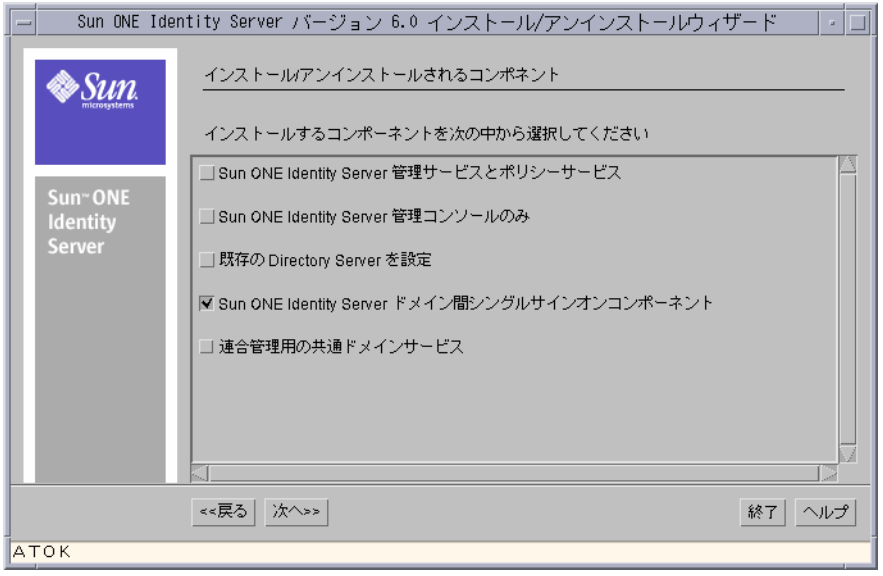
4. `setup` プログラムを実行します。このプログラムは、製品 CD の `/cdrom/idserv_60` ディレクトリにあります。製品バイナリをダウンロードした場合、このプログラムはバイナリファイルを展開したディレクトリにあります。

   コマンド行に `./setup` と入力します。インストールプログラムが起動し、開始パネルが開きます。

5. ライセンス契約を確認して同意します。

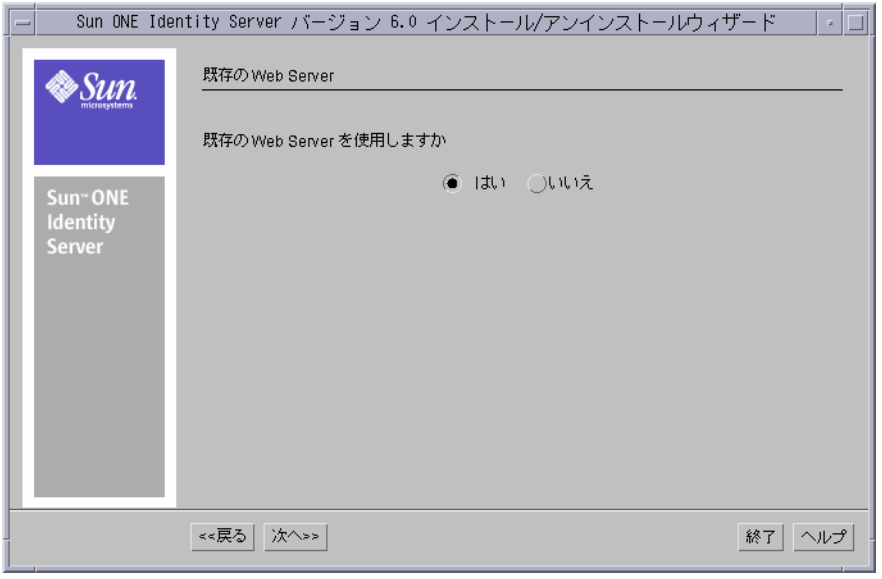
6. 「インストール / アンインストールされるコンポーネント」パネルで、「Sun ONE Identity Server ドメイン間シングルサインオンコンポーネント」だけを選択します。

図 8-1　「インストール / アンインストールされるコンポーネント」パネル



7. 「次へ」をクリックし、「既存の Web Server」パネルで次の情報を入力します。

図 8-2　「既存の Web Server」パネル

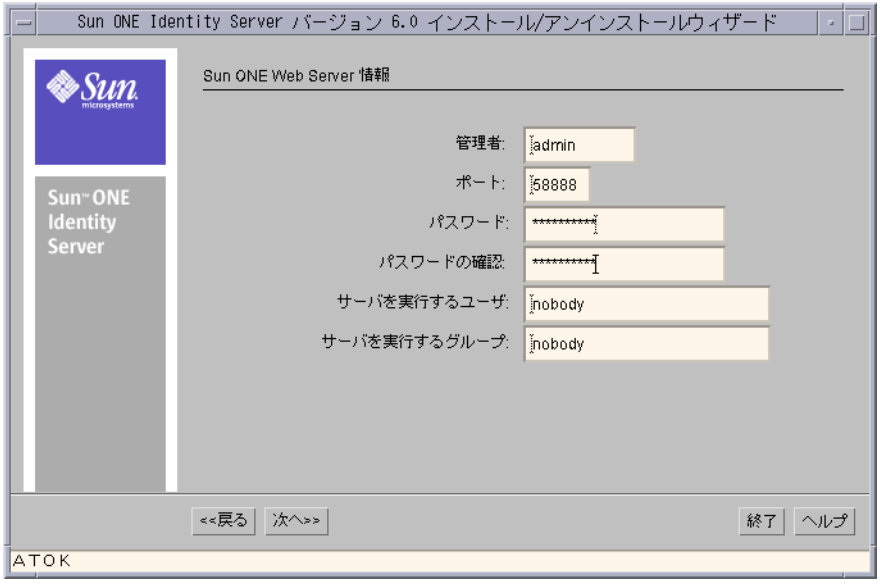


既存の Web Server を使用しますか : 既存の Sun ONE Web Server を使用する場合は、「はい」をクリックします。

Identity Server に付属の Sun ONE Web Server をインストールする場合は、「いいえ」をクリックします。

8. 「次へ」をクリックします。上の手順で「いいえ」を選択した場合は、次の情報を入力して、Identity Server 付属の Sun ONE Web Server をインストールし、設定します。「はい」を選択した場合は、この手順を省略して次に進みます。

図 8-3　「Sun ONE Web Server 情報」パネル



管理者 : Web Server を設定する管理者としてのユーザ名を入力します。フィールドに表示されるデフォルト名を上書きすることができます。

ポート : Web Server が使用するポート番号を入力します。フィールドに表示されるデフォルトのポート番号を上書きすることができます。

パスワード : 管理者としてのユーザパスワードを入力します。

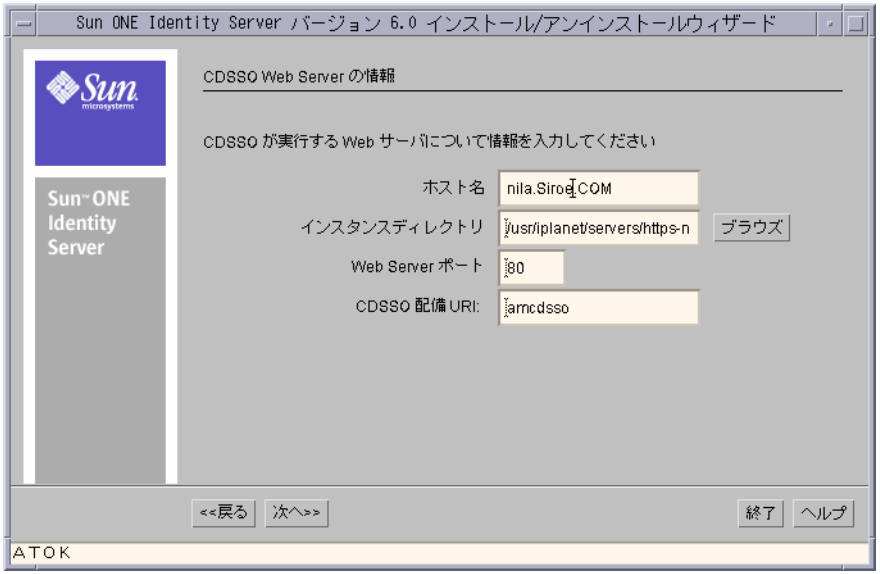
パスワードの確認 : 確認のためにもう一度パスワードを入力します。

サーバを実行するユーザ : Web Server を実行するユーザアカウントを入力します。(例 : nobody)

サーバを実行するグループ : 上述したユーザが属するグループを入力します。(例 : nobody)

9. 「次へ」をクリックし、「CDSSO Web Server の情報」パネルで、次の情報を指定して「次へ」をクリックします。

図 8-4　「CDSSO Web Server の情報」パネル



ホスト名：参加 DNS ドメインを管理するコンピュータの完全指定のドメイン名を入力します。

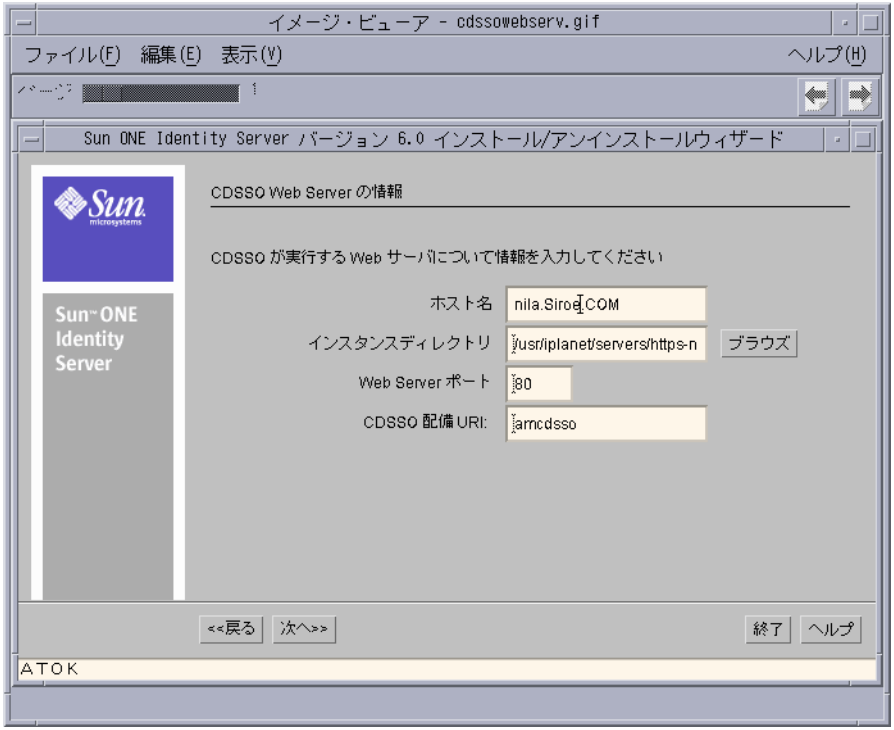
インスタンスディレクトリ：Web Server がインストールされているディレクトリの完全パスおよび Web Server のインスタンス名を入力します。このフィールドは、前の手順で既存の Web Server の使用を選択した場合にのみ有効です。

Web Server ポート：上で指定した Web Server のポート番号を入力します。

CDSSO 配置 URI: URI (Universal Resource Identifier) は、CDSSO コンポーネントが使用する HTML ページの格納場所を示します。URI 接頭辞を入力します。デフォルトは、`/amcdsso` です。

10. 「次へ」をクリックし、「Sun ONE Identity Server サービス情報」パネルで次の情報を入力します。

図 8-5　「Sun ONE Identity Server Sun ONE Identity Server サービス情報」パネル



Sun ONE Identity Server サービスホスト : Sun ONE Identity Server 管理およびポリシーサービスがインストールされているコンピュータシステムの完全指定名を入力します。

Sun ONE Identity Server サービスポート : Sun ONE Identity Server サービスを実行する Web Server のポート番号を入力します。

サービス配備 URI: Web Server は、URI (Universal Resource Identifier) 接頭辞の指定に従って、Sun ONE Identity Server サービスに関連付けられた HTML ページやほかの Web アプリケーション固有の情報 (クラス、jar などに関する情報) を検索します。Identity Server のインストール時に指定した URI 接頭辞を入力してください。デフォルトは、`/amserver` です。

11. 「現在選択されている設定」パネルで、入力した設定情報を確認します。変更が必要な場合は、「戻る」をクリックします。変更の必要がない場合は、「次へ」をクリックして処理を続行します。

12. 「インストールの準備完了」パネルで、インストール情報を確認します。変更が必要な場合は、「戻る」をクリックします。それ以外の場合は、「今すぐインストール」をクリックしてインストールを開始します。

13. 「インストールの要約」パネルで、「詳細」をクリックして、インストール中に処理された設定情報の詳細を確認します。「閉じる」をクリックしてプログラムを終了します。

コマンド行からの CDSSO コンポーネントのインストール

Identity Server インストールプログラムのコマンド行バージョンを使用して CDSSO をインストールすることもできます。インストールプログラムを実行するには、root 権限が必要です。

コマンド行から CDSSO コンポーネントをインストールするには、次の手順に従います。

1. `nodisplay` モードで `setup` プログラムを実行します。このプログラムは、製品 CD の `/cdrom/Idserv_60` ディレクトリにあります。製品バイナリをダウンロードした場合、このプログラムはバイナリファイルを展開したディレクトリにあります。

   コマンド行から `./setup -nodisplay` と入力します。

   Windows 上でインストールする場合は、次のコマンドを使用します。

   ```
   java am -nodisplay
   ```

2. 画面に表示される手順を確認します。インストーラが示すさまざまなプロンプトに対する応答方法の説明が表示されます。手順を確認したら、Enter を押してソフトウェアライセンス契約を確認します。インストールのどの段階でも、`<` を入力して前のプロンプトに戻ることができます。また、`!` を入力してインストールプログラムを終了することができます。
3. ライセンス契約を確認し、`y` (Yes) と入力してライセンス契約に同意します。
4. 画面に示された手順を確認し、インストーラが示すさまざまなプロンプトに対する応答方法を理解します。手順を確認したら、Enter を押してソフトウェアライセンス契約を確認します。
5. ライセンス契約を確認し、`yes` と入力してライセンス契約に同意します。
6. 次のプロンプトで、Identity Server をインストールするディレクトリを指定します。

```
Sun ONE Identity Server コンポーネントは、次のディレクトリにインストール
されます。そのディレクトリは、" インストールディレクトリ " と呼ばれます。この
ディレクトリを使用するには、Enter キーだけを押します。別のディレクトリを使用
するには、そのディレクトリの完全パスを入力した後に Enter キーを押します。

   Sun ONE Identity Server コンポーネントをインストールするディレクトリ
[/opt] {"<" 戻る , "!" 終了 }:
```

