Oracle® Solaris 11.1 でのネームサービスおよびディレクトリサービスの作業

Part No: E36689–02
2012 年 10 月

ORACLE

121210@25097

目次

表目次

例目次

はじめに

『Oracle Solaris 11.1 でのネームサービスおよびディレクトリサービスの作業』では、Oracle Solaris オペレーティングシステム (OS) ネームサービスとディレクトリサービス DNS、NIS、および LDAP の設定と管理について説明します。このガイドは、Oracle Solaris 管理情報の大部分について説明している複数巻から成るドキュメントセットの一部です。

注 – この Oracle Solaris のリリースでは、SPARC および x86 系列のプロセッサアーキテクチャーを使用するシステムをサポートしています。サポートされるシステムは、Oracle Solaris OS: Hardware Compatibility Lists に記載されています。このドキュメントでは、プラットフォームにより実装が異なる場合は、それを特記します。

関連ドキュメント

- Oracle Directory Server Enterprise Edition の配備ガイド
- 『Oracle Directory Server Enterprise Edition 管理ガイド』
- 『DNS & BIND』、Cricket Liu および Paul Albitz 著、(第 5 版、オライリー・ジャパン、2008 年)
- 『Understanding and Deploying LDAP Directory Services』、Timothy A. Howes, Ph.D. および Mark C. Smith 著

Oracle サポートへのアクセス

Oracle のお客様は、My Oracle Support を通じて電子的なサポートを利用することができます。詳細は、`http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` を参照してください。聴覚に障害をお持ちの場合は、`http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` を参照してください。

表記上の規則

次の表では、このドキュメントで使用される表記上の規則について説明します。

表 P–1 表記上の規則

字体	説明	例
`AaBbCc123`	コマンド名、ファイル名、ディレクトリ名、画面上のコンピュータ出力、コード例を示します。	`.login` ファイルを編集します。 `ls -a` を使用してすべてのファイルを表示します。 `machine_name% you have mail.`
`AaBbCc123`	ユーザーが入力する文字を、画面上のコンピュータ出力と区別して示します。	`machine_name%` **`su`** `Password:`
aabbcc123	プレースホルダ: 実際に使用する特定の名前または値で置き換えます。	ファイルを削除するには、 `rm` *filename* と入力します。
AaBbCc123	書名、新しい単語、および強調する単語を示します。	『ユーザーズガイド』の第 6 章を参照してください。 キャッシュは、ローカルに格納されるコピーです。 ファイルを保存しないでください。 注: いくつかの強調された項目は、オンラインでは太字で表示されます。

コマンド例のシェルプロンプト

Oracle Solaris OS に含まれるシェルで使用する、UNIX のシステムプロンプトとスーパーユーザープロンプトを次に示します。コマンドの例では、シェルプロンプトは、そのコマンドを通常のユーザーまたは特権を持つユーザーのどちらが実行するべきかを示します。

表 P–2 シェルプロンプト

シェル	プロンプト
Bash シェル、Korn シェル、および Bourne シェル	$
Bash シェル、Korn シェル、および Bourne シェルのスーパーユーザー	#

表 P–2 シェルプロンプト (続き)

シェル	プロンプト
C シェル	machine_name%
C シェルのスーパーユーザー	machine_name#

パート I

ネームサービスとディレクトリサービスについて

ここでは、Oracle Solaris OS のネームサービスとディレクトリサービスの概要について説明します。また、異なるローカルおよびリモートディレクトリサービスを使用して検索を調整できるように、サービス管理機能 (SMF) を使用してネームサービスを構成する方法についても説明します。また、ドメインネームサービス (DNS) や Active Directory クライアントを構成する方法についても説明します。

◆ ◆ ◆ 第 1 章

ネームサービスとディレクトリサービス (概要)

この章では、Oracle Solaris リリースに含まれているネームサービスとディレクトリサービスの概要について説明します。また、DNS、NIS、および LDAP ネームサービスについても簡単に説明します。

この章の内容は次のとおりです。

ネームサービスとは

ネームサービスは、次のような、格納されている情報の検索を実行します。

- ホスト名とアドレス
- ユーザー名
- パスワード
- アクセス権
- グループメンバーシップ、自動マウントのマップ、その他

これらの情報はユーザーに使用可能になるため、ユーザーは各自のホストにログインし、リソースにアクセスして、アクセス許可を取得することができます。ネームサービス情報は、各種の形式のデータベースファイルにローカルに格納することも、中央のネットワークベースのリポジトリまたはデータベースに格納することもできます。

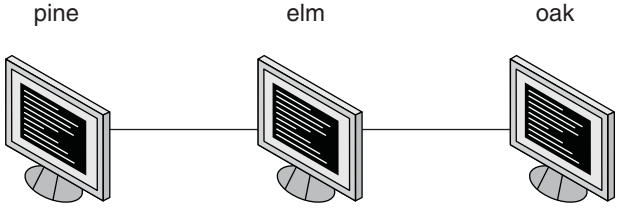
中央のネームサービスが存在しない場合、各ホストは、これらの情報の独自のコピーを保持する必要があります。ネームサービス情報はファイルまたは
マップ、データベーステーブルの形で格納できます。すべてのデータを 1 カ所で管理すれば、管理がより簡単になります。

ネームサービスは、どのようなコンピュータネットワークにも欠かせないものです。ネームサービスは、数ある機能のなかでも特に、次のことを行う機能を提供します。

- 名前とオブジェクトを対応付ける (「バインド」する)
- オブジェクトの名前を解決する
- バインドを解除する
- 名前を一覧表示する
- 情報の名前を変更する

ネットワーク情報サービスを使用すると、システムを数値アドレスではなく、共通名で識別できます。これにより、ユーザーは `192.168.0.0` のような扱いにくい数値アドレスを記憶して入力する必要がなくなるため、通信が簡単になります。

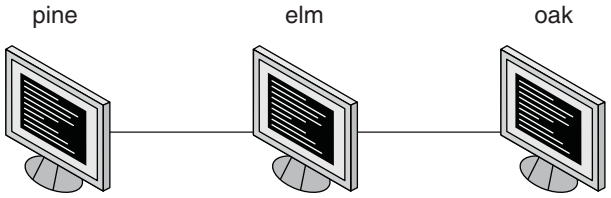
たとえば、`pine`、`elm`、`oak` という名前の 3 つのシステムで構成されるネットワークを考えてみます。`pine` が `elm` または `oak` にメッセージを送信するには、その前に `pine` がそれらの数値ネットワークアドレスを知っている必要があります。この理由から、`pine` は、ネットワーク内の (自身を含む) すべてのシステムのネットワークアドレスを格納するファイル `/etc/inet/hosts` を保持します。



`/etc/inet/hosts`

```
10.0.3.1 pine
10.0.3.2 elm
10.0.3.3 oak
```

同様に、`elm` と `oak` が `pine` と通信したり、互いに通信したりするには、これらのシステムが同様のファイルを保持する必要があります。



/etc/inet/hosts
10.0.3.1 pine
10.0.3.2 elm
10.0.3.3 oak

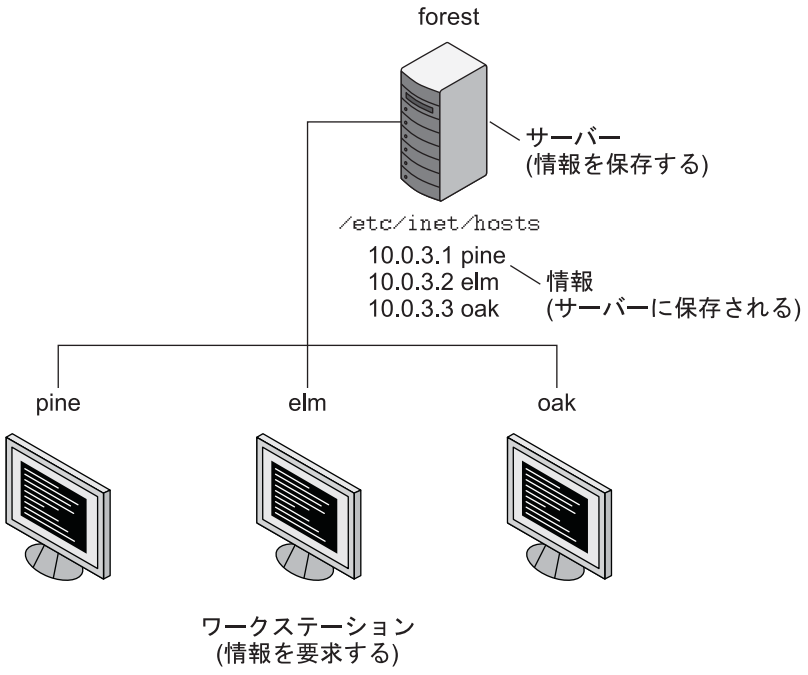
/etc/inet/hosts
10.0.3.1 pine
10.0.3.2 elm
10.0.3.3 oak

/etc/inet/hosts
10.0.3.1 pine
10.0.3.2 elm
10.0.3.3 oak

アドレスの格納に加えて、システムは、セキュリティー情報、メールデータ、ネットワークサービスの情報なども格納します。ネットワークによって提供されるサービスが増えるにつれて、格納する情報の種類も増えていきます。その結果、各システムが、`/etc/inet/hosts` のようなファイルのセット全体を保持する可能性があります。

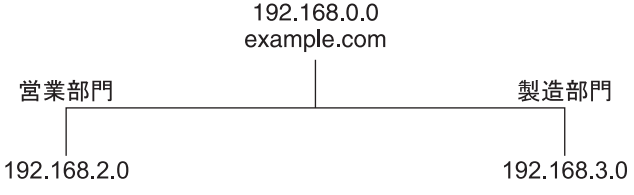
ネットワーク情報サービスは、どのシステムからでも照会できるサーバー上にネットワーク情報を格納します。

これらのシステムは、サーバーのクライアントと呼ばれます。次の図に、クライアントとサーバーの関係を示します。ネットワークについての情報が変更されるたびに、各クライアントのローカルファイルを変更する代わりに、管理者はネットワーク情報サービスが格納する情報だけを更新します。これによって、エラー、クライアント間の不一致、そしてタスク量を減らすことができます。

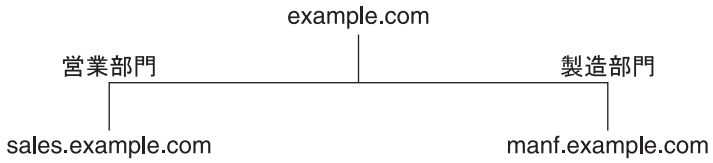


サーバーがネットワーク全体のクライアントに集中管理のサービスを提供しているこの配置は、クライアントサーバーコンピューティングと呼ばれます。

ネットワーク情報サービスの第一の目的は情報の一元管理ですが、もう 1 つの目的はネットワーク名の簡素化です。たとえば、ある会社がネットワークを設定して、インターネットに接続したと仮定します。インターネットはこのネットワークに、ネットワークアドレス `192.168.0.0` とドメイン名 `example.com` を割り当てました。会社には営業 (Sales) と製造 (Manf) という 2 つの部門があるため、このネットワークは 1 つのメインネットワークと、部門ごとに 1 つのサブネットに分割されています。各ネットには独自のアドレスがあります。



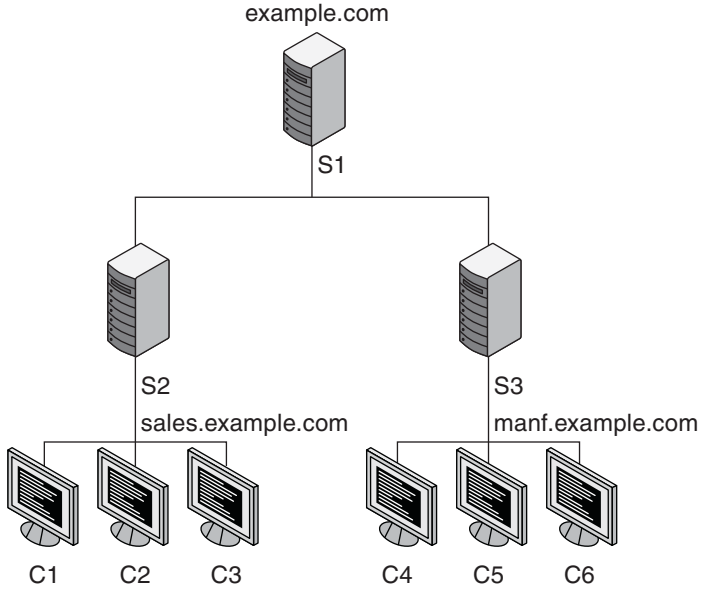
上に示すように、各部はネットワークアドレスで識別することもできますが、ネームサービスによって使用可能となる説明的な名前の方が便利です。



メールやその他のネットワーク通信を 198.168.0.0 にアドレス指定する代わりに、メールの宛先を example.com にすることができます。メールを 192.168.2.0 または 192.168.3.0 にアドレス指定する代わりに、メールの宛先を sales.example.com または manf.example.com にすることができます。

名前はまた、物理アドレスよりもはるかに柔軟です。物理的なネットワークはめったに変更されませんが、企業の組織はよく変化します。

たとえば、example.com ネットワークが 3 台のサーバー S1、S2、および S3 によってサポートされているとします。それらのサーバーのうちの 2 台 S2 と S3 がクライアントをサポートしているとします。



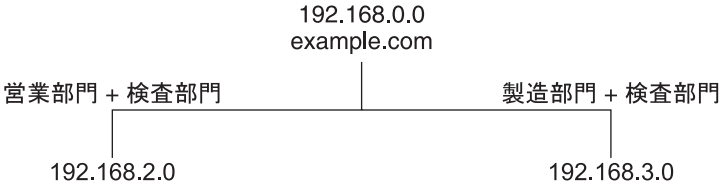
クライアント C1、C2、および C3 は、サーバー S2 からネットワーク情報を取得します。クライアント C4、C5、および C6 は、サーバー S3 から情報を取得します。結果と

して構成されるネットワークの概要を、次の表に示します。表は、前記のネットワークを一般化して表現したもので、実際のネットワーク情報マップとは異なります。

表 1–1　example.com ネットワークの表現

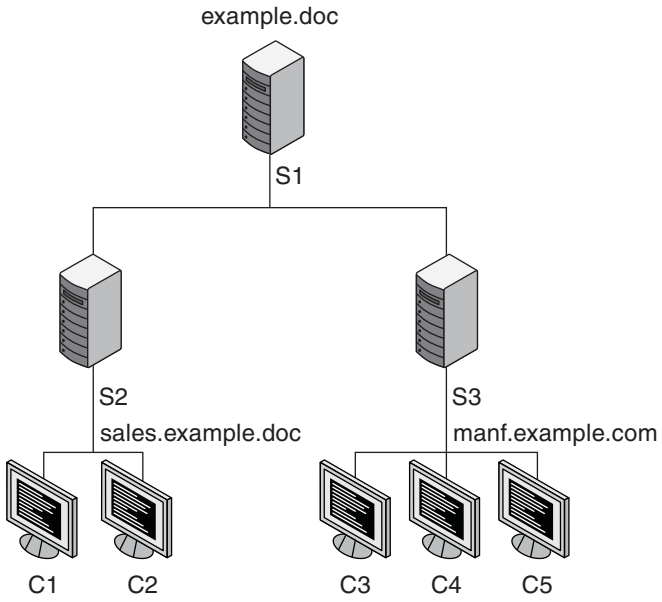
ネットワークアドレス	ネットワーク名	サーバー	クライアント
192.168.1.0	example.com	S1	
192.168.2.0	sales.example.com	S2	C1、C2、C3
192.168.3.0	manf.example.com	S3	C4、C5、C6

2 つの部門からある人数の人材を借りて第 3 の検査部門を新設し、第 3 のサブネットは開設しなかったとします。その結果、物理ネットワークは、企業の組織とは対応しなくなります。



検査部門のトラフィックには独自のサブネットはなく、代わりに 192.168.2.0 と 192.168.3.0 の間で分割されます。ここで、ネットワーク情報サービスを使用することにより、検査部門のトラフィックにも専用のネットワークを備えることができます。

このように、組織が変更された場合、そのネットワーク情報サービスでは次に示すようにマッピングを変更できます。



現在、クライアント C1 と C2 は、サーバー S2 から情報を取得します。C3、C4、および C5 は、サーバー S3 から情報を取得します。

組織内でそのあとに行われる変更に対しては、ハードウェアのネットワーク構造を再編成することなく、ネットワーク情報構造を変更することにより対応できます。

Oracle Solaris のネームサービス

Oracle Solaris プラットフォームは、次のネームサービスを提供します。

- ドメインネームシステム (DNS) (30 ページの「DNS ネームサービスの説明」を参照)
- 初期の UNIX ネームシステムである /etc ファイル (30 ページの「/etc ファイルネームサービスの説明」を参照)
- ネットワーク情報サービス (NIS) (31 ページの「NIS ネームサービスの説明」を参照)
- Lightweight Directory Access Protocol (LDAP) (パート III「LDAP ネームサービス」の「LDAP ネームサービスの設定と管理」を参照)

最新のほとんどのネットワークは、これらのサービスの 2 つ以上を組み合わせて使用します。特定の検索に対してどのネームサービスが使用されるかは、第 2 章「ネームサービススイッチ (概要)」で説明されているネームサービススイッチによって調整されます。

DNS ネームサービスの説明

ドメインネームシステム (DNS) は、TCP/IP ネットワーク上に実装された、階層的な分散型データベースです。これは主に、インターネットホスト名に対する IP アドレス、および IP アドレスに対するホスト名を検索するために使用されます。これらのデータはネットワーク全体にわたって分散しており、右から左に読み取られる、ピリオドで区切られた名前を使用して検索されます。DNS はまた、メール交換のルーティング情報、場所のデータ、使用可能なサービスなどの、その他のインターネット関連のホスト情報を格納するためにも使用されます。このサービスの階層的な性質により、ローカルドメインのローカルでの管理が可能になるだけでなく、インターネット、イントラネット、またはその両方に接続されたほかのドメインに国際的に対処できるようになります。

DNS クライアントは、ホスト名に関する情報を 1 つまたは複数のネームサーバーにリクエストし、その応答を待ちます。DNS サーバーは、DNS マスター上のファイルまたはサードパーティー製データベースから読み込まれた情報キャッシュから、または連携する DNS スレーブサーバーからネットワーク経由で、あるいは以前のクエリーから格納された情報からリクエストに応答します。応答が見つからず、そのサーバーが問題のドメインを担当していない場合、このサービスは、応答を返すほかのサーバーやキャッシュにホスト名を再帰的にリクエストします (この動作が許可されている場合)。

マルチキャスト DNS およびサービス検出の説明

DNS プロトコルに対する 2 つの拡張機能が、`svc:network/dns/multicast` サービスによって管理されています。マルチキャスト DNS (mDNS) では、従来の DNS サーバーがインストールされていなかった小規模なネットワーク内に DNS が実装されます。また、DNS サービス検出 (DNS-SD) によって、マルチキャスト DNS が単純なサービス検出 (ネットワークブラウジング) を提供するように拡張されます。詳細は、43 ページの「マルチキャスト DNS」および 44 ページの「マルチキャスト DNS サービス検出」を参照してください。

注意 – mDNS サービスは `.local` のドメイン名を使用するため、競合の可能性を避けるために、その名前は DNS で使用しないでください。

/etc ファイルネームサービスの説明

ホストベースの初期の UNIX ネームシステムは、スタンドアロンの UNIX マシン用に開発されたあと、ネットワークで使用するように適応されました。多くの古い UNIX オペレーティングシステムやマシンは引き続き、ローカルファイルのみを使用してすべてのネームデータを管理しています。ただし、ローカルファイルによるホスト、ユーザー、その他のネームデータの管理は、大規模で複雑なネットワークには

適していません。各 /etc ファイルは、それぞれの関連するマニュアルページで説明されています。たとえば、/etc/inet/hosts ファイルは、hosts(4) のマニュアルページで説明されています。

NIS ネームサービスの説明

ネットワーク情報サービス (NIS) は、DNS とは独立して開発されました。DNS が数値 IP アドレスの代わりにマシン名を使うことによって、通信を簡略化することに焦点を当てているのに対して、NIS は、多様なネットワーク情報を集中管理することによりネットワーク管理機能を高めることに焦点を当てています。NIS には、ネットワーク、マシンの名前とアドレス、ユーザー、およびネットワークサービスに関する情報も格納されます。このようなネットワーク情報の集まりを「NIS の名前空間」と呼びます。

NIS 名前空間情報は NIS マップに格納されています。NIS マップは、UNIX の /etc ファイルおよびほかの構成ファイルを置換するように設計されているので、名前やアドレスよりはるかに多くの情報を保存できます。その結果、NIS 名前空間には非常に大きなマップの集合が含まれることになります。詳細については、104 ページの「NIS マップに関する作業」を参照してください。

NIS は DNS に似たクライアントサーバーの配列を持っています。複製の NIS サーバーは NIS クライアントへサービスを提供します。主体サーバーはマスターサーバーと呼ばれ、信頼性のために、これらのサーバーにはバックアップ (または、スレーブ) サーバーが割り当てられます。どちらのサーバーも NIS 検索ソフトウェアを使用し、NIS マップを格納します。NIS アーキテクチャーおよび NIS の管理についての詳細は、第 6 章「NIS の設定と構成 (タスク)」および第 7 章「NIS の管理 (タスク)」を参照してください。

LDAP ネームサービスの説明

Lightweight Directory Access Protocol (LDAP) は、ディレクトリサーバーにアクセスして分散型ネームサービスやその他のディレクトリサービスを使用するために使用される、セキュアなネットワークプロトコルです。この標準ベースのプロトコルは、階層的なデータベース構造をサポートしています。同じプロトコルを使用して、UNIX とマルチプラットフォームの両方の環境でネームサービスを提供できます。

Oracle Solaris OS は、Oracle Directory Server Enterprise Edition (以前の名称は SunJavaSystem Directory Server) やその他の LDAP ディレクトリサーバーと組み合わせて LDAP をサポートしています。

LDAP ネームサービスについては、第 9 章「LDAP ネームサービスの紹介 (概要)」を参照してください。

NIS から LDAP への移行については、第 15 章「NIS から LDAP への移行 (タスク)」を参照してください。

シングルサインオンや、Kerberos 認証サービスの設定および保守については、『Oracle Solaris 11.1 の管理: セキュリティーサービス』のパート VI「Kerberos サービス」を参照してください。

ネームサービススイッチの説明

ネームサービススイッチは、クライアントがネーミング情報を取得するために DNS、LDAP、NIS、またはローカルファイルのデータソースを検索できるようにするためのメカニズムです。このスイッチは、`svc:/system/name-service/switch` サービスによって管理されます。詳細は、第 2 章「ネームサービススイッチ (概要)」を参照してください。

ネームサービスの比較一覧

	DNS	NIS	LDAP	ファイル
名前空間	階層	一層	階層	ファイル
データストレージ	ファイル/リソースレコード	2 列のマップ	ディレクトリ (可変) インデックス化したデータベース	テキストベースのファイル
サーバー	マスター/スレーブ	マスター/スレーブ	マスター/複製 複数マスター複製	なし
セキュリティー	DNSSEC (可変)	なし (root またはなし)	Kerberos、 TLS、 SSL (可変)	なし
トランスポート	TCP/IP	RPC	TCP/IP	ファイル入出力
規模	グローバル	LAN	グローバル	ローカルホストのみ
データ	ホスト	すべて	すべて	すべて

注 – DNS は、LDAP やファイルベースのネーミングに対するホストまたはネットワークアドレス検索に推奨されるサービスです。

◆ ◆ ◆ 第 2 章

2 ネームサービススイッチ (概要)

この章では、ネームサービススイッチについて説明します。ネームサービススイッチは、異なるネームサービスの使用方法を調整するために使います。この章の内容は次のとおりです。

ネームサービススイッチについて

ネームサービススイッチは、管理者がネットワーク情報のタイプごとに、どのネーム情報サービスまたはソースを使用するかを指定できるようにする、構成可能な選択サービスです。これらのサービスは、データベースと呼ばれます。ネームサービススイッチは、次のような `getXbyY()` インタフェースのいずれかを呼び出すクライアントアプリケーションによって使用されます。

- `gethostbyname()`
- `getpwuid()`
- `getpwnam()`
- `getaddrinfo()`

各システムは、SMF リポジトリ内に独自の構成を持っています。ネームサービススイッチで定義された各プロパティーによって、ホスト、パスワード、グループなどの特定のデータベースが識別されます。各プロパティーに割り当てられた値によって、情報をリクエストする先の 1 つまたは複数のソースが一覧表示されます。これらの値にガイダンスまたはオプションが含まれる場合もあります。このガイダンスには、サービスで試みるべき再試行の回数、適用するタイムアウトの種類、サービスが失敗した場合の処理などが含まれている可能性があります。

ネームサービススイッチのデータベースとソース

ネームサービススイッチでは、次のデータベースがサポートされています。

表 2–1 ネームサービススイッチのデータベース

情報データベース	説明
alias	電子メールアドレスと別名を一覧表示します。
auth_attr	承認名と説明を一覧表示します。
automount	ローカルにマウントできるリモートファイルシステムに関する情報を一覧表示します。
bootparam	ディスクレスクライアントのブート情報を一覧表示します。
ether	Ethernet アドレスおよび一致するホスト名を一覧表示します。
group	ファイルへのアクセスを共有するために使用できるグループに関する情報を一覧表示します。
host	IP アドレスおよび一致するホスト名を一覧表示します。
netgroup	共有 NFS ファイルシステムの情報を一覧表示します。
netmask	IP サブネットを実装するために使用されるネットワークマスクを一覧表示します。
network	ネットワークごとの名前と番号を一覧表示します。
password	ユーザーアカウント情報を一覧表示します。
prof_attr	実行プロファイルの名前、説明、およびその他の属性を一覧表示します。
project	プロジェクト名、一意の識別子、および関連付けられたリソース割り当てを一覧表示します。
protocol	インターネットプロトコルの名前、番号、および別名 (存在する場合) を一覧表示します。
publickey	公開鍵情報を一覧表示します。
rpc	RPC プログラムの名前と番号を一覧表示します。
service	インターネットサービスの名前、ポート、およびプロトコルを一覧表示します。
tnrhdb	Oracle Solaris の Trusted Extensions 機能を使用しているホストのセキュリティー属性を一覧表示します。
tnrhtp	Trusted Extensions によって使用されるテンプレートを一覧表示します。

さらに、ネームサービススイッチ内の default プロパティーによって、ほかでは定義されないすべてのデータベースのソース文字列が定義されます。ネットワークでほとんどのデータベースに同じソースを使用している場合は、default プロパティーを変更し、データベースごとのプロパティーを定義しないようにすることができます。手順については、40 ページの「すべてのネームデータベースのソースを変更する方法」を参照してください。

以前のリリースをサポートするには、enable_passwd_compat および enable_group_compat プロパティーを true に設定すると、パスワードやグループ情報のための compat モードを有効にすることができます。このモードでは、適切なデータベースでの旧形式の「+」または「-」構文に対するサポートが提供されます。現在のリリースでは、この機能は pam_list モジュールによって置き換えられています。

次の表では、上に示されているデータベースのネームサービススイッチで一覧表示できるソースのタイプについて説明します。

表 2–2 ネームサービススイッチの情報ソース

情報ソース	説明
ad	Active Directory サーバー上に格納されているデータベースを識別します。
compat	パスワードやグループ情報に compat を使用すると、/etc/passwd、/etc/shadow、および /etc/group ファイルで旧形式の「+」または「-」構文をサポートできます。この機能は、pam_list モジュールによって置き換えられています。
dns	ホスト情報を DNS から取得するように指定します。
files	クライアントの /etc ディレクトリ内に格納されているファイルを指定します (たとえば、/etc/passwd)。
ldap	エントリを LDAP ディレクトリから取得するように指定します。
mdns	マルチキャスト DNS (mDNS) を使用してホスト情報を指定します。
nis	NIS マップを指定します (たとえば、hosts マップ)。

ネームサービススイッチの検索条件

次の検索条件形式を使用すると、1 つまたは複数の情報ソースを選択したり、ソースが使用される順序を指定したりすることができます。

- 単一ソース — 情報タイプに 1 つのソースのみが含まれている場合 (`files` など)、スイッチを使用する検索ルーチンは、そのソース内の情報のみを検索します。情報が見つかった場合、「`success`」というステータスメッセージが返されます。情報が見つからない場合は、検索が停止され、「success」以外のステータスメッセージが返されます。ステータスメッセージに基づいて何をするかは、ルーチンによって異なります。
- 複数ソース — データベースに特定の情報タイプの複数のソースが含まれている場合、スイッチは検索ルーチンに、最初に一覧表示されているソース内を検索するよう指示します。情報が見つかった場合、「`success`」というステータスメッセージが返されます。最初のソースで情報が見つからない場合は、次のソースが検索されます。このルーチンは、情報を見つけるか、または `return` 指定によって停止されるまで、すべてのソースを検索します。必要な情報がどのソースにもなかったとき、ルーチンは検索を停止し、`non-success` というステータスメッセージを返します。

Oracle Solaris 11 リリース のデフォルトでは、最初のソースは `files` です。この構成によって、一覧表示されている次のソースが使用できない場合でもシステムのハングアップが回避されます。

ネームサービススイッチのステータスメッセージ

ルーチンが情報を見つけた場合、そのルーチンは `success` ステータスメッセージを返します。探している情報が見つからない場合は、3 種類のエラーステータスメッセージのいずれかが返されます。表示されるステータスメッセージを次の表に示します。

表 2–3 ネームサービススイッチのステータスメッセージ

ステータスメッセージ	説明
`SUCCESS`	要求されたエントリがソース内で発見された。
`UNAVAIL`	ソースが応答しない、または使用不可。つまり、どのデータベースソースも見つからなかったか、またはアクセスできませんでした。
`NOTFOUND`	ソースが「エントリなし」と応答した。つまり、データベースにはアクセスしましたが、必要な情報が見つかりませんでした。
`TRYAGAIN`	ソースはビジー状態にあり、次回は応答する可能性があります。つまり、データベースは見つかりましたが、クエリーに応答できませんでした。

ネームサービススイッチのスイッチアクションオプション

ネームサービススイッチに、次の表に示す 2 つのアクションのいずれかでステータスメッセージに応答するよう指示できます。

表 2–4 ネームサービススイッチからステータスメッセージへの応答

アクション	説明
return	情報の検索を停止します。
continue	次のソースの検索を試みます。

さらに、TRYAGAIN ステータスメッセージについては、次のアクションを定義できます。

- forever – 現在のソースを無期限に再試行します。
- *n* – 現在のソースをさらに *n* 回再試行します。

ネームサービススイッチのデフォルトの検索条件

ネームサービススイッチのステータスメッセージとアクションオプションの組み合わせによって、検索ルーチンが各ステップで何を実行するかが決定されます。ステータスメッセージとアクションオプションの組み合わせによって、検索条件が構成されます。

スイッチのデフォルトの検索条件は、どのソースでも同じです。この一覧には、いくつかの検索条件の説明が含まれています。

- SUCCESS=return。情報の検索を停止します。見つかった情報を使用して処理を続行します。
- UNAVAIL=continue。次のネームサービススイッチソースに移動し、検索を続行します。次のソースがなければ、「NOTFOUND」というステータスを返します。
- NOTFOUND=continue。次のネームサービススイッチソースに移動し、検索を続行します。次のソースがなければ、「NOTFOUND」というステータスを返します。
- TRYAGAIN=continue。次のネームサービススイッチソースに移動し、検索を続行します。次のソースがなければ、「NOTFOUND」というステータスを返します。

デフォルトの検索条件は、前の一覧に示されている *STATUS=action* 構文を使用して、ほかの何らかの条件を明示的に指定することによって変更できます。たとえば、NOTFOUND 状態に対するデフォルトのアクションは、次のソースに検索を続行することです。ネットワークデータベースの検索条件が次のように報告される可能性があります。

```
svc:/system/name-service/switch> listprop config/network
config/network  astring             "nis [NOTFOUND=return] files"
```

networks: nis [NOTFOUND=return] files エントリは、NOTFOUND ステータスに対するデフォルト以外の条件を指定します。デフォルト以外の条件は角括弧で区切られます。

この例では、検索ルーチンは次のような働きをします。

- network データベースが使用可能であり、必要な情報を含んでいる場合、このルーチンは SUCCESS ステータスメッセージを返します。
- network データベースが使用可能でない場合、このルーチンは UNAVAIL ステータスメッセージを返します。デフォルトでは、このルーチンは次に一覧表示されている条件を使用して、引き続き検索を実行します。
- network データベースが使用可能であり、見つかったが、そのデータベースに必要な情報が含まれていない場合、このルーチンは NOTFOUND メッセージを返します。ただし、引き続き次のソースを検索するのではなく (これがデフォルトの動作です)、このルーチンは検索を停止します。
- network データベースがビジー状態にある場合、このルーチンは TRYAGAIN ステータスメッセージを返し、デフォルトでは引き続き network データベースを検索します。

注 – ネームサービススイッチでの検索は、項目が一覧表示されている順序で実行されます。ただし、passwd -r *repository* コマンドを使用して特に指定されていないかぎり、パスワード更新は逆の順序で実行されます。詳細は、41 ページの「ネームサービススイッチとパスワード情報」を参照してください。

構文が間違っている場合の処理

クライアントのライブラリルーチンには、ネームサービススイッチで特定の SMF プロパティーまたは default の SMF プロパティーが定義されていない場合や、プロパティーが構文的に正しくない場合に使用される、コンパイル時に組み込まれるデフォルトのエントリが含まれています。通常、これらのコンパイル時に組み込まれるデフォルトは「files」のみです。

auto_home と auto_master

auto_home テーブル、auto_master テーブルとマップのスイッチ検索基準は、automount と呼ばれる1 つのカテゴリに統合されます。

timezone とネームサービススイッチ

timezone テーブルではネームサービススイッチが使用されないため、このテーブルはスイッチのプロパティーリストに含まれていません。

ネームサービススイッチ内の keyserv および publickey エントリ

注意 – ネームサービススイッチを変更したあと、その変更を有効にするには、keyserv デーモンを再起動する必要があります。

keyserv デーモンは、keyserv が起動されている場合にのみ、ネームサービススイッチ内の publickey プロパティーを読み取ります。ネームサービススイッチのプロパティーが変更された場合は、svcadm refresh svc:/network/rpc/keyserv:default を使用して keyserv デーモンが再起動されるまで、keyserv はその変更を登録しません。プロパティーの変更が SMF リポジトリに読み込まれるように、このコマンドはプロパティーが変更され、name-service/switch サービスがリフレッシュされたあとに実行する必要があります。

ネームサービススイッチの管理

マシンのネームサービスを変更した場合は、それに応じて、そのマシンのネームサービススイッチ情報を変更する必要があります。たとえば、マシンのネームサービスをファイルから NIS に変更した場合は、NIS を使用するようにネームサービススイッチを構成する必要があります。

▼ 従来の nsswitch.conf ファイルを使用する方法

1. 管理者になります。
   詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2. **nsswitch.conf** ファイルを新しいシステムにコピーします。
   ファイル /etc/nsswitch.conf を指定するようにしてください。

3. このファイルの情報を SMF リポジトリに読み込みます。

   ```
   # nscfg import -f svc:/system/name-service/switch:default
   ```

4. ネームサービススイッチのサービスをリフレッシュします。

   ```
   # svcadm refresh name-service/switch
   ```

▼ データベースのソースを切り替える方法

1 管理者になります。

詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2 選択したデータベースのソース定義を変更します。

この例では、データベースの検索順序は最初に `files`、次に `nis` です。

```
# svccfg -s system/name-service/switch
svc:/system/name-service/switch> setprop config/host = astring: "files nis"
svc:/system/name-service/switch> quit
```

3 ネームサービススイッチのサービスをリフレッシュします。

```
# svcadm refresh name-service/switch
```

▼ すべてのネームデータベースのソースを変更する方法

1 管理者になります。

詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2 **`config/default`** プロパティーを変更します。

このプロパティーは、もっとも一般的なソース定義を使用しています。この例では、データベースの検索順序は最初に `files`、次に `nis` です。

```
# svccfg -s system/name-service/switch
svc:/system/name-service/switch> setprop config/default = astring: "files nis"
svc:/system/name-service/switch> quit
```

3 (省略可能) 個々のデータベースのプロパティーを変更します。

このコマンドは、`config/default` プロパティーで選択されている順序を使用しない、いずれかのデータベースのソース定義を変更する場合に使用します。

```
# svccfg -s system/name-service/switch
svc:/system/name-service/switch> setprop config/host = astring: "files dns nis"
svc:/system/name-service/switch> quit
```

4 ネームサービススイッチのサービスをリフレッシュします。

```
# svcadm refresh name-service/switch
```

DNS とインターネットでのアクセス

ネームサービススイッチはまた、次の章で説明されているように、クライアントの DNS 転送も制御します。DNS 転送によって、クライアントへのインターネットでのアクセスが可能になります。

ネームサービススイッチとパスワード情報

files や nis などの複数のリポジトリ内にパスワード情報を含め、それらの情報にアクセスすることができます。それらの情報の検索順序を確立するには、ネームサービススイッチ内の config/password プロパティーを使用できます。

注意 – システムへのサービス拒否 (DoS) 攻撃を回避するために、files を passwd 情報に対するネームサービススイッチ内の最初のソースにするようにしてください。

NIS 環境では、ネームサービススイッチ内の config/password プロパティーによって、次の順序でリポジトリが一覧表示されるようにしてください。

```
config/password  astring             "files nis"
```

ヒント – 最初に files を一覧表示することにより、システムで何らかのネットワークまたはネームサービスの問題が発生した場合でも、root ユーザーはほとんどの状況でログインできるようになります。

同じユーザーのために複数のリポジトリを保持しないでください。ほとんどの場合、ネームサービスは、最初の定義のみを検索して返します。重複したエントリは通常、セキュリティーの問題を覆い隠します。

たとえば、ファイルとネットワークリポジトリの両方に同じユーザーを保持すると、(config/password の name-service/switch 構成に応じて) 1 つのログイン ID がもう 1 つのログイン ID より優先して使用されます。特定のマシンの最初に一致した ID が、ログインセッションに使用される ID になります。ID がファイルとネットワークリポジトリの両方に存在するときに、セキュリティー上の理由からネットワークリポジトリが無効になった場合は、その ID が存在し、ネットワーク ID が無効にされる前にアクセスされたすべてのマシンがセキュアでなくなり、セキュアでない迷惑なアクセスに対して脆弱になる可能性があります。

◆ ◆ ◆ 第 3 章

DNS の管理 (タスク)

この章では、DNS サーバーとクライアントサービスについて説明します。次の項目について説明します。

DNS の概要

DNS には、ほとんどのネットワークプロトコルと同様に、答えを提供するサービスと、そのサービスに照会するクライアントという 2 つの部分があります。Oracle Solaris オペレーティングシステムでは、デフォルトの DNS サービスは Internet Systems Consortium (ISC) の BIND と、それに関連付けられたデーモン `named` によって提供されます。DNS クライアントは、ユーティリティーとライブラリの集まりで構成されます。

マルチキャスト DNS

マルチキャスト DNS (mDNS) は、ローカルリンク上のシステムに設定と保守の容易なネームサービスシステムを提供します。同じローカルリンク上の参加しているすべてのネットワークデバイスが、ユニキャストではなく mDNS を使用して標準の DNS 機能を実行するため、ユニキャスト DNS サーバーは必要ありません。管理者にとって、mDNS の主な利点は、ローカルネットワーク上でユニキャスト DNS サーバーを保守する必要がない点にあります。たとえば、ホスト名を、mDNS を使用しているローカルリンク上のシステムへの IP アドレスリクエストに解決するために、ホスト名を更新してファイル内に保持する必要はありません。

マルチキャスト DNS サービス検出

ネットワークサービスには、出力、ファイル転送、音楽共有や、写真、ドキュメント、その他のファイル共有のためのサーバー、およびほかのローカルデバイスによって提供されるサービスが含まれます。Oracle Solaris での DNS サービス検出のサポートには、アプリケーションがこの Oracle Solaris リリースで DNS を使用してネットワークサービスを通知したり、検出したりできるようにするための、Apple Inc. からのオープンソースフレームワークおよびツールが含まれます。

ユーザーにとっては、手動で検索しなくてもネットワーク上のサービスを参照できるようになるため、ネットワークサービス検出によってコンピューティングがより容易になります。ほかの企業やグループによって事前に形成された既存の標準および作業により、クロスプラットフォームサポートを使用できることが保証されます。

DNS についての関連資料

DNS と BIND の管理については、次のドキュメントを参照してください。

- ISC の Web サイト (http://www.isc.org) にある『BIND 9 管理者のマニュアル』
- `/usr/share/doc/bind/migration.txt` ファイル内の『BIND 9 Migration Notes』のドキュメント
- BIND の機能、既知のバグと不具合、および ISC の Web サイト (http://www.isc.org) 上の資料へのリンク
- 『DNS & BIND 第 5 版』、Paul Albitz および Cricket Liu 著、(オライリー・ジャパン、2008 年)

DNS とサービス管理機能

DNS サーバーデーモン `named` は、サービス管理機能 (SMF) を使用して管理する必要があります。SMF の概要については、『Oracle Solaris 11.1 でのサービスと障害の管理』の第 1 章「サービスの管理 (概要)」を参照してください。また、詳細については `svcadm`(1M)、`svcs`(1)、`svccfg`(1M) の各マニュアルページも参照してください。

次の一覧は、SMF サービスを使用して DNS サービスを管理するために必要ないくつかの重要な情報の簡単な概要を示しています。

- このサービスに対する管理操作 (有効化、無効化、再起動など) を実行するには、`svcadm` コマンドを使用します。

ヒント – -t オプションを使用してサービスを一時的に無効にすると、そのサービス構成に対するある程度の保護が提供されます。-t オプションを使用してサービスを無効にした場合は、リブートのあと、そのサービスの元の設定が復元されます。-t なしでサービスを無効にした場合は、リブートのあとも、そのサービスは無効のままになります。

- DNS サービスの Fault Managed Resource Identifier (FMRI) は、svc:/network/dns/server:*instance* および svc:/network/dns/client:*instance* です。
- DNS サーバーおよびクライアントのステータスの照会は、svcs コマンドを使用して実行できます。
  - 次に、svcs コマンドとその出力の例を示します。

```
# svcs \*dns\*
STATE          STIME    FMRI
disabled       Nov_16   svc:/network/dns/multicast:default
online         Nov_16   svc:/network/dns/server:default
online         Nov_16   svc:/network/dns/client:default
```

  - 次に、svcs -l コマンドとその出力の例を示します。

```
# svcs -l /network/dns/server
fmri         svc:/network/dns/server:default
name         BIND DNS server
enabled      true
state        online
next_state   none
state_time   Tue Jul 26 19:26:12 2011
logfile      /var/svc/log/network-dns-server:default.log
restarter    svc:/system/svc/restarter:default
contract_id  83
manifest     /lib/svc/manifest/network/dns/server.xml
dependency   require_all/none svc:/system/filesystem/local (online)
dependency   require_any/error svc:/network/loopback (online)
dependency   optional_all/error svc:/network/physical (online)
```

- DNS サービスを異なるオプションで起動する必要がある場合は、svccfg コマンドを使用して svc:/network/dns/server サービスのプロパティーを変更します。例については、47 ページの「DNS サーバーのオプションを構成する方法」を参照してください。

DNS サーバーデーモン named が SMF によって管理されている場合は、named の異常終了の原因となる予期しないイベントが発生すると、そのサーバーが自動的に再起動されます。さらに、svcadm コマンドを使用して、そのサービスを再起動することもできます。rndc コマンドを使用することによって可能になる BIND 固有の管理は、SMF では同時に使用できます。

DNS の管理 (タスク)

次のタスクがドキュメント化されています。

▼ DNS パッケージをインストールする方法

通常、DNS パッケージは Oracle Solaris リリースとともに自動的にインストールされます。サーバーがインストールされたときにこのパッケージが含まれていなかった場合は、次の手順を使用してパッケージをインストールします。

1 管理者になります。

詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2 DNS パッケージをインストールします。

```
# pkg install pkg:/service/network/dns/bind
```

▼ DNS サーバーを構成する方法

注 – ルートディレクトリの変更を指定するために named を構成することはお勧めできません。よりセキュアなオプションは、Solaris ゾーンを作成し、そのゾーン内で動作するように named を構成することです。

---

1 管理者になります。

詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2 DNS 構成ファイルを作成して検証します。

named デーモンが起動する前に、有効な構成ファイルが存在する必要があります。このファイルの名前は、デフォルトでは /etc/named.conf です。named の構成は、非常

に簡単になることがあります。DNS ルートサーバーがアクセス可能である場合は、空ファイルによって、キャッシュのみのサーバーを構成するための十分な情報が提供されます。

```
# touch /etc/named.conf
# named-checkconf -z /etc/named.conf
```

3 (省略可能) **rndc** 構成ファイルを作成します。

このファイルは、DNS サーバーのリモート制御アクセスを構成するために使用されます。

```
# rndc-confgen -a
wrote key file "/etc/rndc.key"
```

4 (省略可能) **dns/server** サービスの構成情報を変更します。

47 ページの「DNS サーバーのオプションを構成する方法」を参照してください。

5 **DNS** サービスを起動します。

```
# svcadm enable network/dns/server
```

▼ rndc.conf ファイルを作成する方法

/etc/rndc.conf ファイルは、rndc コマンドを使用して、DNS サーバーデーモン named のリモート制御アクセスを構成するために使用されます。デフォルトファイルを作成するには、次の手順を使用します。詳細なオプションについては、rndc.conf(4) のマニュアルページを参照してください。

1 管理者になります。

詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2 **rndc** 構成ファイルを作成します。

```
# rndc-confgen -a
wrote key file "/etc/rndc.key
```

3 **DNS** サービスを再起動します。

```
# svcadm restart dns/server:default
```

▼ DNS サーバーのオプションを構成する方法

この手順では、named トラフィックのための IPv4 トランスポートプロトコルを選択する方法について説明します。named(1M) のマニュアルページを参照してください。

1 管理者になります。

詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2 **dns/server** サービスの構成情報を変更します。

```
# svccfg -s network/dns/server
svc:/network/dns/server:default> setprop options/ip_interfaces = "IPv4"
svc:/network/dns/server:default> quit
```

3 **SMF** リポジトリを更新し、**DNS** サービスを有効にします。

```
# svcadm refresh network/dns/server
# svcadm enable network/dns/server
```

▼ DNS サービスを代替ユーザーとして実行する方法

この手順では、ユーザーに named デーモンを管理するための関連する承認を割り当てる方法について説明します。

1 管理者になります。

詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2 ユーザーを適切な役割に追加します。

```
# usermod -A solaris.smf.manage.bind dnsadmin
```

3 ユーザーのサービスプロパティーを設定します。

```
# svccfg -s network/dns/server
svc:/network/dns/server:default> setprop start/user = dnsadmin
svc:/network/dns/server:default> setprop start/group = dnsadmin
svc:/network/dns/server:default> exit
```

4 新しいプロセス **ID** ファイルのためのディレクトリを作成します。

デフォルトのプロセス ID ファイル /var/run/named/named.pid を作成するための書き込みアクセス権を持っているのは root だけであるため、named デーモンを、代わりのファイルを使用するように構成する必要があります。

```
# mkdir /var/named/tmp
# chown dnsadmin /var/named/tmp
```

5 新しいディレクトリを使用するように構成を変更します。

named.conf ファイルに次の行を追加します。

```
# head /etc/named.conf
options {
directory "/var/named";
pid-file "/var/named/tmp/named.pid";
};
```

6 SMF リポジトリを更新し、DNS サービスを再起動します。

```
# svcadm refresh svc:/network/dns/server:default
# svcadm restart svc:/network/dns/server:default
```

▼ DNS クライアントを有効にする方法

1 管理者になります。

詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2 DNS ドメインを構成します。

まず、検索するドメインと、DNS ネームサーバーの IP アドレスを一覧表示します。次に、SMF リポジトリを更新します。

```
# svccfg -s network/dns/client
svc:/network/dns/client> setprop config/search = astring: ("example.com" "sales.example.com")
svc:/network/dns/client> setprop config/nameserver = net_address: (192.168.1.10 192.168.1.11)
svc:/network/dns/client> select network/dns/client:default
svc:/network/dns/client:default> refresh
svc:/network/dns/client:default> quit
```

3 DNS を使用するようにネームサービススイッチ情報を更新します。

最初のコマンドによって、SMF リポジトリ内の DNS 構成情報が更新されます。

```
# svccfg -s system/name-service/switch
svc:/system/name-service/switch> setprop config/host = astring: "files dns"
svc:/system/name-service/switch> select system/name-service/switch:default
svc:/system/name-service/switch:default> refresh
svc:/system/name-service/switch:default> quit
```

4 /etc/resolv.conf ファイルに新しい情報を書き込みます。

/etc/resolv.conf は引き続き一部のプロセスによって使用されるため、このファイルの内容を変える変更を SMF リポジトリに対して行なったら、ファイルを再作成するようにしてください。

```
# nscfg export svc:/network/dns/client:default
```

5 DNS クライアントを実行するために必要なサービスを起動します。

```
# svcadm enable network/dns/client
# svcadm enable system/name-service/switch
```

▼ DNS サーバーの起動に関する問題をトラブルシューティングする方法

これらのすべての手順を実行する必要はありません。早い段階で問題が見つかったと思われる場合は、手順 6 に進み、サービスを正常に動作させることができます。

1 管理者になります。

詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2 **DNS** サービスのステータスをチェックします。

```
# svcs -x dns/server:default
svc:/network/dns/server:default (BIND DNS server)
 State: online since Tue Oct 18 19:35:00 2011
   See: named(1M)
   See: /var/svc/log/network-dns-server:default.log
Impact: None.
```

3 **DNS** サービスログファイルをチェックします。

```
# tail /var/svc/log/network-dns-server:default.log
```

4 **syslog** メッセージをチェックします。

```
# grep named /var/adm/messages
```

5 **named** デーモンを手動で起動します。

named をフォアグラウンドで実行すると、問題が識別しやすくなるように、すべてのログが強制的に標準エラーに出力されます。

```
# named -g
```

6 問題が解決されたら、保守に必要な状態をクリアーします。

```
# svcadm clear dns/server:default
# svcs dns/server:default
STATE          STIME    FMRI
online         17:59:08 svc:/network/dns/server:default
```

▼ DNS 構成を検証する方法

DNS 構成を変更している場合は、named-checkzone コマンドを使用して /etc/named.conf ファイルの構文を検証できます。

1 管理者になります。

詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2 必要に応じて、構成ファイルを変更します。

この例では、デフォルトディレクトリが変更されます。

```
# echo 'options {directory "/var/named";};' > /etc/named.conf
```

3 ファイルの内容を検証します。

```
# named-checkconf
/etc/named.conf:1: change directory to '/var/named' failed: file not found

/etc/named.conf:1: parsing failed
```

この例では、/var/namedディレクトリがまだ作成されていないため、チェックが失敗しました。

4 報告されたエラーをすべて修正します。

```
# mkdir /var/named
```

5 エラーが報告されなくなるまで、手順**3**と**4**を繰り返します。

6 (省略可能) 実行中のサービスに変更を反映するには、次の方法のいずれかを使用します。

- 行なった変更に応じて、**reload**または**reconfig**オプションを指定し、**rndc**コマンドを使用して構成を更新します。
- **named**サービスを再起動します。

  ```
  # svcadm restart svc:/network/dns/server:default
  ```

マルチキャスト**DNS**の管理

次のセクションでは、マルチキャストDNS (mDNS) およびDNSサービス検出を有効にする方法について説明します。また、DNSサービス検出のためのリソースを通知する方法の例も示されています。

▼ **mDNS**および**DNS**サービス検出を有効にする方法

mDNSおよびDNSサービス検出が機能するには、mDNSに参加させるすべてのシステム上にmDNSが配備されている必要があります。mDNSサービスは、システム上で提供されているサービスの可用性を通知するために使用されます。

1 管理者になります。

詳細は、『Oracle Solaris 11.1の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2 必要に応じて、**mDNS**パッケージをインストールします。

```
# pkg install pkg:/service/network/dns/mdns
```

3 ネームサービススイッチ情報を更新します。

ローカルホストを解決できるようにするには、name-service/switch サービスの config/host プロパティーを変更して、ソースとして mdns を含めます。例:

```
#  /usr/sbin/svccfg -s svc:/system/name-service/switch
svc:/system/name-service/switch> setprop config/host = astring: "files dns mdns"
svc:/system/name-service/switch> select system/name-service/switch:default
svc:/system/name-service/switch:default> refresh
svc:/system/name-service/switch> quit
```

4 **mDNS サービスを有効にします。**

```
# svcadm enable svc:/network/dns/multicast:default
```

このようにして mDNS を有効にすると、加えた変更が、アップグレードやリブートを行なったあとも維持されるようになります。詳細は、svcadm(1M) のマニュアルページを参照してください。

5 **(省略可能) 必要に応じて、mDNS エラーログをチェックします。**

mDNS サービスログ /var/svc/log/network-dns-multicast:default.log にエラーやメッセージがないかどうかをチェックします。

DNS のためのリソースの通知

ping または traceroute コマンドを使用する場合と同様に、dns-sd コマンドをネットワーク診断ツールとして使用して、サービスを参照したり、検出したりすることができます。

dns-sd コマンドは主に、対話型で使用されます。その主な理由として、そのコマンド行引数や出力形式が時間とともに変化する場合があり、それがシェルスクリプトからの起動を予測不可能で、かつ危険なものにしていることが挙げられます。さらに、DNS サービス検出 (DNS-SD) は非同期の性質を持っているため、スクリプト指向のプログラミングには適していません。

詳細は、dns-sd(1M) のマニュアルページを参照してください。DNS サービスをアプリケーションに組み込むには、libdns-sd(3DNS_SD) のマニュアルページを参照してください。

次に、DNS サービス検出を使用してサービスを通知する例を示します。

例 3–1 印刷サービスの通知

次のコマンドは、My Test という名前のシステムのポート 515 上に LPR 印刷サービスが存在することを通知して、そのサービスを DNS-SD と互換性のある印刷クライアントから使用できるようにします。

```
# dns-sd -R "My Test" _printer._tcp. . 515 pdl=application/postscript
```

例 3–1 印刷サービスの通知 (続き)

この登録を有効にするには、LPR サービスがポート 515 上で使用可能である必要があります。

例 3–2 Web ページの通知

次のコマンドは、My Test システムのポート 80 上で HTTP サーバーによって処理されている Web ページを通知します。この Web ページは、Safari やその他の DNS-SD と互換性のある Web クライアント内の Bonjour リストに表示されます。

```
# dns-sd -R "My Test" _http._tcp . 80 path=/path-to-page.html
```

