NIS+ への移行

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303
U.S.A. 650–960–1300

Part Number 806-2970–10
2000 年 3 月

原典: *NIS+ Transition Guide*

Part No: 806-2904-10

Revision A

Adobe PostScript

目次

はじめに

このマニュアルでは、ネットワーク情報サービス (NIS) のネームサービスを実行するサイトを、ネットワーク情報サービスプラス (NIS+) のネームサービスを実行するサイトに変換する方法を説明します。このマニュアルは、Solaris™ 8 システムおよびネットワーク管理マニュアルセットの一部です。

対象読者

このマニュアルは、NIS から NIS+ へ移行したいと考えているシステム管理者とネットワーク管理者を対象としています。NIS+ の初期設定と構成については、『*Solaris* ネーミングの設定と構成』を参照してください。NIS+ のカスタマイズと詳しい管理方法については、『*Solaris* ネーミングの管理』を参照してください。

このマニュアルでは、NIS+ に関連するネットワーク概念について紹介しますが、ネットワークの基礎や Solaris 環境が提供する管理ツールについては説明しません。このマニュアルでは、読者がすでに管理ツールの使用方法を知っていて、使いやすいツールも選択していることを仮定して説明を進めます。

内容の紹介

このマニュアルは、次の 6 つの章で構成されています。

第 1 章では、NIS と NIS+ の機能の違いと、推奨する移行方法の概要を説明します。

第 2 章では、NIS+ の名前空間を設計する方法を説明します。

第 3 章では、NIS+ のセキュリティ機能と、この機能が管理と移行の計画に与える影響について説明します。

第 4 章では、NIS クライアントと NIS+ クライアントを同時に使用する方法と、NIS+ サーバーを NIS 互換モードで使用する方法を説明します。

第 5 章では、実際に移行を始める前に必要な作業を示します。

第 6 章では、NIS から NIS+ へ移行するために必要なステップを示します。

関連マニュアル

NIS+ と DNS の詳細については、次のマニュアルを参考にしてください。

- 『*Solaris* ネーミングの設定と構成』- NIS+ 名前空間の計画、設定、構成の方法について説明しています。
- 『*Solaris* ネーミングの管理』 - NIS+ 名前空間の運用を管理する方法と、そのセキュリティレベルを変更する方法について説明しています。

Sun のマニュアルの注文方法

専門書を扱うインターネットの書店 Fatbrain.com から、米国 Sun Microsystems™, Inc. (以降、Sun™ とします) のマニュアルをご注文いただけます。

マニュアルのリストと注文方法については、`http://www1.fatbrain.com/documentation/sun` の Sun Documentation Center をご覧ください。

Sun のオンラインマニュアル

`http://docs.sun.com` では、Sun が提供しているオンラインマニュアルを参照することができます。マニュアルのタイトルや特定の主題などをキーワードとして、検索をおこなうこともできます。

表記上の規則

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

表 P–1 表記上の規則

字体または記号	意味	例
AaBbCc123	コマンド名、ファイル名、ディレクトリ名、画面上のコンピュータ出力、コード例を示します。	.login ファイルを編集します。 ls -a を使用してすべてのファイルを表示します。 system%
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。	system% **su** password:
AaBbCc123	変数を示します。実際に使用する特定の名前または値で置き換えます。	ファイルを削除するには、rm *filename* と入力します。
『 』	参照する書名を示します。	『コードマネージャ・ユーザーズガイド』を参照してください。
「 」	参照する章、節、ボタンやメニュー名、強調する単語を示します。	第 5 章「衝突の回避」を参照してください。 この操作ができるのは、「スーパーユーザー」だけです。
\	枠で囲まれたコード例で、テキストがページ行幅を超える場合に、継続を示します。	sun% **grep '^#define ** **XV_VERSION_STRING'**

