インストールガイド

iPlanet Directory Server

Version 5.1

816-4122-01
2001 年 12 月

目 次

本書について

iPlanet Directory Server をご利用いただきありがとうございます。このマニュアルでは、iPlanet Directory Server をインストールする前に決定しておく設計および計画についての全体像について詳しく説明します。それから、いくつかの異なるインストール手順について説明します。

iPlanet Directory Server 5.1 は、業界標準の LDAP (Lightweight Directory Access Protocol) に基づく、スケーラブルで強力な分散型ディレクトリサーバです。iPlanet Directory Server は、社内イントラネット、取引先とのエクストラネット、あるいは顧客との窓口となる公共のインターネット上で使用できる、集中・分散型のデータリポジトリを構築するための基盤となります。

このリリースの iPlanet Directory Server の新機能および拡張機能に関する最新情報は、次のオンラインリリースノートを参照してください。

```
http://docs.iplanet.com/docs/manuals/directory.html
```

このインストールガイドは、Solaris™ 9 オペレーティング環境にプリインストールされた iPlanet Directory Server パッケージには適用されません。Directory Server の設定に関する情報と手順について Solaris 9 ユーザは、『Solaris のシステム管理 (ネーミングとディレクトリサービス : DNS、NIS、LDAP 編)』を参照してください。Solaris のマニュアルは、`http://docs.sun.com/` で参照できます。

お読みになる前に

Directory Server をインストールする前に、『iPlanet Directory Server 導入ガイド』をお読みいただくことを推奨します。『導入ガイド』には、ディレクトリサービスの設計および計画方法についての重要な概念が説明されています。

ディレクトリサービスの計画が完了したら、このマニュアルの手順に従って iPlanet Directory Server と関連ソフトウェアコンポーネントをインストールしてください。

表記上の規則

ここでは、このマニュアルで使用している表記上の規則について説明します。

クーリエ（等幅）フォント: この書体は、属性名やオブジェクトクラス名などの文字列を本文中に示すときに使用します。また、URL、ファイル名、および例の記述にも使用します。

イタリック体: これは、新出用語や、パス名の可変部分などの実際の値の代わりに使用するテキストを強調するために使用します。

大なり括弧 (>) は、一連のメニュー項目を選択するときのセパレータとして使用します。たとえば、「オブジェクト」>「新規」>「ユーザ」は、「オブジェクト」メニューのプルダウンメニューを開き、マウスをドラッグして「新規」を強調表示し、「新規」のサブメニューから「ユーザ」を選択することを意味します。

注	「注」、「注意」、および「ヒント」は、重要な条件や制限事項を強調します。必ずこれらの注意事項を読んでから、次の作業を続けるようにしてください。

このマニュアルでは、パスとファイル名に次の形式を使用しています。

installDir/slapd-*serverID*/...

実際のパスとサーバ識別子は、プラットフォーム、インストール、および構成によって異なります。デフォルトパスは、プラットフォームによって次のようになります。

Solaris 9 プラットフォーム	/var/ds5/slapd-*serverID*/...
その他の UNIX プラットフォーム	/usr/iplanet/servers/slapd-*serverID*/...
Windows プラットフォーム	C:¥iPlanet¥Servers¥slapd-*serverID*¥...

Directory Server を別の場所にインストールした場合は、それに合わせてパスを変更してください。*serverID* は、サーバのインストール時に指定したサーバ識別子を示します。たとえば、Directory Server に phonebook という名前を付けた場合、実際のパスは次のようになります。

Solaris 9 プラットフォーム	/var/ds5/slapd-phonebook/...
その他の UNIX プラットフォーム	/usr/iplanet/servers/slapd-phonebook/...
Windows プラットフォーム	C:¥iPlanet¥Servers¥slapd-phonebook¥...

このマニュアルに記載されている大半のパスとコマンドは UNIX 形式です。Windows ベースの Directory Server を使用する場合は、UNIX 形式のパスとコマンドを Windows 形式のパスとコマンドに読み替えてください。Windows プラットフォームのコマンドには、UNIX と同じコマンド名に拡張子 .exe または .bat が付きます。

関連情報

iPlanet Directory Server のマニュアルセットには、次のマニュアルも含まれています。

『iPlanet Directory Server 管理者ガイド』ディレクトリサービスの日常的な管理手順について説明し、サーバ側プラグインの設定に関する情報を提供します。

『iPlanet Directory Server 導入ガイド』Directory Server の導入計画の概要について説明し、導入の事例を提供します。

『iPlanet Directory Server 構成、コマンド、およびファイルのリファレンス』Directory Server に付属するコマンド行スクリプトの使用方法について説明します。

『iPlanet スキーマリファレンス』Directory Server に含まれている、クライアントアプリケーションで役立つ LDAP スキーマに関する情報を提供します。

その他の有用な情報は、次の Web サイトから入手できます。

- iPlanet 製品のオンラインマニュアル :
  `http://docs.iplanet.com/docs/manuals/`
- iPlanet 製品の技術情報 :
  `http://www.iplanet.com/support/technical_resources/`
- iPlanet プロフェッショナルサービスに関する情報 :
  `http://www.iplanet.com/services/professional_services_3_3.html`
- Solaris 対応 Sun Enterprise Service のパッチとサポート :
  `http://www.sun.com/service/`
- iPlanet の開発者向け情報 :
  `http://developer.iplanet.com/`
- iPlanet のトレーニング情報 :
  `http://www.iplanet.com/learning/index.html`
- iPlanet 製品のデータシート :
  `http://www.iplanet.com/products/index.html`

第 1 章

Directory Server のインストールの準備

iPlanet Directory Server をインストールする前に、Directory Server のさまざまなコンポーネントと事前に決定しなければならない設計と構成について理解しておく必要があります。

iPlanet Directory Server のインストールの準備に役立つように、以降の節で説明する概念を理解しておいてください。

- インストールコンポーネント
- 構成の決定
- インストールプロセスの概要
- インストール特権
- 環境変数の設定解除 (AIX のみ)

『iPlanet Directory Server 導入ガイド』には、基本的なディレクトリの概念と、ディレクトリサービスの設計および導入に役立つガイドラインが示されています。インストール作業を開始する前に、このマニュアルで説明されている概念を理解しておいてください。

警告　このマニュアルの情報は、Solaris™ 9 オペレーティング環境にすでにインストールされている iPlanet Directory Server には適用されません。Solaris 9 ユーザは、Directory Server の構成に関する情報と手順については、『Solaris のシステム管理 (ネーミングとディレクトリサービス : DNS、NIS、LDAP 編)』を参照してください。

Solaris のマニュアルは、`http://docs.sun.com/` で参照できます。

インストールコンポーネント

iPlanet Directory Server には、次のソフトウェアコンポーネントが含まれています。

- iPlanet Console : すべての iPlanet サーバ製品に共通のユーザインタフェースを提供する。このインタフェースからは、サーバの起動や停止、新しいサーバインスタンスのインストール、およびユーザ情報とグループ情報の管理など、共通のサーバ管理機能を実行できる。iPlanet Console は、スタンドアロンアプリケーションとして任意のマシン上にインストールできる。また、ネットワーク上にインストールして、リモートサーバを管理することも可能である
- Administration Server : すべての iPlanet サーバに共通のフロントエンド。iPlanet Console からの通信を受け取り、それを適切な iPlanet サーバに渡す。サイト上では、iPlanet サーバをインストールした各サーバルートに対して少なくとも 1 つの Administration Server を持つことになる
- Directory Server : iPlanet の LDAP 実装。Directory Server は、`ns-slapd` プロセス (UNIX) または `slapd` サービス (Windows NT および Windows 2000) として実行される。このサーバはディレクトリデータベースを管理し、クライアントからの要求に対応する。Directory Server は、必須のコンポーネントである

これらのさまざまなコンポーネントのインストールと構成の順番は、新規インストールの場合とアップグレードの場合で異なります。詳細は、19 ページの「インストールプロセスの概要」を参照してください。

構成の決定

Directory Server のインストール時には、基本的な構成情報を入力する必要があります。インストールする前に、これらの基本的なパラメタの構成方法を決めておいてください。実行するインストールの内容に応じて、次の項目の一部またはすべてを入力する必要があります。

- ポート番号 (13 ページの「一意のポート番号の選択」を参照)
- サーバルート (13 ページの「新しいサーバルートの作成」を参照)
- サーバを実行するユーザまたはグループ (14 ページの「iPlanet サーバ用のユーザとグループの決定 (UNIX® のみ)」を参照)
- ディレクトリ接尾辞 (16 ページの「ディレクトリ接尾辞の決定」を参照)
- いくつかの異なる認証ユーザ ID (15 ページの「認証エンティティの定義」を参照)
- 構成およびユーザの Directory Server の位置 (16 ページの「構成ディレクトリの位置の決定」および 17 ページの「ユーザディレクトリの位置の決定」を参照)
- 管理ドメイン (18 ページの「管理ドメインの決定」を参照)

一意のポート番号の選択

ポート番号には 1 から 65535 の任意の数を指定することができます。Directory Server のポート番号を選ぶ場合は、次の点に注意してください。

- 標準の Directory Server (LDAP) ポート番号は 389 である
- ポート番号 636 は LDAPS (SSL 経由の LDAP) から予約されている。したがって、ポート番号 636 が使用されていない場合でも、標準の LDAP インストールに 636 を使用しないこと。ただし、標準 LDAP ポートでは、TLS 経由の LDAP を使用することもできる
- 1 から 1024 のポート番号は、IANA (Internet Assigned Numbers Authority) によって割り当て済みである。ほかのサービスとの重複を避けるため、Directory Server で使用する 1024 以下のポート番号は、389 (LDAP で使用) と 636 (LDAPS で使用) だけに留めること
- UNIX プラットフォーム上では、ポート番号 389 または 636 で待機する場合は、Directory Server を root として実行する必要がある
- Windows NT および Windows 2000 でポート番号 389 または 636 を使用する場合は、ディレクトリサービスに administrator の特権が必要である
- 必ずほかで使用されていないポートを選択すること。また、LDAP 通信と LDAPS 通信の両方を使用している場合は、これら 2 種類のアクセスに使用されているポート番号が同じでないことを確認すること

Directory Server 用の LDAPS (SSL 経由の LDAP) の設定方法については、『iPlanet Directory Server 管理者ガイド』を参照してください。

新しいサーバルートの作成

サーバルートとは、iPlanet サーバをインストールするディレクトリのことです。iPlanet Directory Server のデフォルトのサーバルートは、`/usr/iplanet/servers` です。

サーバルートは、次の条件を満たしている必要があります。

- サーバルートはローカルディスクドライブ上のディレクトリでなければならず、ネットワークドライブにインストールすることはできない。また、AFS、NFS、SMB などのファイル共有プロトコルは、ファイルをロックできず、Directory Server での使用に適した性能を提供しない。特に、サーバデータベースインデックスファイルがローカルファイルシステム上に置かれていない場合は、これらのインデックスファイルが破損する恐れがある
- すでに存在しているディレクトリを使用してはならない。また、デフォルトは空でなければならない

- セットアッププログラムを実行しているディレクトリをサーバルートディレクトリとすることはできない

デフォルトでは、サーバルートディレクトリは次の位置になります。

- `/usr/iplanet/servers` (UNIX システム)
- `c:¥iplanet¥servers` (Windows NT および Windows 2000 システム)

iPlanet サーバ用のユーザとグループの決定 (UNIX® のみ)

セキュリティ上の理由から、UNIX ベースの実際のサーバは、通常のユーザ権限で実行するのがもっとも望ましい方法です。つまり、root 特権で Directory Server を実行するのはお勧めできません。ただし、デフォルトの Directory Server ポートを使用している場合は、root 特権で Directory Server を実行する必要があります。Directory Server を Administration Server によって起動する場合は、Administration Server を root として実行するか、または Directory Server と同じユーザとして実行する必要があります。

したがって、次の目的に対してどのユーザアカウントを使用するかを決定する必要があります。

- Directory Server を実行するユーザとグループ

  Directory Server を root として実行しない場合は、すべての iPlanet サーバに使用するユーザアカウントを作成するよう強く推奨する。既存のオペレーティングシステムアカウントは使用ない。同じく、`nobody` というアカウント名も使用しない。Directory Server ファイルに対しては共通グループを作成する必要がある。この場合も、`nobody` というグループ名は使用しない

- Administration Server を実行するユーザとグループ

  インストールにデフォルトのポート番号を使用する場合は、Administration Server を root として実行する必要がある。しかし、1024 よりも大きいポート番号を使用する場合は、すべての iPlanet サーバに対してユーザアカウントを作成し、このアカウントを使用して Administration Server を実行する必要がある

  Administration Server を root として実行する場合は、セキュリティ上の予防措置として未使用時は停止する

すべての iPlanet サーバに対して `gid iPlanet` などの共通のグループを使用し、必要な場合はサーバ間でファイルを共有できるようにします。

使用するユーザアカウントとグループアカウントがシステム上に存在することを確認してから、Directory Server および Administration Server をインストールしてください。

認証エンティティの定義

iPlanet Directory Server および Administration Server をインストールするときは、さまざまなユーザ名、識別名 (DN)、およびパスワードを入力する必要があります。このログインエンティティおよびバインドエンティティのリストは、実行するインストールのタイプによって異なります。

- ディレクトリマネージャ DN とパスワード

  ディレクトリマネージャ DN は、アクセス制御が適用されない特殊なディレクトリエントリである。ディレクトリマネージャは、ディレクトリのスーパーユーザであるとみなすことができる (以前のリリースの Directory Server では、ディレクトリマネージャ DN は root DN と呼ばれていた)

  デフォルトのディレクトリマネージャ DN は、`cn=Directory Manager` である。ディレクトリマネージャ DN は特殊なエントリなので、必ずしも Directory Server 用に構成された接尾辞に従うとは限らない。したがって、ディレクトリマネージャ DN と同じ DN を持つ実際の Directory Server エントリを手動で作成してはいけない

  ディレクトリマネージャのパスワードは、8 文字以上の ASCII 文字、数字、および記号で指定する必要がある

- 構成ディレクトリ管理者 ID およびパスワード

  iPlanet Console からアクセス可能なすべての iPlanet サーバの管理に責任のある人を、構成ディレクトリ管理者と呼ぶ。このユーザ ID でログインした場合は、iPlanet Console のサーバトポロジ領域に表示されるすべての iPlanet サーバを管理できる

  セキュリティ上の理由から、構成ディレクトリ管理者は、ディレクトリ管理者とは異なるアカウントを使用すること。デフォルトの構成ディレクトリ管理者の ID は `admin`

- Administration Server ユーザとパスワード

  このユーザとパスワードが必要になるのは、カスタムインストールのときに限られる。Administration Server ユーザは、ローカルの Administration Server に対してすべての特権を持つ特殊なユーザである。このユーザとして認証されると、ローカルサーバルートに格納されたすべての iPlanet サーバを管理できる

  Administration Server ユーザの ID とパスワードが必要となるのは、Directory Server がダウンして、構成ディレクトリ管理者としてログインできない場合に限られる。このユーザ ID でログインすると、Administration Server にアクセスして、Directory Server の起動、ログファイルの読み取りなどの障害回復操作ができる

  通常、Administration Server ユーザの ID とパスワードは、構成ディレクトリ管理者の ID とパスワードと同じにする。これは、標準インストール時のデフォルト動作である。カスタムインストール時の Administration Server ユーザのデフォルト値は、`admin`

ディレクトリ接尾辞の決定

ディレクトリ接尾辞は、ディレクトリツリーの最初のエントリを表すディレクトリエントリです。企業のデータを格納するツリーには、少なくとも 1 つのディレクトリ接尾辞が必要です。企業で使用されている DNS ホスト名に対応したディレクトリ接尾辞を使うのが、一般的なやり方です。たとえば、その企業が `siroe.com` という DNS 名を使用している場合には、`dc=siroe,dc=com` という接尾辞を選択します。

ディレクトリサービス用の接尾辞の計画については、『iPlanet Directory Server 導入ガイド』を参照してください。

構成ディレクトリの位置の決定

Directory Server 5.1 を含む多くの iPlanet サーバでは、Directory Server のインスタンスを使用して構成情報を格納します。この情報は、`o=NetscapeRoot` ディレクトリツリー内に格納されます。構成情報は、必ずしもディレクトリデータと同じ Directory Server 上に置く必要はありません。構成ディレクトリとは、iPlanet サーバが使用する `o=NetscapeRoot` ツリーを含む Directory Server です。

ほかの iPlanet サーバをサポートするためだけに Directory Server をインストールする場合は、その Directory Server が構成ディレクトリになります。一般的なディレクトリサービスの一部として使用するために Directory Server をインストールする場合は、企業内に複数の Directory Server がインストールされることになるので、どのサーバが構成ディレクトリツリーである `o=NetscapeRoot` をホストするのかを決める必要があります。これは、最初の iPlanet サーバ (iPlanet Directory Server を含む) をインストールする前に決めておいてください。

アップグレードを容易にするため、`o=NetscapeRoot` ツリーのサポート専用の Directory Server インスタンスを使用します。このサーバインスタンスでは、企業のディレクトリデータの管理に関するその他の機能は実行しないでください。また、このサーバインスタンスではポート番号 389 を使用しないでください。ポート番号 389 を使用すると、企業のディレクトリデータの管理に使用可能なホストに Directory Server をインストールできなくなる可能性があります。

通常、構成ディレクトリに対するトラフィックは極めて少ないため、ほかのもっと負荷の高い Directory Server インスタンスが置かれたマシン上にそのサーバインスタンスを一緒に置くことができます。ただし、多くの iPlanet サーバをインストールする大規模なサイトにおいては、ローエンドのマシンを構成ディレクトリ専用にし、ほかのサーバの性能を損なわないようにすることもできます。iPlanet サーバをインストールすると、構成ディレクトリへの書き込みが行われます。ある程度の大きさを持つサイトでは、この書き込み動作がほかのディレクトリの動作性能に一時的に悪影響を与えることがあります。

また、ディレクトリのインストール時は、可用性と信頼性を向上させるために、構成ディレクトリの複製を検討してください。ディレクトリの可用性向上のためにレプリケーションと DNS ラウンドロビンを使用する方法については、『iPlanet Directory Server 導入ガイド』を参照してください。

警告 構成ディレクトリツリーが破損すると、その構成ディレクトリに登録されているほかのすべての iPlanet サーバをインストールし直さなければならないことがあります。構成ディレクトリを扱う場合は、次のガイドラインに留意してください。

- 新しく iPlanet サーバをインストールしたら、必ず構成ディレクトリのバックアップをとる
- 構成ディレクトリが使用しているホスト名やポート番号は変更しない
- 構成ディレクトリツリーを直接変更しない。設定変更は、さまざまな iPlanet サーバ用のセットアッププログラムによるものに限る

ユーザディレクトリの位置の決定

構成ディレクトリが iPlanet サーバの管理で使用される Directory Server であるのと同様に、ユーザディレクトリは企業内のユーザとグループのエントリが置かれる Directory Server です。

ほとんどの場合、ユーザディレクトリと構成ディレクトリは、別個のサーバインスタンスでなければなりません。これらのサーバインスタンスは同じマシン上にインストールできますが、構成ディレクトリを別のマシン上に置く方がよい結果が得られます。

ユーザディレクトリは、構成ディレクトリよりも多くのディレクトリトラフィックを受信します。したがって、ユーザディレクトリに、最大のマシン資源を当てる必要があります。一方、構成ディレクトリが受け取るトラフィックの量は非常に少ないことが予想されるため、極めて限られた資源のマシン (最小限の装備の Pentium など) 上にインストールできます。

また、ユーザディレクトリにはデフォルトのディレクトリポート (389 および 636) を使用します。構成ディレクトリを、専用のサーバインスタンスで管理する場合には、その構成ディレクトリに対しては標準以外のポートを使用します。

ネットワーク上のどこかに構成ディレクトリをインストールするまでは、ユーザディレクトリをインストールすることはできません。

管理ドメインの決定

管理ドメインによって、サーバの管理業務を簡単に分散するために、iPlanet サーバを論理的にグループ化することができます。たとえば、会社内の 2 つの部門が、それぞれ自部門の iPlanet サーバを制御するとします。その一方で、社内のすべてのサーバを集中的に管理することも必要だとします。この場合、管理ドメインを使用することで、このような相反する要求を満たすことができます。

管理ドメインには次のような特徴があります。

- 所属するドメインにかかわらず、すべてのサーバが同じ構成ディレクトリを共有する
- 2 つの異なるドメインに属するサーバが、認証とユーザ管理に 2 つの異なるユーザディレクトリを使用できる
- 構成ディレクトリ管理者は、インストールされているすべての iPlanet サーバに対し、そのサーバが所属するドメインに関係なく、すべてのアクセス権を持つ
- 各管理ドメインは、1 人の管理ドメイン所有者とペアで構成できる。所有者は、ドメイン内のすべてのサーバに対してすべてのアクセス権を持つが、ほかの管理ドメイン内のサーバに対するアクセス権はない
- 管理ドメイン所有者は、ドメイン内のサーバごとに、個々のユーザにサーバ上での管理アクセス権限を与えることができる