7. Enter を押して、コンポーネントをデフォルトディレクトリにインストールします。別のディレクトリにインストールする場合は、そのディレクトリへの絶対パスを入力して Enter を押します。そのディレクトリに対するアクセス権が存在することを確認します。
8. 次のプロンプトで、4 を入力します。

```
インストールするコンポーネントを次の中から選択してください。インストールする
コンポーネントの番号を入力し、Enter キーを押してください。

1. Sun ONE Identity Server 管理サービスとポリシーサービス
2. Sun ONE Identity Server 管理コンソールのみ
3. 既存の Directory Server を設定
4. Sun ONE Identity Server ドメイン間シングルサインオンコンポーネント
5. 連合管理用の共通ドメインサービス

   コンポーネントを選択し ENTER キーを押します [1] {"<" 戻る , "!" 終了 }
4
```

9. 次のプロンプトで、使用する Web Server を指定します。

```
既存の Web Server
   既存の Web Server を使用しますか [no] {"<" 戻る , "!" 終了 }
```

既存の Web Server を使用しますか [no]: 既存の Web Server を使用する場合は、yes を入力して Enter を押します。Sun ONE Identity Server に付属の Sun ONE Web Server をインストールする場合は、Enter を押します。

10. 新しい Sun ONE Web Server をインストールし、設定する場合は、次の情報を入力します。既存の Web Server を選択した場合は、この手順を省略して次に進みます。

```
Sun ONE Web Server 情報

管理者 [admin] {"<" 戻る , "!" 終了 }:
ポート [58888] {"<" 戻る , "!" 終了 }:
パスワード :
パスワードの確認 :
サーバを実行するユーザ [nobody] {"<" 戻る , "!" 終了 }:
サーバを実行するグループ [nobody] {"<" 戻る , "!" 終了 }:
```

管理者 [admin]: Sun ONE Web Server のサーバ管理者としてのユーザ名を入力します。Enter を押して、デフォルトのユーザ ID (admin) を選択します。

ポート [58888]: Identity Server サービスを実行する Web Server のポート番号を入力します。デフォルトのポート番号は 58088 です。デフォルトのポート番号を選択する場合は Enter を押します。

パスワード : Web Server 管理者のパスワードを入力します。パスワードの指定には 8 文字以上必要です。

パスワードの確認 : 確認のためにもう一度 Web Server 管理者パスワードを入力します。

サーバを実行するユーザ [nobody]: Web Server を実行するユーザアカウントを入力します。Enter を押して、デフォルトユーザ nobody を選択します。デフォルト名を使用する場合は、Enter を押します。

サーバを実行するグループ [nobody]: 上述したユーザが属するグループを入力します。例 : nobody など。デフォルト名を使用する場合は、Enter を押します。

11. 次の情報を入力して、CDSSO Web Server を設定します。

```
CDSSO Web Server の情報
CDSSO が実行する Web サーバについて情報を入力してください

   ホスト名 [nila.Siroe.COM] {"<" 戻る , "!" 終了 }
   インスタンスディレクトリ :
/opt/SUNWam/servers/https-nila.Siroe.COM
   Web Server ポート [80] {"<" 戻る , "!" 終了 }
   CDSSO 配備 URI [amcdsso] {"<" 戻る , "!" 終了 }:
```

ホスト名 : Web Server を管理するコンピュータの完全指定のドメイン名を入力します。

インスタンスディレクトリ : CDSSO Web Server をインストールするディレクトリの完全パスおよび Web Server のインスタンス名を入力します。新しく Web Server をインストールすると、インストールプログラムによりデフォルトのディレクトリとインスタンス名が表示されます。デフォルトをそのまま使用するか、あるいは別のインスタンスディレクトリを入力することができます。ただし、前の手順で既存の CDSSO Web Server を指定するよう選択した場合は、ここでその Web Server へのパスを入力する必要があります。

Web Server ポート : 上で指定した Web Server のポート番号を入力します。

CDSSO 配備 URI: URI (Universal Resource Identifier) は、CDSSO コンポーネントが使用する HTML ページの格納場所を示します。URI 接頭辞を入力します。デフォルトは、`/amcdsso` です。

12. 次の情報を入力して、Identity Server サービスを設定します。

```
Sun ONE Identity Server サービス情報
   Sun ONE Identity Server サービスホスト [seine.Sesta.COM] {"<" 戻る , "!"
終了 }:
   Sun ONE Identity Server サービスポート [58080] {"<" 戻る , "!" 終了 }:
   サービス配備 URI [amserver] {"<" 戻る , "!" 終了 }:
```

Sun ONE Identity Server サービスホスト : Sun ONE Identity Server 管理およびポリシーサービスがインストールされているコンピュータシステムの完全指定名を入力します。

Sun ONE Identity Server サービスポート : Sun ONE Identity Server サービスを実行する Web Server のポート番号を入力します。

サービス配備 URI: Web Server は、URI (Universal Resource Identifier) 接頭辞の指定に従って、Sun ONE Identity Server サービスに関連付けられた HTML ページやほかの Web アプリケーション固有の情報 (クラス、jar などに関する情報) を検索します。Identity Server のインストール時に指定した URI 接頭辞を入力してください。デフォルトは、`/amserver` です。

13. 次のプロンプトで、1 を入力してインストールを開始します。

```
ディスク容量を調べています ....
次のコンポーネントがインストールされます :
プロダクト : Sun ONE Identity Server
場所 : /opt
サイズ : 85.83 KB
--------------------------------
Sun ONE Web Server
Sun ONE Identity Server ドメイン間シングルサインオン
リソースパッケージ

インストールの準備完了
1. 今すぐインストール
2. 開始
3. 終了
   上のオプションを 1 つ選択してください [1] {"<" 戻る , "!" 終了 }
```

CDSSO コンポーネントを設定するには

1. インストールされた CDSSO コンポーネントの `AMConfig.properties` ファイルを編集します。このファイルは IS_root/SUNWam/web-apps/cdsso/WEB-INF/lib ディレクトリにあります。

   `com.iplanet.services.cdsso.CDCURL` プロパティを、Identity Server サービスを実行中のドメイン間コントローラサービスの URL に設定します。次に例を示します。

   ```
   com.iplanet.services.cdsso.CDCURL =
   ```
   http(s)://*IS_host:IS_port*/services/cdcservlet

2. インストールされた CDSSO コンポーネントの `CDSSO.properties` ファイルを編集します。このファイルは IS_root/SUNWam/web-apps/cdsso/WEB-INF/classes ディレクトリにあります。

   `com.iplanet.services.cdsso.cookieDomain` プロパティを、CDSSO コンポーネントを管理するドメイン名に設定します。次に例を示します。

   ```
   com.iplanet.services.cdsso.cookieDomain = .sales.com
   ```

   CDSSO コンポーネントは、`sales.com` ドメインで管理されます。

   `com.iplanet.services.cdsso.cookieDomain` プロパティは、cookie が設定される CDSSO コンポーネントが実行されているドメイン名のリストを指定します。プロパティフィールドを空白のままにすると、cookie ドメインは CDSSO コンポーネントの管理ドメインであるとみなされます。cookie ドメインは 1 個ずつコンマ (,) で区切ります。

CDSSO コンポーネントと連携するように Identity Server Web エージェントを設定するには

リモート Web サーバにインストールされた Identity Server エージェントを構成して、DNS 参加ドメインにインストールされた CDSSO コンポーネントと連携するように設定できます。

1. エージェントの `AMAgent.properties` ファイルを編集します。エージェントのドメインのドメイン間シングルサインオンサービス URL を指すように `com.sun.am.policy.agents.url.loginURL` のプロパティを変更します。次に例を示します。

   `com.sun.am.policy.agents.url.loginURL` = http://*CDSSO_host:CDSSO_port*/CDSSO_URI/cdsso

   この場合、`loginURL` は CDSSO コンポーネントの URL です。

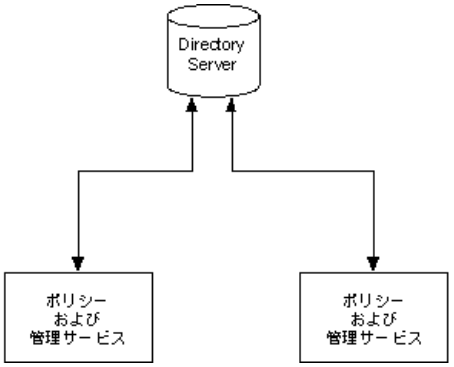
2. 適用されていないエージェントのリストに CDSSO URL を追加します。

同じ Directory Server に対する複数の Identity Server インスタンスのインストール

パフォーマンスの向上、ディレクトリのレプリケーション、またはエージェントのフェイルオーバのために、Identity Server の複数のインスタンスをこの Directory Server にインストールできます。初めて Identity Server インストールプログラムを実行するときは、通常 Sun ONE Identity Server ポリシーおよび管理サービスをインストールします。このオプションを使用すると、自動的に Directory Server がインストールされます。これがマスター Directory Server になります。同じマスターディレクトリに複数の Identity Server をインストールする場合は、`ammultiserverinstall` スクリプトを実行してください。

図 8-6 では、単一の Directory Server にインストールされた 2 つの Identity Server インスタンスを示します。

図 8-6　単一の Directory Server にインストールされた 2 つの Identity Server インスタンス



同じ Directory Server に複数の Identity Server インスタンスをインストールするには

複数の Identity Server インスタンスを作成およびインストールするには、ルートアクセス権が必要です。

1. 次のディレクトリに移動します。

   `cd` *IS_root*`/SUNWam/bin`

2. コマンド行に次のコマンドを入力します。

   `./ammultiserverinstall` *instance_name port_number*

   この場合、*instance_name* はこれから作成する新しい Identity Server インスタンス、*port_number* はそのポート番号です。

   新しいインスタンスをインストールすると、次のファイルおよびディレクトリが作成されます。

   - 新しい `amserver` スクリプトファイル :

     /IS_root`/SUNWam/bin/`*amserver.instance_name*

   - 新しい `AMConfig.properties` ファイル :

     /IS_root`/SUNWam/lib/AMConfig-instance_name.properties`

   - 新しい Web サーバインスタンスディレクトリ :

     /IS_root`/SUNWam/servers/https-instance_name`

Identity Server インスタンスの起動

- 単一の Identity Server インスタンスを起動するには、次のコマンドを入力します。

```
./amserver.instance_name start
```

- すべての Identity Server インスタンスを起動するには、次のコマンドを入力します。

```
./amserver startall
```

Identity Server インスタンスの停止

- 単一の Identity Server インスタンスを停止するには、次のコマンドを入力します。

```
./amserver.instance_name stop
```

- すべての Identity Server インスタンスを停止するには、次のコマンドを入力します。

```
./amserver stopall
```

Identity Server インスタンスの削除

- Identity Server インスタンスを削除するには、次のコマンドを入力します。

```
./amserver delete instance_name
```

ディレクトリレプリケーションと高可用性のサポート

レプリケートされたサーバ間の負荷均衡とユーザに近いレプリケートされたサーバの検索が、企業のサーバの性能と応答時間を向上させる 2 つの方法です。Identity Server の導入でディレクトリレプリケーションアグリーメントを実装して、Identity Server サーバとサービスの可用性と性能を高めることができます。シングルサプライヤ構成またはマルチサプライヤ構成で Identity Server ディレクトリサーバをセットアップできます。また、iPlanet Directory Access Router などの負荷均衡アプリケーションを設定して Identity Server と連携できます。

レプリケーションに関する検討事項

Identity Server をインストールする前に、レプリケーション用のディレクトリサーバを設定します。これにより、サプライヤとコンシューマのデータベースが始めから同期され、レフェラルや更新が正しく行われていることを確認できます。情報は、各 Identity Server データベースで同じである必要があります。

レプリケーション用の Identity Server をインストールする場合は、Directory Server の各インスタンスおよび Identity Server の各インスタンスに、以下の項目に同じ値を指定してください。

- ディレクトリマネージャ
- ディレクトリマネージャのパスワード
- Directory Server の管理者 ID
- サーバ管理者のパスワード
- ベース接尾辞
- デフォルトの組織

Identity Server の導入でディレクトリレプリケーションを実装できない場合もあります。たとえば、認証サーバのホスト名や IP アドレスが同じでなければならない場合などです。この場合、地理的に離れているレプリケートされた Identity Server サーバは使用できません。リモートサーバは、それぞれの LAN に対してだけローカルなサーバに対して認証を実行できません。

Directory Server のレプリケーションの計画と実装に関する総合的な情報については、Sun ONE Directory Server の『導入ガイド』および『インストールガイド』を参照してください。これらのガイドは、インターネット上の次のアドレスでアクセスできます。

`http://docs.sun.com/db/prod/s1dirsrv`

ディレクトリレプリケーションをサポートするための Identity Server の設定

シングルサプライヤまたはマルチサプライヤのレプリケーションと連携するように Identity Server を設定できます。この節で示されているそれぞれの構成で同じ手順に従います。このマニュアルの 179 ページの「ディレクトリレプリケーションと連携するように Identity Server を設定するには」を参照してください。

図 8-7 は、コンシューマが読み取り専用のデータベースであるシングルサプライヤ構成を示しています。書き込み操作の要求は、サプライヤデータベースに対して照会されます。この設定は、作業負荷を複数のディレクトリに分散することにより、サーバの性能をある程度向上させます。

図 8-7　シングルサプライヤレプリケーション

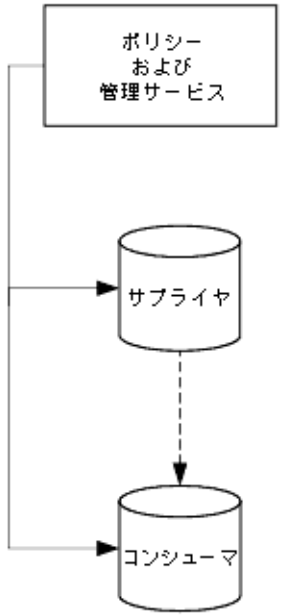


図 8-8 は、Identity Server の複数のインスタンスを使用するマルチサプライヤ構成を示しています。この構成では、フェイルオーバ保護と高可用性が提供されるため、サーバの性能がさらに向上します。