ただし AnswerBook2™ では、ユーザーが入力する文字と画面上のコンピュータ出力は区別して表示されません。

コード例は次のように表示されます。

- C シェルプロンプト

```
system% command y|n [filename]
```

- Bourne シェルおよび Korn シェルのプロンプト

```
system$ command y|n [filename]
```

- スーパーユーザーのプロンプト

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

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

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

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

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

一般規則

- このマニュアルでは、英語環境での画面イメージを使っています。このため、実際に日本語環境で表示される画面イメージとこのマニュアルで使っている画面イメージが異なる場合があります。本文中で画面イメージを説明する場合には、日本語のメニュー、ボタン名などの項目名と英語の項目名が、適宜併記されています。
- このマニュアルでは、「IA」という用語は、Intel 32 ビットのプロセッサアーキテクチャを意味します。これには、Pentium、Pentium Pro、Pentium II、Pentium II Xeon、Celeron、Pentium III、Pentium III Xeon の各プロセッサ、および AMD、Cyrix が提供する互換マイクロプロセッサチップが含まれます。

第 1 章

概要

この章では、ネットワーク情報サービス (NIS) からネットワーク情報サービスプラス (NIS+) へ移行する場合の問題点について説明します。ここでは、2 つのネームサービスの違いについて説明し、推奨する移行方法の概要を示します。

NIS と NIS+ の相違

NIS と NIS+ の間には、移行に影響を与える相違点がいくつかあります。たとえば、NIS は、1 つのドメイン (またはいくつかの別々のドメイン) を持つ平坦な (階層型ではない) 名前空間を使用しますが、NIS+ は、DNS に似たドメイン階層を使用します。このため、NIS+ に変換する前に、NIS+ の名前空間を設計する必要があります。また、 NIS+ にはセキュリティを強化するための機能があります。これにより、名前空間内の情報だけでなく、名前空間の構造的な構成要素へのアクセスも制限されます。

このような相違点から、NIS+ が単に NIS をアップグレードしたものではなく、完全に新しい製品であることがわかります。NIS から NIS+ へ移行する際は、主にこれらの製品間の相違がポイントになります。

この章では、これらの相違点について、次に示す一般的な用語を使って説明します。NIS+ への移行を正しく行うには、これらの用語を理解することが重要です。

- ドメイン構造

- 相互運用性
- サーバーの構成
- 情報の管理
- セキュリティ

ドメインの構造

NIS+ は、NIS に置き換わるものとして設計されており、単に NIS をアップグレードしたものではありません。このことは、NIS+ のドメイン構造を調べると明らかです。NIS のドメインは平坦で、階層を持つことができません。これに対して、NIS+ のドメインは平坦な場合もありますが、階層構造のドメインを作成できます。この階層は、ルートドメインと、その下の任意の数のサブドメインから構成されます。

NIS のドメイン構造は、1980 年代に一般的であったクライアントとサーバー間のコンピューティングネットワークの管理の要件に対応したものでした。つまり、数百のクライアントと少数の多目的サーバーを持つ、クライアントとサーバー間のネットワークを対象としていました。

NIS+ は、世界中のサイトの専用サーバー 10～100 台によってサポートされるクライアント 100～10000 台をサポートするネットワークを対象としています。こうしたネットワークは、複数の「信頼性の低い」公衆ネットワークに接続されています。このようなネットワークの規模と構成を維持するには、新しい独立した管理方式が必要です。NIS+ のドメイン構造は、次の図に示すように、DNS のドメイン構造に似ています。