インストールによっては、管理ドメインが 1 つだけになる場合があります。この場合は、その組織を識別できるような名前を付けます。それ以外の場合は、そのサイトでの必要性に応じて複数のドメインを置くことが考えられます。後者の場合、管理ドメインには、該当するドメイン内のサーバを制御する組織を識別できるような名前を付けます。

たとえば、ISP とあなたが 3 つの顧客を持ち、それぞれに iPlanet サーバをインストールして管理する場合は、それぞれの顧客にちなんだ名前を付けた 3 つの管理ドメインを作成します。

インストールプロセスの概要

Directory Server のインストールは、いくつかのインストールプロセスから 1 つを選んで行うことができます。どの方法でもインストールプロセスの指示が表示され、さまざまなコンポーネントを正しい順番でインストールできるようになっています。

以降の節では、利用できるインストールプロセス、旧リリースの iPlanet Directory Server からのアップグレード方法、およびインストールの準備のためのソフトウェアの開梱方法についての概要を示します。

インストールプロセスの選択

Directory Server ソフトウェアのインストールでは、セットアッププログラムに用意された次の 4 つのインストール方法の中から 1 つを選択します。

- **高速インストール** : 評価やテストの目的で iPlanet Directory Server をインストールする場合は、この方法を使用する。高速インストールについては、47 ページの「高速インストールの使用」を参照
- **標準インストール** : 通常の構成で Directory Server をインストールする場合は、この方法を使用する。標準インストールについては、49 ページの「標準インストールの使用」を参照
- **カスタムインストール** : iPlanet Directory Server 5.1 でのカスタムインストールプロセスは、標準インストールプロセスとよく似ている。主な違いは、カスタムインストールプロセスでは、デフォルトで作成されたユーザディレクトリデータベースを、初期化するために LDIF ファイルをインポートできるという点
- **サイレントインストール** : インストールプロセスをスクリプト化する場合は、この方法を使用する。この方法は、企業で複数のコンシューマサーバをインストールする場合などに便利。サイレントインストールについては、第 4 章「サイレントインストール」を参照

使用するインストールプロセスの決定によらず、iPlanet Directory Server のインストールには次のプロセスがあります。

1. ディレクトリサービスの内容を決めます。事前にディレクトリツリーの構造を決めておくことにより、組織が拡大した場合でも管理と拡張が容易なサービスを設計できます。ディレクトリサービスの内容を計画する上でのガイダンスについては、『iPlanet Directory Server 導入ガイド』を参照してください。
2. このマニュアルに記載されている手順に従って Directory Server をインストールします。

3. ディレクトリ接尾辞とデータベースを作成します。この時点でディレクトリを入力する必要はありませんが、主なルートおよび分岐点を含むツリーの基本的構造を作成する必要があります。ディレクトリエントリを作成する別の方法については、『iPlanet Directory Server 管理者ガイド』を参照してください。
4. 追加の Directory Server インスタンスを作成し、Directory Server 間のレプリケーションアグリーメントを確立してデータを使用できるようにします。

アップグレードプロセス

iPlanet Directory Server 5.1 は、Directory Server 4.1、4.11、4.12、および 5.0 からの移行をサポートしています。移行プロセスについては、第 6 章「旧バージョンからの移行」を参照してください。

レプリケーションアグリーメントに関するサーバの移行については、『iPlanet Directory Server 管理者ガイド』を参照してください。

ソフトウェアの開梱

iPlanet Web サイトから iPlanet Directory Server 5.1 ソフトウェアをダウンロードした場合は、ソフトウェアを解凍してからインストールを始めます。

1. 次のコマンドを実行して、インストール用に新しいディレクトリ作成します。

   ```
   # mkdir ds5.1
   ```

   ```
   # cd ds5.1
   ```
2. 製品のバイナリファイルをインストールディレクトリにダウンロードします。
3. UNIX の場合は、次のコマンドを実行して製品のバイナリファイルを解凍します。

   ```
   # gzip -dc file_name.tar.gz | tar -xvof -
   ```

   ここでの *file_name* は、解凍する製品のバイナリファイル名を表します。

   Windows NT および Windows 2000 の場合は、製品バイナリファイルを解凍 (unzip) します。

インストール特権

UNIX では、デフォルトの LDAP ポートである 389 や 636 (LDAPS) など、1024 以下のポートでサーバを実行する場合は、root としてインストールする必要があります。1024 よりも大きいポート番号を使用する場合は、有効なものであればどの UNIX ログイン名でもインストール可能です。

Windows NT または Windows 2000 では、administrator としてインストールを行う必要があります。

環境変数の設定解除 (AIX のみ)

AIX マシン上に Directory Server をインストールする場合は、インストールプログラムによって次のファイルが実行されます (使用しているシェルによって異なる)。

シェル名	ファイル
sh (bourne シェル)	$HOME/.profile
csh および tcsh シェル	$HOME/.login $HOME/.cshrc
ksh (korn シェル)	$HOME/.profile $HOME/.kshrc
bash (bourne again シェル)	$HOME/.profile $HOME/.bashrc

各シェル内の環境変数の設定は、インストールプログラムによって解除されません。したがって、ファイルに印刷出力やその他の情報が含まれている場合は、予期しないエラーメッセージや動作を示し、インストールに影響を及ぼすことがあります。

たとえば、korn シェル内の .profile および .kshrc ファイルの設定を解除するには、次のコマンドを実行します。

```
unset ENV
```

第 2 章

コンピュータシステムの要件

iPlanet Directory Server 5.1 をインストールする前に、ソフトウェアをインストールするシステムが、ハードウェアおよびオペレーティングシステムの最低限の要件を満たしているかどうかを確認しておく必要があります。

以降の節では、これらの要件について、プラットフォームごとに詳しく説明します。

- サポートされているプラットフォーム
- オペレーティングシステムの要件
- ハードウェアの要件

サポートされているプラットフォーム

iPlanet Directory Server 5.1 は、Sun Solaris 9 for UltraSPARC (32 および 64 ビット) および Sun Solaris 9 for x86 オペレーティング環境にプリインストールされています。Solaris 9 プラットフォームで Directory Server を構成する方法の詳細は、Solaris の『System Administration Guide: Naming and Directory Services, Vol. 5』を参照してください。

このマニュアルでは、サポートされている次のプラットフォームに iPlanet Directory Server 5.1 をインストールする方法について説明します。

- Sun Solaris 8 for UltraSPARC (32 および 64 ビット) オペレーティング環境
- Microsoft Windows NT 4.0 Server Service Pack 6A (x86 のみ)
- Microsoft Windows 2000 Server および Advanced Server Service Pack 2 (x86 のみ)
- Hewlett-Packard HP-UX 11.0 (PA-RISC 1.1 または 2.0)
- IBM AIX 4.3.3 (Power PC)

このリリースの Directory Server は、Linux、Tru64 UNIX、OpenVMS ではサポートされていません。

注	以降の節の説明に従い、プラットフォームごとに必要なパッチとカーネルのパラメタ設定を確認してください。

ハードウェアの要件

いずれのプラットフォームにおいても、次の条件を満たしている必要があります。

- 最小限の設定によるインストールの場合、約 2G バイトのディスク容量。実際のシステムで、製品のバイナリファイル、データベース、ログファイル (ログファイルにはデフォルトで 1G バイト必要) を扱うには、最低でも 2G バイトが必要。非常に大規模なディレクトリの場合は 4G バイト以上必要になることがある
- 256M バイトの RAM。ただし、大規模な実際のシステムにおいては、最適な性能を実現するために、256M バイトから 1G バイトの RAM の実装を計画しておくべきである

次の表に、Directory Server が管理するエントリの数に応じて必要なディスク容量とメモリーのガイドラインを示します。この表は、LDIF ファイル内のエントリのサイズが約 100 バイトで、推奨されるインデックスだけが設定されていることを前提としています。それより大きなエントリを使用する場合は、LDIF ファイルの少なくとも 4 倍の空き容量をディスク上に確保してください。

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

オペレーティングシステムの要件

この節では、必要なオペレーティングシステムのバージョンとパッチについて説明します。

idsktune ユーティリティ

UNIX プラットフォーム用の iPlanet Directory Server には、システム上に適切なパッチがインストールされているかどうかを確認するためのユーティリティが備わっています。また、このユーティリティにより、カーネルのパラメタを変更して性能を最適化するための情報とアドバイスを得ることができます。このユーティリティは `idsktune` と呼ばれ、`/usr/iplanet/servers/bin/slapd/server` ディレクトリに置かれています。`idsktune` の実行方法については、第 7 章「トラブルシューティング」を参照してください。

注	iPlanet Directory Server をインストールする前に、DNS がシステム上に適切に構成されており、システムが静的な IP アドレスを保持していることを確認してください。

Solaris 8 オペレーティングシステム

このリリースの iPlanet Directory Server は、Solaris 2.6 以前および Solaris 7 ではサポートされていません。

このリリースの iPlanet Directory Server は 64 ビットの Solaris 8 環境でも使用できますが、32 ビットプロセスとして稼働し、プロセスメモリーも 3.7G バイトに制限されます。

ディスク容量の要件

ソフトウェアをダウンロードする前に、充分なディスク容量があることを確認してください。

ダウンロード先となるディレクトリ : 120M バイト
`/usr/iplanet` を含むパーティション : 2G バイト

システムモジュールの要件

注	iPlanet Directory Server 5.1 は、UltraSPARC チップセットに合わせて最適化されているため、SPARCv8 以前のチップセットでは動作しません。

パッチ

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してください。Sun の推奨パッチクラスタは、`http://sunsolve.sun.com` あるいは Solaris のサポートベンダから入手可能です。

システムにインストールされているパッチを確認するには、`patchadd -p` を使用します。

iPlanet Directory Server とともにインストールされる `idsktune` ユーティリティでは、パッチを追加してインストールするように推奨されている場合があります。`idsktune` の実行方法については、第 7 章「トラブルシューティング」を参照してください。

パッチのインストールが完了したら、マシンを再起動してください。

セキュリティ上の問題に対応する方法については、`http://www.sun.com/blueprints/0100/security.pdf` にある Solaris Operating Environment Security Sun Blueprint を参照してください。

システムのチューニング

基本的な Solaris のチューニングに関するガイドラインを示した本が何冊か出版されています。『Sun Performance and Tuning: Java and the Internet』(ISBN 0-13-095249-4) はその一例です。詳細なチューニング情報に関しては、`http://docs.sun.com/ab2/coll.707.1/` にある『Solaris Tunable Parameters Reference Manual』(806-4015) を参照してください。

ファイルディスクリプタ

iPlanet Directory Server に設定できる同時接続の数は、システム全体としてのファイルディスクリプタテーブルの最大サイズの設定によって決まります。管理パラメタ `rlim_fd_max` は、`/etc/system` ファイル内に設定されます。このパラメタが存在しない場合、デフォルトでは最大サイズは 1024 に設定されます。`/etc/system` に次の行を追加することにより、4096 まで値を大きくすることができます。

```
set rlim_fd_max=4096
```

変更が完了したらシステムを再起動してください。このパラメタを 4096 よりも大きな値に設定する場合は、システムの安定性に悪影響を及ぼすことがないか、設定の前に必ず Sun Solaris のサポート窓口に相談してください。

TCP のチューニング

デフォルトでは、Solaris カーネルの TCP/IP 実装は、インターネットまたはインターネットサービス用に最適化されていません。次の /dev/tcp チューニングパラメタを確認し、必要な場合は、インストール環境のネットワークトポロジに合わせて変更してください。

Solaris 8 の tcp_time_wait_interval は、TCP 接続を閉じてからカーネルのテーブル内に接続をそのまま維持する時間をミリ秒で設定します。この値が 30000 (30 秒) よりも大きく、ディレクトリが LAN、MAN、または単一ネットワークの管理下で使用されている場合は、/etc/init.d/inetinit ファイルに次のような行を追加して、値を減らす必要があります。

```
ndd -set /dev/tcp tcp_close_wait_interval 30000
```

tcp_conn_req_max_q0 および tcp_conn_req_max_q パラメタは、iPlanet Directory Server プロセスのためにカーネルが受け入れる接続のバックログの最大値を制御します。多数のクライアントホストによって 1 つのディレクトリが同時に使用されることが予想される場合は、/etc/init.d/inetinit ファイルに次のような行を追加して、これらの値を少なくとも 1024 に増やす必要があります。

```
ndd -set /dev/tcp tcp_conn_req_max_q0 1024
ndd -set /dev/tcp tcp_conn_req_max_q 1024
```

tcp_keepalive_interval は、各 TCP オープン接続に対し、Solaris が keep-alive パケットを送る間隔を秒数で指定します。このパラメタは、ネットワークから接続が解除されたクライアントへの接続を削除するときに使用することもできます。

LAN、または高速の MAN や WAN 上でサーバの性能テストを行う場合は、tcp_rexmit_interval_initial の値を確認します。広域のインターネット上での運用では、この値を変更する必要はありません。

tcp_smallest_anon_port は、サーバに対して設定できる同時接続の数を制御します。rlim_fd_max の値を 4096 以上に増やした場合は、/etc/init.d/inetinit ファイルに次のような行を追加することによって、この値を減らす必要があります。

```
ndd -set /dev/tcp tcp_smallest_anon_port 8192
```

クライアントが主に Windows TCP/IP スタックを使用する場合は、tcp_slow_start_initial パラメタを確認します。

Windows NT 4.0 サーバ

この節では、Windows NT 上への iPlanet Directory Server のインストール方法について説明します。

iPlanet Directory Server 実行のためのマシンの構成

iPlanet Directory Server をインストールするコンピュータは、ネットワークレベルのファイアウォールによって、公共インターネットから隔離する必要があります。これは、Windows NT オペレーティングシステムを IP ベースの攻撃から守るために必要です。

このコンピュータにはほかのネットワーク機能を持たせないようにします。このコンピュータはデュアルブートシステムであってはならず、また、ほかのオペレーティングシステムを実行してはなりません。コンピュータシステムには、最低限 256M バイトの RAM、2G バイトのディスク容量、Pentium II 以上のプロセッサ、100Mbps のイーサネット接続が必要です。

ソフトウェアをダウンロードする前に、充分なディスク容量があることを確認してください。

- ダウンロード先となるドライブ : 120M バイト
- インストールドライブ : 200M バイト

システムモジュールの要件

iPlanet Directory Server 5.1 は、Windows NT 3.5.1 以前のリリース、または Alpha アーキテクチャの Windows NT ではサポートされていません。また、Windows NT Workstation でもサポートされていません。これは、このオペレーティングシステムの形式が、スケーラブルなインターネットサーバまたはイントラネットサーバの配置に適していないためです。Windows NT Workstation は、接続バックログの設定に制限があります。Windows NT Server では、接続バックログを 10 より大きい値に設定できます。負荷の大きな TCP/IP サーバにおいては、この程度のバックログが必要となります。

Windows NT Server のインストール

Windows NT をインストールするときは、次の事項に従ってください。

- すでにコンピュータ上にオペレーティングシステムがインストールされている場合でも、アップグレードではなく新規インストールを選択する
- NTFS ではファイルおよびディレクトリにアクセス制御を設定できるので、FAT ではなく NTFS でドライブをフォーマットする

- スタンドアロンサーバとしてコンピュータを設定し、既存のドメインやワークグループのメンバーにはしない。これによって、ネットワークセキュリティサービスへの依存度を下げることができる
- 管理者用パスワードは 9 文字以上にする。最初の 7 文字の中には、句読文字またはアルファベット以外の文字を使用する
- IIS (Internet Information Server) はインストールしない
- ネットワークプロトコルとしては TCP/IP だけを指定し、その他のネットワークサービスはインストールしない

サードパーティユーティリティのインストール

Directory Server ソフトウェアを解凍するには、UNZIP ユーティリティが必要です。PKZIP や Winzip を始めとして、ライセンスが必要な市販ツール、フリーウェアやシェアウェアなどの多くのツールがあります。PKZIP 2.70 はシェアウェアですが、未登録のものはインターネット上の広告サービスなどに TCP/IP 接続されるので、このシステムへのインストールには必ずしも適していません。

マニュアルを読むには、Adobe Acrobat Reader をインストールする必要があります。Acrobat Reader は、次のサイトからダウンロードできます。

```
http://www.adobe.com/products/acrobat/readstep2.html
```

サーバ構成ファイルを編集するには、大容量のテキストファイルの処理が可能なテキストエディタが必要です (メモ帳とワードパッドは適さない)。UNIX の Emacs を使い慣れている場合は、`ftp://ftp.cs.washington.edu/pub/ntemacs/` から Windows 版をダウンロードできます。その他多くのシェアウェアや市販のテキストエディタが入手可能です。

Netscape ブラウザで英語以外の文字を表示する場合は、次の URL から国際化に関する一般的なアドバイスおよび Bitstream Cyberbit フォント固有の情報を入手できます。

```
http://developer.netscape.com/software/jdk/i18n.html
```

Bitstream Cyberbit フォントをダウンロードする場合は、次の ftp リンクを使用してください。

```
ftp://ftp.netscape.com/pub/communicator/extras/fonts/windows
```

フォントをダウンロードする前に、`READMEfirst.txt` および `ReadMe.htm` をお読みください。

Microsoft ユーティリティのインストール

Windows NT オペレーティングシステムのセキュリティ機能を向上させるには、次の追加ユーティリティを推奨します。これらのユーティリティは、iPlanet Directory Server の操作に必須のものではありません。

Microsoft Press 製の Resource Kit CD-ROM がある場合は、Windows NT Server Resource Kit から「passprop.exe」というユーティリティをシステム上にコピーします。このユーティリティは、CD の i386\netadmin ディレクトリに置かれています。これは、管理者アカウントのロックアウトができるように、あとで必要になります。

Service Pack 4 以降がまだインストールされていない場合は、この時点でインストールする必要があります。これは、Microsoft Internet Explorer 5 のインストールに必要です。サービスパックは、http://www.microsoft.com/windows/servicepacks/ から入手できます。

Microsoft Internet Explorer 5 以降はセキュリティ構成マネージャで使用するので、インストールしておく必要があります。

Microsoft のセキュリティ構成マネージャは、Service Pack 4 の CD-ROM に収められています。
また、ftp://ftp.microsoft.com/bussys/winnt/winnt-public/tools/scm/ からダウンロードすることもできます。このツールについては、Microsoft Knowledge Base の Article Q195227 を参照してください。

システム時刻の正確性の確認

ログファイルの時刻および日付のタイムスタンプがほかのコンピュータシステムのタイムスタンプと連動して使用できるように、システム時刻は正しく、充分な精度で同期させる必要があります。NET TIME コマンドは NetBIOS を必要としますが、NetBIOS はインストール後のシステム設定中は無効にされるため、TCP/IP ベースの NTP クライアント (シェアウェアプログラム Tardis など) をインストールするか、その他の時刻を同期させる仕掛けを実装します。Windows NT 用の NTP クライアントについては、http://www.ntp.org/ を参照してください。

Windows のサービスパックとホットフィックス (Hotfix) のインストール

Windows NT のサービスパックには、オペレーティングシステムのセキュリティと信頼性を維持するのに重要な修正が含まれています。ホットフィックス (Hotfix) シリーズには、サービスパックリリース後に確認された問題に対する重要な変更が含まれています。

Windows NT 4.0 Service Pack 6a 以降のインストール

このサービスパックは、http://www.microsoft.com/windows/servicepacks/ からダウンロードできます。サービスパックのインストール後に、システムは再起動されます。

ホットフィックス (Hotfix) のインストール

Service Pack 6a 用の `post-sp6a` など、システムにインストールされているサービスパックに対応した Windows NT 4.0 ホットフィックス (Hotfix) をダウンロードしてインストールします。ホットフィックス (Hotfix) は、`ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/` からダウンロードできます。通常、各ホットフィックス (Hotfix) のインストール後は、システムを再起動する必要があります。

TCP ISN パッチのインストール

ディレクトリにアクセスするユーザの認証を行う場合は、TCP 接続に対するハイジャック攻撃が弱点となります。Microsoft は、シリアル番号に関するセキュリティを強化するためのパッチ、`q243835i.exe` をリリースしています。詳細は、以下を参照してください。