図 8-8 マルチマスターレプリケーション (MMR) とも呼ばれるマルチサプライヤ構成

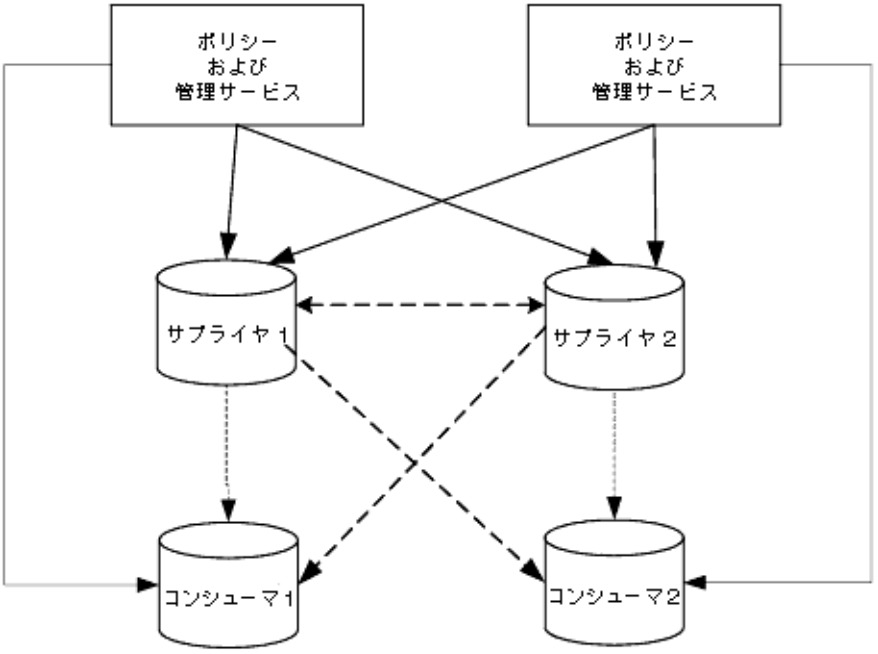
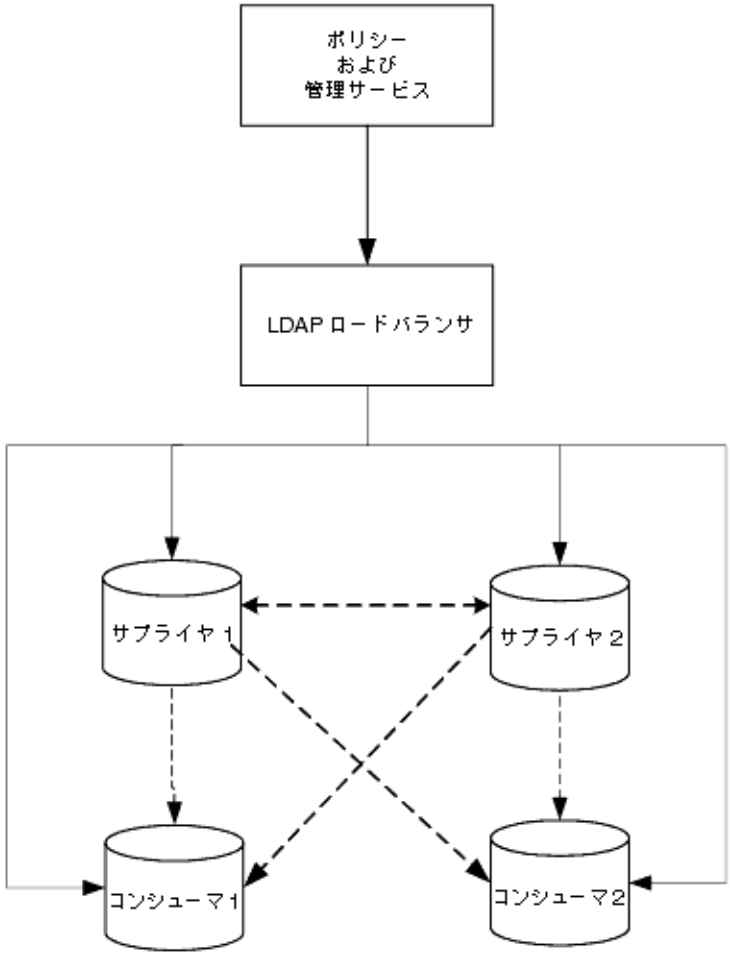


図 8-9 は、iPlanet Access Router を含むマルチサプライヤ構成を示しています。この構成は、Identity Server がサポートするフェイルオーバ、高可用性、および負荷均衡の管理を最大限に活用しています。

図 8-9　負荷均衡処理を行うマルチサプライヤレプリケーション



ディレクトリレプリケーションと連携するように Identity Server を設定するには

次の手順に従って、Identity Server ディレクトリツリーのルートレベル、つまり最上位レベルでレプリケーションを設定します。この手順に従って、デフォルトの組織のレベルでレプリケーションを設定することもできます。

1. サプライヤとコンシューマの Directory Server (バージョン 5.1) をインストールします。手順については、Directory Server の『インストールガイド』を参照してください。

2. サプライヤとコンシューマの Directory Server 間でレプリケーションアグリーメントを設定してから、ディレクトリのレフェラルや更新が正しく行われていることを確認します。手順については、Directory Server の『管理者ガイド』を参照してください。
3. 5.1 より前の既存の Directory Server のユーザデータを持つ Identity Server を使用する場合は、次の処理に進む前に、ユーザデータを移行して、ディレクトリ情報ツリー (DIT) を変更する必要があります。このマニュアルの第 5 章「既存の Directory Server を使用する Identity Server のインストール」に記載されている詳細手順に従います。手順 5 に進んでください。
4. 初めて Identity Server および Directory Server を導入する場合、または既存のユーザデータを Identity Server で使用する予定でない場合は、Identity Server インストールプログラムを実行して Identity Server 管理およびポリシーサービスをインストールします。

   インストール中に、既存の Directory Server を使用するかどうかを尋ねられます。「はい」と答え、手順 1 でインストールしたサプライヤ Directory Server のホスト名とポート番号を指定します。

   詳しい手順については、第 5 章の 80 ページの「既存の Directory Server を使用する Identity Server のインストール」を参照してください。
5. Identity Server 管理およびポリシーサービスがインストールされているサーバで、次のファイルを変更します。

   IS_root/SUNWam/lib/AMConfig.properties

   a. 手順 1 でインストールしたコンシューマ Directory Server のホスト名とポート番号を反映するように次のプロパティを変更します。
      - com.iplanet.am.directory.host
      - com.iplanet.am.directory.port

   b. 次のプロパティを変更します。
      - replica.enabled=true
      - com.iplanet.am.replica.retries

        要求されたエントリが見つからない場合は、Identity Server が同じ要求を繰り返す回数を指定します。
      - com.iplanet.am.replica.delay.between.retries

        Identity Server が許可する再試行間隔をミリ秒単位で指定します。

6. 有効にした各 Identity Server 認証モジュールで、手順 1 でインストールしたコンシューマディレクトリを指定する必要があります。この手順では、LDAP 認証モジュールを例として使用しています。

   a. Identity Server コンソールの「表示」フィールドで、「サービス管理」を選択します。

   b. 「サービス名」列の「認証」で、設定し直す必要があるモジュールを探します。「プロパティ」列で、設定し直す必要のあるモジュールに対応する矢印をクリックします。

   c. 右側の区画に、**「LDAP サーバとポート」**という名前のフィールドが 2 つあります。

      - **「LDAP サーバとポート」**という名前の最初のフィールドで、プライマリ (コンシューマ) Directory Server のホスト名とポート番号を入力します。
        例 : `consumer1.madisonparc.com:389`
      - **「LDAP サーバとポート」**という名前の 2 番目のフィールドで、セカンダリ (サプライヤ) ディレクトリのホスト名とポート番号を入力します。
        例 : `supplier1.madisonparc.com:399`

   d. 「実行」をクリックします。

7. 次の *IS_root*`/SUNWam/config/ums/serverconfig.xml` で、手順 1 でインストールしたコンシューマディレクトリのホスト名とポート番号を指定します。次に例を示します。

```
<iPlanetDataAccessLayer>
<ServerGroup name="default" minConnPool="1"
maxConnPool="10">
<Server name="Server1"
host="consumer1.madisonparc.com" port="389"
type="SIMPLE" />
```

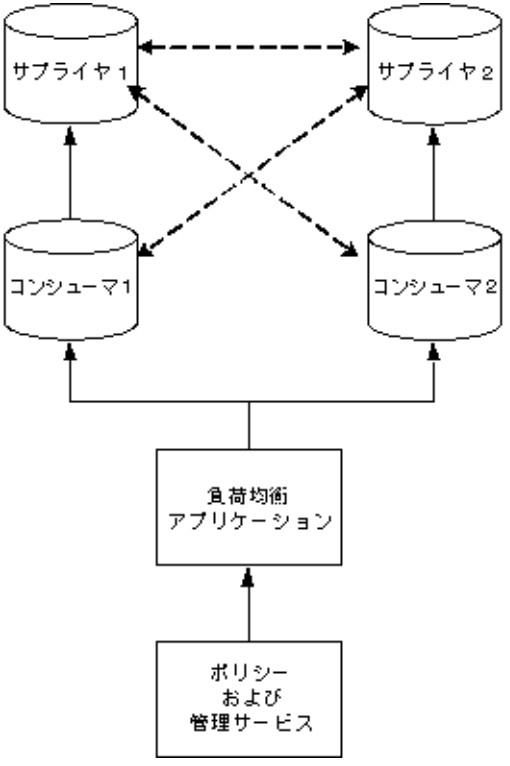
8. 次のコマンドを使って、Identity Server を再起動します。

   ```
   /etc/init.d/amserver start
   ```

Identity Server と連携する LDAP 負荷均衡アプリケーションの設定

iPlanet Directory Access Router などの LDAP 負荷均衡アプリケーションを設定して Identity Server と連携させることができます。iPlanet Directory Access Router は、設定された一連のディレクトリサーバ間でダイナミックに LDAP 処理の負荷均衡を行います。1 つ以上のディレクトリサーバが使用できなくなると、負荷が残りのサーバ間でバランスよく分散し直されます。ディレクトリサーバが復旧すると、負荷はバランスよくダイナミックに割り当てし直されます。

図 8-10　負荷均衡管理を行うマルチマスターレプリケーション



LDAP 負荷均衡アプリケーションを使用すると、Identity Server が提供する基本的なレベルを超える高可用性とディレクトリのフェイルオーバ保護が可能になります。たとえば、iPlanet Directory Access Router を設定する際、1 台のサーバが使用できなくなったときに各サーバに分散し直す負荷の割合を指定できます。iPlanet Directory Access Router は要求トラフィックの管理を続行し、すべてのバックエンド LDAP サーバが使用できなくなるとクライアントの照会を拒否し始めます。

これに比べて、Identity Server の高可用性機能は、同じように厳密に設定または管理できません。ただし、iPlanet Directory Access Router などの LDAP 負荷均衡アプリケーションを追加すると、Identity Server はすべての要求をその負荷均衡アプリケーションにシームレスに転送するので全体的な管理が向上します。

負荷均衡アプリケーションのインストールを選択する場合、アプリケーションを認識するように Identity Server を設定する必要があります。

負荷均衡アプリケーションと連携するように Identity Server を設定するには

1. 次の手順を実行する前に、次のことを行う必要があります。
   - レプリケーション用の Directory Server をセットアップします。ディレクトリレプリケーションの総合的な情報と詳しいセットアップ手順については、『Sun ONE Directory Server 管理者ガイド』の「複製処理の管理」を参照してください。
   - LDAP 負荷均衡アプリケーションをインストールおよび設定します。製品に付属のマニュアルに記載されている手順に従ってください。
2. 手順 1 でインストールしたコンシューマ Directory Server のホスト名とポート番号を反映するように、*IS_root*`/SUNWam/lib/AMconfig.properties` ファイルの次のプロパティを変更します。
   - `com.iplanet.am.directory.host`
   - `com.iplanet.am.directory.port`
3. 有効にした各 Identity Server 認証モジュールで、手順 1 でインストールしたコンシューマディレクトリを指定する必要があります。この手順では、LDAP 認証モジュールを例として使用しています。
   a. Identity Server コンソールの「表示」フィールドで、「サービス管理」を選択します。
   b. 「サービス名」列の「認証」で、設定し直す必要があるモジュールを探します。「プロパティ」列で、設定し直す必要のあるモジュールに対応する矢印をクリックします。
   c. 右側の区画に、**「LDAP サーバとポート」**という名前のフィールドが 2 つあります。

- 「LDAP サーバとポート」という名前の最初のフィールドで、次の形式でプライマリ (コンシューマ) Directory Server のホスト名とポート番号を入力します。

  proxyhostname:port

- 「LDAP サーバとポート」という名前の 2 番目のフィールドには、何も入力しません。

d. 「実行」をクリックします。

4. *IS_root*/SUNWam/config/ums/serverconfig.xml で、手順 1 でインストールしたコンシューマディレクトリのホスト名とポート番号を指定します。

   次に例を示します。

```
<iPlanetDataAccessLayer>
<ServerGroup name="default" minConnPool="1"
maxConnPool="10">
<Server name="Server1"
host="idar.madisonparc.com" port="389"
type="SIMPLE" />
```

5. 次のコマンドを使って、Identity Server を再起動します。

   ```
   /etc/init.d/amserver start
   ```

第 9 章

サイレントインストール

Identity Server は、GUI インストールおよびコマンド行からのインストール (CLI) に加えて、サイレントインストールを行うことができます。この章では、サイレントインストールの実行手順を説明します。この章には次のトピックがあります。

- サイレントインストールについて
- Solaris 上の StateFile の生成
- Statefile を使用したインストール
- Windows 上の StateFile の生成
- Statefile を使用したインストール
- Statefile の変数

サイレントインストールについて

サイレントインストールでは、インストールスクリプトを提供することにより、Identity Server をインストールできます。サイレントインストールを実行するときに、通常は対話的な操作でセットアッププログラムに入力するすべての項目を、*StateFile* を使って提供することができます。こうすると、各インスタンスに同じパラメータを使用して複数の Identity Server インスタンスをインストールする場合に、時間を短縮することができ、有効です。

サイレントインストールには、簡単な 2 つの処理があります。まず、インストール処理とすべての入力項目を記録した *Statefile* を生成します。次に、*StateFile* を入力ソースとして、インストールプログラムを実行します。

Solaris 上の StateFile の生成

Solaris 上で *StateFile* を生成するには、次の手順に従います。

1. インストールプログラムのあるディレクトリに移動します。
2. 次のコマンドを入力します。

   ```
   # ./setup -saveState StateFile
   ```

   Statefile に好きな名前を指定できます。
3. インストールプログラムを続行します。プロンプトに対する応答が *StateFile* に記録されます。

   インストールが完了すると、`setup` と同じディレクトリに *StateFile* が作成されます。

Statefile を使用したインストール

サイレントインストールを実行するには、次の手順に従います。

次のコマンドを入力して、サイレントインストールを実行します。

```
# ./setup -nodisplay -noconsole -state StateFile
```

ユーザからは見えない状態でインストールが実行されます。インストールが完了すると、プログラムが自動的に終了し、プロンプトが表示されます。*Statefile* で指定したインストールディレクトリに移動して、すべてのファイルがコピーされているかどうかを確認します。