DNS 参照

このセクションには、DNS サービスに関連付けられているファイル、デーモン、およびコマンドの表が含まれています。さらに、ISC バージョンの BIND が構築されたときに使用されたいくつかのフラグの表も含まれています。

DNS ファイル

次の表では、DNS サービスに関連付けられているファイルについて説明します。

表 3–1 DNS ファイル

ファイル名	機能
/etc/named.conf	named デーモンの構成情報を提供します。詳細は、named.conf(4) のマニュアルページを参照してください。
/etc/rndc.conf	rndc コマンドの構成情報を提供します。詳細は、rndc.conf(4) のマニュアルページを参照してください。

DNS コマンドおよびデーモン

次の表では、DNS サービスに関連付けられているコマンドおよびデーモンについて説明します。

表 3–2 DNS コマンドおよびデーモン

ファイル名	機能
/usr/bin/dns-sd	mDNS サービスによって使用されるリソースを検索または一覧表示します。詳細は、dns-sd(1M) のマニュアルページを参照してください。

表 3–2 DNS コマンドおよびデーモン (続き)

ファイル名	機能
/usr/sbin/dig	DNS サーバーに DNS 応答をリクエストします。多くの場合は、トラブルシューティングに使用されます。詳細は、dig(1M) のマニュアルページを参照してください。
/usr/sbin/dnssec-dsfromkey	鍵ファイルから DS RR を生成します。詳細は、dnssec-dsfromkey(1M) のマニュアルページを参照してください。
/usr/sbin/dnssec-keyfromlabel	暗号化デバイスから選択された鍵を取得し、鍵ファイルを構築します。詳細は、dnssec-keygen(1M) のマニュアルページを参照してください。
/usr/sbin/dnssec-keygen	セキュアな DNS およびトランザクション署名 (TSIG) のための鍵と鍵ファイルを作成します。詳細は、dnssec-keygen(1M) のマニュアルページを参照してください。
/usr/sbin/dnssec-signzone	DNS ゾーンに署名します。詳細は、dnssec-signzone(1M) のマニュアルページを参照してください。
/usr/sbin/host	単純な DNS 検索を実行し、多くの場合はホスト名を IP アドレスに、または IP アドレスをホスト名に変換します。詳細は、host(1M) のマニュアルページを参照してください。
/usr/sbin/named	DNS サーバーデーモン。クライアントからの情報リクエストに応答します。詳細は、named(1M) のマニュアルページを参照してください。
/usr/sbin/named-checkconf	named.conf ファイルの構文をチェックします。詳細は、named(1M) のマニュアルページを参照してください。
/usr/sbin/named-checkzone	DNS ゾーンファイルの構文と完全性をチェックします。詳細は、named-checkzone(1M) のマニュアルページを参照してください。
/usr/sbin/named-compilezone	DNS ゾーンファイルを変換します。詳細は、named-compilezone(1M) のマニュアルページを参照してください。
/usr/sbin/nscfg	従来のネームサービス構成ユーティリティー。resolv.conf の内容を SMF リポジトリにインポートまたはエクスポートします。詳細は、nscfg(1M) のマニュアルページを参照してください。
/usr/sbin/nslookup	非推奨: DNS サーバーに照会します。代わりに dig コマンドを使用してください。
/usr/sbin/nsupdate	DNS 更新リクエストを DNS サーバーに送信します。詳細は、nsupdate(1M) のマニュアルページを参照してください。

表 3–2 DNS コマンドおよびデーモン (続き)

ファイル名	機能
/usr/sbin/rndc	DNS サーバーデーモンのリモート制御を提供します。詳細は、rndc(1M) のマニュアルページを参照してください。
/usr/sbin/rndc-confgen	rndc コマンドの構成ファイルを生成します。詳細は、rndc-confgen(1M) のマニュアルページを参照してください。

BIND が構築されたときに使用されたコンパイルフラグ

named -V コマンドを使用することによって、BIND をコンパイルするために使用されたフラグを表示できます。この表は、Oracle Solaris 11 リリース用に ISC バージョンの BIND を構築するときに使用されたいくつかのコンパイルフラグを示しています。

表 3–3 BIND のコンパイルフラグ

フラグ名	機能
with-openssl	DNSSEC に必要な、暗号化と Secure Sockets Layer (SSL) のサポートを使用して BIND を構築します。
enable-threads	マルチスレッド化を有効にします。
enable-devpoll	多数のファイル記述子に対する高速ポーリングのために /dev/poll ドライバを使用します。
disable-openssl-version-check	OpenSSL が別のダイナミックライブラリによって提供されるため、OpenSSL バージョンのチェックを無効にします。
enable-fixed-rrset	下位互換性に必要な、固定されたリソースレコードセットの順序付けを有効にします。
with-pkcs11	OpenSSL 暗号化ハードウェアサポートの使用を有効にします。

◆ ◆ ◆ 第 4 章

Oracle Solaris Active Directory クライアントの設定 (タスク)

nss_ad ネームサービスモジュールは、passwd、shadow、および group ファイルのバックエンドを提供します。nss_ad モジュールは、Active Directory (AD) とそのネイティブなスキーマをネームサービスとして使用して、AD フォレスト全体にわたるユーザー名やグループ名と ID を解決します。次の項目について説明します。

nss_ad ネームサービスモジュールの概要

いずれかの AD 相互運用性機能 (nss_ad を含む) を使用できるようにするには、その前に Oracle Solaris クライアントが AD ドメインに参加している必要があります。kclient ユーティリティーは、クライアントを AD に参加させるために使用されます。参加の操作中、kclient は、そのクライアント上に Kerberos v5 を構成します。それ以降は、nss_ad を使用すると、サポートされるデータベースの nsswitch.conf ファイル内のソースとして ad を指定することによって、ネームサービスリクエストを解決できます。nss_ad モジュールは、ホスト資格を使用して AD 内のネームサービス情報を検索します。

nss_ad モジュールは、DNS サーバーのレコードを使用して、ドメインコントローラやグローバルカタログサーバーなどの AD ディレクトリサーバーを自動検出します。そのため、DNS が Oracle Solaris クライアント上で正しく構成されている必要があります。nss_ad モジュールはまた、LDAP v3 プロトコルを使用して AD サーバーのネーミング情報にアクセスします。nss_ad はネイティブな AD スキーマで動作するため、AD サーバーのスキーマに変更は必要ありません。

nss_ad モジュールは現在、Windows ユーザーの Oracle Solaris システムへのログインをサポートしていません。このようなログインがサポートされるまで、このようなユーザーは、引き続き nis や ldap などの従来のバックエンドを使用してログインするようにしてください。

nss_ad を使用するには、idmap および svc:/system/name-service/cache サービスが有効になっている必要があります。nss_ad モジュールは、idmap サービスを使用して、Windows セキュリティー識別子 (SID)、UNIX ユーザー識別子 (UID)、およびグループ識別子 (GID) の間をマップします。

AD ユーザーおよびグループ名がすべて、ドメイン名で修飾されていることを確認してください (user@domain や group@domain など)。たとえば、dana が domain という名前のドメイン内の有効な Windows ユーザーである場合、getpwnam(dana) は失敗しますが、getpwnam(dana@domain) は成功します。

また、次の追加の規則も nss_ad モジュールに関連します。

- AD と同様に、nss_ad は、ユーザーおよびグループ名の大文字と小文字が区別されないマッチングを実行します。
- nss_ad モジュールは、UTF-8 ロケール、またはユーザーやグループの名前に ASCII 文字のみが存在するドメインでのみ使用してください。
- 既知の SID として、Windows の世界における汎用ユーザーまたは汎用グループを識別する一連の SID があります。これらはドメイン固有の SID ではなく、その値はすべての Windows オペレーティングシステムにわたって一定のままです。既知の SID の名前は、文字列 BUILTIN で修飾されます (たとえば、Remote Desktop Users@BUILTIN)。
- nss_ad モジュールは、列挙をサポートしていません。そのため、それを使用する getpwent() および getgrent() インタフェースやコマンド (getent passwd や getent group など) は AD から情報を取得できません。
- nss_ad モジュールは現在、passwd および group ファイルのみをサポートしています。nss_ad は、passwd エントリに従うほかのネームサービスデータベース (audit_user や user_attr など) をサポートしていません。ad バックエンドが (構成に基づいて) 処理された場合は、これらのデータベースに対して「NOT FOUND」が返されます。

▼ nss_ad モジュールを構成する方法

nss_ad モジュールでは、Oracle Solaris クライアントがホスト解決に DNS を使用する必要があります。

1 **DNS サービスを構成します。**

手順については、49 ページの「DNS クライアントを有効にする方法」を参照してください。

注 – AD ドメイン名は、domain 指令を使用して、または search 指令で指定された一覧内の最初の項目として指定する必要があります。

両方の指令が指定されている場合は、最後に指定されているものが優先されます。これは、idmap 自動検出機能が正しく機能するために必要です。

次の例では、dig コマンドは、名前と IP アドレスを使用して AD サーバーを解決できることを確認します。

```
# dig -x 192.168.11.22 +short
myserver.ad.example
# dig myserver.ad.example +short
192.168.11.22
```

2 **hosts** に対するネームサービスの一覧に **dns** を追加します。

```
# svccfg -s svc:/system/name-service/switch
svc:/system/name-service/switch> setprop config/host = astring: "files dns"
svc:/system/name-service/switch> select system/name-service/switch:default
svc:/system/name-service/switch:default> refresh
svc:/system/name-service/switch:default> quit
```

注 – ホスト解決のために nis や ldap などの追加のネームサービスを含めるには、それらを dns のあとに追加します。

---

3 **DNS** サービスが有効であり、オンラインになっていることを確認します。

例:

```
# svcs svc:/network/dns/client
STATE STIME FMRI
online Oct_14 svc:/network/dns/client:default
```

4 **kclient** ユーティリティーを使用して、システムを **AD** ドメインに参加させます。

例:

```
# /usr/sbin/kclient -T ms_ad
```

5 **password** と **group** に対するネームサービスの一覧 **ad** を追加します。

```
# svccfg -s svc:/system/name-service/switch
svc:/system/name-service/switch> setprop config/password = astring: "files nis ad"
svc:/system/name-service/switch> setprop config/group = astring: "files nis ad"
svc:/system/name-service/switch> select system/name-service/switch:default
svc:/system/name-service/switch:default> refresh
svc:/system/name-service/switch:default> quit
```

6 **idmap** サービスを有効にします。

```
# svcadm enable idmap
```

7 ネームサービススイッチサービスの SMF リポジトリを更新します。

```
# svcadm refresh name-service/switch
```

注 – ネームサービススイッチがリフレッシュされた場合は常に、必要に応じて nscd モジュールは自動的に再起動します。

8 AD から user と group の情報にアクセスできることを確認します。

例:

```
# getent passwd 'test_user@example'
test_user@example:x:2154266625:2154266626:test_user::
# getent passwd 2154266625
test_user@example:x:2154266625:2154266626:test_user::
```

パスワード更新

passwd(4) のマニュアルページには、ネームサービススイッチ内の config/passwd プロパティーの有効な形式の一覧が含まれています。これらの構成への ad の追加がサポートされています。ただし、passwd コマンドを使用した AD ユーザーのパスワードの変更はサポートされていません。パスワード更新中に passwd エントリ内に見つかった場合、ad はスキップされます。AD ユーザーのパスワードを更新するには、kpasswd コマンドを使用します。

ネームサービススイッチ内の既存の有効な password および group エントリに ad の検索順序を追加できます。例:

```
# svccfg -s svc:/system/name-service/switch
svc:/system/name-service/switch> setprop config/password = astring: "files nis ad"
svc:/system/name-service/switch> setprop config/group = astring: "files nis ad"
svc:/system/name-service/switch> select system/name-service/switch:default
svc:/system/name-service/switch:default> refresh
svc:/system/name-service/switch:default> quit
```

nss_ad ネームサービスモジュールが AD からデータを取得する方法

次のセクションでは、nss_ad モジュールが AD から対応するデータを取得することによって、passwd、shadow、および group ファイルに対するネームサービスリクエストを解決する方法について説明します。

passwd 情報の取得

次の構文は、passwd エントリの正しい形式を示しています。

username:*password*:*uid*:*gid*:*gecos*:*home-directory*:*login-shell*

詳細は、passwd(4) のマニュアルページを参照してください。

nss_ad モジュールは、AD から passwd 情報を次のように取得します。

- *username* – フィールドは samAccountName AD 属性の値を使用し、オブジェクトが存在するドメイン名で修飾されます (たとえば、terryb@example.com)。
- *password* – フィールドは、AD オブジェクトではユーザーパスワードが使用できないため、x の値を使用します。
- *uid* – フィールドは objectSID AD 属性の Windows ユーザーの SID を使用し、それが idmap サービスを使用して UID にマップされます。
- *gid* – フィールドは Windows ユーザーのプライマリグループ SID を使用し、それが idmap サービスを使用して GID にマップされます。このグループ SID は、primaryGroupID AD 属性の値をドメイン SID に追加することによって取得されます。AD 内のユーザーの場合、primaryGroupID 属性はオプション属性であるため、存在しない可能性があります。この属性が存在しない場合、nss_ad は idmap の対角マッピング機能を使用して、objectSID 属性のユーザー SID をマップします。
- *gecos* – CN AD 属性の値。
- *home-directory* – 値が存在する場合は、homeDirectory AD 属性の値。それ以外の場合、このフィールドは空のままになります。
- *login-shell* – フィールドは、ネイティブな AD スキーマにはログインシェル属性が存在しないため、空のままになります。

shadow 情報の取得

次の構文は、shadow エントリの正しい形式を示しています。

username:*password*:*lastchg*:*min*:*max*:*warn*:*inactive*:*expire*:*flag*

詳細は、shadow(4) のマニュアルページを参照してください。

nss_ad モジュールは、AD から shadow 情報を次のように取得します。

- *username* – フィールドは samAccountName AD 属性の値を使用し、オブジェクトが存在するドメイン名で修飾されます (たとえば、terryb@example.com)。
- *password* – フィールドは、AD オブジェクトではユーザーパスワードが使用できないため、*NP* の値を使用します。

シャドウフィールドは AD や Kerberos v5 には関係しないため、シャドウフィールドの残りは空のままになります。

group 情報の取得

次の構文は、group エントリの正しい形式を示しています。

groupname:*password*:*gid*:*user-list*

詳細は、group(4) のマニュアルページを参照してください。

nss_ad モジュールは、AD から情報を次のように取得します。

- *groupname* – フィールドは samAccountName AD 属性の値を使用し、オブジェクトが存在するドメイン名で修飾されます (たとえば、admins@example)。
- *password* – フィールドは、Windows グループにはパスワードがないため、空のままになります。
- *gid* – フィールドは objectSID AD 属性の Windows グループの SID を使用し、それが idmap サービスを使用して GID にマップされます。
- *user-list* – フィールドは空のままになります。

パート II

NISの設定と管理

ここでは、ネットワーク情報サービス (NIS) ネームサービスの概要のほか、Oracle Solaris OS 内での NIS の設定、管理、およびトラブルシューティングについて説明します。

◆ ◆ ◆ 第 5 章

ネットワーク情報サービス (概要)

この章では、ネットワーク情報サービス (NIS) の概要について説明します。

NIS とは分散型ネームサービスであり、ネットワーク上のオブジェクトおよびリソースを識別し、探索するメカニズムです。NIS は、ネットワーク全体の情報に関する一様なストレージと検索方法を、トランスポートプロトコルやメディアに依存しない形式で提供します。

この章で扱う内容は、次のとおりです。

NIS の概要

システム管理者は、NIS を実行することによって、マップと呼ばれる管理データベースをさまざまなサーバー (マスターおよびスレーブ) 間に分散させることができます。さらに、これらの管理データベースを一元管理により自動的かつ確実な方法で更新できるため、どのクライアントもネットワーク全体を通して一貫した方法で同じネームサービス情報を共有できます。

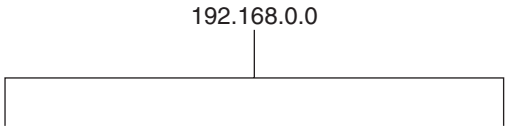
NIS は DNS とは独立に開発されており、少し異なるところに焦点を置いています。DNS は数値 IP アドレスの代わりにマシン名を使うことによって、通信を簡略化することに焦点を当てているのに対して、NIS の場合は、多様なネットワーク情報を集中管理することによりネットワーク管理機能を高めることに焦点を絞っています。NIS には、マシン名とアドレスだけでなく、ユーザー、ネットワークそのもの、ネットワークサービスについての情報も格納されます。このネットワーク情報の集まりを、NIS の名前空間と呼びます。

注 – 「マシン」名の代わりに「ホスト」名が使われることがあります。この説明ではマシンを使用していますが、一部の画面メッセージや NIS マップ名では、ホストまたはマシンが使用される可能性があります。

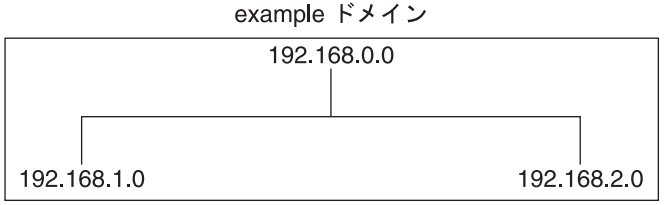
NIS のアーキテクチャー

NIS はクライアントサーバー方式を使用します。NIS サーバーが NIS のクライアントへサービスを提供します。主体サーバーはマスターサーバーと呼ばれ、信頼性のために、複数のバックアップサーバー (または、スレーブサーバーを割り当てることができます。マスターサーバーとスレーブサーバーはどちらも NIS 情報検索ソフトウェアを使用し、どちらも NIS マップを格納します。

NIS はドメインを使用して、マシン、ユーザー、およびネットワークをその名前空間に配置します。ただし、ドメイン階層は使用しません。NIS の名前空間は一層です。



したがって、上記のような物理ネットワークは、次のように 1 つの NIS ドメインに配置されます。



NIS ドメインを、NIS のみを使用してインターネットに直接接続することはできません。ただし、NIS を使用してインターネットへも接続したいと希望する組織では、NIS と DNS を組み合せることができます。その場合、NIS を使用してすべてのローカル情報を管理し、DNS を使用してインターネットのホストを検索できます。NIS はまた、NIS マップ内で情報が見つからない場合にホスト検索を DNS に転送する転送サービスも提供します。また、Oracle Solaris システムでは、ホストの検索リクエストを次の方法で転送できるようにネームサービススイッチサービスを設定することもできます。

- DNS にのみアクセスする

- DNS にアクセスするが、DNS 内にホストが見つからない場合は NIS にアクセスする
- NIS にアクセスするが、NIS によってホストが見つからない場合は DNS にアクセスする

最大の相互運用性を実現するには、ホスト検索のためのサービスとして DNS を推奨します。詳細は、第 2 章「ネームサービススイッチ (概要)」を参照してください。

NIS マシンのタイプ

NIS マシンには、次の 3 つのタイプがあります。

- マスターサーバー
- スレーブサーバー
- NIS サーバーのクライアント

NIS クライアントにはどのマシンでもなれますが、NIS サーバー (マスターまたはスレーブ) となるのはディスクが装備されているマシンだけです。一般にサーバーは、多くの場合はそのサーバー自身のクライアントでもあります。

NIS サーバー

NIS サーバーには、マスターサーバーとスレーブサーバーの 2 つの種類があります。マスターサーバーとして指定されているマシンには、NIS 管理者が必要に応じて作成、更新する一群のマップが保存されます。各 NIS ドメインには、マスターサーバーが 1 つだけ存在している必要があります。マスターサーバーは、パフォーマンスの低下を最小限に抑えながら NIS の更新をスレーブサーバーに伝播できます。

ドメインに別の NIS サーバーをスレーブサーバーとして指定できます。各スレーブサーバーには、マスターサーバーの NIS マップセットの完全なコピーが存在します。マスターサーバーの NIS マップが更新されると、必ずこれらの更新がスレーブサーバーに伝播されます。スレーブサーバーは、マスターサーバーからの要求のオーバーフローに対処して、「サーバー使用不可」エラーを最小限に抑えることができます。

通常、システム管理者はすべての NIS マップに対してマスターサーバーを 1 つ指定します。ただし、各 NIS マップ内ではマスターサーバーのマシン名がエンコードされているので、異なる複数のマップに対して異なる複数のサーバーを、マスターサーバーやスレーブサーバーとして動作するように指定することもできます。管理の複雑さを最小限に抑えるには、1 つのドメイン内で作成されるすべてのマップに対して、マスターサーバーを 1 つだけ指定します。この章の例では、1 つのサーバーがドメイン内のすべてのマップのマスターサーバーとなっています。

NIS クライアント

NIS クライアントでは、サーバー上のマップのデータを要求するプロセスが動作します。各 NIS サーバーに保存されている情報は同じであるはずなので、クライアントではマスターサーバーとスレーブサーバーの区別は行われません。

注 – Oracle Solaris OS は、NIS クライアントとネイティブな LDAP クライアントが同じクライアントシステム上に共存する構成をサポートしていません。

NIS の要素

NIS ネームサービスは、次の要素から構成されています。

- ドメイン (68 ページの「NIS ドメイン」を参照)
- デーモン (69 ページの「NIS デーモン」を参照)
- コマンド (69 ページの「NIS コマンド」を参照)
- マップ (71 ページの「NIS マップ」を参照)

NIS ドメイン

NIS ドメインは、NIS マップの共通のセットを共有するホストの集まりです。各ドメインにはドメイン名があり、マップの共通のセットを共有する各マシンがそのドメインに属しています。

NIS ドメインと DNS ドメインは、必ずしも同じではありません。一部の環境では、NIS ドメインは、企業全体にわたるネットワークサブネット管理レイアウトに基づいて定義されます。DNS 名と DNS ドメインは、インターネットの DNS ネーミング標準および階層によって定義されます。2 つのネームドメインネームシステムは、同じになるように構成される場合も、されない場合もあります。2 つのサービスのドメイン名は個別に制御されるため、異なった方法で構成される可能性があります。

ある特定のドメインのマップ用のサーバーが同じネットワークまたはサブネット内に存在するかぎり、どのホストもそのドメインに属することができます。NIS ドメインの検索では、リモート手続き呼び出し (RPC) が使用されます。そのため、NIS では、すべてのクライアントと、それらのクライアントに直接サービスを提供するすべてのサーバーマシンが同じアクセス可能なサブネット上に存在する必要があります。各管理サブネットを個別の (企業全体にわたる DNS ドメインとは異なる) NIS ドメインとして、ただし、共通のマスターマシンから管理された共通データベースを使用して管理することは、珍しいことではありません。NIS ドメイン名および共有されたすべての NIS 構成情報は、`svc:/network/nis/domain` SMF サービスによって管理されます。

NIS デーモン

NIS サービスは、次の表に示すデーモンによって提供されます。NIS サービスは SMF によって管理されます。このサービスに関する有効化、無効化、再起動などの管理アクションは svcadm コマンドを使用して実行できます。SMF の概要については、『Oracle Solaris 11.1 でのサービスと障害の管理』の第 1 章「サービスの管理 (概要)」を参照してください。また、詳細については svcadm(1M) および svcs(1) のマニュアルページも参照してください。

表 5–1　NIS デーモン

デーモン	機能
nscd	ほとんどのネームサービスリクエストにキャッシュを提供する、svc:/system/name-service/cache サービスによって管理されるクライアントサービス
rpc.yppasswdd	svc:/network/nis/passwd サービスによって管理される NIS パスワード更新デーモン 注 – rpc.yppasswdd デーモンは、r で始まるすべてのシェルを制限付きと見なします。たとえば、/bin/rksh で作業している場合は、そのシェルから別のシェルへの変更を許可されません。r で始まるシェルを持っているが、そのような制約を受けたくない場合は、第 8 章「NIS のトラブルシューティング」の対処方法を参照してください。
rpc.ypupdated	publickey などのほかのマップを変更する、svc:/network/nis/update サービスによって管理されるデーモン
ypbind	svc:/network/nis/client サービスによって管理されるバインドプロセス
ypserv	svc:/network/nis/server サービスによって管理されるサーバープロセス
ypxfrd	svc:/network/nis/xfr サービスによって管理される高速マップ転送デーモン

NIS コマンド

NIS サービスは、次の表で説明されているいくつかのコマンドによってサポートされます。

表 5–2 NIS コマンドのサマリー

コマンド	説明
make	/var/yp/Makefile を読み取ることによって NIS マップを更新します (このコマンドが /var/yp ディレクトリ内で実行されている場合)。make を使うと、入力ファイルに基づいてすべてのマップを更新したり、個々のマップを更新したりできます。NIS のための make の機能については、ypmake(1M) のマニュアルページで説明されています。
makedbm	入力ファイルを取得し、それを dbm.dir および dbm.pag ファイルに変換します。NIS は、有効な dbm ファイルをマップとして使用します。また、マップを構成する鍵と値のペアを表示できるように、makedbm -u を使用してそのマップを分解することもできます。
ypcat	NIS マップの内容を表示します。
ypinit	自動的に入力ファイルから NIS サーバーのマップを作成します。また、クライアント上で初期の /var/yp/binding/*domain*/ypservers ファイルを作成するためにも使用できます。ypinit は、NIS マスターサーバーと NIS スレーブサーバーをはじめて設定するために使用します。
ypmatch	NIS マップ内の指定された 1 つ以上の鍵の値を出力します。システム管理者は、NIS サーバーマップのバージョンを指定することはできません。
yppoll	指定したサーバー上でどのバージョンの NIS マップが実行されているを示します。yppoll はまた、NIS マップのマスターサーバーを一覧表示します。
yppush	NIS マップの新バージョンを NIS マスターサーバーからそのスレーブサーバーにコピーします。yppush コマンドは、NIS マスターサーバー上で実行できます。
ypset	指定された NIS サーバーにバインドするよう ypbind プロセスに指示します。このコマンドは気軽に使用するものではなく、セキュリティーへの影響から、使用しないことが推奨されます。ypbind プロセスの ypset および ypsetme オプションについては、ypset(1M) および ypbind(1M) のマニュアルページを参照してください。
ypwhich	クライアントが現時点で NIS サービスのためにどの NIS サーバーを使用しているかを示します。-m *mapname* オプションを指定して起動されると、このコマンドは、どの NIS サーバーが各マップのマスターであるかを示します。-m のみが使用されている場合、このコマンドは、使用可能なすべてのマップの名前と、それらに対応するマスターサーバーを表示します。
ypxfr	NIS 自体をトランスポートメディアとして使用して、NIS マップをリモートサーバーからローカルの /var/yp/*domain* ディレクトリに取り込みます。ypxfr は対話的に実行するか、または crontab ファイルから定期的に実行できます。また、ypxfr が ypserv によって呼び出されると、転送が開始されます。

NIS マップ

NIS マップ内の情報は、ndbm 形式で格納されます。マップファイルの形式については、ypfiles(4) および ndbm(3C) のマニュアルページで説明されています。

NIS マップは、UNIX の /etc データやその他の構成ファイル (passwd、shadow、group など) へのアクセスを、システムのネットワーク間で同じデータを共有できるように拡張します。これらのファイルの共有によって、これらのデータファイルの管理上の更新や管理が簡略化されます。NIS は、最小の労力で配備できます。ただし、より大規模な企業、特にセキュリティー要件を満たす必要のある企業は、代わりに LDAP ネームサービスの使用を考慮するべきです。NIS が動作しているネットワーク上では、各 NIS ドメインの NIS マスターサーバーは、照会されるドメイン内のほかのマシンの NIS マップセットを保持します。NIS スレーブサーバーは、NIS マスターサーバーのマップのコピーを保持します。NIS クライアントマシンは、マスターサーバーまたはスレーブサーバーから名前空間情報を取得できます。

NIS マップは基本的に、2 つの列からなるテーブルです。1 つの列は鍵であり、もう 1 つの列は鍵に関連する情報です。NIS は、鍵を検索してクライアントに関する情報を見つけます。各マップでは異なる鍵が使われるので、一部の情報はいくつかのマップに保存されます。たとえば、マシン名とアドレスは、 hosts.byname および hosts.byaddr という 2 つのマップに保存されます。サーバーがマシンの名前を持っており、そのマシンのアドレスを見つける必要がある場合は、サーバーは hosts.byname マップを調べます。アドレスを持っていて、名前を見つける必要がある場合は、hosts.byaddr マップを調べます。

NIS Makefile は、インストール時に NIS サーバーとして指定されたマシンの /var/yp ディレクトリ内に格納されます。そのディレクトリ内で make を実行すると、makedbm が入力ファイルからデフォルトの NIS マップを作成するか、または変更します。

注 – マップは必ずマスターサーバー上で作成してください。スレーブサーバーで作成したマップはマスターサーバーに自動的に格納されません。

デフォルトの NIS マップ

Oracle Solaris システムには、NIS マップのデフォルトセットが用意されています。システム管理者は、これらのマップをすべて使用することも一部だけを使用することもできます。また、ほかのソフトウェア製品のインストール時にシステム管理者が作成または追加したマップもすべて NIS で使用できます。

NIS ドメインのデフォルトのマップは、各サーバーの /var/yp/*domain-name* ディレクトリ内にあります。たとえば、ドメイン test.com に属しているマップは、各サーバーの /var/yp/test.com ディレクトリ内にあります。

次の表では、デフォルトの NIS マップについて説明し、各マップに対応するソースファイル名の一覧を示しています。

表 5–3 NIS マップの説明

マップ名	対応するソースファイル	説明
audit_user	audit_user	ユーザー監査の事前選択データを含みます。
auth_attr	auth_attr	承認名と説明を含みます。
bootparams	bootparams	ブート中にクライアントに必要なファイルのパス名を含みます (ルート、スワップなど)。
ethers.byaddr	ethers	マシン名と Ethernet アドレスを含みます。Ethernet アドレスはマップ内の鍵です。
ethers.byname	ethers	ethers.byaddr と同じです。ただし鍵は、Ethernet アドレスではなくマシン名です。
exec_attr	exec_attr	プロファイルの実行属性を含みます。
group.bygid	group	グループセキュリティー情報を含みます。鍵はグループ ID です。
group.byname	group	グループセキュリティー情報を含みます。鍵はグループ名です。
hosts.byaddr	hosts	マシン名と IP アドレスを含みます。鍵は IP アドレスです。
hosts.byname	hosts	マシン名と IP アドレスを含みます。鍵はマシン (ホスト) 名です。
mail.aliases	aliases	エイリアスとメールアドレスを含みます。鍵はエイリアスです。
mail.byaddr	aliases	メールアドレスとエイリアスを含みます。鍵はメールアドレスです。
netgroup.byhost	netgroup	グループ名、ユーザー名、マシン名を含みます。キーはマシン名です。
netgroup.byuser	netgroup	netgroup.byhost と同じです。ただし、鍵はユーザー名です。
netgroup	netgroup	netgroup.byhost と同じです。ただし、鍵はグループ名です。
netid.byname	passwd、hosts group	UNIX スタイルの認証に使用されます。マシン名とメールアドレスを含みます (ドメイン名も含む)。netid ファイルがある場合には、ほかのファイルを使用して利用できるデータのほかにそれが参照されます。

表5–3 NISマップの説明 (続き)

マップ名	対応するソースファイル	説明
publickey.byname	publickey	Secure RPCによって使用される公開鍵データベースを含みます。
netmasks.byaddr	netmasks	IP送出時に使用するネットワークマスクを含みます。鍵はアドレスです。
networks.byaddr	networks	システムに認識されているネットワーク名、およびIPアドレスを含みます。鍵はIPアドレスです。
networks.byname	networks	networks.byaddrと同じです。ただし、鍵はネットワーク名です。
passwd.adjunct.byname	passwdおよびshadow	C2クライアント用の監査情報と隠蔽されたパスワード情報を含みます。
passwd.byname	passwdおよびshadow	パスワード情報を含みます。鍵はユーザー名です。
passwd.byuid	passwdおよびshadow	passwd.bynameと同じです。ただし、鍵はユーザーIDです。
prof_attr	prof_attr	実行プロファイルの属性を含みます。
protocols.byname	protocols	システムに認識されているネットワークプロトコルを含みます。
protocols.bynumber	protocols	protocols.bynameと同じです。ただし、鍵はプロトコル番号です。
rpc.bynumber	rpc	システムに認識されているRPCのプログラム番号と名前を含みます。鍵はRPCのプログラム番号です。
services.byname	services	ネットワークに認識されているインターネットサービスを一覧表示します。鍵はポートまたはプロトコルです。
services.byservice	services	ネットワークに認識されているインターネットサービスを一覧表示します。鍵はサービス名です。
user_attr	user_attr	ユーザーと役割に関する拡張属性を含みます。
ypservers	該当なし	ネットワークに認識されているNISサーバーを一覧表示します。

ageing.bynameマッピングには、NISからLDAPへの移行が実装されたときに、yppasswddデーモンがディレクトリ情報ツリー(DIT)との間のパスワード有効期

限情報の読み取りと書き込みを行うために使用する情報が含まれています。パスワードの有効期限を使用しない場合は、この情報をマッピングファイルからコメントアウトします。NIS から LDAP への移行についての詳細は、第 15 章「NIS から LDAP への移行 (タスク)」を参照してください。

NIS マップの使用

NIS を使用すると、ネットワークデータベースの更新が /etc ファイルシステムを使用した場合よりはるかに簡単になります。ネットワーク環境を変更するたびに、すべてのマシン上で /etc 管理ファイルを変更する必要はなくなります。

ただし、NIS では、/etc ファイルで提供される以上のセキュリティーは追加されません。ネットワークデータベースへのアクセスの制限、SSL を使用したネットワーク経由での検索結果の送信、Kerberos でセキュリティー保護された検索などのより高度な機能の使用といった、追加のセキュリティーが必要な場合は、代わりに LDAP ネームサービスを使用するようにしてください。

たとえば、NIS を実行しているネットワークに新しいユーザーを追加する場合は、マスターサーバー内の入力ファイルを更新し、make コマンドを実行するだけで済みます。このコマンドは、passwd.byname および passwd.byuid マップを自動的に更新します。次に、これらのマップはスレーブサーバーに転送され、ドメインのクライアントマシンとそのプログラムのすべてで使用できるようになります。クライアントマシンまたはアプリケーションがユーザー名または UID を使用して情報をリクエストすると、NIS サーバーは必要に応じて passwd.byname または passwd.byuid マップを参照し、リクエストされた情報をクライアントに送信します。

ypcat コマンドを使用して、マップ内の値を表示できます。ypcat の基本的な使用形式は、次のとおりです。

```
% ypcat mapname
```

mapname は、調べたいマップ名またはその「ニックネーム」です。ypservers の場合のように、マップが鍵のみで構成されている場合は、ypcat -k を使用します。それ以外の場合、ypcat は空行を出力します。ypcat のその他のオプションについては、ypcat(1) のマニュアルページで説明されています。

ypwhich コマンドを使用すると、どのサーバーが特定のマップのマスターであるかを判定できます。次のように入力します。

```
% ypwhich -m mapname
```

mapname は、検索するマスターサーバーのマップ名またはニックネームです。mapname を入力すると、マスターサーバー名が表示されます。詳細は、ypwhich(1) のマニュアルページを参照してください。

NIS マップのニックネーム

「ニックネーム」は、マップのフルネームのエイリアスです。使用可能なマップのニックネーム (たとえば、passwd.byname の場合は passwd) を一覧表示するには、ypcat -x または ypwhich -x と入力してください。

ニックネームは、/var/yp/nicknames ファイル内に格納されます。このファイルには、マップのニックネームのあとにスペースで区切られてマップの完全指定名が含まれます。このリストは、追加または変更が可能です。ニックネーム数は現在、500 に制限されています。

NIS のバインド

NIS クライアントは、バインドプロセスによって NIS サーバーに接続されます。このプロセスは、svc:/network/nis/client および svc:/network/nis/domain サービスによってサポートされます。いずれかの NIS サービスが動作するには、これらのサービスが有効になっている必要があります。svc:/network/nis/client サービスは、サーバーリストまたはブロードキャストの 2 つのモードのどちらかで動作できます。

- サーバーリスト — サーバーリストモードでは、ypbind プロセスは、svc:/network/nis/domain サービスにドメイン内のすべての NIS サーバーの名前を照会します。ypbindプロセスは、このファイルに存在するサーバーにだけバインドされます。

  NIS サーバーは、svccfg コマンドを使用して追加できます。これらは、svc:/network/nis/domain サービス内の config/ypservers プロパティーに追加されます。各プロパティー値が特定の NIS サーバーを表します。

  さらに、NIS のバインドが機能するには、svc:/network/nis/domain サービスで指定されているすべてのサーバー名のエントリが /etc/inet/hosts ファイル内に含まれている必要があります。

- ブロードキャスト — ypbind プロセスは、RPC ブロードキャストを使用してバインドを開始することもできます。ブロードキャストはそれ以上ルーティングされないローカルサブネットのイベントでしかないため、クライアントと同じサブネット上に少なくとも 1 台のサーバー (マスターまたはスレーブ) が存在する必要があります。マップの伝播はサブネット境界を超えて機能するため、これらのサーバー自体が異なるサブネットワークにわたって存在する可能性があります。サブネット環境での 1 つの一般的方法は、NIS サーバーとしてサブネットルーターを使用することです。この方法を使用すると、ドメインサーバーはどちらかのサブネットインタフェース上でクライアントにサービスを提供できます。

  ブロードキャストモードは一般に、推奨される動作モードです。ブロードキャストモードでは、追加のホストエントリを指定する (または、/etc/inet/hosts を変更する) 必要はありません。

通常、クライアントはサーバーにバインドされたあと、何らかの原因でバインドが変更されるまで、そのサーバーにバインドされたままになります。たとえば、サーバーがサービスを提供できなくなると、このサーバーがサービスを提供していたクライアントは、新しいサーバーにバインドされます。

特定のクライアントに現在、どの NIS サーバーがサービスを提供しているかを判定するには、次のコマンドを使用します。

```
% ypwhich machinename
```

ここで、*machinename* はクライアントの名前です。マシン名が指定されていない場合、`ypwhich` コマンドはデフォルトで、ローカルマシン (つまり、そのコマンドが実行されているマシン) を使用します。

サーバーリストモード

サーバーリストモードでは、バインドプロセスは次のように動作します。

1. NIS マップによって提供される情報を必要としている、NIS クライアントマシン上で動作している任意のプログラムが `ypbind` にサーバーの名前を問い合わせます。
2. `ypbind` デーモンが `/var/yp/binding/`*domainname*`/ypservers` ファイルを調べて、ドメインの NIS サーバーのリストを取得します。
3. `ypbind` デーモンが、リスト内の最初のサーバーへのバインドを開始します。そのサーバーが応答しない場合、サーバーが見つかるか、またはリストの最後に達するまで、`ypbind` は 2 番目以降のサーバーを順番に試みます。
4. `ypbind` デーモンが、クライアントプロセスに、どのサーバーに接続するかを指示します。次に、クライアントプロセスが直接、サーバーに要求を送信します。
5. NIS サーバー上の `ypserv` デーモンが、該当するマップを調べることによってリクエストを処理します。
6. `ypserv` デーモンは、リクエストされた情報をクライアントに送り返します。

ブロードキャストモード

ブロードキャストモードでは、バインドプロセスは次のように動作します。

1. ブロードキャストオプション (`broadcast`) を設定して、`ypbind` デーモンを起動する必要があります。
2. `ypbind` デーモンが、NIS サーバーを検索するために RPC ブロードキャストを発行します。

注 – このようなクライアントをサポートするには、NIS サービスを要求している各サブネット上に 1 つの NIS サーバーが存在する必要があります。

3. ypbind デーモンが、ブロードキャストに応答した最初のサーバーへのバインドを開始します。
4. ypbind デーモンが、クライアントプロセスに、どのサーバーに接続するかを指示します。次に、クライアントプロセスが直接、サーバーに要求を送信します。
5. NIS サーバー上の ypserv デーモンが、該当するマップを調べることによってリクエストを処理します。
6. ypserv デーモンは、リクエストされた情報をクライアントに送り返します。

◆ ◆ ◆ 第 6 章

NISの設定と構成(タスク)

この章では、ネットワーク情報サービス (NIS) の初期の設定と構成について説明します。

注 – 「マシン」名の代わりに「ホスト」名が使われることがあります。この説明では「マシン」を使用していますが、一部の画面メッセージやNISマップ名では、ホストまたはマシンが使用される可能性があります。

この章で扱う内容は、次のとおりです。

NISの構成 — タスクマップ

タスク	説明	説明
変換用のソースファイルを準備します。	ローカルの /etc ファイルからNISマップを構築する前に、それらのファイルをクリーンアップします。	84 ページの「変換用のソースファイルを準備する方法」
マスターサーバーを設定します。	NIS情報のプライマリソースであるマスターサーバーを作成します。	87 ページの「マスターサーバーを設定する方法」

タスク	説明	説明
マスターサーバー上で NIS を起動します。	NIS サーバーからの NIS 情報の提供を開始します。	90 ページの「NIS サーバー上の NIS サービスの起動と停止」
スレーブサーバーを設定します。	NIS 情報のセカンダリソースであるスレーブサーバーを作成します。	92 ページの「スレーブサーバーを設定する方法」
NIS クライアントを設定します。	クライアントが NIS 情報を使用できるようにします。	96 ページの「NIS クライアントの管理」

NIS の構成を始める前に

NIS の名前空間を構成する前に、次の操作を行う必要があります。

- NIS ドメインを設計する。詳細は、82 ページの「NIS ドメインの設計」を参照してください。
- NIS を使用する予定のすべてのマシン上に、正しく構成されたネームサービススイッチ情報をインストールします。詳細は、第 2 章「ネームサービススイッチ (概要)」を参照してください。

NIS とサービス管理機能

NIS サービスはサービス管理機能によって管理されます。SMF の概要については、『Oracle Solaris 11.1 でのサービスと障害の管理』の第 1 章「サービスの管理 (概要)」を参照してください。また、詳細については svcadm(1M) および svcs(1) のマニュアルページも参照してください。

次の一覧は、SMF サービスを使用して NIS を管理するために必要ないくつかの重要な情報の簡単な概要を示しています。

- このサービスに関する有効化、無効化、再起動などの管理アクションは svcadm コマンドを使用して実行できます。NIS を開始または停止するには、コマンド行から ypstart および ypstop も使用できます。詳細は、ypstart(1M) および ypstop(1M) のマニュアルページを参照してください。

  ヒント – -t オプションを使用してサービスを一時的に無効化すると、そのサービス構成に対していくらかの保護を提供できます。-t オプションを指定してサービスを無効にした場合、リブート後に元の設定が復元されます。-t オプションを指定しないでサービスを無効にした場合、リブート後もそのサービスは無効のままです。

- NIS の障害管理リソース識別子 (FMRI) は次のとおりです。

- NIS サーバーには svc:/network/nis/server
- NIS クライアントには svc:/network/nis/client
- ドメイン名には svc:/network/nis/domain

- svcs コマンドを使用して、NIS サービスのステータスを照会できます。
  - 次に、svcs コマンドとその出力の例を示します。

```
$ svcs network/nis/server
STATE        STIME    FMRI
online       Jan_10   svc:/network/nis/server:default

$ svcs \*nis\*
STATE          STIME    FMRI
online         Oct_09   svc:/network/nis/domain:default
online         Oct_09   svc:/network/nis/client:default
```

  - 次に、svcs -l コマンドとその出力の例を示します。

```
$ svcs -l /network/nis/client
fmri         svc:/network/nis/client:default
name         NIS (YP) client
enabled      true
state        online
next_state   none
state_time   Tue Aug 23 19:23:28 2011
logfile      /var/svc/log/network-nis-client:default.log
restarter    svc:/system/svc/restarter:default
contract_id  88
manifest     /lib/svc/manifest/network/nis/client.xml
manifest     /lib/svc/manifest/network/network-location.xml
manifest     /lib/svc/manifest/system/name-service/upgrade.xml
manifest     /lib/svc/manifest/milestone/config.xml
dependency   require_all/none svc:/system/filesystem/minimal (online)
dependency   require_all/restart svc:/network/rpc/bind (online)
dependency   require_all/restart svc:/network/nis/domain (online)
dependency   optional_all/none svc:/network/nis/server (absent)
dependency   optional_all/none svc:/network/location:default (online)
dependency   optional_all/none svc:/system/name-service/upgrade (online)
dependency   optional_all/none svc:/milestone/config (online)
dependency   optional_all/none svc:/system/manifest-import (online)
dependency   require_all/none svc:/milestone/unconfig (online)
```

  - svccfg ユーティリティーを使用すると、サービスに関するより詳細な情報を取得できます。svccfg(1M) のマニュアルページを参照してください。
  - ps コマンドを使用して、デーモンの存在を確認できます。

```
$ ps -ef |grep ypbind
daemon 100813   1   0   Aug 23 ?     0:00 /usr/lib/netsvc/yp/ypbind -broadcast
```

NIS ドメインの設計

NIS サーバーまたはクライアントとしてマシンを構成する前に、NIS ドメインを設計する必要があります。

まず、NIS ドメインに入れるマシンを決めます。NIS ドメインが DNS ドメインをミラー化する必要はありません。DNS ドメインに複数の NIS ドメインを含めることができ、NIS ドメインの外部にあるマシンが DNS ドメイン内に存在できます。

NIS ドメイン名の最大文字数は 256 です。ドメイン名が 32 文字を超えないように制限するとよいでしょう。NIS ドメイン名では大文字と小文字が区別されます。便宜上、NIS ドメイン名の基礎としてインターネットのドメイン名を使用することを選択できます。NIS ドメイン名には大文字が含まれているが、DNS ドメイン名には含まれていない場合、ユーザーが混乱する可能性があるので注意してください。たとえば、インターネットのドメイン名が `example.com` である場合は、NIS ドメインの名前も `example.com` にすることができます。`example.com` を 2 つの NIS ドメインに (たとえば、1 つを営業部門に、もう 1 つを製造部門に) 分割する場合は、1 つのドメインの名前を `sales.example.com` に、もう 1 つのドメインの名前を `manf.example.com` にすることができます。

注 – 分割された NIS ドメインのマージや管理は非常に困難な場合があるため、NIS ドメインを分割する十分な理由があることを確認してください。

マシンが NIS サービスを使用するには、その前に正しい NIS ドメイン名とマシン名が設定されている必要があります。マシンの名前は、`hostname` コマンドによって設定されます。マシンのドメイン名は、`domainname` コマンドによって設定されます。`hostname` および `domainname` コマンドを使用すると、マシン名と NIS ドメイン名を表示できます。

NIS サーバーとクライアントを特定する

マスターサーバーになるマシンを 1 つ選択します。どのマシンをスレーブサーバーにするかを決定します。

NIS クライアントになるマシンを決定します。通常は、NIS ドメイン内のすべてのマシンが NIS クライアントとして設定されますが、これは必須ではありません。

マスターサーバーの準備

以降のセクションでは、マスターサーバーのソースファイルと passwd ファイルを準備する方法を説明します。

ソースファイルのディレクトリ

ソースファイルは通常、マスターサーバー上の /etc ディレクトリ内にあります。ただし、マップの内容がマスターサーバー上のローカルファイルの内容と同じになるため、ソースファイルを /etc に置いたままにしておくことはお勧めできません。すべてのユーザーがマスターサーバーのマップにアクセスでき、root パスワードが passwd マップを通してすべての NIS クライアントに渡されるため、これは passwd および shadow ファイルの特殊な問題です。詳細は、83 ページの「passwd ファイルと名前空間のセキュリティー」を参照してください。

ただし、ソースファイルをほかのディレクトリに入れた場合は、/var/yp 内の Makefile の DIR=/etc 行を DIR=/*your-choice* に変更する必要があります。*your-choice* はソースファイルを格納するためのディレクトリの名前です。これによって、サーバー上のローカルファイルをクライアント上のファイルのように扱うことができます。(最初に、元の Makefile のコピーを保存することをお勧めします。)

さらに、audit_user、auth_attr、exec_attr、および prof_attr NIS マップを、デフォルト以外のディレクトリから作成するようにしてください。RBACDIR =/*etc/security* を *RBACDIR=/your-choice* に変更することによって /var/yp/Makefile を修正します。

passwd ファイルと名前空間のセキュリティー

セキュリティー上の理由から未承認の root アクセスを防ぐために、NIS のパスワードマップの構築に使用されるファイルには root のエントリを含めないでください。このため、パスワードマップはマスターサーバーの /etc ディレクトリに置かれたファイルから構築しないでください。パスワードマップを構築するために使用されるパスワードファイルは、そこから root エントリを削除し、未承認のアクセスから保護できるディレクトリ内に配置するようにしてください。

たとえば、マスターサーバーのパスワード入力ファイルは、ファイル自体が別のファイルへのリンクではなく、ファイルの場所が Makefile に指定されている限り、/var/yp/ などのディレクトリに格納されているか、選択したディレクトリに格納されている必要があります。Makefile で指定された構成に従って、正しいディレクトリオプションが自動的に設定されます。

注意 – PWDDIR で指定されたディレクトリ内の passwd ファイルに root のエントリが含まれていないことを確認してください。

ソースファイルが /etc 以外のディレクトリ内に存在する場合は、/var/yp/Makefile 内の PWDIR パスワードマクロを、passwd および shadow ファイルが存在するディレクトリを参照するように変更する必要があります。PWDIR=/etc の行を PWDIR=/*your-choice* に変更します。ここで、*your-choice* は、passwd マップのソースファイルを格納するために使用するディレクトリの名前です。

▼ 変換用のソースファイルを準備する方法

この手順では、NIS マップへの変換のためのソースファイルを準備する方法について説明します。

1. 管理者になります。

   詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2. マスターサーバー上のソースファイルをチェックして、そこにシステムが反映されていることを確認します。

   次のファイルを確認します。

   - audit_user
   - auth_attr
   - auto.home または auto_home
   - auto.master または auto_master
   - bootparams
   - ethers
   - exec_attr
   - group
   - hosts
   - ipnodes
   - netgroup
   - netmasks
   - networks
   - passwd
   - protocols
   - rpc
   - service
   - shadow
   - user_attr

3 これらのすべてのソースファイル (**passwd** と **shadow** を除く) を、選択したソースディレクトリにコピーします。

ソースディレクトリは、DIR マクロによって /var/yp/Makefile で定義されています。

4 **passwd** および **shadow** ファイルを、選択したパスワードのソースディレクトリにコピーします。

パスワードのソースディレクトリは、PWDIR マクロによって Makefile で定義されています。

5 **audit_user**、**auth_attr**、**exec_attr**、および **prof_attr** ファイルを、選択した **RBAC** のソースディレクトリにコピーします。

RBAC のソースディレクトリは、RBACDIR マクロによって /var/yp/Makefile で定義されています。必要に応じて、auth_attr ファイルをコピーする前に、/etc/security/auth_attr.d ディレクトリ内のファイルの内容をそのファイルのコピーにマージします。同様に、必要に応じて、exec_attr.d および prof_attr.d ディレクトリ内のファイルを exec_attr と prof_attr に結合します。

注意 – これらのファイルは、システムがアップグレードされるときは常に再マージする必要があるため、これらのローカルファイルを /etc/security/*.d ディレクトリ内のリリースファイルとは別に保管してください。

6 **/etc/mail/aliases** ファイルを確認します。

ほかのソースファイルとは異なり、/etc/mail/aliases ファイルは別のディレクトリに移動できません。このファイルは /etc/mail ディレクトリに格納されていなければなりません。詳細は、aliases(4) のマニュアルページを参照してください。

注 – /var/yp/Makefile 内の ALIASES = /etc/mail/aliases エントリが別の場所を指すようにすることによって、NIS 固有のメールエイリアスファイルを追加できます。そのあとに make コマンドを実行すると、ALIASES エントリによって mail.aliases マップが作成されます。/etc/nsswitch.conf ファイルで files に加えて nis が正しく指定されている場合、sendmail サービスは、/etc/mail/aliases ファイルに加えてこのマップを使用します。107 ページの「/var/yp/Makefile の変更および使用」を参照してください。

7 ソースファイルからすべてのコメントと、その他の余計な行や情報を取り除きます。

これらの操作は、sed や awk のスクリプトか、またはテキストエディタを使用して実行できます。/var/yp/Makefile は一部のファイルクリーニングを自動的に実行しますが、make コマンドを実行する前に、これらのファイルを手動で調べてクリーンアップすることをお勧めします。

8 すべてのソースファイルのデータが正しい形式になっていることを確認します。

ソースファイルのデータは、その特定のファイルに適した形式になっている必要があります。該当するマニュアルページを参照して、各ファイルが正しい形式になっていることを確認します。

/var/yp/Makefile の準備

ソースファイルをチェックしてソースファイルのディレクトリにコピーしたら、次に、これらのソースファイルを NIS サービスが使用する ndbm 形式のマップに変換する必要があります。87 ページの「マスターサーバーを設定する方法」で説明されているように、これは、マスターサーバー上で呼び出されると ypinit によって自動的に実行されます。

ypinit スクリプトは、/var/yp/Makefile を使用する make プログラムを呼び出します。このファイルのデフォルトのコピーが /var/yp ディレクトリに用意されており、このコピーには、ソースファイルを目的の ndbm 形式のマップに変換するために必要なコマンドが含まれています。

デフォルトの Makefile はそのまま使用することも、変更することもできます。デフォルトの Makefile を変更する場合は、将来使用する場合の必要に備えて、必ず最初に元のデフォルトの Makefile をコピーして保管するようにしてください。次に説明する Makefile への修正のうち、必要に応じて 1 つまたは複数を実行します。

- デフォルト以外のマップ

  独自のデフォルト以外のソースファイルを作成しており、それを NIS マップに変換する場合は、これらのソースファイルを Makefile に追加する必要があります。

- DIR 値

  83 ページの「ソースファイルのディレクトリ」で説明しているように、/etc 以外のディレクトリに格納されたソースファイルを Makefile で使用する場合は、Makefile の DIR の値を、使用するディレクトリに変更してください。Makefile 内のこの値を変更する場合は、その行をインデントしないでください。

- PWDIR 値

  Makefile で、/etc 以外のどこかのディレクトリ内に格納されている passwd、shadow、および adjunct ソースファイルを使用する場合は、Makefile 内の PWDIR の値を、使用するディレクトリに変更する必要があります。Makefile 内のこの値を変更する場合は、その行をインデントしないでください。

- RBACDIR 値

Makefile で、/etc 以外のどこかのディレクトリ内に格納されている audit_user、auth_attr、exec_attr、および prof_attr ソースファイルを使用する場合は、Makefile 内の RBACDIR の値を、使用するディレクトリに変更する必要があります。Makefile 内のこの値を変更する場合は、その行をインデントしないでください。