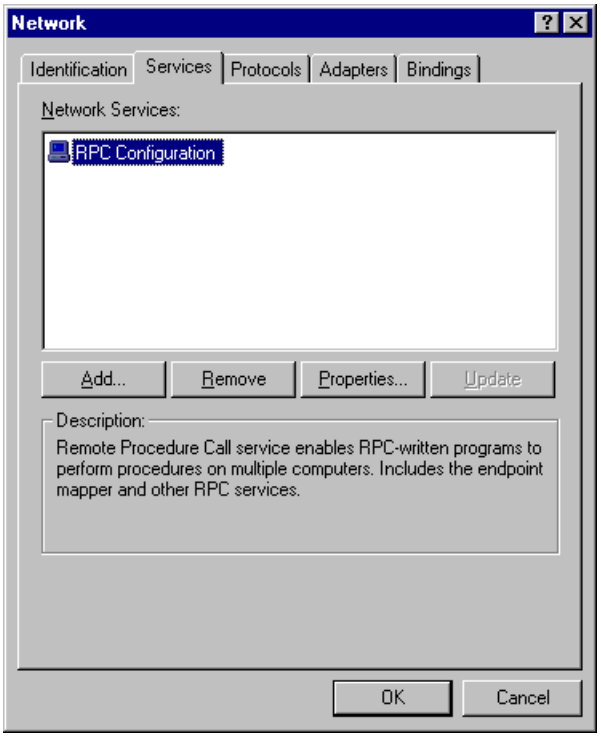
```
http://www.microsoft.com/security/bulletins/ms99-046.asp
```

インストール後に行うその他のシステム構成

Windows 環境では、動作環境内での iPlanet Directory Server の性能を最適化するためのチューニングが必要です。マルチスレッドのインターネットサービスのための Windows NT のチューニング方法については、Windows のシステム管理者用マニュアルを参照してください。以降の節に、いくつかのガイドラインを示します。

ネットワークサービスの制限

iPlanet Directory Server ではネットワークによるファイル共有は必要ないので、無効にする必要があります。「コントロールパネル (Control Panel)」の「ネットワーク (Network)」アイコンを開きます。「サービス (Network Services)」タブから、「ワークステーション (Workstation)」、「コンピュータブラウザ (Computer Browser)」、「NetBIOS インターフェイス (NetBIOS Interface)」、「リモートアクセスサービス (Remote Access Service)」、「サーバーサービス (Server Services)」を削除します。「RPC 構成」はそのまま残します。

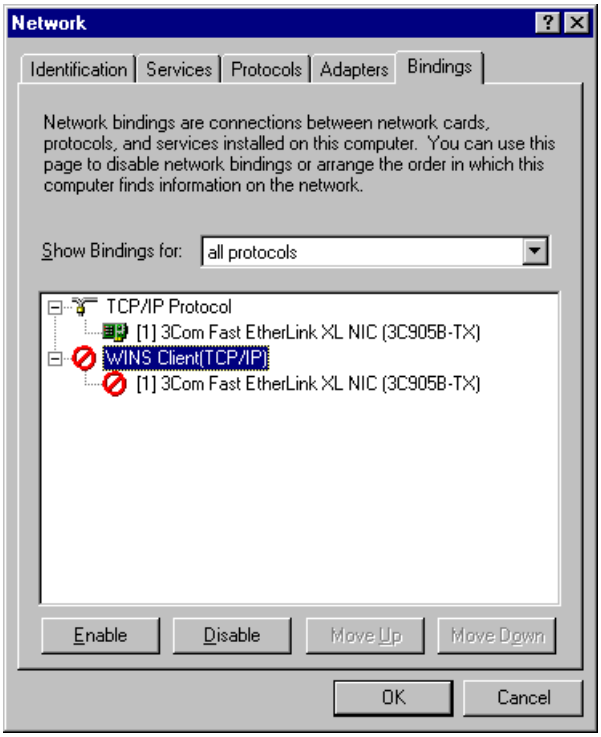


SNMP 監視機能を使用する場合は、SNMP サービスを残すことも可能です。

これ以後、「コントロールパネル (Control Panel)」の「ネットワーク (Network)」アイコンを開くたびに、Windows NT Networking のインストールを求めるダイアログボックスが表示されます。このダイアログボックスに対しては、常に「いいえ (No)」と応答してください。

NETBIOS の削除

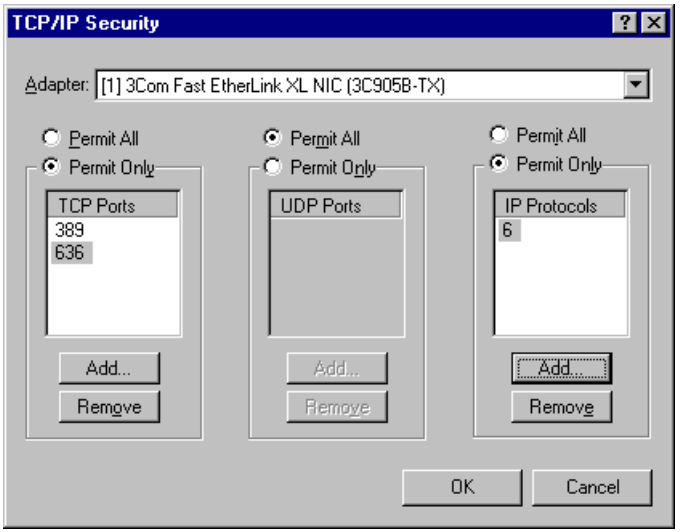
サーバでは TCP/IP だけを使用するので、Microsoft のネットワークサービスは必要ありません。「コントロールパネル (Control Panel)」の「ネットワーク (Network)」アイコンを開き、「バインド (Bindings)」タブで「すべてのプロトコル (All Protocols)」を選択します。次に「WINS クライアント (WINS Client)」を無効にします。これによって、NETBIOS と TCP/IP のバインドが解除されます。



ポートフィルタリングの有効化

RPC サービスは、Microsoft ソフトウェアがループバックインタフェース上で RPC 接続を確立するために必要になることがあるので、削除しません。ただし、RPC ポートはほかのシステムにアクセスできないようにする必要があります。

「コントロールパネル (Control Panel)」の「ネットワーク (Network)」アイコンを開き、「プロトコル (Protocols)」タブを選択します。次に、「TCP/IP プロトコル (TCP/IP)」>「プロパティ (Properties)」ボタン >「詳細 (Advanced)」>「セキュリティ処理を行う (Enable Security and Configure)」の順に選択します。「TCP/IP のセキュリティ (TCP/IP Filtering)」ウィンドウで、TCP ポート 389 と 636、管理ポート番号、および IP プロトコル 6 (TCP) だけを許可し、UDP ポートは許可しないように設定します。インタフェースが複数ある場合、インタフェースごとにこの操作を繰り返す必要があります。



この変更を加えたあとは、Microsoft コマンド行 FTP クライアントは使用できなくなります。これは、Microsoft クライアントでは FTP サーバが逆方向の接続を確立しなければならないにもかかわらず、LDAP 以外のポートはすべてブロックされているためです。

IP 転送の無効化

「TCP/IP プロトコル (TCP/IP Protocol)」のウィンドウで、「IP 転送を行う (IP Routing)」を無効にします。

WINS クライアントの無効化

「コントロールパネル (Control Panel)」の「デバイス (Devices)」アイコンを開き、「WINS Client」を無効にします。

レジストリからの OS/2 および POSIX サブシステムキーの削除

iPlanet Directory Server には、OS/2 および POSIX サブシステムは必要ありません。`regedit` を使用して次のレジストリ操作を行い、これらを削除します。

次のすべてのサブキーを削除します。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for NT
```

CurrentControlSet\Control の下には SessionManager (名前にスペースは入りません) という名前の別のキーがあります。このキーの下にあるものには変更を加えないでください。

このキーの中にある Os2LibPath の値を削除します。

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment
```

次のキーの「Optional」の項目の値を 2 バイトの「00 00」に変更します。

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems
```

次のキーから Posix および OS/2values を削除します。

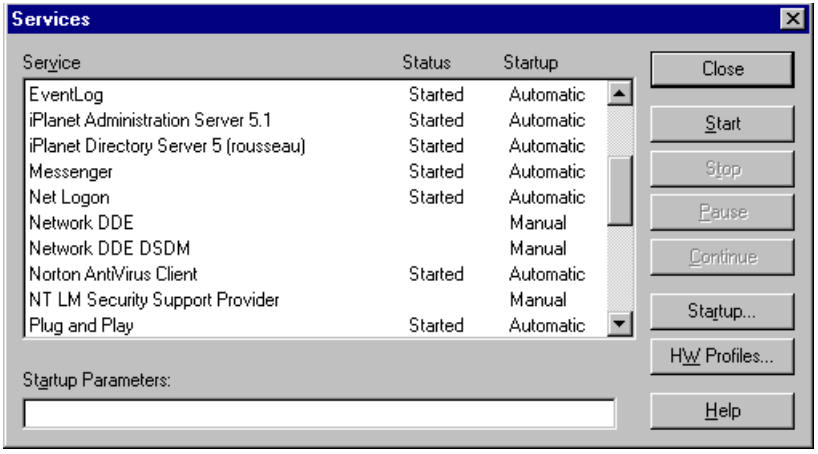
```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems
```

OS/2 DLL の削除

`%SystemRoot%\system32\os2` ディレクトリおよびそのすべてのサブディレクトリ内のすべてのファイルを削除します。

不要なサービスの停止

「コントロールパネル (Control Panel)」の「サービス (Services)」アイコンを開きます。EventLog、iPlanet Directory Server、iPlanet Administration Server、NT LM Security Support Provider、Plug and Play、Protected Storage、Remote Procedure Call (RPC) Service、および SNMP 以外の、すべてのサービスは停止および無効化しておきます。ただし、「スタートアップ (Startup)」が「手動 (Manual)」になっているサービスは、無効にする必要はありません。

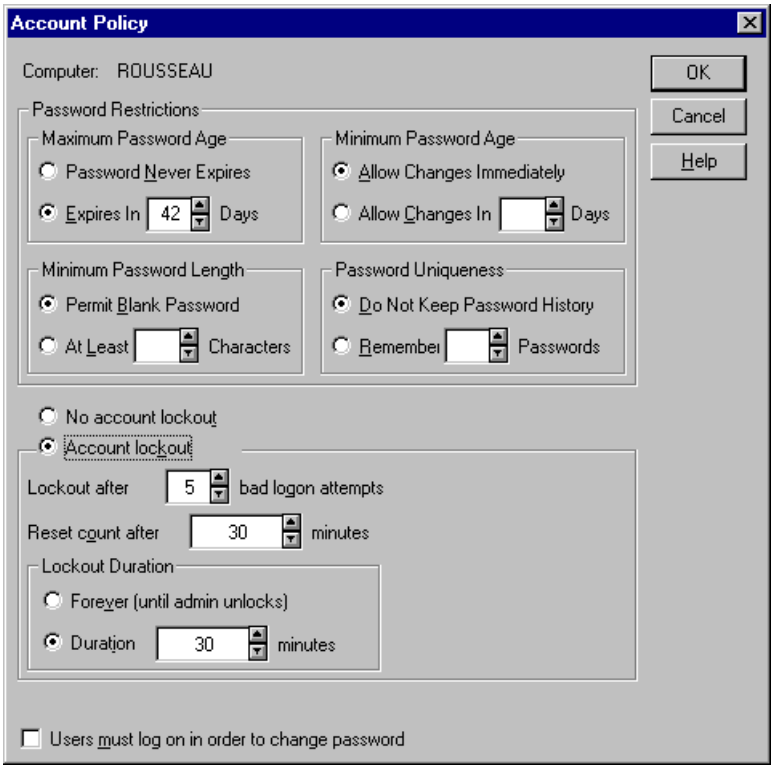


エラー発生時のシステムの再起動の自動化

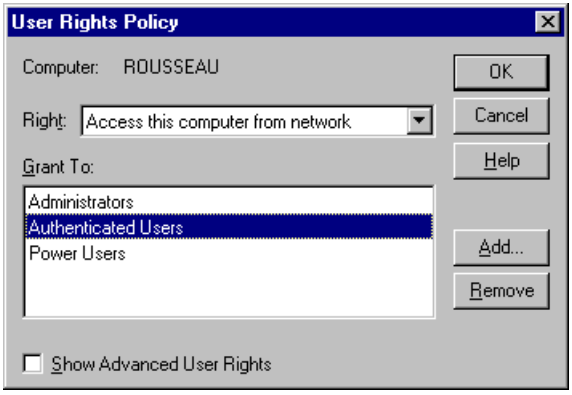
「コントロールパネル (Control Panel)」の「システム (System)」アイコンを開きます。「起動 / シャットダウン (Startup/Shutdown)」タブで、「待ち時間 (Show list time)」を 0 秒に設定し、「自動的に再起動する (Automatic reboot)」チェックボックスの選択を解除します。

ユーザアカウントの構成

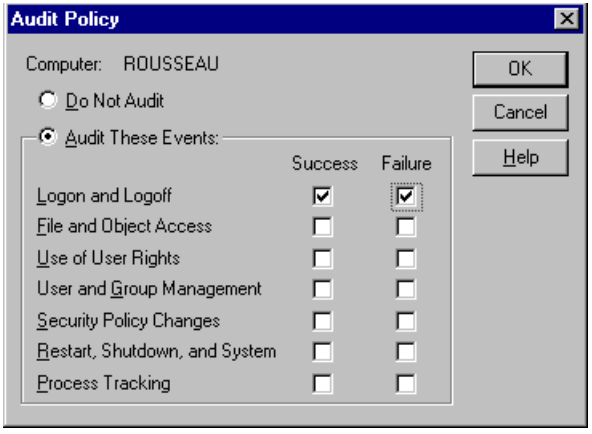
管理ツールを開きます (「スタート (Start)」> 「プログラム (Programs)」> 「管理ツール (Administrative Tools)」> 「ユーザーマネージャ (User Manager)」)。「原則 (Policies)」メニューの「アカウント (Account)」を選択して「アカウントの原則 (Account Policies)」ウィンドウを表示します。ロックアウトするアカウントのチェックボックスを選択します。



次に、「原則 (Policies)」メニューの「ユーザーの権利 (User Rights)」を選択します。「ネットワーク経由でコンピュータへアクセス (Access this computer from the network)」を選択して、「Everyone」を削除し、リストに「Authenticated Users」を追加します。



次に、「原則 (Policies)」メニューの「監査 (Audit)」を選択します。ダイアログで「監査するイベント (Audit These Events)」を選択し、「ログオンとログオフ (Logon and Logoff)」イベントの「成功 (Success)」および「失敗 (Failure)」ボックスの両方にチェックマークを付けます。



管理者アカウント名を、部外者が推測できないような名前に変更することもできます。

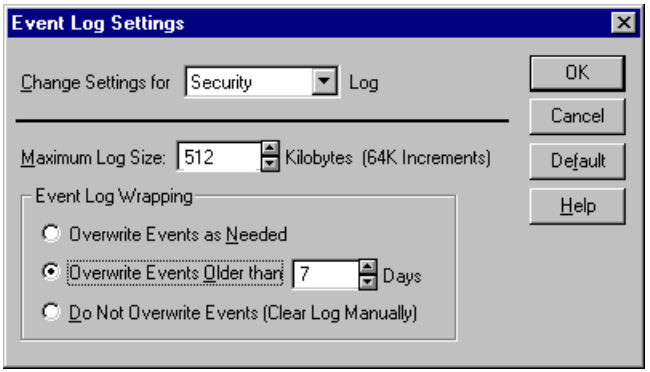
NT Server Resource Kit から `passprop` ユーティリティをコピーした場合は、これをコマンド行で `passprop/adminlockout` として実行すると、管理者アカウントのロックアウトを可能にすることができます。

アカウントデータベースの暗号化

syskey プログラムを実行すると、Windows NT のユーザアカウントデータベースである SAM を保護します。このプログラムは、管理者用のパスワードを暗号化し、レジストリ抽出型のハッカーツールでパスワードを使用できないようにします。

イベントログの構成

イベントビューアを開き (「スタート (Start)」> 「プログラム (Programs)」> 「管理ツール (Administrative Tools)」> 「イベントビューア (Event Viewer)」)、「イベントログの処理」(「ログ (Log)」> 「ログの設定 (Log Settings)」にある) の値をユーザの導入に適した値に設定します。



チューニングパラメタの構成

転送制御ブロック (TCB) は、各 TCP 接続のデータを格納します。制御ブロックは、アクティブな接続ごとに TCB ハッシュテーブルに追加されます。LDAP 接続が TCP/IP によってサーバに達したときに充分な制御ブロックがない場合は、追加制御ブロックが作成されるのを待つため、さらに遅延が生じます。TCB timewait テーブルのサイズを大きくすることによって、より多くのクライアント接続に対するサービスが高速になるため、応答時間の負荷を削減できます。この値を調整するには、次のレジストリキーにパラメタを追加します。

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
```

ここに、MaxFreeTcbs の値を 0xFA0 にして追加します。

この例では、TCB timewait テーブルのサイズを、デフォルトの 2,000 エントリから 4,000 エントリに増やしています。これで iPlanet Directory Server の TCP によるオーバーヘッド時間が小さくなったので、次に対応する TCB 保存用のハッシュテーブルを調整します。ハッシュテーブルの調整は、次のレジストリキーにパラメタを追加して行います。

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

ここに、MaxHashTableSize の値を 0x400 にして追加します。

これによって TCB ハッシュテーブルのサイズが 512 から 1,024 になり、より多くの接続情報を格納できるようになります。TCB 情報は、ページ分けされていないメモリプールに格納されます。iPlanet Directory Server にメモリー上のボトルネックが生じ、サーバに対してそれ以上のメモリーを割り当てられない場合は、上記の値を小さくしてください。

マルチプロセッサシステム上では、NIC と CPU の関係を最適化することを推奨します。ネットワーク経由で LDAP 要求が受信されると、サービスを要求しているプロセッサでは割り込みが発生します。プロセッサによって、割り込み要求の緊急度が高い (割り込みレベルが高い) ものではないと判断されると、その要求の処理は延期されます。この延期された割り込み要求が DPC (Deferred Procedure Call) となります。サーバが受ける要求が増えるに従って、割り込みと DPC の数は増えていきます。

割り込みが特定の CPU に送られ、その処理が延期された場合、この DPC がサーバ内のほかの CPU に送られると (サーバが SMP に対応している場合)、サーバの負荷がさらに増えることになります。これは、Windows のデフォルト動作で、性能の面から考えると好ましくありません。このような DPC の転送が発生しないようにするには、次のレジストリにパラメタを追加します。

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NDIS\Parameters

ここに、ProcessorAffinityMask の値を 0 にして追加します。

これによって、割り込みを処理した CPU が、その CPU に対応する DPC の処理も行うようになります。また、1 つまたは複数のネットワークインタフェースカードが、特定の CPU に固定されないことを保障します。その結果、割り込みとネットワークインタフェースカードで生成される DPC に対する CPU の処理が改善されます。

Windows NT には、TCP/IP、NBF (NetBEUI)、および NWLink など、さまざまな転送ドライバが付属しています。これらの転送では、すべて TDI インタフェースを最上層に、NDIS (Network Driver Interface Specification) を最下層にしてエクスポートが行われます (Windows NT には AppleTalk と DLC も付属していますが、これらには TDI インタフェースがありません)。TCP/IP プロトコルがバインドリストの最初にある場合は、接続の平均セットアップ時間が短くなります。

Windows NT では、TCP の高速な転送と回復のための Van Jacobson アルゴリズムを実装し、ACKS 受信時に、再送タイマーの時間切れを待つことなく、失われたセグメントを迅速に転送し直すことができます。Van Jacobson アルゴリズムを実装するには、次のパラメタを編集します。

HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Tcpip/Parameters

ここで、TcpMaxDupAcks という名前の値を追加して、タイプを REG_DWORD に、値を ACK の数に設定します。有効な値は 1 から 3 で、デフォルトは 2 です。

Windows 2000 Server および Advanced Server

iPlanet Directory Server 実行のためのマシンの構成

iPlanet Directory Server をインストールするコンピュータは、ネットワークレベルのファイアウォールによって、公共インターネットから隔離する必要があります。これは、オペレーティングシステムを IP ベースの攻撃から守るために必要です。

このコンピュータにはほかのネットワーク機能を持たせないようにします。このコンピュータはデュアルブートシステムであってはならず、また、ほかのオペレーティングシステムを実行してはなりません。コンピュータシステムには、256M バイトの RAM、16M バイトのディスク容量、Pentium II 以上のプロセッサ、100Mbps のイーサネット接続が最低限必要です。

ソフトウェアをダウンロードする前に、充分なディスク容量があることを確認してください。

- ダウンロード先となるドライブ : 120M バイト
- インストールドライブ : 200M バイト

システムモジュールの要件

iPlanet Directory Server 5.1 は、Windows 2000 Pro および Windows 2000 DataCenter サーバではサポートされていません。