Windows 上の StateFile の生成

Windows 2000 上で *StateFile* を生成するには、次の手順に従います。

1. `setup` プログラムのあるディレクトリから、インストールプログラムを実行します。DOS のコマンドウィンドウを開いて、次のコマンドを入力します。

   ```
   java am -saveState StateFile
   ```
2. インストールプログラムを続行します。プロンプトに対する応答が *StateFile* に記録されます。

インストールが完了すると、`setup.exe` と同じディレクトリに *StateFile* が作成されます。

Statefile を使用したインストール

1. 次のコマンドを入力します。

```
java am -nodisplay -noconsole -state StateFile
```

ユーザからは見えない状態でインストールが実行されます。インストールが完了すると、プログラムが自動的に終了し、プロンプトが表示されます。*Statefile* で指定したインストールディレクトリに移動して、すべてのファイルがコピーされているかどうかを確認します。

Statefile の変数

次の表は、`Statefile` で使用する変数とその簡単な説明および使用可能な値を示します。

表 9-1 Statefile 変数の説明

変数	説明	値
defaultInstallDirectory	インストールプログラムで入力の必要な、Identity Server をインストールするデフォルトディレクトリを表示する	ディレクトリの絶対パス。たとえば、Solaris の場合 `/opt`、Windows の場合 `c:\SunONE\SunONEIS`
currentInstallDirectory	ユーザが選択した、Identity Server をインストールするディレクトリを表示する	ディレクトリの絶対パス。たとえば、`/identity60`
com.iplanet.install.panels.common.ComponentPanel.selectedcomponents	ユーザが選択した、インストール用の Identity Server コンポーネントの名前を表示する	コンポーネントの名前。たとえば、Sun ONE IdentityServerManagementandPolicyServices SunONEIdentityServerCrossDomainSingleSignon
CUSTOM_JDK	既存の JDK を使用するか、あるいは Identity Server 6.0 に付属の JDK をインストールするよう選択したかを示す	true または false カスタム JDK を指定した場合 true Identity Server に付属の JDK のインストールを選択した場合 false
JDK_PATH	Solaris プラットフォームでの JDK の相対パスを表示する	java

表 9-1 Statefile 変数の説明 (続き)

変数	説明	値
JDK_BASE_DIR	Java SDK がインストールされているディレクトリを表示する	JDK ディレクトリの絶対パス。たとえば、/identity60/SUNWam/java
IWS_INSTALL	Identity Server 6.0 によって配布された新しい Web Server に CDSSO コンポーネントと共通ドメインサービスをインストールしたかどうかを表示する	true または false 新しい Web Server にこれらのコンポーネントをインストールした場合は true
IWS_ADMIN_ID	Sun ONE Web Server を管理する管理者としてのユーザ名を表示する	デフォルト値は admin。変更可能
IWS_ADMIN_PORT	Sun ONE Web Server が使用するポート番号を表示する	デフォルトは 58888。変更可能
IWS_ADMIN_PASSWD	Web Server 管理者のパスワードを表示する	パスワードの指定には 8 文字以上必要
SYS_USR	Web Server を実行する UNIX ユーザアカウントを表示する	デフォルトユーザは nobody。変更可能。この変数は Windows で作成された Statefile では使用できない
SYS_GRP	上述のユーザが属する UNIX グループを表示する	デフォルトグループは nobody。変更可能。この変数は Windows で作成された Statefile では使用できない
CDSSO_BASE_WSDIR	Sun ONE Web Server がインストールされているディレクトリのパスを表示する	
CDSSO_HOST	CDSSO コンポーネントをインストールしたコンピュータの FQDN を表示する	通常、値は *host.siroe*.com の形式となる
CDSSO_WSDIR	Web Server インスタンスを格納するディレクトリのパスを表示する	インスタンス名を含む絶対パス。たとえば、/*Is_root*/SUNWam/servers/https-*host.siroe*.com
CDSSO_PORT	CDSSO コンポーネントが使用する Web Server のポート番号を表示する	デフォルト値は 80
CDSSO_PROTOCOL	CDSSO コンポーネントが使用するプロトコルを表示する	http または https。デフォルト値は http
CDSSO_DEPLOY_URI	CDSSO にアクセスするための URI を表示する	デフォルトは amcdsso。変更可能

表 9-1 Statefile 変数の説明 (続き)

変数	説明	値
WS_INSTANCE	Web Server インスタンスの名前を表示する	デフォルト値は https-*host.siroe*.com
DSAME_SERVER	Sun ONE Identity Server を実行するホストマシンの FQDN を表示する	通常、値は *host.siroe*.com の形式となる
DSAME_PORT	Identity Server サービスを実行する Web Server が使用するポート番号を表示する	通常、デフォルトは 58080
DSAME_PROTOCOL	Identity Server が使用するプロトコルを表示する	http または https。デフォルトは http
SERVER_DEPLOY_URI	Identity Server サービスにアクセスするための URI を表示する	デフォルトは amserver。変更可能
CDS_HOST	共通ドメインサービスをインストールしたマシンの FQDN を表示する	*host.siroe*.com
CDS_WSDIR	共通ドメインサービスが使用する Web Server インスタンスのパスを表示する	Web Server インスタンス名を含む絶対パス。たとえば、/Is-root/SUNWam/servers/https-siroe60.siroe.com
CDS_PORT	共通ドメインサービスが使用するポート番号を表示する	通常、デフォルトは 58080
CDS_PROTOCOL	共通ドメインサービスが使用するプロトコルを表示する	http または https。デフォルトは http
CDS_DEPLOY_URI	Web Server の共通ドメインサービスにアクセスするための URI を表示する	デフォルトは common。変更可能
CDS_BASE_WSDIR	共通ドメインサービスが使用する Web Server ディレクトリのパスを表示する	*IS_root*/SUNWam/servers
DSAME_HOST	Directory Server をインストールしたホスト名を表示する。ホスト名は、通常 FQDN の最初のラベルとなる	*host*
DSAME_DEF_DOMAIN	Directory Server をインストールしたドメインを表示する	ドメイン名。例 : *siroe*.com
DSAME_FULL_DOMAIN	Identity Server をインストールしたドメイン名 (ホスト名なし) を表示する	*siroe*.com

表 9-1 Statefile 変数の説明 (続き)

変数	説明	値
DSAME_SUB_DOMAIN	FQDN のサブドメインラベルを表示する。サブドメインは FQDN の 2 番目のラベル。たとえば、*nila.country.siroe*.com の場合、*country* がサブドメインとなる	サブドメインがある場合にのみ必要
DEFAULT_ORG1	DSAME_DEF_DOMAIN と同じ値を表示する	ドメイン名。 例 : *siroe*.com
EXIST_DIT_SCHEMA	既存の DIT およびスキーマを使用するよう選択したかどうかを表示する	true または false
ADMIN_COMPONENT_SELECTED	Identity Server コンソールを配備するよう選択したかどうかを表示する	true または false
CONSOLE_DEPLOY_URI	Identity Server コンソールにアクセスするための URI を表示する	デフォルトは *amconsole*。変更可能
DSAME_CONSOLE	Identity Server コンソールをインストールしたコンピュータの FQDN	*nila.siroe.com*
DSAME_CONSOLE_HOST	Identity Server コンソールを管理するマシンの名前を表示する	ホストマシンの名前
CONSOLE_PROTO	Identity Server コンソールが使用するプロトコルを示す	http
DSAME_CONSOLE_PORT	Identity Server コンソールが使用するポート番号を示す	58080
DSAME_CONSOLE_DEF_DOMAIN	Identity Server をインストールしたドメインを表示する	*siroe*.com
DSAME_CONSOLE_FULL_DOMAIN	Identity Server コンソールをインストールしたドメインを表示する。これは、通常 FQDN の最後の 2 つのラベルで識別される	*siroe*.com
DSAME_CONSOLE_SUB_DOMAIN	FQDN の 2 番目のラベルを表示する	指定するサブドメインがある場合にのみ必要
USE_DSAME_SERVICES_WEB_CONTAINER	新しいまたは既存の Identity Server サービスとともに Identity Server コンソールをインストールしたかどうかを示す	Identity Server サービスとともに Identity Server コンソールをインストールした場合、値は 1。Identity Server コンソールだけをインストールした場合、値は 0 (ゼロ)

表 9-1 Statefile 変数の説明 (続き)

変数	説明	値
DIT_COMPLIANCE	既存の Identity Server 準拠 DIT があるかどうかを示す	false
DS_ALREADY_EXISTS	既存の Directory Server を使用するよう指定したかどうかを示す	true または false
LOAD_DIT	Identity Server 準拠 DIT を読み込むように選択したかどうかを示す	yes または no
AUTO_LOAD	インストール時に、Identity Server 6.0 準拠 DIT またはスキーマを読み込むように選択したかどうかを示す	DIT またはスキーマを読み込むように選択した場合は true、それ以外の場合は false
CUSTOM_DIRECTORY	既存の Directory Server を格納するカスタムディレクトリを指定したかどうかを示す	true または false
DS_ROOT_SUFFIX	ディレクトリツリーで定義したルート接尾辞を表示する	dc=*siroe* dc=com, o=*siroe*.com
DC_TREE	DIT で定義したルート接尾辞を表示する	dc=*siroe*, dc=com, o=*siroe*.com
ORG_BASE	DS_ROOT_SUFFIX と同じ値を表示する	
DS_SERVER	Directory Server をインストールしたコンピュータの FQDN を表示する	*host*.*siroe*.com
DS_HOST	Directory Server をインストールしたコンピュータの名前を表示する	コンピュータの名前
DS_PORT	Directory Server が使用するポートを表示する	デフォルトは 389。1 ～ 65535 の任意の番号に変更可能
DS_INSTALL_DIR	Directory Server をインストールしたディレクトリのパスを表示する	デフォルトは `/usr/iplanet/servers`
DS_ROOT_DN	DIT で定義した DN を表示する	cn=Directory manager
DS_ROOT_PASSWD	Directory Server の管理者ユーザとして設定したパスワードを表示する	8 文字以上の長さのパスワード
LOCAL_IDS	既存の Directory Server が、ローカルにインストールされているか、リモートホストにインストールされているかを示す	Directory Server がローカルホストにインストールされている場合は true、リモートホストにインストールされている場合は false

表 9-1 Statefile 変数の説明 (続き)

変数	説明	値
ORG_OBJECT_CLASS	既存の DIT の組織用に定義されたマーカーオブジェクトクラスを表示する この変数は、既存の Directory Server に対して Identity Server をインストールする場合にのみ設定が必要	デフォルトは organization
ORG_NAMING_ATTR	既存の DIT の組織を定義するために使用するネーミング属性を表示する この変数は、既存の Directory Server に対して Identity Server をインストールする場合にのみ設定が必要	o, dc
USER_OBJECT_CLASS	既存の DIT のユーザ用に定義されたオブジェクトクラスを表示する この変数は、既存の Directory Server に対して Identity Server をインストールする場合にのみ設定が必要	デフォルトは inetorgperson
USER_NAMING_ATTR	既存の DIT のユーザを定義するために使用するネーミング属性を表示する この変数は、既存の Directory Server に対して Identity Server をインストールする場合にのみ設定が必要	uid
DS_ADMIN_ID	Directory Server を管理する Administration Server の管理者として定義されたユーザ名を表示する	デフォルトは admin
DS_ADMIN_PORT	Administration Server が使用するポート番号を表示する	デフォルトは 58900
DS_ADMIN_PASSWD	Administration Server の管理者として定義されたパスワードを表示する	デフォルトは admin123
LDAPUSER	ユーザ ID *amldapuser* を表示する	これは、*amldapuser* として事前定義され、変更できない
LDAPUSERPASSWD	*amldapuser* に設定したパスワードを表示する	このパスワードは、amadmin ユーザと異なっている必要がある
SUPERADMIN	最上位管理者に割り当てられたユーザ名を表示する。これは Identity Server によって割り当てられ、変更できない	デフォルトは amAdmin。変更不可能

表 9-1 Statefile 変数の説明 (続き)

変数	説明	値
SUPERADMINPASSWD	最上位管理者に割り当てたパスワードを表示する	このパスワードは、amldap ユーザに設定したパスワードと異なっている必要がある
START_SERVER	インストール処理の終了後、Identity Server を自動的に起動するように選択したかどうかを示す	true または false
COOKIE_DOMAIN_LIST		.siroe.com
DOMAINURLS		
FRESH_DS_WITH_SERVICES	Identity Server に付属する Directory Server をインストールしたかどうかを示す	yes または no
STATE_BEGIN	Statefile の開始タグ。このタグは、製品名とウィザード ID が付加され、製品のビルドに対して一意に決められている	
STATE_DONE	Statefile の終了タグ。このタグは、製品名とウィザード ID が付加され、製品のビルドに対して一意に決められている	

第 10 章

インストール後のタスク

この章では、Identity Server をインストールした後に実行する必要があるタスクについて説明します。また、この章では、必要に応じて Identity Server をアンインストールする方法についても説明します。

この章には次のトピックがあります。

- Identity Server サービスの起動
- Identity Server へのログオン
- Solaris 上の Identity Server のアンインストール
- Windows 上の Identity Server のアンインストール

Identity Server サービスの起動

Solaris の場合

Identity Server を自動的に起動しない選択をした場合は、手動で起動してからでなければログインできません。コマンド行に次のコマンドを入力します。

/IS_root/SUNWam/bin/amserver start

Windows の場合

Windows 2000 の場合、次の手順を使って Identity Server を起動できます。

1. DOS のプロンプトウィンドウを開いて、次のコマンドを入力します。

   ```
   cd IS_root¥bin
   amserver start
   ```

2. 「スタート」メニューから、「プログラム」>「管理ツール」>「サービス」を選択します。あるいは、「設定」>「コントロールパネル」>「管理ツール」>「サービス」を選択します。
3. 「サービス」ウィンドウで、Identity Server-*hostname* のアイコンを右クリックします。メニューから、「開始」を選択します。

Identity Server へのログオン

Solaris の場合

インストールの終了時に、自動的に Identity Server を起動する選択をした場合は、ブラウザから Identity Server にログインできます。

1. 次の適切な URL に移動します。
   - Identity Server サービスを Sun ONE Web Server で実行している場合は、次のフォームを使ってログイン URL に移動します。

     http://*host.domain:port*/amconsole

     この場合、*host* はシステムのホスト名、*domain* は Identity Server サービスを実行するサーバのドメイン名、*port* は Identity Server サービスのポート番号です。

     例 : *http://nila.siroe.com*:58080/amconsole

     この場合、nila は Identity Server を管理するマシンです。
2. 「ログイン」ページで、インストール時に指定した最上位管理者のユーザ ID とパスワードを入力します。