- ドメインネームリゾルバ

  NIS サーバーで、現在のドメイン内にないマシンのためにドメインネームリゾルバを使用する場合は、Makefile の行 B= をコメントアウトし、行 B=-b をコメント解除 (有効に) します。

Makefile の機能は、all の下にリストされている各データベースの適切な NIS マップを作成することです。データは makedbm を通過したあと、mapname.dir と mapname.pag の 2 つのファイル内に収集されます。このどちらのファイルも、マスターサーバー上の /var/yp/*domainname* ディレクトリ内にあります。

Makefile は、必要に応じて、/PWDIR/passwd、/PWDIR/shadow、および /PWDIR/security/passwd.adjunct ファイルから passwd マップを構築します。

▼ NIS マスターサーバーパッケージをインストールする方法

通常、NIS マスターサーバーパッケージは、Oracle Solaris リリースの必要に応じてインストールされます。システムをインストールしたときにこのパッケージが含まれていなかった場合は、次の手順を使用してこのパッケージをインストールします。

1. 管理者になります。

   詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2. NIS マスターサーバーパッケージをインストールします。

```
# pkg install pkg:/service/network/nis
```

▼ マスターサーバーを設定する方法

ypinit スクリプトは、マスターサーバー、スレーブサーバー、およびクライアントを、NIS を使用するように設定します。また、最初に make コマンドを実行して、マスターサーバー上にマップも作成します。

ypinit コマンドを使用して、マスターサーバー上に NIS マップの新しいセットを構築するには、次の手順を完了します。

1 **NIS マスターサーバー上の管理者になります。**

詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2 **`/etc/inet/hosts` ファイルを編集します。**

各 NIS サーバーのホスト名と IP アドレスを追加します。*IPaddress FQDN-hostname aliases* の形式を使用します。

例:

```
129.0.0.1    master.example.com master
129.0.0.2    slave1.example.com slave1
129.0.0.3    slave2.example.com slave2
```

3 **新しいマップをマスターサーバーに作成します。**

```
# /usr/sbin/ypinit -m
```

4 **NIS サーバーの名前を入力します。**

`ypinit` から、NIS スレーブサーバーになるほかのマシンのリストを入力するよう求められたら、作業しているサーバーの名前を、`/etc/inet/hosts` ファイルで指定した NIS スレーブサーバーの名前とともに入力します。

5 **NIS ドメイン名が設定されていることを確認します。**

```
# domainname
example.com
```

6 **`y` を入力して、致命的でないエラーが発生した場合にプロセスを停止することを選択します。**

`ypinit` から、致命的でないエラーが最初に発生したときに手順を終了するか、または致命的でないエラーが発生しても続行するかを尋ねられたら、**`y`** を入力します。**`y`** を選択すると、`ypinit` は最初の問題が発生したときに終了します。その場合は、その問題を解決してから `ypinit` を再起動できます。`ypinit` を初めて実行する場合はこの手順に従うようにしてください。処理を継続する場合は、発生する問題をすべて手動で解決してから `ypinit` を再起動します。

注 – マップファイルの一部が存在しないと、致命的でないエラーが発生することがあります。これは NIS の機能に影響を与えるエラーではありません。マップが自動的に作成されない場合は、必要に応じて手動で追加します。すべてのデフォルトの NIS マップの詳細については、71 ページの「デフォルトの NIS マップ」を参照してください。

---

7 **ソースファイルを削除するかどうかを選択します。**

`ypinit` コマンドから、`/var/yp/`*domain-name* ディレクトリ内の既存のファイルを破棄してもよいかどうか尋ねられます。このメッセージは、NIS が以前に設定されている

場合にだけ表示されます。通常、以前のインストールのファイルをクリーンアップする場合は、ソースファイルを削除することを選択します。

8 **ypinit** コマンドは、サーバーのリストを作成したあと **make** コマンドを起動します。

このプログラムは、`/var/yp` にある `Makefile` (デフォルトファイルまたは変更したファイルのどちらか) に含まれている手順を使用します。`make` コマンドは、指定されたファイルから残っているコメント行をすべて削除します。また、指定したファイルに対して `makedbm` を実行して適切なマップを作成し、各マップにマスターサーバー名を設定します。

`Makefile` によってプッシュされているマップが、マスター上の `domainname` コマンドによって返されたドメイン以外のドメインに対応している場合は、次のように、`ypinit` シェルスクリプト内で変数 `DOM` の正しい ID を指定して `make` を起動することによって、それらのマップが正しいドメインに確実にプッシュされるようにすることができます。

```
# make DOM=domain-name  passwd
```

このコマンドによって、マスターサーバーが属するドメインではなく目的のドメインに `passwd` マップが転送されます。

9 必要に応じて、ネームサービススイッチに変更を加えます。

39 ページの「ネームサービススイッチの管理」を参照してください。

▼ 1 つのマスターサーバー上で複数の NIS ドメインをサポートする方法

通常、NIS マスターサーバーがサポートする NIS ドメインは 1 つだけです。ただし、マスターサーバーを使用して複数のドメインをサポートする場合は、追加のドメインをサポートするようにサーバーを設定するときに、87 ページの「マスターサーバーを設定する方法」で説明されている手順を少し変更する必要があります。

1 NIS マスターサーバー上の管理者になります。

詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2 NIS ドメイン名を変更します。

```
# domainname sales.example.com
```

3 NIS ファイルを作成します。

```
# make DOM=sales.example.com
```

NIS サーバー上の NIS サービスの起動と停止

これでマスターのマップが作成されたため、マスターサーバー上の NIS デーモンを起動してサービスを開始できます。NIS サービスを有効にすると、サーバー上で ypserv および ypbind デーモンが起動します。クライアントがサーバーに情報をリクエストした場合、クライアントからの情報リクエストを NIS マップ内で検索したあと、それに応答するデーモンは ypserv です。ypserv および ypbind デーモンは、1 単位として管理されます。

次に、サーバー上で NIS サービスを起動または停止するための 3 つの方法を示します。

- NIS サービスが以前に有効になっていた場合は、ブートプロセス中に SMF サービスが NIS サービスを自動的に起動します。
- svcadm enable *fmri* および svcadm disable *fmri* コマンドの使用は、推奨される手動の方法です。
- ypstart および ypstop コマンドによって別の手動の方法が提供されますが、SMF を使用して NIS サービスを管理できるように、svcadm コマンドを使用することをお勧めします。

NIS サービスの自動起動

svc:/network/nis/server サービス有効になっている場合、ypserv デーモンはブート時に自動的に起動されます。詳細は、87 ページの「マスターサーバーを設定する方法」を参照してください。

▼ NIS サーバーサービスを手動で有効にする方法

svcadm コマンドを使用するとき、サービスの複数のインスタンスを実行している場合のみインスタンス名が必要です。詳細は、80 ページの「NIS とサービス管理機能」または svcadm(1M) のマニュアルページを参照してください。

1. 管理者になります。

   詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2. 必要な NIS サーバーサービスを起動します。

```
# svcadm enable network/nis/domain
# svcadm enable network/nis/server
```

注 – NIS サービスはまた、ypstart コマンドを使用して有効にすることもできますが、svcadm コマンドを使用することをお勧めします。

▼ NIS サーバーサービスを無効にする方法

svcadm コマンドを使用するとき、サービスの複数のインスタンスを実行している場合のみ特定のインスタンス名が必要です。詳細は、80 ページの「NIS とサービス管理機能」または svcadm(1M) のマニュアルページを参照してください。

1. 管理者になります。

   詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2. 必要な NIS サーバーサービスを無効にします。

```
# svcadm disable network/nis/domain
# svcadm disable network/nis/server
```

注 – NIS サービスはまた、ypstop コマンドを使用して無効にすることもできます。

▼ NIS サーバーサービスをリフレッシュする方法

この手順では、構成の変更が行われたあとに NIS サーバーサービスをリフレッシュする方法について説明します。

svcadm コマンドを使用するとき、サービスの複数のインスタンスを実行している場合のみ特定のインスタンス名が必要です。詳細は、80 ページの「NIS とサービス管理機能」または svcadm(1M) のマニュアルページを参照してください。

1. 管理者になります。

   詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2. 必要な NIS サーバーサービスをリフレッシュします。

```
# svcadm refresh network/nis/domain
# svcadm refresh network/nis/server
```

NIS スレーブサーバーの設定

ネットワークは 1 つ以上のスレーブサーバーを持つことができます。スレーブサーバーを持つことで、マスターサーバーが利用できない場合にも NIS サービスを継続して利用できます。

スレーブサーバーを準備する

実際に `ypinit` コマンドを実行してスレーブサーバーを作成する前に、まず `svc:/network/nis/domain` サービスが構成されていることを確認してください。

注 – NIS ドメイン名は大文字と小文字が区別されますが、DNS ドメイン名は区別されません。

NIS スレーブサーバーを構成する前に、ネットワークが適切に機能していることを確認してください。特に、`sshd` コマンドを使用して NIS マスターサーバーから NIS スレーブにファイルを送信できることを確認してください。

▼ スレーブサーバーを設定する方法

次の手順では、スレーブサーバーを設定する方法について説明します。この手順を、NIS スレーブサーバーとして構成するマシンごとに繰り返してください。

1. 管理者になります。

   詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2. **`/etc/inet/hosts` ファイルを編集します。**

   ほかの各 NIS サーバーの名前と IP アドレスを追加します。*IPaddress FQDN-hostname aliases* の形式を使用します。

   例:

   ```
   129.0.0.1    master.example.com master
   129.0.0.2    slave1.example.com slave1
   129.0.0.3    slave2.example.com slave2
   ```

3. スレーブサーバー上の **`/var/yp`** ディレクトリに移動します。

注 – まず、新しいスレーブサーバーを NIS クライアントとして構成して、最初にマスターサーバーから NIS マップを取得できるようにする必要があります。詳細は、96 ページの「NIS クライアントの管理」を参照してください。

4 スレーブサーバーを **NIS** クライアントとして初期化します。

```
# /usr/sbin/ypinit -c
```

ypinit コマンドによって、NIS サーバーのリストを求めるプロンプトが表示されます。まず、作業しているローカルスレーブの名前を入力してから、マスターサーバーの名前のあとに、ドメイン内のほかの NIS スレーブサーバーの名前を入力します。ほかのスレーブサーバーについては、ネットワーク的に物理的にもっとも近いものからもっとも遠いものへの順序に従います。

5 クライアントサービスが実行されているかどうかを判定してから、必要に応じてサービスを起動または再起動します。

```
# svcs \*nis\*
STATE          STIME     FMRI
online         20:32:56  svc:/network/nis/domain:default
online         20:32:56  svc:/network/nis/client:default
```

サービスが online の状態で表示される場合、NIS は実行されています。サービス状態が disabled である場合、NIS は実行されていません。

a. クライアントサービスが実行されている場合は、クライアントサービスを再起動します。

```
# svcadm restart network/nis/domain
# svcadm restart network/nis/client
```

b. クライアントサービスが実行されていない場合は、クライアントサービスを起動します。

```
# svcadm enable network/nis/domain
# svcadm enable network/nis/client
```

6 **NIS** マスターサーバーが実行されているかどうかを判定してから、必要に応じてサービス起動または再起動します。

```
# svcs network/nis/server
STATE          STIME     FMRI
offline        20:32:56  svc:/network/nis/server:default
```

a. **NIS** マスターサーバーが実行されている場合は、サービスを再起動します。

```
# svcadm restart network/nis/server
```

b. **NIS** マスターサーバーが実行されていない場合は、サービスを起動します。

```
# svcadm enable network/nis/server
```

7 このマシンをスレーブサーバーとして初期化します。

```
# /usr/sbin/ypinit -s master
```

ここで、*master* は既存の NIS マスターサーバーのマシン名です。

▼ スレーブサーバーで NIS を開始する方法

次の手順では、スレーブサーバー上で NIS を起動する方法について説明します。

1 管理者になります。

詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2 クライアントサービスを再起動し、すべての NIS サーバープロセスを起動します。

```
# svcadm restart network/nis/domain
# svcadm restart network/nis/client
# svcadm enable network/nis/server
```

▼ 新しいスレーブサーバーを追加する方法

NIS が実行されたあと、`ypinit` コマンドに指定した最初のリストに含めなかった NIS スレーブサーバーの作成が必要になることがあります。新しい NIS スレーブサーバーを追加するには、この手順を使用します。

1 NIS マスターサーバー上の管理者になります。

詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2 NIS ドメインディレクトリに移動します。

```
# cd /var/yp/domainname
```

3 **ypservers** ファイルを分解します。

```
# makedbm -u ypservers >/tmp/temp_file
```

`makedbm` コマンドは、`ypservers` を `ndbm` 形式から一時的な ASCII ファイル `/tmp/temp_file` に変換します。

4 **/tmp/temp_file** ファイルを編集します。

つまり、新しいスレーブサーバー名をサーバーリストに追加します。そのあと、このファイルを保存して閉じます。

5 入力ファイルとして **temp_file** を、出力ファイルとして **ypservers** を指定して **makedbm** コマンドを実行します。

```
# makedbm /tmp/temp_file ypservers
```

これにより、makedbm コマンドは ypservers を変換して ndbm 形式に戻します。

6 **ypservers** マップが正しいことを確認します。

ypservers の ASCII ファイルは存在しないため、スレーブサーバー上で次のように入力します。

```
slave3# makedbm -u ypservers
```

makedbm コマンドは、画面上に ypservers 内の各エントリを表示します。

注 – ypservers にマシン名が存在しない場合は、ypservers はマップファイルの更新を受信しません。これは、yppush がこのマップでスレーブサーバーリストを調べるからです。

---

7 新しい **NIS** スレーブサーバー上の管理者になります。

詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

8 **NIS** ドメイン名が設定されていることを確認します。

```
# domainname
example.com
```

9 新しいスレーブサーバーの **NIS** ドメインディレクトリを設定します。

マスターサーバーから NIS マップセットをコピーしてから、NIS クライアントを起動します。ypinit コマンドを実行するときは、プロンプトに従って、NIS サーバーを優先順にリストします。

```
slave3# cd /var/yp
slave3# ypinit -c
```

10 このマシンをスレーブサーバーとして初期設定します。

```
slave3# /usr/sbin/ypinit -s ypmaster
```

ypmaster は、既存の NIS マスターサーバーのマシン名です。

11 **NIS** クライアントとして実行されているマシンを停止します。

```
slave3# svcadm disable network/nis/client
```

12 クライアントサービスが実行されているかどうかを判定してから、必要に応じてサービスを起動または再起動します。

```
# svcs \*nis\*
STATE          STIME     FMRI
online         20:32:56  svc:/network/nis/domain:default
online         20:32:56  svc:/network/nis/client:default
```

サービスが online の状態で表示される場合、NIS は実行されています。サービス状態が disabled である場合、NIS は実行されていません。

a. クライアントサービスが実行されている場合は、クライアントサービスを再起動します。

```
# svcadm restart network/nis/domain
# svcadm restart network/nis/client
```

b. クライアントサービスが実行されていない場合は、クライアントサービスを起動します。

```
# svcadm enable network/nis/domain
# svcadm enable network/nis/client
```

13 NIS サーバーが実行されているかどうかを判定してから、必要に応じてサービスを起動または再起動します。

```
# svcs network/nis/server
STATE          STIME    FMRI
offline        20:32:56  svc:/network/nis/server:default
```

a. NIS サーバーが実行されている場合は、サービスを再起動します。

```
slave3# svcadm restart network/nis/server
```

b. NIS サーバーが実行されていない場合は、サービスを起動します。

```
slave3# svcadm enable network/nis/server
```

NIS クライアントの管理

このセクションでは、ネームサービスとして NIS を使用するようにクライアントマシンを構成するための 2 つの方法について説明します。

注 – Oracle Solaris OS は、NIS クライアントとネイティブな LDAP クライアントが同じクライアントマシン上に共存する構成をサポートしていません。

- ブロードキャストの方法 — NIS を使用するようにクライアントマシンを構成するための推奨される方法です。手順については、97 ページの「ブロードキャストモードで NIS クライアントを構成する方法」を参照してください。
- サーバーリストの方法 — ypinit コマンドを使用してサーバーを指定する、クライアントマシンを構成するための別の方法です。手順については、97 ページの「特定の NIS サーバーを使用して NIS クライアントを構成する方法」を参照してください。

▼ ブロードキャストモードで NIS クライアントを構成する方法

これは、NIS クライアントを確立するための推奨される方法です。

`nis/client` サービスを起動すると、このサービスが `ypbind` コマンドを実行し、これにより NIS サーバーのローカルサブネットが検索されます。サブネットが見つかると、`ypbind` がそこにバインドします。この検索をブロードキャストと呼びます。クライアントのローカルサブネット上に NIS サーバーが存在しない場合は、`ypbind` がバインドに失敗し、クライアントマシンは NIS サービスから名前空間データを取得できません。手順については、97 ページの「特定の NIS サーバーを使用して NIS クライアントを構成する方法」を参照してください。

1. 管理者になります。

   詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2. NIS ドメイン名を設定します。

   ```
   # domainname example.com
   ```

3. 必要に応じて、ネームサービススイッチに変更を加えます。

   39 ページの「ネームサービススイッチの管理」を参照してください。

4. NIS クライアントサービスを起動します。

   ```
   # svcadm enable network/nis/domain
   # svcadm enable network/nis/client
   ```

▼ 特定の NIS サーバーを使用して NIS クライアントを構成する方法

始める前に　次の手順では、手順 3 で入力されるホスト名を DNS が解決できることが必要です。DNS を使用していない場合や、IP アドレスの代わりにホスト名を入力する場合は、クライアント上の `/etc/hosts` ファイルに各 NIS サーバーの適切なエントリを必ず追加してください。詳細は、`ypinit(1M)` のマニュアルページを参照してください。

1. 管理者になります。

   詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2 NIS ドメイン名を設定します。

```
# domainname example.com
# svcadm enable network/nis/domain
```

3 クライアント構成スクリプトを実行します。

```
# ypinit -c
```

クライアントがネームサービス情報を取得する元の NIS サーバーを指定するよう求められます。マスターサーバーと、必要な数のスレーブサーバーをリストできます。指定するサーバーはドメイン内のどこにあってもかまいません。最初に、マシンに (ネットワーク的に) もっとも近いサーバーをリストし、次にネットワークのより遠い部分に存在するサーバーをリストすることをお勧めします。

▼ NIS クライアントサービスの無効化

1 管理者になります。

詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2 NIS クライアントサービスを無効にします。

```
# svcadm disable network/nis/domain
# svcadm disable network/nis/client
```

◆ ◆ ◆ 第 7 章

NIS の管理 (タスク)

この章では、NIS の管理方法について説明します。次の項目について説明します。

注 – NIS サービスはサービス管理機能によって管理されます。このサービスに関する有効化、無効化、再起動などの管理アクションは `svcadm` コマンドを使用して実行できます。NIS で SMF を使用する場合の詳細については、80 ページの「NIS とサービス管理機能」を参照してください。SMF の概要については、『Oracle Solaris 11.1 でのサービスと障害の管理』の第 1 章「サービスの管理 (概要)」を参照してください。また、詳細については `svcadm(1M)` および `svcs(1)` のマニュアルページも参照してください。

NIS サービスはまた、`ypstart` および `ypstop` コマンドを使用して起動および停止することもできます。詳細は、`ypstart(1M)` および `ypstop(1M)` のマニュアルページを参照してください。

パスワードファイルと名前空間のセキュリティー

セキュリティーの関係上、次のガイドラインに従ってください。

- マスターサーバーの NIS マップへのアクセスは制限します。
- 未承認のアクセスから保護するために、NIS パスワードマップを構築するために使用されるファイルに `root` のエントリを含めてはいけません。これを実現するために、パスワードマップを構築するために使用されるパスワードファイルは、そ

こから root エントリを削除し、マスターサーバーの /etc ディレクトリ以外のディレクトリ内に配置するようにしてください。このディレクトリへの未許可アクセスは、防止しなければなりません。

たとえば、マスターサーバーのパスワード入力ファイルは、そのファイル自体が別のファイルへのリンクではなく、Makefile で指定されているかぎり、/var/yp などのディレクトリや、選択した任意のディレクトリ内に格納できます。サービス管理機能または ypstart スクリプトのどちらかを使用して NIS サービスを起動すると、Makefile で指定された構成に従って、正しいディレクトリオプションが設定されます。

注 – 古い Solaris 1 バージョンの passwd ファイルの形式に加えて、この NIS の実装では、NIS パスワードマップを構築するための入力として Solaris 2 の passwd および shadow ファイルの形式を受け入れます。

NIS ユーザーの管理

このセクションでは、ユーザーパスワードの設定、NIS ドメインへの新しいユーザーの追加、およびネットグループへのユーザーの割り当てについて説明します。

▼ NIS ドメインに新しい NIS ユーザーを追加する方法

1 **NIS マスターサーバー上の管理者になります。**

詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2 **useradd コマンドを使用して、新しいユーザーのログイン ID を作成します。**

```
# useradd userID
```

ここで、*userID* は新しいユーザーのログイン ID です。このコマンドは、NIS マスターサーバー上の /etc/passwd および /etc/shadow ファイル内にエントリを作成します。

3 新しいユーザーの初期パスワードを作成します。

新しいユーザーがログインするための初期パスワードを作成するには、passwd コマンドを実行します。

```
# passwd userID
```

ここで、*userID* は新しいユーザーのログイン ID です。このユーザーに割り当てるパスワードを入力するようにプロンプトが表示されます。

この手順が必要なのは、useradd コマンドによって作成されたパスワードエントリがロックされており、新しいユーザーがログインできないためです。初期パスワードを指定することで、このパスワードエントリのロックが解除されます。

4 新しいエントリをマスターサーバーの **passwd** マップ入力ファイルにコピーします。

マスターサーバー上のマップソースファイルは、/etc 以外のディレクトリにあります。/etc/passwd および /etc/shadow ファイルの新しい行をサーバー上の passwd マップ入力ファイルにコピー&ペーストします。詳細については、99 ページの「パスワードファイルと名前空間のセキュリティー」を参照してください。

たとえば、新しいユーザー brown を追加した場合は、passwd 入力ファイルにコピーする /etc/passwd の行は次のようになります。

```
brown:x:123:10:User brown:/home/brown:/bin/csh:
```

/etc/shadow からコピーする brown の行は次のようになります。

```
brown:$5$YiFpYWXb$6jJkG/gKdfkKtlTbemORnbeH.qsvO9MwBD3ulTihq9B:6445::::::
```

5 パスワード入力ファイルが格納されているディレクトリが **Makefile** で正しく指定されていることを確認します。

6 **/etc/passwd** および **/etc/shadow** 入力ファイルから、新しいユーザーのエントリを削除します。

セキュリティー上の理由から、NIS マスターサーバーの /etc/passwd および /etc/shadow ファイル内にユーザーエントリを保持しないでください。ほかのディレクトリに存在する NIS マップソースファイルに新しいユーザーのエントリをコピーしたあと、マスターサーバー上で userdel コマンドを使用して新しいユーザーを削除します。

たとえば、マスターサーバーの /etc ファイルから新しいユーザー brown を削除するには次のように入力します。

```
# userdel brown
```

userdel についての詳細は、userdel(1M) のマニュアルページを参照してください。

7 **NIS の passwd** マップを更新します。

マスターサーバー上の passwd 入力ファイルを更新したら、ソースファイルを含むディレクトリ内で make を実行することによって passwd マップを更新します。

```
# userdel brown
# cd /var/yp
# make passwd
```

8 新しいユーザーのログイン **ID** に割り当てられた初期パスワードを新しいユーザーに通知します。

ログイン後、新しいユーザーはいつでも passwd を実行して別のパスワードに変更できます。

ユーザーパスワードの設定

ユーザーは、passwd を実行して自分のパスワードを変更します。

% **passwd** *username*

パスワードファイルを更新するために、ユーザーが自分のパスワードを変更する前にマスターサーバー上で rpc.yppasswdd デーモンを起動する必要があります。

rpc.yppasswdd デーモンは、マスターサーバー上で自動的に起動します。rpc.yppasswdd に -m オプションが指定されていると、ファイルが変更されたあと、ただちに /var/yp 内で make コマンドが実行されます。passwd ファイルが変更されるたびに make コマンドが実行されることを回避する場合は、ypstart スクリプト内の rpc.yppasswd コマンドから -m オプションを削除し、passwd マップのプッシュを crontab ファイルによって制御します。

NIS ネットグループ

NIS ネットグループは、NIS 管理者が管理目的のために定義するユーザーまたはマシンのグループ (集合) です。たとえば、次のようなネットグループを作成できます。

- 特定マシンにアクセスできる一群のユーザーを定義する
- 特定のファイルシステムにアクセスできる一群の NFS クライアントマシンを定義する
- 特定の NIS ドメインのすべてのマシンに対して管理者権限を持つ一群のユーザーを定義する

各ネットグループには、1 つのネットグループ名が与えられます。ネットグループはアクセス権を直接設定しません。代わりに、ユーザー名またはマシン名が一般に使用される場所ではネットグループ名がほかの NIS マップで使用されます。たとえば、netadmins という名前のネットワーク管理者のネットグループを作成したとします。netadmins ネットグループのすべてのメンバーに特定のマシンへのアクセス権を付与するには、そのマシンの /etc/passwd ファイルに netadmin エントリを追加するだけで済みます。ネットグループ名を /etc/netgroup ファイルに追加して、NIS グループマップに追加することもできます。ネットグループの使用についての詳細は、netgroup(4) のマニュアルページを参照してください。

NIS を使用しているネットワーク上では、NIS マスターサーバー上の netgroup 入力ファイルを使用して、netgroup、netgroup.byuser、netgroup.byhost の 3 つのマップが生成されます。netgroup マップには、netgroup 入力ファイル内の基本情報が含まれています。ほかの 2 つの NIS マップには、マシン名またはユーザー名が指定されると、ネットグループ情報の検索が高速化される形式で情報が含まれています。

netgroup 入力ファイル内のエントリの形式は *name ID* です。ここで、*name* はネットグループに付ける名前であり、*ID* はネットグループに属するマシンまたはユーザーを識別します。ネットグループの ID (メンバー) は、コンマで区切っていく

つでも指定できます。たとえば、3 つのメンバーを含むネットグループを作成する場合、netgroup 入力ファイルのエントリは *name ID, ID, ID* という形式になります。netgroup 入力ファイルのエントリ内のメンバー ID の形式は次のようになります。

```
([-|machine], [-|user], [domain])
```

ここで、*machine* はマシン名、*user* はユーザー ID、*domain* はマシンまたはユーザーの NIS ドメインです。「ドメイン」エレメントは任意指定ですが、ほかの NIS ドメインのマシンまたはユーザーを示す場合には必ず指定します。各メンバーのエントリの *machine* と *user* の要素は必須ですが、空を示すにはダッシュ (-) が使用されます。エントリでは、「マシン」エレメントと「ユーザー」エレメントの関係を示す必要はありません。

次に、netgroup 入力ファイルの 2 つのサンプルエントリを示します。これらの各サンプルエントリでは、リモートドメイン sales に存在するユーザー hauri および juanita と、マシン altair および sirius で構成された admins という名前のネットグループを作成します。

```
admins (altair, hauri), (sirius,juanita,sales)
admins (altair,-), (sirius,-), (-,hauri), (-,juanita,sales)
```

さまざまなプログラムが、ログイン、リモートマウント、リモートログイン、およびリモートシェル作成中のアクセス許可のチェックのためにネットグループの NIS マップを使用します。これらのプログラムには、mountd や login が含まれます。login コマンドは、passwd データベース内でネットグループ名を見つけた場合に、ネットグループマップでユーザー分類を調べます。mountd デーモンは、/etc/dfs/dfstab ファイル内にネットグループ名を検出すると、マシンの分類のためにネットグループマップを参照します。実際、ruserok インタフェースを使用するプログラムはすべて、/etc/hosts.equiv または .rhosts ファイル内にネットグループ名を検出すると、マシンとユーザーの両方の分類のためにネットグループマップをチェックします。

ネットワークに新しい NIS ユーザーまたはマシンを追加する場合は、netgroup 入力ファイルの該当ネットグループに追加してください。次に、make でネットグループマップを作成し、これを yppush コマンドですべての NIS サーバーに転送してください。ネットグループおよびネットグループ入力ファイルの構文の使用についての詳細は、netgroup(4) のマニュアルページを参照してください。

NIS マップに関する作業

このセクションには次の情報が含まれます。

マップ情報の取得

ユーザーは、ypcat、ypwhich、および ypmatch コマンドを使用して、マップの情報やマップに関する情報をいつでも取得できます。以降の例では、*mapname* はマップの正式な名前とそのニックネーム (存在する場合) の両方を指します。

マップ内のすべての値を一覧表示するには、次のように入力します。

```
% ypcat mapname
```

マップ内の鍵と値 (存在する場合) の両方を一覧表示するには、次のように入力します。

```
% ypcat -k mapname
```

マップのすべてのニックネームを一覧表示するには、次のいずれかのコマンドを入力します。

```
% ypcat -x
% ypmatch -x
% ypwhich -x
```

使用可能なすべてのマップとそのマスターを一覧表示するには、次のように入力します。

```
% ypwhich -m
```

特定のマップのマスターサーバーを一覧表示するには、次のように入力します。

```
% ypwhich -m mapname
```

鍵をマップ内のエントリと照合するには、次のように入力します。

```
% ypmatch key mapname
```

探している項目がマップ内の鍵でない場合は、次のように入力します。

```
% ypcat mapname | grep item
```

item は検索している情報です。ほかのドメインに関する情報を取得するには、これらのコマンドの `-d domainname` オプションを使用します。

デフォルト以外のドメインの情報をリクエストしているマシンに、リクエストしたドメインのバインドがない場合、`ypbind` は、`/var/yp/binding/`*domainname*`/ypservers` ファイルを参照してそのドメインのサーバーのリストを探します。このファイルが存在しない場合、ypbind は RPC ブロードキャストを送出してサーバーを検索します。この場合、検索先であるドメインのサーバーは要求元マシンと同じサブネットに存在している必要があります。

マップのマスターサーバーの変更

選択したマップのマスターサーバーを変更するには、まず新しい NIS マスター上にマップを構築する必要があります。古いマスターサーバー名は既存のマップ内に鍵と値のペアとして現れるため (このペアは `makedbm` によって自動的に挿入されます)、新しいマスターにマップをコピーしたり、`ypxfr` を使用して新しいマスターにコピーを転送したりするだけでは不十分です。鍵と新しいマスターサーバー名との対応づけをし直す必要があります。マップに ASCII ソースファイルが存在する場合は、このファイルを新しいマスターサーバーにコピーします。

▼ マップのマスターサーバーを変更する方法

1. **NIS マスターサーバー上の管理者になります。**

   詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2. **ディレクトリを変更します。**

   ```
   newmaster# cd /var/yp
   ```

3. **作成するマップを指定する前に、`/var/yp/Makefile` に新しいマップのエントリが存在する必要があります。**

   そうでない場合は、ここで `Makefile` を編集します。この例では、`sites.byname` という名前のマップのエントリを追加します。

4. **マップを更新または再作成するには、次のように入力します。**

   ```
   newmaster# make sites.byname
   ```

5. **古いマスターが NIS サーバーとして残っている場合は、古いマスターにリモートログイン (`ssh`) して `/var/yp/Makefile` を編集します。**

   `sites.byname` マップを作成した `Makefile` のセクションをコメントアウトして、そのマップがもうそこで作成されないようにしてください。

6 **sites.byname** が **ndbm** ファイルとしてのみ存在する場合は、新しいマスターサーバー上でそれを再作成します。

まず、ypcat コマンドを使用して、sites.byname ファイルのコピーを分解します。次に、makedbm を使用して、分解されたバージョンを実行します。

```
newmaster# cd /var/yp
newmaster# ypcat sites.byname | makedbm domain/sites.byname
```

新しいマスター上にマップを作成したあと、新しいマップのコピーをほかのスレーブサーバーに送信する必要があります。yppush を使用しないでください。これを使用すると、ほかのスレーブは新しいマスターではなく、古いマスターから新しいコピーを取得しようとします。このような動作を回避するには、一般にマップのコピーを新しいマスターサーバーから古いマスターサーバーに送り返すという方法が使用されます。これを行うには、古いマスターサーバーでスーパーユーザーになるか、同等の役割になり、次のように入力します。

```
oldmaster# /usr/lib/netsvc/yp/ypxfr -h newmaster sites.byname
```

これで、yppush を使用できます。スレーブサーバーは古いマスターサーバーを現行のマスターサーバーとして認識しているので、マップの現行バージョンを古いマスターサーバーから取得しようとします。クライアントがこの処理を行うときは、新しいマスターサーバーが現行のマスターサーバーとして指定されている新しいマップを取得します。

この方法が失敗した場合は、各 NIS サーバーに root としてログインし、上に示すように ypxfr コマンドを実行することができます。

構成ファイルの変更

NIS は設定ファイルを正確に構文解析します。このため NIS 管理は容易になりますが、設定ファイルおよび構成ファイルにおける変更により、NIS の動作は影響を受けます。

次のいずれかを実行する場合は、このセクションの手順を使用します。

- /var/yp/Makefile による、サポートされるマップの追加または削除
- C2 セキュリティーを許可または拒否するための $PWDIR/security/passwd.adjunct の追加または削除 ($PWDIR は /var/yp/Makefile で定義されます)

▼ 構成ファイルを更新する方法

次の点に注意してください。

- NIS マスターサーバーからマップまたはソースファイルを削除しても、スレーブサーバー上の対応するマップまたはソースファイルは自動的には削除されません。スレーブサーバー上の対応するマップまたはソースファイルの削除は、NIS 管理者が手作業で行う必要があります。

- 新しいマップは、自動的には既存のスレーブサーバーに転送されません。新しいマップを既存のスレーブサーバーに転送するには、NIS 管理者がそのスレーブサーバーで `ypxfr` を実行してください。

1 管理者になります。

詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2 NIS サーバーを停止します。

```
# svcadm disable network/nis/server
```

3 必要に応じてファイルを変更します。

4 NIS サーバーを起動します。

```
# svcadm enable network/nis/server
```

`/var/yp/Makefile` の変更および使用

`/var/yp` で提供されたデフォルトの `Makefile` を更新することにより、NIS 管理者のニーズを満たすことができます。マップを追加したり削除したり、一部のディレクトリの名前を変更できます。

ヒント – 将来の参照のために、変更していない、元の `Makefile` のコピーを保存しておいてください。

`Makefile` での作業

新しい NIS マップを追加するには、そのマップの `ndbm` ファイルのコピーを、ドメイン内の各 NIS サーバー上の `/var/yp/`*domainname* ディレクトリに取得する必要があります。通常これは、`Makefile` によって行われます。どの NIS サーバーをそのマップのマスターにするかを決定したあと、マップを容易に再構築できるように、マスターサーバー上の `Makefile` を変更します。異なるサーバーを異なるマップのマスターサーバーとして設定することも可能ですが、このようにするとたいていの場合、管理上の混乱を招きます。したがって、1 つのサーバーだけをすべてのマップのマスターサーバーとして設定するようにしてください。

通常、人間が読める形式のテキストファイルは、`makedbm` への入力に適したものにするために `awk`、`sed`、または `grep` によってフィルタリングされます。デフォルトの `Makefile` を参照してください。`make` コマンドに関する一般情報については、`make(1S)` を参照してください。

`make` が認識する依存関係の作成方法を決定する場合は、`Makefile` にすでに用意されているメカニズムを使用します。`make` では、依存ルール内の行の始まりにタブが存

在するか否かが重要であることに注意してください。ほかの設定が正しくても、タブが存在しないというだけでエントリが無効になることがあります。

Makefile にエントリを追加する場合は、次の作業を行なってください。

- データベース名を all ルールに追加する
- time ルールを作成する
- データベースのルールを追加する

たとえば、Makefile をオートマウンタ入力ファイルで動作させるには、auto_direct.time および auto_home.time マップを NIS データベースに追加する必要があります。

これらのマップを NIS データベースに追加するには、Makefile を変更する必要があります。

Makefile のマクロおよび変数の変更

Makefile の先頭で定義されている変数の設定は、等号 (=) の右側にある値を変更することによって変更できます。たとえば、マップへの入力として /etc にあるファイルを使用せず、代わりに /var/etc/domainname などの別のディレクトリにあるファイルを使用する場合は、DIR を DIR=/etc から DIR=/var/etc/*domainname* に変更するようにしてください。また、PWDIR も PWDIR=/etc から PWDIR=/var/etc/*domainname* に変更するようにしてください。

これらの変数を次に示します。

- *DIR*= passwd と shadow を除く、すべての NIS 入力ファイルを含むディレクトリ。デフォルト値は /etc です。マスターサーバーの /etc ディレクトリのファイルを NIS 入力ファイルとして使用することは望ましくないので、この値は変更しなければなりません。
- *PWDIR*= passwd と shadow の NIS 入力ファイルを含むディレクトリ。マスターサーバーの /etc ディレクトリのファイルを NIS 入力ファイルとして使用することは望ましくないので、この値は変更しなければなりません。
- *DOM*= NIS ドメイン名。DOM のデフォルト値は、domainname コマンドを使用して設定できます。

Makefile エントリの変更

次の手順では、Makefile にデータベースを追加したり削除したりする方法を説明します。

▼ 特定のデータベースを使用するように /var/yp/Makefile を変更する方法

この手順を実行するには、NIS マスターサーバーがすでに構成されている必要があります。

1. 管理者になります。

   詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2. **all** という単語で始まる行を、追加したいデータベースの名前を追加することによって変更します。

```
all: passwd group hosts ethers networks rpc services protocols \
    netgroup bootparams aliases netid netmasks \
    audit_user auth_attr exec_attr prof_attr \
  auto_direct auto_home auto_direct.time auto_home.time
```

   エントリの順序は任意ですが、継続行の始まりの空白はスペースではなくタブにしてください。

3. **Makefile** の最後に次の行を追加します。

```
auto_direct: auto_direct.time
auto_home: auto_home.time
```

4. ファイルの途中に **auto_direct.time** のエントリを追加します。

```
auto_direct.time: $(DIR)/auto_direct
 @(while read L; do echo $$L; done < $(DIR)/auto_direct
 $(CHKPIPE)) | \ (sed -e "/^#/d" -e "s/#.*$$//" -e "/^ *$$/d"
 $(CHKPIPE)) | \ $(MAKEDBM) - $(YPDBDIR)/$(DOM)/auto_direct;
 @touch auto_direct.time;
 @echo "updated auto_direct";
 @if [ ! $(NOPUSH) ]; then $(YPPUSH) auto_direct; fi
 @if [ ! $(NOPUSH) ]; then echo "pushed auto_direct"; fi
```

   次に、各変数について説明します。

   - CHKPIPE は、結果を次のコマンドにパイプする前に、パイプ (|) の左側の操作が正常に完了したことを確認します。パイプの左側の動作が正しく行われなかった場合は、「NIS make terminated」というメッセージが表示されてプロセスは終了します。
   - NOPUSH は、makefile が、新しいマップをスレーブサーバーに転送するために yppush を呼び出すことを防止します。NOPUSH が設定されていない場合は、転送は自動的に行われます。

   先頭にある while ループは、入力ファイル内のバックスラッシュで拡張された行をすべて削除するように設計されています。sed スクリプトは、コメントと空の行を削除します。

   ほかのすべてのオートマウンタマップ (auto_home や、ほかのデフォルト以外のすべてのマップなど) でも、同じ手順に従います。

5 **make** コマンドを実行します。

```
# make mapname
```

ここで、*mapname* は作成するマップの名前です。

▼ データベースを削除するために **Makefile** を変更する方法

Makefile で特定データベースのマップを作成しない場合は、Makefile を次のように編集してください。

1 **all** 規則からデータベースの名前を削除します。

2 削除するデータベースのデータベースルールを削除またはコメントアウトします。

たとえば、hosts データベースを削除するには、hosts.time エントリを削除してください。

3 **time** ルールを削除します。

たとえば、hosts データベースを削除するには、hosts: hosts.time エントリを削除してください。

4 マスターサーバーとスレーブサーバーからマップを削除します。

既存のマップの更新

NIS のインストール終了後、頻繁に更新しなければならないマップとまったく更新する必要がないマップがあることに気づく場合があります。たとえば、大企業のネットワークでは passwd.byname マップが頻繁に変更される場合があるのに対して、auto_master マップはほとんど変更されません。

71 ページの「デフォルトの NIS マップ」で説明されているように、デフォルトの NIS マップのデフォルトの場所は、マスターサーバー上の /var/yp/*domainname* 内にあります。ここで、*domainname* は NIS ドメインの名前です。マップを更新する必要がある場合は、マップがデフォルトのマップか否かによって 2 つの更新手順のどちらかを使用できます。

- デフォルトのマップは、ネットワークデータベースから ypinit コマンドによって作成されるデフォルトセット内のマップです。
- デフォルト以外のマップは次のいずれかです。
  - ベンダーから購入したアプリケーションに含まれているマップ
  - サイト専用に作成されたマップ
  - テキスト以外のファイルから作成されたマップ

このセクションでは、さまざまな更新ツールの使用方法について説明します。これらは実際には、システムがすでに起動され、実行されたあとにデフォルト以外のマップを追加したり、NIS サーバーのセットを変更したりする場合にのみ使用するようになる可能性があります。

▼ デフォルトセットに付いているマップを更新する方法

デフォルトセットに付属のマップを更新するには、次の手順を使用します。

1. **NIS マスターサーバー上の管理者になります。**
   詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2. **変更するマップのソースファイルを編集します。**
   このファイルは `/etc` か、または選択したほかのディレクトリ内に存在する可能性があります。

3. **`make` コマンドを実行します。**

   ```
   # cd /var/yp
   # make mapname
   ```

   これにより、`make` コマンドは、対応するファイルに加えられた変更に従ってマップを更新します。make コマンドはまた、これらの変更をほかのサーバーに伝播します。

更新されたマップの管理

以降のセクションでは、デフォルトセットで提供されているマップの更新完了後に実行する手順について説明します。

NIS マップを伝播する

マップが変更されたあと、`Makefile` は `yppush` を使用して、新しいマップをスレーブサーバーに伝播します (`Makefile` で `NOPUSH` が設定されていないかぎり)。これは、`ypserv` デーモンに通知してマップ転送要求を送ることで実行されます。次に、スレーブ上の `ypserv` デーモンが `ypxfr` プロセスを起動し、このプロセスがさらにマスターサーバー上の `ypxfrd` デーモンに接続します。いくつかの基本的なチェック (たとえば、マップが実際に変更されたかどうか) が行われたあと、そのマップが転送されます。そのあと、スレーブ上の `ypxfr` が `yppush` プロセスに、転送が成功したかどうかを示す応答を送信します。

注 – 上の手順は、まだスレーブサーバー上に存在しない新しく作成されたマップに対しては機能しません。スレーブサーバー上で ypxfr を実行して、新しいマップをスレーブサーバーに転送する必要があります。

ときには、マップの伝播に失敗し、ypxfr を使用して新しいマップ情報を手動で送信することが必要になる場合があります。ypxfr は、root の crontab ファイルを通して定期的に使用するか、またはコマンド行で対話的に使用するかの 2 つの異なる方法を選択できます。これらの方法については、以降のセクションで説明します。

マップ転送のための cron コマンドの使用

マップの更新頻度はマップによってそれぞれ異なります。たとえば、デフォルトのマップにある protocols.byname や、デフォルト以外のマップにある auto_master など、一部のマップは何か月も変更されないことがあります。一方で、passwd.byname は 1 日に数回変更される場合があります。crontab コマンドを使用してマップ転送をスケジュールすると、個々のマップごとに特定の伝播回数を設定できます。

マップに適した頻度で ypxfr を定期的に実行するには、各スレーブサーバー上の root の crontab ファイルに適切な ypxfr エントリを含めるようにしてください。ypxfr はマスターサーバーに接続し、マスターサーバー上のコピーがローカルのコピーより新しい場合にのみマップを転送します。

注 – マスターサーバーでデフォルトの -m オプションを指定して rpc.yppasswdd が実行されると、だれかが自分の yp パスワードを変更するたびに passwd デーモンが make を実行し、それによって passwd マップが再構築されます。

cron と ypxfr でのシェルスクリプトの使用

NIS 管理者は、各マップに対する crontab エントリを個々に作成するという方法ではなく、root の crontab コマンドでシェルスクリプトを実行してすべてのマップを定期的に更新するという方法を使用することもできます。マップ更新シェルスクリプトのサンプルは、/usr/lib/netsvc/yp ディレクトリに入っています。これらのスクリプト名は、ypxfr_1perday、ypxfr_1perhour、および ypxfr_2perday です。これらのシェルスクリプトは、サイトの要件に合うように変更したり、置き換えたりすることができます。次の例は、デフォルトの ypxfr_1perday シェルスクリプトを示しています。

例 7–1　ypxfr_1perday シェルスクリプト

```
#! /bin/sh
#
# ypxfr_1perday.sh - Do daily yp map check/updates
PATH=/bin:/usr/bin:/usr/lib/netsvc/yp:$PATH
export PATH
```

例 7–1　ypxfr_1perday シェルスクリプト　　*(続き)*

```
# set -xv
ypxfr group.byname
ypxfr group.bygid
ypxfr protocols.byname
ypxfr protocols.bynumber
ypxfr networks.byname
ypxfr networks.byaddr
ypxfr services.byname
ypxfr ypservers
```

このシェルスクリプトは、root の `crontab` が毎日実行される場合は 1 日に 1 回マップを更新します。また、1 週間に 1 回、1 か月に 1 回、1 時間に 1 回などの頻度でマップを更新するスクリプトを作成することもできます。ただし、マップを頻繁に伝播するとパフォーマンスが低下する可能性があることに注意してください。詳細は、`crontab(1)` のマニュアルページを参照してください。

NIS ドメイン用に構成された各スレーブサーバー上で `root` として同じシェルスクリプトを実行します。各サーバー上の実行時間を変更して、マスターサーバーが動作不能にならないようにしてください。

特定のスレーブサーバーからマップを転送する場合は、シェルスクリプト内で `ypxfr` の `-h` *machine* オプションを使用します。シェルスクリプトに記述するコマンドの構文は、次のとおりです。

```
# /usr/lib/netsvc/yp/ypxfr -h machine [ -c ] mapname
```

machine は転送するマップが存在するサーバー名です。*mapname* は要求されたマップ名です。マシンを指定することなく `-h` オプションを指定すると、`ypxfr` はマスターサーバーからマップを取得しようとします。`ypxfr` 実行時に `ypserv` がローカルに実行されていない場合は、`ypxfr` がローカル `ypserver` に現在のマップ要求の取消しを送信しないよう、`-c` フラグを使用してください。

`-s` *domain* オプションを使用すると、別のドメインからローカルドメインにマップを転送できます。これらのマップは、ドメイン間で同じである必要があります。たとえば、2 つのドメインで同じ `services.byname` および `services.byaddr` マップを共有する可能性があります。あるいは、より細かく制御するために、`rcp` または `rsync` を使用してドメイン間でファイルを転送することもできます。

`ypxfr` コマンドの直接の起動

`ypxfr` コマンドの 2 番目の起動方法は、コマンドとしての実行です。一般に、ypxfr をコマンドとして実行するのは例外的状況においてだけです。たとえば、一時的に NIS サーバーを設定して試験環境を作成する場合や、動作不能になっていた NIS サーバーをほかのサーバーと迅速に整合させようとする場合などです。

ypxfr のアクティビティーのロギング

ypxfr が試みた転送およびその転送結果は、ログファイルに記録されます。/var/yp/ypxfr.log というファイルが存在する場合は、転送結果はこのファイルに記録されます。このログファイルのサイズには制限がありません。このログファイルのサイズが無限に大きくなることを防止するには、ときどき次のように入力してこのログファイルを空にしてください。

```
# cd /var/yp
# cp ypxfr.log ypxfr.log.old
# cat /dev/null > /var/yp/ypxfr.log
```

これらのコマンドは、crontab で 1 週間に 1 回実行させることができます。記録を取らないようにするには、ログファイルを削除してください。

デフォルト以外のマップの変更

デフォルト以外のマップを更新するには、次の手順を実行する必要があります。

1. 対応するテキストファイルを作成または編集します。
2. 新しいマップまたは更新されたマップを作成 (または再作成) します。マップ作成には 2 つの方法があります。
   - Makefile を使用する方法。デフォルトでないマップを作成するには、この方法をお勧めします。Makefile にマップのエントリが含まれている場合は、make *name* を実行します。ここで、*name* は構築するマップの名前です。Makefile にマップのエントリが含まれていない場合は、107 ページの「/var/yp/Makefile の変更および使用」の手順に従って、そのエントリの作成を試みます。
   - /usr/sbin/makedbm プログラムを使用します。このコマンドについては、makedbm(1M) のマニュアルページで詳細に説明されています。

デフォルト以外のマップを変更するための makedbm コマンドの使用

入力ファイルが存在しない場合、makedbm を使用してマップを変更する方法には次の 2 種類があります。

- makedbm -u の出力先を一時ファイルに変更し、一時ファイルを更新して更新済みの一時ファイルを makedbm の入力として使用します。
- makedbm -u の出力を、makedbm に入力されるパイプライン内で操作します。これは、分解されたマップを awk、sed、または cat のいずれかを追加して更新できる場合に適しています。

テキストファイルからの新しいマップの作成

テキストファイル /var/yp/mymap.asc がマスターサーバー上のエディタまたはシェルスクリプトで作成されていると仮定します。このファイルから NIS マップを作成し、それを *home-domain* サブディレクトリ内に配置しようとしています。マスターサーバー上で次のように入力してください。

```
# cd /var/yp
# makedbm mymap.asc home-domain/mymap
```

mymap マップは現在、マスターサーバー上のディレクトリ *home-domain* 内に存在します。この新しいマップをスレーブサーバーに転送するには、ypxfr を実行してください。

ファイルをベースとしたマップにエントリを追加する

mymap へのエントリの追加は簡単です。まず、テキストファイル /var/yp/*mymap*.asc を更新します。対応するテキストファイルを更新しないで実際のdbmファイルを更新した場合は、更新内容が失われます。次に、上記のように makedbm を実行してください。

標準入力からマップを作成する

元のテキストファイルが存在しない場合は、次のように makedbm へ入力することによって、キーボードから NIS マップを作成します (Control-D で終了します)。

```
ypmaster# cd /var/yp
ypmaster# makedbm home-domain/mymap key1 value1  key2 value2  key3 value3
```

標準入力から作成されたマップを更新する

あとでマップを変更する必要がある場合は、makedbm を使用してマップを分解し、一時的な中間テキストファイルを作成することができます。マップを分解して一時ファイルを作成するには、次のように入力します。

```
% cd /var/yp
% makedbm -u homedomain/mymap > mymap.temp
```

作成される一時ファイル *mymap*.temp には、1 行に 1 つのエントリが含まれています。このファイルは、任意のテキストエディタで必要に応じて編集できます。

マップを更新するには、次のように入力して、変更された一時ファイルの名前を makedbm に指定します。

```
% makedbm mymap.temp homedomain/mymap
% rm mymap.temp
```

次に、root になり、次のように入力して、マップをスレーブサーバーに伝播します。

```
# yppush mymap
```

前の段落では、makedbm を使用してマップを作成する方法について説明しました。ただし、システムがすでに起動され、実行されたあとにデータベースにデフォルト以外のマップを追加したり、NIS サーバーのセットを変更したりしないかぎり、ypinit コマンドと /var/yp/Makefile を使用することによって、実際に必要なほぼすべてのことを実行できます。

/var/yp 内の Makefile を使用するか、またはほかの何らかの手順を使用するかにかかわらず、その目的は同じです。最終的には、正しく作成された dbm ファイルの新しいペアが、マスターサーバー上の maps ディレクトリ内に存在する必要があります。

NIS サーバーの操作

次の手順は、特定の NIS サーバーにバインドし、NIS ドメイン名を設定し、ホスト検索を DNS に転送し、さらに NIS サービスを無効にすることによって NIS 構成を変更する方法を示しています。

特定の NIS サーバーへのバインド

指定した NIS サーバーにバインドするには、次の手順に従います。詳細は、ypinit(1M)、ypstart(1M)、および svcadm(1M) の各マニュアルページを参照してください。

1. NIS サーバーのホスト名とその IP アドレスを /etc/hosts ファイルに追加します。
2. NIS ドメイン名が設定されていることを確認します。

   ```
   # domainname
   example.com
   ```
3. NIS サーバーホスト名を要求します。

   ```
   # /usr/sbin/ypinit -c
   Server name:      Type the NIS server host name
   ```
4. 次のいずれかの手順を実行することによって、NIS サービスを再起動します。
   - リブートのあとも持続するサービスの場合は、svcadm コマンドを実行します。

     ```
     # svcadm enable svc:/network/nis/client
     ```
   - リブートまでしか持続しないサービスの場合は、ypstop および ypstart コマンドを実行します。

```
# /usr/lib/netsvc/yp/ypstop
# /usr/lib/netsvc/yp/ypstart
```

▼ マシンの NIS ドメイン名を設定する方法

マシンの NIS ドメイン名を変更するには、次の手順を使用します。

1. 管理者になります。

   詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2. NIS ドメイン名を定義します。

   ```
   # domainname research.example.com
   ```

3. ドメインネームサービスを更新して実行します。

   ```
   # svccfg -s nis/domain:default refresh
   # svcadm enable nis/domain
   ```

4. マシンを NIS クライアント、スレーブサーバー、またはマスターサーバーとして設定します。

   詳細は、第 6 章「NIS の設定と構成 (タスク)」を参照してください。

▼ NIS と DNS を使用してマシンのホスト名とアドレスの検索を構成する方法

通常、NIS クライアントは、マシン名とアドレスの検索に NIS のみを使用するように `nsswitch.conf` ファイルを使用して構成されます。このような検索が失敗した場合は、NIS サーバーはこれらの結果を DNS に転送します。

1. 管理者になります。

   詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2. **`YP_INTERDOMAIN`** キーを追加します。

   `hosts.byname` と `hosts.byaddr` という 2 つのマップファイルには、`YP_INTERDOMAIN` キーが必要です。このキーをテストするには、`/var/yp/Makefile` を編集し、次の行を変更します。

   ```
   #B=-b
   B=
   ```

から

```
B=-b
#B=
```

これで、マップの作成時に makedbm が -b フラグで起動され、YP_INTERDOMAIN キーが ndbm ファイルに挿入されます。

3 **make** コマンドを実行してマップを作成し直します。

```
# make hosts
```

4 **DNS** ネームサーバーが正しく設定されていることを確認します。

次のコマンドは、DNS ネームサーバーのすべての IP アドレスを一覧表示します。

```
# svcprop -p config/nameserver network/dns/client
```