Windows 2000 サーバのインストール

Windows 2000 をインストールするときは、次の事項に従ってください。

- すでにコンピュータ上にオペレーティングシステムがインストールされている場合でも、アップグレードではなく新規インストールを選択する
- NTFS ではファイルおよびディレクトリにアクセス制御を設定できるので、FAT ではなく NTFS でドライブをフォーマットする
- スタンドアロンサーバとしてコンピュータを設定し、既存のドメインやワークグループのメンバーにはしない。これによって、ネットワークセキュリティサービスへの依存度を下げることができる
- 管理者用パスワードは 9 文字以上にする。最初の 7 文字の中には、句読文字またはアルファベット以外の文字を使用する
- IIS (Internet Information Server) はインストールしない

- ネットワークプロトコルとしては TCP/IP だけを指定し、その他のネットワークサービスはインストールしない

サードパーティユーティリティのインストール

Directory Server ソフトウェアを解凍するには、UNZIP ユーティリティが必要です。PKZIP や Winzip を始めとして、ライセンスが必要な市販ツール、フリーウェアやシェアウェアなどの多くのツールがあります。PKZIP 2.70 はシェアウェアですが、未登録のものはインターネット上の広告サービスなどに TCP/IP 接続されるので、このシステムへのインストールには必ずしも適していません。

マニュアルを読むには、Adobe Acrobat Reader をインストールする必要があります。Acrobat Reader がインストールされていない場合は、次のサイトからダウンロードできます。

```
http://www.adobe.com/products/acrobat/readstep2.html
```

サーバ構成ファイルを編集するには、大容量のテキストファイルの処理が可能なテキストエディタが必要です (メモ帳とワードパッドは適さない)。UNIX の Emacs を使い慣れている場合は、`ftp://ftp.cs.washington.edu/pub/ntemacs/` から Windows 版をダウンロードできます。その他多くのシェアウェアや市販のテキストエディタが入手可能です。

Netscape ブラウザで英語以外の文字を表示する場合は、次の URL から国際化に関する一般的なアドバイスおよび Bitstream Cyberbit フォント固有の情報を入手できます。

```
http://developer.netscape.com/software/jdk/i18n.html
```

Bitstream Cyberbit フォントをダウンロードする場合は、次の ftp リンクを使用してください。

```
ftp://ftp.netscape.com/pub/communicator/extras/fonts/windows
```

フォントをダウンロードする前に、`READMEfirst.txt` および `ReadMe.htm` をお読みください。

システム時刻の正確性の確認

ログファイルの時刻および日付のタイムスタンプがほかのコンピュータシステムのタイムスタンプと連動して使用できるように、システム時刻は正しく、充分な精度で同期させる必要があります。NET TIME コマンドは NetBIOS を必要としますが、NetBIOS はインストール後のシステム設定中は無効にされるため、TCP/IP ベースの NTP クライアント (シェアウェアプログラム Tardis など) をインストールするか、その他の時刻を同期させる仕掛けを実装します。Windows 用の NTP クライアントについては、`http://www.ntp.org/` を参照してください。

Windows のサービスパックとホットフィックス (Hotfix) のインストール

Windows 2000 のサービスパックには、オペレーティングシステムのセキュリティと信頼性を維持するのに重要な修正が含まれています。ホットフィックス (Hotfix) シリーズには、サービスパックがリリースされた後に確認された問題に対する重要な変更が含まれています。iPlanet Directory Server は Service Pack 2 に対応しています。

インストール後に行うその他のシステム構成

Windows 2000 環境では、動作環境内での iPlanet Directory Server の性能を最適化するためのチューニングが必要です。マルチスレッドのインターネットサービスのための Windows 2000 のチューニング方法については、Windows 2000 のシステム管理者用マニュアルを参照してください。

HP-UX 11 オペレーティングシステム

ディスク容量の要件

ソフトウェアをダウンロードする前に、充分なディスク容量があることを確認してください。

- ダウンロード先となるドライブ : 120M バイト
- インストールドライブ : 2G バイト

システムモジュールの要件

iPlanet Directory Server 5.1 は、HP-UX 10 以前のバージョンではサポートされていません。システムモジュールには、少なくとも HP-UX 11 が必要です。iPlanet Directory Server は 64 ビットの HP-UX 11 環境でも使用できますが、32 ビットプロセスとして動作し、プロセスメモリーも 1G バイトに制限されます。

iPlanet Directory Server 5.1 を最適な条件で使用するには、PA-RISC 1.1 または PA-RISC 2.0 CPU を備えた HP 9000 アーキテクチャのマシンが必要です。

注	iPlanet Directory Server の今後のバージョンは、PA-RISC 1.1 CPU を使用した HP システム上でサポートされなくなる可能性があります。サポートの対象外となる可能性があるのは、9000/7xx シリーズ、C100、C110、C160L、J200、J210、J210XC、B132L、B132L+、B160L、および B180L システムです。

パッチ

Directory Server をインストールする前に、パッチをインストールしてください。HP-UX 11.0 上で iPlanet Directory Server を実行するには、次のパッチが必要です。

- PHCO_19491
- PHKL_14750
- PHCO_19666
- PHKL_20016
- PHKL_18543
- PHCO_17556
- PHKL_17038、PHCO_17792、PHKL_20079、および PHKL_20674 は、PHKL_18543 パッチとの依存関係がある
- AWT を使用するアプリケーションには、PHSS_20141、PHSS_17535、PHSS_20140、および PHSS_19964 を使用すること

  PHNE_20094 および PHSS_20145 は、PHSS_20140 パッチとの依存関係がある
- システム上に HP C++ 実行時ライブラリがインストールされていることを確認すること。最新バージョンはパッチ PHSS_16587 として入手できる

また、次の Web サイトで、最新のパッチ要件に関する情報を確認してください。

```
http://www.hp.com/products1/unix/java/infolibrary/patches.html
```

システムチューニングの確認

カーネルパラメタを次のように設定します。

- カーネルパラメタ `maxdsize` が少なくとも次の値であることを確認する

  cachesize × entrysize ＋ 4096

  つまり、Directory Server の cachesize が 1000 (デフォルト) で、平均ディレクトリエントリサイズが 20K バイトの場合は、カーネルパラメタ `maxdsize` が少なくとも (1000 × 20000) ＋ 4096、または少なくとも 21M バイトであることを確認します。
- `max_thread_proc` (1 プロセスあたりの最大スレッド数) を 128 に設定する
- `ncallout` (タイムアウト待ちの最大数) を `128+NPROC` に設定する
- `maxfiles` を少なくとも 120 に設定する

HP-UX マシン上では、iPlanet Directory Server を正しく動作させるためには、管理者はラージファイルのサポートを有効化する必要があります。

ラージファイルのない既存のファイルシステムでラージファイルを受け入れられるようにするには、次の操作を実行します。

1. 次のように umount コマンドを使用して、システムのマウントを解除します。たとえば、次のようにします。

   ```
   umount  /export
   ```

2. ラージファイルシステムを作成します。たとえば、次のようにします。

   ```
   fsadm -F vxfs -o largefiles /dev/vg01/rexport
   ```

3. ファイルシステムをマウントし直します。たとえば、次のようにします。

   ```
   /usr/sbin/mount -F vxfs -o largefiles /dev/vg01/export
   ```

これらのパラメタ設定の詳細および推奨事項については、使用しているシステムの HP マニュアルを参照してください。

サードパーティユーティリティのインストール

Directory Server ソフトウェアを解凍するには、gunzip ユーティリティが必要です。GNU gzip および gunzip プログラムについては、http://www.gnu.org/software/gzip/gzip.html を参照してください。これらのプログラムは、さまざまなサイトからダウンロードできます。

マニュアルを読むには、Adobe Acrobat Reader をインストールする必要があります。Acrobat Reader がインストールされていない場合は、次のサイトからダウンロードできます。
http://www.adobe.com/products/acrobat/readstep2.html

IBM AIX 4.3.3 オペレーティングシステム

ディスク容量の要件

ソフトウェアをダウンロードする前に、充分なディスク容量があることを確認してください。

- ダウンロード先となるディレクトリ : 120M バイト
- /usr を含むパーティション : 2G バイト

システムモジュールの要件

AIX 4.3.3 以降のバージョンが必要です。iPlanet Directory Server 5.1 は、AIX 4.3.2 以前のリリースではサポートされていません。また、AIX 5.0L でもサポートされていません。

パッチ

ご使用のシステムに必要なパッチまたは APAR については、次のサイトを参照してください。

http://server.software.ibm.com/cgi-bin/support/rs6000.support/downloads

サードパーティユーティリティのインストール

Directory Server ソフトウェアを解凍するには、gunzip ユーティリティが必要です。GNU gzip および gunzip プログラムについては、http://www.gnu.org/software/gzip/gzip.html を参照してください。これらのプログラムは、さまざまなサイトからダウンロードできます。

マニュアルを読むには、Adobe Acrobat Reader をインストールする必要があります。Acrobat Reader がインストールされていない場合は、次のサイトからダウンロードできます。

http://www.adobe.com/products/acrobat/readstep2.html

DNS および NIS の要件 (UNIX のみ)

インストールの前に、DNS リソルバと NIS ドメイン名を構成しておく必要があります。

DNS リソルバは、通常、/etc/resolv.conf ファイルによって設定されます。ただし、同時に /etc/nsswitch.conf ファイルと、Solaris の場合は /etc/netconfig ファイルも確認し、DNS リソルバを名前検索で使用できるようにしてください。

NIS をまだ使用していない場合は、デフォルトの NIS ドメイン名も設定する必要があります。通常、この設定は /etc/defaultdomain ファイル内に NIS ドメイン名を設定してコンピュータを再起動するか、domainname コマンドを使用して行います。

第 3 章

高速インストールと標準インストールの使用

この章では、基本的なインストール手順について説明します。この章は、次の節で構成されています。

- 高速インストールの使用
- 標準インストールの使用

注 iPlanet Directory Server 5.1 は、Solaris 9 オペレーティング環境にプリインストールされています。Solaris 9 プラットフォームで Directory Server を構成する方法の詳細は、Solaris の『Solaris のシステム管理 (ネーミングとディレクトリサービス : DNS、NIS、LDAP 編)』を参照してください。Solaris のマニュアルは、`http://docs.sun.com/` で参照できます。

高速インストールの使用

製品の評価またはテストのために Directory Server をインストールする場合は、高速インストールを使用します。高速インストールではサーバのポート番号やディレクトリ接尾辞は選択できないので、正規のインストールにはこの方法は使用しないでください。

高速インストールを行うには、次の手順を実行します。

1. UNIX の場合は、root としてログインします (高速インストールを行うには、root としてログインする必要がある)。Windows NT および Windows 2000 の場合は、administrator 権限を持つユーザとしてログインします。

2. 新しいディレクトリを作成します。

   ```
   # mkdir ds5.1
   # cd ds5.1
   ```

   製品のバイナリファイルをまだダウンロードしていない場合は、インストールディレクトリにダウンロードします。

3. UNIX の場合は、次のコマンドを実行して製品のバイナリファイルを解凍します。

   ```
   # gunzip -dc file_name.tar.gz | tar -xvof -
   ```

   ここでの *file_name* は、解凍する製品のバイナリファイル名を表します。

   Windows NT および Windows 2000 の場合は、製品のバイナリファイルを解凍 (unzip) します。

4. セットアッププログラムを実行します。セットアッププログラムは、バイナリファイルを解凍したディレクトリにあります。UNIX システムの場合は、次のコマンドを実行します。

   ```
   ./setup
   ```

   「yes」を選択してインストールを続行し、次に使用許諾契約に同意する場合は、「yes」を選択します。

5. インストールするプログラムを確認する画面が表示されたら、デフォルトの「iPlanet Servers」を選択します。

6. インストールのタイプを確認する画面が表示されたら、「高速インストール」を選択します。

7. サーバルートまたはインストール先ディレクトリの設定画面で、サーバをインストールするディレクトリを絶対パスで入力します。

   セットアッププログラムを実行しているディレクトリをインストール先に指定することはできません。指定したディレクトリが存在しない場合は、そのディレクトリが自動的に作成されます。

8. UNIX のみ。サーバを実行するユーザおよびグループの設定画面で、このサーバの実行に使用する識別情報を入力します。サーバの実行時に使用する必要のあるユーザおよびグループについては、14 ページの「iPlanet サーバ用のユーザとグループの決定 (UNIX® のみ)」を参照してください。

9. 構成ディレクトリ管理者の ID とパスワードの設定画面で、すべての特権を持つユーザ (iPlanet Console におけるルートまたはスーパーユーザと同じようなものと考えてください) として Console に認証させるときに使用するユーザ名とパスワードを指定します。

サーバの開梱、最小限の構成、および起動が行われます。Administration Server が待機するホストとポート番号が表示されます。

新たにインストールされた Directory Server については、次のことに留意してください。

- Directory Server は、ポート 389 上で待機します。
- サーバは、次の接尾辞を使用するように構成されます。

  dc= あなたのマシンのドメイン名。つまり、マシン名が test.siroe.com の場合、このサーバの接尾辞は dc=siroe,dc=com と設定されます。

  o=NetscapeRoot

o=NetscapeRoot 接尾辞の下にあるディレクトリの内容は変更しないでください。このためには、最初の接尾辞の下に新しいデータを作成するか、使用する新しい接尾辞を作成するかのいずれかを行います。Directory Server で新しい接尾辞を作成する方法については、『iPlanet Directory Server 管理者ガイド』を参照してください。

標準インストールの使用

Directory Server 5.1 をはじめてインストールする場合は、セットアッププログラムの標準インストールオプションを使用するのが一般的です。標準インストールの操作は、UNIX の場合と Windows NT/Windows 2000 の場合で多少異なります。以降の節では、それぞれの手順について説明します。

UNIX 上での標準インストールの使用

UNIX 上で標準インストールを実行するには、次の手順に従います。

1. root としてログインします。
2. 新しいディレクトリを作成します。

   ```
   # mkdir ds5.1
   # cd ds5.1
   ```

3. 製品のバイナリファイルをまだダウンロードしていない場合は、インストールディレクトリにダウンロードします。
4. 次のコマンドを実行して製品のバイナリファイルを解凍します。

   ```
   # gunzip -dc file_name.tar.gz | tar -xvof -
   ```

   ここでの *file_name* は、解凍する製品のバイナリファイル名を表します。

5. セットアッププログラムを実行します。セットアッププログラムは、バイナリファイルを解凍したディレクトリにあります。インストールディレクトリから次のコマンドを実行します。

   ```
   ./setup
   ```

6. セットアッププログラムにより、セットアップの続行を確認するメッセージが表示されます。デフォルトを選択する場合は、Enter キーを押し (このプロンプトのデフォルトは「yes」)、セットアッププログラムを終了する場合は n を押します。

   root またはスーパーユーザ (su) としてログインしたい場合は、セットアッププログラムを終了する必要があります。

7. 次に、使用許諾契約への同意を確認する画面が表示されます。同意する場合は y を押します。

8. インストールするプログラムを確認する画面が表示されます。Enter キーを押して、デフォルトの「iPlanet Servers」を選択します (項目 1)。

9. インストールのタイプを確認する画面が表示されます。Enter キーを押して、デフォルトの「標準インストール」を選択します。

10. サーバルートの選択画面で、サーバをインストールするディレクトリを絶対パスで入力します。

    セットアップを実行しているディレクトリをインストール先に指定することはできません。指定したディレクトリが存在しない場合は、そのディレクトリが自動的に作成されます。

    デフォルトでは、自動的に次のパスが使用されます。

    ```
    /usr/iplanet/servers
    ```

    このディレクトリツリーにソフトウェアをインストールする場合は、Enter キーを押します。ほかのディレクトリを指定する場合は、そのパスを入力します。

11. Server Products Core Components、Directory Suite、Administration Services、nsPerl、および PerLDAP のインストール画面で、Enter キーを押してデフォルト (すべてのコンポーネント) を選択します。

12. Enter キーを押して、Server Products Core Components すべてを選択します。

13. Enter キーを押して、Directory Suite のすべてのコンポーネントを選択します。

14. Enter キーを押して、Administration Services のすべてのコンポーネント (iPlanet Administration Server と Administration Server Console) を選択します。

15. ホスト名の設定画面で、完全指定を指定するか、デフォルト (local host) を選択します。

警告 インストールプログラムがシステム内の DNS 名を特定できない場合は、デフォルトのホスト名が誤ったものになることがあります。たとえば、システムで NIS が使用されている場合、DNS が使用されていない可能性があります。

ホスト名には、絶対パスによるホスト名とドメイン名を指定しなければなりません。デフォルトのホスト名が絶対パスによるホスト名とドメイン名ではない場合は、インストールが失敗します。完全指定によるドメイン名の入力については、87 ページの「一般的なインストール上の問題」を参照してください。

16. ここで、システムユーザ名とシステムグループ名の入力を求める画面が表示されます。サーバの実行に使用するシステムユーザとシステムグループの識別名を入力します。

    iPlanet サーバの実行時に使用するユーザ名およびグループ名については、14 ページの「iPlanet サーバ用のユーザとグループの決定 (UNIX® のみ)」を参照してください。

17. 構成ディレクトリについて、このディレクトリが `o=NetscapeRoot` ツリーをホストする場合は、デフォルトを選択します。ホストしない場合は、`Yes` と入力します。ここで、構成ディレクトリへのアクセス情報を求める画面が表示されます。

    現在インストールしているサーバが構成ディレクトリではない場合、このインストールを続行するには、構成ディレクトリが存在する必要があります。

18. 次に、現在インストールしているサーバがユーザデータの格納用かどうかを確認する画面が表示されます。通常はデフォルトを選択します。ただし、このサーバインスタンスを構成ディレクトリとしてのみ使用する場合は、`Yes` と入力する必要があります。

19. Directory Server のポートの設定画面で、デフォルト (389) を選択します。ただし、ほかのアプリケーションがすでにこのポートを使用している場合を除きます。

20. サーバ識別子の設定画面で、ほかと重複しないものを指定します (通常はデフォルトを使用)。

    この名前は、Directory Server インスタンスがインストールされるディレクトリ名の一部として使用されます。たとえば、マシンのホスト名が `phonebook` の場合はこの値がデフォルトとなり、この名前を選択すると `slapd-phonebook` というラベルが付いたディレクトリに Directory Server インスタンスがインストールされます。

警告 Directory Server 識別子には、ピリオドは使用できません。たとえば、`siroe.server.com` をサーバ識別名にすることはできません。

21. 構成ディレクトリ管理者の ID とパスワードの設定画面で、すべての特権を持つユーザとして Console に認証させるときに使用するユーザ名とパスワードを指定します。
22. ディレクトリ接尾辞の設定画面で、企業名が判断できるようなわかりやすい識別名を指定します。

    ここで指定した文字列は、組織内のすべてのディレクトリエントリの名前に使用されます。そのため、組織を識別できるような名前を使用するようにします。インターネット DNS 名に対応した接尾辞の使用をお勧めします。

    たとえば、組織の DNS 名が `siroe.com` の場合は、`dc=siroe,dc=com` と入力します。
23. ディレクトリマネージャの DN の設定画面で、無制限の特権を使用してディレクトリの内容を管理するときに使用する識別名を入力します。

注	識別名では、UTF-8 文字セットエンコードを使用する必要があります。ISO-8859-1 などの古いエンコードはサポートされません。

    以前のリリースの Directory Server では、ディレクトリマネージャは root DN と呼ばれていました。これは、アクセス制御を無視するときにディレクトリにバインドするエントリです。この識別名は短いものでよく、ディレクトリに構成された接尾辞に合わせる必要はありません。ただし、ディレクトリ内に保存された実際のエントリとは異なるものでなければなりません。
24. ディレクトリマネージャ用のパスワードの設定画面で、8 文字以上の値を指定します。
25. 管理ドメインの設定画面で、このサーバを所属させるドメインを指定します。

    入力するドメイン名は、一意の文字列で、ドメインを管理する組織が識別できるものにします。管理ドメインについては、18 ページの「管理ドメインの決定」を参照してください。
26. 管理ポート番号の設定画面で、ほかと重複しない番号を入力します (たとえば、5100 で Directory Server 5.1 を示すことができます)。この値は必ず記録してください。
27. Administration Server の実行に使用するユーザの設定画面で、`root` と入力します。この値がデフォルトです。

    Administration Server を root として実行する必要がある理由については、14 ページの「iPlanet サーバ用のユーザとグループの決定 (UNIX® のみ)」を参照してください。

サーバの開梱、最小限の構成、および起動が行われます。Administration Server が待機するホストとポート番号が表示されます。

サーバは、次の接尾辞を使用するように構成されます。

- 構成した接尾辞
- o=NetscapeRoot

o=NetscapeRoot 接尾辞の下にあるディレクトリの内容は変更しないでください。このためには、最初の接尾辞の下に新しいデータを作成するか、使用する新しい接尾辞を作成するかのいずれかを行います。Directory Server で新しい接尾辞を作成する方法については、『iPlanet Directory Server 管理者ガイド』を参照してください。