Windows の場合

ブラウザから Identity Server にログインすることができます。

1. 適切なログイン URL に移動します。
   - Identity Server サービスを Sun ONE Web Server で実行している場合は、次のフォームを使ってログイン URL に移動します。

http://*host.domain:port*/amconsole

この場合、*host* はシステムのホスト名、*domain* は Identity Server サービスを実行するサーバのドメイン名、*port* は Identity Server サービスのポート番号です。

例 : *http://myserver.siroe.com.com*:58080/amconsole

2. 「ログイン」ページで、インストール時に指定した最上位管理者のユーザ ID とパスワードを入力します。

Solaris 上の Identity Server のアンインストール

Sun ONE Identity Server のアンインストールは、インストールと同様に、GUI を使用するか、またはコマンド行から実行できます。

このプログラムを使用して、製品全体を削除するか、あるいは次に示す製品の個々のコンポーネントを削除することもできます。

- JDK 1.3.1_06
- Sun ONE Directory Server
- Sun ONE Web Server
- ユーティリティ、サンプル、javadoc などを含むその他のパッケージ
- Sun ONE Identity Server 管理およびポリシーサービス
- Sun ONE Identity Server コンソール
- Identity Server 用 Sun ONE Directory Server 設定
- Sun ONE Identity Server ドメイン間シングルサインオン
- 共通ドメインサービス

注 アンインストールプログラムは、作成したカスタムファイルおよびディレクトリを含むすべてのファイルを、コンソールおよびサービスを配備したディレクトリから削除します。このため、アンインストールを行う前に、カスタムファイルおよびディレクトリをバックアップするようお勧めします。

既存の DIT を使用する既存の Directory Server をアンインストールする場合は、Identity Server スキーマだけが削除されます。Identity Server が作成または変更した組織、グループ、ロール、コンテナ、ユーザ、ポリシー、サービス、ACI は、Directory Server にそのまま保持されます。元の DIT を復元するには、DIT を移行する前に `ldif2db` または `bak2db` を使って保存したデータを復元できます。

GUI プログラムを使用したアンインストール

Identity Server インストールプログラムを実行するには、root 権限が必要です。アンインストールプログラムを開始する前に、すべての Web ブラウザを終了させてください。

1. Identity Server をインストールしたディレクトリに移動します。
2. 新しい端末ウィンドウを開き、`xhost +` と入力してマシンのアクセス制御を無効にします。
3. 次のコマンドのいずれか 1 つを使って DISPLAY 変数を設定します。
   - csh または tcsh を使用している場合、次のように入力します。

     `setenv DISPLAY` *host.siroe.COM:0.0*
   - sh、ksh、または bash を使用している場合、次のように入力します。

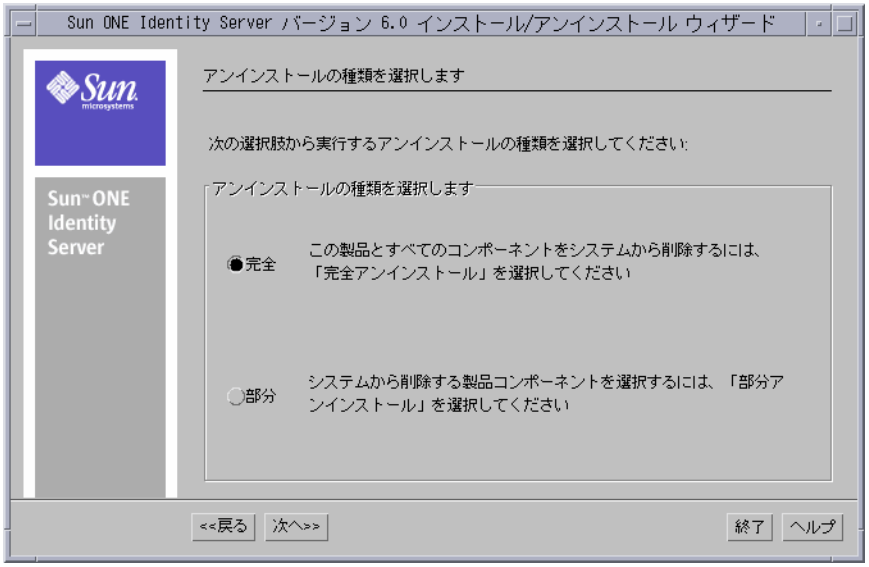
     `export DISPLAY=`*host.siroe.COM:0.0*

   この場合、`host` はインストールプログラムを実行しているマシンです。
4. Identity Server ディレクトリで、コマンド行に次のコマンドを入力します。

   ```
   # ./uninstall
   ```

   アンインストールプログラムが起動し、開始パネルが開きます。
5. 「次へ」をクリックして、「アンインストールの種類を選択」パネルを開き、アンインストールの種類を選択します。

図 10-1 「アンインストールの種類を選択」パネル



完全 : システムから製品およびすべてのコンポーネントを削除します。

部分 : Identity Server の特定のコンポーネントだけを削除します。「次へ」をクリックすると、サービスにインストールされたすべてのコンポーネントの一覧が表示されます。アンインストールするコンポーネントを選択して、「次へ」をクリックします。

6. 「アンインストールの準備完了」ウィンドウで、アンインストール情報を確認します。変更が必要な場合は、「戻る」をクリックします。それ以外の場合は、「今すぐアンインストールする」をクリックします。プログラムは、指定された製品またはコンポーネントをアンインストールします。

7. アンインストールが終了したら、`SUNWam` パッケージが削除されているかどうかを確認します。次のコマンドを使って確認します。

   ```
   pkginfo | grep SUNWam
   ```

8. パッケージが存在する場合は、次のコマンドを使って手動で削除します。

   ```
   pkgrm SUNWam
   ```

9. `/var/sadm/install` ディレクトリに移動し、`ls-al` コマンドを使って、次のファイルがまだ残っているかどうかを確認します。

   - `productregistry`
   - `lockfile`
   - `.pkg.lock`

10. ファイルがある場合は、rm コマンドを使って、手動で削除します。

コマンド行からの Identity Server のアンインストール

Identity Server インストールプログラムを実行するには、root 権限が必要です。アンインストールプログラムを開始する前に、すべての Web ブラウザを終了させてください。

1. Identity Server ディレクトリで、コマンド行に次のコマンドを入力します。

   ```
   ./uninstall -nodisplay
   ```

2. 画面に表示されるメッセージとプロンプトを確認して、アンインストールを続行します。
3. 手順を確認し、Enter を押して続行します。

```
Sun ONE Identity Server インストール /
アンインストールプログラムへようこそ

インストール / アンインストールプログラムを実行する前にすべてのプログラムを終
了してください。ほかのプログラムを実行している場合、Ctrl-C を押してインス
トールプログラムを終了し、実行中のプログラムを終了させてください。

警告 : このプログラムは、著作権法および国際条約によって保護されています。
書面による承諾なく、このプログラムのすべてまたは一部を複製または配布すると、
民法または刑法上の罰則を課せられるほか、法律の定める範囲で起訴されます。

< 継続するには ENTER キーを押してください >
```

4. 次のプロンプトで、Identity Server をアンインストールする方法を選択します。製品全体をアンインストールするか、または選択したコンポーネントだけをアンインストールすることができます。

```
次の選択肢から実行するアンインストールの種類を選択してください：

この製品とすべてのコンポーネントをシステムから削除するには、「完全アンインス
トール」を選択してください
システムから削除する製品コンポーネントを選択するには、「部分アンインストール」
を選択してください
1．完全
2．部分
    上のオプションを 1 つ選択してください [1] {"<" 戻る , "!" 終了 }
```

- **完全** : このオプションを選択すると、アンインストールプログラムは Identity Server のすべてのコンポーネントを削除します。プロンプトで 1 を入力して、このオプションを選択します。
- **部分** : このオプションを選択すると、アンインストールするコンポーネントを選択できます。プログラムは、選択したコンポーネントだけを削除します。プロンプトで 2 を入力して、このオプションを選択します。アンインストールするコンポーネントを選択する画面が表示されます。

5. オプションの番号を入力して、Enter を押します。完全アンインストールを選択した場合は、手順 11 で示すプロンプトが表示されます。部分アンインストールを選択した場合、プログラムはインストール済みコンポーネントの一覧を表示します。この一覧から、アンインストールするコンポーネントを選択する必要があります。
6. 前のプロンプトで「完全」を選択した場合は、ここで 1 を入力してアンインストールを開始します。

```
アンインストールの準備完了
1．今すぐアンインストール
2．開始
3．終了
```

アンインストールが正常に完了すると、アンインストールプログラムは次のプロンプトを表示します。

```
アンインストール中 Sun ONE Identity Server

|-1%--------------25%-----------------50%-----------------75%--
------------100%|
アンインストールの要約
製品 要約の結果 詳細
1. Sun ONE Identity Server
完全
ログを表示するには 1、終了するには 2 を入力してください。
終了
オプションを 1 つ選択してください [2] {"!" exits}
```

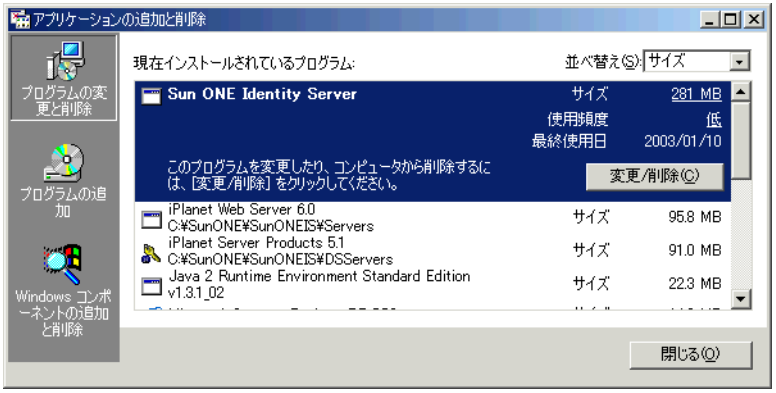
7. Enter を押して、アンインストールプログラムを終了します。

Windows 上の Identity Server のアンインストール

Sun ONE Identity Server アンインストールプログラムを実行するには、管理者特権が必要です。プログラムを開始する前に、すべての Web ブラウザを終了させてください。

1. 「スタート」メニューから、「設定」>「コントロールパネル」を選択します。
2. 「コントロールパネル」で、「アプリケーションの追加と削除」をダブルクリックします。
3. 「アプリケーションの追加と削除」ウィンドウで、「Sun ONE Identity Server」を選択して、「変更 / 削除」をクリックします。

図 10-2　「アプリケーションの追加と削除」ウィンドウ



Sun ONE Identity Server アンインストールプログラムが起動します。

注　別の方法として、DOS のコマンドプロンプトウィンドウからアンインストールプログラムを起動することもできます。*IS_root* ディレクトリで、次のコマンドを入力します。

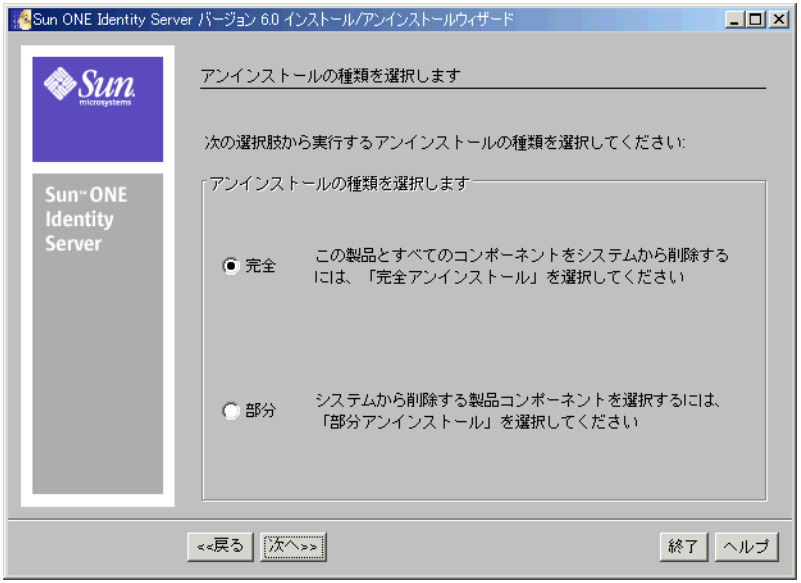
```
java uninstall_Sun_ONE_Identity_Server
```

このコマンドもアンインストールプログラムを起動します。

---

4. 「アンインストールプログラム」ウィンドウで、「次へ」をクリックして続行します。
5. 「アンインストールの種類を選択」ウィンドウで、次のオプションのいずれかを選択します。

図 10-3 「アンインストールの種類を選択」パネル



完全 : ローカルコンピュータシステムにインストールされた Identity Server サービスと Directory Server を削除する場合に、このオプションを選択します。

部分 : Sun ONE Identity Server のコンポーネントの一部だけを削除する場合は、このオプションを選択します。このウィンドウで「次へ」をクリックすると、プログラムはインストールされたすべてのコンポーネントを表示します。アンインストールするコンポーネントをクリックします。

6. 「アンインストールの準備完了」ウィンドウで、「今すぐアンインストールする」をクリックします。

   「要約」ウィンドウの「詳細」をクリックして、アンインストールの結果の詳細を参照できます。「終了」をクリックしてプログラムを終了します。

DSAME 5.1 から Identity Server 6.0 へのデータの移行

概要

この付録では、DSAME 5.1 から Identity Server 6.0 にデータを移行する手順について説明します。移行手順は、この付録で説明する順序で実行する必要があります。

データ移行処理には次の手順が含まれます。

1. すべての DSAME 5.1 データのバックアップ
2. Directory Server 5.1 を除く DSAME 5.1 のアンインストール
3. Identity Server 6.0 スキーマ用の Directory Server の設定
4. 既存の Directory Server および DIT を使用する Identity Server 6.0 のインストール
5. Identity Server 6.0 への DSAME 5.1 サービス、ポリシー、および認証エントリの移行

移行手順を実行する担当者は、Directory Server コマンド、スキーマセマンティクス、DIT、Identity Server スキーマおよび Identity Server DIT 構造に精通している必要があります。さらに、XML および Identity Server のインストール手順を熟知している必要があります。

Identity Server 6.0 は、DSAME 5.1 データを Identity Server 6.0 に移行するための一連の Perl スクリプトを提供します。移行手順は複雑ですが、これらのスクリプトにより多くの複雑な手順を処理することができます。通常、スクリプトは入力ファイルと出力ファイルを生成します。入力ファイルと出力ファイルは、スクリプトの実行後も保持されます。これは、出力ファイルのエントリを確認するのに便利です。入力ファイルには 5.1 形式のエントリが含まれ、出力ファイルには 6.0 形式のエントリが含まれます。出力ファイルは、`ldapmodify` コマンドを使って読み込む必要があります。ファイルを読み込む前にエントリの確認ができるように、出力ファイルの読み込みは自動