5 **DNS** 転送を有効にするために、各サーバーを再起動します。

```
# svcadm restart network/nis/server:instance
```

この NIS の実装では、-d オプションで ypserv デーモンが自動的に起動して DNS にリクエストを転送します。

NIS サービスをオフにする

NIS マスター上の ypserv デーモンが無効になっていると、どの NIS マップも更新できなくなります。

- クライアント上の NIS を無効にするには、次のように入力します。

  ```
  # svcadm disable network/nis/domain
  # svcadm disable network/nis/client
  ```

- 特定のスレーブまたはマスターサーバー上の NIS を無効にするには、そのサーバー上で次のように入力します。

  ```
  # svcadm disable network/nis/domain
  # svcadm disable network/nis/server
  ```

◆ ◆ ◆ 第 8 章

NISのトラブルシューティング

この章では、NISを実行しているネットワーク上で発生する問題の解決方法について説明します。ここでは、NISクライアントとNISサーバーの両方で検出される問題を取り上げています。

NISサーバーまたはクライアントをデバッグしようとする前に、NIS環境について説明している第5章「ネットワーク情報サービス(概要)」を確認してください。次に、現在の問題をもっともよく表しているこのセクション内のサブ見出しを探してください。

注 – NISサービスはサービス管理機能によって管理されます。このサービスに関する有効化、無効化、再起動などの管理アクションは`svcadm`コマンドを使用して実行できます。NISでSMFを使用する場合の詳細については、80ページの「NISとサービス管理機能」を参照してください。SMFの概要については、『Oracle Solaris 11.1でのサービスと障害の管理』の第1章「サービスの管理(概要)」を参照してください。また、詳細については`svcadm(1M)`および`svcs(1)`のマニュアルページも参照してください。

NISサービスはまた、`ypstart`および`ypstop`コマンドを使用して起動および停止することもできます。詳細は、`ypstart(1M)`および`ypstop(1M)`のマニュアルページを参照してください。

NISのバインドに関する問題

NISのバインドに関する問題の現象

NISのバインドに関する一般的な問題には、次のようなものがあります。

- `ypbind`がサーバーを見つけることができない、またはサーバーと通信できないというメッセージ

- サーバーが応答していないというメッセージが表示される
- NIS が使用できないというメッセージが表示される
- クライアントのコマンドがバックグランドモードでゆっくりと処理されているか、通常よりも機能に時間がかかる
- クライアント上のコマンドがハングアップする。システム全体は正常で新しいコマンドを実行できる場合でも、コマンドがハングすることがあります
- クライアントのコマンドがあいまいなメッセージとともに、またはまったくメッセージなしでクラッシュする

1 台のクライアントに影響する NIS の問題

1 台か 2 台のクライアントだけで、NIS のバインドに関する問題を示す症状が発生している場合は、そのクライアントに問題があると考えられます。複数のクライアントが正しくバインドできない場合は、1 台以上の NIS サーバーに問題があると考えられます。124 ページの「複数のクライアントに影響する NIS の問題」を参照してください。

ypbind がクライアントで実行されていない

あるクライアントに問題がありますが、同じサブネット上のほかのクライアントは正常に動作しています。問題のあるクライアント上の、多数のユーザー (そのクライアントの /etc/passwd ファイルにないユーザーも含む) が所有するファイルが含まれているディレクトリ (/usr など) で ls -l を実行します。その結果の表示に、ローカルの /etc/passwd にないファイル所有者が名前ではなく、番号として一覧表示される場合は、そのクライアント上で NIS サービスが動作していないことを示します。

通常これらの症状は、クライアント ypbind プロセスが実行されていないことを示します。NIS クライアントサービスが実行されているかどうかを確認します。

```
client# svcs \*nis\*
STATE          STIME    FMRI
disabled       Sep_01   svc:/network/nis/domain:default
disabled       Sep_01   svc:/network/nis/client:default
```

これらのサービスが disabled 状態にある場合は、root としてログインするか、または同等の役割になり、NIS クライアントサービスを起動します。

```
client# svcadm enable network/nis/domain
client# svcadm enable network/nis/client
```

ドメイン名が指定されていないか間違っている

あるクライアントに問題があり、ほかのクライアントは正常に動作しています が、ypbind はその問題のあるクライアント上で実行されています。クライアントのドメインの設定が間違っている可能性があります。

クライアント上で domainname コマンドを実行して、どのドメイン名が設定されているのかを調べます。

```
client7# domainname
example.com
```

この出力を、NIS マスターサーバー上の /var/yp 内の実際のドメイン名と比較します。実際の NIS ドメインは、/var/yp ディレクトリ内のサブディレクトリとして表示されます。

```
client7# ls -l /var/yp
-rwxr-xr-x 1 root Makefile
drwxr-xr-x 2 root binding
drwx------ 2 root example.com
```

マシン上で domainname を実行することによって返されたドメイン名が、/var/yp 内のディレクトリとして一覧表示されたサーバードメイン名と同じでない場合は、マシンの /etc/defaultdomain ファイルで指定されたドメイン名が正しくありません。117 ページの「マシンの NIS ドメイン名を設定する方法」で示すように、NIS ドメイン名をリセットします。

注 – NIS ドメイン名では大文字と小文字が区別されます。

クライアントがサーバーにバインドされない

ドメイン名が正しく設定されており、ypbind が実行されていてもコマンドがまだハングアップする場合は、ypwhich コマンドを実行することによって、クライアントがサーバーにバインドされていることを確認します。ypbind を起動したばかりの場合は、ypwhich を何回か実行します (通常、1 回目にはドメインがバインドされていないことが報告され、2 回目には成功します)。

サーバーが使用できない

ドメイン名が正しく設定されていて ypbind が実行中のときに、クライアントがサーバーと通信できないというメッセージを受け取った場合には、いくつかの問題が考えられます。

- クライアントに、バインド先のサーバーのリストが含まれた /var/yp/binding/*domainname*/ypservers ファイルが存在しますか。ない場合には、ypinit -c を実行して、設定の順番にクライアントのバインド先のサーバーを指定します。
- クライアントに /var/yp/binding/*domainname*/ypservers ファイルがあり、1 つ以上のサーバーが使用できない場合には、十分な数のサーバーがあるかどうかを調べます。存在しない場合は、ypinit -c を実行することによって、このリストにサーバーを追加します。

- /etc/inet/hosts ファイル内に、選択された NIS サーバーのエントリがありますか。選択された NIS サーバーを表示するには、svcprop -p config/ypservers nis/domain コマンドを使用します。これらのホストがローカルの /etc/inet/hosts ファイル内に含まれていない場合は、104 ページの「NIS マップに関する作業」の説明に従って ypinit -c または ypinit -s コマンドを実行することによって、hosts の NIS マップにサーバーを追加してマップを再構築します。
- ネームサービススイッチは NIS に加えて、マシンのローカルの hosts ファイルをチェックするように設定されていますか。このスイッチについての詳細は、第 2 章「ネームサービススイッチ (概要)」を参照してください。
- ネームサービススイッチは、services と rpc で最初に files をチェックするように設定されていますか。スイッチについての詳細は、第 2 章「ネームサービススイッチ (概要)」を参照してください。

ypwhich の表示に一貫性がない

ypwhich を同じクライアントで数回使うと、NIS サーバーが変わるので結果の表示も変わります。これは正常です。NIS クライアントから NIS サーバーへのバインドは、ネットワークや NIS サーバーを使用中の場合は時間の経過に伴って変化します。ネットワークは、すべてのクライアントが受け入れ可能な応答時間を NIS サーバーから得られる点で安定した状態になります。クライアントのマシンが NIS サービスを得ている限りは、サービスの供給元は問題にはなりません。たとえば、NIS サーバーマシンがそれ自体の NIS サービスを、ネットワーク上の別の NIS サーバーから受けることもあります。

サーバーのバインドが不可能な場合

ローカルなサーバーのバインドが不可能な場合には ypset コマンドを使用すると、別のネットワークまたはサブネットの別のサーバーが使用可能な場合には、そのサーバーへのバインドが一時的に可能になります。ただし、-ypset オプションを使用するには、ypbind を -ypset または -ypsetme のどちらかのオプションを使用して起動する必要があります。詳細は、ypbind(1M) のマニュアルページを参照してください。

```
# /usr/lib/netsvc/yp/ypbind -ypset
```

別の方法については、116 ページの「特定の NIS サーバーへのバインド」を参照してください。

注意 – セキュリティー上の理由から、-ypset オプションや -ypsetme オプションの使用はお勧めできません。これらのオプションは、制御された環境でのデバッグの目的にのみ使用してください。-ypset オプションや -ypsetme オプションを使用すると、これらのデーモンの実行中にだれでもサーバーのバインドを変更でき、ほかのユーザーでトラブルが発生したり、機密データへの未承認のアクセスが許可されたりするため、重大なセキュリティー違反が発生する場合があります。これらのオプションを使用して ypbind デーモンを起動する必要がある場合は、問題を解決したあとに ypbind プロセスを強制終了し、これらのオプションなしでこのデーモンを再起動する必要があります。

ypbind デーモンを再起動するには、SMF を次のように使用します。

```
# svcadm enable -r svc:/network/nis/client:default
```

ypbind のクラッシュ

ypbind デーモンが、起動されるたびにほぼ即座にクラッシュする場合は、svc:/network/nis/client:default サービスログ内で問題を探します。次のように入力して、rpcbind デーモンが存在するかどうかをチェックします。

```
% ps -e |grep rpcbind
```

rpcbind が存在しないか、または安定しなかったり、異常な動作を行なったりする場合は、svc:/network/rpc/bind:default ログファイルをチェックします。詳細は、rpcbind(1M) および rpcinfo(1M) のマニュアルページを参照してください。

正常に機能しているマシンから、問題のあるクライアント上の rpcbind と通信ができる場合があります。正常に機能しているマシンから、次のように入力します。

```
% rpcinfo client
```

問題のあるマシン上の rpcbind が正常である場合、rpcinfo は次の出力を生成します。

```
    program    version    netid     address    service    owner
...
    100007    3    udp6       ::.191.161          ypbind     1
    100007    3    tcp6       ::.135.200          ypbind     1
    100007    3    udp        0.0.0.0.240.221     ypbind     1
    100007    2    udp        0.0.0.0.240.221     ypbind     1
    100007    1    udp        0.0.0.0.240.221     ypbind     1
    100007    3    tcp        0.0.0.0.250.107     ypbind     1
    100007    2    tcp        0.0.0.0.250.107     ypbind     1
    100007    1    tcp        0.0.0.0.250.107     ypbind     1
    100007    3    ticlts     2\000\000\000       ypbind     1
    100007    2    ticlts     2\000\000\000       ypbind     1
    100007    3    ticotsord  9\000\000\000       ypbind     1
    100007    2    ticotsord  9\000\000\000       ypbind     1
    100007    3    ticots     @\000\000\000       ypbind     1
...
```

使用中のマシンには異なる複数のアドレスがあります。それらのアドレスが表示されない場合は、ypbind によってそのサービスが登録できていません。マシンをリブートして再度 rpcinfo を実行します。ypbind プロセスがそこに存在し、NIS サービスを再起動しようとするたびに変更される場合は、rpcbind デーモンが実行されていてもシステムをリブートします。

複数のクライアントに影響する NIS の問題

1 台か 2 台のクライアントだけで、NIS のバインドに関する問題を示す症状が発生している場合は、そのクライアントに問題があると考えられます。120 ページの「1 台のクライアントに影響する NIS の問題」を参照してください。複数のクライアントが正しくバインドできない場合は、1 台以上の NIS サーバーに問題があると考えられます。

rpc.yppasswdd が r で始まる制限のないシェルを制限付きと見なしている

1. 次のような特殊な文字列が含まれている /etc/default/yppasswdd を作成します。
   "check_restricted_shell_name=1"
2. 「check_restricted_shell_name=1」 の文字列がコメントアウトされている場合、「r」のチェックは実行されません。

ネットワークまたはサーバーに到達できない

ネットワークまたは NIS サーバーが過負荷状態であるために、ypserv デーモンが、クライアントの ypbind プロセスに返される応答をタイムアウト期間内に受信できない場合は、NIS がハングアップすることがあります。NIS はまた、ネットワークがダウンしている場合にもハングアップすることがあります。

こういった状態では、ネットワーク上のすべてのクライアントで同じまたは類似した問題が発生します。ほとんどの場合、この状態は一時的です。これらのメッセージは通常、NIS サーバーがリブートして ypserv を再起動するか、NIS サーバー上またはネットワーク自体の負荷が減るか、またはネットワークが正常な動作を再開すると消えます。

サーバーの誤動作

サーバーが起動され、実行されていることを確認します。サーバーが物理的に近くにない場合には、ping コマンドを使ってください。

NISデーモンが実行されていない

サーバーが起動されていて実行中の場合には、クライアントマシンが正常に動作していることを調べて、ypwhichコマンドを実行します。ypwhichが応答しない場合は、そのコマンドを強制終了します。次に、NISサーバー上でrootとしてログインし、次のように入力して、NISプロセスが実行されているかどうかをチェックします。

```
# ptree |grep ypbind
100759 /usr/lib/netsvc/yp/ypbind -broadcast
        527360 grep yp
```

ypserv (NISサーバー) とypbind (NISクライアント) のどちらのデーモンも実行されていない場合は、次のように入力してそれらを再起動します。

```
# svcadm restart network/nis/client
```

NISサーバー上でypservプロセスとypbindプロセスの両方が実行されている場合は、ypwhichコマンドを実行します。このコマンドが応答しない場合は、ypservデーモンがおそらくハングアップしているため、再起動してください。サーバー上でrootとしてログインしている間に、次のように入力してNISサービスを再起動します。

```
# svcadm restart network/nis/server
```

サーバーに別のバージョンのNISマップが存在する

NISはマップをサーバー間で伝播するので、ネットワーク上のさまざまなNISサーバーに、同じマップの異なるバージョンが存在することがあります。このバージョンの不一致は、これらの違いが短時間しか続かなければ正常であり、許容可能です。

マップの不一致のもっとも一般的な原因は、マップの正常な伝播を妨げる何かが存在するためです。たとえば、NISサーバーまたはルーターが、NISサーバー間でダウンしている場合です。すべてのNISサーバーと、それらのサーバー間にあるルーターが実行されている場合、ypxfrは成功します。

サーバーとルーターが正常に機能している場合には、次のことをチェックします。

- ypxfrのログ出力をチェックします。126ページの「ypxfrの出力のロギング」を参照してください。
- svc:/network/nis/xfr:defaultログファイルにエラーが表示されていないかどうかをチェックします。
- 制御ファイルをチェックします。126ページの「crontabファイルとypxfrシェルスクリプトをチェックする」を参照してください。
- マスターサーバー上のypserversマップをチェックします。(126ページの「ypserversマップをチェックする」を参照)。

ypxfr の出力のロギング

特定のスレーブサーバーでマップの更新に関する問題が発生した場合は、そのサーバーにログインし、ypxfr コマンドを対話的に実行します。このコマンドが失敗した場合は、失敗した理由が示されるため、問題を解決することができます。このコマンドは成功するが、ときどき失敗していたと思われる場合は、メッセージのロギングを有効にするためにログファイルを作成します。ログファイルを作成するには、スレーブ上で次のように入力します。

```
ypslave# cd /var/yp
ypslave# touch ypxfr.log
```

これによって、ypxfr からのすべての出力を保存する ypxfr.log ファイルが作成されます。

この出力は、ypxfr が対話形式で実行しているときに表示する出力と似ていますが、ログファイルの各行にはタイムスタンプが記録されます。(タイムスタンプが通常とは異なった順序になることがあります。これは問題ありません。タイムスタンプは、ypxfr が実行を開始した時間を示します。ypxfr の複数のコピーが同時に実行されたが、それらの動作時間が異なった場合は、各サマリーステータス行が、それぞれの起動順序とは異なる順序で実際にログファイルに書き込まれることがあります。)断続的に発生するあらゆる種類の障害がログに記録されます。

注 – 問題を解決したら、ログファイルを削除してログを停止します。削除し忘れた場合は、そのファイルが無制限に拡張し続けます。

---

crontab ファイルと ypxfr シェルスクリプトをチェックする

root の crontab ファイルを調べ、それが起動する ypxfr シェルスクリプトをチェックします。これらファイルにタイプミスがあると、伝播に関する問題が発生します。/var/spool/cron/crontabs/root ファイル内でシェルスクリプトを参照できない場合や、任意のシェルスクリプト内でマップを参照できない場合にも、エラーが発生します。

ypservers マップをチェックする

また、NIS スレーブサーバーが、そのドメインのマスターサーバー上の ypservers マップ内にリストされていることも確認します。リストされていない場合には、スレーブサーバーはサーバーとして正しく機能しますが、yppush はマップの変更をスレーブサーバーに伝播しません。

壊れたスレーブサーバー上のマップを更新するための回避方法

NIS スレーブサーバーの問題が明らかでない場合は、scp または ssh コマンドを使用して、一貫性のないマップの最新バージョンをいずれかの正常な NIS サーバーから

コピーすることによって、問題のデバッグ中に回避方法を実行できます。次に、問題のあるマップを転送する方法を示します。

```
ypslave# scp ypmaster:/var/yp/mydomain/map.\* /var/yp/mydomain
```

* の文字はコマンド行でエスケープされているため、ypslave 上でローカルにではなく、ypmaster 上で展開されます。

ypserv のクラッシュ

ypserv プロセスがほぼ即座にクラッシュし、起動を繰り返しても安定しない場合は、デバッグプロセスが 123 ページの「ypbind のクラッシュ」で説明されている状況と実質的に同じです。まず、次のコマンドを実行して、何らかのエラーが報告されているかどうかを確認します。

```
# svcs -vx nis/server
```

rpcbind デーモンが存在するかどうかを、次のようにチェックします。

```
# ptree |grep rpcbind
```

デーモンが見つからない場合は、サーバーをリブートします。それ以外の場合は、デーモンが実行されていれば、次のように入力して同様の出力を探します。

```
% rpcinfo -p ypserver

% program     vers     proto     port     service
100000    4    tcp    111    portmapper
100000    3    tcp    111    portmapper
100068    2    udp    32813    cmsd
...
100007    1    tcp    34900    ypbind
100004    2    udp    731    ypserv
100004    1    udp    731    ypserv
100004    1    tcp    732    ypserv
100004    2    tcp    32772    ypserv
```

使用中のマシンには、異なる複数のポート番号があることがあります。ypserv プロセスを表す 4 つのエントリは次のとおりです。

```
100004     2     udp     731     ypserv
100004     1     udp     731     ypserv
100004     1     tcp     732     ypserv
100004     2     tcp     32772     ypserv
```

エントリが 1 つもなく、ypserv がそのサービスを rpcbind で登録できない場合にはマシンをリブートしてください。エントリが存在する場合は、ypserv を再起動する前に、rpcbind からこのサービスの登録を解除します。rpcbind からこのサービスの登録を解除するには、サーバー上で次のように入力します。

```
# rpcinfo -d number 1
# rpcinfo -d number 2
```

ここで、*number* は `rpcinfo` によって報告された ID 番号 (前の例では `100004`) です。

パート III

LDAP ネームサービス

ここでは、LDAP ネームサービスの概要を説明します。さらに、Oracle Directory Server Enterprise Edition の使用に焦点を当てて、Oracle Solaris OS での LDAP ネームサービスの設定、構成、管理、およびトラブルシューティングについても説明します。

◆ ◆ ◆ 第 9 章

LDAP ネームサービスの紹介 (概要)

この LDAP の章では、Oracle Directory Server Enterprise Edition (以前の名称は SunJavaSystem Directory Server) で動作するように LDAP ネームサービスクライアントを設定する方法について説明します。Oracle Directory Server Enterprise Edition の使用を推奨しますが、必須ではありません。汎用ディレクトリサーバーの要件については、第 14 章「LDAP ネームサービス (リファレンス)」で簡潔に説明されています。

注 – ディレクトリサーバーは、必ずしも LDAP サーバーである必要はありません。しかし、この章では「ディレクトリサーバー」という言葉は「LDAP サーバー」と同じ意味で使っています。

この章の内容は次のとおりです。

対象読者

LDAP ネームサービスに関するこれらの章は、LDAP に関する実務上の知識を持つシステム管理者を対象としています。次のリストはこの章を読む前によく理解しておく必要のある概念の一部です。これらの概念を理解していないと、このガイドを使用して Oracle Solaris システムに LDAP ネームサービスを配備することは難しい場合があります。

- LDAP 情報モデル (エントリ、オブジェクトクラス、属性、タイプ、値)
- LDAP ネームモデル (ディレクトリ情報ツリー (DIT) 構造)
- LDAP 機能モデル (検索パラメータ: ベースオブジェクト (DN)、スコープ、サイズ制限、時間制限、フィルタ (Oracle Directory Server Enterprise Edition のインデックスを表示する)、属性リスト)
- LDAP セキュリティーモデル (認証方式、アクセス制御モデル)
- データの計画方法と DIT、トポロジ、複製、セキュリティーの設計方法を含む LDAP ディレクトリサービスの計画と設計全般

推奨される前提知識

前述の概念についての詳細、また一般的な LDAP とディレクトリサービスの導入について知りたい場合は、次のドキュメントを参照してください。

- Oracle Directory Server Enterprise Edition の配備ガイド

  このガイドでは、基本的なディレクトリ計画 (ディレクトリ設計、スキーマ設計、ディレクトリツリー、トポロジ、複製、およびセキュリティーを含む) が説明されています。最後の章では、単純で小規模な配備計画と、複雑な世界に広がる配備計画の両方のシナリオを説明しています。
- 『Oracle Directory Server Enterprise Edition 管理ガイド』

その他の前提条件

Oracle Directory Server Enterprise Edition をインストールする場合は、使用しているバージョンの Oracle Directory Server Enterprise Edition の『インストールガイド』を参照してください。

LDAP ネームサービスとその他のネームサービスの比較

DNS、NIS、および LDAP ネームサービスの比較については、32 ページの「ネームサービスの比較一覧」を参照してください。

LDAP ネームサービスの利点

- LDAP を使用すると、アプリケーション固有の情報を置き換えて情報の整理統合を実行し、管理するデータベースの数を減らすことができる。
- LDAP を使用すると、異なる複数のネームサービス間でデータを共有できる。
- LDAP により、データの集中的なリポジトリ (格納場所) が提供される。
- LDAP を使用すると、マスターと複製との間でより頻繁にデータの同期を取ることができる。
- LDAP では、プラットフォーム間およびベンダー間の互換性が維持されている。

LDAP ネームサービスの欠点

次に、LDAP ネームサービスに関連したいくつかの制限事項を示します。

- LDAP サーバーは現在、自身のクライアントとしてはサポートされていません。
- LDAP ネームサービスの設定と管理はより複雑な作業であるため、注意深い計画が必要になります。
- NIS クライアントとネイティブな LDAP クライアントは、同じクライアントマシン上で共存できません。

注 – ディレクトリサーバー (LDAP サーバー) をそのクライアントとして使用することはできません。つまり、ディレクトリサーバーソフトウェアを実行中のマシンを、LDAP ネームサーバークライアントにするように構成することはできません。

LDAP ネームサービスの設定 (タスクマップ)

タスク	説明
ネットワークモデルを計画します。	162 ページの「LDAP ネットワークモデルの計画」
ディレクトリ情報ツリーを計画します。	第 10 章「LDAP ネームサービスの計画要件 (タスク)」

タスク	説明
複製サーバーを設定します。	164 ページの「LDAP と複製サーバー」
セキュリティーモデルを計画します。	165 ページの「LDAP セキュリティーモデルの計画」
クライアントプロファイルとデフォルトの属性値を選択します。	167 ページの「LDAP 用のクライアントプロファイルおよびデフォルト属性値の計画」
データの生成を計画します。	167 ページの「LDAP データ生成の計画」
LDAP ネームサービスで使用する前に Oracle Directory Server Enterprise Edition を構成します。	『Oracle Directory Server Enterprise Edition』
LDAP ネームサービスクライアントで使用するように Oracle Directory Server Enterprise Edition を設定します。	第 11 章「LDAP クライアントと Oracle Directory Server Enterprise Edition の設定 (タスク)」
LDAP クライアントを初期化します。	191 ページの「LDAP クライアントの初期化」
プロファイルを使用してクライアントを初期化します。	192 ページの「プロファイルを使用して LDAP クライアントを初期化する方法」
クライアントを手動で初期化します。	196 ページの「LDAP クライアントを手動で初期化する方法」
クライアントの初期化を解除します。	197 ページの「LDAP クライアントの初期化を解除する方法」
サービス検索記述子を使用してクライアントプロファイルを変更します。	174 ページの「サービス検索記述子を使用してさまざまなサービスへのクライアントアクセスを変更する」
ネームサービス情報を取得します。	201 ページの「LDAP ネームサービス情報の検出」
クライアント環境をカスタマイズします。	202 ページの「LDAP クライアント環境のカスタマイズ」

LDAP データ交換フォーマット

LDAP データ交換フォーマット (LDIF) は、`ldapadd` や `ldapmodify` などの多くの LDAP ツールの間での共通のテキストベースの交換フォーマットとして使用されます。LDIF は、LDIF RFC 2849 で詳細に説明されています。次に、`ldapadd` コマンドによって作成された LDIF 出力の 2 つの例を示します。次の情報を表示するには、`-l` オプションを指定して `ldaplist(1)` を使用します。

```
% ldaplist -l hosts myhost
hosts

dn: cn=myhost+ipHostNumber=7.7.7.115,ou=Hosts,dc=mydc,dc=mycom,dc=com
```

```
cn: myhost
iphostnumber: 7.7.7.115
objectclass: top
objectclass: device
objectclass: ipHost
description: host 1 - floor 1 - Lab a - building b
% ldaplist -l passwd user1
passwd

dn: uid=user1,ou=People,dc=mydc,dc=mycom,dc=com
uid: user1
cn: user1
userpassword: {crypt}duTx91g7PoNzE
uidnumber: 199995
gidnumber: 20
gecos: Joe Smith [New York]
homedirectory: /home/user1
loginshell: /bin/csh
objectclass: top
objectclass: shadowAccount
objectclass: account
objectclass: posixAccount
```

LDAPでの完全指定ドメイン名の使用

ホスト名の解決にLDAPが使用されている場合、LDAPクライアントは常に、ホスト名として完全修飾ドメイン名(FQDN)を返します。LDAPのFQDNは、DNSによって返されるFQDNに似ています。たとえば、次のドメイン名を考えてみましょう。

```
west.example.net
```

ホスト名*server*を検索する場合、`gethostbyname()`および`getnameinfo()`はホスト名をFQDNで返します。

```
server.west.example.net
```

デフォルトのディレクトリ情報ツリー

デフォルトでは、LDAPクライアントは、ディレクトリ情報ツリー(DIT)が特定の構造を持っていると想定して情報にアクセスします。LDAPサーバーがサポートするドメインごとに、想定された構造を持つサブツリーがあります。ただしこのデフォルト構造は、サービス検索記述子(Service Search Descriptor、SSD)を指定することでオーバーライドできます。指定されたドメインでは、デフォルトDITがベースコンテナを保持し、ベースコンテナに特定の情報タイプのエントリを含む既知のコンテナが多数含まれます。これらのサブツリー名については次の表を参照してください。これらの情報は、RFC 2307などで確認できます。

表 9–1 DIT のデフォルトの場所

デフォルトコンテナ	情報タイプ
ou=Ethers	bootparams、ethers
ou=Group	group
ou=Hosts	hosts、ipnodes、publickey (ホスト用)
ou=Aliases	aliases
ou=Netgroup	netgroup
ou=Networks	networks、netmasks
ou=People	passwd、shadow、user_attr、audit_user、publickey (ユーザー用)
ou=Protocols	protocols
ou=Rpc	rpc
ou=Services	services
ou=SolarisAuthAttr	auth_attr
ou=SolarisProfAttr	prof_attr、exec_attr
ou=projects	project
automountMap=auto_*	auto_*

デフォルトの LDAP スキーマ

スキーマは、LDAP ディレクトリ内にエントリとして格納可能な情報タイプの定義です。LDAP ネームサービスクライアントをサポートするために、ディレクトリサーバースキーマの拡張が必要な場合があります。IETF および Oracle Solaris 固有のスキーマについての詳細は、第 14 章「LDAP ネームサービス (リファレンス)」を参照してください。また、IETF の Web サイト http://www.ietf.org でもさまざまな RFC にアクセスできます。

サービス検索記述子とスキーママッピング

注 – スキーママッピングは、注意深くかつ一貫した方法で使用する必要があります。マッピングされた属性の構文が、マッピング先の属性との一貫性を保持していることを確認してください。つまり、単一値の属性が単一値の属性にマッピングされ、属性の構文が一致しており、マッピングされたオブジェクトクラスが適正な必須 (通常はマッピングされた) 属性を保持することを確認します。

先に説明したように、LDAP ネームサービスは、デフォルトでは DIT が特定の方法で構造化されていると想定します。必要に応じて、サービス検索記述子 (SSD) を使用して、DIT 内のデフォルト以外の場所で検索するよう LDAP ネームサービスに指示することができます。また、デフォルトのスキーマで指定された属性やオブジェクトクラスの代わりに、別の属性やオブジェクトクラスを指定して使用することもできます。デフォルトフィルタの一覧については、232 ページの「LDAP ネームサービスで使用されるデフォルトフィルタ」を参照してください。

SSD の説明

`serviceSearchDescriptor` 属性は、LDAP ネームサービスクライアントが特定のサービスに関する情報を検索する方法と場所を定義します。`serviceSearchDescriptor` には、サービス名のあとに、1 つ以上のセミコロンで区切られたベース - スコープ - フィルタのセットが含まれています。これらのベース - スコープ - フィルタのセットは特定のサービス専用の検索定義に使用され、指定された順番で検索されます。特定のサービスに対して複数のベース - スコープ - フィルタが指定されている場合、このサービスは、特定のエントリを検索する際、指定されたスコープおよびフィルタを保持する各ベースを検索します。

注 – SSD では、デフォルト位置は SSD に含められていない限り、サービス (データベース) の検索対象にはなりません。サービスに複数の SSD が指定されている場合、予期しない結果になることがあります。

次の例では、LDAP ネームサービスクライアントは、`ou=west,dc=example,dc=com` 内で `passwd` サービスに対する 1 レベルの検索を実行したあとに、`ou=east,dc=example,dc=com` 内で 1 レベルの検索を実行します。ユーザーの `username` の `passwd` データを検索するために、各 `BaseDN` に対してデフォルトの LDAP フィルタ `(&(objectClass=posixAccount)(uid=username))` が使用されます。

```
serviceSearchDescriptor: passwd:ou=west,dc=example,dc=com;ou=east,
dc=example,dc=com
```

次の例では、LDAP ネームサービスクライアントは、ou=west,dc=example,dc=com 内で passwd サービスに対するサブツリー検索を実行します。ユーザー username の passwd データを検索するために、LDAP フィルタ (&(fulltimeEmployee=TRUE)(uid=username)) を使用してサブツリー ou=west,dc=example,dc=com が検索されます。

```
serviceSearchDescriptor: passwd:ou=west,dc=example,
dc=com?sub?fulltimeEmployee=TRUE
```

特定のサービスタイプに複数のコンテナを関連付けることも可能です。次の例では、サービス検索記述子が 3 つのコンテナでパスワードエントリを検索することを指定しています。

```
ou=myuser,dc=example,dc=com
ou=newuser,dc=example,dc=com
ou=extuser,dc=example,dc=com
```

例の末尾の「,」は、SSD の相対ベースに defaultSearchBase が付加されることを意味します。

```
defaultSearchBase: dc=example,dc=com
serviceSearchDescriptor: \
passwd:ou=myuser,;ou=newuser,;ou=extuser,dc=example,dc=com
```

attributeMap 属性

LDAP ネームサービスでは、1 つ以上の属性名を、そのいずれかのサービスに再マッピングできます。(LDAP クライアントは、第 14 章「LDAP ネームサービス (リファレンス)」で説明されている既知の属性を使用します。)属性を対応づける場合、その属性が元の属性と同じ意味および構文を必ず保持するようにしてください。userPassword 属性のマッピングによって問題が発生する可能性があることに注意してください。

スキーママッピングを使用する理由として、次の 2 つが挙げられます。

- 既存のディレクトリサーバー内の属性を対応づけしたい
- 大文字小文字のみが異なるユーザー名を使用する場合、大文字小文字を無視する uid 属性を、大文字小文字を無視しない属性に対応づける必要があります

この属性の書式は、service:attribute-name=mapped-attribute-name です。

指定されたサービスに対して複数の属性を対応づける場合は、複数の attributeMap 属性を定義できます。

次の例では、uid および homeDirectory 属性を passwd サービスで利用する場合、常に employeeName および home 属性が使用されます。

```
attributeMap: passwd:uid=employeeName
attributeMap: passwd:homeDirectory=home
```

passwd サービスの gecos 属性を複数の属性にマップできる特殊なケースが 1 つあります。次に例を示します。

```
attributeMap: gecos=cn sn title
```

これにより、gecos 値が cn、sn、および title 属性値のスペースで区切られたリストにマップされます。

objectclassMap 属性

LDAP ネームサービスでは、オブジェクトクラスを、そのいずれかのサービスに再マッピングできます。特定のサービス用に複数のオブジェクトクラスを対応づける場合、複数の objectclassMap 属性を定義できます。次の例では、posixAccount オブジェクトクラスを使用する場合、常に myUnixAccount オブジェクトクラスが使用されます。

```
objectclassMap: passwd:posixAccount=myUnixAccount
```

LDAP クライアントプロファイル

クライアントの設定を単純化し、クライアントごとに同じ情報を再入力する必要性をなくすには、ディレクトリサーバー上に 1 つのクライアントプロファイルを作成します。この単一のプロファイルに、使用するすべてのクライアントの構成を定義します。プロファイル属性への以降の変更はすべて、定義されたリフレッシュ頻度でクライアントに送信されます。

LDAP クライアントプロファイルで指定された構成情報は、svc:/network/ldap/client サービスが起動されたときに SMF リポジトリに自動的にインポートされます。

クライアントプロファイルはすべて、LDAP サーバー上の既知の場所に格納されます。指定されたドメインのルート DN には、nisDomainObject のオブジェクトクラスと、クライアントのドメインを含む nisDomain 属性が含まれている必要があります。すべてのプロファイルは、このコンテナと相対的な関係にある ou=profile コンテナ内に配置されます。これらのプロファイルは、匿名で読み取り可能にする必要があります。

LDAP クライアントのプロファイル属性

次の表に、LDAP クライアントのプロファイル属性を示します。これらの属性は、idsconfig を実行したときに自動的に設定できます。クライアントプロファイルを手動で設定する方法については、196 ページの「LDAP クライアントを手動で初期化する方法」および idsconfig(1M) のマニュアルページを参照してください。

表 9–2 LDAP クライアントのプロファイル属性

属性	説明
cn	プロファイル名。デフォルト値はありません。必ず指定する必要があります。
preferredServerList	優先使用されるサーバーのホストアドレスの、空白で区切られたリスト。(ホスト名は使用しない)。このリスト内のサーバーは、正常な接続が作成されるまで、defaultServerList 内のサーバーの前に順番に試行されます。デフォルト値はありません。preferredServerList または defaultServerList に 1 つ以上のサーバーを指定する必要があります。
defaultServerList	デフォルトサーバーのホストアドレスの、空白で区切られたリスト。(ホスト名は使用しない)。preferredServerlist 内のサーバーが試行されたあと、接続が作成されるまで、クライアントのサブネット上のこれらのデフォルトサーバーが試行され、そのあとに残りのデフォルトサーバーが試行されます。preferredServerList または defaultServerList に 1 つ以上のサーバーを指定する必要があります。このリスト内のサーバーへの接続は、優先サーバーリストのサーバーへの接続試行後に試みられます。デフォルト値はありません。
defaultSearchBase	よく知られたコンテナの検索に使用する相対識別名。デフォルト値はありません。ただしこの値は、serviceSearchDescriptor 属性で指定されたサービスでオーバーライドできます。
defaultSearchScope	クライアントによるデータベース検索の適用範囲を定義します。この値は、serviceSearchDescriptor 属性でオーバーライドできます。指定可能な値は one または sub です。デフォルト値は 1 レベルの検索 (値はone) です。
authenticationMethod	クライアントが使用する認証方式を示します。デフォルト値は none (匿名) です。詳細は、149 ページの「LDAP ネームサービスの認証方法の選択」を参照してください。
credentialLevel	クライアントが認証に使用する証明書タイプを示します。選択肢は、anonymous、proxy、または self (「ユーザー別」とも呼ばれます) です。デフォルトは anonymous です。
serviceSearchDescriptor	クライアントがネームデータベースを検索する方法および場所を定義します (例、クライアントが DIT 内の 1 つ以上の場所を検索する)。デフォルトでは、SSD は定義されていません。
serviceAuthenticationMethod	クライアントが特定のサービスで使用する認証メソッド。デフォルトでは、サービス認証メソッドは定義されていません。サービスで serviceAuthenticationMethod が定義されていない場合、authenticationMethod の値がデフォルトになります。
attributeMap	クライアントが使用する属性マッピング。デフォルトでは、attributeMap は定義されていません。

表 9–2 LDAP クライアントのプロファイル属性 (続き)

属性	説明
objectclassMap	クライアントが使用するオブジェクトクラスマッピング。デフォルトでは、objectclassMap は定義されていません。
searchTimeLimit	クライアントが許可する、タイムアウトまでの最長検索時間 (秒)。この値は、LDAP サーバーが許可する、検索完了までの時間に影響を与えません。デフォルト値は 30 秒です。
bindTimeLimit	クライアントがサーバーとのバインドに許可する最長時間 (秒)。デフォルト値は 30 秒です。
followReferrals	クライアントが LDAP 参照に準拠するかどうかを指定します。指定可能な値は TRUE または FALSE です。デフォルト値は TRUE です。
profileTTL	ldap_cachemgr(1M) により実行される、LDAP サーバーからのクライアントプロファイルのリフレッシュ間隔。デフォルト値は 43200 秒 (12 時間) です。値が 0 の場合、プロファイルは決してリフレッシュされません。

ローカルの LDAP クライアント属性

次の表は、ldapclient コマンドを使用してローカルに設定できる LDAP クライアント属性の一覧です。詳細は、ldapclient(1M) のマニュアルページを参照してください。

表 9–3 ローカルの LDAP クライアント属性

属性	説明
adminDN	管理者資格の管理者エントリの識別名を指定します。クライアントシステム上で enableShadowUpdate スイッチの値が true であり、credentialLevel に self 以外の値が設定されている場合は、adminDN が指定される必要があります。
adminPassword	管理者資格の管理者エントリのパスワードを指定します。クライアントシステム上で enableShadowUpdate スイッチの値が true であり、credentialLevel に self 以外の値が設定されている場合は、adminPassword が定義される必要があります。
domainName	クライアントのドメイン名 (クライアントシステムのデフォルトドメインになる) を指定します。デフォルト値はなく、必ず指定する必要があります。
proxyDN	プロキシの識別名。クライアントシステムが proxy の credentialLevel で構成されている場合は、proxyDN が指定される必要があります。

表 9–3 ローカルの LDAP クライアント属性 (続き)

属性	説明
proxyPassword	プロキシのパスワード。クライアントシステムが proxy の credentialLevel で構成されている場合は、proxyPassword が定義される必要があります。
certificatePath	証明書データベースを含む、ローカルファイルシステム上のディレクトリ。クライアントシステムが TLS を使用して authenticationMethod または serviceAuthenticationMethod で構成されている場合は、この属性が使用されます。デフォルト値は /var/ldap です。

注 – SSD 内の BaseDN に末尾のコンマが含まれている場合、その値は defaultSearchBase の相対値として扱われます。検索が実行される前に、defaultSearchBase の値が BaseDN のあとに付加されます。

ldap_cachemgr デーモン

ldap_cachemgr は、LDAP クライアントマシン上で稼働するデーモンです。ldap_cachemgr デーモンは svc:/network/ldap/client サービスによって管理されるため、このデーモンが正しく動作するには、このサービスが有効になっている必要があります。このデーモンは、次の主要機能を実行します。

- root として動作して、構成データへのアクセスを取得します。
- サーバー上のプロファイルに格納されたクライアント構成情報をリフレッシュして、クライアントからこのデータを引き出す
- 使用可能な LDAP サーバーのソート済みリストを管理する
- さまざまなクライアントから送信される一般的な検索要求をキャッシュして、検索効率を向上させる
- ホスト検索の効率を向上させる
- enableShadowUpdate スイッチが true に設定されている場合は、構成された管理者資格へのアクセスを取得し、shadow データへの更新を実行します。

注 – LDAP ネームサービスを機能させるには、ldap_cachemgr が常に実行されている必要があります。

詳細は、ldap_cachemgr(1M) のマニュアルページを参照してください。

LDAP ネームサービスのセキュリティーモデル

LDAP ネームサービスは、LDAP リポジトリを 2 つの異なる方法で使用できます。1 つは、ネームサービスと認証サービスの両方のソースとして使用する方法です。もう 1 つは、厳密にネームデータのソースとして使用する方法です。このセクションでは、クライアント識別情報の概念、認証方法、pam_ldap モジュールと pam_unix_* モジュール、および LDAP リポジトリがネームサービスと認証サービスの両方として使用される場合のアカウント管理について説明します。このセクションではまた、LDAP ネームサービスを Kerberos 環境 (『Oracle Solaris 11.1 の管理: セキュリティーサービス』のパート VI「Kerberos サービス」) および pam_krb5(5) モジュールと組み合わせて使用する方法についても説明します。

注 – 以前は、pam_ldap アカウント管理を有効にすると、システムにログインする際には、常にすべてのユーザーが認証用にログインパスワードを入力する必要がありました。そのため、ssh などのツールを使用した、パスワードに基づかないログインは失敗します。

アカウント管理を実行し、ユーザーがログインしているときに Directory Server への認証を行わずにユーザーのアカウントステータスを取得します。Directory Server 上の新しい制御は 1.3.6.1.4.1.42.2.27.9.5.8 です。これはデフォルトで有効になっています。

この制御をデフォルト以外に変更する場合は、Directory Server 上でアクセス制御情報 (ACI) を追加します。

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
     allow (read, search, compare, proxy)
     (groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

注 – Kerberos を認証システムとして使用し、LDAP ネームシステムに統合する場合は、Kerberos を利用して企業内でシングルサインオン (SSO) 環境を実現できます。また、ユーザーまたはホストごとに LDAP ネームデータのクエリー検索を実行する際にも、同じ識別システムを使用できます。

LDAP リポジトリ内の情報にアクセスするには、クライアントはまず、ディレクトリサーバーに識別情報を確立できます。この識別情報は匿名にすることも、LDAP サーバーによって認識されたホストまたはユーザーとして指定することもできま

す。クライアントの識別情報とサーバーのアクセス制御情報 (ACI) に基づいて、LDAP サーバーは、クライアントによるディレクトリ情報の読み取りを許可します。ACI の詳細については、使用しているバージョンの Oracle Directory Server Enterprise Edition の『管理者ガイド』を参照してください。

識別情報がリクエストの送信元のホストに基づいている場合は、プロキシ認証を使用しています。ホストが認証されると、そのホスト上のすべてのユーザーがアクセスを取得します。識別情報がユーザーに基づいている場合は、ユーザー別の認証を使用しています。アクセスを取得するには、ホスト上の各ユーザーが認証される必要があります。

特定の要求に関して匿名以外で接続している場合、クライアントは、クライアントとサーバーの両方がサポートする認証方式でサーバーに識別情報を証明する必要があります。クライアントは識別情報を確立後に、さまざまな LDAP 要求を実行できます。

システムにログインすると、PAM サービスはログインの試行を成功させるかどうかを決定するために、ローカルマシンからの情報、LDAP サービスからの情報、Kerberos サーバーからの情報、またはこれらの 3 つのいずれかの組み合わせを使用できます。`pam_kerb` モジュールが使用されている場合、アクセスを許可する決定は Kerberos サーバーによって行われます。`pam_ldap` モジュールが使用されている場合、この決定の半分は LDAP サーバーから来る必要があり、残りの半分はローカルホストから来ます。ローカルホストからの情報の場合、`pam_unix_*` モジュールを使用して、決定はローカルに行われます。

LDAP サービスを使用して `pam_ldap` でログインする場合、ネームサービスと認証サービス (`pam_ldap`) がディレクトリにアクセスする方法には違いがあります。ネームサービスは、事前定義された識別情報に基づくディレクトリから、さまざまなエントリおよびその属性を読み取ります。認証サービスは、ユーザーの名前とパスワードを使用して LDAP サーバーへの認証を行い、ユーザーが適正なパスワードを入力したかどうかを確認します。認証サービスについての詳細は、`pam_ldap(5)` のマニュアルページを参照してください。

Kerberos を認証に使用する場合、および LDAP ネームサービス内の認証も有効にする場合 (ユーザー別の認証方式で必要)、Kerberos は二重の機能を提供できます。ディレクトリへの認証に、サーバーへの Kerberos 認証、および主体 (ユーザーまたはホスト) に対する Kerberos 識別情報が使用されます。これにより、システムの認証に使用されるのと同じユーザー識別情報がディレクトリの認証にも使用され、検索と更新が実行されます。管理者は、必要に応じ、アクセス制御情報 (ACI) をディレクトリ内で使用して、ネームサービスで得られる結果を制限できます。

Transport Layer Security

TLS (Transport Layer Security) プロトコルを使用すると、LDAP クライアントとディレクトリサーバーの間の通信をセキュリティー保護して、プライバシとデータの完全

性の両方を提供することができます。TLS プロトコルは、Secure Sockets Layer (SSL) プロトコルのスーパーセットです。LDAP ネームサービスは、TLS 接続をサポートしています。SSL を使用すると、ディレクトリサーバーおよびクライアントに負荷がかかることに留意してください。

SSL 対応のディレクトリサーバーを設定する必要があります。SSL 対応の Oracle Directory Server Enterprise Edition の設定方法の詳細については、使用しているバージョンの Oracle Directory Server Enterprise Edition の『管理者ガイド』を参照してください。SSL 対応の LDAP クライアントも設定する必要があります。

TLS を使用する場合は、必要なセキュリティーデータベースをインストールしなければなりません。具体的には証明書ファイルと鍵データベースファイルが必要です。たとえば、Netscape Communicator のより古いデータベースフォーマットを採用する場合は、`cert7.db` と `key3.db` の 2 つのファイルが必要です。または、Mozilla の新しいデータベースフォーマットを使用する場合は、`cert8.db`、`key3.db`、`secmod.db` の 3 つのファイルが必要です。`cert7.db` または `cert8.db` ファイルには、信頼できる証明書が含まれています。`key3.db` ファイルには、クライアントの鍵が含まれています。LDAP ネームサービスクライアントがクライアントの鍵を使用しない場合でも、このファイルは必要です。`secmod.db` ファイルには、`PKCS#11` などのセキュリティーモジュールが入ります。このファイルは、古いフォーマットを使用する場合には必要ありません。

詳細については、198 ページの「TLS のセキュリティーの設定」を参照してください。

クライアント資格レベルの割り当て

LDAP ネームサービスクライアントは、クライアントの資格レベルに従って LDAP サーバーへの認証を行います。LDAP クライアントには、ディレクトリサーバーへの認証を行うための複数のレベルを割り当てることができます。

- `anonymous`
- `proxy`
- `proxy anonymous`
- `self` (このドキュメントでは「ユーザー別」と呼ばれます)

LDAP anonymous 資格レベル

匿名でのアクセスを利用する場合、すべてのユーザーが使用可能なデータだけにアクセスできます。匿名モードでは、LDAP BIND 操作は実行されません。また、セキュリティーの問題も考慮する必要があります。ディレクトリの特定部分に匿名アクセスを許可する場合、そのディレクトリへのアクセス権を保持するすべてのユーザーが読み取りアクセスを保持することになります。資格レベルとして `anonymous` を使用する場合、すべての LDAP ネームエントリおよび属性に読み取りアクセスを許可する必要があります。

注意 – ディレクトリへの anonymous 書き込みを決して許可してはいけません。すべてのユーザーが、書き込みアクセス権を持っている DIT 内の情報 (別のユーザーのパスワードやそれらのユーザー独自の識別情報を含む) を変更できてしまうためです。

注 – Oracle Directory Server Enterprise Edition を使用すると、IP アドレス、DNS 名、認証方式、および時間に基づいてアクセスを制限できます。さらに指定を加えて、アクセスを制限することもできます。詳細については、使用しているバージョンの Oracle Directory Server Enterprise Edition の『管理者ガイド』のアクセス権の管理に関する章を参照してください。

LDAP proxy 資格レベル

クライアントは、LDAP バインド資格の単一の共有セット (プロキシアカウントとも呼ばれます) への認証またはバインドを行います。このプロキシアカウントには、ディレクトリへのバインドを許可されるエントリを設定できます。このプロキシアカウントは、LDAP サーバー上でネームサービス機能を実行するのに十分のアクセス権を必要とします。プロキシアカウントは、システムごとに共有されるリソースです。つまり、root ユーザーを含む、プロキシアクセスを使ってシステムにログインした各ユーザーには、そのシステム内のほかのすべてのユーザーと同じ結果が表示されます。proxy 資格レベルを使用して、すべてのクライアント上で proxyDN と proxyPassword を構成する必要があります。暗号化された proxyPassword はローカルのクライアントに格納されます。別のクライアントグループに対しては別のプロキシを設定できます。たとえば全営業クライアント用のプロキシを構成する場合、企業全体からアクセス可能なディレクトリと営業ディレクトリの両方へのアクセスを許可しつつ、給与情報を保持する人事ディレクトリへのアクセスを許可しない、という方法が可能です。もっとも極端な例として、各クライアントに別個のプロキシを割り当てることや、すべてのクライアントに同じプロキシを割り当てることも可能です。一般的な LDAP 配備はこの両極端の中間に位置します。選択は慎重に行なってください。プロキシエージェントが不足していると、リソースへのユーザーアクセスを制御する能力が制限されます。ただし、プロキシが多過ぎる場合、システムの設定および保守が困難になります。適切な権限をプロキシユーザーに付与する必要がありますが、その程度は環境によって異なります。どの認証方法が構成にもっとも適しているかを判定する方法については、148 ページの「LDAP クライアントの資格ストレージ」を参照してください。

プロキシユーザーのパスワードを変更した場合、そのプロキシユーザーを使用するすべてのクライアントで情報を更新する必要があります。LDAP アカウントのパスワード有効期間を設定する場合、プロキシユーザーに関してはこの設定を解除してください。

注 – プロキシ資格レベルは、指定されたシステムのすべてのユーザーおよびプロセスに適用されます。2 人のユーザーが異なるネーミングポリシーを使用する場合は、別個のマシンを使用するか、ユーザー別の認証モデルを使用する必要があります。

さらに、クライアントが proxy 資格を使用して認証を行う場合は、すべてのサーバー上で proxyDN の proxyPassword が同じである必要があります。

LDAP proxy anonymous 資格レベル

proxy anonymous は、複数の資格レベルが定義されているという点で複数値のエントリです。匿名プロキシレベルを割り当てられたクライアントは、最初にそのプロキシ識別情報を使用して認証を試みます。ユーザーのロックアウト、パスワードの有効期限切れなどの何らかの理由でクライアントがプロキシユーザーとしての認証ができなかった場合、クライアントは匿名アクセスを使用します。この場合、ディレクトリの構成に応じて、別のサービスレベルに移行する可能性があります。

LDAP ユーザー別の認証

ユーザー別 (self) の認証では、ディレクトリサーバーの認証時に Kerberos 識別情報 (主体) を使用して各ユーザーまたは各システムの検索が実行されます。ユーザー別の認証では、システム管理者は、アクセス制御情報 (ACI)、アクセス制御リスト (ACL)、役割、グループ、またはその他のディレクトリアクセス制御メカニズムを使用して、特定のユーザーまたはシステムの特定のネームサービスデータへのアクセスを許可または拒否できます。

注 – ユーザー別のモードを構成する場合は、このモードを表す構成値「self」を使用します。

ユーザー別の認証モデルを使用するには、Kerberos シングルサインオンサービスを配備する必要があります。また、配備に使用する 1 つ以上のディレクトリサーバーで SASL および SASL/GSSAPI 認証メカニズムをサポートする必要があります。Kerberos では、ホスト名の検索に LDAP ではなく、ファイルおよび DNS を使用することを前提としているため、この環境には DNS を配備するようにしてください。また、ユーザー別の認証を使用するには、nscd を有効にする必要があります。この構成では、nscd デーモンはオプションのコンポーネントではありません。

enableShadowUpdate スイッチ

クライアント上で enableShadowUpdate スイッチが true に設定されている場合は、シャドウデータを更新するために管理者資格が使用されます。シャドウデータは、ディレクトリサーバー上の shadowAccount オブジェクトクラス内に格納されます。管理者資格は、141 ページの「ローカルの LDAP クライアント属性」で説明され

ている adminDN および adminPassword 属性の値によって定義されます。これらの管理者資格は、それ以外の目的には使用されません。

管理者資格のプロパティーは Proxy 資格のプロパティと類似しています。管理者資格の場合、シャドウデータを読み取ったり更新するには、ユーザーはゾーンのすべての特権を持つか、root の有効な UID を持っている必要があるという例外があります。管理者資格は、ディレクトリへのバインドが許可されるエントリに割り当てることができます。ただし、LDAP サーバーの同じディレクトリマネージャー識別情報 (cn=Directory Manager) を使用しないでください。

管理者資格が設定されたこのエントリは、ディレクトリ内のシャドウデータに対する十分な読み取りおよび書き込みアクセスを持っている必要があります。このエントリはシステムごとに共有されるリソースであるため、すべてのクライアント上で adminDN および adminPassword 属性を構成する必要があります。暗号化された adminPassword はローカルのクライアントに格納されます。パスワードには、クライアント用に構成された認証方式と同じ方式が使用されます。管理者資格は、シャドウデータの読み取りと更新を行うために、特定のシステムのすべてのユーザーおよびプロセスによって使用されます。

LDAP クライアントの資格ストレージ

プロキシ識別情報を使用するようにクライアントを構成した場合、そのクライアントは、プロキシ情報を svc:/network/ldap/client サービス内に保存します。現在の LDAP 実装では、プロキシ資格がクライアントのプロファイル内に格納されません。初期化中に ldapclient を使用して設定されたプロキシ資格はすべて、SMF リポジトリ内に格納されます。このため、プロキシの DN およびパスワード情報に関するセキュリティーが向上します。クライアントプロファイルの設定方法の詳細については、第 12 章「LDAP クライアントの設定 (タスク)」を参照してください。

同様に、シャドウデータの更新を有効にするようにクライアントを構成し、クライアントの資格レベルが self でない場合、そのクライアントは自身の情報を svc:/network/ldap/client サービス内に保存します。