Windows NT および Windows 2000 での標準インストールの使用

Windows NT または Windows 2000 上で標準インストールを実行するには、次の手順に従います。

1. administrator の権限を持つユーザとしてログインします。
2. 製品のバイナリファイルをまだダウンロードしていない場合は、インストールディレクトリにダウンロードします。
3. 製品のバイナリファイルを解凍 (unzip) して、セットアッププログラムを実行します。
4. インストールするプログラムを確認する画面が表示されたら、デフォルトの「iPlanet Servers」を選択します。
5. インストールのタイプを確認する画面が表示されたら、デフォルトの「標準」を選択します。
6. サーバルートの選択画面で、サーバをインストールするディレクトリを絶対パスで入力します。

   セットアップを実行しているディレクトリをインストール先に指定することはできません。指定したディレクトリが存在しない場合は、そのディレクトリが自動的に作成されます。
7. 構成ディレクトリで、このディレクトリが o=NetscapeRoot ツリーをホストする場合は、デフォルトを選択します。ホストしない場合は、構成ディレクトリの適切な接続情報を入力します。

   この Directory Server インスタンスが構成ディレクトリではない場合、このインストールを続行するには、構成ディレクトリが存在し、実行されている必要があります。

8. データを格納するディレクトリの設定画面で、この Directory Server インスタンスに企業のデータを格納するかどうかを決定する必要があります。通常は、デフォルトの「この Directory Server にデータを保存する」を選択します。ただし、この Directory Server インスタンスを構成ディレクトリとしてのみ使用する場合、「既存の Directory Server にデータを保存する」を選択する必要があります。

9. サーバ識別子の設定画面で、ほかと重複しないものを指定します (通常はデフォルトを使用)。

   この名前は、Directory Server インスタンスがインストールされるディレクトリ名の一部として使用されます。たとえば、マシンのホスト名が `phonebook` の場合はこの値がデフォルトとなり、この名前を選択すると `slapd-phonebook` というラベルが付いたディレクトリに Directory Server インスタンスがインストールされます。

10. ディレクトリ接尾辞の設定画面で、企業名が判断できるようなわかりやすい識別名を指定します。

    ここで指定した文字列は、組織内のすべてのディレクトリエントリの名前に使用されます。そのため、組織を識別できるような名前を使用するようにします。インターネット DNS 名に対応した接尾辞の使用をお勧めします。たとえば、組織の DNS 名が `siroe.com` の場合は、`dc=siroe,dc=com` と入力します。

11. Directory Server のポートの設定画面で、デフォルト (389) を選択します。ただし、ほかのアプリケーションがすでにこのポートを使用している場合を除きます。

12. 構成ディレクトリ管理者の ID とパスワードの設定画面で、すべての特権を持つユーザとして Console にログインするときに認証させるユーザ名とパスワードを指定します。

13. 管理ドメインの設定画面で、このサーバを所属させるドメインを指定します。

    入力するドメイン名は、一意の文字列で、そのドメインを管理する組織が識別できるものにします。管理ドメインについては、18 ページの「管理ドメインの決定」を参照してください。

14. ディレクトリマネージャの DN の設定画面で、無制限の特権を使用してディレクトリの内容を管理するときに使用する識別名を入力します。

注　識別名では、UTF-8 文字セットエンコードを使用する必要があります。ISO-8859-1 などの古いエンコードはサポートされません。

以前のリリースの Directory Server では、ディレクトリマネージャは root DN と呼ばれていました。これは、アクセス制御を無視するときにディレクトリにバインドするエントリです。この識別名は短いものでよく、ディレクトリに構成された接尾辞に合わせる必要はありません。ただし、ディレクトリ内に保存された実際のエントリとは異なるものでなければなりません。

15. ディレクトリマネージャ用のパスワードの設定画面で、8 文字以上の値を指定します。
16. 管理ポート番号の設定画面で、ほかと重複しない番号を入力します。この値は必ず記録してください。

サーバの開梱、最小限の構成、および起動が行われます。Administration Server が待機するホストとポート番号が表示されます。

サーバは、次の接尾辞を使用するように構成されます。

- 構成した接尾辞
- `o=NetscapeRoot`

`o=NetscapeRoot` 接尾辞の下にあるディレクトリの内容は変更しないでください。このためには、最初の接尾辞の下に新しいデータを作成するか、使用する新しい接尾辞を作成するかのいずれかを行います。Directory Server で新しい接尾辞を作成する方法については、『iPlanet Directory Server 管理者ガイド』を参照してください。

第 4 章

サイレントインストール

サイレントインストールでは、通常はセットアッププログラムに対して対話的な操作で入力するすべての項目を、1 つのファイルに事前に定義しておくことができます。これによって、Directory Server のインストールをスクリプト化することができます。

この章は、次の節で構成されます。

- サイレントインストールの使用
- サイレントインストールファイルの準備
- インストール指令

サイレントインストールの使用

サイレントインストールを使用するには、`-s` および `-f` コマンド行オプションを使用してセットアッププログラムを実行します。つまり、サイレントインストールを使用するには、次の操作を実行します。

1. UNIX マシンの場合は、`root` としてログインします。Windows NT および Windows 2000 コンピュータでは、administrator の権限を持つユーザとしてログインします。
2. 新しいディレクトリを作成します。

   ```
   # mkdir ds5.1
   # cd ds5.1
   ```

3. 製品のバイナリファイルをまだダウンロードしていない場合は、インストールディレクトリにダウンロードします。
4. UNIX の場合は、次のコマンドを実行して製品のバイナリファイルを解凍します。

   ```
   # gunzip -dc file_name.tar.gz | tar -xvof-
   ```

   ここでの *file_name* は、解凍する製品のバイナリファイル名を表します。

5. Windows NT および Windows 2000 の場合は、製品のバイナリファイルを解凍 (unzip) します。
6. インストール指令を書き込むファイルを用意します。
7. `-s` および `-f` コマンド行オプションを使用してセットアッププログラムを実行します。

   `setup -s -f` *file_name*

   ここでの *file_name* は、インストール指令を書き込んだファイル名を表します。

次の節では、サイレントインストールファイルの例をいくつか示します。その次の節では、Directory Server のインストールに使用できるサイレントインストール用のすべての指令についても記述します。

サイレントインストールファイルの準備

サイレントインストールは、多くのサーバインスタンスの作成が必要なサイトで使用することを目的としています。Directory Server では、多数のコンシューマサーバが存在する、複製頻度の高いサイトでは特に便利です。

この節では、はじめにサイレントインストールファイルの作成方法を説明します。また、次に示すような一般的なインストール環境でのサイレントインストールを使用する例を示します。

- 標準インストール
- 既存の構成ディレクトリの使用
- スタンドアロンの iPlanet Console の インストール

個々のインストール指令の定義については、63 ページの「インストール指令」を参照してください。

注	ファイルの中で使用する識別名には、すべて UTF-8 文字セットエンコードを使用します。

サイレントインストールファイルの作成

サイレントインストールに使用するファイルの最適な作成方法は、セットアッププログラムを使用し、企業で複製したいタイプのサーバインスタンスを対話的に作成することです。

これを実行するには、`-k` フラグを使用してセットアッププログラムを実行します。セットアッププログラムによって次のファイルが作成されます。

/<ServerRoot>/setup/install.inf

このファイルには、サーバインスタンスを作成するためにサイレントインストールで使用されるすべての指令が書き込まれます。その後、このファイルを使用して、同じタイプの別のサーバインスタンスを作成できます。

ほかのコンピュータ上で使用する場合は、ファイルに多少の修正を加える必要があります。次の点を確認してください。

- iPlanet Directory Server をインストールするマシンがローカルマシンでない場合は、インストールするマシンに合わせて FullMachineName 指令を適切な値に設定します。FullMachineName はデフォルトでローカルホスト名が割り当てられるので、通常はこの指令は使用しないでください。ただし、カスタムインストールを使用して最初のサーバインスタンスを作成する場合は、install.inf ファイル内にこの指令が記述されます。
- ローカルマシンに応じた適切な ServerIPAddress 指令を設定します。ServerIPAddress の使用規則は FullMachineName の場合と同じです。ただし、絶対に必要な場合 (マルチホームシステムの場合などは必要となる可能性がある) を除き、install.inf ファイル内には ServerIPAddress を含めないでください。
- ServerRoot 指令のインストールパスを確認します。Windows NT または Windows 2000 マシンと、UNIX マシンの両方にインストールする場合は、それぞれ適切なパスの区切り文字が使用されていることを確認します。また、インストール先のホストに合わせて Windows NT または Windows 2000 のドライブ文字指定を追加または削除します。
- 同じホスト上に複数の Directory Server をインストールする場合は、ServerIdentifier 指令に、各サーバインスタンスの一意の値が含まれていることを確認します。
- Windows NT または Windows 2000 のマシン上に install.inf ファイルを作成する場合は、SuiteSpotUserID 指令と SuiteSpotGroup 指令を両方とも nobody に設定します。このファイルをこの後続けて UNIX マシン上で使用する場合は、これらの指令によって指定されるユーザおよびグループが、そのマシンに適したものとなるようにします。SuiteSpotUserID 指令と SuiteSpotGroup 指令は、UNIX システム上にインストールした場合は、どのユーザおよびグループの下でサーバを実行するかを決定します。

install.inf ファイルにはパスワードが暗号化されずに記述されるので、このファイルは必ずプロテクトしてください。

サイレントインストールファイルで使用可能な指令については、63 ページの「インストール指令」を参照してください。

標準インストール

次に、標準インストール用に作成した install.inf ファイルの例を示します。

```
[General]
FullMachineName=   dir.siroe.com
SuiteSpotUserID=   nobody
SuiteSpotGroup=   nobody
ServerRoot=   /usr/iplanet/servers
AdminDomain=   siroe.com
ConfigDirectoryAdminID=   admin
ConfigDirectoryAdminPwd=   admin
ConfigDirectoryLdapURL= ldap://dir.siroe.com:389/o=NetscapeRoot
UserDirectoryAdminID=   admin
UserDirectoryAdminPwd=   admin
UserDirectoryLdapURL= ldap://dir.siroe.com:389/o=siroe.com
Components=   svrcore,base,slapd,admin

[slapd]
SlapdConfigForMC=   Yes
SecurityOn=   No
UseExistingMC=   No
UseExistingUG=   No
ServerPort=   389
ServerIdentifier=   dir
Suffix=   o=mcom.com
RootDN=   cn=Directory Manager
UseReplication=   No
SetupSupplier=   No
SetupConsumer=   No
AddSampleEntries=   No
InstallLdifFile=   suggest
AddOrgEntries=   Yes
DisableSchemaChecking=   No
RootDNPwd=   admin123
Components=   slapd,slapd-client

[admin]
SysUser=   root
Port=   23611
ServerIpAddress=   111.11.11.11
ServerAdminID=   admin
ServerAdminPwd=   admin
Components=   admin,admin-client,base-jre

[base]
Components=   base,base-client
```

既存の構成ディレクトリの使用

次に、標準インストールで、既存の Directory Server を構成ディレクトリとして使用するときに作成される `install.inf` ファイルの例を示します。

```
[General]
FullMachineName=   dir.siroe.com
SuiteSpotUserID=   nobody
SuiteSpotGroup=   nobody
ServerRoot=   /usr/netscape/server4
AdminDomain=   siroe.com
ConfigDirectoryAdminID=   admin
ConfigDirectoryAdminPwd=   admin
ConfigDirectoryLdapURL= ldap://dir.siroe.com:25389/o=NetscapeRoot
UserDirectoryLdapURL= ldap://dir.siroe.com:18257/dc=siroe,dc=com
UserDirectoryAdminID=   cn=Directory Manager
UserDirectoryAdminPwd=   admin123
Components=   svrcore,base,slapd,admin

[slapd]
SlapdConfigForMC=   No
SecurityOn=   No
UseExistingMC=   y
UseExistingUG=   No
ServerPort=   18257
ServerIdentifier=   directory
Suffix=   o=siroe.com
RootDN=   cn=Directory Manager
UseReplication=   No
SetupSupplier=   No
SetupConsumer=   No
AddSampleEntries=   No
InstallLdifFile=   suggest
AddOrgEntries=   Yes
DisableSchemaChecking=   No
RootDNPwd=   admin123
Components=   slapd,slapd-client

[admin]
SysUser=   root
Port=   33646
ServerIpAddress=   111.11.11.11
ServerAdminID=   admin
ServerAdminPwd=   admin
```

```
Components=   admin,admin-client,base-jre

[base]
Components=   base,base-client, base-jre

[nsperl]
Components=   nsperl553

[perldap]
Components=   perldap14
```

スタンドアロンの iPlanet Console のインストール

次に、iPlanet Console だけをインストールするときに作成される `install.inf` ファイルの例を示します。

```
[General]
FullMachineName=   dir.siroe.com
ConfigDirectoryLdapURL= ldap://dir.siroe.com:389/o=NetscapeRoot
SuiteSpotUserID=   nobody
SuiteSpotGroup=   nobody
ConfigDirectoryAdminID=   admin
ConfigDirectoryAdminPwd=   admin
ServerRoot=   /usr/netscape/server4
Components=   svrcore,base,slapd,admin

[base]
Components=   base-client

[slapd]
Components=   slapd-client

[admin]
Components= admin-client,base-jre
```

インストール指令

この節では、サイレントインストールで使用されるファイルの基本的な形式について説明します。その後、サイレントインストールファイルの各領域で使用可能な指令についても説明します。ここでは、次の項目について紹介します。

- サイレントインストールファイルの形式
- [General] インストール指令
- [Base] インストール指令
- [slapd] インストール指令
- [admin] インストール指令

サイレントインストールファイルの形式

サイレントインストールを使用する場合は、すべてのインストール情報を 1 つのファイルに記述します。このファイルは、次の形式で構成されます。

```
[General]
指令 = 値
指令 = 値
指令 = 値
...
[Base]

指令 = 値
指令 = 値
指令 = 値
...
[slapd]
指令 = 値
指令 = 値
指令 = 値
...
[admin]
指令 = 値
指令 = 値
指令 = 値
....
```

キーワードの [General]、[slapd]、および [admin] は必須の項目です。これらのキーワードは、その後に続く指令がインストールの特定の側面に対するものであることを示します。ファイル内のキーワードの順番は、上述のとおりにする必要があります。

[General] インストール指令

[General] インストール指令には、サイト上にインストールされる iPlanet サーバの全体的な情報を指定します。つまり、ここで指定した情報は、すべての iPlanet サーバに共通に適用されます。

[General] インストール指令には次のようなものがあります。

表 4-1　[General] インストール指令

指令	内容
Components	インストールするコンポーネントを指定します。インストール可能なコンポーネントのリストは、インストールメディアに収められている iPlanet サーバによって異なります。スタンドアロンディレクトリのインストールの場合、コンポーネントのリストは次のとおりです。 • `srvrcore` : アンインストール用バイナリ • `base` : ベースインストールパッケージ • `admin` : Administration Server 用バイナリ • `slapd` : Directory Server 用バイナリ この指令は必須です。少なくとも次の指定が必要です。 `components = srvrcore, base, admin`
ServerRoot	iPlanet サーババイナリをインストールするディレクトリへの絶対パスを指定します。この指令は必須です。
FullMachineName	サーバをインストールするマシンのドメイン名を絶対パスで指定します。デフォルトはローカルホスト名です。
SuiteSpotUserID	UNIX のみ。iPlanet サーバを実行するユーザ名を指定します。このパラメタは、Administration Server を実行するユーザには適用されません。詳細は、表 4-5 の SysUser 指令を参照してください。デフォルトはユーザ `nobody` ですが、通常は変更する必要があります。
SuiteSpotGroup	UNIX のみ。iPlanet サーバを実行するグループを指定します。デフォルトはグループ `nobody` ですが、通常は変更する必要があります。
ConfigDirectoryLdapURL	構成ディレクトリへの接続に使用する LDAP URL を指定します。LDAP URL については、『iPlanet Directory Server 管理者ガイド』を参照してください。この指令は必須です。

表 4-1　[General] インストール指令 (続き)

指令	内容
AdminDomain	このサーバが登録される管理ドメインを指定します。管理ドメインについては、18 ページの「管理ドメインの決定」を参照してください。
ConfigDirectoryAdminID	構成ディレクトリに対して管理者権限を持つエントリのユーザ ID を指定します。この指令は必須です。
ConfigDirectoryAdminPwd	ConfigDirectoryAdminID のパスワードを指定します。この指令は必須です。
UserDirectoryLdapURL	ユーザおよびグループのデータを格納するディレクトリへの接続に使用される LDAP URL を指定します。この指令に指定がない場合は、代わりに構成ディレクトリが使用されます。LDAP URL については、『iPlanet Directory Server 管理者ガイド』を参照してください。
UserDirectoryAdminID	ユーザディレクトリに対して管理者権限を持つエントリのユーザ ID を指定します。
UserDirectoryAdminPwd	UserDirectoryAdminID のパスワードを指定します。

[Base] インストール指令

[Base] インストール指令は 1 つしかなく、この指令で iPlanet Console をインストールするかどうかを決定します。

表 4-2　[Base] インストール指令

指令	内容
Components	インストールするベースコンポーネントを指定します。ベースコンポーネントは次のとおりです。 • `base` : すべての Server Console で使用する共有ライブラリをインストールする。ほかの iPlanet サーバもインストールする場合は、必ずこのパッケージをインストールする必要がある • `base-client` : Server Console が使用する Java ランタイム環境をインストールする • `base-jre` : Java ランタイム環境がインストールされる iPlanet サーバをインストールする場合は、この指令が必要です (iPlanet Console のみインストールする場合は不要)。iPlanet サーバをインストールする場合は、両方のパッケージをインストールする必要があります。

[slapd] インストール指令

[slapd] インストール指令は、現在インストールしている Directory Server インスタンスにのみ関係する情報を指定します。これらの指令については、次の節で説明します。

- 必須の [slapd] インストール指令
- 省略可能な [slapd] インストール指令

必須の [slapd] インストール指令

Directory Server のサイレントインストールを実行するときは、次の指令を指定する必要があります。

表 4-3　必須の [slapd] インストール指令

指令	内容
Components	インストールする slapd コンポーネントを指定します。slapd コンポーネントは次のとおりです。 • `slapd` : Directory Server をインストールする • `slapd-client` : Directory Server Console をインストールする この指令は必須です。Directory Server をインストールする場合は、常に両方のコンポーネントをインストールすることをお勧めします。
ServerPort	サーバが LDAP 接続に使用するポートを指定します。サーバポート番号の選択については、13 ページの「一意のポート番号の選択」を参照してください。この指令は必須です。
ServerIdentifier	サーバ識別子を指定します。この指令は必須です。 この名前は、Directory Server インスタンスのインストール先ディレクトリ名の一部として使用されます。たとえば、マシンのホスト名が `phonebook` の場合はこの値がデフォルトとなり、この名前を選択すると `slapd-phonebook` というラベルが付いたディレクトリに Directory Server インスタンスがインストールされます。
Suffix	ディレクトリデータを格納する接尾辞を指定します。接尾辞については、16 ページの「ディレクトリ接尾辞の決定」を参照してください。この指令は必須です。
RootDN	ディレクトリマネージャが使用する識別名を指定します。ディレクトリマネージャについては、15 ページの「認証エンティティの定義」を参照してください。この指令は必須です。
RootDNPwd	ディレクトリマネージャのパスワードを指定します。この指令は必須です。

省略可能な [slapd] インストール指令

Directory Server のサイレントインストールを実行するときは、次の指令を使用することができます。

表 4-4　省略可能な [slapd] インストール指令

指令	内容
AddSampleEntries	この指令を Yes に設定すると、siroe.ldif サンプルディレクトリが読み込まれます。評価の目的で Directory Server をインストールする場合、ディレクトリに実装するための LDIF ファイルがまだ存在しないときは、この指令を使用します。デフォルトは no です。
AddOrgEntries	この指令を Yes に設定すると、推奨されるディレクトリ構造とアクセス制御を使用した新しい Directory Server インスタンスが作成されます。この指令と InstallLdifFile を同時に使用した場合は、この指令は無効になります。デフォルトは no です。
InstallLdifFile	LDIF ファイルの内容を使用してディレクトリに実装されます。

[admin] インストール指令

[admin] インストール指令は、ユーザの Directory Server の Administration Server にのみ関係する情報を指定します。つまり、この情報は、現在インストールしている Directory Server インスタンスの管理に使用される Administration Server にとって必要なインストール情報です。