的に行われません。スクリプトを複数回実行する場合は、スクリプトが生成した古い入力および出力ファイルを必ず削除してください。`ldapmodify` コマンドの実行中にエラーが発生し、一部のスクリプトが既存のファイルに出力を追加する場合があります。

各スクリプトには、追加情報があります。スクリプトを実行する前に、この情報を確認する必要があります。さらに、各スクリプトで、スクリプトを実行する前にいくつかの変数を設定するか、変数の値を確認する必要があります。

注 上述の手順は、一般的な移行手順を示しています。データの移行のために、さまざまな方法でスクリプトを使用できます。たとえば、DSAME 5.1 に付属の既存の Directory Server をエクスポートし、新しい Directory Server にロードすることができます。移行スクリプトは、この新しい Directory Server で実行することができます。

既存のインストールのバックアップ

移行を開始する前に、DSAME 5.1 インストールを完全にバックアップする必要があります。

- Directory Server のバックアップツールを使って、DSAME 5.1 の Directory Server データをバックアップします。設定およびスキーマを含むすべての 5.1 データをバックアップする必要があります。
- DSAME 5.1 インストール後に変更されたすべてのデータをコピーして、Web Server データをバックアップします。

Web Server データは手動でバックアップする必要があります。`copy` コマンドと `tar` コマンドを使用することができます。5.1 インストール後に Web Server に対して行なったすべての変更をバックアップする必要があります。次のディレクトリもバックアップする必要があります。

表 A-1 バックアップするディレクトリ

バックアップするディレクトリ	内容
`<IS install dir>/SUNWam/web-apps/applications`	IS コンソールファイル
`<IS install dir>/SUNWam/web-apps/services`	IS サービスファイル
`<IS install dir>/SUNWam/servers/alias`	証明書
`<IS install dir>/SUNWam/config`	各種 XML ファイル
`<IS install dir>/SUNWam/lib/`	プロパティファイル
`<IS install dir>/SUNWam/locale`	ロケールファイル

Identity Server 6.0 のインストール後に、これらのバックアップを参照して必要な変更を行うことができます。これらの変更は、Identity Server 6.0 のインストール後に手動で行う必要があります。

ログ、デバッグ、インストールファイルもバックアップする必要があります。次の表は、これらのファイルがあるディレクトリの一覧です。

表 A-2　バックアップするファイル

ファイル	場所
ログファイル	/var/<IS 5.1 install dir>/SUNWam/logs
デバッグファイル	/var/<IS 5.1 install dir>/SUNWam/debug
インストールファイル	/var/<IS 5.1 install dir>/SUNWam/install

6.0 移行後に更新する必要があるその他のデータをバックアップします。

DSAME 5.1 のアンインストール

DSAME 5.1 アンインストールプログラムを使用して DSAME コンポーネントを削除します。ただし、Directory Server 5.1 は決して削除しないでください。

Solaris の場合

Solaris で DSAME コンポーネントを削除するには、次の手順に従います。

1. DSAME 5.1 から、`aminstall` スクリプトを実行します。
2. 次のオプションを選択します。

   1) 既存のコンポーネントを削除してから、インストールを続行します。
3. 次に表示されるプロンプトで、次のオプションを選択して、DSAME 管理およびポリシーサービスを削除します。

   1) DSAME 管理およびポリシーサービス
4. もう一度 `aminstall` スクリプトを実行して、オプション 1 を選択します。

5. 次に表示されるプロンプトで、次のオプションを選択して、Directory Server 設定を削除します。

   3) DSAME 用の iPlanet Directory Server 設定

   Directory Server のスキーマ設定が削除されます。

6. アンインストールが完了したら、次のコマンドを使用して SUNWamjdk パッケージをチェックします。

   ```
   pkginfo |grep SUNWamjdk
   ```

7. SUNWamjdk パッケージが存在する場合は、次のコマンドを使用して削除します。

   ```
   pkgrm SUNWamjdk
   ```

8. DSAME コンポーネントをアンインストールしたら、Directory Server を再起動します。

Windows の場合

DSAME 5.1 コンポーネントをアンインストールするには、次の手順に従います。

1. DSAME 5.1 アンインストールプログラムを実行します。手順の詳細については、『DSAME 5.1 インストールおよび構成ガイド』を参照してください。このガイドは、次の Web サイトにあります。
   http://docs.sun.com/source/816-5626-10/
2. 部分アンイストールを選択します。
3. DSAME 管理およびポリシーサービスを選択します。

上の手順では、Windows の DSAME 用 Directory Server 設定は削除されません。次の手順で DSAME 5.1 の Directory Server を Identity Server 6.0 スキーマに対して設定するために、DSAME 5.1 スキーマ設定をアンインストールする必要があります。Directory Server スキーマディレクトリから、DSAME 5.1 スキーマファイル 95ns-amschema.ldif を削除します。さらに、productregistry ファイルを更新して、Directory Server 設定コンポーネントを削除する必要があります。productregistry ファイル自体を削除することができます。productregistry ファイルを必ずバックアップしてください。productregistry ファイルを削除する場合、あとで「アプリケーションの追加と削除」を選択して Directory Server インストールを削除することができます。

4. DSAME コンポーネントをアンインストールしたら、Directory Server を再起動します。

IS 6.0 スキーマ用 Directory Server の設定

Identity Server 6.0 インストールプログラムを使用して、Identity Server 6.0 と連携するように Directory Server を設定します。手順の詳細は、本書の 74 ページの「既存の Directory Server の設定」を参照してください。

Directory Server 5.1 での Identity Server 6.0 のインストール

DSAME に存在する Directory Server を一部変更する必要があります。この Directory Server は、次のように DIT をサポートします。

```
o=isp
|
o=siroe.com
```

この場合、実際は isp は組織ではありません。このような場合、Identity Server 6.0 をインストールする前に、エントリ *isp* を更新する必要があります。DSAME 5.1 Directory Server に最上位レベルエントリとしての組織 (フラット DIT) がある場合は、Identity Server 6.0 のインストール前にこの変更を行う必要はありません。最上位レベルエントリに iplanet-am-service-status 属性セットがある場合は、Identity Server 6.0 インストールにより Directory Server DIT は変更されません。5.1 DIT 構造を維持するには、この属性を最上位レベルエントリに追加します。

1. 最上位レベルエントリが組織でない場合は、次のコマンドを実行して更新します。

```
<5.1 Directory Server install dir>/shared/bin/ldapmodify -D
"cn=directory manager" -w <password>
dn:o=isp
changetype: modify
delete: objectClass
objectClass:iplanet-am-managed-org
-
add: objectClass
objectClass: sunManagedOrganization
-
add: iplanet-am-service-staus
iplanet-am-service-status:iPlanetAMAuthService
```

2. 上のコマンドでは、インストール用の適切な dn を使用します。DSAME 5.1 DIT の最上位エントリが組織の場合は、上のコマンドを実行する必要はありません。最上位レベルエントリで、`ldapsearch` を実行して、この属性が設定されているかどうかを確認します。
3. ここで、この Directory Server で Identity Server 6.0 をインストールします。インストール時に、既存の DIT のインストールオプションを選択します。
4. Identity Server 6.0 のインストール時に、次のエントリが DSAME 5.1 インストールの場合と同じ値であることを確認します。
   - ディレクトリルート接尾辞
   - ディレクトリマネージャパスワード
   - Admin ユーザ
   - Admin パスワード
   - ディレクトリサーバホスト
   - ディレクトリサーバポート
   - コンソール配備記述子
   - サービス配備記述子

   値が確認できない場合は、DSAME 5.1 インストールのバックアップから `AMConfig.properties` ファイルを参照してください。組織のオブジェクトクラス、組織のネーミング属性、ユーザのオブジェクトクラス、ユーザのネーミング属性には DSAME 5.1 の値を使用してください。

この手順では、Directory Server データおよびスキーマを変更しません。Identity Server 6.0 パッケージ、ライブラリ、設定ファイル、jar ファイルなどをインストールするだけです。

Directory Server データの移行

Identity Server 6.0 のインストールと Directory Server スキーマの更新が完了したら、Directory Server データを Identity Server 6.0 形式に変更する必要があります。このために必要なすべての移行スクリプトは、`<install dir>/SUNWam/migration/51to60` ディレクトリにあります。このスクリプトには、スクリプトを実行する前に読む必要のある追加情報が含まれています。この追加情報は、各スクリプトで変数を設定し、変数の値を確認するのに便利です。

Identity Server 6.0 では、ポリシー、認証、およびコンソールコンポーネントが DSAME 5.1 から大幅に変更されているため、移行が必要になります。ただし、ロール、グループ、ユーザ、組織、組織単位、ACI などの Identity Server エントリは、DSAME 5.1 のまま使用されます。これらを移行する必要はありません。

DSAME 5.1 の次のエントリは、Identity Server 6.0 用に更新する必要があります。

- サービス分岐
- 組織
- 組織単位
- ポリシー
- ロール
- ユーザ

移行タスク

データ移行処理には次のタスクが含まれます。

- スキーマ変更の移行
- DSAME 5.1 ポリシーの移行
- 認証エントリの移行
- サービスの移行
- 認証エントリの Identity Server 6.0 への更新
- ポリシーの Identity Server 6.0 への更新
- エージェントの移行

スキーマ変更の移行

Identity Server 6.0 では、DSAME 5.1 からいくつかのスキーマ変更が行われています。たとえば、組織のオブジェクトクラス iplanet-am-managed-org は sunManagedOrganization に変更されています。属性 iplanet-am-domain-name は sunPreferredDomain に変更されます。同様に、ほかにもスキーマ変更があります。スキーマ変更の移行のために、スクリプト `update-schema.pl` が用意されています。このスクリプトを実行してスキーマ変更を移行します。追加情報については、スクリプトを参照してください。このスクリプトは、入力ファイル `51entries.ldif` と出力ファイル `60entries.ldif` を生成します。この出力 `ldif` ファイルで、`ldapmodify` を実行します。このスクリプトの最終行は、出力ファイルで `ldapmodify` コマンドを実行する構文を指定します。このスクリプトを実行すると、DSAME 5.1 エントリが Identity Server 6.0 スキーマに更新されます。

DSAME 5.1 ポリシーの移行

DSAME 5.1 は、ポリシーの実装のために CoS (サービスクラス) テンプレートを使用します。ポリシー定義には、ポリシーが割り当てられたサブジェクトは含まれません。代わりに、ポリシーをロールまたは組織に明示的に割り当てる必要があります。ポリシーを組織またはロールに割り当てると、CoS (サービスクラス) テンプレートが作成されます。URL ポリシーを割り当てた各組織またはロールには 1 個の CoS (サービスクラス) テンプレートがあります。

Identity Server 6.0 では、ポリシーの実装は CoS (サービスクラス) テンプレートを使用して行われません。ポリシー定義自体には、組織またはロールのようなサブジェクトが含まれています。ポリシー CoS (サービスクラス) テンプレートを使用して、DSAME 5.1 ポリシーを Identity Server 6.0 ポリシーに変換し、ポリシー定義自体にサブジェクトが含まれるようにする必要があります。

DSAME 5.1 ポリシーを Identity Server 6.0 ポリシーに変換するために、スクリプト `update-polices.pl` が用意されています。このスクリプトは、各組織または最上位レベルの組織で実行できます。組織を 1 つだけスクリプトに指定した場合、スクリプトは 6.0 形式に変換された 5.1 ポリシーを含む 1 つの出力ファイルをその組織用に生成します。最上位レベル組織を指定した場合は、最上位レベル組織の下にポリシーを持つ各組織用に 1 つの XML ファイルが生成されます。出力ファイルの名前は `<rdn>-<rdn>.xml` 形式です。たとえば、`o=iplanet.com,o=isp` にいくつかのポリシーがある場合、出力ファイルは `o=iplanet.com-o=isp.xml` となります。DSAME 5.1 にポリシーを持つ組織用に XML ファイルを生成するには、`update-policies.pl` スクリプトを実行します。追加情報については、スクリプトを参照してください。

DSAME 5.1 にはドメイン URL サービスがあります。このサービスを使って、ポリシー委譲の制御を実行できます。これは Identity Server 6.0 の参照ポリシーに似ています。定義済みのドメイン URL ポリシーがある場合は、この移行手順を手動でバックアップする必要があります。

各ドメイン URL ポリシーに対して、Identity Server 6.0 内に参照ポリシーを作成する必要があります。ドメイン URL ポリシーに基づき、Identity Server 6.0 内に対応する参照ポリシーを作成する必要があります。これは手動で実行する必要があります。このためのスクリプトは用意されていません。詳細は、219 ページの「ポリシーの Identity Server 6.0 への更新」の節を参照してください。

この手順は、移行サービスの前に実行する必要があります。この手順で生成された出力は、219 ページの「ポリシーの Identity Server 6.0 への更新」の手順のあとで使用されます。

DSAME 5.1 用の URL ポリシー DTD は `DSAME_root/SUNWam/dtd` の下にあります。

Identity Server 6.0 用の URL ポリシー DTD は `IS_root/SunWam/dtd` の下にインストールされます。

認証エントリの移行

Identity Server 6.0 では、認証サービスは大幅に変更されています。これらの変更には、属性名、属性値、属性のデフォルト値および属性の削除が含まれています。認証情報は各組織に存在します。移行により、すべての組織の認証エントリを更新する必要があります。

認証移行スクリプト `update-auth.pl` を実行します。このスクリプトは、出力ファイル `51to60auth-entries.ldif` を生成します。また、入力ファイル `51auth-entries.dn` も生成します。

この手順で生成された出力ファイルは、216 ページの「認証エントリの Identity Server 6.0 への更新」の手順で使用されます。

DSAME 5.1 から Identity Server 6.0 への認証サービスの変更の詳細については、222 ページの「認証サービスの変更」の節を参照してください。

サービスの移行

各 DSAME サービスを削除し、対応する Identity Server 6.0 サービスをロードする必要があります。さらに、すべての新しい Identity Server 6.0 サービスもロードする必要があります。サービス分岐には各サービスに対するグローバルスキーマ情報があり、組織に固有のエントリが含まれています。最上位レベル DSAME エントリが、`o=sun.com` のような組織自体の場合、`sun.com` の下のサービス分岐にはグローバルスキーマと組織固有のエントリが同様に含まれます。組織固有のエントリは、この組織に登録されたサービスの種類によって異なります。次の手順に従って、サービス分岐を更新します。