ユーザー別の認証を使用するようクライアントを構成している場合、認証時に各主体 (各ユーザーまたはホスト) 用の Kerberos 識別情報および Kerberos チケット情報が使用されます。この環境では、ディレクトリサーバーは Kerberos 主体を DN にマッピングします。この DN の認証には、Kerberos 資格が使用されます。次に、ディレクトリサーバーは、必要に応じアクセス制御情報 (ACI) メカニズムを使用して、ネームサービスデータへのアクセスを許可または拒否します。この状況では、ディレクトリサーバーの認証に Kerberos チケット情報が使用されます。システムが、認証 DN またはパスワードをシステムに保存することはありません。そのため、このタイプの構成の場合、クライアントが ldapclient コマンドで初期化されるときに adminDN および adminPassword 属性を指定する必要はありません。

LDAP ネームサービスの認証方法の選択

クライアントに proxy または proxy-anonymous 資格レベルを割り当てる場合は、プロキシがディレクトリサーバーへの認証を行う方法も選択する必要があります。デフォルトの認証方式は none (匿名によるアクセス) です。認証方式には、関連するトランスポートセキュリティーオプションも含まれます。

この認証方法は、資格レベルと同様に、複数値にすることができます。たとえば、クライアントプロファイルを設定することにより、クライアントが TLS でセキュリティー保護された simple メソッドを最初に使用してバインドを試みるようにできます。これが成功しない場合、クライアントは sasl/digest-MD5 メソッドを使用してバインドを試みます。それにより、authenticationMethod は tls:simple;sasl/digest-MD5 になります。

LDAP ネームサービスは、いくつかの Simple Authentication and Security Layer (SASL) メカニズムをサポートします。これらのメカニズムを使用すると、TLS なしでセキュリティー保護されたパスワードを交換できます。ただし、これらのメカニズムはデータの完全性や機密性を保証するものではありません。SASL の詳細については、RFC 2222 を参照してください。

次の認証メカニズムがサポートされています。

- none

  クライアントは、ディレクトリへの認証を行いません。これは、anonymous 資格レベルと等価です。

- simple

  認証方式 simple を使用する場合、クライアントシステムはユーザーのパスワードを平文で送信してサーバーへのバインドを実行します。このため、セッションが IPsec により保護されていない限り、パスワードが漏洩しやすくなります。simple 認証方法を使用する主な利点は、すべてのディレクトリサーバーでサポートされていることと、設定が容易なことです。

- sasl/digest-MD5

  認証時にクライアントのパスワードは保護されますが、セッションは暗号化されません。Oracle Directory Server Enterprise Edition を含む一部のディレクトリサーバーも sasl/digest-MD5 認証方法をサポートしています。digest-MD5 の主な利点は、認証中にパスワードが平文で転送されないことと、そのために simple 認証方法よりセキュアなことです。digest-MD5 については、RFC 2831 を参照してください。digest-MD5 は、セキュリティーが強化されるため、cram-MD5 に対する機能強化と見なされています。

  sasl/digest-MD5 を使用する場合、認証はセキュリティー保護されますがセッションは保護されません。

注 – Oracle Directory Server Enterprise Edition を使用している場合、パスワードをディレクトリ内に「平文」で格納する必要があります。

- `sasl/cram-MD5`

  この場合、LDAP セッションは暗号化されませんが、`sasl/cram-MD5` を使用して認証が実行されるため、認証中にクライアントのパスワードが保護されます。この認証方法は廃止されているため、使用しないでください。

- `sasl/GSSAPI`

  この認証方式は、ユーザー別の検索を有効にする場合に、self 資格モードとともに使用されます。クライアントの資格を使用するために割り当てられたユーザー別の nscd は、sasl/GSSAPI 方式およびクライアントの Kerberos 資格を使用して、ディレクトリサーバーへのバインドを実行します。ディレクトリサーバーでは、アクセスをユーザー別に制御できます。

- `tls:simple`

  クライアントは、`simple` を使用してバインドを行い、セッションは暗号化されます。パスワードは保護されます。

- `tls:sasl/cram-MD5`

  `sasl/cram-MD5` を使用して、LDAP セッションの暗号化およびクライアントによるディレクトリサーバーへの認証が行われます。

- `tls:sasl/digest-MD5`

  `sasl/digest-MD5` を使用して、LDAP セッションの暗号化およびクライアントによるディレクトリサーバーへの認証が行われます。

注意 – Oracle Directory Server Enterprise Edition で `digest-MD5` を使用する場合、パスワードを平文で格納する必要があります。認証方法が `sasl/digest-MD5` または `tls:sasl/digest-MD5` に設定されている場合は、プロキシユーザーのパスワードを平文で格納する必要があります。`userPassword` 属性を平文で格納する場合は、適切な ACI を設定することによって、この属性が読み取り不可になるように特に注意してください。

次の表に、さまざまな認証方式およびその特性の概要を示します。

表 9–4 認証方法

	バインド	通信時のパスワード	Oracle Directory Server Enterprise Edition でのパスワード	セッション
none	なし	該当なし	該当なし	暗号化なし

表 9–4 認証方法 (続き)

	バインド	通信時のパスワード	Oracle Directory Server Enterprise Edition でのパスワード	セッション
simple	あり	平文	任意	暗号化なし
sasl/digest-MD5	あり	暗号化	平文	暗号化なし
sasl/cram-MD5	あり	暗号化	該当なし	暗号化なし
sasl/GSSAPI	あり	Kerberos	Kerberos	暗号化
tls:simple	あり	暗号化	任意	暗号化
tls:sasl/cram-MD5	あり	暗号化	該当なし	暗号化
tls:sasl/digest-MD5	あり	暗号化	平文	暗号化

LDAP 内の特定のサービスの認証方法の指定

特定のサービスの認証方法は、serviceAuthenticationMethod 属性で指定できます。次のサービスでは、認証方法を選択できます。

- passwd-cmd

  このサービスは、ログインパスワードとパスワード属性を変更するために、passwd(1) によって使用されます。

- keyserv

  このサービスは、ユーザーの Diffie-Hellman 鍵ペアを作成および変更するために、chkey(1) および newkey(1M) ユーティリティーによって使用されます。

- pam_ldap

  このサービスは、pam_ldap(5) でユーザーを認証するために使用されます。

  pam_ldap は、アカウントの管理をサポートします。

注 – サービスで serviceAuthenticationMethod が設定されていない場合は、デフォルトで authenticationMethod 属性の値が使用されます。

注 – ユーザー別モードでは、154 ページの「Kerberos サービスモジュール」 (pam Kerberos) が認証サービスとして使用されます。この動作モードでは、ServiceAuthenticationMethod は必要ありません。

注 – enableShadowUpdate スイッチが true に設定されている場合、ldap_cachemgr デーモンは、passwd-cmd の serviceAuthenticationMethod パラメータで定義されている認証方法を使用して LDAP サーバーにバインドします (この方法が定義されている場合)。このパラメータが存在しない場合、authenticationMethod が使用されます。このデーモンは、none 認証方法を使用しません。

次に示す例は、クライアントプロファイルの 1 セクションです。ここで、ユーザーはディレクトリサーバーへの認証に sasl/digest-MD5 を使用しますが、パスワードの変更には SSL セッションを使用します。

```
serviceAuthenticationMethod=pam_ldap:sasl/digest-MD5
serviceAuthenticationMethod=passwd-cmd:tls:simple
```

プラグイン可能な認証方法

PAM フレームワークを使用すると、pam_unix_*、pam_krb5、および pam_ldap_* モジュールを含む複数の認証サービスから選択できます。

ユーザー別の認証方式を使用する場合、上記の 3 つの認証サービスの中でもっとも強力な pam_krb5 を有効にする必要があります。pam_krb5(5) および『Oracle Solaris 11.1 の管理: セキュリティーサービス』を参照してください。

ユーザー別の認証が有効でない場合でも、pam_krb5 認証システムを使用できます。プロキシまたは匿名の資格レベルを使用してディレクトリサーバーのデータにアクセスする場合、ディレクトリデータへのアクセスをユーザーごとに制限することはできません。

匿名またはプロキシ認証方法が使用される場合は、pam_unix_* モジュールの使用よりも、より高い柔軟性、より強力な認証方法のサポート、およびアカウント管理を使用する機能を備えた pam_ldap モジュールの使用をお勧めします。

pam_unix_* サービスモジュール

/etc/pam.conf ファイルを変更していない場合は、デフォルトで UNIX 認証が有効になります。

注 – pam_unix モジュールは削除されており、Oracle Solaris リリースではサポートされなくなりました。その他のサービスモジュールによって、同等またはそれ以上の機能が提供されます。したがって、このガイドでは、pam_unix は pam_unix モジュールではなくその同等の機能を指します。

次に示すのは、元の pam_unix モジュールと同等の機能を提供するモジュールの一覧です。

pam_authtok_check(5)
pam_authtok_get(5)
pam_authtok_store(5)
pam_dhkeys(5)
pam_passwd_auth(5)
pam_unix_account(5)
pam_unix_auth(5)
pam_unix_cred(5)
pam_unix_session(5)

pam_unix_* モジュールは、次に説明されている従来の UNIX 認証モデルに従います。

1. クライアントは、ネームサービスからユーザーの暗号化されたパスワードを取得します。
2. ユーザーは、ユーザーパスワードの入力を求められます。
3. ユーザーのパスワードが暗号化されます。
4. クライアントは、暗号化された 2 つのパスワードを比較して、ユーザーを認証するかどうかを決定します。

さらに、pam_unix_* モジュールを使用する場合は 2 つの制限事項があります。

- パスワードは、平文を含むほかの暗号化方式ではなく、UNIX crypt 形式で格納する必要があります。
- userPassword 属性は、ネームサービスから読み取り可能でなければなりません。

  たとえば、資格レベルを anonymous に設定した場合は、すべてのユーザーが userPassword 属性を読み取れる必要があります。同様に、資格レベルを proxy に設定した場合は、プロキシユーザーが userPassword 属性を読み取れる必要があります。

注 – Oracle Directory Server Enterprise Edition で digest-MD5 を使用するにはパスワードを平文で格納する必要があるため、UNIX 認証は sasl 認証方法の digest-MD5 と互換性がありません。UNIX 認証では、パスワードを crypt 形式で格納する必要があります。

注 – pam_unix_account モジュールは、enableShadowUpdate スイッチが true に設定されている場合はアカウント管理をサポートします。リモート LDAP ユーザーアカウントに対する制御は、passwd および shadow ファイルで定義されたローカルユーザーアカウントに適用される制御と同じように適用されます。enableShadowUpdate モードでは、LDAP アカウントについてはシステムが更新を行い、パスワードの有効期限管理とアカウントのロックのために LDAP サーバー上のシャドウデータを使用します。ローカルアカウントのシャドウデータはローカルクライアントシステムに適用されるのに対して、LDAP ユーザーアカウントのシャドウデータはすべてのクライアントシステムのユーザーに適用されます。

パスワードの履歴チェックは、ローカルクライアントに対してのみサポートされ、LDAP ユーザーアカウントに対してはサポートされません。

Kerberos サービスモジュール

pam_krb5(5) のマニュアルページおよび『Oracle Solaris 11.1 の管理: セキュリティーサービス』を参照してください。

LDAP サービスモジュール

LDAP 認証を実装する場合、ユーザーは、pam_ldap の serviceAuthenticationMethod パラメータで定義されている認証方法を使用して LDAP サーバーにバインドします (このパラメータが存在する場合)。このパラメータが存在しない場合、authenticationMethod が使用されます。

pam_ldap が、ユーザーの識別情報および指定されたパスワードでサーバーにバインドできれば、ユーザーが認証されたことになります。

注 – 以前は、pam_ldap アカウント管理を有効にすると、システムにログインする際には、常にすべてのユーザーが認証用にログインパスワードを入力する必要がありました。そのため、ssh などのツールを使用した、パスワードに基づかないログインは失敗します。

アカウント管理を実行し、ユーザーがログインしているときに Directory Server への認証を行わずにユーザーのアカウントステータスを取得します。Directory Server 上の新しい制御は 1.3.6.1.4.1.42.2.27.9.5.8 です。これはデフォルトで有効になっています。

この制御をデフォルト以外に変更する場合は、Directory Server 上でアクセス制御情報 (ACI) を追加します。

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
     allow (read, search, compare, proxy)
     (groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

pam_ldap は、userPassword 属性を読み取りません。そのため、UNIX 認証を使用しているほかのクライアントが存在しないかぎり、userPassword 属性を読み取るためのアクセス権を付与する必要はありません。また、pam_ldap は none 認証方法もサポートしていません。そのため、クライアントが pam_ldap を使用できるように、serviceAuthenticationMethod または authenticationMethod 属性を定義する必要があります。詳細は、pam_ldap(5) のマニュアルページを参照してください。

注意 – 認証方式 simple を使用する場合、第三者がネットワーク上で userPassword 属性を読み取ることができます。

次の表に、認証メカニズム間の主な相違点を示します。

表 9–5 LDAP での認証動作

イベント	pam_unix_*	pam_ldap	pam_krb5
パスワードの送信	passwd サービス認証方式を使用します	passwd サービス認証方式を使用します	パスワードではなく、Kerberos シングルサインオンテクノロジを使用します

表 9–5 LDAP での認証動作 (続き)

イベント	pam_unix_*	pam_ldap	pam_krb5
新規パスワードの送信	暗号化される	暗号化しません (TLS を使用しない場合)	Kerberos を使用します。パスワードはネットワークに送信されません
新規パスワードの格納	crypt 形式	Oracle Directory Server Enterprise Edition で定義されたパスワード格納スキーム	パスワードは Kerberos を使って管理されます
パスワードの読み取りが必要か	あり	なし	なし
パスワード変更後の sasl/digestMD5 の互換性	ありません。パスワードは平文では格納されません。ユーザーを認証できません。	あり。デフォルトのストレージスキームが平文 (clear) に設定されていれば、ユーザーを認証できます。	ありません。sasl/GSSAPI が使用されます。Kerberos kdc を使用して LDAP ディレクトリサーバー内のパスワードデータベースを管理する場合を除き、パスワードがネットワーク上に送信されることも、ディレクトリサーバーに保存されることもありません。
パスワードポリシーがサポートされるか	はい。enableShadowUpdate を true に設定する必要があります。	はい (構成されている場合)。	pam_krb5(5)、Kerberos V5 アカウント管理モジュールを参照してください。

PAM およびパスワードの変更

パスワードを変更するには、passwd コマンドを使用します。enableShadowUpdate スイッチが true に設定されていない場合、userPassword 属性がユーザーによって書き込み可能である必要があります。enableShadowUpdate スイッチが true に設定されている場合、管理者資格で userPassword 属性を更新できる必要があります。passwd-cmd の serviceAuthenticationMethod によって、この操作のための authenticationMethod がオーバーライドされることに注意してください。使用する認証方式によっては、現行のパスワードの暗号化解除がネットワーク上で行われる場合があります。

UNIX 認証の場合は、新しい userPassword 属性が UNIX crypt 形式を使用して暗号化され、タグ付けされてから LDAP に書き込まれます。このため、新規パスワード

は、サーバーへのバインドに使用される認証方式に関係なく、ネットワーク上で暗号化されます。詳細は、pam_authtok_store(5) のマニュアルページを参照してください。

enableShadowUpdate スイッチが true に設定されている場合は、ユーザーパスワードが変更されると、pam_unix_* モジュールも関連するシャドウ情報を更新します。pam_unix_* モジュールは、ローカルのユーザーパスワードが変更されたときにこれらのモジュールが更新するローカルの shadow ファイル内の同じ shadow フィールドを更新します。

pam_ldap では、パスワード更新がサポートされなくなりました。pam_ldap のパスワード更新機能は現在、server_policy オプションを指定した pam_authtok_store によって置き換えられています。pam_authtok_store を使用した場合、新しいパスワードは平文で LDAP サーバーに送信されます。このため、機密性を保つために TLS を使用する必要があります。TLS が使用されていない場合は、新しい userPassword が漏洩する危険性があります。Oracle Directory Server Enterprise Edition でタグなしパスワードを設定すると、ソフトウェアは、passwordStorageScheme 属性を使用してパスワードを暗号化します。passwordStorageScheme の詳細については、使用しているバージョンの Oracle Directory Server Enterprise Edition の『管理者ガイド』の ユーザーアカウントの管理に関するセクションを参照してください。

注 – passwordStorageScheme 属性を設定する際、次の構成上の問題を考慮する必要があります。NIS や、UNIX 認証を使用している別のクライアントが LDAP をリポジトリとして使用している場合は、passwordStorageScheme を crypt にする必要があります。また、Oracle Directory Server Enterprise Edition で sasl/digest-MD5 の LDAP 認証を使用している場合は、passwordStorageScheme を平文に設定する必要があります。

LDAP アカウント管理

アカウントおよびパスワードの管理システムとして pam_krb5 を選択すると、アカウント、パスワード、アカウントロックアウト、およびアカウント管理のその他の詳細情報がすべて Kerberos 環境により管理されます。pam_krb5(5) および『Oracle Solaris 11.1 の管理: セキュリティーサービス』を参照してください。

pam_krb5 を使用しない場合は、LDAP ネームサービスを構成して、Oracle Directory Server Enterprise Edition のパスワードおよびアカウントロックアウトポリシーのサポートを活用できます。ユーザーアカウント管理をサポートするように pam_ldap(5) を構成できます。passwd(1) を適切な PAM 構成で使用すると、Oracle Directory Server Enterprise Edition パスワードポリシーによって設定されたパスワードの構文規則が適用されます。

pam_ldap(5) によって、次のアカウント管理機能がサポートされます。これらの機能は、Oracle Directory Server Enterprise Edition のパスワードとアカウントのロックアウトポリシー構成を利用しています。必要な機能を必要な数だけ利用できます。

- 古くなったり、有効期限の切れたパスワードを通知する

  パスワードは、予定にしたがって変更する必要があります。構成された期間内にパスワードを変更しないとそのパスワードは無効になります。期限切れのパスワードでは、ユーザーが認証されません。

  期限切れの警告期間内のログイン時には、常に警告メッセージを表示します。メッセージには期限切れまでの日数と時間が表示されます。

- パスワードの構文チェック

  新規パスワードは、最小文字数の条件を満たしている必要があります。さらに、パスワードを、ユーザーのディレクトリエントリ内の `uid`、`cn`、`sn`、または `mail` 属性の値に一致させることはできません。

- パスワードの履歴チェック

  パスワードの再利用はできません。ユーザーがパスワードを以前使用されていたものに変更しようとすると、`passwd(1)` は失敗します。LDAP 管理者は、サーバーの履歴リストに保持するパスワードの数を構成することができます。

- ユーザーアカウントのロックアウト

  認証の失敗が設定された回数に達すると、そのユーザーアカウントはロックアウトされます。管理者がアカウントを非アクティブにした場合も、そのユーザーはロックアウトされます。アカウントのロックアウト期間が経過するか、管理者が再びアカウントをアクティブにするまで、認証は成功しません。

注 – 以上のアカウント管理機能は、Oracle Directory Server Enterprise Edition だけで有効です。サーバー上のパスワードとアカウントのロックアウトポリシーの構成についての詳細は、使用しているバージョンの Oracle Directory Server Enterprise Edition の『管理者ガイド』の「ユーザーアカウントの管理」の章を参照してください。212 ページの「アカウント管理に `pam_ldap` モジュールを使用した `pam_conf` ファイルの例」も参照してください。`proxy` アカウントに対するアカウント管理を有効にしないでください。

Oracle Directory Server Enterprise Edition でパスワードとアカウントのロックアウトポリシーを構成する前に、すべてのホストで `pam_ldap` アカウント管理による「最新の」LDAP クライアントが使用されていることを必ず確認してください。

さらに、クライアントに、正しく構成された `pam.conf(4)` ファイルが存在することも確認してください。正しい構成ファイルを保持していない場合、LDAP ネームサービスは `proxy` やユーザーパスワードが期限切れの時に動作しません。

注 – 以前は、pam_ldap アカウント管理を有効にすると、システムにログインする際には、常にすべてのユーザーが認証用にログインパスワードを入力する必要がありました。そのため、ssh などのツールを使用した、パスワードに基づかないログインは失敗します。

アカウント管理を実行し、ユーザーがログインしているときに Directory Server への認証を行わずにユーザーのアカウントステータスを取得します。Directory Server 上の新しい制御は 1.3.6.1.4.1.42.2.27.9.5.8 です。これはデフォルトで有効になっています。

この制御をデフォルト以外に変更する場合は、Directory Server 上でアクセス制御情報 (ACI) を追加します。

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
     allow (read, search, compare, proxy)
     (groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

pam_unix_* モジュールによる LDAP アカウント管理

クライアント上で enableShadowUpdate スイッチが true に設定されている場合は、ローカルアカウントに使用可能なアカウント管理機能が LDAP アカウントにも使用できます。この機能には、パスワードの有効期限管理、アカウントの有効期限管理および通知、ログインに失敗したアカウントのロックなどが含まれます。また、passwd コマンドの -dluNfnwx オプションが LDAP でサポートされるようになりました。これにより、ファイルネームサービスでの passwd コマンドと pam_unix_* モジュールのすべての機能が LDAP ネームサービスでサポートされます。enableShadowUpdate スイッチは、ファイルと LDAP スコープの両方で定義されているユーザーのための一貫性のあるアカウント管理を実装する方法を提供します。

ユーザーが自身のアカウント管理データを変更するのを防ぐため、また、パスワードポリシーを回避するために、LDAP サーバーは、サーバー上にあるユーザー自身のシャドウデータに対するユーザーの書き込みアクセスを防止するように構成されています。管理者資格を持つ管理者は、クライアントシステムに対してシャドウデータの更新を実行します。しかし、この構成は、ユーザーによるパスワードの変更が必要な pam_ldap モジュールと競合してしまいます。そのため、pam_ldap と pam_unix_* モジュールによるアカウント管理には互換性がありません。

注意 – 同じ LDAP ネームドメイン内で `pam_ldap` モジュールと `pam_unix_*` モジュールの両方を使用しないでください。すべてのクライアントが `pam_ldap` モジュールを使用するか、またはすべてのクライアントが `pam_unix_*` モジュールを使用するかのどちらかです。この制限により、専用の LDAP サーバーが必要になる場合があります。たとえば、Web または電子メールアプリケーションでは、ユーザーが LDAP サーバー上にあるパスワードを変更する必要がある場合があります。

`enableShadowUpdate` の実装にはまた、管理者資格 (`adminDN` および `adminPassword`) がすべてのクライアント上でローカルに格納されていることも必要です。この情報は、`svc:/network/ldap/client` サービス内に格納されます。

アカウント管理に `pam_ldap` を使用する場合とは異なり、アカウント管理に `pam_unix_*` モジュールを使用する場合は `/etc/pam.conf` ファイルへの変更は必要ありません。デフォルトの `/etc/pam.conf` ファイルで十分です。

◆ ◆ ◆ 第 10 章

10 LDAP ネームサービスの計画要件 (タスク)

この章では、サーバーとクライアントの設定およびインストール処理を開始する前に実行する必要のある上流工程の計画について説明します。

この章の内容は次のとおりです。

LDAP の計画の概要

LDAP クライアントプロファイルは、LDAP クライアントが使用する構成情報の集合体です。 LDAP クライアントは、このプロファイルを使用して、サポートする LDAP サーバーについての LDAP ネームサービス情報にアクセスします。この章では、LDAP ネームサービスのさまざまな分野での計画方法を説明します。その中には、ネットワークモデル、ディレクトリ情報ツリー、セキュリティーモデル、さまざまなプロファイル属性のデフォルト値、およびデータ生成の準備が含まれます。

LDAP ネットワークモデルの計画

可用性およびパフォーマンスを考慮すると、企業規模のネットワークの各サブネットが LDAP サーバーを独自に保持して、サブネット内のすべての LDAP クライアントにサービスを提供する方法が最善です。これらのサーバーの 1 つだけをマスター LDAP サーバーにする必要があります。残りはすべてマスターサーバーの複製にできます。

ネットワーク構成を計画する前に、使用可能なサーバーの数、クライアントがサーバーにアクセスする方法、複数のサーバーへのアクセス順序について考慮する必要があります。サブネットごとに 1 つのサーバーが存在する場合、`defaultServerList` 属性を使用してすべてのサーバーのリストを作成し、LDAP クライアントからアクセス順序をソートおよび操作できます。速度やデータ管理上の理由でサーバーに特定の順序でアクセスする必要がある場合は、`preferredServerList` 属性を使用して、サーバーにアクセスするときの固定された順序を定義するようにしてください。`defaultServerList` がリスト内のすべてのサーバーを均等に処理するのに対して、`preferredServerList` でのサーバーは優先順位の順になります。ここで、リスト内の最初のサーバーが使用するための最適なサーバーです。主な違いは、`preferredServerList` が使用されている場合は、もっとも高い優先順位を持つ使用可能なサーバーが、より低い優先順位を持つ別の使用可能なサーバーより優先して使用される点にあります。より高い優先順位を持つサーバーが使用可能になった場合は、より低い優先順位のサーバーからクライアントマシンが切り離されます。`defaultServerList` が使用されている場合は、すべてのサーバーが等しい優先順位を持つため、あるサーバーがオンラインになっても既存のサーバーは置き換えられません。1 つの構成内で両方のリストを使用できます。マスターサーバーをこれらのリストに配置しないことで、マスターサーバーへの負荷を軽減できます。

さらに、サーバーおよびネットワーク構成を計画する際に考慮するに値する 3 つの属性があります。`bindTimeLimit` 属性は TCP 接続要求のタイムアウト値の設定に使用されます。`searchTimeLimit` 属性は LDAP 検索操作のタイムアウト値の設定に、`profileTTL` 属性は LDAP クライアントによるサーバーからのプロファイルのダウンロード頻度の制御に、それぞれ使用できます。速度が遅いか不安定なネットワークの場合、`bindTimeLimit` および `searchTimeLimit` 属性にデフォルト値より大きい値を設定することが必要な場合があります。配備の初期テスト段階で、`profileTTL` 属性値を引き下げて、頻繁に行われる LDAP サーバー内のプロファイルの変更をクライアントが取得するようにしてもよいでしょう。

ディレクトリ情報ツリーの計画

LDAP ネームサービスは、デフォルトのディレクトリ情報ツリー (DIT) および関連するデフォルトのスキーマを保持します。たとえば、ou=people コンテナには、ユーザーアカウント、パスワード、およびシャドウ情報が含まれています。ou=hosts コンテナには、ネットワーク内のシステムに関する情報が含まれています。ou=people コンテナ内の各エントリは、objectclass posixAccount および shadowAccount のエントリになります。

デフォルト DIT は適切に設計されたディレクトリ構造であり、オープンな標準に基づいています。詳細は、RFC 2307bis および RFC 4876 を参照してください。デフォルト DIT は、ほとんどのネームサービスニーズにとって十分であり、変更なしで使用することが推奨されます。デフォルト DIT を使用することを選択した場合は、特定のドメインに関して、ディレクトリツリー内のどのノード (ベース DN) からネームサービス情報を検索するかを決定するだけで済みます。このノードは、defaultSearchBase 属性を使用して指定されます。さらに、defaultSearchScope 属性を設定して、ネームサービスが実行する検索範囲をクライアントに指定することもできます。検索範囲には、識別名 (DN) 内の 1 レベルだけを検索するか (one)、DN 内のサブツリー全体を選択するか (sub) を指定できます。

ただし、既存の DIT を利用する場合でも、ディレクトリツリー内に散在するネームサービスデータを使用してより複雑な DIT を処理する場合でも、LDAP ネームサービスにより高度な柔軟性が求められる場合があります。たとえば、ユーザーアカウントエントリがツリーの別の場所に存在する場合があります。クライアントプロファイル内の serviceSearchDescriptor、attributeMap、および objectclassMap 属性は、これらの状況に対処するように設計されています。

サービス検索記述子を使用して、特定のサービスのデフォルト検索ベース、検索範囲、および検索フィルタをオーバーライドできます。137 ページの「サービス検索記述子とスキーママッピング」を参照してください。

attributeMap および objectclassMap 属性は、スキーママッピングの方法を提供します。これらの属性を使用すると、既存の DIT で LDAP ネームサービスを動作させることができます。たとえば、posixAccount オブジェクトクラスを既存のオブジェクトクラス myAccount にマップできます。posixAccount オブジェクトクラス内の属性を myAccount オブジェクトクラス内の属性へマップできます。

複数のディレクトリサーバー

複数の LDAP サーバーで 1 つの DIT を構成することも可能です。たとえば、DIT のいくつかのサブツリーを、ほかの LDAP サーバー上に配置できます。この場合、LDAP サーバーは、既知ではあるが自身のデータベース内に存在しないネームデータを求める LDAP クライアントを、別のサーバーに委ねることができます。このような DIT 構成を計画する場合は、クライアントのプロファイル属性 followReferrals を設定し

て、サーバー参照に従ってネームサービスの検索を続行するよう LDAP ネームサービスに指示するようにしてください。ただし可能であれば、指定されたドメインのネームデータすべてを単独のディレクトリサーバー上に配置するのが最善です。

クライアントが通常は読み取り専用の複製にアクセスし、必要な場合にのみ読み取り/書き込み可能なマスターサーバーへの参照を利用する場合、参照が役に立ちます。この方法では、要求が複製により処理されるため、マスターサーバーに過度の負荷がかかることはありません。

ほかのアプリケーションとのデータ共有

LDAP を最大限に活用するには、論理エントリごとに 1 つの LDAP エントリが存在する必要があります。たとえば、ユーザーのために、企業白書の情報だけでなく、アカウント情報や、場合によってはアプリケーション固有のデータも保持できます。`posixAccount` と `shadowAccount` は補助オブジェクトクラスであるため、ディレクトリ内の任意のエントリに追加できます。このため、注意深い計画、設定、および管理が必要になります。

ディレクトリ接尾辞の選択

適切なディレクトリ接尾辞を選択する方法については、Oracle Directory Server Enterprise Edition のドキュメントを参照してください。

LDAP と複製サーバー

複製サーバーを設定する場合、次の 3 つの方法が存在します。

- 単一マスター複製
- 浮動マスター複製
- 複数マスター複製

単一マスター

単一マスター複製では、指定されたパーティションまたはパーティション化されていないネットワークに対して、1 つのマスターサーバーだけが、ディレクトリエントリの書き込み可能なコピーを保持します。複製サーバーは、ディレクトリエントリの読み込み専用コピーを保持します。複製とマスターの両方が検索、比較、およびバインド操作を実行できますが、書き込み操作を実行できるのはマスターサーバーだけです。

単一マスター複製の不利な点は、マスターサーバーで単一点障害が発生した場合です。マスターサーバーがダウンした場合、どの複製サーバーからも書き込み操作を実行できません。

浮動マスター

浮動マスターは、指定されたパーティション化されたネットワークまたはパーティション化されていないネットワークに対し、書き込み権限を保持するマスターサーバーは常に 1 つだけである点で、単一マスターを使用する場合と似ています。ただし浮動マスターを使用すると、マスターサーバーがダウンした場合、アルゴリズムにより複製の 1 つが自動的にマスターサーバーに変化します。

浮動マスター複製の不利な点は、ネットワークがパーティション化され、どちらの側のパーティション上の複製もマスターになった場合、ネットワークを再結合する際、新規マスター間の調整が非常に複雑になり得ることです。

複数マスター

複数マスター複製では、ディレクトリエントリデータの独自の読み取り/書き込み複製を保持する、複数のマスターサーバーが存在します。複数マスターを使用すると、単一点障害を防ぐことができますが、サーバー間で更新による競合が発生する可能性があります。つまり、2 つのマスター上でエントリの属性が同時に変更される場合、競合による障害の解決ポリシー (最後の書き込みを優先するなど) の適用が必要になります。

複製サーバーを設定する方法については、使用しているバージョンの Oracle Directory Server Enterprise Edition の『管理者ガイド』を参照してください。一般に、大規模なエンタープライズ配備には、複数マスター複製が推奨されるオプションです。

LDAP セキュリティーモデルの計画

セキュリティーモデルを計画する場合、最初に、LDAP クライアントが LDAP サーバーとの通信に使用する識別情報を考慮する必要があります。たとえば、企業全体でシングルサインオンソリューションを使用するかどうか、ネットワークにパスワードを送信しないかどうか、ネットワークに流れるデータの暗号化、およびディレクトリサーバーで生成される制御データへのユーザー別のアクセス機能などを決定する必要があります。また、強力な認証を使用してネットワーク上を流れるユーザーパスワードを保護するかどうか、また LDAP クライアントと LDAP サーバー間のセッションを暗号化して送信される LDAP データを保護する必要があるかなども決定する必要があります。

これには、プロファイル内の `credentialLevel` および `authenticationMethod` 属性が使用されます。`credentialLevel` に指定できる資格レベルとして、`anonymous`、`proxy`、`proxy anonymous`、`self` の 4 つがあります。LDAP ネームサービスのセキュリティー概念については、143 ページの「LDAP ネームサービスのセキュリティーモデル」を参照してください。

注 – 以前は、pam_ldap アカウント管理を有効にすると、システムにログインする際には、常にすべてのユーザーが認証用にログインパスワードを入力する必要がありました。そのため、ssh などのツールを使用した、パスワードに基づかないログインは失敗します。

アカウント管理を実行し、ユーザーがログインしているときに Directory Server への認証を行わずにユーザーのアカウントステータスを取得します。Directory Server 上の新しい制御は 1.3.6.1.4.1.42.2.27.9.5.8 です。これはデフォルトで有効になっています。

この制御をデフォルト以外に変更する場合は、Directory Server 上でアクセス制御情報 (ACI) を追加します。

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
     allow (read, search, compare, proxy)
     (groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

注 – 企業全体のシングルサインオンソリューションとして pam_krb5 および Kerberos を有効にする場合、セッション開始時にのみログインパスワードを必要とするシステムを設計できます。詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』を参照してください。一般に、Kerberos を有効にする場合には、DNS も有効にする必要があります。詳細については、このマニュアルの DNS に関する章を参照してください。

セキュリティーモデルを計画する際の主要な決定事項を次に示します。

- Kerberos およびユーザー別の認証を使用するか。
- LDAP クライアントは、どの資格レベルおよび認証方式を使用するか。
- TLS を使用するか。
- NIS との下位互換性が必要ですか。つまり、クライアントは pam_unix_* または pam_ldap モジュールのどちらを使用しますか。
- サーバーの passwordStorageScheme 属性をどのように設定するか。
- アクセス制御情報をどのように設定するか。

  ACI の詳細については、使用しているバージョンの Oracle Directory Server Enterprise Edition の『管理者ガイド』を参照してください。

- クライアントは、pam_unix_* または pam_ldap モジュールのどちらを使用して LDAP アカウント管理を実行しますか。

LDAP 用のクライアントプロファイルおよびデフォルト属性値の計画

前述の計画手順 (ネットワークモデル、DIT、およびセキュリティーモデル) を理解することにより、次のプロファイル属性の値についてアイデアを得ることができるでしょう。

- cn
- defaultServerList
- preferredServerList
- bindTimeLimit
- searchTimeLimit
- profileTTL
- defaultSearchBase
- defaultSearchScope
- serviceSearchDescriptor
- attributeMap
- objectclassMap
- followReferrals
- credentialLevel
- authenticationMethod
- serviceCredentialLevel
- serviceAuthenticationMethod

上記の属性の中で、必須属性は cn、defaultServerList、および defaultSearchBase だけです。これらの属性には、デフォルト値は存在しません。残りの属性はオプションであり、デフォルト値がないオプションも存在します。

LDAP クライアントの設定の詳細については、第 12 章「LDAP クライアントの設定 (タスク)」を参照してください。

LDAP データ生成の計画

データを使用して LDAP サーバーを生成する場合、適切な DIT およびスキーマを使用して LDAP サーバーを構成したあとで、新しい ldapaddent ツールを使用します。このツールは、対応する /etc ファイルから LDAP コンテナ内のエントリを作成します。このツールを使用して、次のデータタイプ用のコンテナ内にデータを生成することができます。aliases、 auto_*、 bootparams、 ethers、 group、 hosts (IPv6 アドレスを含む)、 netgroup、 netmasks、 networks、 passwd、 shadow、 protocols、

publickey、 rpc、 および services。また、RBAC 関連のファイル /etc/user_attr、 /etc/security/auth_attr、 /etc/security/prof_attr、 および /etc/security/exec_attr も追加できます。

デフォルトでは、ldapaddent は標準入力からこのデータを読み取って、コマンド行で指定されたデータベースに関連付けられた LDAP コンテナに追加します。ただし、データを読み取る入力ファイルは、-f オプションを使用して指定できます。

エントリはクライアントの構成に基づき、ディレクトリ内に格納されるため、LDAP ネームサービスを使用するようにクライアントを構成する必要があります。

パフォーマンスを向上させるため、次の順序でデータベースをロードしてください。

1. passwd データベースの次に shadow データベース
2. networks データベースの次に netmasks データベース
3. bootparams データベースの次に ethers データベース

オートマウンタのエントリを追加する場合は、データベース名の形式が auto_* (たとえば、auto_home) になることに注意してください。

別のホストの /etc ファイルを LDAP サーバーに追加する場合は、それらをすべて同じ /etc ファイルにマージしてから、1 つのホスト上で ldapaddent コマンドを使用してファイルを追加するか、または各ホストがすでに LDAP クライアントとして構成されていると想定して、別のホスト上で ldapaddent コマンドを 1 つずつ実行するかのどちらかを行うことができます。

ネームサービスデータがすでに NIS サーバー内に存在し、そのデータを LDAP ネームサービスの LDAP サーバーに移動する場合は、ypcat コマンドを使用して NIS マップをファイルにダンプします。次に、これらのファイルに対して ldapaddent コマンドを実行して LDAP サーバーにデータを追加します。

次の作業は、テーブルが yp クライアントから抽出されることを想定しています。

▼ ldapaddent コマンドを使用してサーバーに host エントリを生成する方法

1 **idsconfig** コマンドを使用して、**Oracle Directory Server Enterprise Edition** が設定されていることを確認します。

2 クライアントマシンで、スーパーユーザーになるか、同等の役割になります。

役割には、認証と特権コマンドが含まれます。役割についての詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の第 9 章「役割に基づくアクセス制御の使用 (タスク)」を参照してください。

3 そのマシンを LDAP クライアントに設定します。

```
# ldapclient init -a profileName=new -a domainName=west.example.com 192.168.0.1
```

4 データを指定してサーバーを生成します。

```
# ldapaddent -D “cn=directory manager” -f /etc/hosts hosts
```

パスワードの入力を求められます。

この例では、ldapaddent コマンドは、プロファイル new 内に構成されている認証方法を使用します。「simple」を選択した場合、パスワードは平文で送信されます。詳細は、ldapaddent(1M) のマニュアルページを参照してください。

スタンドアロンモードでは、このコマンドは次のように表示されます。

```
# ldapaddent -h 192.168.0.1 -N new -M west.example.com -a simple-D “cn=directory manager” -f /etc/hosts hosts
```

◆ ◆ ◆ 第 11 章

LDAP クライアントと Oracle Directory Server Enterprise Edition の設定 (タスク)

この章では、LDAP ネームサービスクライアントのネットワークをサポートするように Oracle Directory Server Enterprise Edition を構成する方法について説明します。この情報は、Oracle Directory Server Enterprise Edition に固有の情報です。ディレクトリサーバーのインストールと構成については、Oracle Directory Server Enterprise Edition のドキュメントを参照してください。

注 – Oracle Directory Server Enterprise Edition を構成して LDAP クライアントを使用する前に、Oracle Directory Server Enterprise Edition に付属するインストールおよび構成のドキュメントで説明されているすべての手順を実行しておく必要があります。

注 – ディレクトリサーバー (LDAP サーバー) をそのクライアントとして使用することはできません。

この章の内容は次のとおりです。

idsconfig コマンドを使用した Oracle Directory Server Enterprise Edition の構成

サーバーのインストール用チェックリストの作成

サーバーのインストールプロセス中に、非常に重要な変数を定義します。idsconfig を起動する前に、これらの変数を使用して、次に示すようなチェックリストを作成するようにしてください。209 ページの「LDAP を構成するための空白のチェックリスト」で提供されている空白のチェックリストを使用できます。

注 – 次の情報は、LDAP 関連の章で示されるすべての例の基礎となります。ドメインの例は、全国規模で店舗を展開する部品会社である Example, Inc. のものです。これらの例では、west.example.com のドメイン名を持つ West Coast Division を扱っています。

表 11–1　example.com ネットワークで定義されているサーバー変数

変数	サンプルネットワークの定義
インストールしたディレクトリサーバーインスタンスのポート番号	389 (デフォルト)
サーバーの名前	myserver (FQDN myserver.west.example.com または 192.168.0.1 のホスト名から)
複製サーバー (IP 番号:ポート番号)	192.168.0.2 [myreplica.west.example.com の場合]
ディレクトリマネージャー	cn=directory manager (デフォルト)
サービスされるドメイン名	west.example.com
クライアント要求の処理がタイムアウトするまでの時間 (秒)	1
各検索要求で返されるエントリの最大数	1

注 – defaultServerList または preferredServerList の定義でホスト名を使用している場合は、LDAP がホスト検索に使用されていないことを確認する必要があります。つまり、svc:/network/name-service/switch サービスの config/host プロパティーで ldap が構成されていてはいけません。

表 11–2　example.com ネットワークで定義されているクライアントプロファイル変数

変数	サンプルネットワークの定義
プロファイル名 (デフォルト名は「default」)	WestUserProfile
サーバーリスト (デフォルトはローカルサブネット)	192.168.0.1
優先されるサーバーリスト (優先順に記載)	none
検索範囲 (検索するディレクトリツリーレベルの数、「One」(デフォルト) または「Sub」)	one (デフォルト)
サーバーへのアクセスに使用する資格。デフォルトは anonymous です。	proxy
参照に従うかどうか (メインサーバーが使用できない場合の別のサーバーへのポインタ)。デフォルトは no です。	Y
検索時にサーバーが情報を返すまでの待機時間の制限 (デフォルトは 30)	default
サーバーとの通信時のバインド時間の制限 (デフォルトは 10 秒)	default
認証方式。デフォルトは none	simple

注 – クライアントプロファイルはドメインごとに定義されます。指定されたドメインで、1 つ以上のプロファイルを定義する必要があります。

属性インデックス

idsconfig コマンドは、パフォーマンス向上のために、次の属性のリストのインデックスを作成します。

```
membernisnetgroup    pres,eq,sub
nisnetgrouptriple    pres,eq,sub
ipHostNumber         pres,eq,sub
uidNumber            pres,eq
gidNumber            pres,eq
ipNetworkNumber      pres,eq
automountkey         pres,eq
oncRpcNumber         pres,eq
```

スキーマ定義

idsconfig(1M) によって、必要なスキーマ定義が自動的に追加されます。LDAP 管理に精通しているユーザー以外、サーバースキーマを手動で変更してはなりません。LDAP ネームサービスによって使用されるスキーマの拡張されたリストについては、第 14 章「LDAP ネームサービス (リファレンス)」を参照してください。

インデックス表示の使用

Oracle Directory Server Enterprise Edition のインデックス表示機能は、仮想リスト表示 (VLV) とも呼ばれ、クライアントが非常に長いリストから選択したグループまたは選択した数のエントリを表示するための方法を提供します。これにより、各クライアントでの検索プロセスにかかる時間が短縮されます。インデックス表示により、LDAP ネームサービスクライアントがさまざまなサービスの特定の情報によりすばやくアクセスするために使用できる、最適化された定義済みの検索パラメータが提供されます。インデックス表示を作成しない場合は、サーバーの制限を超えると、クライアントが特定のタイプの一部のエントリにアクセスしなくなることに注意してください。たとえば、5000 のパスワードエントリがあっても、1000 エントリのサイズ制限が有効になっている場合は、一部の検索操作中に 4000 のエントリは返されません。これにより、クライアントマシンで、ログインやその他の重大な障害が発生する場合が多くあります。

VLV はディレクトリサーバー上に構成されるため、プロキシユーザーはこれらのインデックスに読み取りアクセス権限を保持します。

Oracle Directory Server Enterprise Edition 上でインデックス表示を構成する前に、これらのインデックスの使用に関連したパフォーマンスのコストを検討してください。詳細については、使用しているバージョンの Oracle Directory Server Enterprise Edition の管理者ガイドを参照してください。

`idsconfig` は、複数の VLV インデックスのエントリを作成します。詳細は、idsconfig(1M) のマニュアルページを参照してください。`idsconfig` によって作成された VLV エントリを確認するには、`idsconfig` コマンドの出力を参照してください。`idsconfig` のサンプル出力については、177 ページの「`idsconfig` 設定の例」を参照してください。

サービス検索記述子を使用してさまざまなサービスへのクライアントアクセスを変更する

サービス検索記述子 (SSD) は、LDAP 内の特定の操作に対するデフォルトの検索リクエストを、ユーザーが定義した検索に変更します。SSD は、たとえば、カスタマイ

ズされたコンテナ定義または別のオペレーティングシステムで LDAP を使用してきたが、現在は最新の Oracle Solaris リリースに移行している場合に特に役立ちます。SSD を使用すると、既存の LDAP データベースおよびデータを変更しなくても LDAP ネームサービスを構成できます。

idsconfig コマンドを使用した SSD の設定

前出の Example, Inc. が LDAP を構成済みで、ユーザーを ou=Users コンテナに格納しているものとします。現在は最新の Oracle Solaris リリースにアップグレードしています。定義によると、LDAP クライアントは、ユーザーエントリが ou=People コンテナ内に格納されていると想定しています。このままでは、LDAP クライアントは passwd サービス検索時に DIT の ou=people レベルを検索するため、適切な値を検出できません。

この問題を解決する手のかかる方法の 1 つは Example, Inc. の既存の DIT を完全に置き換え、Example, Inc. のネットワーク上の既存アプリケーションすべてを書き換えて、新規 LDAP ネームサービスとの互換性を持たせる方法です。2 つ目の、はるかに望ましい解決策は、LDAP クライアントにデフォルトの ou=people コンテナではなく、ou=Users コンテナ内のユーザー情報を検索するよう指示する SSD を使用することです。

必要な SSD は、Oracle Directory Server Enterprise Edition の構成中に idsconfig を使用して定義します。プロンプト行は次のようになります。

```
Do you wish to setup Service Search Descriptors (y/n/h? y
  A  Add a Service Search Descriptor
  D  Delete a SSD
  M  Modify a SSD
  P  Display all SSD's
  H  Help
  X  Clear all SSD's

  Q  Exit menu
Enter menu choice: [Quit] a
Enter the service id: passwd
Enter the base: service ou=user,dc=west,dc=example,dc=com
Enter the scope: one[default]
  A  Add a Service Search Descriptor
  D  Delete a SSD
  M  Modify a SSD
  P  Display all SSD's
  H  Help
  X  Clear all SSD's

  Q  Exit menu
Enter menu choice: [Quit] p

Current Service Search Descriptors:
==================================
```

```
Passwd:ou=Users,ou=west,ou=example,ou=com?

Hit return to continue.

  A  Add a Service Search Descriptor
  D  Delete a SSD
  M  Modify a SSD
  P  Display all SSD's
  H  Help
  X  Clear all SSD's

  Q  Exit menu
Enter menu choice: [Quit] q
```

idsconfig コマンドの実行

注 – idsconfig の実行には特別な権限は不要であり、LDAP ネームサービスクライアントになる必要もありません。idsconfig を実行する準備として、172 ページの「サーバーのインストール用チェックリストの作成」で説明されているチェックリストを作成することを忘れないでください。サーバーまたは LDAP ネームサービスクライアントマシンから idsconfig を実行する必要はありません。idsconfig は、ネットワーク上の任意の Oracle Solaris マシンから実行できます。

注意 – idsconfig は、ディレクトリマネージャーのパスワードを平文で送信します。これが実行されないようにするには、クライアント上ではなく、ディレクトリサーバー自体で idsconfig を実行する必要があります。

▼ idsconfig コマンドを使用して Oracle Directory Server Enterprise Edition を構成する方法

1 ターゲットの **Oracle Directory Server Enterprise Edition** が起動して実行中であることを確認してください。

2 **idsconfig** コマンドを実行します。

```
# /usr/lib/ldap/idsconfig
```

この章の最初の172 ページの「サーバーのインストール用チェックリストの作成」にあるサーバーとクライアントのチェックリストに示されている定義を使用して idsconfig を実行する例については、例 11–1 を参照してください。

3 表示される質問に答えます。

ユーザー入力のデフォルトは「no」です。質問の詳細を表示する場合は、

h

と入力します。すると、簡単なヘルプが表示されます。

idsconfig によるディレクトリの設定が完了したら、サーバー設定を完了してサーバーをクライアント対応にする前に、サーバー上で指定されたコマンドを実行する必要があります。

idsconfig 設定の例

このセクションでは、多くのデフォルト値を使用した基本的な idsconfig 設定の例を示します。クライアントプロファイルを変更するもっとも複雑な方法は、SSD を作成する方法です。詳細については、174 ページの「サービス検索記述子を使用してさまざまなサービスへのクライアントアクセスを変更する」を参照してください。

プロンプトの後ろにある [ ] 内のデータは、そのプロンプトのデフォルト値を表しています。デフォルト値を使用する場合は、Return キーを押します。

注 – サマリー画面で空白になっているパラメータは設定されません。

---

idsconfig によるディレクトリの設定が完了したら、サーバー設定を完了してサーバーをクライアント対応にする前に、サーバー上で指定されたコマンドを実行する必要があります。

例 11–1 Example, Inc. のネットワーク用の idsconfig コマンドの実行

次の例では、サーバーインスタンスが LDAP サーバーに作成された直後に、idsconfig ユーティリティーが実行されます。

```
# usr/lib/ldap/idsconfig
It is strongly recommended that you BACKUP the directory server
before running idsconfig.

Hit Ctrl-C at any time before the final confirmation to exit.

Do you wish to continue with server setup (y/n/h)? [n] y
Enter the JES Directory Server's  hostname to setup: myserver
Enter the port number for DSEE (h=help): [389]
Enter the directory manager DN: [cn=Directory Manager]
Enter passwd for cn=Directory Manager :
Enter the domainname to be served (h=help): [west.example.com]
Enter LDAP Base DN (h=help): [dc=west,dc=example,dc=com]
  Checking LDAP Base DN ...
  Validating LDAP Base DN and Suffix ...
  No valid suffixes were found for Base DN dc=west,dc=example,dc=com
```

例 11–1　Example, Inc. のネットワーク用の idsconfig コマンドの実行　　(続き)

```
Enter suffix to be created (b=back/h=help): [dc=west,dc=example,dc=com]
Enter ldbm database name (b=back/h=help): [west]
  sasl/GSSAPI is not supported by this LDAP server
Enter the profile name (h=help): [default] WestUserProfile
Default server list (h=help): [192.168.0.1]
Preferred server list (h=help):
Choose desired search scope (one, sub, h=help):  [one]
The following are the supported credential levels:
  1  anonymous
  2  proxy
  3  proxy anonymous
  4  self
Choose Credential level [h=help]: [1] 2
The following are the supported Authentication Methods:
  1  none
  2  simple
  3  sasl/DIGEST-MD5
  4  tls:simple
  5  tls:sasl/DIGEST-MD5
  6  sasl/GSSAPI
Choose Authentication Method (h=help): [1] 2


Current authenticationMethod: simple
Do you want to add another Authentication Method? n
Do you want the clients to follow referrals (y/n/h)? [n]
Do you want to modify the server timelimit value (y/n/h)? [n] y
Enter the time limit for DSEE (current=3600): [-1]
Do you want to modify the server sizelimit value (y/n/h)? [n] y
Enter the size limit for DSEE (current=2000): [-1]
Do you want to store passwords in "crypt" format (y/n/h)? [n] y
Do you want to setup a Service Authentication Methods (y/n/h)? [n]
Client search time limit in seconds (h=help): [30]
Profile Time To Live in seconds (h=help): [43200]
Bind time limit in seconds (h=help): [10]
Do you want to enable shadow update (y/n/h)? [n]
Do you wish to setup Service Search Descriptors (y/n/h)? [n]

             Summary of Configuration

  1  Domain to serve               : west.example.com
  2  Base DN to setup              : dc=west,dc=example,dc=com
        Suffix to create           : dc=west,dc=example,dc=com
        Database to create         : west
  3  Profile name to create        : WestUserProfile
  4  Default Server List           : 192.168.0.1
  5  Preferred Server List         :
  6  Default Search Scope          : one
  7  Credential Level              : proxy
  8  Authentication Method         : simple
  9  Enable Follow Referrals       : FALSE
 10  DSEE Time Limit                : -1
 11  DSEE Size Limit                : -1
 12  Enable crypt password storage : TRUE
 13  Service Auth Method pam_ldap  :
```

例 11–1 Example, Inc. のネットワーク用の idsconfig コマンドの実行 *(続き)*

```
 14  Service Auth Method keyserv   :
 15  Service Auth Method passwd-cmd:
 16  Search Time Limit             : 30
 17  Profile Time to Live          : 43200
 18  Bind Limit                    : 10
 19  Enable shadow update          : FALSE
 20  Service Search Descriptors Menu

Enter config value to change: (1-20 0=commit changes) [0]
Enter DN for proxy agent: [cn=proxyagent,ou=profile,dc=west,dc=example,dc=com]
Enter passwd for proxyagent:
Re-enter passwd:

WARNING: About to start committing changes. (y=continue, n=EXIT) y

  1. Changed timelimit to -1 in cn=config.
  2. Changed sizelimit to -1 in cn=config.
  3. Changed passwordstoragescheme to "crypt" in cn=config.
  4. Schema attributes have been updated.
  5. Schema objectclass definitions have been added.
  6. Database west successfully created.
  7. Suffix dc=west,dc=example,dc=com successfully created.
  8. NisDomainObject added to dc=west,dc=example,dc=com.
  9. Top level "ou" containers complete.
  10. automount maps: auto_home auto_direct auto_master auto_shared processed.
  11. ACI for dc=west,dc=example,dc=com modified to disable self modify.
  12. Add of VLV Access Control Information (ACI).
  13. Proxy Agent cn=proxyagent,ou=profile,dc=west,dc=example,dc=com added.
  14. Give cn=proxyagent,ou=profile,dc=west,dc=example,dc=com read permission
      for password.
  15. Generated client profile and loaded on server.
  16. Processing eq,pres indexes:
      uidNumber (eq,pres)   Finished indexing.
      ipNetworkNumber (eq,pres)   Finished indexing.
      gidnumber (eq,pres)   Finished indexing.
      oncrpcnumber (eq,pres)   Finished indexing.
      automountKey (eq,pres)   Finished indexing.
  17. Processing eq,pres,sub indexes:
      ipHostNumber (eq,pres,sub)   Finished indexing.
      membernisnetgroup (eq,pres,sub)   Finished indexing.
      nisnetgrouptriple (eq,pres,sub)   Finished indexing.
  18. Processing VLV indexes:
      west.example.com.getgrent vlv_index   Entry created
      west.example.com.gethostent vlv_index   Entry created
      west.example.com.getnetent vlv_index   Entry created
      west.example.com.getpwent vlv_index   Entry created
      west.example.com.getrpcent vlv_index   Entry created
      west.example.com.getspent vlv_index   Entry created
      west.example.com.getauhoent vlv_index   Entry created
      west.example.com.getsoluent vlv_index   Entry created
      west.example.com.getauduent vlv_index   Entry created
      west.example.com.getauthent vlv_index   Entry created
      west.example.com.getexecent vlv_index   Entry created
      west.example.com.getprofent vlv_index   Entry created
      west.example.com.getmailent vlv_index   Entry created
```