[admin] インストール指令には次のようなものがあります。

表 4-5　[admin] インストール指令

指令	内容
Components	インストールする admin コンポーネントを指定します。ベースコンポーネントは次のとおりです。 • admin : Administration Server をインストールする。ほかの iPlanet サーバもインストールする場合は、必ず Administration Server をインストールする必要がある • admin-client : iPlanet Console をインストールする。iPlanet Console をスタンドアロンとしてインストールする場合は、このコンポーネントのみを指定する。サーバの管理をリモートで行っている場合、このコンポーネントはインストールしてはならない。iPlanet Console はユーザのネットワーク上の別の場所にインストールされる

表 4-5　[admin] インストール指令 (続き)

指令	内容
SysUser	UNIX のみ。Administration Server を実行するユーザを指定します。デフォルトの iPlanet ポート番号を使用するデフォルトインストールの場合は、このユーザは root でなければなりません。デフォルトは root です。サーバを実行するユーザについては、14 ページの「iPlanet サーバ用のユーザとグループの決定 (UNIX® のみ)」を参照してください。
Port	Administration Server が使用するポートを指定します。Administration Server のホスト名は、`FullMachineName` 指令で指定されることに注意してください。`FullMachineName` については、表 4-1 を参照してください。
ServerAdminID	構成ディレクトリが応答しない場合に、この Administration Server へのアクセスに使用できる管理者 ID を指定します。デフォルトでは、`ConfigDirectoryAdminID` 指令で指定された値が使用されます。この指令については、15 ページの「認証エンティティの定義」を参照してください。
ServerAdminPwd	ServerAdminID のパスワードを指定します。
ServerIPAddress	Administration Server が待機する IP アドレスを指定します。マルチホームシステム上にインストールする場合、Administration Server に最初の IP アドレスを使用しないときは、この指令を使用します。

第 5 章

インストール後の手順

この章では、オンラインヘルプの起動とディレクトリツリーの実装に必要な、インストール後に行う手順について説明します。

ヘルプシステムの起動

iPlanet Directory Server のヘルプシステムは、iPlanet Administration Server に依存しています。Administration Server からはリモートとなるマシンで iPlanet Directory Server Console が稼働している場合は、次の項目を確認する必要があります。

Administration Server 上で承認されたクライアント IP アドレス : iPlanet Directory Server Console を実行しているマシンは、Administration Server にアクセスする必要があります。Administration Server がクライアントマシンの IP アドレスを受け入れるように構成するには、次の操作を実行します。

1. iPlanet Administration Server Console を起動します。Console は Administration Server と同じマシン上で実行している必要があります。
2. 「構成」タブをクリックしてから、「ネットワーク」タブをクリックします。
3. 「接続制限の設定」プルダウンメニューから「許可する IP アドレス」を選択します。「編集」をクリックします。
4. 「IP アドレス」フィールドを次のように編集します。*.*.*.*

   これで、すべてのクライアントが Administration Server にアクセスできるようになります。
5. Administration Server を再起動します。これで、Directory Server Console の「ヘルプ」ボタンをクリックして、オンラインヘルプを起動することができます。

Administration Server 上で承認されたプロキシ : Directory Server Console を実行しているクライアントマシン上の HTTP 接続でプロキシを使用する場合は、次のいずれかの操作を実行する必要があります。

- Directory Server Console を実行しているマシンからプロキシを削除する。これによって、クライアントマシンが直接 Administration Server にアクセスできるようになる

  Directory Server Console を実行しているコンピュータからプロキシを削除するには、次の操作を実行します。

  I. ヘルプの実行に使用するブラウザのプロキシ構成を変更する。

  II. Netscape Communicator の場合は、「編集」メニューの「設定」を選択します。

  III. 次に、「詳細」の「プロキシ」を選択してプロキシ構成を表示します。

  IV. Internet Explorer の場合は、「インターネットオプション」の「ツール」メニューを選択します。

または

- Administration Server の使用可能な IP アドレスのリストに、クライアントマシンのプロキシ IP アドレスを追加する

警告 Administration Server にクライアントマシンの IP アドレスを追加すると、システムに潜在的なセキュリティホールが発生する可能性があります。

ディレクトリツリーの実装

インストール時に、シンプルなディレクトリデータベースが作成されています。また、ユーザが使用できるシンプルなディレクトリ構造もデータベース内に作成されています。このディレクトリ構造には、推奨されるディレクトリ構造の基本的なアクセス制御と主な分岐点が含まれています。

この時点で、データベースにユーザエントリを実装する必要があります。ディレクトリ接尾辞を作成して実装する方法はいくつかあります。詳細については、『iPlanet Directory Server 管理者ガイド』を参照してください。

主な方法は次のとおりです。

- LDIF からデータベースを作成する : この方法を使用するのは、Directory Server 付属のサンプルディレクトリデータを使用したり、LDIF によってほかのディレクトリからエントリをインポートしたり、多くのエントリを一度に追加したりする場合である。インストールで提供されるサンプル LDIF ファイルは、*installDir*/slapd-*serverID*/ldif に格納される。LDIF の詳細は、『iPlanet Directory Server 管理者ガイド』を参照

- データベースが空の状態で Directory Server を起動し、LDAP によってデータをインポートする : この方法では、Directory Server Console などの LDAP クライアントを使用するか、`ldapmodify` コマンド行ユーティリティを使用して、ディレクトリを実装する必要がある

ディレクトリを実装する際は、必要なアクセス制御を考慮し、それに従って必要なアクセス制御を設定します。アクセス制御については、『iPlanet Directory Server 導入ガイド』および『iPlanet Directory Server 管理者ガイド』を参照してください。

Windows NT 4 および Windows 2000 におけるキャッシュサイズのチューニング

Windows NT 4.0 では、アプリケーションが使用可能な最大アドレス空間は 2G バイトです。この制限により、Directory Server は 2G バイトを超える仮想メモリは使用できないため、サーバ用に構成するキャッシュの合計を 2G バイト未満にする必要があります。エントリキャッシュおよびデータベースキャッシュのサイズがこの制限を超えると、Directory Server はエラーメッセージを表示して終了します。

キャッシュサイズを設定する場合は、次の推奨事項を適用してください。

- Windows NT では、データベースキャッシュを 1.5G バイト未満に設定する。1.5G バイト以上にすると、サーバが起動しなくなる可能性がある。データベースキャッシュの属性は `nsslapd-dbcachesize` で、エントリ `cn=config,cn=ldbm database,cn=plugins,cn=config` 内に格納される。この属性の詳細は、『iPlanet Directory Server 構成、コマンド、およびファイルのリファレンス』を参照
- データベースキャッシュのサイズを 1.5G バイト以上に増やす必要がある場合は、データベースキャッシュを構成するメモリチャンクの数を指定する `nsslapd-dbncache` 属性の設定を変更することができる。この属性は、エントリ `cn=config,cn=ldbm database,cn=plugins,cn=config` 内に格納され、デフォルト値は 1 である。この属性値を増やすと、オペレーティングシステムが 1 つの大きなメモリ領域の代わりに複数の小さなメモリ領域にキャッシュを割り当てることができるようになるため、データベースキャッシュのサイズが増加する。2G バイトの制限は依然として適用される
- Microsoft Knowledge Base の article Q171793 に記載されているように、Windows NT4/Enterprise Edition および Windows 2000 Advanced Server では、アプリケーションから利用可能なアドレス空間を 3G バイトまで増やすことができる

第 6 章

旧バージョンからの移行

Netscape Directory Server 4.0、4.1、4.11、4.12、4.13、または 5.0 は、iPlanet Directory Server 5.1 にアップグレードできます。この章では、次の各節でその方法を説明します。

- 移行の概要
- 移行前の確認事項
- カスタムスキーマの識別
- 移行手順
- レプリケートサイトの移行

この章には、Innosoft Distributed Directory Server 4.5.1 からのアップグレード方法については記載されていません。この方法については、『Innosoft Distributed Directory Server Transition Guide』を参照してください。

移行の概要

ディレクトリサービスを iPlanet Directory Server 5.1 に移行する前に、このリリースの Directory Server の新しい機能をよく理解する必要があります。

移行プロセスは、古いバージョンの Directory Server がインストールされているシステム上で、`migrateInstance5` スクリプトを実行して行います。この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。

移行スクリプトは、次のタスクを順番に実行します。

- スキーマ構成ファイルを確認し、標準構成ファイルと現在システム上にあるファイルとの相違点をレポートする

- 古いバージョンの Directory Server に格納されている各接尾辞のデータベースを作成する (Directory Server 5.0 および 5.1 では複数のデータベースを持つことができるが、各データベースに使用できる接尾辞は 1 つだけである)
- サーバパラメタとデータベースパラメタを移行する (Directory Server 5.0 および 5.1 では、これらのパラメタは LDAP エントリとして `dse.ldif` ファイルに格納される)
- ユーザ定義のスキーマオブジェクトを移行する
- インデックスを移行する
- 標準サーバプラグインを移行する
- 証明書データベースおよび SSL パラメタを移行する
- データベースリンクを移行する
- レプリケーションエントリ (レプリケーション、レプリケーションアグリーメントエントリ、バインド dn エントリ、更新履歴ログ) を移行する
- SNMP 構成を移行する

移行プロセスを実行する前に、移行スクリプトによって古いバージョンの Directory Server が停止されます。また、移行スクリプトによって現在の構成のバックアップも作成されます。

移行前の確認事項

この節では、移行プロセスを開始する前に、システムで満たしていなければならない条件について説明します。

- 移行できるのは Directory Server 4.0、4.1、4.11、4.12、4.13、または 5.0 に限られる。移行スクリプトを実行するときは、古いバージョンのサーバプロセス `ns-slapd` を停止しておく必要がある
- 古いバージョンの Directory Server と新しい Directory Server 5.1 は、同じホスト上にインストールする必要がある。移行はネットワークドライブを介して行うことはできない
- 古いバージョンの Directory Server をそのまま稼働させておきたい場合は、iPlanet Directory Server 5.1 のインストール時に、古いバージョンの Directory Server で使用しているものとは異なるポートを、LDAP トラフィック用とセキュリティ保護された接続用に選択する

  古いバージョンの Directory Server を稼働させない場合は、静的な構成情報 (Directory Server のポート番号を含む) を持つすべてのディレクトリクライアントがそのまま機能するように、同じポート番号を使用する

- 移行スクリプトを実行する時は、iPlanet Directory Server 5.1 が稼働中でなければならない
- 古いバージョンの Directory Server 4.x で作成したすべてのカスタムスキーマは、デフォルトファイルに格納するか、include 文を使用して `slapd.conf` ファイルに含める必要がある。Directory Server 4.x の場合、カスタムスキーマのデフォルトファイルは、`slapd.user_oc.conf` ファイルおよび `slapd.user_at.conf` ファイルである。これらのファイルに格納されていないカスタムスキーマがある場合は、「カスタムスキーマの識別」で説明する手順に従ってカスタムスキーマをこれらのファイルに移動する
- Directory Server 5.0 で作成したすべてのカスタムスキーマを `/usr/iplanet/servers/slapd-`*serverID*`/config/schema` ディレクトリ内の LDIF ファイルに格納する必要がある
- UNIX の場合は、次の環境変数を設定する

  ```
  PERL5LIB=/usr/iplanet/servers/bin/slapd/admin/bin
  PATH=/usr/iplanet/servers/bin/slapd/admin/bin:$PATH
  ```

- Windows NT の場合は、次の環境変数を設定する

  ```
  PERL5LIB=server5root\bin\slapd\admin\bin
  ```

  また、`PATH` 環境変数に `server5root/bin/slapd/admin/bin` を追加する。`server5root` は、Directory Server がインストールされているディレクトリに置き換える

カスタムスキーマの識別

`slapd.at.conf` または `slapd.oc.conf` ディレクトリを変更することにより、古いバージョンの Directory Server 内のスキーマをカスタマイズした場合、そのカスタムスキーマは、サーバ移行プロセスでは移行できません。この場合は、標準スキーマが変更されているためにユーザが手動で修正しなければならないという内容のメッセージが移行中に表示されます。その後の移行プロセスでは、スキーマファイルのコピーが保存され、代わりに古いバージョンの標準スキーマファイルがその場所で使用されます。

移行はこの時点で完了しますが、この状態では Directory Server 5.1 内のデータは変更できません。したがって、カスタムスキーマは、移行を行う前に別のファイルにコピーすることをお勧めします。標準の `slapd.user_oc.conf` ファイルと `slapd.user_at.conf` ファイル、または `slapd.conf` 内で `useroc` および `userat` キーワードによって指定したファイルを使用できます。

カスタムスキーマと標準スキーマを識別するには、次の手順を実行します。

1. 古い slapd.at.conf ファイルと slapd.oc.conf ファイルを調べ、追加されたすべてのスキーマを見つけます。

   標準ファイルに加えた変更箇所をすべて判別できたか確認するには、それらを /bin/slapd/install/version4 ディレクトリにある標準ファイルと比較します。または、すでに migrateInstance5 スクリプトを実行した場合は、このスクリプトによって示される表示を使用することもできます。

2. カスタムスキーマ要素を、次のファイルに移動します。

   /usr/iplanet/servers/slapd-*serverID*/config/slapd.user_at.conf および /usr/iplanet/servers/slapd-*serverID*/config/slapd.user_oc.conf

   これらのファイル名は、4.x のスキーマ構成エディタが書き込みを行うので、これらのファイル名を使用することをお勧めします。ただし、ほかのファイル名を使用することもできます。

   カスタム定義された複数のオブジェクトクラスで継承関係がある場合は、スキーマ構成ファイルにおけるオブジェクトの出現の順番に注意してください。上位のオブジェクトクラスは、その他のものよりも先に定義する必要があります。

3. userat 指令および useroc 指令を使用して、これらのファイルを slapd.conf ファイル内に含めます。新しい指令は、ファイル内のほかの構成ファイル用の include 文が置かれている場所に置きます。

   構成ファイルを含める順番は重要ではありません。

その後、カスタム属性を slapd.oc.conf 内の標準オブジェクトクラスに追加した場合は、次の手順を実行する必要があります。

4. slapd.user_oc.conf ファイル (またはユーザが作成した同等のファイル) 内に、カスタム属性を含む新しいオブジェクトクラスを作成します。
5. この新しいオブジェクトクラスを、ディレクトリ内の、カスタム属性を使用するすべてのエントリに追加します。

移行手順

移行スクリプトによって、現在の Directory Server の構成のバックアップも作成されます。

Directory Server 4.x から移行する場合は、/usr/netscape/server4/slapd-*serverID*/config ディレクトリにあるすべてのファイルのバックアップが /usr/netscape/server4/slapd-*serverID*/config_backup に作成されます。

Directory Server 5.0.x からアップグレードする場合、/usr/iplanet/servers/slapd-*serverID*/config ディレクトリにあるすべてのファイルのバックアップが、/usr/iplanet/servers/slapd-*serverID*/config_backup に作成されます。

構成ファイルがデフォルト以外の場所に格納されている場合は、サーバを移行する前に構成ファイルを安全な場所にコピーしておいてください。

重要な構成情報をバックアップしたら、次の手順に従ってサーバを 5.1 に移行します。

1. 古いバージョンの Directory Server を停止します。

注	古いバージョンの Directory Server を停止しなかった場合は、移行スクリプトによって自動的に停止されます。

2. 古いバージョンの Directory Server がインストールされているマシン上に、Directory Server 5.1 をインストールします。

   インストールプロセスについては、第 3 章「高速インストールと標準インストールの使用」または第 4 章「サイレントインストール」を参照してください。

   静的な構成情報 (Directory Server のポート番号を含む) を持つすべてのディレクトリクライアントを確実にそのまま機能させるには、古いバージョンのサーバと同じポート番号を使用します。

3. 移行スクリプトを実行します。root ユーザ (UNIX) または administrator (Windows NT) として、/usr/iplanet/servers/bin/slapd/admin/bin ディレクトリに移動します。次のコマンドを入力します。

   UNIX の場合 :

```
migrateInstance5 -D rootDN -w passwd -p port -o oldServerPath -n newServerPath
```

   または

```
migrateInstance5 -D rootDN -j passwdFile -p port -o oldServerPath -n newServerPath
```

   Windows NT の場合 :

```
perl migrateInstance5 -D rootDN -w passwd -p port -o oldServerPath -n newServerPath
```

   または

```
perl migrateInstance5 -D rootDN -j passwdFile -p port -o oldServerPath -n newServerPath
```

   各オプションは、次のように指定します。

   - *rootDN* には、Directory Server 5.1 でのディレクトリマネージャの DN を指定します。

- *passwd* には、Directory Server 5.1 でのディレクトリマネージャのパスワードを指定します。
- *passwdFile* には、Directory Server 5.1 でのディレクトリマネージャのパスワードを格納したファイル指定します。
- *port* には、Directory Server 5.1 での LDAP ポート番号を指定します。
- *oldServerPath* には、古いバージョンの Directory Server のディレクトリへのパス (たとえば /usr/netscape/server4/slapd-*serverID*) を指定します。
- *newServerPath* には、Directory Server 5.1 のディレクトリへのパス (たとえば /usr/iplanet/servers/slapd-*serverID*) を指定します。

UNIX マシンで Directory Server 4.11 から Directory Server 5.1 に移行するコマンド例を示します。

```
migrateInstance5 -D "cn=Directory Manager" -w secret -p 1389 -o
/usr/netscape/server4/slapd-coolwave -n /usr/iplanet/servers/slapd-coolwave
```

NT マシンで同様の操作を行うコマンド例を示します。

```
perl migrateInstance5 -D "cn=Directory Manager" -w secret -p 1389 -o
/usr/netscape/server4/slapd-coolwave -n /usr/iplanet/servers/slapd-coolwave
```

UNIX マシンで Directory Server 5.0 から Directory Server 5.1 に移行するコマンド例を示します。

```
migrateInstance5 -D "cn=Directory Manager" -w secret -p 1389 -o
/usr/iPlanet/DS50/slapd-migrate -n /usr/iPlanet/DS51/slapd-migrate
```

NT マシンで同様の操作を行うコマンド例を示します。

```
perl migrateInstance5 -D "cn=Directory Manager" -w secret -p 1389 -o
/usr/iPlanet/DS50/slapd-migrate -n /usr/iPlanet/DS51/slapd-migrate
```

4. バックアップディレクトリのパスとファイル名を入力します。または、デフォルトをそのまま使用します。

   スクリプト出力の一部を示します。

```
Parse the configuration file:
/space/iPlanet/server4_11/slapd-coolwave/config/slapd.conf...

Suffix o=France.Sun.COM doesn't exist

Backend: MigratedDB_0 has been created !!!

Suffix dc=coolwave,dc=France,dc=Sun,dc=COM doesn't exist

Backend: MigratedDB_1 has been created !!!

For the suffix o=NetscapeRoot, we do nothing

Suffix dc=radius.fr doesn't exist

Backend: MigratedDB_2 has been created !!!
```

```
Update general server parameters...
Update successfully passwordHistory
Update global LDBM parameters...
Update successfully nsslapd-mode
Update specific backend parameters...
Migrate DSE entries...
Migrate attributes...
Migrate objectclasses...
Migrate indexes...
Migrate plugin's...
```

Directory Server 5.0 から Directory Server 5.1 に移行する場合のスクリプト出力の一部を示します。

```
Shutting down server slapd-migrate . . .
Backup /usr/iplanet/DS51/slapd-migrate/config on
/usr/iplanet/DS51/slapd-migrate/config_backup ...
Migrate the schema...
Connected to 5.1 LDAP server
Parse the old DSE ldif file: /usr/iplanet/DS50/slapd-migrate/config/dse.ldif
Migrate DSE entries...
Migrate LDBM backend instances...
Migrate default indexes...
Migrate indexes...
Migrate replicas...
Migrate replication agreements...
Migrate key/cert databases...
Migrate Certmap.conf...
***** Close the LDAP connection to the 5.1 Directory Server instance *****
Shutting down server slapd-migrate . . .
***** Migrate ReplicaBindDN entries...
***** Migrate MultiplexorBindDN entries...
****** End of migration ******
```

これで、古いバージョンの Directory Server からの移行は完了します。移行の結果、古いバージョンの Directory Server から取得した構成情報を使用して、新しい Directory Server 5.1 インスタンスがインストールされます。また、古いサーバからのデータが新しいサーバに移行され、新しいサーバが起動されます。

レプリケートサイトの移行

Directory Server 5.0 から Directory Server 5.1 にアップグレードする場合は、`migrateInstance5` スクリプトを実行すると、レプリケーション構成の移行が自動的に行われます。

この節では、4.x サーバの複製トポロジを 5.1 ディレクトリサーバの複製トポロジに手動で移行する手順を説明します。

Directory Server 4.0、4.1、4.11、4.12、および 4.13 のインスタンスを移行できるのは、これらのリリースの Directory Server はコンシューマとして構成された Directory Server 5.1 へレプリケートすることが可能なためです。