1. 最上位レベルエントリが組織ではない場合 (Identity Server 組織ではない `o=isp` など)、手順 3 に進みます。最上位レベルが組織の場合、手順 2 に進みます。
2. `update-toporg-services.pl` スクリプトを実行します。このスクリプトは、最上位レベル組織に登録されたさまざまな認証サービスと Identity Server コンソールサービスの組織エントリをバックアップします。サービスの組織エントリは、最上位レベル組織のグローバルサービスエントリの下にあります。グローバルサービスを 6.0 に更新するには、これらのサービスを削除して 6.0 からロードする必要があります。この手順では、グローバルサービスエントリの下にある組織エントリのバックアップを保持します。詳細は、このスクリプトを参照してください。組織固有のエントリを持つすべてのサービスが網羅されていることを確認します (手順 3 も参照)。

   このスクリプトは、出力ファイル `51to60toporg-template.ldif` を生成します。また、入力ファイル `51toporg-template.dn` も生成します。
3. Directory Server コンソールを使って、DSAME サービスを削除します。ほかのサービスを追加した場合は、それらを削除しないでください。次のサービスを削除する必要があります。

   ```
   iPlanetAMAdminConsoleService

   iPlanetAMAuthService

   iPlanetAMAuthAnonymousService

   iPlanetAMAuthCertService

   iPlanetAMAuthLDAPService

   iPlanetAMAuthMembershipService

   iPlanetAMAuthNTService

   iPlanetAMAuthRadiusService

   iPlanetAMAuthSafewordService

   iPlanetAMAuthUnixService

   iPlanetAMClientDetectionService
   ```

```
iPlanetAMDomainURLAccessService

iPlanetAMEntrySpecificService

iPlanetAMLoggingService

iPlanetAMNamingService

iPlanetAMPlatformService

iPlanetAMPolicyService

iPlanetAMSessionService

iPlanetAMUserService

iPlanetAMWebAgentService

DAI
```

ほかの追加サービスを何も追加していない場合は、最上位レベルエントリの下のサービス分岐全体を削除することができます。

4. `load-services.pl` を実行して、Identity Server 6.0 サービスをロードします。このスクリプトは、すべての Identity Server 6.0 サービスをロードします。これは、XML サービス `<install dir>/SUNWam/config/ums/ums.xml` および `<install dir>/SUNWam/config/xml` の下の XML ファイルを使用します。
5. 上の手順 2 で生成した出力ファイル (`51to60toporg-template.ldif`) を読み込みます。このファイルは、最上位レベル組織が Identity Server 組織の場合にのみ必要です。`ldapmodify` コマンドを使って、出力ファイルを読み込みます。構文については、出力ファイルの最終行を参照してください (この構文は Perl スクリプト自体から実行されるので「System」は不要です)。

6.0 における Identity Server サービスの変更の詳細については、228 ページの「Identity Server 6.0 のサービス」を参照してください。

認証エントリの Identity Server 6.0 への更新

「認証エントリの移行」の手順で生成した出力ファイルを読み込みます。`ldapmodify` コマンドを使って、このファイルを読み込みます。構文については、スクリプトの最終行を参照してください。この手順では、DSAME 5.1 認証エントリを Identity Server 6.0 に移行します。さらに、次の手順を実行する必要があります。

カスタマイズされた 5.1 HTML テンプレートがある場合は、6.0 JSP ベースのテンプレートに変更する必要があります。

すべてのカスタマイズされた認証モジュールは、`AMLoginModule.java` を使用して書き換える必要があります。画面プロパティは、XML ベースの認証モジュールプロパティを使用して変更する必要があります。カスタム認証モジュールの記述に関する詳細については、Identity Server 6.0 のマニュアルを参照してください。

ユーザの認証モジュール設定は自動的に移行されません。DSAME 5.1 のユーザ用に認証モジュールが選択されている場合は、移行後、この認証モジュールはそのユーザは使用できません。必要な認証モジュールは、Identity Server 6.0 のそのユーザ用に手動で設定する必要があります。

ユーザのデフォルトログイン URL 属性 (iplanet-am-user-default-url) は 6.0 では使用できません。この属性は自動的に 6.0 に移行されません。この属性の値は、コア認証サービスの iplanet-am-auth-login-success-url、または認証設定サービスの planet-am-auth-login-success-url、あるいは配備の必要性に応じてカスタム属性に設定できます。この属性は、移行してユーザエントリから削除する必要があります。そうしないと、この属性を持つユーザエントリを変更できません (オブジェクトクラス違反エラーとなります)。

Identity Server コンソールサービスエントリの 6.0 への更新

コンソールの表示に影響を与える Identity Server 6.0 コンソールサービスに変更があります。ドメイン URL サービスは 6.0 では使用できません。6.0 におけるポリシーの変更により、Web エージェントサービスおよびドメイン URL サービスを組織、ロール、およびユーザエントリに登録する必要がなくなりました。これらの変更を反映させるために、エントリを更新するスクリプトが用意されています。

1. サービスが何らかの組織に登録されている場合は、`update-services.pl` スクリプトを実行してコンソールサービスを更新します。このスクリプトは、入力ファイル `51console.ldif` と `51services.ldif`、および出力ファイル `60services.ldif` を生成します。

2. 出力ファイル `60services.ldif` で、`ldapmodify` コマンドを実行します。このコマンドを実行すると、組織に登録されたコンソールサービスエントリを移行できます。また、ドメイン URL および Web エージェントサービスの組織、ロール、およびユーザエントリも移行できます。

連合管理の有効化

Identity Server 6.0 は、Liberty Alliance (フェーズ 1) 仕様を実装しています。サービスを移行する場合 (214 ページの「サービスの移行」を参照)、連合管理用の 2 つのサービスがロードされます。`iPlanetAMAuthenticationDomainConfigService` と `iPlanetAMProviderConfigService` です。これらのサービスは、連合管理機能を使用する前に登録する必要があります。これらのサービスを登録するために、`liberty-services.ldif` という名前の ldif ファイルが用意されています。

このファイルの ROOT_SUFFIX の値を最上位レベルの組織に置き換えます。この ldif ファイルで、`ldapmodify` を実行します。このファイルで指定されたエントリが Identity Server 6.0 に存在する場合は、この ldif ファイルからこれらのエントリを削除し、残りのエントリを読み込みます。この手順を実行すると、Identity Server 6.0 で連合管理が有効になります。

サービスと認証エントリが移行されると、ユーザは Identity Server 6.0 にログインできるようになります。Directory Server が Identity Server 6.0 と同じマシンにある場合は、<installdir>/bin/amserver スクリプトを編集して、適切な Directory Server インスタンスを指すように NDS_SERVER 変数を変更します。

Identity Server を再起動して、Identity Server 6.0 コンソールにログインします。コア認証サービスの 5.1 のデフォルトログイン URL (<protocol>://<host>:<port>/amserver/login) が変更されていない場合は、Identity Server 6.0 のデフォルトログイン URL (<protocol>://<host>:<port>/amserver/UI/Login) を使用して Identity Server 6.0 コンソールにログインできます。5.1 には、デフォルトログイン URL が、コア認証サービスの <protocol>://<host>/amserver/login ではなく /amserver/login に設定される場合があるという既知の問題があります。この場合、6.0 のデフォルトログイン URL を使用してログインすることができません。6.0 のデフォルトログイン URL (<protocol>://<host>/amserver/UI/Login) に対するデフォルト組織の関連するドメイン属性を変更して、6.0 のデフォルトログイン URL を使用するコンソールにアクセスする必要があります。ホストの完全指定のドメイン名を使用し、URL に適切な配備記述子を使用します。関連するドメイン属性の値にポート番号がありませんが、コンソールにアクセスするときにはポートを指定する必要があることに注意してください。

また、<protocol>://<host>:<port>/amserver/UI/Login?org=<org RDN> 形式の URL を使用することもできます。ほかのエントリを移行する前に、ログインを確認することが大切です。移行は段階的な処理であり、その都度および可能なときに手順を検証する必要があります。

ユーザ管理は、デフォルトでは有効ではありません。Identity Server コンソールにログイン後、「サービス設定」タブに移動します。管理サービスを編集します。「ユーザ管理を有効」チェックボックスをクリックして、サービスを保存します。ここで、ユーザ管理機能の「アイデンティティ管理」タブに移動できます。

IS 6.0 では、新しいユーザ amldapuser が導入されました。このユーザは、LDAP、メンバーシップ認証モジュール用のディレクトリをバインドおよび検索するために使用されます。また、このユーザはポリシー設定サービスでも使用されます。LDAP、メンバーシップ、またはポリシー設定サービスを組織に登録したら、このユーザのパスワードをこれらのサービスに明示的に入力する必要があります。パスワードは、Identity Server 6.0 のインストール時に入力した amldapuser のパスワードです。さらに、このユーザを作成する必要もあります。次の 2 つのコマンドを実行して、このユーザを作成し、このユーザへのアクセス権を設定します。

```
<path to ldapmodify>/ldapmodify -D "cn=directory manager" -w
<password>
dn: cn=amldapuser,ou=DSAME Users,ROOT_SUFFIX
changetype: add
objectclass:inetuser
objectclass:organizationalperson
objectclass:person
objectclass:top
cn: amldapuser
sn: amldapuser
userPassword: <password>
<path to ldapmodify>/ldapmodify -D "cn=directory manager" -w
<password>
dn: ROOT_SUFFIX
changetype: modify
add: aci
aci: (target="ldap:///ROOT_SUFFIX")(targetattr="*")(version 3.0;
acl "special ldap auth user rights"; allow (read,search) userdn =
"ldap:///cn=amldapuser,ou=DSAME Users,ROOT_SUFFIX";)
```

上のコマンドでは、-w オプションを付けて、ディレクトリマネージャのパスワードを指定します。ROOT_SUFFIX をインストールルートエントリに置き換えます。最初のコマンドの userPassword 属性で、amldapuser パスワードを指定します。

LDAP およびメンバーシップサービスがすでに IS 5.1 の組織に登録されている場合は、ユーザ検索に使用されるバインド DN は「dsameuser」であることに注意してください。このユーザを上記のコマンドで作成した「amldapuser」に変更し、パスワードも amldapuser パスワードに変更します。これら 2 つのサービスが登録されているすべての組織でこの変更を行う必要があります。ユーザを「dsameuser」のままにしておくこともできますが、Identity Server 6.0 では「amldapuser」を使用することをお勧めします。

Identity Server ユーザのプロファイルには、アカウント有効期限属性があります。DSAME 5.1 のアカウント有効期限属性の形式は mm/dd/yy hh:mm ですが、6.0 のアカウント有効期限属性の形式は mm/dd/yyyy hh:mm です。この属性形式は、`locale` という名前のディレクトリにある `amUser.properties` ファイルにあります。DSAME 5.1 のユーザにアカウント有効期限属性が設定されている場合は、日付形式を 6.0 の形式に変更して、Identity Server コンソールからのユーザプロファイルの変更時に、ユーザプロファイル変更を保存する必要があります。あるいは、`amUser.properties` の DSAME 5.1 形式を使って、日付形式を変更することができます。`ldapmodify` コマンドを使用して、アカウント有効期限属性の値を変更することもできます。

また、DSAME 5.1 で、`AMConfig.properties` に特定の変更が行われている場合は、Identity Server 6.0 のインストール後、`AMConfig.properties` にこれらの変更を行う必要があります。

ポリシーの Identity Server 6.0 への更新

Directory Server で更新済みのポリシーを読み込む前に、DSAME 5.1 ポリシーを削除する必要があります。`delete-policies` スクリプトを実行して、すべてのポリシーを削除します。スクリプトは、入力ファイル `delete-policies.dn` と出力ファイル `delete-policies.ldif` を生成します。`delete-policies.ldif` で `ldapdelete` コマンドを実行して、すべての 5.1 ポリシーを削除します。`delete-policies.ldif` で指定されたすべてのエントリが削除されていることを確認します。Directory Server に存在しないエントリについてエラーが発生した場合は、ldif ファイルからこれらのエントリを削除し、ファイルのその他のエントリの削除を続行します。`delete-policies.ldif` ファイルには、重複エントリが存在する場合があります。すでに削除されたエントリ (重複エントリ) を削除するときにエラーが発生する場合があります。このようなエラーは無視することができます。`ldapdelete` を連続モードで実行して、このエラーを無視できます。

Identity Server 6.0 には新しいポリシー設定サービスがあります。このサービスは、サブジェクト、レフェラル、条件などのポリシーコンポーネントで使用されるさまざまな設定属性を指定します。組織のポリシーを作成するには、ポリシー設定サービスを登録する必要があります。組織にポリシーを読み込む前に、各組織に対して、このサービスを登録する必要があります。Identity Server 6.0 コンソールにログインして、各組織にこのサービスを登録することができます。また、amadmin コマンドを使って、各組織にこのサービスを登録することもできます。

最上位レベル組織から開始し、次のコマンドを実行して Identity Server 6.0 ポリシーをロードします。

IS_root/bin/amadmin -u *amadmin id* -w *password* -t *output migrated policy file for the organization*

Identity Server 6.0 では、ポリシーはポリシー名で記述できます。また、ルール、サブジェクト、条件、レフェラルなどポリシーの個々の要素も名前を持ちます。DSAME 5.1 ポリシーのインポート時に、これらの要素の名前と説明は自動的に生成されます。名前は、ポリシーのインポート後に変更できます。

Identity Server 6.0 には、参照ポリシーの概念があります。詳細は、Identity Server 6.0 のマニュアルを参照してください。サブ組織でポリシーを作成するには、最上位レベルの組織からの参照ポリシーが必要です。参照ポリシーは、リソース参照に基づいてポリシーを委譲します。次の DIT について検討します。

```
        o=isp
          /¥
o=siroe.com     o=iplanet.com
```

siroe.com または iplanet.com でポリシーを作成するには、o=isp.com に siroe.com および iplanet.com に対する参照ポリシーが必要です。

o=isp.com の参照ポリシーには、o=siroe.com または o=iplanet.com で管理されるリソースまたはリソース接頭辞が含まれている必要があります。siroe.com が http://www.siroe.com/ を管理している場合、o=isp.com の参照ポリシーは、そのルールにリソース http://www.siroe.com/ を含み、siroe.com の組織を参照している必要があります。o=siroe.com で管理されるその他のリソースの場合、その他の参照ポリシーを o=isp で作成する必要があります。必ず最上位レベルの参照ポリシーを作成してから、上に指定したコマンドを実行して、サブ組織のポリシーを更新する必要があります。 サブ組織レベルのポリシーで指定したリソースの親レベルに参照ポリシーがない場合、ポリシーの作成はできません。このため、上のコマンドを実行する前に、サブ組織レベルの親レベルに参照ポリシーを作成することが重要です。各サブ組織のポリシー出力ファイルを参照して、XML ファイルに含まれるリソースを確認します。そのサブ組織のポリシー出力 XML ファイルを読み込む前に、これらのリソースのそれぞれに対して、最上位レベルに参照ポリシーが必要です。