例 11–1 Example, Inc. のネットワーク用の idsconfig コマンドの実行 (続き)

```
      west.example.com.getbootent vlv_index   Entry created
      west.example.com.getethent vlv_index   Entry created
      west.example.com.getngrpent vlv_index   Entry created
      west.example.com.getipnent vlv_index   Entry created
      west.example.com.getmaskent vlv_index   Entry created
      west.example.com.getprent vlv_index   Entry created
      west.example.com.getip4ent vlv_index   Entry created
      west.example.com.getip6ent vlv_index   Entry created

idsconfig: Setup of DSEE server myserver is complete.


Note: idsconfig has created entries for VLV indexes.

      For DS5.x, use the directoryserver(1m) script on myserver
      to stop the server.  Then, using directoryserver, follow the
      directoryserver examples below to create the actual VLV indexes.

      For DSEE6.x, use dsadm command delivered with DS on myserver
      to stop the server.  Then, using dsadm, follow the
      dsadm examples below to create the actual VLV indexes.

  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getgrent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.gethostent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getnetent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getpwent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getrpcent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getspent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getauhoent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getsoluent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getauduent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getauthent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getexecent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getprofent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getmailent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getbootent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getethent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getngrpent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getipnent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getmaskent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getprent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getip4ent
  directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getip6ent

<install-path>/bin/dsadm reindex -l -t west.example.com.getgrent <directory-instance-path>
 dc=west,dc=example,dc=com
<install-path>/bin/dsadm reindex -l -t west.example.com.gethostent <directory-instance-path>
 dc=west,dc=example,dc=com
.
.
.
<install-path>/bin/dsadm reindex -l -t west.example.com.getip6ent <directory-instance-path>
 dc=west,dc=example,dc=com
```

ldapaddent コマンドを使用したディレクトリサーバーのデータ生成

注 – pam_unix_* モジュールを使用している場合は、ディレクトリサーバーにデータを生成する前に、パスワードを UNIX Crypt 形式で格納するようにサーバーを構成する必要があります。pam_ldap を使用している場合、任意の形式でパスワードを格納できます。UNIX crypt 形式でパスワードを設定する方法については、Oracle Directory Server Enterprise Edition のドキュメントを参照してください。

ldapaddent は、標準入力から (/etc/filename passwd など) データを読み取り、このデータをサービスに関連付けられたコンテナに配置します。クライアント構成により、デフォルトのデータ書き込み方法が決定されます。

▼ ldapaddent コマンドを使用して Oracle Directory Server Enterprise Edition にユーザーパスワードデータを生成する方法

- **ldapaddent コマンドを使用してサーバーに /etc/passwd エントリを追加します。**

```
# ldapaddent -D "cn=directory manager" -f /etc/passwd passwd
```

ldapaddent(1M) のマニュアルページを参照してください。LDAP セキュリティーおよびディレクトリサーバーへの書き込みアクセスについては、第 9 章「LDAP ネームサービスの紹介 (概要)」も参照してください。

メンバー属性を使用したグループメンバーシップの指定

Internet-Draft rfc2307bis は、groupOfMembers オブジェクトクラスをグループサービスの LDAP エントリのための便利な構造クラスとしても使用できると規定しています。それにより、このようなグループエントリの識別名 (DN) に、グループメンバーシップを指定するメンバー属性値を含めることができます。Oracle Solaris の LDAP クライアントはこのようなグループエントリをサポートしており、グループメンバーシップの解決のためにメンバー属性値を使用します。

これらの LDAP クライアントはまた、groupOfUniqueNames オブジェクトクラスと uniqueMember 属性を使用するグループエントリもサポートしています。ただし、このオブジェクトクラスと属性の使用はお勧めできません。

posixGroup オブジェクトクラスと memberUid 属性を持つグループエントリを定義する既存の方法も引き続きサポートされています。このタイプのグループエントリは引き続き、グループサービスのために LDAP サーバーにデータを生成するときに ldapaddent コマンドによって作成されるエントリです。グループエントリに member 属性は追加されません。

groupOfMembers オブジェクトクラスと member 属性値を持つグループエントリを追加するには、ldapadd ツールと、次のような入力ファイルを使用します。

```
dn: cn=group1,ou=group,dc=mkg,dc=example,dc=com
objectClass: posixGroup
objectClass: groupOfNames
objectClass: top
cn: group1
gidNumber: 1234
member: uid=user1,ou=people,dc=mkg,dc=example,dc=com
member: uid=user2,ou=people,dc=mkg,dc=example,dc=com
member: cn=group2,ou=group,dc=mkg,dc=example,dc=com
```

LDAP クライアントは、memberUid、member、および uniqueMember 属性のいずれかまたはすべてを含むグループエントリや、どの属性も含まないグループエントリを処理します。メンバーシップの評価結果として、グループに、3 つのすべての属性の和集合から重複が削除されたメンバーシップが与えられます。つまり、グループエントリ G がユーザー U1 と U2 を参照する memberUid 値、ユーザー U2 を参照する member 値、およびユーザー U3 を参照する uniqueMember 値を持っている場合、グループ G には U1、U2、および U3 の 3 つのメンバーが含まれます。また、入れ子のグループもサポートされます。つまり、メンバー属性は、ほかのグループを指し示す値を持つことができます。

グループメンバーシップを効率的に評価して、ユーザーがメンバーになっているグループ (入れ子のグループを含む) を確認するには、LDAP サーバー上で memberOf プラグインが構成され、有効になっている必要があります。そうでない場合は、含んでいるグループ (入れ子のグループを除く) のみが解決されます。デフォルトでは、memberOf プラグインは ODSEE サーバーによって有効になります。このプラグインが有効になっていない場合は、ODSEE の dsconf ツールを使用して有効にします。

追加プロファイルを使用してディレクトリサーバーを生成する

指定された属性に基づいて構成プロファイルの LDIF 表現を作成するには、genprofile オプションを指定して ldapclient コマンドを使用します。作成したプロファイルは、次に LDAP サーバーに読み込まれ、クライアントプロファイルとして使用されます。クライアントプロファイルは、 ldapclient init を使うことによりクライアントからダウンロードできます。

ldapclient genprofile の使用については、ldapclient(1M) を参照してください。

▼ ldapclient コマンドを使用してディレクトリサーバーに追加のプロファイルを生成する方法

1. 管理者になります。
   詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。
2. **ldapclient** コマンドを **genprofile** オプションとともに使用します。

```
# ldapclient genprofile \
-a profileName=myprofile \
-a defaultSearchBase=dc=west,dc=example,dc=com \
-a "defaultServerList=192.168.0.1 192.168.0.2:386" \> myprofile.ldif
```

3. 新規プロファイルをサーバーにアップロードします。

```
# ldapadd -h 192.168.0.1 -D “cn=directory manager” -f myprofile.ldif
```

ディレクトリサーバーを構成してアカウント管理を有効にする

pam_ldap を使用するクライアントと pam_unix_* モジュールを使用するクライアントに対してアカウント管理を実装できます。

注意 – 同じ LDAP ネームドメイン内で pam_ldap と pam_unix_* モジュールの両方を使用しないでください。すべてのクライアントが pam_ldap を使用するか、またはすべてのクライアントが pam_unix_* モジュールを使用するかのどちらかです。この制限により、専用の LDAP サーバーが必要になる場合があります。

pam_ldap モジュールを使用するクライアントの場合

pam_ldap が正しく動作するには、パスワードとアカウントのロックアウトポリシーがサーバー上で正しく構成されている必要があります。ディレクトリサーバーコンソールまたは ldapmodify を使用して、LDAP ディレクトリのアカウント管理ポリシーを構成できます。手順と詳細情報については、使用している

バージョンの Oracle Directory Server Enterprise Edition の『管理者ガイド』にある「ユーザーアカウントの管理」の章を参照してください。

注 – 以前は、pam_ldap アカウント管理を有効にすると、システムにログインする際には、常にすべてのユーザーが認証用にログインパスワードを入力する必要がありました。そのため、ssh などのツールを使用した、パスワードに基づかないログインは失敗します。

アカウント管理を実行し、ユーザーがログインしているときに Directory Server への認証を行わずにユーザーのアカウントステータスを取得します。Directory Server 上の新しい制御は 1.3.6.1.4.1.42.2.27.9.5.8 です。これはデフォルトで有効になっています。

この制御をデフォルト以外に変更する場合は、Directory Server 上でアクセス制御情報 (ACI) を追加します。

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
     allow (read, search, compare, proxy)
     (groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

---

proxy ユーザーのパスワードは、決して期限が切れてはいけません。proxy パスワードが期限切れになった場合、 proxy 資格レベルを使用するクライアントはサーバーからネームサービス情報を取り出すことができません。proxy ユーザーのパスワードの期限が切れないことを保証するために、次のスクリプトを記述して proxy アカウントを変更します。

```
# ldapmodify -h ldapserver -D administrator DN \
-w administrator password <<EOF
dn: proxy user DN
DNchangetype: modify
replace: passwordexpirationtime
passwordexpirationtime: 20380119031407Z
EOF
```

注 – pam_ldap のアカウント管理は、Oracle Directory Server Enterprise Edition をもとにユーザーのパスワードやアカウントの有効期限情報を維持し、ユーザーに知らせます。ディレクトリサーバーは、シャドウエントリの対応するデータを解釈してユーザーアカウントを検証することはしません。ただし、pam_unix_* モジュールはシャドウデータを検査して、アカウントがロックされているか、またはパスワードの期限が切れているかどうかを判定します。シャドウデータが LDAP ネームサービスやディレクトリサーバーによって最新の状態に保持されるわけではないため、これらのモジュールは、シャドウデータに基づいてアクセスを許可するべきではありません。シャドウデータは、proxy 識別情報を使用して取得されます。そのため、proxy ユーザーに userPassword 属性への読み取りアクセスを許可しないでください。proxy ユーザーの userPassword への読み取りアクセス権を拒否することにより、PAM サービスが無効なアカウントの検証を行うことはなくなります。

pam_unix_* モジュールを使用するクライアントの場合

LDAP クライアントがアカウント管理に pam_unix_* モジュールを使用できるようにするには、シャドウデータの更新を有効にするようにサーバーを設定する必要があります。pam_ldap のアカウント管理とは異なり、pam_unix_* モジュールには追加の構成手順が必要ありません。idsconfig ユーティリティーを実行することによって、すべての構成を実行できます。基本的な idsconfig の実行については、例 11–1を参照してください。

次に 2 つの idsconfig 実行の出力を示します。

最初の idsconfig 実行では、既存のクライアントプロファイルを使用します。

```
# /usr/lib/ldap/idsconfig

It is strongly recommended that you BACKUP the directory server
before running idsconfig.

Hit Ctrl-C at any time before the final confirmation to exit.

Do you wish to continue with server setup (y/n/h)? [n] y
Enter the JES Directory Server's  hostname to setup: myserver
Enter the port number for DSEE (h=help): [389]
Enter the directory manager DN: [cn=Directory Manager]
Enter passwd for cn=Directory Manager :
Enter the domainname to be served (h=help): [west.example.com]
Enter LDAP Base DN (h=help): [dc=west,dc=example,dc=com]
  Checking LDAP Base DN ...
  Validating LDAP Base DN and Suffix ...
  sasl/GSSAPI is not supported by this LDAP server

Enter the profile name (h=help): [default] WestUserProfile
```

```
Profile 'WestUserProfile' already exists, it is possible to enable
shadow update now. idsconfig will exit after shadow update
is enabled. You can also continue to overwrite the profile
or create a new one and be given the chance to enable
shadow update later.

Just enable shadow update (y/n/h)? [n] y
Add the administrator identity (y/n/h)? [y]
Enter DN for the administrator: [cn=admin,ou=profile,dc=west,dc=example,dc=com]
Enter passwd for the administrator:
Re-enter passwd:
  ADDED: Administrator identity cn=admin,ou=profile,dc=west,dc=example,dc=com.
         Proxy ACI LDAP_Naming_Services_proxy_password_read does not
         exist for dc=west,dc=example,dc=com.
  ACI SET: Give cn=admin,ou=profile,dc=west,dc=example,dc=com read/write access
           to shadow data.
  ACI SET: Non-Admin access to shadow data denied.

  Shadow update has been enabled.
```

2 つ目の idsconfig 実行では、後で使用するための新しいプロファイルを作成します。出力の一部のみが表示されています。

```
# /usr/lib/ldap/idsconfig

It is strongly recommended that you BACKUP the directory server
before running idsconfig.

Hit Ctrl-C at any time before the final confirmation to exit.

Do you wish to continue with server setup (y/n/h)? [n] y
Enter the JES Directory Server's  hostname to setup: myserver
Enter the port number for DSEE (h=help): [389]
Enter the directory manager DN: [cn=Directory Manager]
Enter passwd for cn=Directory Manager :
Enter the domainname to be served (h=help): [west.example.com]
Enter LDAP Base DN (h=help): [dc=west,dc=example,dc=com]
  Checking LDAP Base DN ...
  Validating LDAP Base DN and Suffix ...
  sasl/GSSAPI is not supported by this LDAP server

Enter the profile name (h=help): [default] WestUserProfile-new
Default server list (h=help): [192.168.0.1]
.
.
.
Do you want to enable shadow update (y/n/h)? [n] y

              Summary of Configuration

  1  Domain to serve               : west.example.com
  2  Base DN to setup              : dc=west,dc=example,dc=com
        Suffix to create           : dc=west,dc=example,dc=com
  3  Profile name to create        : WestUserProfile-new
.
```

```
.
.
 19  Enable shadow update          : TRUE
.
.
.
Enter DN for the administrator: [cn=admin,ou=profile,dc=west,dc=example,dc=com]
Enter passwd for the administrator:
Re-enter passwd:


WARNING: About to start committing changes. (y=continue, n=EXIT) y

  1. Changed timelimit to -1 in cn=config.
  2. Changed sizelimit to -1 in cn=config.
.
.
.
  11. ACI for dc=test1,dc=mpklab,dc=sfbay,dc=sun,dc=com modified to
      disable self modify.
.
.
.
  15. Give cn=admin,ou=profile,dc=west,dc=example,dc=com write permission for shadow.
...
```

◆ ◆ ◆ 第 12 章

12 LDAP クライアントの設定 (タスク)

この章では、LDAP ネームサービスクライアントを設定する方法について説明します。この章で扱う内容は、次のとおりです。

LDAP クライアント設定の前提条件

Oracle Solaris クライアントで LDAP をネームサービスとして使用するには、次の要件が満たされている必要があります。

- クライアントのドメイン名が LDAP サーバーによって処理されている必要があります。
- ネームサービススイッチが、必要なサービスの LDAP を指し示している必要があります。
- クライアントに、その動作を定義する特定のパラメータがすべて構成されている必要があります。
- `ldap_cachemgr` がクライアント上で実行されている必要があります。
- クライアントが構成されているサーバーが少なくとも 1 つ起動され、実行されている必要があります。

`ldapclient` ユーティリティーは、サーバーの起動を除き、上記の手順をすべて実行するので、LDAP クライアントを設定するための鍵となります。この章の残りでは、`ldapclient` ユーティリティーを使用して LDAP クライアントを設定する方法や、その他のさまざまな LDAP ユーティリティーを使用して LDAP クライアントに関する情報を取得したり、そのステータスをチェックしたりする方法の例を示します。

LDAP とサービス管理機能

LDAP クライアントサービスは、サービス管理機能を使用して管理されます。SMF の概要については、『Oracle Solaris 11.1 でのサービスと障害の管理』の第 1 章「サービスの管理 (概要)」を参照してください。また、詳細については svcadm(1M) および svcs(1) のマニュアルページも参照してください。

次の一覧は、SMF サービスを使用して LDAP クライアントサービスを管理するために必要ないくつかの重要な情報の簡単な概要を示しています。

- LDAP クライアントサービスに対する管理操作 (有効化、無効化、再起動など) は、svcadm コマンドを使用して実行できます。

  ヒント – -t オプションを使用してサービスを一時的に無効化すると、そのサービス構成に対していくらかの保護を提供できます。-t オプションを指定してサービスを無効にした場合、リブート後に元の設定が復元されます。-t オプションを指定しないでサービスを無効にした場合、リブート後もそのサービスは無効のままです。

- LDAP クライアントサービスに対する障害管理リソース識別子 (FMRI) は、svc:/network/ldap/client です。
- 構成プロセス中は、network/ldap/client サービスによって使用されるドメイン名を提供するために、network/nis/domain サービスも有効になります。
- svcs コマンドを使用して、LDAP クライアントおよび ldap_cachemgr デーモンのステータスを照会できます。
  - 次に、svcs コマンドとその出力の例を示します。

    ```
    # svcs \*ldap\*
    STATE          STIME    FMRI
    online         15:43:46 svc:/network/ldap/client:default
    ```

  - svcs -l コマンドと出力の例を、次に示します。次に示す出力を得るには、FMRI でインスタンス名を使用する必要があります。

    ```
    # svcs -l network/ldap/client:default
    fmri         svc:/network/ldap/client:default
    name         LDAP Name Service Client
    enabled      true
    state        online
    next_state   none
    restarter    svc:/system/svc/restarter:default
    manifest     /lib/svc/manifest/network/ldap/client.xml
    manifest     /lib/svc/manifest/network/network-location.xml
    manifest     /lib/svc/manifest/system/name-service/upgrade.xml
    manifest     /lib/svc/manifest/milestone/config.xml
    dependency   require_all/none svc:/system/filesystem/minimal (online)
    dependency   require_all/none svc:/network/initial (online)
    dependency   optional_all/none svc:/network/location:default (online)
    ```

```
dependency    require_all/restart svc:/network/nis/domain (online)
dependency    optional_all/none svc:/system/name-service/upgrade (online)
dependency    optional_all/none svc:/milestone/config (online)
dependency    optional_all/none svc:/system/manifest-import (online)
dependency    require_all/none svc:/milestone/unconfig (online)
```

- 次のコマンドを使用して、デーモンの存在をチェックできます:
  - サーバー上で、ptree コマンドを使用します。

    ```
    # ptree ‘pgrep slapd‘
    6410 zsched
    11565 /export/dsee/dsee6/ds6/lib/64/ns-slapd -D /export/dsee/test1 -i /export
    ```

  - クライアント上で、次のコマンドを使用します。

    ```
    # ldapsearch -h server-name -b "" -s base "objectclass=*" |grep -i context
    namingContexts: dc=example,dc=com
    ```

LDAP クライアントの初期化

ldapclient コマンドは、Oracle Solaris システム上で LDAP クライアントを設定するために使用されます。このコマンドは、サーバーに、適切なクライアントプロファイルがすでに構成されていると想定しています。サーバーをインストールして、適切なプロファイルで構成してからクライアントを設定する必要があります。

注 – LDAP と NIS は network/nis/domain サービスで定義されている同じドメイン名コンポーネントを使用するため、Oracle Solaris OS は、NIS クライアントとネイティブな LDAP クライアントが同じクライアントシステム上に共存する構成をサポートしていません。

---

ldapclient を使用してクライアントを設定するには主に 2 つの方法があります。

- プロファイル

  少なくとも、使用するプロファイルとドメインを含むサーバーアドレスを指定する必要があります。プロファイルが指定されていない場合は、デフォルトのプロファイルが使用されます。プロキシと認証データベースの情報を除いて、必要な情報はサーバーから入手できます。クライアントの資格レベルがプロキシまたは匿名プロキシである場合は、プロキシのバインド DN とパスワードを入力してください。詳細は、145 ページの「クライアント資格レベルの割り当て」を参照してください。

  シャドウデータの更新を有効にするには、管理者資格 (adminDN および adminPassword) を指定する必要があります。

- 手動

  クライアント自体でプロファイルを構成します。つまり、コマンド行からすべてのパラメータを定義します。このため、プロファイル情報はキャッシュファイルに格納されサーバーによってリフレッシュされることはありません。

注 – エンタープライズ環境では、プロファイルがマシン間で共有されている場合に LDAP 構成プロファイルを使用すると複雑さを軽減できます。

▼ プロファイルを使用して LDAP クライアントを初期化する方法

1 管理者になります。

詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2 **init** オプションを使用して **ldapclient** コマンドを実行します。

```
# ldapclient init -a profileName=new \
-a domainName=west.example.com 192.168.0.1
System successfully configured
```

▼ ユーザー別の資格を使用して LDAP クライアントを初期化する方法

始める前に ユーザー別の資格を使用して LDAP クライアントを設定する前に、次がすでに構成されている必要があります。

- 1 つまたは複数の Kerberos 鍵配布センター (KDC) サーバーが構成され、実行されている必要があります。
- DNS、DNS サーバーへのクライアントアクセス、および少なくとも 1 つの DNS サーバーが構成され、実行されている必要があります。
- クライアントマシン上の Kerberos が構成され、有効にされている
- 次のような Kerberos クライアントのインストールプロファイルが存在する必要があります。

```
# cat /usr/tmp/krb5.profile
REALM EXAMPLE.COM
KDC kdc.example.com
ADMIN super/admin
FILEPATH /usr/tmp/krb5.conf
NFS 1
DNSLOOKUP none
```

- LDAP サーバーがインストールされ、`sasl/GSSAPI` をサポートするように構成されている必要があります。
- 適切な識別情報マッピング構成が存在する
- ディレクトリサーバーおよび KDC 用の Kerberos ホスト主体が KDC 内で設定されている

- 使用されるディレクトリサーバー DIT 上で idsconfig コマンドが実行されている必要があります。
- ユーザー別の適切な gssapi プロファイル (gssapi_EXAMPLE.COM など) が作成済みである

  次の部分的な例には、idsconfig コマンド内のユーザー別のプロファイルの図が示されています。

```
# /usr/lib/ldap/idsconfig
Do you wish to continue with server setup (y/n/h)? [n] y
Enter the Directory Server's hostname to setup: kdc.example.com
Enter the port number for DSEE (h=help): [389] <Enter your port>
Enter the directory manager DN: [cn=Directory Manager] <Enter your DN>
Enter passwd for cn=Directory Manager : <Enter your password>
Enter the domainname to be served (h=help): [example.com] <Enter your domain>
Enter LDAP Base DN (h=help): [dc=example,dc=com] <Enter your DN>
GSSAPI is supported. Do you want to set up gssapi:(y/n) [n] y
Enter Kerberos Realm: [EXAMPLE.COM] EXAMPLE.COM
```

注 – さらに、gssapi プロファイルの場合は、4 self の資格レベルと、6 sasl/GSSAPI の認証方法を指定する必要があります。

- 必要なユーザー主体が KDC 内に存在する必要があります。
- クライアントマシン上で、次のようなコマンドで、クライアントプロファイルを使用して Kerberos が初期化されている必要があります。

```
# /usr/sbin/kclient -p /usr/tmp/krb5.profile
```

- ネームサービススイッチが、hosts に dns を使用するように構成されている必要があります。次のコマンドで、現在のリポジトリ値をチェックします。

```
% svcprop -p config/host system/name-service/switch
files\ dns\ nis
```

- DNS が構成され、DNS サービスが実行されている必要があります。詳細は、このドキュメントの DNS に関する章を参照してください。
- ディレクトリサーバー DIT が、(少なくとも) このクライアントマシンのユーザー、クライアントホスト、および必要な auto_home LDAP エントリを使用して事前に読み込まれている必要があります。ldapaddent コマンドを使用してエントリを追加する方法についての詳細は、このマニュアルのほかのセクションを参照してください。

注 – どちらのクライアント構成ファイルも直接編集しないでください。これらのファイルの内容を作成または変更する場合は、ldapclient コマンドを使用してください。

---

1. **ldapclient init** を実行することにより、**gssapi** プロファイルを使用してクライアントを初期化します。

   ```
   # /usr/sbin/ldapclient init -a profilename=gssapi_EXAMPLE.COM -a \
   domainname=example.com 9.9.9.50
   ```

2. ユーザーとしてログインを試みます。

   - **kinit -p** *user* を実行します。
   - ユーザーのログインセッションで **ldaplist -l passwd** *user* を実行すると、**userpassword** が表示されます。
   - **ldaplist -l passwd bar** を実行すると、**userpassword** なしでエントリを取得できます。デフォルトでは、**root** はすべてのユーザーの **userpassword** を引き続き表示できます。

参考 ユーザー別の資格の使用について

- syslog ファイルにメッセージ libsldap: Status: 7 Mesg: openConnection: GSSAPI bind failed - 82 Local error が表示される場合は、Kerberos が初期化されていないか、またはそのチケットの有効期限が切れている可能性があります。それを参照するには、klist コマンドを実行します。たとえば、kinit -p foo または kinit -R -p foo を実行し、再試行します。
- 必要に応じて、/etc/pam.conf に pam_krb5.so.1 を追加することにより、ログイン時に kinit コマンドが自動的に実行されるようにすることができます。

  例:

  ```
  login   auth optional pam_krb5.so.1
  rlogin  auth optional pam_krb5.so.1
  other   auth optional pam_krb5.so.1
  ```

- ユーザーが kinit コマンドを実行し、syslog メッセージに Invalid credential が示されている場合は、root ホストエントリまたはユーザーエントリが LDAP ディレクトリ内に存在しないか、またはマッピング規則が正しくないことが問題である可能性があります。
- ldapclient init コマンドが実行されると、LDAP プロファイルに self/ sasl/GSSAPI 構成が含まれているかどうかがチェックされます。そのコマンドがスイッチのチェックに失敗した場合は、一般的には DNS がホストデータベースの検索条件ではなかったことが原因です。
  - DNS クライアント ID が有効でないためにチェックに失敗した場合は、svcs -l dns/client を実行して、サービスが無効になっているかどうかを判定します。サービスを有効にするには、svcadm enable dns/client を実行します。
  - sasl/GSSAPI バインドのためにチェックに失敗した場合は、syslog をチェックして問題を確認します。

詳細は、このガイドおよび『Oracle Solaris 11.1 の管理: セキュリティーサービス』にあるほかの参照資料を参照してください。

▼ プロキシ資格を使用して LDAP クライアントを初期化する方法

注 – どちらのクライアント構成ファイルも直接編集しないでください。これらのファイルの内容を作成または変更する場合は、`ldapclient` コマンドを使用してください。

---

1 管理者になります。

詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2 プロキシ値を定義します。

```
# ldapclient init \
-a proxyDN=cn=proxyagent,ou=profile,dc=west,dc=example,dc=com \
-a domainName=west.example.com \
-a profileName=pit1 \
-a proxyPassword=test1234 192.168.0.1
System successfully configured
```

使用されるプロファイルが `proxy` 用に設定される場合は、`-a proxyDN` と `-a proxyPassword` が必要です。サーバーに保存されているプロファイルにはこの資格情報が含まれていないため、クライアントを初期設定するときは資格情報を入力する必要があります。この方法は、プロキシの資格情報をサーバーに保存していた従来の方法に比べて安全性が高くなります。

これらのプロキシ情報は、`config` および `cred` プロパティーグループ内の `svc:/network/ldap/client` サービス内に格納されます。

▼ LDAP クライアントを初期化してシャドウデータの更新を有効にする方法

1 管理者になります。

詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2 **enableShadowUpdate** スイッチを設定し、管理者資格を定義するには、**ldapclient** コマンドを実行します。

- すでに実行されている **LDAP** クライアントを更新するには、次のコマンドを実行します。

```
# ldapclient mod -a enableShadowUpdate=TRUE \
-a adminDN=cn=admin,ou=profile,dc=west,dc=example,dc=com \
-a adminPassword=admin-password
System successfully configured
```

- **LDAP** クライアントを初期化するには、次のコマンドを実行します。

```
# ldapclient init \
-a adminDN=cn=admin,ou=profile,dc=west,dc=example,dc=com \
-a adminPassword=admin-password
-a domainName=west.example.com \
-a profileName=WestUserProfile \
-a proxyDN=cn=proxyagent,ou=profile,dc=west,dc=example,dc=com \
-a proxyPassword=<proxy_password> \
192.168.0.1
System successfully configured
```

3 構成を検証するには、**network/ldap/client** サービスの **cred** プロパティーの内容を表示します。

出力は次のようになります。

```
# svcprop -p cred svc:/network/ldap/client
cred/read_authorization astring solaris.smf.value.name-service.ldap.client
cred/value_authorization astring solaris.smf.value.name-service.ldap.client
cred/bind_dn astring cn=proxyagent,ou=profile,dc=west,dc=example,dc=com
cred/bind_passwd astring {NS1}4a3788f8eb85de11
cred/enable_shadow_update boolean true
cred/admin_bind_dn astring cn=admin,ou=profile,dc=west,dc=example,dc=com
cred/admin_bind_passwd astring {NS1}4a3788f8c053434f
```

▼ LDAP クライアントを手動で初期化する方法

root ユーザーまたは同等の役割を持つ管理者は、手動の LDAP クライアント構成を実行できます。ただし、この処理では多数のチェックが省略されるため、システムを正しく構成できないことがよくあります。また、プロファイルを使用するときのように一括に設定するのではなく、「マシンごとに」設定を変更する必要があります。

1 管理者になります。

詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2 クライアントを初期化します。

```
# ldapclient manual \
-a domainName=dc=west.example.com -a credentialLevel=proxy \
```

```
-a defaultSearchBase=dc=west,dc=example,dc=com \
-a proxyDN=cn=proxyagent,ou=profile,dc=west,dc=example,dc=com \
-a proxyPassword=testtest 192.168.0.1
```

3 **LDAP** クライアント構成を検証します。

```
# ldapclient list
NS_LDAP_FILE_VERSION= 2.0
NS_LDAP_BINDDN= cn=proxyagent,ou=profile,dc=west,dc=example,dc=com
NS_LDAP_BINDPASSWD= {NS1}4a3788e8c053424f
NS_LDAP_SERVERS= 192.168.0.1
NS_LDAP_SEARCH_BASEDN= dc=west,dc=example,dc=com
NS_LDAP_CREDENTIAL_LEVEL= proxy
```

▼ 手動の LDAP クライアント構成を変更する方法

1 管理者になります。

詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2 **ldapclient mod** コマンドを使用して、認証方法を **simple** に変更します。

```
# ldapclient mod -a authenticationMethod=simple
```

3 **LDAP** クライアント構成に対して変更が行われたを検証します。

```
# ldapclient list
NS_LDAP_FILE_VERSION= 2.0
NS_LDAP_BINDDN= cn=proxyagent,ou=profile,dc=west,dc=example,dc=com
NS_LDAP_BINDPASSWD= {NS1}4a3788e8c053424f
NS_LDAP_SERVERS= 192.168.0.1
NS_LDAP_SEARCH_BASEDN= dc=west,dc=example,dc=com
NS_LDAP_AUTH= simple
NS_LDAP_CREDENTIAL_LEVEL= proxy
```

注意事項 LDAP クライアント構成には、mod サブコマンドでは変更できない属性があります。たとえば、profileName 属性や profileTTL 属性は変更できません。これらの属性を変更するには、192 ページの「プロファイルを使用して LDAP クライアントを初期化する方法」の説明に従って、ldapclient init コマンドを使用して新しいプロファイルを作成します。または、196 ページの「LDAP クライアントを手動で初期化する方法」の説明に従って、ldapclient manual コマンドを実行します。

▼ LDAP クライアントの初期化を解除する方法

ldapclient uninit コマンドは、クライアントのネームサービスを、最新の init、modify、または manual 操作の前の状態に復元します。つまり、このコマンドは、最後に実行された手順に対して「元に戻す」を実行します。たとえ

ば、profile1 を使用するようにクライアントを構成したあとで profile2 を使用するように変更した場合、ldapclient uninit を実行すると、クライアントで profile1 を使用するように構成が元に戻ります。

1 管理者になります。

詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2 **LDAP クライアントの初期化を解除します。**

```
# ldapclient uninit
System successfully recovered
```

TLS のセキュリティーの設定

注 – セキュリティーデータベースファイルは、すべてのユーザーから読み取れるようにする必要があります。key3.db ファイル内にはどの非公開鍵も含めないでください。

TLS (Transport Layer Security) を使用している場合は、必要なセキュリティーデータベースがインストールされている必要があります。特に、証明書ファイルと鍵データベースファイルが必要です。たとえば、Mozilla Firefox のより新しいデータベースフォーマットを使用する場合は、cert8.db、key3.db、secmod.db の 3 つのファイルが必要です。cert8.db ファイルには、信頼できる証明書が含まれています。key3.db ファイルには、クライアントの鍵が入ります。LDAP ネームサービスクライアントがクライアントの鍵を使用しない場合でも、このファイルは必要です。secmod.db ファイルには、 PKCS#11 などのセキュリティーモジュールが入ります。このファイルは、古いフォーマットを使用する場合には必要ありません。

注 – ldapclient を実行する前に、このセクションに記述されている必要なセキュリティーデータベースファイルを設定およびインストールしておく必要があります。

使用しているバージョンの Oracle Directory Server Enterprise Edition 用管理者ガイドの「SSL 管理」の章にある、SSL を使用するための LDAP クライアントの構成に関するセクションを参照してください。これらのファイルを作成および管理する方法について。これらのファイルを構成したら、LDAP ネームサービスクライアントで使用できるように所定の場所にそれらを格納する必要があります。この場所を判断するために、属性 certificatePath が使用されます。この属性はデフォルトで /var/ldap です。

たとえば、Mozilla Firefox を使用して、必要な cert8.db、key3.db、および secmod.db ファイルを設定したあと、それらのファイルを次のようにデフォルトの場所にコピーします。

```
# cp $HOME/.mozilla/firefox/*.default/cert8.db /var/ldap
# cp $HOME/.mozilla/firefox/*.default/key3.db /var/ldap
# cp $HOME/.mozilla/firefox/*.default/secmod.db /var/ldap
```

次に、すべてのユーザーに読み取り権を付与します。

```
# chmod 444 /var/ldap/cert8.db
# chmod 444 /var/ldap/key3.db
# chmod 444 /var/ldap/secmod.db
```

注 – Mozilla Firefox では、cert8.db、key3.db、および secmod.db ファイルが、$HOME/.mozilla の下にあるサブディレクトリ内で管理されます。このため、それらのセキュリティーデータベースを LDAP ネームサービスクライアントで使用する場合は、そのコピーをローカルファイルシステム上に格納する必要があります。

PAM の構成

pam_ldap モジュールは、LDAP のための 1 つの認証およびアカウント管理 PAM モジュールオプションです。pam_ldap で現在サポートされている機能についての詳細は、pam_ldap(5) のマニュアルページを参照してください。

ユーザー別モードと self 資格オプションの両方を選択した場合は、PAM Kerberos pam_krb5 モジュールも有効にする必要があります。詳細は、pam_krb5(5) のマニュアルページおよび『Oracle Solaris 11.1 の管理: セキュリティーサービス』のドキュメントを参照してください。

UNIX policy を使用するための PAM の構成

UNIX policy を使用するように PAM を構成するには、デフォルトの /etc/pam.conf ファイルを使用します。変更は必要ありません。詳細については、pam.conf(4) のマニュアルページを参照してください。

ただし、shadow データによって制御されるパスワードの有効期限とパスワードポリシーが必要な場合は、クライアントを enableShadowUpdate スイッチを使用して構成および実行する必要があります。詳細は、195 ページの「LDAP クライアントを初期化してシャドウデータの更新を有効にする方法」を参照してください。

LDAP server_policy を使用するための PAM の構成

LDAP server_policy を使用するように PAM を構成するには、212 ページの「アカウント管理に pam_ldap モジュールを使用した pam_conf ファイルの例」にあるサンプルに従ってください。pam_ldap.so.1 を含む行をクライアントの /etc/pam.conf ファイ

ルに追加します。さらに、サンプルの pam.conf ファイル内のいずれかの PAM モジュールで binding フラグと server_policy オプションが指定されている場合は、クライアントの /etc/pam.conf ファイル内の対応するモジュールで同じフラグとオプションを使用します。また、サービスモジュール pam_authtok_store.so.1 を含む行にも server_policy オプションを追加します。

注 – 以前は、pam_ldap アカウント管理を有効にすると、システムにログインする際には、常にすべてのユーザーが認証用にログインパスワードを入力する必要がありました。そのため、ssh などのツールを使用した、パスワードに基づかないログインは失敗します。

アカウント管理を実行し、ユーザーがログインしているときに Directory Server への認証を行わずにユーザーのアカウントステータスを取得します。Directory Server 上の新しい制御は 1.3.6.1.4.1.42.2.27.9.5.8 です。これはデフォルトで有効になっています。

この制御をデフォルト以外に変更する場合は、Directory Server 上でアクセス制御情報 (ACI) を追加します。

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
     allow (read, search, compare, proxy)
     (groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

- binding 管理フラグ

  binding 管理フラグを使うことにより、ローカルパスワードがリモート (LDAP) パスワードをオーバーライドします。たとえば、ローカルファイルと LDAP 名前空間の両方にユーザーアカウントが見つかった場合、リモートパスワードよりローカルアカウントのパスワードの方が優先されます。したがって、ローカルパスワードの期限が切れているときは、たとえリモート LDAP パスワードがまだ有効であっても認証に失敗します。

- server_policy オプション

  server_policy オプションによって、pam_unix_auth、 pam_unix_account、および pam_passwd_auth は LDAP 名前空間で検出されたユーザーを無視し、pam_ldap による認証やアカウント検証が可能になります。pam_authtok_store は、新しいパスワードを暗号化せずに LDAP サーバーに渡します。そのため、パスワードはサーバー上で構成されるパスワードの暗号化スキームに基づいたディレクトリに保存されます。詳細は、pam.conf(4) および pam_ldap(5) を参照してください。

LDAP ネームサービス情報の検出

ldaplist ユーティリティーを使用して、LDAP ネームサービスに関する情報を取得できます。この LDAP ユーティリティーは、LDAP サーバーから取得したネームサービス情報を LDIF フォーマットで表示します。このユーティリティーは、トラブルシューティングに役立ちます。詳細は、ldaplist(1) を参照してください。

すべての LDAP コンテナを表示する

ldaplist は、レコードを空行で区切って出力を表示します。この表示方法は、複数行にまたがる大きなレコードに有効です。

注 – ldaplist の出力は、クライアントの構成によって変わります。たとえば、ns_ldap_search の値が one ではなく sub である場合は、ldaplist によって、現在の検索 baseDN の下にあるすべてのエントリが一覧表示されます。

次に ldaplist の出力例を示します。

```
# ldaplist
dn: ou=people,dc=west,dc=example,dc=com

dn: ou=group,dc=west,dc=example,dc=com

dn: ou=rpc,dc=west,dc=example,dc=com

dn: ou=protocols,dc=west,dc=example,dc=com

dn: ou=networks,dc=west,dc=example,dc=com

dn: ou=netgroup,dc=west,dc=example,dc=com

dn: ou=aliases,dc=west,dc=example,dc=com

dn: ou=hosts,dc=west,dc=example,dc=com

dn: ou=services,dc=west,dc=example,dc=com

dn: ou=ethers,dc=west,dc=example,dc=com

dn: ou=profile,dc=west,dc=example,dc=com

dn: automountmap=auto_home,dc=west,dc=example,dc=com

dn: automountmap=auto_direct,dc=west,dc=example,dc=com

dn: automountmap=auto_master,dc=west,dc=example,dc=com

dn: automountmap=auto_shared,dc=west,dc=example,dc=com
```

すべてのユーザーエントリ属性を表示する

ユーザーの passwd エントリなど特定の情報を表示する場合は、次のように getent を使用します。

```
# getent passwd user1
user1::30641:10:Joe Q. User:/home/user1:/bin/csh
```

すべての属性を表示する場合は、-l オプションを指定して ldaplist コマンドを実行します。

```
# ldaplist -l passwd user1
        dn: uid=user1,ou=People,dc=west,dc=example,dc=com
        uid: user1
        cn: user1
        uidNumber: 30641
        gidNumber: 10
        gecos: Joe Q. User
        homeDirectory: /home/user1
        loginShell: /bin/csh
        objectClass: top
        objectClass: shadowAccount
        objectClass: account
        objectClass: posixAccount
        shadowLastChange: 6445
```

LDAP クライアント環境のカスタマイズ

次のセクションでは、LDAP クライアント環境をカスタマイズする方法について説明します。

どのサービスも変更できますが注意が必要です。変更したサービスのデータがサーバー上に生成されない場合、カスタマイズは無効になります。また、ファイルがデフォルトで設定されない場合もあります。

LDAP 用のネームサービススイッチの変更

ネームサービススイッチを変更して、各ネームサービスが自身の情報にアクセスする場所をカスタマイズできます。39 ページの「ネームサービススイッチの管理」を参照してください。

LDAP で DNS を有効にする

DNS を有効にする場合は、49 ページの「DNS クライアントを有効にする方法」を参照してください。ユーザー別の認証が使用されている場合、sasl/GSSAPI および Kerberos メカニズムは DNS ネームサービスが構成され、有効になっていることを想定します。

◆ ◆ ◆ 第 13 章

13 LDAP のトラブルシューティング (リファレンス)

この章では、LDAP 構成に関する問題について説明し、それらの問題を解決するための方法を提案します。

LDAP クライアントステータスの監視

以降のセクションでは、LDAP クライアント環境の状態判定に使用するさまざまなコマンドを紹介します。使用可能なオプションの詳細については、マニュアルページも参照してください。

サービス管理機能 (SMF) の概要については、『Oracle Solaris 11.1 でのサービスと障害の管理』の第 1 章「サービスの管理 (概要)」を参照してください。また、詳細については svcadm(1M) および svcs(1) のマニュアルページも参照してください。

ldap_cachemgr デーモンが実行中であることの確認

ldap_cachemgr デーモンは、常に実行中で適切に機能している必要があります。このデーモンが機能していない場合、システムは動作しません。LDAP クライアントサービス svc:/network/ldap/client を設定して起動すると、クライアントの SMF メソッドは ldap_cachemgr デーモンを自動的に起動します。次の方法により、LDAP クライアントサービスがオンラインかどうかを判定します。

- svcs コマンドを使用して、このサービスが有効になっているかどうかを確認します。

```
# svcs \*ldap\*
STATE          STIME    FMRI
disabled       Aug_24   svc:/network/ldap/client:default
```

- 次のコマンドを使用して、このサービスに関するすべての情報を確認します。

```
# svcs -l network/ldap/client:default
fmri svc:/network/ldap/client:default
name LDAP Name Service Client
enabled false
state disabled
next_state none
state_time Thu Oct 20 23:04:11 2011
logfile /var/svc/log/network-ldap-client:default.log
restarter svc:/system/svc/restarter:default
contract_id
manifest /lib/svc/manifest/network/ldap/client.xml
manifest /lib/svc/manifest/milestone/config.xml
manifest /lib/svc/manifest/network/network-location.xml
manifest /lib/svc/manifest/system/name-service/upgrade.xml
dependency optional_all/none svc:/milestone/config (online)
dependency optional_all/none svc:/network/location:default (online)
dependency require_all/none svc:/system/filesystem/minimal (online)
dependency require_all/none svc:/network/initial (online)
dependency require_all/restart svc:/network/nis/domain (online)
dependency optional_all/none svc:/system/manifest-import (online)
dependency require_all/none svc:/milestone/unconfig (online)
dependency optional_all/none svc:/system/name-service/upgrade (online)
```

- `ldap_cachemgr` に `-g` オプションを渡します。

  このオプションによって、問題の診断に役立つより広範なステータス情報がダンプされます。

```
# /usr/lib/ldap/ldap_cachemgr -g
cachemgr configuration:
server debug level          0
server log file "/var/ldap/cachemgr.log"
number of calls to ldapcachemgr         19

cachemgr cache data statistics:
Configuration refresh information:
  Previous refresh time: 2010/11/16 18:33:28
  Next refresh time:     2010/11/16 18:43:28
Server information:
  Previous refresh time: 2010/11/16 18:33:28
  Next refresh time:     2010/11/16 18:36:08
  server: 192.168.0.0, status: UP
  server: 192.168.0.1, status: ERROR
    error message: Can't connect to the LDAP server
Cache data information:
  Maximum cache entries:          256
  Number of cache entries:          2
```

`ldap_cachemgr` デーモンの詳細については、`ldap_cachemgr(1M)` のマニュアルページを参照してください。

現在のプロファイル情報の確認

スーパーユーザーになるか、または同等の役割になり、`list` オプションを指定して `ldapclient` を実行します。

```
# ldapclient list
NS_LDAP_FILE_VERSION= 2.0
NS_LDAP_BINDDN= cn=proxyagent,ou=profile,dc=west,dc=example,dc=com
NS_LDAP_BINDPASSWD= {NS1}4a3788e8c053424f
NS_LDAP_SERVERS= 192.168.0.1, 192.168.0.10
NS_LDAP_SEARCH_BASEDN= dc=west,dc=example,dc=com
NS_LDAP_AUTH= simple
NS_LDAP_SEARCH_REF= TRUE
NS_LDAP_SEARCH_SCOPE= one
NS_LDAP_SEARCH_TIME= 30
NS_LDAP_SERVER_PREF= 192.168.0.1
NS_LDAP_PROFILE= pit1
NS_LDAP_CREDENTIAL_LEVEL= proxy
NS_LDAP_SERVICE_SEARCH_DESC= passwd:ou=people,?sub
NS_LDAP_SERVICE_SEARCH_DESC= group:ou=group,dc=west,dc=example,dc=com?one
NS_LDAP_BIND_TIME= 5
```

現在のプロファイル情報は、`svccfg` または `svcprop` コマンドか、あるいは `list` オプションを指定した `ldapclient` コマンドを使用して表示できます。使用可能なすべてのプロパティー設定に関する特定の情報については、`ldapclient(1M)` のマニュアルページを参照してください。

基本的なクライアント/サーバー間通信の検証

クライアントが LDAP サーバーに対して通信を行なっていることを確認する最善の方法は、`ldaplist` コマンドを使用することです。引数なしで `ldaplist` を使用すると、サーバー上のすべてのコンテナがダンプされます。この方法はコンテナが存在している限り可能で、コンテナを生成する必要がありません。詳細は、`ldaplist(1)` のマニュアルページを参照してください。

最初の手順が成功したら、`ldaplist passwd` *username* または `ldaplist hosts` *hostname* を試すことができますが、それに大量のデータが含まれる場合は、生成されるデータの少ないサービスを選択するか、またはデータを `head` や `more` にパイプすることもできます。

クライアント以外のマシンからのサーバーデータの確認

前のセクションにあるほとんどのコマンドでは、LDAP クライアントがすでに作成されていることを前提としています。クライアントを作成していない状態でサーバー上のデータをチェックする場合は、`ldapsearch` コマンドを使用します。次の例では、すべてのコンテナをリスト表示します。

```
# ldapsearch -h server1 -b "dc=west,dc=example,dc=com" -s one "objectclass=*"
```

`ldapsearch` コマンドのデフォルト出力は、RFC-2849 で定義されている業界標準の LDIF フォーマットです。`ldapsearch` のすべてのバージョンで、`-L` オプションを使用することによって LDIF フォーマットを出力できます。

LDAP の構成で発生する問題とその解決方法

以降のセクションでは、LDAP の構成で発生する問題とそれらの解決方法について説明します。

未解決のホスト名

LDAP クライアントのバックエンドは、ホスト検索に対して (`gethostbyname()` や `getaddrinfo()` によって返されるホスト名などの) 完全修飾ホスト名を返します。格納済みの名前が指定されている (1 つ以上のドットが含まれている) 場合、クライアントはその名前をそのまま返します。たとえば、格納されている名前が `hostB.eng` であれば、返される名前も `hostB.eng` です。

LDAP ディレクトリに格納された名前が指定されていない (ドットが含まれない) 場合、クライアントのバックエンドは、その名前にドメイン部分を追加します。たとえば、格納されている名前が `hostA` であれば、返される名前は `hostA.domainname` となります。

LDAP ドメイン内のシステムにリモートアクセスできない

DNS ドメイン名が LDAP ドメイン名とは異なる場合、格納されたホスト名が完全指定でない限り LDAP ネームサービスをホスト名に対して使用することはできません。

ログインできない

LDAP クライアントはログイン中、ユーザー認証に PAM モジュールを使用します。UNIX 標準の PAM モジュールでは、パスワードをサーバーから読み込みクライアント側で検査します。このプロセスは、次のいずれかの理由で失敗することがあります。

1. `ldap` が、ネームサービススイッチ内の `passwd` データベースに関連付けられていない。
2. プロキシエージェントが、サーバーリスト上のユーザーの `userPassword` 属性を読み取ることができない。プロキシエージェントが比較のためにパスワードをクライアントに返すので、少なくともプロキシエージェントはパスワードを読めなければならない。`pam_ldap` に関しては、パスワードへの読み取りアクセスを必要としない
3. プロキシエージェントが適切なパスワードを保持していない
4. 該当するエントリに `shadowAccount` オブジェクトクラスが定義されていない

5. パスワードが定義されていない

   `ldapaddent` を使用する場合、`-p` オプションを使用してパスワードをユーザーエントリに確実に追加する必要があります。`ldapaddent` を `-p` オプションなしで使用すると、`ldapaddent` を使用して `/etc/shadow` ファイルも追加しないかぎり、ユーザーのパスワードはディレクトリ内に格納されません。

6. LDAP サーバーに到達することができない

   サーバーのステータスを確認します。

   ```
   # /usr/lib/ldap/ldap_cachemgr -g
   ```

7. `pam.conf` の構成が不正である
8. LDAP 名前空間でユーザーが定義されていない
9. `pam_unix_*` モジュールに関して `NS_LDAP_CREDENTIAL_LEVEL` が `anonymous` に設定されているため、匿名ユーザーが `userPassword` を使用できない。
10. パスワードが `crypt` 形式で格納されていない
11. アカウント管理をサポートするように `pam_ldap` が構成されている場合は、次のいずれかの原因でログインに失敗します。
    - ユーザーのパスワード期限が切れている
    - ログインを何回も行なったために、ユーザーアカウントがロックされる
    - 管理者がユーザーアカウントを非アクティブにした
    - ユーザーが、`ssh` や `sftp` などの、パスワードを使用しないプログラムを使用してログインしようとした。
12. ユーザー別の認証および sasl/GSSAPI を使用している場合、一部の Kerberos コンポーネントまたは `pam_krb5` 構成が正しく設定されません。これらの問題の解決についての詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』を参照してください。

検索が遅すぎる

LDAP データベースは、検索パフォーマンス向上にインデックスを使用します。インデックスが正しく構成されていない場合、大幅にパフォーマンスが低下することがあります。このドキュメントには、インデックスを作成する必要のある共通の属性セットを記述しています。また、独自のインデックスを追加して、パフォーマンスの向上を図ることができます。

ldapclient コマンドがサーバーにバインドできない

profileName 属性が指定された init オプションを使用しているときに、ldapclient コマンドがクライアントの初期化に失敗しました。考えられる失敗の原因は次のとおりです。

1. コマンド行で不正なドメイン名が指定された
2. 指定されたクライアントドメインのエントリポイントを表す nisDomain 属性が DIT (ディレクトリ情報ツリー) 内に設定されていない
3. アクセス制御情報がサーバー上で適正に設定されていないため、LDAP データベース内の匿名検索が許可されない
4. ldapclient コマンドに正しくないサーバーアドレスが渡されました。ldapsearch コマンドを使用してサーバーアドレスを確認してください。
5. ldapclient コマンドに正しくないプロファイル名が渡されました。ldapsearch コマンドを使用して DIT 内のプロファイル名を確認してください。
6. クライアントのネットワークインタフェースに対して snoop を実行して外向きのトラフィックを検査して、どのサーバーにアクセスしているかを確認する

デバッグでの ldap_cachemgr デーモンの使用

-g オプションを指定して ldap_cachemgr デーモンを実行すると、現在のクライアント構成や統計情報を表示できるため、デバッグのための有効な方法になることがあります。例:

```
# ldap_cachemgr -g
```

この結果、すでに説明したように、すべての LDAP サーバーのステータスを含む現在のクライアント構成および統計が標準出力に出力されます。このコマンドを実行するのに、スーパーユーザーになる必要はありません。

設定中に ldapclient コマンドがハングアップする

ldapclient コマンドがハングアップした場合、Ctrl-C キーを押すと以前の環境を復元したあとで終了します。この状況が発生する場合、サーバーが動作していることをサーバー管理者に確認してください。

プロファイルまたはコマンド行に指定されたサーバーリスト属性で、サーバー情報が適正であることを確認してください。

◆ ◆ ◆ 第 14 章

LDAP ネームサービス (リファレンス)

この章の内容は次のとおりです。

LDAP を構成するための空白のチェックリスト

表 14–1 サーバー変数の定義のための空白のチェックリスト

変数	_____ ネットワークの定義
インストールしたディレクトリサーバーインスタンスのポート番号 (389)	
サーバーの名前	
複製サーバー (IP 番号:ポート番号)	
ディレクトリマネージャー [dn: cn=directory manager]	
サービスされるドメイン名	

表 14–1 サーバー変数の定義のための空白のチェックリスト (続き)

変数	_____ ネットワークの定義
クライアント要求の処理がタイムアウトするまでの時間 (秒)	
各検索要求で返されるエントリの最大数	

表 14–2 クライアントプロファイル変数の定義のための空白のチェックリスト

変数	_____ ネットワークの定義
プロファイル名	
サーバーリスト (デフォルトはローカルサブネット)	
優先されるサーバーリスト (優先順に記載)	
検索範囲 (検索するディレクトリツリーレベルの数、「One」または「Sub」)	
サーバーへのアクセスに使用する資格。デフォルトは anonymous です。	
参照に従うかどうか。(メインサーバーが利用不可能な場合に使用される、別のサーバーへのポインタ)。デフォルトは no	
サーバーが情報を返すのを待つサーチ時間の制限 (秒単位)。デフォルトは 30 秒です。	
サーバーに接続するためのバインド制限の時間 (秒単位)。デフォルトは 30 秒です。	
認証方式。デフォルトは none	