次に、レプリケート環境の移行に関する制約事項、方法、および手順の概要を示します。

制約事項

レプリケート環境をうまく移行させるには、次に示す制約事項に従ってください。

- 古いバージョンのサーバの複製トポロジは、有効なトポロジでなければならない
- 新しい Directory Server 5.x は、Directory Server 4.x のコンシューマでなければならない
- Directory Server 5.x は、古いバージョンのコンシューマとして構成しなければならない
- 4.x サプライヤサーバと 5.x コンシューマサーバとの間のレプリケーションアグリーメントは、4.x のサプライヤ主導レプリケーションアグリーメントでなければならない

方法

制約に従い、4.x サーバの複製トポロジの移行は次のように行われます。

1. Directory Server 5.1 をインストールし、次の両方に従って構成します。

- 変更を記録する読み書き可能複製として構成する (移行プロセス完了後にサーバが担う役割)
- 古いバージョンのコンシューマとして構成する (移行プロセス中にサーバが担う必要のある役割)

2. Directory Server 5.1 に更新データが送られるように、4.x サプライヤを構成します。
3. 4.x コンシューマサーバを Directory Server 5.1 にアップグレードし、そのサプライヤサーバを手順 1 で構成した Directory Server 5.1 に変更します。

   これで、この Directory Server はハブサプライヤとして動作するようになります。
4. 4.x サプライヤ構成を解除します。

   これで、手順 1 で構成した Directory Server 5.1 がトポロジ内で唯一のサプライヤとなります。

例：手順の詳細

次のような非常にシンプルな複製トポロジを考えてみます。

- サプライヤサーバは 1 台で、これをサーバ A とする
- コンシューマサーバは 2 台で、これをサーバ B およびサーバ C とする
- サーバ A は、サーバ B およびサーバ C に対する、サプライヤ主導複製処理契約を持つ
- サーバ A、B、および C は、4.0、4.1、4.11、または 4.12 の Directory Server である

注 サーバ B および C がサーバ A に対する CIR 複製契約を持つ場合は、トポロジを移行できます。ただし、Directory Server 5.1 では CIR (コンシューマ主導複製処理) がサポートされていないので、新しい複製環境で CIR 契約を持つことはできません。

このトポロジを移行するには、次の手順を実行します。

1. 新しいサーバであるサーバ D に iPlanet Directory Server 5.1 をインストールします。
2. サーバ D を、移行後の複製トポロジにおける役割を担うように、つまり変更を記録する読み書き可能複製として構成します。

   この手順については、『iPlanet Directory Server 管理者ガイド』のレプリケーションについての章を参照してください。

3. 次に、サーバ D を古いバージョンのコンシューマとして設定します。

   この手順については、『iPlanet Directory Server 管理者ガイド』のレプリケーションについての章を参照してください。

4. 『iPlanet Directory Server インストールガイド』の説明に従って、サーバ B を iPlanet Directory Server 5.1 にアップグレードします。

5. サーバ B をサーバ D の読み取り専用レプリカにします。

   これで、サーバ D がハブサプライヤとなります。サーバ D はサーバ A から更新データを受け取り、今度は自分がサーバ B を更新します。

6. サーバ C を iPlanet Directory Server 5.1 にアップグレードして、サーバ D の読み取り専用レプリカにします。

7. サーバ A のサプライヤ設定を解除します。サーバ D の古いバージョンのコンシューマ設定を無効にします。

   これによって、サーバ D はコンシューマサーバ B および C に対して唯一のサプライヤとなります。

複製トポロジの移行が完了したら、そのトポロジを発展させて多重マスター複製を使用できるようにすることができます。そのためには、レプリケーショントポロジのマスターとなる新しい iPlanet Directory Server 5.1 を追加する必要があります。読み取り専用レプリカを読み書き可能レプリカに変更することはできません。

マルチマスターレプリケーションのトポロジについては、『iPlanet Directory Server 管理者ガイド』を参照してください。

第 7 章

トラブルシューティング

この章では、もっとも一般的なインストール上の問題とその解決方法について説明します。また、システムのパッチレベルとカーネルパラメタ設定の確認に関するいくつかのヒントも記載します。

idsktune の実行

idsktune ユーティリティを使用すると、使用システムのパッチレベルとカーネルパラメタ設定を簡単に確認できます。idsktune を実行するには、事前に Directory Server をインストールしておく必要があります。idsktune は、Windows NT および Windows 2000 では使用できません。

idsktune は次の手順で実行します。

1. Directory Server のインストールディレクトリに移動します。

   デフォルトのインストールディレクトリは、/usr/iplanet/servers です。

2. サブディレクトリ bin/slapd/server に移動します。
3. root として、次のコマンドを入力します。

   ```
   # ./idsktune
   ```

次に、idsktune の実行結果の例を示します。idsktune 自体はシステムに何の変更も加えないことに注意してください。

```
iPlanet Directory Server system tuning analysis version 30-OCT-2000.
Copyright 2000 Sun Microsystems, Inc.
NOTICE : System is usparc-sun-solaris5.8 (SUNW,Ultra-5_10) (1 processor).
NOTICE : Patch 109320-01 is not installed.
```

```
NOTICE : Patch 108875-04 is present, but 108875-07 is a more recent version.

NOTICE : Patch 108652-04 is present, but 108652-13 is a more recent version.

NOTICE : Solaris patches can be obtained from http://sunsolve.sun.com or your
Solaris support representative.

WARNING: The tcp_close_wait_interval is set to 240000 milliseconds (240
seconds).This value should be reduced to allow for more simultaneous connections
to the server.A line similar to the following should be added to the
/etc/init.d/inetinit file:

ndd -set /dev/tcp tcp_time_wait_interval 30000

NOTICE : The tcp_conn_req_max_q value is currently 128, which will limit the value
of listen backlog which can be configured.It can be raised by adding to
/etc/init.d/inetinit, after any adb command, a line similar to:

ndd -set /dev/tcp tcp_conn_req_max_q 1024

NOTICE : The tcp_keepalive_interval is set to 7200000 milliseconds (120
minutes).This may cause temporary server congestion from lost client connections.

NOTICE : The tcp_keepalive_interval can be reduced by adding the following line to
/etc/init.d/inetinit:

ndd -set /dev/tcp tcp_keepalive_interval 600000

NOTICE : The NDD tcp_rexmit_interval_initial is currently set to 3000 milliseconds
(3 seconds).This may cause packet loss for clients on Solaris 2.5.1 due to a bug
in that version of Solaris.If the clients are not using Solaris 2.5.1, no problems
should occur.

NOTICE : If the directory is service is intended only for LAN or private
high-speed WAN environment, this interval can be reduced by adding to
/etc/init.d/inetinit:

ndd -set /dev/tcp tcp_rexmit_interval_initial 500

NOTICE : The NDD tcp_smallest_anon_port is currently 32768.  This allows a maximum
of 32768 simultaneous connections.More ports can be made available by adding a
line to /etc/init.d/inetinit:

ndd -set /dev/tcp tcp_smallest_anon_port 8192

WARNING: tcp_deferred_ack_interval is currently 100 milliseconds.This will cause
Solaris to insert artificial delays in the LDAP protocol.It should be reduced
during load testing.

This line can be added to the /etc/init.d/inetinit file:

ndd -set /dev/tcp tcp_deferred_ack_interval 5
```

```
WARNING: There are only 1024 file descriptors available, which limit the number of
simultaneous connections.Additional file descriptors, up to 65536, are available
by adding to /etc/system a line like set rlim_fd_max=4096

NOTICE : / partition has less space available, 245MB, than the largest allowable
core file size of 460MB.A daemon process which dumps core could cause the root
partition to be filled.

#
```

一般的なインストール上の問題

クライアントがサーバを検出できない

まず、ホスト名を使用してみます。ホスト名を使用しても検出できない場合は、完全指定 (`www.domain.com` など) を使用し、サーバが DNS に登録されていることを確認します。それでも検出できない場合は IP アドレスを使用します。

ポートが使用中である

アップグレードの前に、サーバを停止しなかった可能性があります。古いサーバを停止し、アップグレードしたサーバを手動で起動します。

あるいは、インストールされているほかのサーバがそのポートを使用している可能性があります。選択したポートがほかのサーバで使用されていないことを確認してください。

LDAP 認証エラーになりインストールに失敗する

DNS 命名規則ではなく NIS 命名規則を使用しているネットワークに Directory Server をインストールする場合は、次のエラーが発生することがあります。

```
ERROR: Ldap authentication failed for url ldap://incorrect.DNS.address
user id admin (151:Unknown error.)

Fatal Slapd Did not add Directory Server information to
Configuration Server.

ERROR.Failure installing iPlanet Directory Server.Do you want to
continue [n]?
```

マシンで DNS 命名規則が使用されるように正しく構成されていないと、このエラーが発生します。これは、インストール時に示されるデフォルトの絶対パスによるホスト名とドメイン名が正しくないことが原因です。つまり、デフォルトを使用すると、LDAP 認証エラーが発生します。

インストールを正しく行うには、ローカルホスト名とそのドメイン名から成る完全指定によるドメイン名を指定する必要があります。ホスト名は、コンピュータに割り当てられた論理名です。たとえば、`mycomputer` がホスト名で、`siroe.com` が完全指定によるドメイン名です。

絶対パスによるドメイン名を使用すると、インターネット上のすべてのホストのインターネットアドレスを一意に識別できます。同じ命名方式は、インターネット上にない一部のホストにも使用されますが、電子メールアドレスは同じネームスペースを共有します。

ディレクトリマネージャの DN とパスワードを忘れてしまった場合

ディレクトリマネージャの DN は、`/usr/iplanet/servers/slapd-`*server ID*`/config/dse.ldif` の `nsslapd-rootdn` 属性で確認できます。

また、ディレクトリマネージャ DN のパスワードを忘れた場合は、次の手順により設定し直すことができます。

1. slapd.conf 内の `nsslapd-rootpw` 属性を探します。属性値がまったく暗号化もされていない (つまり、`{SHA}` または `{CRYPT}` で始まっていない) 場合は、パラメタに示されているものがパスワードです。
2. 属性が暗号化されている場合は、その属性値を削除してクリアテキストの値に置き換えます。たとえば、`nsslapd-rootpw` 属性を次のように変更したとします。

   ```
   nsslapd-rootpw: my_password
   ```

   この場合、ディレクトリマネージャ DN のパスワードは `my_password` です。
3. Directory Server を再起動します。
4. サーバを再起動したら、ディレクトリマネージャとしてログインし、パスワードを変更します。パスワード変更時には、必ず暗号化スキーマを選択してください。

ディレクトリマネージャ用パスワードの変更については、『iPlanet Directory Server 管理者ガイド』を参照してください。

用語集

ACI　Access Control Instruction の略称。ディレクトリ内のエントリに対するアクセス権を許可または拒否する命令。

ACL　アクセス制御リスト。ディレクトリへのアクセスを制御するメカニズム。

Authenticating Directory Server　PTA (パススルー認証) における、要求元クライアントの認証資格を保持する Directory Server を指す。PTA が有効なホストは、クライアントから受信する PTA 要求をバインドホストに送信する。

CA　「認証局 (Certificate Authority)」を参照。

ciphertext　この情報を復号化する適切な鍵がないと読むことができない、暗号化された情報。

CIR　「コンシューマ主導レプリケーション処理 (consumer-initiated replication)」を参照。

CoS　アプリケーションに認識されない方法で、エントリ間で属性を共有する方法。

CoS 定義エントリ (CoS definition entry)　使用中の CoS のタイプを特定する。対象とする分岐の下に LDAP サブエントリとして格納される。

CoS テンプレートエントリ (CoS template entry)　共有属性値のリストを含む。

DAP　Directory Access Protocol の略称。クライアントがディレクトリにアクセスするための ISO X.500 標準プロトコル。

Directory Access Protocol　「DAP」を参照。

Directory Server Console　ディレクトリの内容を表示、設定、および管理するためのグラフィックユーザインタフェースを提供する LDAP クライアントアプリケーション。iPlanet Directory Server 製品のコンポーネント。

DIT　「ディレクトリツリー (directory tree)」を参照。

DM 「ディレクトリマネージャ (Directory Manager)」を参照。

DN 「識別名 (distinguished name)」を参照。

DNS ドメインネームシステム。標準の IP アドレス (198.93.93.10 など) をホスト名 (`www.iPlanet.com` など) と関連付けるために、ネットワーク上のマシンが使用するシステム。マシンは通常、ホスト名の IP アドレスを DNS サーバから取得するか、システム上で維持されているテーブルから検索する。

DNS エイリアス (DNS alias) DNS サーバが別のホストを指していることを認識しているホスト名
(特に、DNS CNAME レコード)。マシンは常に実際の名前を 1 つ持つが、1 つ以上のエイリアスを持つこともできる。たとえば、`www.[yourdomain].[domain]` などのエイリアスは、現在サーバが存在する `realthing.[yourdomain].[domain]` という名前の実際のマシンをポイントできる。

HTML ハイパーテキストマークアップ言語。World Wide Web 上のドキュメントで使用されるフォーマット化言語。HTML ファイルはフォーマット化コードを含むプレーンテキストファイルであり、Netscape Navigator などのブラウザにテキストの表示方法、グラフィックの配置方法、および項目の配列方法を指示し、ほかのページへのリンクを表示する。

HTTP ハイパーテキスト転送プロトコル。HTTP サーバとクライアントの間で情報を交換するための規約。

HTTP-NG 次世代のハイパーテキスト転送プロトコル。

HTTPD HTTP デーモンまたはサービスの略称で、HTTP プロトコルを使用して情報を提供するプログラム。一般に、このデーモンまたはサービスは、httpd と呼ばれる。

HTTPS セキュリティ保護を強化した HTTP。SSL (Secure Sockets Layer) を使用して実装される。

IP アドレス (IP address) インターネットプロトコルアドレス。ドットで区切られた一組の数字で、インターネット上にあるマシンの実際の位置を指定する。たとえば、
198.93.93.10 など。

ISO 国際標準化機構。

LDAP Lightweight Directory Access Protocol の略称。TCP/IP を介して複数のプラットフォーム間で動作するように設計されたディレクトリサービスプロトコル。

LDAP Data Interchange Format 「LDIF」を参照。

LDAP URL DNS を使用して Directory Server を検出し、LDAP を介して照会を完了する方法を提供する。たとえば、`ldap://ldap.iplanet.com` など。

LDAP クライアント (LDAP client)　LDAP Directory Server からの LDAP エントリを要求および表示するために使用されるソフトウェア。「*ブラウザ (browser)*」も参照。

LDAPv3　LDAP プロトコルのバージョン 3。Directory Server のスキーマ形式は、このプロトコルに基づく。

LDBM データベース (LDBM database)　高性能なディスクベースのデータベースで、このデータベースに割り当てられたすべてのデータを含む一連の大きなファイルで構成される。Directory Server の一次データ記憶域である。

LDIF　LDAP Data Interchange Format の略称。Directory Server のエントリをテキスト形式で表すために使用される形式。

Lightweight Directory Access Protocol　「LDAP」を参照。

MD5　RSA Data Security, Inc. によるメッセージダイジェストアルゴリズム。データの短いダイジェストの生成に使用できる。このダイジェストは、高い確率で一意となるため、同じメッセージダイジェストを生成するデータの作成は、数学的に見て非常に困難である。

MD5 シグニチャ (MD5 signature)　MD5 アルゴリズムで生成されたメッセージダイジェスト。

MIB　管理情報ベース。SNMP ネットワークと関連付けられたすべてのデータ、またはその一部。MIB は、すべての SNMP 管理対象オブジェクトの定義を含むデータベースとみなすことができる。MIB は、ツリーに似た階層を持つ。最上位にはネットワークに関するもっとも一般的な情報が含まれており、下位では個別のネットワーク領域に固有の情報を扱う。

MIB ネームスペース (MIB namespace)　管理情報ネームスペース。ディレクトリのデータに名前を設定し、参照する方法。ディレクトリツリーとも呼ばれる。

N + 1 ディレクトリ問題 (n + 1 directory problem)　さまざまなディレクトリで同じ情報の複数のインスタンスを管理する場合の問題。結果的に、ハードウェアにかかる費用と人的費用が増大する。

Network Management Station　「NMS」を参照。

NIS　Network Information Service の略称。UNIX マシンが使用する、プログラムとデータファイルから構成されるシステムで、コンピュータネットワーク全体のマシン、ユーザ、ファイルシステム、およびネットワークパラメタに関する各マシン固有の情報を収集、照合、および共有するためのサービスを提供する。

NMS　Network Management Station の略称。1 つ以上のネットワーク管理アプリケーションがインストールされたパワフルなワークステーション。

ns-slapd　iPlanet LDAP Directory Server のデーモンまたはサービスで、Directory Server のすべてのアクションに関連する。「slapd」も参照。

OID　「オブジェクト識別子 (object identifier)」を参照。

PDU　Protocol Data Unit の略称。SNMP デバイス間のデータ交換の基礎となる符号化されたメッセージ。

Protocol Data Unit　「PDU」を参照。

PTA　パススルー認証。バインド資格を確認するために、1 つの Directory Server がほかの Directory Server と交信するメカニズム。

PTA Directory Server　パススルー認証 (PTA) で、受信したバインド要求を Authenticating Directory Server に送信 (パススルー) するサーバ。

PTA LDAP URL　パススルー認証で、Authenticating Directory Server、パススルーサブツリー、および省略可能なパラメタを定義する URL。

RAM　ランダムアクセスメモリ。コンピュータ内部にあり、多数の半導体で構成された物理的な記憶装置。RAM 内に格納されている情報は、コンピュータが停止すると消失する。

rc.local　マシンの起動時に実行されるプログラムを記述した Unix マシン上のファイル。格納位置から、`/etc/rc.local` とも呼ばれる。

RDN　相対識別名。完全な識別名を形成するために文字列にエントリの祖先を追加する前の、エントリ自体の名前。

RFC　Request For Comments の略称。インターネットコミュニティに提出される手順あるいは標準文書。技術が標準として受け入れられる前に、ユーザは技術に関してコメントを送ることができる。

root　Unix マシン上でもっとも高いレベルの特権を持つユーザ。root ユーザは、マシン上のすべてのファイルに対して完全なアクセス特権を持つ。

Secure Sockets Layer　「SSL」を参照。

SIE　サーバインスタンスのエントリ。

SIR　「サプライヤ主導レプリケーション処理 (supplier-initiated replication)」を参照。

slapd　LDAP Directory Server のデーモンまたはサービス。複製以外のディレクトリのほとんどの機能を受け持つ。「*ns-slapd*」も参照。

SNMP　簡易ネットワーク管理プロトコル。ネットワーク処理に関するデータを交換することによって、サーバ上で実行しているアプリケーションプロセスを監視および管理するために使用される。

SNMP サブエージェント (SNMP subagent)　管理対象のデバイスに関する情報を収集し、その情報をマスターエージェントに渡すソフトウェア。

SNMP マスターエージェント (SNMP master agent)　さまざまなサブエージェントと NMS の間で情報を交換するソフトウェア。

SSL　Secure Sockets Layer の略称。クライアントとサーバとの間にセキュリティ保護された接続を確立するソフトウェアライブラリ。セキュリティ保護が強化された HTTP である HTTPS の実装に使用される。

TCP/IP　Transmission Control Protocol/Internet Protocol の略称。インターネットや企業内ネットワークにおける主要なネットワークプロトコル。

TLS　Transport Layer Security の略称。SSL の新標準で、公開鍵に基づいたプロトコル。

Transport Layer Security　「TLS」を参照。

uid　Unix システム上で、各ユーザと関連付けられた一意の番号。

URL　Uniform Resource Locator の略称。サーバおよびクライアントが文書の要求に使用するアドレス指定システム。ロケーションとも呼ばれる。URL の形式は、`[protocol]://[machine:port]/[document]`。ポート番号は一部のサーバでのみ必要であり、多くの場合サーバによって割り当てられるので、その場合ユーザは URL でポート番号を指定する必要はない。

X.500 標準 (X.500 standard)　Directory Server の実装で使用される、推奨する情報モデル、オブジェクトクラス、および属性を概説する一連の ISO/ITU-T 文書。

アカウントの無効化 (account inactivation)　ユーザアカウント、アカウントのグループ、またはドメイン全体を無効にして、すべての認証の試行に対して、自動的に拒否するようにする。

アクセス権 (permission)　アクセス制御で、ディレクトリ情報へのアクセスの許可または拒否、および許可または拒否されるアクセスのレベルを規定する。「アクセス権限」も参照。

アクセス権限 (access rights)　アクセス制御で、許可または拒否されているアクセスのレベルを指す。アクセス権限は、ディレクトリで実行できる操作のタイプと関連している。読み取り、書き込み、追加、削除、検索、比較、本人による書き込み、プロキシなど、すべての権利を許可または拒否できる。