DSAME 5.1 にはドメイン URL サービスがあります。このサービスを使って、ポリシー委譲の制御を実行できます。これは Identity Server 6.0 の参照ポリシーに似ています。主な違いは、ポリシー評価時にドメイン URL サービスが適用され、ポリシー評価だけでなくポリシー作成時にも参照ポリシーが適用されることです。DSAME 5.1 では、デフォルトで、最上位レベルの管理者だけがドメイン URL ポリシーを作成することができます。

DSAME 5.1 では、上記の DIT を使って、`iplanet.com` にあるリソースにアクセスできるように `siroe.com` にポリシーを作成することができます。また、その逆も可能です。ただし、`o=isp` の最上位管理者は、`o=siroe.com,o=isp` にドメイン URL サービスを作成することができます。このポリシーは、この組織で何を許可するかを指定します。ドメイン URL ポリシーで `http://www.siroe.com/*` を許可するように指定すると、`http://www.siroe.com/*` と一致する URL ポリシーで許可されるリソースだけがポリシー評価時に返されます。これにより、6.0 の参照ポリシーの使用が適用されます。DSAME 5.1 で作成した各ドメイン URL ポリシーの場合は、対応する参照ポリシーを 6.0 で作成する必要があります。この手順は手動で実行する必要があります。

Identity Server 6.0 には、ポリシー管理のためのポリシー管理者ロールがあります。ポリシー管理者には、ポリシーを作成、削除、または変更し、サービスを組織に割り当てる権限があります。6.0 の各組織の場合は、ポリシー管理者ロールを作成する必要があります。`update-policy-roles.pl` スクリプトを実行します。出力ファイル `add-policy-roles.ldif` が生成されます。また、入力ファイル `51org-entries.dn` も生成されます。`ldapmodify` を使って、このスクリプトで生成された出力ファイルを読み込みます。スクリプトの末尾の構文を参照してください。

この手順は、Directory Server にさまざまなポリシー管理者ロールを作成します。

コンソールの変更の移行

DSAME 5.1 でコンソールのカスタマイズを行なった場合は、これらの変更を Identity Server 6.0 のコンソールファイルに移行する必要があります。

この手順は手動で実行する必要があります。このためのスクリプトは用意されていません。

上記の手順を行うと、Directory Server のデータ、スキーマ、およびすべてのカスタマイズデータが 6.0 に移行します。この手順が完了したら、Identity Server 6.0 を再起動する必要があります。

エージェントの移行

Agents 1.0 または 1.1 は、Identity Server 6.0 で動作しません。Identity Server 6.0 で動作するには Agents 2.0 が必要です。エージェントを移行するには、Agents 1.0 または 1.1 をアンインストールしてから、Agents 2.0 をインストールする必要があります。

1. 1.0 または 1.1 エージェントで行なったすべての設定変更をバックアップします。AMAgent.properties に対して行なった変更などをバックアップします。
2. 2.0 エージェントをインストールします。
3. 2.0 設定ファイルを変更します。
4. エージェントを再起動します。

注

1. DSAME 5.1 XML ファイルに対して行なった変更は、この手順では移行されません。Identity Server 6.0 をインストールしてから、6.0 XML ファイルでこれらの変更を手動で更新する必要があります。これを実行する 1 つの方法は、読み込む前に 6.0 XML ファイルを更新することです。
2. スクリプト update-rootsuffix.pl は、この移行手順では使用されません。このスクリプトが別の Identity Server 6.0 インストールで使用可能な場合に、このスクリプトは「Directory Server 5.1 での Identity Server 6.0 のインストール」の手順 4 で使用することができます。このスクリプトは、iplanet-am-service-staus 属性を持つ最上位レベルエントリを更新します。

認証サービスの変更

この節では、認証サービスの変更について詳細に説明します。

認証サービス (コア) [amAuth.xml]

属性の変更

グローバル

1. 「iplanet-am-auth-login-worker-classes」が削除されました。
2. 「iplanet-am-auth-sleep-interval」が追加されました。

組織

1. 「iplanet-am-auth-chaining-modules」が削除されました。

2. 「iplanet-am-auth-chaining-enabled」が削除されました。
3. 「iplanet-am-auth-non-interactive-modules」が削除されました。
4. 「iplanet-am-auth-default-url」が削除されました。
5. 「iplanet-am-auth-user-based」が削除されました。
6. 「iplanet-am-auth-login-worker-class」が削除されました。
7. 「iplanet-am-auth-org-config」が追加されました。
8. 「iplanet-am-auth-login-success-url」が追加されました。
9. 「iplanet-am-auth-login-failure-url」が追加されました。
10. 「iplanet-am-auth-post-login-process-class」が追加されました。
11. 「iplanet-am-auth-username-generator-enabled」が追加されました。
12. 「iplanet-am-auth-username-generator-class」が追加されました。
13. 「iplanet-am-auth-menu」が「iplanet-am-auth-allowed-modules」に変更されました。
14. 「iplanet-am-auth-admin-auth-module」で、
    - 'type' が「single_choice」から「single」に変更されました。
    - 'syntax' が「string」から「xml」に変更されました。
    - 属性 'propertiesViewBeanURL' が追加され、「/amconsole/auth/ACModuleList」に設定されました。
    - 属性 'uitype' が追加され「link」に設定されました。
    - サブ要素 ChoiceValues が削除されました。
    - デフォルト値が、プレーン文字列から XML 文字列に変更されました。
15. 「iplanet-am-auth-login-failure-count」で、デフォルト値が 3 から 5 に変更されました。
16. 「iplanet-am-auth-login-failure-duration」で、デフォルト値が 15 から 300 に変更されました。
17. 「iplanet-am-auth-lockout-warn-user」で、デフォルト値が 1 から 4 に変更されました。
18. 「iplanet-am-auth-default-auth-level」で、'syntax' が「string」から「number」に変更されました。

ユーザサービス [amUser.xml] における認証関連属性の変更

属性の変更

ダイナミック

1. 「iplanet-am-user-auth-modules」が削除されました。

ユーザ

1. 「iplanet-am-user-auth-modules」が削除されました。
2. 「iplanet-am-user-default-url」が削除されました。
3. 「iplanet-am-user-auth-config」が追加されました。
4. 「iplanet-am-user-alias-list」が追加されました。
5. 「iplanet-am-user-success-url」が追加されました。
6. 「iplanet-am-user-failure-url」が追加されました。
7. 「iplanet-am-user-account-life」で、'syntax' が「date」から「string」に変更されました。

次の XML ファイルにあるすべての「組織」属性

- amAuthLDAP.xml
  - 「iplanet-am-auth-ldap-search-filter」で、'syntax' が「string」から「xml」に変更されました。
  - 「iplanet-am-auth-ldap-auth-level」で、'syntax' が「string」から「number」に変更されました。
- amAuthAnonymous.xml
  - 「iplanet-am-auth-anonymous-auth-level」で、'syntax' が「string」から「number」に変更されました。
- amAuthMembership.xml
  - 「iplanet-am-auth-membership-search-filter」で、'syntax' が「string」から「xml」に変更されました。
  - 「iplanet-am-auth-membership-auth-level」で、'syntax' が「string」から「number」に変更されました。
- amAuthRadius.xml
  - 「iplanet-am-auth-radius-auth-level」で、'syntax' が「string」から「number」に変更されました。

- amAuthUnix.xml
  - 「iplanet-am-auth-unix-auth-level」で、'syntax' が「string」から「number」に変更されました。
- amAuthCert.xml
  - 「iplanet-am-auth-cert-auth-level」で、'syntax' が「string」から「number」に変更されました。
- amAuthSafeWord.xml
  - 「iplanet-am-auth-safeword-auth-level」で、'syntax' が「string」から「number」に変更されました。

次の表で、認証インタフェースの UI の変更について説明します。

表 A-3 認証インタフェースにおける GUI の変更

	DSAME 5.1.1 ファイル名	説明	IS 6.0 ファイル名
1.	account_expired.html	アカウントの有効期限が終了しました。システム管理者に問い合わせてください。	account_expired.jsp
2.	configuration.html	設定エラーです。	configuration.jsp
3.	disclaimer.html	これは免責条項テンプレートの例です。	disclaimer.jsp
4.	invalidPCookieUserid.html	持続 Cookie ユーザ名が、持続 Cookie ドメインに存在しません。	invalidPCookieUserid.jsp
5.	invalidPassword.html	入力したパスワードの文字数が足りません。	invalidPassword.jsp
6.	invalid_domain.html	このようなドメインはありません。	invalid_domain.jsp
7.	login_denied.html	この組織にユーザのプロファイルがありません。	login_denied.jsp
8.	login_fail_template.html	認証が失敗しました。	login_failed_template.jsp
9.	login_menu.html	認証メニュー タグ行は login_menu_modules.html に置き換えられました。	削除されました。

表 A-3　認証インタフェースにおける GUI の変更 (続き)

	DSAME 5.1.1 ファイル名	説明	IS 6.0 ファイル名
10.	login_menu_modules.html	認証メニューがループしたため、使用できるすべてのモジュールでこのファイルが表示されます (内部タグが置き換えられます)。	削除されました。
11.	login_prompt.html	ユーザベースのログインページです。	Login.jsp
12.	login_success.html	正常にログインしましたが、システムにデフォルトログインページがありません。	Login.jsp
13.	login_template.html	ログイン / パスワードページです。	Login.jsp
14.	login_timeout_template.html	ログインセッションがタイムアウトしました。	session_timeout.jsp
15.	logout.html	ログアウトしました。	Logout.jsp
16.	max_sessions.html	最大セッション制限時間に達しました。	Message.jsp
17.	membership.html	自己登録モジュールです。	membership.jsp
18.	membershipSkeleton.html		削除されました。
19.	missingReqField.html	必須フィールドの 1 つが完了しませんでした。	missingReqField.jsp
20.	module_denied.html	認証モジュールが拒否されました。	module_denied.jsp
21.	noConfirmation.html	パスワード確認フィールドが存在しません。	noConfirmation.jsp
22.	noLoginWorker.html	認証ページジェネレータが見つかりません。	削除されました。
23.	noPassword.html	入力したパスワードがありませんでした。	noPassword.jsp
24.	noUserName.html	入力したユーザ名がありませんでした。	noUserName.jsp
25.	noUserProfile.html	ユーザ名と一致するユーザプロファイルが見つかりませんでした。	noUserProfile.jsp

表 A-3　認証インタフェースにおける GUI の変更 (続き)

	DSAME 5.1.1 ファイル名	説明	IS 6.0 ファイル名
26.	org_inactive.html	この組織は有効ではありません。	org_inactive.jsp
27.	passwordMismatch.html	入力したパスワードが確認パスワードと一致しません。	passwordMismatch.jsp
28.	privilege_failure.html	ユーザはこの操作にアクセスできません。	Message.jsp
29.	profileException.html	ユーザプロファイルを保存中にエラーが発生しました。	profileException.jsp
30.	radius_patch.html	RADIUS 認証には i-Planet パッチ 1 が必要です。	Message.jsp
31.	register.html	自己登録です。	register.jsp
32.	session_invalid.html	セッションが無効です。	削除されました。
33.	session_timeout.html	セッションがタイムアウトしました。	session_timeout.jsp
34.	userExists.html	この名前のユーザがすでに存在します。	userExists.jsp
35.	userPasswordSame.html	ユーザ名とパスワードフィールドは同じ値を持つことができません。	userPasswordSame.jsp
36.	user_inactive.html	このユーザは有効ではありません。	user_inactive.jsp
37.	wrongPassword.html	入力したパスワードが無効です。	wrongPassword.jsp
38.	追加	内部認証フレームワークエラーを表示します。	auth_error_template.jsp
39.	追加	組織のユーザに対する設定が見つからないか定義されていません。	noConfig.jsp
40.	追加	ユーザがロール内にありません ('role' ベース認証の場合)。	userDenied.jsp

Identity Server 6.0 のサービス

Identity Server 6.0 の新しいサービスは次のとおりです。

- SAML サービス (amSAML.xml)
- セキュリティサービス (amDSS.xml)
- ポリシー設定サービス (amPolicyConfig.xml)
- 認証設定サービス (amAuthConfig.xml)

次のサービスは 6.0 で削除されました。

- ドメイン URL サービス (amDomainURLAccess.xml)

次のサービスは Identity Server 6.0 および DSAME 5.1 の場合でほぼ同じです。

- Identity Server コンソールサービス (amAdminConsole.xml)
- 認証匿名サービス (amAuthAnonymous.xml)
- 認証メンバーシップサービス (amAuthMembership.xml)
- 認証証明サービス (amAuthCert.xml)
- 認証 LDAP サービス (amAuthLDAP.xml)
- 認証 NT サービス (amAuthNT.xml)
- 認証 Radius サービス (amAuthRadius.xml)
- 認証 SafeWord サービス (amAuthSafeWord.xml)
- 認証 Unix サービス (amAuthUnix.xml)
- クライアントディテクションサービス (amClientDetection.xml)
- ネーミングサービス (amNaming.xml)
- プラットフォームサービス (amPlatform.xml)
- セッションサービス (amSession.xml)
- URL エージェントサービス (amWebAgent.xml)
- エントリ指定サービス (amEntrySpecific.xml)
- ユーザサービス (amUser.xml)

次のサービスは 6.0 で大幅に変更されました。

- 認証サービス (amAuth.xml)
- ログサービス (amLogging.xml)
- ポリシーサービス (amPolicy.xml)

- ユーザサービス (amUser.xml)

属性とオブジェクトクラスの名前変更

次の属性は Identity Server 6.0 で名前が変更されました。

表 A-4 属性の名前変更

旧属性名	新属性名
iplanetserviceschema	sunserviceschema
iplanetserviceid	sunserviceid
iplanetsmspriority	sunservicepriority
iplanetpluginschema	sunpluginschema
iplanetkeyvalue	sunkeyvalue
iplanetpluginid	sunpluginid
iplanetxmlkeyvalue	sunxmlkeyvalue
iplanet-am-domain-name	sunPrefferedDomain

次のオブジェクトクラスは Identity Server 6.0 で名前が変更されました。

表 A-5 オブジェクトクラスの名前変更

旧オブジェクトクラス	新オブジェクトクラス
iplanetservice	sunservice
iplanetservicecomponent	sunservicecomponent
iplanetorgservice	sunorgservice
iplanetserviceplugin	sunserviceplugin
iplanet-am-managed-org	sunManagedOrganization

上記の他、Identity Server コンソールサービスで、iplanet-am-unique-attribute-list および iplanet-am-attribute-uniqueness-enabled 属性が削除されました。新しいオブジェクトクラス sunNameSpace の新しい属性 sunNameSapceUniqueAttrs が Identity Server コンソールサービスから削除された一意の属性リストに対応するように、組織エントリに追加されました。

索引

L

O

R

S

U

ま

ゆ

よ

り

れ

ろ