LDAP コマンド

Oracle Solaris システムには、LDAP 関連のコマンドのセットが 2 つあります。1 つのセットは一般的な LDAP ツールで、LDAP ネームサービスを使用してクライアントを構成する必要はありません。2 つ目のセットは、クライアント上の共通の LDAP 構成を使用し、LDAP ネームサービスとともに、またはなしで構成されているクライアント上で実行できます。

一般的な LDAP ツール

LDAP コマンド行ツールは、認証やバインドパラメータを含む、一般的なオプションセットをサポートします。次のツールは、LDAP データ交換フォーマット (LDIF) というディレクトリ情報を表現する共通のテキストベース書式をサポートします。これらのコマンドを使用して、ディレクトリエントリを直接操作できます。

ldapsearch(1)
ldapmodify(1)
ldapadd(1)
ldapdelete(1)

LDAP ネームサービスを必要とする LDAP ツール

表 14–3 LDAP ツール

ツール	機能
ldapaddent(1M)	LDAP コンテナ内に、/etc 内のファイルに対応するエントリを作成する。このツールを使用して、ファイルからディレクトリを生成できる。たとえば、/etc/passwd 形式のファイルを読み取り、ディレクトリ内に passwd エントリを生成します。
ldaplist(1)	ディレクトリから、さまざまなサービスの内容をリスト表示するのに使用する
idsconfig(1M)	LDAP ネームサービスクライアント対応の Oracle Directory Server Enterprise Edition の設定に使用する

アカウント管理に **pam_ldap** モジュールを使用した **pam_conf** ファイルの例

注 – 以前は、pam_ldap アカウント管理を有効にすると、システムにログインする際には、常にすべてのユーザーが認証用にログインパスワードを入力する必要がありました。そのため、ssh などのツールを使用した、パスワードに基づかないログインは失敗します。

アカウント管理を実行し、ユーザーがログインしているときに Directory Server への認証を行わずにユーザーのアカウントステータスを取得します。Directory Server 上の新しい制御は 1.3.6.1.4.1.42.2.27.9.5.8 です。これはデフォルトで有効になっています。

この制御をデフォルト以外に変更する場合は、Directory Server 上でアクセス制御情報 (ACI) を追加します。

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
     allow (read, search, compare, proxy)
     (groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

```
#
# Authentication management
#
# login service (explicit because of pam_dial_auth)
#
login   auth requisite        pam_authtok_get.so.1
login   auth required         pam_dhkeys.so.1
login   auth required         pam_unix_cred.so.1
login   auth required         pam_dial_auth.so.1
login   auth binding          pam_unix_auth.so.1 server_policy
login   auth required         pam_ldap.so.1
#
# rlogin service (explicit because of pam_rhost_auth)
#
rlogin  auth sufficient       pam_rhosts_auth.so.1
rlogin  auth requisite        pam_authtok_get.so.1
rlogin  auth required         pam_dhkeys.so.1
rlogin  auth required         pam_unix_cred.so.1
rlogin  auth binding          pam_unix_auth.so.1 server_policy
rlogin  auth required         pam_ldap.so.1
#
# rsh service (explicit because of pam_rhost_auth,
# and pam_unix_auth for meaningful pam_setcred)
```

```
#
rsh     auth sufficient       pam_rhosts_auth.so.1
rsh     auth required         pam_unix_cred.so.1
rsh     auth binding          pam_unix_auth.so.1 server_policy
rsh     auth required         pam_ldap.so.1
#
# PPP service (explicit because of pam_dial_auth)
#
ppp     auth requisite        pam_authtok_get.so.1
ppp     auth required         pam_dhkeys.so.1
ppp     auth required         pam_dial_auth.so.1
ppp     auth binding          pam_unix_auth.so.1 server_policy
ppp     auth required         pam_ldap.so.1
#
# Default definitions for Authentication management
# Used when service name is not explicitly mentioned for authentication
#
other   auth requisite        pam_authtok_get.so.1
other   auth required         pam_dhkeys.so.1
other   auth required         pam_unix_cred.so.1
other   auth binding          pam_unix_auth.so.1 server_policy
other   auth required         pam_ldap.so.1
#
# passwd command (explicit because of a different authentication module)
#
passwd  auth binding          pam_passwd_auth.so.1 server_policy
passwd  auth required         pam_ldap.so.1
#
# cron service (explicit because of non-usage of pam_roles.so.1)
#
cron    account required      pam_unix_account.so.1
#
# Default definition for Account management
# Used when service name is not explicitly mentioned for account management
#
other   account requisite     pam_roles.so.1
other   account binding       pam_unix_account.so.1 server_policy
other   account required      pam_ldap.so.1
#
# Default definition for Session management
# Used when service name is not explicitly mentioned for session management
#
other   session required      pam_unix_session.so.1
#
# Default definition for  Password management
# Used when service name is not explicitly mentioned for password management
#
other   password required     pam_dhkeys.so.1
other   password requisite    pam_authtok_get.so.1
other   password requisite    pam_authtok_check.so.1
other   password required     pam_authtok_store.so.1 server_policy
#
# Support for Kerberos V5 authentication and example configurations can
# be found in the pam_krb5(5) man page under the "EXAMPLES" section.
#
```

LDAP 用の IETF スキーマ

スキーマは、サーバーのディレクトリ内にエントリとして格納可能な情報タイプを記述した定義です。

ディレクトリサーバーが LDAP ネームサービスクライアントをサポートするには、スキーマがクライアントのスキーママッピング機能を使用してマップされていないかぎり、この章で定義されたスキーマがサーバー内で構成されている必要があります。

次のいくつかの必要な LDAP スキーマが IETF によって定義されています: RFC 2307 ネットワーク情報サービススキーマと RFC 2307bis、Lightweight Directory Access Protocol (LDAP) ベースのエージェント用の構成プロファイルスキーマ (RFC 4876)、およびプリンタサービス用の LDAP スキーマ。NIS をサポートするには、これらのスキーマの定義をディレクトリサーバーに追加する必要があります。IETF の Web サイト (`http://www.ietf.org`) で、さまざまな RFC にアクセスできます。

注 – インターネットドラフト (RFC 2307bis など) は、最大 6 か月間有効なドラフトドキュメントであり、いつでもほかのドキュメントによって更新または廃止される可能性があります。

RFC 2307bis ネットワーク情報サービススキーマ

LDAP サーバーは、改訂された RFC 2307bis をサポートするように構成される必要があります。

`nisSchema` OID は `1.3.6.1.1` です。RFC 2307bis 属性を次に示します。

```
( nisSchema.1.0 NAME 'uidNumber'
DESC 'An integer uniquely identifying a user in an
        administrative domain'
EQUALITY integerMatch SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.1 NAME 'gidNumber'
DESC 'An integer uniquely identifying a group in an
        administrative domain'
EQUALITY integerMatch SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.2 NAME 'gecos'
DESC 'The GECOS field; the common name'
EQUALITY caseIgnoreIA5Match
SUBSTRINGS caseIgnoreIA5SubstringsMatch
SYNTAX 'IA5String' SINGLE-VALUE )

( nisSchema.1.3 NAME 'homeDirectory'
DESC 'The absolute path to the home directory'
EQUALITY caseExactIA5Match
SYNTAX 'IA5String' SINGLE-VALUE )
```

```
( nisSchema.1.4 NAME 'loginShell'
DESC 'The path to the login shell'
EQUALITY caseExactIA5Match
SYNTAX 'IA5String' SINGLE-VALUE )

( nisSchema.1.5 NAME 'shadowLastChange'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.6 NAME 'shadowMin'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.7 NAME 'shadowMax'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.8 NAME 'shadowWarning'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.9 NAME 'shadowInactive'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.10 NAME 'shadowExpire'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.11 NAME 'shadowFlag'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.12 NAME 'memberUid'
EQUALITY caseExactIA5Match
SUBSTRINGS caseExactIA5SubstringsMatch
SYNTAX 'IA5String' )

( nisSchema.1.13 NAME 'memberNisNetgroup'
EQUALITY caseExactIA5Match
SUBSTRINGS caseExactIA5SubstringsMatch
SYNTAX 'IA5String' )

( nisSchema.1.14 NAME 'nisNetgroupTriple'
DESC 'Netgroup triple'
SYNTAX 'nisNetgroupTripleSyntax' )

( nisSchema.1.15 NAME 'ipServicePort'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.16 NAME 'ipServiceProtocol'
SUP name )

( nisSchema.1.17 NAME 'ipProtocolNumber'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )
```

```
( nisSchema.1.18 NAME 'oncRpcNumber'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.19 NAME 'ipHostNumber'
DESC 'IP address as a dotted decimal, eg. 192.168.1.1
        omitting leading zeros'
SUP name )

( nisSchema.1.20 NAME 'ipNetworkNumber'
DESC 'IP network as a dotted decimal, eg. 192.168,
        omitting leading zeros'
SUP name SINGLE-VALUE )

( nisSchema.1.21 NAME 'ipNetmaskNumber'
DESC 'IP netmask as a dotted decimal, eg. 255.255.255.0,
         omitting leading zeros'
EQUALITY caseIgnoreIA5Match
SYNTAX 'IA5String{128}' SINGLE-VALUE )

( nisSchema.1.22 NAME 'macAddress'
DESC 'MAC address in maximal, colon separated hex
      notation, eg. 00:00:92:90:ee:e2'
EQUALITY caseIgnoreIA5Match
SYNTAX 'IA5String{128}' )

( nisSchema.1.23 NAME 'bootParameter'
DESC 'rpc.bootparamd parameter'
SYNTAX 'bootParameterSyntax' )

( nisSchema.1.24 NAME 'bootFile'
DESC 'Boot image name'
EQUALITY caseExactIA5Match
SYNTAX 'IA5String' )

( nisSchema.1.26 NAME 'nisMapName'
SUP name )

( nisSchema.1.27 NAME 'nisMapEntry'
EQUALITY caseExactIA5Match
SUBSTRINGS caseExactIA5SubstringsMatch
SYNTAX 'IA5String{1024}' SINGLE-VALUE )

( nisSchema.1.28 NAME 'nisPublicKey'
DESC 'NIS public key'
SYNTAX 'nisPublicKeySyntax' )

( nisSchema.1.29 NAME 'nisSecretKey'
DESC 'NIS secret key'
SYNTAX 'nisSecretKeySyntax' )

( nisSchema.1.30 NAME 'nisDomain'
DESC 'NIS domain'
SYNTAX 'IA5String' )

( nisSchema.1.31 NAME 'automountMapName'
DESC 'automount Map Name'
EQUALITY caseExactIA5Match
SUBSTR caseExactIA5SubstringsMatch
```

```
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )

( nisSchema.1.32 NAME 'automountKey'
DESC 'Automount Key value'
EQUALITY caseExactIA5Match
SUBSTR caseExactIA5SubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )

( nisSchema.1.33 NAME 'automountInformation'
DESC 'Automount information'
EQUALITY caseExactIA5Match
SUBSTR caseExactIA5SubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )
```

nisSchema OID は 1.3.6.1.1 です。RFC 2307 objectClasses を次に示します。

```
( nisSchema.2.0 NAME 'posixAccount' SUP top AUXILIARY
  DESC 'Abstraction of an account with POSIX attributes'
  MUST ( cn $ uid $ uidNumber $ gidNumber $ homeDirectory )
  MAY ( userPassword $ loginShell $ gecos $ description ) )

( nisSchema.2.1 NAME 'shadowAccount' SUP top AUXILIARY
  DESC 'Additional attributes for shadow passwords'
  MUST uid
  MAY ( userPassword $ shadowLastChange $ shadowMin
        shadowMax $ shadowWarning $ shadowInactive $
        shadowExpire $ shadowFlag $ description ) )

( nisSchema.2.2 NAME 'posixGroup' SUP top STRUCTURAL
  DESC 'Abstraction of a group of accounts'
  MUST ( cn $ gidNumber )
  MAY ( userPassword $ memberUid $ description ) )

( nisSchema.2.3 NAME 'ipService' SUP top STRUCTURAL
  DESC 'Abstraction an Internet Protocol service.
        Maps an IP port and protocol (such as tcp or udp)
        to one or more names; the distinguished value of
        the cn attribute denotes the service's canonical
        name'
  MUST ( cn $ ipServicePort $ ipServiceProtocol )
  MAY ( description ) )

( nisSchema.2.4 NAME 'ipProtocol' SUP top STRUCTURAL
  DESC 'Abstraction of an IP protocol. Maps a protocol number
        to one or more names. The distinguished value of the cn
        attribute denotes the protocol's canonical name'
  MUST ( cn $ ipProtocolNumber )
  MAY  description )

( nisSchema.2.5 NAME 'oncRpc' SUP top STRUCTURAL
  DESC 'Abstraction of an Open Network Computing (ONC)
        [RFC1057] Remote Procedure Call (RPC) binding.
        This class maps an ONC RPC number to a name.
        The distinguished value of the cn attribute denotes
        the RPC service's canonical name'
  MUST ( cn $ oncRpcNumber $ description )
  MAY  description )
```

```
( nisSchema.2.6 NAME 'ipHost' SUP top AUXILIARY
  DESC 'Abstraction of a host, an IP device. The distinguished
        value of the cn attribute denotes the host's canonical
        name. Device SHOULD be used as a structural class'
  MUST ( cn $ ipHostNumber )
  MAY ( l $ description $ manager $ userPassword ) )

( nisSchema.2.7 NAME 'ipNetwork' SUP top STRUCTURAL
  DESC 'Abstraction of a network. The distinguished value of
        the cn attribute denotes the network's canonical name'
  MUST ipNetworkNumber
  MAY ( cn $ ipNetmaskNumber $ l $ description $ manager ) )

( nisSchema.2.8 NAME 'nisNetgroup' SUP top STRUCTURAL
  DESC 'Abstraction of a netgroup. May refer to other netgroups'
  MUST cn
  MAY ( nisNetgroupTriple $ memberNisNetgroup $ description ) )

( nisSchema.2.9 NAME 'nisMap' SUP top STRUCTURAL
  DESC 'A generic abstraction of a NIS map'
  MUST nisMapName
  MAY description )

( nisSchema.2.10 NAME 'nisObject' SUP top STRUCTURAL
  DESC 'An entry in a NIS map'
  MUST ( cn $ nisMapEntry $ nisMapName )
  MAY description )

( nisSchema.2.11 NAME 'ieee802Device' SUP top AUXILIARY
  DESC 'A device with a MAC address; device SHOULD be
        used as a structural class'
  MAY macAddress )

( nisSchema.2.12 NAME 'bootableDevice' SUP top AUXILIARY
  DESC 'A device with boot parameters; device SHOULD be
  used as a structural class'
  MAY ( bootFile $ bootParameter ) )

( nisSchema.2.14 NAME 'nisKeyObject' SUP top AUXILIARY
  DESC 'An object with a public and secret key'
  MUST ( cn $ nisPublicKey $ nisSecretKey )
  MAY ( uidNumber $ description ) )

( nisSchema.2.15 NAME 'nisDomainObject' SUP top AUXILIARY
  DESC 'Associates a NIS domain with a naming context'
  MUST nisDomain )

( nisSchema.2.16 NAME 'automountMap' SUP top STRUCTURAL
  MUST ( automountMapName )
  MAY description )

( nisSchema.2.17 NAME 'automount' SUP top STRUCTURAL
  DESC 'Automount information'
  MUST ( automountKey $ automountInformation )
  MAY description )

( nisSchema.2.18 NAME 'groupOfMembers' SUP top STRUCTURAL
  DESC 'A group with members (DNs)'
  MUST cn
```

```
  MAY ( businessCategory $ seeAlso $ owner $ ou $ o $
        description $ member ) )
```

メールエイリアススキーマ

メールエイリアス情報は、このインターネットドラフトによって定義されたスキーマを使用します。新しいスキーマが使用可能になるまで、LDAP クライアントは、引き続きこのスキーマをメールエイリアス情報として使用します。

元の LDAP メールグループスキーマには、多数の属性とオブジェクトクラスが含まれています。LDAP クライアントによって使用されるのは、2 つの属性と 1 つのオブジェクトクラスだけです。次にその内容を示します。

メールエイリアス属性を次に示します。

```
( 0.9.2342.19200300.100.1.3
  NAME 'mail'
  DESC 'RFC822 email address for this person'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String(256)'
  SINGLE-VALUE )

( 2.16.840.1.113730.3.1.30
  NAME 'mgrpRFC822MailMember'
  DESC 'RFC822 mail address of email only member of group'
  EQUALITY CaseIgnoreIA5Match
  SYNTAX 'IA5String(256)' )
```

`mailGroup` オブジェクトクラスのスキーマを次に示します。

```
( 2.16.840.1.113730.3.2.4
  NAME 'mailGroup'
  SUP top
  STRUCTURAL
  MUST mail
  MAY ( cn $ mailAlternateAddress $ mailHost $ mailRequireAuth $
   mgrpAddHeader $ mgrpAllowedBroadcaster $ mgrpAllowedDomain $
   mgrpApprovePassword $ mgrpBroadcasterModeration $ mgrpDeliverTo $
   mgrpErrorsTo $ mgrpModerator $ mgrpMsgMaxSize $
   mgrpMsgRejectAction $ mgrpMsgRejectText $ mgrpNoMatchAddrs $
   mgrpRemoveHeader $ mgrpRFC822MailMember ))
```

ディレクトリユーザーエージェントのプロファイル (DUAProfile) のスキーマ

`DUAConfSchemaOID` は `1.3.6.1.4.1.11.1.3.1` です。

```
DESC 'Default LDAP server host address used by a DUA'
            EQUALITY caseIgnoreMatch
            SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
```

```
  SINGLE-VALUE )

( DUAConfSchemaOID.1.0 NAME 'defaultServerList'
  DESC 'Default LDAP server host address used by a DUAList'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE )

( DUAConfSchemaOID.1.1 NAME 'defaultSearchBase'
  DESC 'Default LDAP base DN used by a DUA'
  EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  SINGLE-VALUE )

( DUAConfSchemaOID.1.2 NAME 'preferredServerList'
  DESC 'Preferred LDAP server host addresses to be used by a
  DUA'
  EQUALITY caseIgnoreMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE )

( DUAConfSchemaOID.1.3 NAME 'searchTimeLimit'
  DESC 'Maximum time in seconds a DUA should allow for a
  search to complete'
  EQUALITY integerMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
  SINGLE-VALUE )

( DUAConfSchemaOID.1.4 NAME 'bindTimeLimit'
  DESC 'Maximum time in seconds a DUA should allow for the
  bind operation to complete'
  EQUALITY integerMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
  SINGLE-VALUE )

( DUAConfSchemaOID.1.5 NAME 'followReferrals'
  DESC 'Tells DUA if it should follow referrals
  returned by a DSA search result'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
  SINGLE-VALUE )

( DUAConfSchemaOID.1.6 NAME 'authenticationMethod'
  DESC 'A keystring which identifies the type of
  authentication method used to contact the DSA'
  EQUALITY caseIgnoreMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE )

( DUAConfSchemaOID.1.7 NAME 'profileTTL'
  DESC 'Time to live before a client DUA
  should re-read this configuration profile'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
  SINGLE-VALUE )

( DUAConfSchemaOID.1.9 NAME 'attributeMap'
  DESC 'Attribute mappings used by a DUA'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

```
( DUAConfSchemaOID.1.10 NAME 'credentialLevel'
  DESC 'Identifies type of credentials a DUA should
  use when binding to the LDAP server'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
  SINGLE-VALUE )

( DUAConfSchemaOID.1.11 NAME 'objectclassMap'
  DESC 'Objectclass mappings used by a DUA'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

( DUAConfSchemaOID.1.12 NAME 'defaultSearchScope'
  DESC 'Default search scope used by a DUA'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE )

( DUAConfSchemaOID.1.13 NAME 'serviceCredentialLevel'
  DESC 'Identifies type of credentials a DUA
  should use when binding to the LDAP server for a
  specific service'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

( DUAConfSchemaOID.1.14 NAME 'serviceSearchDescriptor'
  DESC 'LDAP search descriptor list used by Naming-DUA'
  EQUALITY caseIgnoreMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

( DUAConfSchemaOID.1.15 NAME 'serviceAuthenticationMethod'
  DESC 'Authentication Method used by a service of the DUA'
  EQUALITY caseIgnoreMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

   ( DUAConfSchemaOID.2.4 NAME 'DUAConfigProfile'
        SUP top STRUCTURAL
     DESC 'Abstraction of a base configuration for a DUA'
     MUST ( cn )
     MAY ( defaultServerList $ preferredServerList $
    defaultSearchBase $ defaultSearchScope $
    searchTimeLimit $ bindTimeLimit $
    credentialLevel $ authenticationMethod $
    followReferrals $ serviceSearchDescriptor $
    serviceCredentialLevel $ serviceAuthenticationMethod $
    objectclassMap $ attributeMap $
    profileTTL ) )
```

Oracle Solaris のスキーマ

Oracle Solaris プラットフォームに必要なスキーマを次に示します。

- プロジェクトスキーマ
- アクセス制御および実行プロファイルスキーマに基づく役割
- プリンタスキーマ

プロジェクトスキーマ

/etc/project ファイルは、プロジェクトに関連付けられた属性のローカルソースです。詳細は、user_attr(4) のマニュアルページを参照してください。

プロジェクト属性を次に示します。

```
( 1.3.6.1.4.1.42.2.27.5.1.1 NAME 'SolarisProjectID'
  DESC 'Unique ID for a Solaris Project entry'
  EQUALITY integerMatch
  SYNTAX INTEGER SINGLE )

( 1.3.6.1.4.1.42.2.27.5.1.2 NAME 'SolarisProjectName'
  DESC 'Name of a Solaris Project entry'
  EQUALITY caseExactIA5Match
  SYNTAX IA5String SINGLE )

( 1.3.6.1.4.1.42.2.27.5.1.3 NAME 'SolarisProjectAttr'
  DESC 'Attributes of a Solaris Project entry'
  EQUALITY caseExactIA5Match
  SYNTAX IA5String )

( 1.3.6.1.4.1.42.2.27.5.1.30 NAME 'memberGid'
  DESC 'Posix Group Name'
  EQUALITY caseExactIA5Match
  SYNTAX 'IA5String' )
```

プロジェクト objectClass を次に示します。

```
( 1.3.6.1.4.1.42.2.27.5.2.1 NAME 'SolarisProject'
  SUP top STRUCTURAL
  MUST ( SolarisProjectID $ SolarisProjectName )
  MAY ( memberUid $ memberGid $ description $ SolarisProjectAttr ) )
```

役割ベースのアクセス制御と実行プロファイルスキーマ

/etc/user_attr ファイルは、ユーザーと役割に関連付けられた拡張属性のローカルソースです。詳細は、user_attr(4) のマニュアルページを参照してください。

役割に基づくアクセス制御の属性を次に示します。

```
( 1.3.6.1.4.1.42.2.27.5.1.4 NAME 'SolarisAttrKeyValue'
  DESC 'Semi-colon separated key=value pairs of attributes'
  EQUALITY caseIgnoreIA5Match
  SUBSTRINGS caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.7 NAME 'SolarisAttrShortDesc'
  DESC 'Short description about an entry, used by GUIs'
  EQUALITY caseIgnoreIA5Match
```

```
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.8 NAME 'SolarisAttrLongDesc'
  DESC 'Detail description about an entry'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.9 NAME 'SolarisKernelSecurityPolicy'
  DESC 'Solaris  kernel security policy'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.10 NAME 'SolarisProfileType'
  DESC 'Type of object defined in profile'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.11 NAME 'SolarisProfileId'
  DESC 'Identifier of object defined in profile'
  EQUALITY caseExactIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.12 NAME 'SolarisUserQualifier'
  DESC 'Per-user login attributes'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.13 NAME 'SolarisReserved1'
  DESC 'Reserved for future use'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.14 NAME 'SolarisReserved2'
  DESC 'Reserved for future use'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )
```

役割に基づくアクセス制御 `objectClassses` を次に示します。

```
( 1.3.6.1.4.1.42.2.27.5.2.3 NAME 'SolarisUserAttr' SUP top AUXILIARY
  DESC 'User attributes'
  MAY ( SolarisUserQualifier $ SolarisAttrReserved1 $ \
        SolarisAttrReserved2 $ SolarisAttrKeyValue ) )

( 1.3.6.1.4.1.42.2.27.5.2.4 NAME 'SolarisAuthAttr' SUP top STRUCTURAL
  DESC 'Authorizations data'
  MUST cn
  MAY ( SolarisAttrReserved1 $ SolarisAttrReserved2 $ \
        SolarisAttrShortDesc $ SolarisAttrLongDesc $ \
        SolarisAttrKeyValue ) )

( 1.3.6.1.4.1.42.2.27.5.2.5 NAME 'SolarisProfAttr' SUP top STRUCTURAL
  DESC 'Profiles data'
  MUST cn
  MAY ( SolarisAttrReserved1 $ SolarisAttrReserved2 $ \
        SolarisAttrLongDesc $ SolarisAttrKeyValue ) )

( 1.3.6.1.4.1.42.2.27.5.2.6 NAME 'SolarisExecAttr' SUP top AUXILIARY
```

```
  DESC 'Profiles execution attributes'
  MAY ( SolarisKernelSecurityPolicy $ SolarisProfileType $ \
        SolarisAttrReserved1 $ SolarisAttrReserved2 $ \
        SolarisProfileId $ SolarisAttrKeyValue ) )
```

LDAP 用の Internet Printing Protocol 情報

次のセクションでは、Internet Print Protocol とプリンタの属性および `ObjectClass` について説明します。

Internet Print Protocol 属性

```
( 1.3.18.0.2.4.1140
NAME 'printer-uri'
DESC 'A URI supported by this printer.
This URI SHOULD be used as a relative distinguished name (RDN).
If printer-xri-supported is implemented, then this URI value
MUST be listed in a member value of printer-xri-supported.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )

( 1.3.18.0.2.4.1107
NAME 'printer-xri-supported'
DESC 'The unordered list of XRI (extended resource identifiers) supported
by this printer.
Each member of the list consists of a URI (uniform resource identifier)
followed by optional authentication and security metaparameters.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

( 1.3.18.0.2.4.1135
NAME 'printer-name'
DESC 'The site-specific administrative name of this printer, more end-user
friendly than a URI.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127}  SINGLE-VALUE )

( 1.3.18.0.2.4.1119
NAME 'printer-natural-language-configured'
DESC 'The configured language in which error and status messages will be
generated (by default) by this printer.
Also, a possible language for printer string attributes set by operator,
system administrator, or manufacturer.
Also, the (declared) language of the "printer-name", "printer-location",
"printer-info", and "printer-make-and-model" attributes of this printer.
For example: "en-us" (US English) or "fr-fr" (French in France) Legal values of
```

```
language tags conform to [RFC3066] "Tags for the Identification of Languages".'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127}  SINGLE-VALUE )

( 1.3.18.0.2.4.1136
NAME 'printer-location'
DESC 'Identifies the location of the printer. This could include
things like: "in Room 123A", "second floor of building XYZ".'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} SINGLE-VALUE )

( 1.3.18.0.2.4.1139
NAME 'printer-info'
DESC 'Identifies the descriptive information about this printer.
This could include things like: "This printer can be used for
printing color transparencies for HR presentations", or
"Out of courtesy for others, please print only small (1-5 page)
jobs at this printer", or even "This printer is going away on July 1, 1997,
please find a new printer".'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127}
SINGLE-VALUE )

( 1.3.18.0.2.4.1134
NAME 'printer-more-info'
DESC 'A URI used to obtain more information about this specific printer.
For example, this could be an HTTP type URI referencing an HTML page
accessible to a Web Browser.
The information obtained from this URI is intended for end user consumption.'
EQUALITY caseIgnoreMatch ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )

( 1.3.18.0.2.4.1138
NAME 'printer-make-and-model'
DESC 'Identifies the make and model of the device.
The device manufacturer MAY initially populate this attribute.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{127}  SINGLE-VALUE )

( 1.3.18.0.2.4.1133
NAME 'printer-ipp-versions-supported'
DESC 'Identifies the IPP protocol version(s) that this printer supports,
including major and minor versions,
i.e., the version numbers for which this Printer implementation meets
the conformance requirements.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )
```

```
( 1.3.18.0.2.4.1132
NAME 'printer-multiple-document-jobs-supported'
DESC 'Indicates whether or not the printer supports more than one
document per job, i.e., more than one Send-Document or Send-Data
operation with document data.'
EQUALITY booleanMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE )

( 1.3.18.0.2.4.1109
NAME 'printer-charset-configured'
DESC 'The configured charset in which error and status messages will be
generated (by default) by this printer.
Also, a possible charset for printer string attributes set by operator,
system administrator, or manufacturer.
For example: "utf-8" (ISO 10646/Unicode) or "iso-8859-1" (Latin1).
Legal values are defined by the IANA Registry of Coded Character Sets and
the "(preferred MIME name)" SHALL be used as the tag.
For coherence with IPP Model, charset tags in this attribute SHALL be
lowercase normalized.
This attribute SHOULD be static (time of registration) and SHOULD NOT be
dynamically refreshed attributetypes: (subsequently).'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{63} SINGLE-VALUE )

( 1.3.18.0.2.4.1131
NAME 'printer-charset-supported'
DESC 'Identifies the set of charsets supported for attribute type values of
type Directory String for this directory entry.
For example: "utf-8" (ISO 10646/Unicode) or "iso-8859-1" (Latin1).
Legal values are defined by the IANA Registry of Coded Character Sets and
the preferred MIME name.'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{63} )

( 1.3.18.0.2.4.1137
NAME 'printer-generated-natural-language-supported'
DESC 'Identifies the natural language(s) supported for this directory entry.
For example: "en-us" (US English) or "fr-fr" (French in France).
Legal values conform to [RFC3066], Tags for the Identification of Languages.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{63} )

( 1.3.18.0.2.4.1130
NAME 'printer-document-format-supported'
DESC 'The possible document formats in which data may be interpreted
and printed by this printer.
Legal values are MIME types come from the IANA Registry of Internet Media Types.'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1129
NAME 'printer-color-supported'
DESC 'Indicates whether this printer is capable of any type of color printing
at all, including highlight color.'
EQUALITY booleanMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.7  SINGLE-VALUE )
```

```
( 1.3.18.0.2.4.1128
NAME 'printer-compression-supported'
DESC 'Compression algorithms supported by this printer.
For example: "deflate, gzip".  Legal values include; "none", "deflate"
attributetypes: (public domain ZIP), "gzip" (GNU ZIP), "compress" (UNIX).'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{255} )

( 1.3.18.0.2.4.1127
NAME 'printer-pages-per-minute'
DESC 'The nominal number of pages per minute which may be output by this
printer (e.g., a simplex or black-and-white printer).
This attribute is informative, NOT a service guarantee.
Typically, it is the value used in marketing literature to describe this printer.'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.27  SINGLE-VALUE )

( 1.3.18.0.2.4.1126 NAME 'printer-pages-per-minute-color'
DESC 'The nominal number of color pages per minute which may be output by this
printer (e.g., a simplex or color printer).
This attribute is informative, NOT a service guarantee.
Typically, it is the value used in marketing literature to describe this printer.'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.27  SINGLE-VALUE )

( 1.3.18.0.2.4.1125 NAME 'printer-finishings-supported'
DESC 'The possible finishing operations supported by this printer.
Legal values include; "none", "staple", "punch", "cover", "bind", "saddle-stitch",
"edge-stitch", "staple-top-left", "staple-bottom-left", "staple-top-right",
"staple-bottom-right", "edge-stitch-left", "edge-stitch-top", "edge-stitch-right",
"edge-stitch-bottom", "staple-dual-left", "staple-dual-top", "staple-dual-right",
"staple-dual-bottom".'
EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{255} )

( 1.3.18.0.2.4.1124 NAME 'printer-number-up-supported'
DESC 'The possible numbers of print-stream pages to impose upon a single side of
an instance of a selected medium. Legal values include; 1, 2, and 4.
Implementations may support other values.'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.27 )

( 1.3.18.0.2.4.1123 NAME 'printer-sides-supported'
DESC 'The number of impression sides (one or two) and the two-sided impression
rotations supported by this printer.
Legal values include; "one-sided", "two-sided-long-edge", "two-sided-short-edge".'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1122 NAME 'printer-media-supported'
DESC 'The standard names/types/sizes (and optional color suffixes) of the media
supported by this printer.
For example: "iso-a4",  "envelope", or "na-letter-white".
```

```
Legal values  conform to ISO 10175, Document Printing Application (DPA), and any
IANA registered extensions.'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{255} )

( 1.3.18.0.2.4.1117 NAME 'printer-media-local-supported'
DESC 'Site-specific names of media supported by this printer, in the language in
"printer-natural-language-configured".
For example: "purchasing-form" (site-specific name) as opposed to
(in "printer-media-supported"): "na-letter" (standard keyword from ISO 10175).'
EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{255} )

( 1.3.18.0.2.4.1121 NAME 'printer-resolution-supported'
DESC 'List of resolutions supported for printing documents by this printer.
Each resolution value is a string with 3 fields:
1) Cross feed direction resolution (positive integer), 2) Feed direction
resolution (positive integer), 3) Resolution unit.
Legal values are "dpi" (dots per inch) and "dpcm" (dots per centimeter).
Each resolution field is delimited by ">".  For example:  "300> 300> dpi>".'
EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{255} )

( 1.3.18.0.2.4.1120 NAME 'printer-print-quality-supported'
DESC 'List of print qualities supported for printing documents on this printer.
For example: "draft, normal".  Legal values include; "unknown", "draft", "normal",
"high".'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1110 NAME 'printer-job-priority-supported'
DESC 'Indicates the number of job priority levels supported.
An IPP conformant printer which supports job priority must always support a
full range of priorities from "1" to "100"
(to ensure consistent behavior), therefore this attribute describes the
"granularity".
 Legal values of this attribute are from "1" to "100".'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.27  SINGLE-VALUE )

( 1.3.18.0.2.4.1118
NAME 'printer-copies-supported'
DESC 'The maximum number of copies of a document that may be printed as a single job.
A value of "0" indicates no maximum limit.
A value of "-1" indicates unknown.'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.27  SINGLE-VALUE )

( 1.3.18.0.2.4.1111
NAME 'printer-job-k-octets-supported'
DESC 'The maximum size in kilobytes (1,024 octets actually) incoming print job that
this printer will accept.
A value of "0" indicates no maximum limit.  A value of "-1" indicates unknown.'
EQUALITY integerMatch
```

```
ORDERING integerOrderingMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.27  SINGLE-VALUE )

( 1.3.18.0.2.4.1113
NAME 'printer-service-person'
DESC 'The name of the current human service person responsible for servicing this
printer.
It is suggested that this string include information that would enable other humans
to reach the service person, such as a phone number.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127}
SINGLE-VALUE )

( 1.3.18.0.2.4.1114
NAME 'printer-delivery-orientation-supported'
DESC 'The possible delivery orientations of pages as they are printed and ejected
from this printer.
Legal values include; "unknown", "face-up", and "face-down".'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1115
NAME 'printer-stacking-order-supported'
DESC 'The possible stacking order of pages as they are printed and ejected from
this printer.
Legal values include; "unknown", "first-to-last", "last-to-first".'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1116
NAME 'printer-output-features-supported'
DESC 'The possible output features supported by this printer.
Legal values include; "unknown", "bursting", "decollating", "page-collating",
"offset-stacking".'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1108
NAME 'printer-aliases'
DESC 'Site-specific administrative names of this printer in addition the printer
name specified for printer-name.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.6.1.4.1.42.2.27.5.1.63
NAME 'sun-printer-bsdaddr'
DESC 'Sets the server, print queue destination name and whether the client generates
protocol extensions.
"Solaris" specifies a Solaris print server extension. The value is represented b the
following value: server "," destination ", Solaris".'
SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.64
NAME 'sun-printer-kvp'
```

```
DESC 'This attribute contains a set of key value pairs which may have meaning to the
print subsystem or may be user defined.
Each value is represented by the following: key "=" value.'
SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

Internet Print Protocol ObjectClass

```
objectclasses: ( 1.3.18.0.2.6.2549
NAME 'slpService'
DESC 'DUMMY definition'
SUP 'top' MUST (objectclass) MAY ())

objectclasses: ( 1.3.18.0.2.6.254
NAME 'slpServicePrinter'
DESC 'Service Location Protocol (SLP) information.'
AUXILIARY SUP 'slpService')

objectclasses: ( 1.3.18.0.2.6.258
NAME 'printerAbstract'
DESC 'Printer related information.'
ABSTRACT SUP 'top' MAY ( printer-name
$ printer-natural-language-configured
$ printer-location
$ printer-info
$ printer-more-info
$ printer-make-and-model
$ printer-multiple-document-jobs-supported
$ printer-charset-configured
$ printer-charset-supported
$ printer-generated-natural-language-supported
$ printer-document-format-supported
$ printer-color-supported
$ printer-compression-supported
$ printer-pages-per-minute
$ printer-pages-per-minute-color
$ printer-finishings-supported
$ printer-number-up-supported
$ printer-sides-supported
$ printer-media-supported
$ printer-media-local-supported
$ printer-resolution-supported
$ printer-print-quality-supported
$ printer-job-priority-supported
$ printer-copies-supported
$ printer-job-k-octets-supported
$ printer-current-operator
$ printer-service-person
$ printer-delivery-orientation-supported
$ printer-stacking-order-supported $ printer! -output-features-supported ))

objectclasses: ( 1.3.18.0.2.6.255
NAME 'printerService'
DESC 'Printer information.'
STRUCTURAL SUP 'printerAbstract' MAY ( printer-uri
$ printer-xri-supported ))
```

```
objectclasses: ( 1.3.18.0.2.6.257
NAME ’printerServiceAuxClass’
DESC ’Printer information.’
AUXILIARY SUP ’printerAbstract’ MAY ( printer-uri $ printer-xri-supported ))

objectclasses: ( 1.3.18.0.2.6.256
NAME ’printerIPP’
DESC ’Internet Printing Protocol (IPP) information.’
AUXILIARY SUP ’top’ MAY   ( printer-ipp-versions-supported $
printer-multiple-document-jobs-supported ))

objectclasses: ( 1.3.18.0.2.6.253
NAME ’printerLPR’
DESC ’LPR information.’
AUXILIARY SUP ’top’ MUST ( printer-name ) MAY ( printer-aliases))

objectclasses: ( 1.3.6.1.4.1.42.2.27.5.2.14
NAME ’sunPrinter’
DESC ’Sun printer information’
SUP ’top’ AUXILIARY MUST (objectclass $ printer-name)  MAY
(sun-printer-bsdaddr $ sun-printer-kvp))
```

プリンタ属性

```
ATTRIBUTE ( 1.3.6.1.4.1.42.2.27.5.1.63
NAME sun-printer-bsdaddr
DESC ’Sets the server, print queue destination name and whether the
     client generates protocol extensions. "Solaris" specifies a
     Solaris print server extension.  The value is represented by
     the following value: server "," destination ", Solaris".’
EQUALITY caseIgnoreIA5Match
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
)


ATTRIBUTE ( 1.3.6.1.4.1.42.2.27.5.1.64
NAME sun-printer-kvp
DESC ’This attribute contains a set of key value pairs which may have
      meaning to the print subsystem or may be user defined.  Each
      value is represented by the following: key "=" value.’
EQUALITY caseIgnoreIA5Match
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15  )
```

Sun プリンタ ObjectClass

```
OBJECTCLASS ( 1.3.6.1.4.1.42.2.27.5.2.14
NAME sunPrinter
DESC ’Sun printer information’
SUP  top
AUXILIARY
MUST ( printer-name )
MAY  ( sun-printer-bsdaddr $ sun-printer-kvp ))
```

LDAP 用の汎用ディレクトリサーバーの要件

LDAP クライアントをサポートするには、すべてのサーバーが LDAP v3 プロトコルと複合ネーミングおよび補助オブジェクトクラスをサポートしている必要があります。また、次の制御を 1 つ以上サポートする必要があります。

- 単純ページモード (RFC 2696)
- 仮想リスト表示制御

  サーバーは、次の認証方式を 1 つ以上サポートする必要があります。

```
anonymous
simple
sasl/cram-MD5
sasl/digest-MD5
sasl/GSSAPI
```

LDAP クライアントが `pam_unix_*` モジュールを使用している場合、サーバーは UNIX crypt 形式でのパスワードの格納をサポートしている必要があります。

LDAP クライアントが TLS を使用している場合、サーバーは SSL または TLS をサポートしている必要があります。

LDAP クライアントが `sasl/GSSAPI` を使用している場合、サーバーは SASL、GSSAPI、Kerberos 5 認証をサポートしている必要があります。ネットワーク上の GSS 暗号化のサポートは、オプションです。

LDAP ネームサービスで使用されるデフォルトフィルタ

SSD を使用して個々のサービスにパラメータを手動で指定しないと、デフォルトフィルタが使用されます。特定のサービスのデフォルトフィルタを表示するには、`-v` オプションを指定して `ldaplist` を実行してください。

次の例では、`filter=(&(objectclass=iphost)(cn=abcde)` によってデフォルトフィルタが定義されます。

```
database=hosts
filter=(&(objectclass=iphost)(cn=abcde)
user data=(&(%s) (cn=abcde))
```

`ldaplist` は、次のデフォルトフィルタのリストを生成します。ここで、`%s` は文字列を示し、`%d` は数値を示します。

```
hosts
(&(objectclass=iphost)(cn=%s))
--------------
```

```
passwd
(&(objectclass=posixaccount)(uid=%s))
--------------
services
(&(objectclass=ipservice)(cn=%s))
--------------
group
(&(objectclass=posixgroup)(cn=%s))
--------------
netgroup
(&(objectclass=nisnetgroup)(cn=%s))
--------------
networks
(&(objectclass=ipnetwork)(ipnetworknumber=%s))
--------------
netmasks
(&(objectclass=ipnetwork)(ipnetworknumber=%s))
--------------
rpc
(&(objectclass=oncrpc)(cn=%s))
--------------
protocols
(&(objectclass=ipprotocol)(cn=%s))
--------------
bootparams
(&(objectclass=bootableDevice)(cn=%s))
--------------
ethers
(&(objectclass=ieee802Device)(cn=%s))
--------------
publickey
(&(objectclass=niskeyobject)(cn=%s))
or
(&(objectclass=niskeyobject)(uidnumber=%d))
--------------
aliases
(&(objectclass=mailGroup)(cn=%s))
--------------
```

表 **14–4** getXbyY 呼び出しで使用される LDAP フィルタ

フィルタ	定義
bootparamByName	(&(objectClass=bootableDevice)(cn=%s))
etherByHost	(&(objectClass=ieee802Device)(cn=%s))
etherByEther	(&(objectClass=ieee802Device)(macAddress=%s))
groupByName	(&(objectClass=posixGroup)(cn=%s))
groupByGID	(&(objectClass=posixGroup)(gidNumber=%ld))
groupByMember	(&(objectClass=posixGroup)(memberUid=%s))
hostsByName	(&(objectClass=ipHost)(cn=%s))
hostsByAddr	(&(objectClass=ipHost)(ipHostNumber=%s))

表 14–4 getXbyY 呼び出しで使用される LDAP フィルタ (続き)

フィルタ	定義
keyByUID	(&(objectClass=nisKeyObject)(uidNumber=%s))
keyByHost	(&(objectClass=nisKeyObject)(cn=%s))
netByName	(&(objectClass=ipNetwork)(cn=%s))
netByAddr	(&(objectClass=ipNetwork)(ipNetworkNumber=%s))
nisgroupMember	(membernisnetgroup=%s)
maskByNet	(&(objectClass=ipNetwork)(ipNetworkNumber=%s))
printerByName	(& (objectClass=sunPrinter)(|(printer-name=%s)(printer-aliases=%s)))
projectByName	(&(objectClass=SolarisProject)(SolarisProjectName=%s))
projectByID	(&(objectClass=SolarisProject)(SolarisProjectID=%ld))
protoByName	(&(objectClass=ipProtocol)(cn=%s))
protoByNumber	(&(objectClass=ipProtocol)(ipProtocolNumber=%d))
passwordByName	(&(objectClass=posixAccount)(uid=%s))
passwordByNumber	(&(objectClass=posixAccount)(uidNumber=%ld))
rpcByName	(&(objectClass=oncRpc)(cn=%s))
rpcByNumber	(&(objectClass=oncRpc)(oncRpcNumber=%d))
serverByName	(&(objectClass=ipService)(cn=%s))
serverByPort	(&(objectClass=ipService)(ipServicePort=%ld))
serverByNameAndProto	(&(objectClass=ipService)(cn=%s)(ipServiceProtocol=%s))
specialByNameserver	(ipServiceProtocol=%s))
ByPortAndProto	(&(objectClass=shadowAccount)(uid=%s))
netgroupByTriple	(&(objectClass=nisNetGroup)(cn=%s))
netgroupByMember	(&(objectClass=nisNetGroup)(cn=%s))
authName	(&(objectClass=SolarisAuthAttr)(cn=%s))
auditUserByName	(&(objectClass=SolarisAuditUser)(uid=%s))
execByName	(&(objectClass=SolarisExecAttr)(cn=%s) (SolarisKernelSecurityPolicy=%s)(SolarisProfileType=%s))

表 14–4 getXbyY 呼び出しで使用される LDAP フィルタ (続き)

フィルタ	定義
execByPolicy	(&(objectClass=SolarisExecAttr)(SolarisProfileId=%s) (SolarisKernelSecurityPolicy=%s)(SolarisProfileType=%s))
profileByName	(&(objectClass=SolarisProfAttr)(cn=%s))
userByName	(&(objectClass=SolarisUserAttr)(uid=%s))

次の表に getent 属性フィルタの一覧を示します。

表 14–5 getent 属性フィルタ

フィルタ	定義
aliases	(objectClass=rfc822MailGroup)
auth_attr	(objectClass=SolarisAuthAttr)
audit_user	(objectClass=SolarisAuditUser)
exec_attr	(objectClass=SolarisExecAttr)
group	(objectClass=posixGroup)
hosts	(objectClass=ipHost)
networks	(objectClass=ipNetwork)
prof_attr	(objectClass=SolarisProfAttr)
protocols	(objectClass=ipProtocol)
passwd	(objectClass=posixAccount)
printers	(objectClass=sunPrinter)
rpc	(objectClass=oncRpc)
services	(objectClass=ipService)
shadow	(objectclass=shadowAccount)
project	(objectClass=SolarisProject)
usr_attr	(objectClass=SolarisUserAttr)

◆ ◆ ◆ 第 15 章

NIS から LDAP への移行 (タスク)

この章では、LDAP ディレクトリに格納されたネーム情報を使用する NIS クライアントの、サポートを有効にする方法について説明します。この章の手順に従うことで、NIS ネームサービスから LDAP ネームサービスへ移行できます。

LDAP への移行の利点を判定するには、133 ページの「LDAP ネームサービスとその他のネームサービスの比較」を参照してください。

この章の内容は次のとおりです。

NIS から LDAP への移行サービスの概要

NIS から LDAP への移行サービス (*N2L* サービス) は、NIS マスターサーバー上の既存の NIS デーモンを NIS から LDAP への移行用デーモンに置き換えます。また、N2L サービスでは、そのサーバー上に NIS から LDAP へのマッピングファイルも作成されます。マッピングファイルでは、NIS マップエントリと、LDAP での同等なディレクトリ情報ツリー (DIT) との間のマッピングを指定します。この移行を完了した NIS マスターサーバーは、「N2L サーバー」と呼ばれます。スレーブサーバーには、`NISLDAPmapping` ファイルはありません。したがって、引き続きそのまま動作します。スレーブサーバーのデータは、N2L サーバーから、通常の NIS マスターからと同様に、定期的に更新されます。

N2L サービスの動作は、ypserv および NISLDAPmapping 構成ファイルによって制御されます。スクリプト inityp2l は、これらの構成ファイルの作成を支援します。いったん N2L サーバーが確立されたあとは、構成ファイルを直接編集して N2L を管理できます。

N2L サービスは、次の操作をサポートします。

- LDAP ディレクトリ情報ツリー (DIT) 内に NIS マップをインポートする
- NIS の速度および拡張性を維持しつつ、クライアントから DIT 情報にアクセスする

あらゆるネームシステムで、1 つのソースの情報だけが正規のソースになります。従来の NIS では、正規の情報は NIS ソースです。N2L サービスを使用する場合、LDAP ディレクトリが正規のデータソースになります。このディレクトリは、第 9 章「LDAP ネームサービスの紹介 (概要)」で説明されているディレクトリ管理ツールを使用して管理されます。

NIS ソースは、緊急時のバックアップまたはバックアウト (LDAP に移行するのではなく、NIS の使用をやめる) にのみ使用します。N2L サービスを使用したあとは、NIS クライアントを段階的に廃止する必要があります。最終的には、すべての NIS クライアントを LDAP ネームサービスクライアントで置き換えるようにしてください。

以降のセクションでは、さらに概要情報を説明します。

- 239 ページの「NIS から LDAP への移行の対象読者」
- 239 ページの「NIS から LDAP への移行サービスを使用しない場合」
- 239 ページの「NIS から LDAP への移行サービスがユーザーに与える影響」
- 240 ページの「NIS から LDAP への移行に関する用語」
- 241 ページの「NIS から LDAP への移行コマンド、ファイル、およびマップ」
- 242 ページの「サポートされる標準マッピング」

NIS から LDAP への移行用ツールとサービス管理機能

NIS と LDAP のサービスはサービス管理機能によって管理されます。これらのサービスに関する有効化、無効化、再起動などの管理アクションは、svcadm コマンドを使用して実行できます。svcs コマンドを使用してサービスのステータスを照会できます。LDAP および NIS での SMF の使用の詳細については、190 ページの「LDAP とサービス管理機能」および80 ページの「NIS とサービス管理機能」を参照してください。SMF の概要については、『Oracle Solaris 11.1 でのサービスと障害の管理』の第 1 章「サービスの管理 (概要)」を参照してください。また、詳細については svcadm(1M) および svcs(1) のマニュアルページも参照してください。

NIS から LDAP への移行の対象読者

この章の手順を実行するには、NIS および LDAP の概念、用語、および ID を理解する必要があります。NIS および LDAP のネームサービスについての詳細は、このドキュメントの以降のセクションを参照してください。

- NIS の概要については、第 5 章「ネットワーク情報サービス (概要)」
- LDAP の概要については、第 9 章「LDAP ネームサービスの紹介 (概要)」

NIS から LDAP への移行サービスを使用しない場合

N2L サービスの目的は、NIS の使用から LDAP の使用への移行ツールとして機能することにあります。次の状況では、N2L サービスを使用しないでください。

- NIS と LDAP ネームサービスクライアント間でデータを共有する予定がない環境。

  このような環境では、N2L サーバーは、過度に複雑な NIS マスターサーバーとして機能します。

- NIS ソースファイルを変更するツール (`yppasswd` 以外のツール) で NIS マップを管理している環境。

  DIT マップから NIS ソースを再生成するタスクは、必ずしも正確ではないため、生成されたマップを手動で確認する必要があります。いったん N2L サービスを使用し始めたあとは、NIS ソースの再生成は NIS をバックアウトするため、または NIS に戻すためにだけ提供されます。

- NIS クライアントのない環境。

  このような環境では、LDAP ネームサービスクライアントとそれに対応するツールを使用してください。

NIS から LDAP への移行サービスがユーザーに与える影響

N2L サービスに関連したファイルを単純にインストールしても、NIS サーバーのデフォルトの動作は変更されません。インストール時に、サーバー上の NIS のマニュアルページの一部が変更され、N2L のヘルパースクリプト `inityp2l` および `ypmap2src` が追加されます。しかし、NIS サーバー上で `inityp2l` を実行したり、N2L 構成ファイルを手動で作成したりしないと、NIS コンポーネントは従来の NIS モードで起動し、通常通りに機能します。

`inityp2l` の実行後に、サーバーとクライアントの動作が少し変更されます。次の表に、NIS および LDAP のユーザータイプと、N2L サービスの配備後に各タイプのユーザーが注意しなければならない部分の説明を示します。

ユーザータイプ	N2L サービスの影響
NIS マスターサーバー管理者	NIS マスターサーバーは、N2L サーバーに変換される。NISLDAPmapping および ypserv 構成ファイルが、N2L サーバーにインストールされます。N2L サーバーの確立後は、LDAP コマンドを使用してネーム情報を管理できる
NIS スレーブサーバー管理者	N2L の変換後も、NIS スレーブサーバーは NIS を通常の方法で動作する。yppush が ypmake から呼び出されると、N2L サーバーは、更新された NIS マップをスレーブサーバーにプッシュします。ypmake(1M) のマニュアルページを参照してください。
NIS クライアント	NIS の読み取り動作は、従来の NIS と同様。LDAP ネームサービスクライアントが DIT 内の情報を変更すると、その情報が NIS マップにコピーされます。コピー操作は、構成可能なタイムアウトの期限が切れると完了する。このような動作は、クライアントが NIS スレーブサーバーに接続された場合の通常の NIS クライアントの動作と同じ
	N2L サーバーが読み取りのために LDAP サーバーにバインドできない場合、N2L サーバーはローカルにキャッシュされたコピーから情報を返す。また、N2L サーバーは内部サーバーエラーを返す場合もある。N2L サーバーの構成によって、どちらの方法で応答することも可能。詳細は、ypserv(1M) のマニュアルページを参照してください。
すべてのユーザー	NIS クライアントがパスワードの変更を要求すると、N2L マスターサーバーとネイティブの LDAP クライアントに変更がただちに反映される
	NIS クライアントでのパスワードの変更を試みて、LDAP サーバーが利用できない場合は、変更は拒絶され N2L サーバーは内部サーバーエラーを返す。この動作によって、キャッシュに誤った情報が書き込まれることを防止する

NIS から LDAP への移行に関する用語

N2L サービスの実装に関連する用語を次に示します。

表 15–1　N2L の移行の関連用語

用語	説明
N2L 構成ファイル	/var/yp/NISLDAPmapping および /var/yp/ypserv ファイル。ypserv デーモンが N2L モードでマスターサーバーを起動するために使用する。詳細は、NISLDAPmapping(4) および ypserv(4) のマニュアルページを参照
マップ	N2L サービスでは、「マップ」は、次の 2 とおりの意味で使用される。 ■ NIS が特定の種類の情報を格納するデータベースファイル ■ LDAP DIT との間の NIS 情報のマッピングプロセス
マッピング	LDAP DIT エントリとの間の NIS エントリの変換プロセス
マッピングファイル	NISLDAPmapping ファイル。NIS と LDAP のファイル間のエントリのマッピング方法を確立する
標準マップ	通常使用される NIS マップ。マッピングファイルへの手動修正が不要で、N2L サービスによってサポートされる。サポートされる標準マップのリストは、242 ページの「サポートされる標準マッピング」を参照