アクセス制御命令 (access control instruction)　「ACI」を参照。

アクセス制御リスト (access control list) 「ACL」を参照。

インデックスキー (index key) ディレクトリが使用する各インデックスは、インデックスキーのテーブルとマッチングエントリ ID リストで構成されている。

エントリ (entry) オブジェクトに関する情報を含む LDIF ファイル内の行のグループ。

エントリ ID リスト (entry ID list) ディレクトリが使用する各インデックスは、インデックスキーのテーブルとマッチングエントリ ID リストで構成されている。エントリ ID リストは、クライアントアプリケーションの検索要求とマッチする可能性があるエントリ候補のリストを構築するために、ディレクトリが使用する。

エントリの配布 (entry distribution) 多数のエントリをサポートできるようスケーリングするために、複数のサーバにディレクトリエントリを配布する手法。

オブジェクトクラス (object class) どの属性がそのエントリ内に含まれるのかを定義することにより、ディレクトリ内のエントリのタイプを定義する。

オブジェクト識別子 (object identifier) オブジェクト指向システムにおいて、オブジェクトクラスや属性などのスキーマ要素を一意に特定する、通常 10 進数の数字の文字列。オブジェクト識別子は、ANSI、IETF、または同様の組織が割り当てる。

親アクセス (parent access) この権限が与えられると、バインド DN がターゲットエントリの親である場合は、ユーザはディレクトリツリー内で自分の下にあるエントリにアクセスできる。

カスケード型レプリケーション (cascading replication) カスケード型レプリケーションでは、1 つのサーバ (一般にハブサプライヤと呼ばれる) が特定のレプリケーションでコンシューマとサプライヤの両方として動作する。このサーバは読み取り専用の複製を保持し、更新履歴ログを管理する。また、データのマスターコピーを保持するサプライヤサーバから更新を受け取り、次にコンシューマにこの更新を供給する。

仮想リスト表示インデックス (virtual list view index) ブラウズインデックスとも呼ばれる。Directory Server Console でエントリ内の表示を高速化する。仮想リスト表示インデックスは、表示の性能を向上させるために、ディレクトリツリー内のすべての分岐点で作成可能。

簡易ネットワーク管理プロトコル (Simple Network Management Protocol) 「SNMP」を参照。

間接 CoS (indirect CoS) 間接 CoS は、ターゲットエントリの属性のうちの 1 つの値を使用してテンプレートエントリを特定する。

管理されているロール (managed role) ユーザは、メンバーの明示的な列挙リストを作成できる。

管理情報ベース (management information base) 「MIB」を参照。

管理対象オブジェクト (managed object) SNMP エージェントがアクセス可能で、NMS に対しても送信できる標準値。各管理対象オブジェクトは、ドット表記法で表現される正式名および数字の識別子で識別される。

近似インデックス (approximate index) 近似あるいは発音のようなもので検索が可能になる。

クライアント (client) 「LDAP クライアント (LDAP client)」を参照。

クラシック CoS (classic CoS) DN およびターゲットエントリの属性値の 1 つを使用して、テンプレートエントリを特定する。

クラス定義 (class definition) 特定のオブジェクトのインスタンスを作成するために必要な情報を指定し、ディレクトリ内のほかのオブジェクトに関連してそのオブジェクトがどのように動作するのかを決定する。

コードページ (code page) 国際化プラグインでロケールが使用する内部テーブル。オペレーティングシステムが、キーボードのキーを画面に表示するための文字フォントと関連付けるときに使用する。

更新履歴ログ (change log) 複製に対する変更を記述した記録。サプライヤサーバは、コンシューマサーバに格納されているレプリカに対して、またはマルチマスターのレプリカの場合はほかのマスターに対して、これらの変更を適用する。

国際化インデックス (international index) 多言語情報を含むディレクトリで、検索にかかる時間を短縮する。

国際標準化機構。(International Standards Organization) **consumer**「ISO」を参照。

コンシューマ (consumer) サプライヤサーバからレプリケートされたディレクトリツリーまたはサブツリーを含むサーバ。

コンシューマサーバ (consumer server) レプリケーション処理で、ほかのサーバからコピーしたレプリカを保持するサーバは、そのレプリカのコンシューマと呼ばれる。

コンシューマ主導レプリケーション処理 (consumer-initiated replication) コンシューマ (consumer) サーバがサプライヤサーバからディレクトリのデータを引き出すレプリケーション構成。

コンシューマレプリカ (consumer replica) すべての追加および変更操作についてマスターレプリカを参照するレプリカ。サーバは任意の数のコンシューマレプリカを保持できる。

サーバサービス (server service)　いったん実行されると、クライアントからの要求を待機して受け入れる Windows プラットフォーム上のプロセス。Windows NT 上の SMB サーバがこれに当たる。

サーバセレクタ (Server Selector)　ユーザがブラウザを使用してサーバを選択および設定できるインタフェース。

サーバデーモン (server daemon)　実行されると、クライアントからの要求を待機し、受け入れるプロセス。

サーバルート (server root)　サーバのプログラムと設定、管理、および情報ファイルの保持をするためのサーバマシン上のディレクトリ。

サービス (service)　Windows マシン上のバックグラウンドプロセスで、特定のシステムタスクを受け持つ。サービスプロセスは、動作を続けるためにユーザの介入を必要としない。

サービスクラス (class of service)　「CoS」を参照。

最下位のエントリ (leaf entry)　その下にほかのエントリが 1 つもないエントリ。最下位のエントリは、ディレクトリツリーで分岐点になることはできない。

サブエージェント (subagent)　「SNMP サブエージェント (SNMP subagent)」を参照。

サブ接尾辞 (sub suffix)　ルート接尾辞の下の分岐。

サプライヤ (supplier)　コンシューマサーバに複製されるディレクトリツリーあるいはサブツリーのマスターコピーを保持するサーバ。

サプライヤサーバ (supplier server)　レプリケーション処理で、別のサーバにコピーされるレプリカを保持するサーバは、そのレプリカのサプライヤと呼ばれる。

サプライヤ主導レプリケーション処理 (supplier-initiated replication)　サプライヤ (supplier) サーバがコンシューマサーバにディレクトリのデータをレプリケーションするレプリケーション構成。

サプライヤレプリカ (supplier replica)　ディレクトリ情報のマスターコピーを含む、更新可能な複製。サーバは任意の数のマスターレプリカを保持できる。

参照整合性 (referential integrity)　関連するエントリ間の関係が、ディレクトリ内で管理されることを保証するメカニズム。

識別名 (distinguished name)　エントリの名前と LDAP ディレクトリ内での位置を文字列で表したもの。

自己アクセス (self access)　この権限が与えられると、バインド DN がターゲットエントリとマッチしている場合は、ユーザは自分のエントリにアクセスできる。

時刻 / 日付の形式 (time / date format)　特定の地域における時刻および日付の習慣的な形式を示す。

システムインデックス (system index)　Directory Server の操作に必須なので削除および変更はできない。

実在インデックス (presence index)　特定のインデックス化された属性を含むエントリの検索を可能にする。

照合順序 (collation order)　ある言語の文字のソート方法について、言語および文化に固有の情報を提供する。この情報には、その文字体系における文字の順序、あるいはアクセント付きの文字とアクセントのない文字とを比較する方法などが含まれる。

証明書 (certificate)　ネットワークユーザの公開鍵を、ディレクトリ内にあるそれらの DN と関連付けるデータの集合。証明書は、ユーザオブジェクトの属性としてディレクトリ内部に格納される。

スーパーユーザ (superuser)　Unix マシン上でもっとも高いレベルの特権を持つユーザ。root とも呼ばれる。スーパーユーザは、マシン上のすべてのファイルに対して完全なアクセス権を持つ。

スキーマ (schema)　ディレクトリにどのようなタイプの情報をエントリとして格納できるかについての定義。スキーマとマッチしない情報がディレクトリに格納されている場合は、そのディレクトリにアクセスを試みているクライアントが正しい結果を表示できないことがある。

スキーマ検査 (schema checking)　ディレクトリ内で追加または変更されたエントリが、定義したスキーマに従っていることを確認する。スキーマ検査はデフォルトでオンになっている。したがって、スキーマに従っていないエントリを格納しようとした場合、エラーメッセージが表示される。

すべての ID のしきい値 (All IDs Threshold)　サーバが管理するすべてのインデックスキーに広域的に適用されるサイズ制限。個々の ID リストのサイズがこの制限値に達すると、サーバによってその ID リストがすべての ID のトークンと置き換えられる。

すべての ID のトークン (All IDs token)　すべてのディレクトリエントリがインデックスキーとマッチするサーバに想定させるメカニズム。実際には、すべての ID のトークンによって、サーバは検索要求で利用可能なインデックスが存在しないかのように動作する。

接尾辞 (suffix)　ディレクトリツリーの頂点にあるエントリの名前で、この下にデータが格納される。同じディレクトリ内に複数の接尾辞が存在できる。各データベースは接尾辞を 1 つだけ持つ。

操作属性 (operational attribute)　操作属性は、ディレクトリが変更およびサブツリーのプロパティを追跡するために内部で使用する情報を含む。明示的に要求しないかぎり、操作属性は検索に応答して返されることはない。

相対識別名 (Relative distinguished name) 「RDN」を参照。

属性 (attribute) エントリを説明する情報を保持する。属性にはラベルと値がある。また、各属性は、属性値として格納される情報のタイプに応じた標準の構文に従う。

属性リスト (attribute list) 特定のエントリタイプまたはオブジェクトクラスに対応する、必須の属性と省略可能な属性のリスト。

ターゲット (target) アクセス制御で、ターゲットは特定の ACI が適用されるディレクトリ情報を識別する。

ターゲットエントリ (target entry) CoS の適用範囲内のエントリ。

対称暗号化 (symmetric encryption) 暗号化と復号化の両方で同じキーを使用する暗号化。対称暗号化アルゴリズムの一例として DES が挙げられる。

単一マスター複製 (single-master replication) コンシューマサーバに対して 2 つのサーバがそれぞれ同じ読み書き可能な複製のコピーを保持する、もっとも基本的な複製モデル。単一マスター複製モデルでは、サプライヤサーバが更新履歴ログを管理する。

知識参照 (knowledge reference) さまざまな データベースに格納されているディレクトリ情報へのポインタ。

通貨形式 (monetary format) 特定の地域で使用されている通貨記号や、通貨記号が数値の前と後ろのどちらに付くのか、および通貨単位の表記方法を指定する。

データベースリンク (database link) 連鎖を実装したもの。データベースリンクはデータベースのように動作するが、持続的な記憶領域を持たない。代わりに、リモートに格納されているデータを指し示す。

データマスター (data master) 特定データ部分のマスターソースであるサーバ。

デーモン (daemon) 特定のシステムタスクを担当する、Unix マシン上のバックグラウンドプロセス。デーモンプロセスは、動作の継続に人の介入を必要としない。

定義エントリ (definition entry) 「CoS 定義エントリ (CoS definition entry)」を参照。

ディレクトリサービス (directory service) 組織内の人材および資源に関する記述的な属性ベースの情報を管理するように設計されたデータベースアプリケーション。

ディレクトリツリー (directory tree) ディレクトリに格納されている情報の論理表現。多くのファイルシステムで使用されているツリーモデルを反映しており、ツリーのルート点が階層の頂点にある。DIT とも呼ばれる。

ディレクトリマネージャ (Directory Manager) UNIX の root ユーザに相当する、特権を持ったデータベース管理者。ディレクトリマネージャにはアクセス制御が適用されない。

デフォルトインデックス (default index) データベースインスタンスごとに作成されるデフォルトインデックスセットの 1 つ。デフォルトインデックスは変更できるが、デフォルトインデックスに依存しているプラグインもあるので、削除する場合は注意が必要。

テンプレートエントリ (template entry) 「CoS テンプレートエントリ (CoS template entry)」を参照。

等価インデックス (equality index) 特定の属性値を含むエントリを効果的に検索できる。

匿名アクセス (anonymous access) この権限が与えられると、どのユーザも、資格の有無およびバインドの条件とは無関係に、ディレクトリ情報にアクセスできる。

トポロジ (topology) ディレクトリツリーが複数の物理的なサーバにわたって、どのように分割されているのか、およびこれらのサーバがどのように相互にリンクをしているのかを示す。

名前の衝突 (name collisions) 同じ識別名を持った複数のエントリ。

認証 (authentication) (1) クライアントユーザの ID を Directory Server に対して示すプロセス。ユーザがディレクトリへのアクセスを許可されるには、バインド DN、および対応するパスワードまたは証明書のどちらかを提示する必要がある。ディレクトリ管理者がユーザに許可したアクセス権に基づき、Directory Server はユーザに機能の実行やファイルおよびディレクトリへのアクセスを許可する。

(2) ほかのコンピュータがそのサーバであるかのように偽装したり、あるいはセキュリティ保護されていないコンピュータにもかかわらず保護されているように装うことを防ぎ、クライアント (client) がセキュリティ保護されたサーバに接続されていることを保証する。

認証局 (Certificate Authority) 認証証明書を販売および発行する会社または組織。ユーザは、信頼する認証局から認証証明書を購入できる。CA とも呼ばれる。

認証証明書 (authentication certificate) 置き換えや偽造の不可能な、第三者が発行するデジタルファイル。認証証明書は、他方を検証し認証するために、サーバからクライアントへ、あるいはクライアントからサーバへ送信される。

ネストされたロール (nested role) ほかのロールを含むロールの作成が可能。

ネットワーク管理アプリケーション (network management application) 稼働または停止しているデバイス、受信したエラーメッセージやその数など、SNMP 管理対象のデバイスに関する情報をグラフィカルで表示する Network Management Station コンポーネント。

バインド DN (bind DN) 操作を実行するときに、Directory Server に対する認証で使用される識別名。

バインド規則 (bind rule) アクセス制御で、ディレクトリ情報にアクセスするために特定のユーザまたはクライアントが満たす必要がある資格および条件を指定する。

バインド識別名 (bind distinguished name) 「バインド DN (bind DN)」を参照。

パススルーサブツリー (pass-through subtree) パススルー認証では、PTA Directory Server は、このサブツリーに DN が含まれているすべてのクライアントからのバインド要求を Authenticating Directory Server に渡す (パススルー)。

パススルー認証 (Pass-through authentication) 「PTA」を参照。

パスワードファイル (password file) Unix ユーザのログイン名、パスワード、およびユーザ ID 番号が格納されている Unix マシン上のファイル。格納場所から、`/etc/passwd` とも呼ばれる。

パスワードポリシー (password policy) ディレクトリ内でのパスワードの使い方の基準となる規則のセット。

ハブサプライヤ (hub supplier) レプリケーション処理で、ほかのサーバからコピーされたレプリカを保持するサーバのことで、このレプリカを第三のサーバにレプリケーションする。「カスケード型複製」も参照。

汎用アクセス (general access) この権限が与えられた場合、認証されたすべてのユーザがディレクトリの情報にアクセスできることを示す。

標準インデックス (standard index) デフォルトで維持されるインデックス。

ファイル拡張子 (file extension) ファイル名のドット (.) より後ろの部分で、通常ファイルタイプを定義する。たとえば、.GIF、.HTML など。`index.html` というファイル名の場合、ファイル拡張子は `html` である。

ファイルタイプ (file type) 特定のファイルの形式。たとえば、グラフィックファイルは GIF 形式で格納される場合が多く、テキストファイルは通常 ASCII テキスト形式で格納される。ファイルタイプは、通常ファイル拡張子 (.GIF、.HTML など) で識別される。

フィルタ (filter) ディレクトリの照会に適用される制約で、返される情報を制限する。

フィルタを適用したロール (filtered role) 各エントリに含まれる属性に応じて、エントリをロールに割り当てることができるようにする。この操作を行うには、LDAP フィルタを指定する必要がある。フィルタにマッチするエントリは、そのロールを所有すると言われる。

部分文字列インデックス (substring index) エントリ内の部分文字列の効率的な検索を可能にする。部分文字列インデックスとして、各エントリの 2 文字以上を指定する必要がある。

ブラウザ (browser) HTML ファイルとして格納されている World Wide Web コンテンツを要求および表示する、Netscape Navigator などのソフトウェア。ブラウザは、ホストサーバとの通信に HTTP プロトコルを使用する。

ブラウズインデックス (browsing index)　仮想表示インデックスとも呼ばれる。Directory Server Console でエントリの表示を高速化する。ディレクトリの性能を向上させるために、ディレクトリツリーのすべての分岐点で作成可能。

プロキシ DN (proxy DN)　プロキシ認証で使用される。プロキシ DN とは、クライアントアプリケーションが操作を実行しようとしている対象へのアクセス権を持つエントリの DN。

プロキシ認証 (proxy authorization)　特殊な形式の認証で、ユーザは自分の ID でディレクトリにバインドするが、別のユーザのアクセス権限を付与される。その別のユーザのことをプロキシユーザ、その DN をプロキシ DN と呼ぶ。

プロトコル (protocol)　ネットワーク上のデバイスが情報を交換する方法を記述した規則のセット。

分岐エントリ (branch entry)　ディレクトリ内でサブツリーの頂点を表すエントリ。

ベース DN (base DN)　ベース識別名。検索処理はベース DN に対して行われる。ベース DN とは、ディレクトリツリー内でエントリおよびその下にあるすべてのエントリの DN のこと。

ベース識別名 (base distinguished name)　「ベース DN (base DN)」を参照。

ポインタ CoS (pointer CoS)　ポインタ CoS は、テンプレート DN だけを使用してテンプレートエントリを識別する。

ホスト名 (hostname)　machine.domain.dom のような書式のマシン名で、IP アドレスに変換される。たとえば、`www.iPlanet.com` は、com ドメインの iPlanet サブドメインにある www というマシンである。

マスターエージェント (master agent)　「SNMP マスターエージェント (SNMP master agent)」を参照。

マッチング規則 (matching rule)　検索処理中にサーバが文字列をどのように比較するかを定めるガイドライン。多言語検索では、サーバが使用する必要がある照合順序および演算子をマッチング規則で規定する。

マッピングツリー (mapping tree)　接尾辞 (サブツリー) の名前をデータベースと関連付けるデータ構造。

マルチプレクサ (multiplexor)　データベースリンクを含むサーバで、リモートサーバと通信する。

マルチマスターレプリカ (multi-master replication)　2 つのサーバがそれぞれ同じ読み書き可能なレプリカのコピーを保持する高度なレプリケーションモデル。各サーバは、レプリカの更新履歴ログを保持する。一方のサーバに対する変更は、自動的にもう一方のサーバにもレプリケーションされる。変更が競合した場合、タイムスタンプを使用してどちらのサーバが最新の変更を保持しているかを決定する。

文字タイプ (character type)　英字を数字やほかの文字と識別し、また大文字と小文字のマッピングを識別する。

ルート接尾辞 (root suffix)　1 つ以上のサブ接尾辞の親。ディレクトリツリーは複数のルート接尾辞を含むことができる。

レフェラル (referral)　(1) サーバが自身では処理できない検索要求あるいは更新要求を LDAP クライアントから受信すると、サーバは通常、その要求を処理できる LDAP サーバへのポインタをクライアントに返信する。

(2) レプリケーション処理では、コンシューマレプリケーションが更新要求を受信すると、対応するマスターレプリカを保持するサーバにこの要求を転送する。この転送プロセスをレフェラルと呼ぶ。

レプリカ (replica)　複製に関与するデータベース。「コンシューマレプリカ (consumer replica)」および「サプライヤレプリカ (supplier replica)」も参照。

レプリケーションアグリーメント (replication agreement)　サプライヤサーバに格納されている設定パラメタのセット。複製対象のデータベース、データをプッシュする先のコンシューマサーバ、複製を実行できる時間、コンシューマにバインドするためにサプライヤが使用する DN と資格、および接続をセキュリティ保護する方法を特定する。

レプリケーション処理 (replication)　ディレクトリツリーまたはサブツリーをサプライヤサーバからコンシューマサーバにコピーする処理。

連鎖 (chaining)　要求をほかのサーバに中継するための手法。要求の結果は収集、コンパイルされてから、クライアントに返される。

ロール (role)　エントリをグループ化するメカニズム。各ロールは、そのロールを所有するエントリであるメンバーを持つ。

ロールに基づく属性 (role-based attributes)　関連付けられた CoS テンプレート内にエントリが特定のロールを所有しているため、エントリに記述される属性。

ロケール (locale)　住む地域や、文化、習慣の異なるユーザが、データを表すために使用するもので、照合順序、文字タイプ、通貨形式、時刻 / 日付の形式を識別する。ロケールには、特定言語のデータの解釈方法、格納方法、または照合方法に関する情報が含まれる。また、特定言語を表現するために使用するコードページを提供する。

索引

か

こ

さ

し

す

せ

て

に