表 15–1 N2L の移行の関連用語 (続き)

用語	説明
非標準マップ	標準の NIS マップであるが、RFC 2307 やその後継で指定されたマッピング以外の、NIS と LDAP DIT 間のマッピングを使用するようにカスタマイズされたマップ
カスタムマップ	標準のマップではないマップ。したがって、NIS から LDAP への移行時にはマッピングファイルの手動修正が必要
LDAP クライアント	従来の LDAP クライアント。LDAP サーバーとの間で読み書きを行う。従来の LDAP クライアントは、任意の LDAP サーバーに対して読み取りおよび書き込みを行うシステム。LDAP ネームサービスクライアントは、ネーミング情報のカスタマイズされたサブセットを処理します。
LDAP ネームサービスクライアント	ネーミング情報のカスタマイズされたサブセットを処理する LDAP クライアント。
N2L サーバー	N2L サービスを使用して、N2L サーバーとして再構成された NIS マスターサーバー。再構成には、NIS デーモンの置き換えと新しい構成ファイルの追加が含まれる。

NIS から LDAP への移行コマンド、ファイル、およびマップ

N2L の移行に関連して 2 つのユーティリティー、2 つの構成ファイル、および 1 つのマッピングがあります。

表 15–2 N2L のコマンド、ファイル、およびマップの説明

コマンド/ファイル/マップ	説明
`/usr/lib/netsvc/yp/inityp2l`	`NISLDAPmapping` および `ypserv` 構成ファイルの作成を支援するユーティリティー。このユーティリティーは、これらのファイルを管理するための汎用ツールではない。熟練したユーザーであれば、`inityp2l` の出力をテキストエディタを使って検証したりカスタマイズしたりすることで、N2L 構成ファイルの管理や、カスタムマッピングの作成を行うことも可能。`inityp2l(1M)` のマニュアルページを参照してください。
`/usr/lib/netsvc/yp/ypmap2src`	標準の NIS マップをほぼ同等の NIS ソースファイルに変換するユーティリティー。`ypmap2src` の主要な用途は、N2L の移行サーバーから従来の NIS への変換。`ypmap2src(1M)` のマニュアルページを参照してください。
`/var/yp/NISLDAPmapping`	NIS マップエントリと、LDAP 内の同等のディレクトリ情報ツリー (DIT) エントリの間のマッピングを指定する構成ファイル。`NISLDAPmapping(4)` のマニュアルページを参照してください。
`/var/yp/ypserv`	NIS から LDAP への移行用デーモンの構成情報を指定するファイル。`ypserv(4)` のマニュアルページを参照してください。
`ageing.byname`	NIS から LDAP への移行の実行時に、DIT でのパスワード有効期限情報の読み取りおよび書き込みのために `yppasswdd` によって使用されるマッピング

サポートされる標準マッピング

デフォルトでは、N2L サービスは、次のマップの一覧と RFC 2307、RFC 2307bis、およびその後継の LDAP エントリの間のマッピングをサポートしています。これらの標準マップでは、マッピングファイルへの手動修正は不要です。システム上で次のリストにないマップは、カスタムマップと見なされ、マッピングファイルの手動修正が必要です。

N2L サービスはまた、`auto.*` マップの自動マッピングもサポートしています。ただし、ほとんどの `auto.*` ファイル名とそのコンテンツは、各ネットワーク構成に固有なので、このリストではこれらのファイルは指定していません。この例外として、標準マップとしてサポートされる `auto.home` および `auto.master` マップがあります。

```
audit_user
auth_attr
auto.home
auto.master
bootparams
ethers.byaddr ethers.byname
exec_attr
group.bygid group.byname group.adjunct.byname
hosts.byaddr hosts.byname
ipnodes.byaddr ipnodes.byname
mail.byaddr mail.aliases
netgroup netgroup.byprojid netgroup.byuser netgroup.byhost
netid.byname
netmasks.byaddr
networks.byaddr networks.byname
passwd.byname passwd.byuid passwd.adjunct.byname
prof_attr
project.byname project.byprojectid
protocols.byname protocols.bynumber
publickey.byname
rpc.bynumber
services.byname services.byservicename
timezone.byname
user_attr
```

NIS から LDAP への移行時に、`yppasswdd` デーモンは、N2L 固有のマップ `ageing.byname` を使用して、 DIT でのパスワード有効期限情報の読み取りと書き込みを行います。パスワード有効期限を使用していない場合は、`ageing.byname` マッピングは無視されます。

NIS から LDAP への移行 (タスクマップ)

次の表に、NIS から LDAP への標準およびカスタムのマッピングで N2L サービスをインストールして管理するために必要な手順を示します。

タスク	説明	説明
すべての前提条件を完了します。	NIS サーバーと Oracle Directory Server Enterprise Edition (LDAP サーバー) を正しく構成すること	243 ページの「NIS から LDAP への移行のための前提条件」
N2L サービスの設定	NIS マスターサーバーで、`inityp2l` を実行して、次のいずれかのマッピングを設定する	
	標準マッピング	245 ページの「標準マッピングを使用して N2L サービスを設定する方法」
	カスタムまたは非標準マッピング	247 ページの「カスタムマッピングまたは非標準マッピングを使用して N2L サービスを設定する方法」
マップのカスタマイズ	N2L の移行のためのカスタムマップの作成方法の例を参照する	249 ページの「カスタムマップの例」
N2L のための Oracle Directory Server Enterprise Edition の構成	N2L 移行のための、LDAP サーバーとして Oracle Directory Server Enterprise Edition を構成し調整する	251 ページの「Oracle Directory Server Enterprise Edition を使用した NIS から LDAP への移行の最良の実践原則」
システムをトラブルシューティングします。	一般的な N2L の問題を特定し解決する	254 ページの「NIS から LDAP への移行のトラブルシューティング」
NIS に戻す方法	次のいずれか適切なマップを使用して NIS に戻す	
	以前の NIS ソースファイルに基づくマップ	260 ページの「以前のソースファイルに基づくマップに戻す方法」
	現在の DIT に基づくマップ	260 ページの「現在の DIT 内容に基づくマップに戻す方法」

NIS から LDAP への移行のための前提条件

N2L サービスを実装する前に、次の項目を確認または完了する必要があります。

- `inityp2l` スクリプトを実行して N2L モードを有効にする前に、システムが従来の NIS サーバーで動作するように設定されていること
- システムで LDAP ディレクトリサーバーを構成していること

NIS から LDAP への移行ツールでは、Oracle Directory Server Enterprise Edition と、Oracle から提供される互換性のあるバージョンのディレクトリサーバーがサポートされています。Oracle Directory Server Enterprise Edition を使用する場合は、N2L サービスを設定する前に、`idsconfig` コマンドを使用してサーバーを構成します。`idsconfig` についての詳細は、第 11 章「LDAP クライアントと Oracle Directory Server Enterprise Edition の設定 (タスク)」および `idsconfig(1M)` のマニュアルページを参照してください。

その他の (サードパーティー製) LDAP サーバーも N2L サービスで動作する可能性がありますが、Oracle ではサポートされません。Oracle Directory Server Enterprise Edition または互換性のある Oracle サーバー以外の LDAP サーバーを使用している場合は、N2L サービスを設定する前に、RFC 2307bis、RFC 4876、またはその後継のスキーマをサポートするようにサーバーを手動で構成する必要があります。

- `config/host` プロパティーでは、`dns` の前に `files` を使用します。
- N2L マスターサーバーと LDAP サーバーのアドレスが N2L マスターサーバー上の `hosts` ファイル内に存在することを確認してください。

  代わりに、`ypserv` 内にホスト名ではなく、LDAP サーバーアドレスをリストする方法もあります。このことは、LDAP サーバーのアドレスが別の場所にもリストされていることを意味しています。したがって、LDAP サーバーと N2L マスターサーバーのどちらかのアドレスを変更するには、別のファイルの修正も必要です。

NIS から LDAP への移行サービスの設定

次の 2 つの手順に示すように、標準のマッピングとカスタムマッピングのどちらかを使用して、N2L サービスを設定できます。

NIS から LDAP への変換の一部として、`inityp2l` コマンドを実行する必要があります。このコマンドは、対話型で、構成情報を入力するスクリプトを実行します。次のリストに、構成に必要な情報の種類を示します。これらの属性の説明については、`ypserv(1M)` のマニュアルページを参照してください。

- 作成する構成ファイルの名前 (デフォルト = `/etc/default/ypserv`)
- LDAP の構成情報を格納する DN (デフォルト = `ypserv`)
- LDAP との間でデータをマッピングするための優先サーバーリスト
- LDAP との間でデータをマッピングするための認証方式
- LDAP との間でデータをマッピングするための TLS (Transport Layer Security)
- LDAP との間でデータを読み書きするためのプロキシのユーザーバインド DN
- LDAP との間でデータを読み書きするためのプロキシのユーザーパスワード
- LDAP バインド動作のタイムアウト値 (秒単位)
- LDAP 検索動作のタイムアウト値 (秒単位)

- LDAP 変更動作のタイムアウト値 (秒単位)
- LDAP 追加動作のタイムアウト値 (秒単位)
- LDAP 削除動作のタイムアウト値 (秒単位)
- LDAP サーバーでの検索動作の制限時間 (秒単位)
- LDAP サーバーでの検索動作の制限サイズ (バイト単位)
- N2L が LDAP 照会に従うかどうか
- LDAP 検索のエラー処理、検索試行回数、および各試行間のタイムアウト (秒単位)
- 格納のエラー処理、検索試行回数、および各試行間のタイムアウト (秒単位)
- マッピングファイル名
- `auto_direct` マップのマッピング情報を生成するかどうか

  スクリプトは、マッピングファイル内の適切な位置にカスタムマップについての情報を配置します。
- ネーミングコンテキスト
- パスワードの変更を有効にするかどうか
- 任意のマップのデフォルトの TTL 値を変更するかどうか

注 – `sasl/cram-md5` 認証は、Oracle Directory Server Enterprise Edition を含むほとんどの LDAP サーバーでサポートされていません。

▼ 標準マッピングを使用して N2L サービスを設定する方法

242 ページの「サポートされる標準マッピング」にリストされているマップを移行する場合は、この手順に従います。カスタムマップまたは非標準マップを使用している場合 は、247 ページの「カスタムマッピングまたは非標準マッピングを使用して N2L サービスを設定する方法」を参照してください。

LDAP サーバーの設定が終わったら、`inityp2l` スクリプトを実行して、プロンプトに従って構成情報を入力します。`inityp2l` は構成を行い、標準および `auto.*` マップのためのマッピングファイルを設定します。

1. **243 ページの「NIS から LDAP への移行のための前提条件」**にリストされた前提条件の手順を完了します。

2. **NIS** マスターサーバー上の管理者になります。

   詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

3 **NIS マスターサーバーを N2L サーバーに変換します。**

```
# inityp2l
```

NIS マスターサーバーで `inityp2l` スクリプトを実行して、プロンプトに従います。指定が必要な情報のリストは、244 ページの「NIS から LDAP への移行サービスの設定」を参照してください。

詳細は、`inityp2l(1M)` のマニュアルページを参照してください。

4 **LDAP ディレクトリ情報ツリー (DIT) が完全に初期化されているかどうかを判定します。**

`NISLDAPmapping` ファイルにリストされたすべてのマップの配備に必要な情報がすでに DIT 内に存在する場合、DIT は完全に初期化されています。

- 初期化されていない場合は、手順 5 に進み、手順 6 をスキップします。
- 初期化されている場合は、手順 5 をスキップして 手順 6 に進みます。

5 **NIS ソースファイルから移行するため、DIT を初期化します。**

この手順は、DIT が完全に初期化されていない場合にのみ実行します。

a. **以前の NIS マップが最新の状態になっていることを確認してください。**

```
# cd /var/yp
# make
```

詳細については、`ypmake(1M)` のマニュアルページを参照してください。

b. **NIS サービスを停止します。**

```
# svcadm disable network/nis/server:default
```

c. **以前のマップを DIT にコピーしてから、マップ用の N2L サポートを初期化します。**

```
# ypserv -IR
```

`ypserv` が終了するまで待ちます。

ヒント – 元の NIS `dbm` ファイルは上書きされません。必要に応じて、これらのファイルを回復できます。

---

d. **DNS および NIS サービスを起動して、これらのサービスが新しいマップを使用していることを確認します。**

```
# svcadm enable network/dns/client:default
# svcadm enable network/nis/server:default
```

これで、標準マップでの N2L サービスの設定を完了します。手順 6 を行う必要はありません。

6 **NIS マップを初期化します。**

DIT が完全に初期化され、手順 5 をスキップした場合に限って、次の手順を実行してください。

a. **NIS サービスを停止します。**

```
# svcadm disable network/nis/server:default
```

b. **DIT 内の情報に従って NIS マップを初期化します。**

```
# ypserv -r
```

ypserv が終了するまで待ちます。

ヒント – 元の NIS dbm ファイルは上書きされません。必要に応じて、これらのファイルを回復できます。

---

c. **DNS および NIS サービスを起動して、これらのサービスが新しいマップを使用していることを確認します。**

```
# svcadm enable network/dns/client:default
# svcadm enable network/nis/server:default
```

▼ カスタムマッピングまたは非標準マッピングを使用して N2L サービスを設定する方法

次の状況に適合する場合、この手順を実行してください。

- 242 ページの「サポートされる標準マッピング」にリストされていないマップがある
- RFC 2307 とは異なるマッピングで LDAP にマップしたい標準の NIS マップがある

1 **243 ページの「NIS から LDAP への移行のための前提条件」にリストされた前提条件の手順を完了します。**

2 **NIS マスターサーバー上の管理者になります。**

詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

役割には、認証と特権コマンドが含まれます。役割についての詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の第 9 章「役割に基づくアクセス制御の使用 (タスク)」を参照してください。

3 **NIS マスターサーバーを N2L サーバーに構成します。**

```
# inityp2l
```

NIS マスターサーバーで `inityp2l` スクリプトを実行して、プロンプトに従います。指定が必要な情報のリストは、244 ページの「NIS から LDAP への移行サービスの設定」を参照してください。

詳細は、`inityp2l(1M)` のマニュアルページを参照してください。

4 **`/var/yp/NISLDAPmapping` ファイルを変更します。**

マッピングファイルの修正方法の例は、249 ページの「カスタムマップの例」を参照してください。

5 **LDAP ディレクトリ情報ツリー (DIT) が完全に初期化されているかどうかを判定します。**

`NISLDAPmapping` ファイルにリストされたすべてのマップの配備に必要な情報がすでに DIT 内に存在する場合、DIT は完全に初期化されています。

- 初期化されていない場合、手順 6、手順 8、および手順 9 を完了します。
- 初期化されている場合、手順 6 をスキップして、手順 7、手順 8、および手順 9 を完了します。

6 **NIS ソースファイルから移行するため、DIT を初期化します。**

a. **以前の NIS マップが最新の状態になっていることを確認してください。**

```
# cd /var/yp
# make
```

詳細については、`ypmake(1M)` のマニュアルページを参照してください。

b. **NIS デーモンを停止します。**

```
# svcadm disable network/nis/server:default
```

c. **以前のマップを DIT にコピーしてから、マップ用の N2L サポートを初期化します。**

```
# ypserv -Ir
```

`ypserv` が終了するまで待ちます。

ヒント – 元の NIS `dbm` ファイルは上書きされません。必要に応じて、これらのファイルを回復できます。

---

d. **DNS および NIS サービスを起動して、これらのサービスが新しいマップを使用していることを確認します。**

```
# svcadm enable network/dns/client:default
# svcadm enable network/nis/server:default
```

e. **手順 7 をスキップして、手順 8 から続行します。**

7 **NIS マップを初期化します。**

DIT が完全に初期化されている場合に限って、この手順を実行します。

a. **NIS デーモンを停止します。**

```
# svcadm disable network/nis/server:default
```

b. **DIT 内の情報に従って NIS マップを初期化します。**

```
# ypserv -r
```

ypserv が終了するまで待ちます。

ヒント – 元の NIS dbm ファイルは上書きされません。必要に応じて、これらのファイルを回復できます。

---

c. **DNS および NIS サービスを起動して、これらのサービスが新しいマップを使用していることを確認します。**

```
# svcadm enable network/dns/client:default
# svcadm enable network/nis/server:default
```

8 **LDAP エントリが正しいことを確認します。**

エントリが間違っている場合、LDAP ネームサービスクライアントからはそのエントリを見つけられません。

```
# ldapsearch -h server -s sub -b "ou=servdates, dc=..." \ "objectclass=servDates"
```

9 **LDAP_ マップの内容を確認します。**

次の出力例は、makedm コマンドを使用して hosts.byaddr マップの内容を確認する方法を示しています。

```
# makedbm -u LDAP_servdate.bynumber
plato: 1/3/2001
johnson: 2/4/2003,1/3/2001
yeats: 4/4/2002
poe: 3/3/2002,3/4/2000
```

出力結果が期待どおりの内容であれば、NIS から LDAP への移行は成功です。

元の NIS dbm ファイルは上書きされないことに注意してください。したがって、いつでもこれらのファイルは回復できます。詳細については、259 ページの「NIS に戻す方法」を参照してください。

カスタムマップの例

次の 2 つの例に、マップをカスタマイズする方法を示します。必要に応じて、任意のテキストエディタを使用して /var/yp/NISLDAPmapping ファイルを変更しま

す。ファイル属性と構文についての詳細は、NISLDAPmapping(4) のマニュアルページ、および第 9 章「LDAP ネームサービスの紹介 (概要)」にある LDAP ネームサービス情報を参照してください。

例 15–1 ホストエントリの移動

この例では、DIT でデフォルトの位置から別の (非標準の) 位置にホストエントリを移動する方法を示します。

NISLDAPmapping ファイル内の nisLDAPobjectDN 属性を新しいベース LDAP 識別名 (DN) に変更します。この例では、LDAP オブジェクトの内部構造は変更されません。したがって、objectClass エントリは変更されません。

変更前:

```
nisLDAPobjectDN hosts: \
                        ou=hosts,?one?, \
                        objectClass=device, \
                        objectClass=ipHost
```

変更後:

```
nisLDAPobjectDN hosts: \
                        ou=newHosts,?one?, \
                        objectClass=device, \
                        objectClass=ipHost
```

この変更によって、エントリは次のようにマッピングされます。

```
dn: ou=newHosts, dom=domain1, dc=sun, dc=com
```

元は、次のようでした。

```
dn: ou=hosts, dom=domain1, dc=sun, dc=com.
```

例 15–2 カスタムマップの実装

この例では、カスタムマップの実装方法を示します。

仮想のマップ「servdate.bynumber」には、システムのサービス日付についての情報が含まれます。このマップには、マシンのシリアル番号でインデックスが付けられます。この例では、123 です。各エントリは、マシンの所有者名、コロン、およびサービス日付のコンマ区切りのリストで構成されます。たとえば、John Smith:1/3/2001,4/5/2003 のようになります。

古いマップ構造は、次の形式の LDAP エントリにマップされます。

```
dn: number=123,ou=servdates,dc=... \
                number: 123 \
                userName: John Smith \
                date: 1/3/2001 \
```

例 15–2 カスタムマップの実装 (続き)

```
                date: 4/5/2003 \
                 .
                 .
                 .
                objectClass: servDates
```

NISLDAPmapping ファイルを調べることによって、必要なパターンにもっとも近いマッピングが group であることを確認できます。カスタムマッピングは group マッピングを参考にできます。マップは 1 つだけなので、nisLDAPdatabaseIdMapping 属性は不要です。NISLDAPmapping に追加される属性は、次のとおりです。

```
nisLDAPentryTtl servdate.bynumber:1800:5400:3600

nisLDAPnameFields servdate.bynumber: \
                        ("%s:%s", uname, dates)

nisLDAPobjectDN servdate.bynumber: \
                        ou=servdates, ?one? \
                        objectClass=servDates:

nisLDAPattributeFromField servdate.bynumber: \
                        dn=("number=%s,", rf_key), \
                        number=rf_key, \
                        userName=uname, \
                        (date)=(dates, ",")

nisLDAPfieldFromAttribute servdate.bynumber: \
                        rf_key=number, \
                        uname=userName, \
                        dates=("%s,", (date), ",")
```

Oracle Directory Server Enterprise Edition を使用した NIS から LDAP への移行の最良の実践原則

N2L サービスは Oracle Directory Server Enterprise Edition をサポートしています。その他のサードパーティー製 LDAP サーバーも N2L サービスで動作する可能性がありますが、Oracle ではサポートされません。Oracle Directory Server Enterprise Edition サーバーまたは互換性のある Oracle サーバー以外の LDAP サーバーを使用している場合は、RFC 2307、RFC 2307bis、および RFC 4876、またはその後継のスキーマをサポートするようにサーバーを手動で構成する必要があります。

Oracle Directory Server Enterprise Edition を使用すれば、ディレクトリサーバーを強化してパフォーマンスを改善できます。これらの強化を行うには、Oracle Directory Server Enterprise Edition 上に LDAP の管理者権限が必要です。また、ディレクトリサーバーのリブートが必要な場合もあります。リブートは、サーバーの LDAP クライアントとの間で調整が必要なタスクです。Oracle Directory Server Enterprise Edition のドキュメントは、Sun Java System Directory Server Enterprise Edition 6.2 の Web サイトで入手できます。

Oracle Directory Server Enterprise Edition を使用した仮想リスト表示インデックスの作成

大規模なマップでは、LDAP の仮想リスト表示 (VLV) インデックスを使用して、LDAP の検索から正しい結果が得られることを保証しなければなりません。Oracle Directory Server Enterprise Edition での VLV インデックスの設定についての詳細は、Sun Java System Directory Server Enterprise Edition 6.2 のドキュメントを参照してください。

VLV の検索結果では、固定ページサイズ 50000 を使用します。Oracle Directory Server Enterprise Edition で VLV を使用する場合は、LDAP サーバーと N2L サーバーの両方でこのサイズの転送を処理できるようにしてください。すべてのマップがこの制限より小規模であることが明らかな場合は、VLV インデックスを使用する必要はありません。ただし、マップがこのサイズ制限より大きい場合、またはすべてのマップのサイズが明確な場合以外には、VLV インデックスを使用して、結果が不完全となることを防止しなければなりません。

VLV インデックスを使用している場合は、次のように適切なサイズ制限を設定します。

- Oracle Directory Server Enterprise Edition では、 `nsslapd-sizelimit` 属性を 50000 以上、または `-1` に設定する必要があります。`idsconfig(1M)` のマニュアルページを参照してください。
- N2L サーバーでは、 `nisLDAPsearchSizelimit` 属性を 50000 以上、または 0 に設定する必要があります。詳細については、`NISLDAPmapping(4)` のマニュアルページを参照してください。

VLV インデックスが作成されたら、Oracle Directory Server Enterprise Edition サーバー上で `vlvindex` オプションを指定して `dsadm` を実行することによって、それらのインデックスを有効にします。詳細は、`dsadm`(1M) のマニュアルページを参照してください。

標準マップ用 VLV

次の状況に適合する場合、Oracle Directory Server Enterprise Edition の `idsconfig` コマンドを使用して、VLV を設定してください。

- Oracle Directory Server Enterprise Edition を使用している。
- 標準マップを RFC 2307bis LDAP エントリにマップしている。

VLV はドメイン固有です。よって、`idsconfig` を実行するたびに、1 つの NIS ドメインに VLV が作成されます。そのため、NIS から LDAP への移行中、`NISLDAPmapping` ファイルに含まれている各 `nisLDAPdomainContext` 属性に対して 1 回 `idsconfig` を実行する必要があります。

カスタムマップおよび非標準マップ用 VLV

次の状況に適合する場合、マップ用に新しい Oracle Directory Server Enterprise Edition の VLV を手動で作成するか、既存の VLV インデックスをコピーして修正しなければなりません。

- Oracle Directory Server Enterprise Edition を使用している場合
- 大規模なカスタムマップがあるか、非標準の DIT 位置にマップされる標準のマップがある場合

既存の VLV インデックスを表示するには、次のように入力します。

```
% ldapsearch -h hostname -s sub -b "cn=ldbm database,cn=plugins,cn=config" "objectclass=vlvSearch"
```

Oracle Directory Server Enterprise Edition によるサーバーのタイムアウトの防止

N2L サーバーがマップをリフレッシュすると、その結果、大規模な LDAP ディレクトリアクセスが行われる場合があります。Oracle Directory Server Enterprise Edition が正しく構成されていない場合、リフレッシュ動作は完了前にタイムアウトになることがあります。ディレクトリサーバーのタイムアウトを防止するには、次の Oracle Directory Server Enterprise Edition 属性を手動で、または `idsconfig` コマンドを実行することによって変更します。

たとえば、サーバーでの検索リクエストの実行にかかる最小時間を秒単位で増やすには、次の属性を修正します。

```
dn: cn=config
nsslapd-timelimit: -1
```

テストのためには、属性値として `-1` を使用できます。この値は、制限がないことを示しています。最適な制限値が決まったら、属性値を変更します。稼働サーバーに、`-1` の属性値が設定されていてはなりません。制限がないと、サーバーがサービス妨害攻撃に無防備になる場合があります。

LDAP での Oracle Directory Server Enterprise Edition の構成についての詳細は、このマニュアルの第 11 章「LDAP クライアントと Oracle Directory Server Enterprise Edition の設定 (タスク)」を参照してください。

Oracle Directory Server Enterprise Edition 使用時のバッファーオーバーランの防止

バッファーオーバーランを防止するには、Oracle Directory Server Enterprise Edition の属性を手動で修正するか、`idsconfig` コマンドを実行します。

1. たとえば、クライアント検索照会に返されるエントリの最大数を増やすには、次の属性を修正します。

```
dn: cn=config
nsslapd-sizelimit: -1
```

2. クライアント検索照会で確認されるエントリの最大数を増やすには、次の属性を修正します。

```
dn: cn=config, cn=ldbm database, cn=plugins, cn=config
nsslapd-lookthroughlimit: -1
```

テストのためには、属性値として -1 を使用できます。この値は、制限がないことを示しています。最適な制限値が決まったら、属性値を変更します。稼働サーバーに、-1 の属性値が設定されていてはなりません。制限がないと、サーバーがサービス妨害攻撃に無防備になる場合があります。

VLV が使用されている場合は、sizelimit 属性値を 252 ページの「Oracle Directory Server Enterprise Edition を使用した仮想リスト表示インデックスの作成」で定義されているように設定してください。VLV を使用していない場合、もっとも大きなコンテナを格納できるようにサイズ制限を設定する必要があります。

LDAP での Oracle Directory Server Enterprise Edition の構成についての詳細は、第 11 章「LDAP クライアントと Oracle Directory Server Enterprise Edition の設定 (タスク)」を参照してください。

NIS から LDAP への移行に関する制限

N2L サーバーの設定が完了すると、以降 NIS ソースファイルは使用されません。したがって、N2L サーバーで ypmake を実行しないでください。既存の cron ジョブの場合など、ypmake が誤って実行されても、N2L サービスは影響を受けません。ただし、yppush を明示的に呼び出すことを推奨する警告がログに記録されます。

NIS から LDAP への移行のトラブルシューティング

このセクションでは、トラブルシューティングの 2 つの領域を説明します。

よくある LDAP エラーメッセージ

N2L サーバーが LDAP 内部の問題に関連するエラーをログに記録して、LDAP 関連のエラーメッセージが表示される場合があります。エラーは致命的なものではありませんが、調査すべき問題を示しています。たとえば、N2L サーバーは動作を継続していても、返される結果が古かったり、不完全になる場合があります。

次のリストに、N2L サービスを実装するときに発生する可能性のある、よくある LDAP エラーメッセージをいくつか示します。エラーの説明、考えられる原因、およびエラーの対策も含みます。

`Administrative limit exceeded`

エラー番号: 11

原因: ディレクトリサーバーの `nsslapd-sizelimit` 属性で許可されているものより大きな LDAP 検索が実行されました。情報の一部だけが返されます。

対処方法: `nsslapd-sizelimit` 属性の値を増やすか、または失敗した検索のための VLV インデックスを実装します。

`Invalid DN Syntax`

エラー番号: 34

原因: 不正な文字を含む DN で LDAP エントリを書き込もうとする試みが行われました。N2L サーバーは、DN 内で生成される + 記号などの不正な文字のエスケープを試みます。

対処方法: LDAP サーバーのエラーログをチェックして、どの不正な DN が書き込まれたかを見つけたあと、不正な DN を生成した `NISLDAPmapping` ファイルを変更します。

`Object class violation`

エラー番号: 65

原因: 無効な LDAP エントリを書き込もうとする試みが行われました。一般に、このエラーは、次のいずれかの状況で起こる可能性のある `MUST` 属性の欠落のために発生します。

- 見つからない属性のエントリを作成する `NISLDAPmapping` ファイルのバグ
- 存在しないオブジェクトへの `AUXILIARY` 属性の追加の試み

  たとえば、ユーザー名がまだ `passwd.byxxx` マップから作成されていない場合、そのユーザーに対する補足情報の追加の試みは失敗します。

対処方法: `NISLDAPmapping` ファイル内のバグの場合は、サーバーのエラーログに書き込まれた内容をチェックして問題の本質を特定します。

`Can’t contact LDAP server`

エラー番号: 81

原因: `ypserv` ファイルが、間違った LDAP ディレクトリサーバーを指し示すように誤って構成されている可能性があります。または、ディレクトリサーバーが稼働していません。

対処方法: 再構成して確認します。

- ypserv ファイルを再構成して、正しい LDAP ディレクトリサーバーを指定します。
- LDAP サーバーが実行中であることを確認するには、次のように入力します。

```
% ping hostname 5 | grep "no answer" || \
      (ldapsearch -h hostname -s base -b ""  \
      "objectclass=*" >/dev/null && echo Directory accessible)
```

サーバーが使用できない場合は、「no answer from *hostname*」というメッセージが表示されます。LDAP サーバーに問題がある場合は、「ldap_search: Can't connect to the LDAP server - Connection refused」というメッセージが表示されます。最後に、すべてが動作している場合は、「 Directory accessible.」というメッセージが表示されます。

Timeout

エラー番号: 85

原因: LDAP 操作がタイムアウトしました。通常は、DIT からのマップの更新中に発生します。古い情報がマップに含まれている可能性があります。

対処方法: ypserv 構成ファイル内の nisLDAPxxxTimeout 属性の値を増やします。

NIS から LDAP への移行に関する問題

N2L サーバーの実行中に、次の問題が発生する場合があります。考えられる原因と対策を説明します。

NISLDAPmapping ファイルのデバッグ

マッピングファイル NISLDAPmapping は複雑なファイルです。多くの潜在的なエラーによって、マッピングが予期しない動作をする場合があります。次の方法を用いて、この問題を解決してください。

ypserv -ir (または -Ir) を実行するとコンソールメッセージが表示される

説明: コンソールに簡単なメッセージが表示され、サーバーが終了します (詳細な説明は syslog に書き込まれます)。

原因: マッピングファイルの構文が正しくない可能性があります。

対処方法: NISLDAPmapping ファイル内の構文をチェックして修正します。

起動時に NIS デーモンが終了する

説明: ypserv またはその他の NIS デーモンを実行すると、LDAP 関連のエラーメッセージがログに記録され、デーモンが終了します。

原因: 次のいずれかの原因が考えられます。

- LDAP サーバーと通信できない
- NIS マップまたは DIT 内のエントリが、指定されたマッピングと互換性がない
- LDAP サーバーへの読み書きの試みがエラーを返す

対処方法: LDAP サーバー上のエラーログを調べます。254 ページの「よくある LDAP エラーメッセージ」にリストされた LDAP エラーを参照してください。

`NIS` 動作からの予期しない結果
説明: NIS 操作が予期された結果を返しませんが、ログにエラーは記録されていません。

原因: LDAP または NIS マップ内に正しくないエントリが存在する可能性があります。これにより、マッピングが意図したように完了しません。

対処方法: LDAP DIT および N2L バージョンの NIS マップ内のエントリをチェックして修正します。

1. LDAP DIT に正しいエントリが存在するかをチェックしてから、必要に応じてエントリを修正します。

   Oracle Directory Server Enterprise Edition を使用している場合は、`dsadm startconsole` コマンドを実行することによって管理コンソールを起動します。
2. 新しく生成されたマップを元のマップと比較することによって、`/var/yp` ディレクトリ内の N2L バージョンの NIS マップに予期されたエントリが含まれていることを確認します。必要に応じてエントリを修正します。

   ```
   # cd /var/yp/domainname
   # makedbm -u test.byname
   # makedbm -u test.byname
   ```

   マップの出力をチェックする場合は、次のことに注意してください。
   - 両方のファイルでのエントリの順序が異なる可能性

     出力を比較する前に、`sort` コマンドを使用します。
   - 両方のファイルでの空白の使い方が異なる可能性

     出力を比較するときは `diff -b` コマンドを使用します。

`NIS` マップの処理順序
説明: オブジェクトクラス違反が発生しました。

原因: `ypserv -i` コマンドを実行すると、各 NIS マップが読み取られ、その内容が DIT に書き込まれます。複数のマップが、同一の DIT オブジェクトに属性を提供する場合もあります。一般に、1 つのマップによって、すべてのオブジェクトの `MUST` 属性を含むほとんどのオブジェクトが作成されます。ほかのマップは、ほかの `MAY` 属性を提供します。

マップは、`NISLDAPmapping` ファイル内で `nisLDAPobjectDN` 属性が現れるのと同じ順序で処理されます。`MAY` 属性を含むマップが `MUST` 属性を含むマップより先に処

理されると、オブジェクトクラス違反が発生します。このエラーについての詳細は、254 ページの「よくある LDAP エラーメッセージ」のエラー 65 を参照してください。

対処方法: マップが正しい順序で処理されるように、`nisLDAPobjectDN` 属性の順序を変更します。

一時的な解決として、`ypserv -i` コマンドを何回か再実行します。コマンドを実行するたびに、より多くの LDAP エントリが作られます。

注 – 1 つのマップからオブジェクトのすべての `MUST` 属性を作成できないマッピングはサポートされていません。

N2L サーバーのタイムアウトの問題

サーバーがタイムアウトします。

原因: N2L サーバーがマップをリフレッシュすると、その結果、大規模な LDAP ディレクトリアクセスが行われる場合があります。Oracle Directory Server Enterprise Edition が正しく構成されていない場合、この動作は完了前にタイムアウトになることがあります。

対処方法: ディレクトリサーバーのタイムアウトを防止するには、Oracle Directory Server Enterprise Edition 属性を手動で、または `idsconfig` コマンドを実行することによって変更します。詳細は、254 ページの「よくある LDAP エラーメッセージ」および251 ページの「Oracle Directory Server Enterprise Edition を使用した NIS から LDAP への移行の最良の実践原則」を参照してください。

N2L のロックファイルの問題

`ypserv` コマンドは起動しますが、`NIS` リクエストに対して応答しません。

原因: N2L サーバーのロックファイルが、NIS マップへのアクセスを正しく同期していません。このような状況が発生してはなりません。

対処方法: N2L サーバー上で次のコマンドを入力します。

```
# svcadm disable network/nis/server:default
# rm /var/run/yp_maplock /var/run/yp_mapupdate
# svcadm enable network/nis/server:default
```

N2L のデッドロックの問題

`N2L` サーバーがデッドロックします。

原因: N2L マスターサーバーと LDAP サーバーのアドレスが `hosts`、`ipnodes`、または `ypserv` ファイル内に正しくリストされていないと、デッドロックが発生する可

能性があります。N2L の正しいアドレス構成についての詳細は、243 ページの「NIS から LDAP への移行のための前提条件」を参照してください。

デッドロックの発生する例として、次の一連の事柄を考えてみてください。

1. NIS クライアントが IP アドレスの検索を試みます。
2. N2L サーバーが、`hosts` エントリは最新ではないことを検出します。
3. N2L サーバーが LDAP からの `hosts` エントリの更新を試みます。
4. N2L サーバーは、その LDAP サーバーの名前を `ypserv` から取得したあと、`libldap` を使用して検索を実行します。
5. `libldap` は、ネームサービススイッチを呼び出して、LDAP サーバー名の IP アドレスへの変換を試みます。
6. ネームサービススイッチの設定に基づき、N2L サーバーへの NIS 呼び出しを行い、デッドロックが発生します。

対処方法: N2L マスターサーバーと LDAP サーバーのアドレスを N2L マスターサーバー上の `hosts` または `ipnodes` ファイル内にリストします。サーバーアドレスを `hosts`、`ipnodes`、またはこの両方のファイル内にリストする必要があるかどうかは、これらのファイルがローカルホスト名を解決するためにどのように構成されているかによって異なります。また、`svc:/network/name-service/switch` サービスの `config/hosts` プロパティーの検索順序で、`files` が `nis` の前に指定されていることも確認してください。

このデッドロックの問題に対する別の方法として、`ypserv` ファイル内にホスト名ではなく、LDAP サーバーアドレスをリストする方法があります。これは、LDAP サーバーアドレスが別の場所に記述されていることを意味しています。したがって、LDAP サーバーと N2L サーバーのどちらかでアドレスを変更する場合には、さらに少し作業が必要になります。

NIS に戻す方法

N2L サービスを使用して NIS から LDAP に移行されたサイトでは、すべての NIS クライアントを LDAP ネームサービスクライアントに徐々に置き換えていくことが望まれます。最終的には、NIS クライアントに対するサポートは不要になります。ただし、必要に応じて、N2L サービスは、次の 2 つの手順に示すように、従来の NIS に復帰するための 2 種類の方法を提供します。

ヒント – 従来の NIS は、N2L バージョンの NIS マップが存在しても、それを無視します。NIS に戻したあとで、サーバー上の N2L バージョンのマップをそのままにしておいた場合でも問題を起こしません。したがって、あとで再度 N2L を有効にする場合に備えて、N2L マップを保管しておくことができます。ただし、マップの保管はディスクスペースを消費します。

▼ 以前のソースファイルに基づくマップに戻す方法

1 管理者になります。

詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2 **NIS** デーモンを停止します。

```
# svcadm disable network/nis/server:default
```

3 **N2L** を無効にします。

このコマンドは、N2L マッピングファイルをバックアップして、移動します。

```
# mv /var/yp/NISLDAPmapping backup_filename
```

4 **NOPUSH** 環境変数を設定して、**ypmake** によって新しいマップが転送されないようにします。

```
# NOPUSH=1
```

5 以前のソースに基づいて、**NIS** マップの新しいセットを作成します。

```
# cd /var/yp
# make
```

6 **(**オプション**) N2L** バージョンの **NIS** マップを削除します。

```
# rm /var/yp/domainname/LDAP_*
```

7 **DNS** および **NIS** サービスを起動します。

```
# svcadm enable network/dns/client:default
# svcadm enable network/nis/server:default
```

▼ 現在の DIT 内容に基づくマップに戻す方法

この手順を実行する前に、従来の NIS ソースファイルをバックアップします。

1 管理者になります。

詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2 **NIS** デーモンを停止します。

```
# svcadm disable network/nis/server:default
```

3 **DIT** に基づいてマップを更新します。

```
# ypserv -r
```

ypserv が終了するまで待ちます。

4 **N2L** を無効にします。

このコマンドは、N2L マッピングファイルをバックアップして、移動します。

```
# mv /var/yp/NISLDAPmapping backup_filename
```

5 **NIS** ソースファイルを再生成します。

```
# ypmap2src
```

6 再生成された **NIS** ソースファイルの内容と構造が正しいことを手動でチェックしてください。

7 再生成された **NIS** ソースファイルを適切なディレクトリに移動します。

8 **(**オプション**) N2L** バージョンのマッピングファイルを削除します。

```
# rm /var/yp/domainname/LDAP_*
```

9 **DNS** および **NIS** サービスを起動します。

```
# svcadm enable network/dns/client:default
# svcadm enable network/nis/server:default
```

用語集

baseDN DIT の一部のベースとなっている DN。これが NIS ドメインエントリの baseDN である場合は、コンテキストとも呼ばれる。

databaseID N2L サービスの場合、databaseID は、同じ形式の NIS エントリを含む (LDAP への同じマッピングを持つ) マップのグループの別名。これらのマップの鍵は異なっている可能性がある。

DBM NIS マップを格納するために当初使用されるデータベース。

DES 「データ暗号化規格 *(DES)*」の項を参照。

DIT 「ディレクトリ情報ツリー」の項を参照。

DN LDAP 内の識別名。ツリー構造を持つ LDAP ディレクトリのアドレススキーム。各 LDAP エントリに一意の名前を付与する。

DNS 「ドメインネームシステム *(DNS)*」の項を参照。

DNS ゾーン ネットワークドメイン内の管理境界であり、多くの場合は 1 つまたは複数のサブドメインで構成される。

DNS ゾーンファイル DNS ソフトウェアがドメイン内のすべてのワークステーションの名前と IP アドレスを格納する一連のファイル。

DNS 転送 NIS サーバーは、自身で応答できないリクエストを DNS サーバーに転送する。

GID 「グループ *ID*」の項を参照。

IP インターネットプロトコル。インターネットプロトコル体系の「ネットワーク層」プロトコル。

IP アドレス ネットワーク内の各ホストを識別する一意の番号。

LDAP Lightweight Directory Access Protocol は、LDAP ネームサービスクライアントおよびサーバーが互いに通信するために使用する、標準の拡張可能なディレクトリアクセスプロトコル。

MIS 経営情報システム (またはサービス)。

N2L サーバー NIS-to-LDAP サーバー。N2L サービスを使用して、N2L サーバーとして再構成された NIS マスターサーバー。再構成には、NIS デーモンの置き換えと新しい構成ファイルの追加が含まれる。

NDBM DBM の改良されたバージョン。

NIS ネットワーク上のシステムおよびユーザーに関する重要な情報が収められている分散型ネットワーク情報サービス。NIS データベースは、「マスターサーバー」とすべての「スレーブサーバー」に格納されている。

NIS マップ 特定の種類の情報 (ネットワーク上のすべてのユーザーのパスワードエントリや、ネットワーク上のすべてのホストマシンの名前など) を保持する NIS によって使用されるファイル。NIS サービスの一部であるプログラムはこれらのマップを参照する。「*NIS*」の項も参照。

RDN 相対識別名。DN の一部。

RFC 2307 標準の NIS マップから DIT エントリへの情報のマッピングを指定した RFC。デフォルトでは、N2L サービスは、更新されたバージョン RFC 2307bis で指定されたマッピングを実装している。

RPC リモート手続き呼び出し (RPC)を参照。

SASL Simple Authentication and Security Layer (簡易認証セキュリティー層)。アプリケーション層プロトコルにおける認証およびセキュリティー層の意味上の取り決め。

searchTriple 特定の属性を検索する DIT 内の場所についての説明。searchTriple は、「ベース DN」、「スコープ」、および「フィルタ」で構成される。これは、RFC 2255 で定義された LDAP URL 形式の一部である。

Secure RPC パスワード Secure RPC プロトコルに必要なパスワード。非公開鍵の暗号化に使用される。このパスワードはユーザーのログインパスワードと同じでなければならない。

SSL SSL は Secure Sockets Layer プロトコルである。LDAP セキュアなどのアプリケーションプロトコルを作成するためのトランスポート層のセキュリティーメカニズムの総称。

TCP 「*Transport Control Protocol (TCP)*」の項を参照。

TCP/IP Transport Control Protocol/Interface Program の略語。このプロトコル群は、最初はインターネット用に開発された。インターネットプロトコル群とも呼ばれる。Oracle Solaris ネットワークは、デフォルトでは TCP/IP 上で動作する。

Transport Control Protocol (TCP) 信頼性の高い、コネクション型の全二重ストリームを提供する、インターネットプロトコル群内の主要なトランスポートプロトコル。配信には IP を使用する。「TCP/IP」の項を参照。

Transport Layer Security (TLS) TLS は、LDAP クライアントとディレクトリサーバーの間の通信をセキュリティー保護して、プライバシとデータの完全性の両方を提供する。TLS プロトコルは、Secure Sockets Layer (SSL) プロトコルのスーパーセットである。

X.500 開放型システム間相互接続 (OSI) 規格によって定義されたグローバルレベルのディレクトリサービス。LDAP の前身。

yp イエローページNIS コード内部で今も使用される NIS の古い名前。

アプリケーションレベルのネームサービス	ファイル、メール、印刷などのサービスを提供するアプリケーションに組み込まれているネームサービスのこと。アプリケーションレベルのネームサービスは、企業レベルのネームサービスの下に位置する。企業レベルのネームサービスが提供するコンテキストの中に、アプリケーションレベルのネームサービスのコンテキストを組み込むことができる。
暗号化	データのプライバシを保護するための手段。
暗号化鍵	「データ暗号化鍵」の項を参照。
インターネットアドレス	*TCP/IP*を使用してホストに割り当てられた 32 ビットアドレス。「ドット形式の *10* 進表記」の項を参照。
インデックス付き名前	テーブル内のエントリを識別するために使用される命名形式。
エントリ	データベーステーブル内の 1 行のデータ (DIT 内の LDAP 要素など)。
鍵 (暗号化)	鍵の管理および配布システムの一部として、ほかの鍵を暗号化および暗号化解除するために使用される鍵。「データ暗号化鍵」の項も参照。
鍵サーバー	非公開鍵を格納する、Oracle Solaris オペレーティング環境のプロセス。
企業レベルのネットワーク	「企業レベルの」ネットワークは、ケーブル、赤外線ビーム、または無線ブロードキャスト経由で通信する単一のローカルエリアネットワーク (LAN) である場合や、ケーブルまたは直接電話接続でリンクされた 2 つ以上の LAN のクラスタである場合がある。企業レベルのネットワーク内では、DNS や X.500/LDAP などのグローバルネームサービスを使用せずに、どのマシンからでも任意のマシンにアクセスできる。
逆解決	DNS ソフトウェアを使用して、ワークステーションの IP アドレスをワークステーション名に変換するプロセス。
クライアント	(1) クライアントは、ネームサーバーにネームサービスをリクエストする主体 (マシンまたはユーザー)。 (2) ファイルシステムのクライアントサーバーモデルでは、クライアントとは、計算パワーや大きな記憶容量などの計算サーバーのリソースにリモートアクセスするマシン。 (3) クライアントサーバーモデルでは、「サーバープロセス」からサービスにアクセスする「アプリケーション」がクライアント。このモデルでは、クライアントとサーバーは同じマシン上または別のマシン上で動作可能。
クライアントサーバーモデル	ネットワークサービスと、これらのサービスのモデルユーザープロセス (プログラム) を説明するための一般的な方法。たとえば、「ドメインネームシステム (DNS)」のネームサーバー/ネームリゾルバパラダイムなど。「クライアント」の項も参照。
グループ **ID**	ユーザーのデフォルトのグループを識別する番号。
グローバルネームサービス	グローバルネームサービスは、電話、衛星、またはその他の通信システムでリンクされているこれらの世界中の企業レベルのネットワークを識別 (名前付け) する。この世界中に相互接続されたネットワークの集合体がいわゆる「インターネット」である。グローバルネームサービスでは、ネットワーク名だけでなく、任意のネットワーク内の個々のマシンやユーザーも識別できる。

広域ネットワーク **(WAN)**	異なる地理的な場所に存在する複数のローカルエリアネットワーク (LAN) またはシステムを電話、光ファイバ、衛星などのリンクで接続するネットワーク。
公開鍵	数学的に生成された数値のペアの公開コンポーネントであり、非公開鍵と組み合わされると DES 鍵が生成される。この DES 鍵を使用すれば、情報のエンコードとデコードを行える。公開鍵は、すべてのユーザーとマシンが使用できる。どのユーザーやマシンにも、固有の公開鍵と非公開鍵が 1 対ある。
コンテキスト	N2L サービスの場合、コンテキストは、一般に NIS ドメインがその下でマップされるもの。「baseDN」の項も参照。
サーバー	(1) NIS、DNS、および LDAP では、ネットワークにネームサービスを提供するホストマシン。 (2) ファイルシステムの「クライアントサーバーモデル」では、サーバーとは計算リソース (計算サーバーとも呼ばれる) と大きな記憶容量を備えたマシン。クライアントマシンはリモートアクセスが可能であり、これらのリソースを使用できる。ウィンドウシステムのクライアントサーバーモデルでは、サーバーとはアプリケーションまたは「クライアントプロセス」にウィンドウサービスを提供するプロセス。このモデルでは、クライアントとサーバーは同じマシン上または別のマシン上で動作可能。 (3) ファイルの提供を実際に処理するデーモン。
サーバーリスト	「優先サーバーリスト」の項を参照。
サブネット	ルーティングを単純化するために、1 つの論理ネットワークをより小さな物理ネットワークに分割する実際的なスキーム。
資格	クライアントソフトウェアが各リクエストとともにネームサーバーに送信する認証情報。この情報によって、ユーザーまたはマシンの ID が検査される。
識別名	識別名は、X.500 ディレクトリ情報ベース (DIB) 内のエントリであり、ルートから指定されたエントリまでつながるパスに沿った、ツリー内の各エントリから選択された属性で構成される。
スキーマ	任意の特定の LDAP DIT 内にどのような種類のデータを格納できるかを定義する一連の規則。
スレーブサーバー	NIS データベースのコピーを保持するサーバーシステム。このシステムには、ディスクと動作環境の完全なコピーが存在する。
接尾辞	LDAP では、DIT の識別名 (DN)。
ソース	NIS ソースファイル
属性	各 LDAP エントリは、いくつかの名前付き属性で構成され、各属性は 1 つまたは複数の値を持つ。 また、N2L サービスマッピングおよび構成ファイルもそれぞれ、いくつかの名前付き属性で構成される。各属性は 1 つまたは複数の値を持つ。

ディレクトリ	(1) LDAP ディレクトリは、LDAP オブジェクトのコンテナ。(2) UNIX では、ファイルまたはサブディレクトリのコンテナのこと。
ディレクトリキャッシュ	ディレクトリオブジェクトに関連付けられたデータを格納するために使用されるローカルファイル。
ディレクトリ情報ツリー	DIT は、特定のネットワークの分散型ディレクトリ構造です。デフォルトでは、クライアントは、DIT が特定の構造を持っていると想定して情報にアクセスする。LDAP サーバーがサポートするドメインごとに、想定された構造を持つ想定されたサブツリーがある。
データ暗号化鍵	暗号化を実行するプログラムを対象としたデータを暗号化および暗号化解除するために使用される鍵。「鍵 (暗号化)」の項も参照。
データ暗号化規格 **(DES)**	データを暗号化および復号化するための、アメリカ商務省標準局によって開発された一般的に使用されている高度なアルゴリズム。「SUN-DES-1」の項も参照。
ドット形式の **10** 進表記	32 ビット整数の構文表現であり、ピリオド (ドット) で区切られた 4 つの 10 進表記の 8 ビット数で構成される。192.67.67.20 のように、インターネットでの IP アドレスを表現するために使用される。
ドメイン	(1) インターネットでは、ネーミング階層の一部であり、通常はローカルエリアネットワーク (LAN)、広域ネットワーク (WAN)、またはこのようなネットワークの一部に対応する。構文上、インターネットドメイン名は小数点 (ドット) によって区切られた一連の名前 (ラベル) から構成される。たとえば、`sales.example.com` などがある。 (2) ISO の開放型システム間相互接続 (OSI) では、「ドメイン」は、MHS プライベート管理ドメイン (PRMD) やディレクトリ管理ドメイン (DMD) などのように、複雑な分散システムの管理パーティションとして使用されるのが普通。
ドメインネームサービス **(DNS)**	ドメイン名やマシン名を企業の外部のアドレス (インターネット上のアドレスなど) にマップするためネーミングポリシーおよびメカニズムを提供するサービス。すなわち DNS は、ドメイン名とマシン名をインターネットなどの企業外部のアドレスにマッピングする場合のネーミングポリシーとメカニズムを提供する。
ドメイン名	DNS 管理ファイルを共有するローカルネットワーク上のシステムのグループに割り当てられた名前。ネットワーク情報サービスのデータベースが正常に動作するためにはドメイン名が必要。「ドメイン」の項も参照。
名前解決	ワークステーション名またはユーザー名をアドレスに変換するプロセス。
名前空間	(1) 名前空間は、ユーザー、ワークステーション、およびアプリケーションがネットワーク全体にわたって通信する必要のある情報を格納する。 (2) ネーミングシステムで使用される名前セット。
認証	サーバーがクライアントの識別情報を検証できるようにするための手段。
ネームサーバー	1 つまたは複数のネットワークネームサービスを実行するサーバー。
ネームサービス	マシン、ユーザー、プリンタ、ドメイン、ルーター、その他のネットワーク名とアドレスを処理するネットワークサービス。

ネームサービススイッチ	ネームサービスクライアントが自身のネットワーク情報を取得できるソースを定義する `svc:/system/name-service/switch` サービス。
ネットワークパスワード	「Secure RPC パスワード」の項を参照。
ネットワークマスク	ローカルサブネットアドレスを特定のインターネットプロトコルアドレスの残りから分離するためにソフトウェアによって使用される数値。
非公開鍵	数学的に生成された数値のペアの非公開コンポーネントであり、非公開鍵と組み合わされると DES 鍵が生成される。この DES 鍵を使用すれば、情報のエンコードとデコードを行える。送信側の非公開鍵は、その鍵の所有者だけが使用できる。どのユーザーやマシンにも、固有の公開鍵と非公開鍵が 1 対ある。
フィールド	NIS マップエントリは、いくつかのコンポーネントと区切り文字で構成される可能性がある。N2L サービスマッピングプロセスの一部として、エントリはまず、いくつかの名前付きフィールドに分解される。
マスターサーバー	特定のドメインのネットワーク情報サービスデータベースのマスターコピーを保持するサーバー。名前空間に対する変更は、必ずマスターサーバーのネームサービスデータベース上で行う。ドメイン中に複数のマスターサーバーを作成できない。
マッピング	NIS エントリと DIT エントリの間の変換を行うプロセス。この処理は、「マッピング」ファイルにより制御される。
メール交換レコード	DNS ドメイン名とそれらに対応するメールホストの一覧が含まれているファイル。
メールホスト	サイトの電子メールのルーターおよび受信側として機能するワークステーション。
優先サーバーリスト	`client_info` テーブルまたは `client_info` ファイルのこと。優先サーバーリストには、あるクライアントマシンまたはドメインから見た優先サーバーが指定される。
リモート手続き呼び出し **(RPC)**	分散コンピューティングのクライアントサーバーモデルを実装するための容易で、一般的なパラダイム。与えられた引数を使用することによって、要求がリモートシステムに送信され、指定された手順が実行される。そのあと、その結果が呼び出し側に返される。
レコード	「エントリ」の項を参照。
ローカルエリアネットワーク **(LAN)**	データやソフトウェアの共有および交換の目的のためにまとまって接続されている、地理的に一か所に存在する複数のシステム。

索引

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X

Y