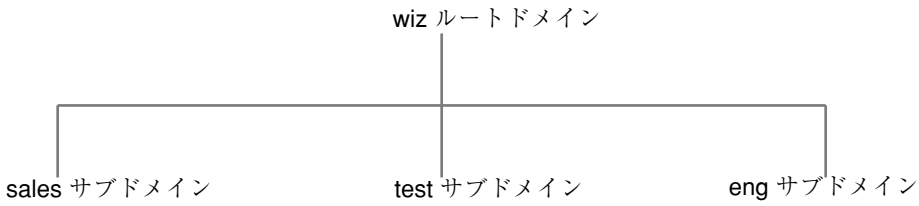

図 1–1　NIS+ のドメイン

ドメインを階層構造にすると、規模の小さいものから非常に大きいものまで、広い範囲のネットワークに NIS+ を使用することができます。また、NIS+ のサービスを

組織の成長に対応させることもできます。NIS+ ドメインの構造の詳細については、『*Solaris* ネーミングの管理』を参照してください。

DNS、NIS、NIS+ の相互運用性

NIS+ が提供する相互運用性とは、NIS からの移行と、NIS サービスによって提供されていた DNS とを継続して併用できることを意味します。 NIS+ には、NIS からの移行に役立つ NIS 互換モードと情報転送ユーティリティがあります。NIS 互換モードを使用すると、Solaris オペレーティング環境 のソフトウェアを実行する NIS+ サーバーは、NIS クライアントからの要求に応じる一方で、NIS+ クライアントからの要求にも引き続き応じることができます。また、管理者は、情報転送ユーティリティを使って NIS のマップと NIS+ のテーブルを同期させることができます。

NIS 互換モードの設定に必要な手順は、標準 NIS+ サーバーで使用する手順と若干異なります。また、NIS 互換モードは、NIS+ 名前空間内のテーブルとセキュリティ上の関連を持っています。手順の違いとセキュリティとの関連については、『*Solaris* ネーミングの設定と構成』、『*Solaris* ネーミングの管理』を参照してください。

NIS+ サーバーが NIS 互換モードで実行されている場合、NIS のクライアントコンピュータは、 NIS+ のクライアントコンピュータとは異なる方法で NIS+ 名前空間にアクセスします。次にこの違いを示します。

- NIS のクライアントマシンは、NIS+ のテーブルパスまたはリンクをたどることも、他のドメインのデータを読み取ることもできません。
- NIS+ サーバー上で `rpc.nisd` に `–Y -B` オプションを付けて実行している場合、NIS+ サーバー内で解決できない NIS のクライアントマシンからのホスト要求を DNS に転送することができます。しかし、NIS+ クライアントからのこのような要求は転送されません。NIS+ クライアントマシンの DNS 要求の転送は、`/etc/resolv.conf` ファイルと `/etc/nsswitch.conf` ファイルの構成によって制御されます。詳細については、『*Solaris* ネーミングの管理』を参照してください。
- 許可を持つ NIS+ の管理者は、`passwd` コマンドを使用して、パスワードの有効期限やロックの設定など、パスワードに関連するすべての管理業務を実行できます。NIS+ クライアントのユーザーは、`passwd` コマンドを使用して、自分自身のパスワードを変更できます。
- ローカルサブネット上のすべてのサーバーが応答しなくなった場合でも、NIS+ クライアントマシンは、そのドメインの複製サーバーのどれかと通信できれば、そのネームサービスの呼び出しに応答を得ることができます。NIS クライアント

マシンは、サーバー名が設定されていないと、そのサブネットの外部にあるネットワーク上の情報にアクセスすることができません。サーバー名は、`ypset` によって、または Solaris NIS クライアントの場合には `ypset` サブネットの外部にあるネットワーク上の情報にアクセスすることによって設定されます。

- NIS クライアントマシンは、受信中のデータが承認された NIS サーバーから送信されたものかどうかについては確認できません。これに対して、承認された NIS+ クライアントでは、承認された NIS+ サーバーからデータが送信されていることを確認できます。
- NIS 環境では、サーバーが応答しなくなったとき、NIS の `yp_match()` 呼び出しは、サーバーが応答して要求に応じるまで、呼び出しを試行し続けます。NIS+ の API (アプリケーションプログラムインタフェース) では、このような事態が発生すると、アプリケーションに対してエラーメッセージを返します。

Solaris 2.3 以降のリリースでは、NIS 互換モードで DNS 転送をサポートします。Solaris 2.2 では、DNS 転送を可能にする「パッチ (patch `#101022-06`)」が提供されています。DNS 転送を可能にするパッチは、Solaris 2.0 と 2.1 では利用できません。

NIS+ ドメインは、インターネットに直接接続することはできませんが、ネームサービススイッチによって、NIS+ クライアントマシンをインターネットに接続することはできます。クライアントは、そのスイッチ構成ファイル (`/etc/nsswitch.conf`) を設定して、NIS+ テーブルだけでなく、DNS ゾーンファイルや NIS マップの情報を検索することもできます。

サーバーの構成

NIS+ のクライアント サーバー構成は、各ドメインが複数のサーバーによってサポートされているという点で、NIS と DNS の構成に似ています。メインサーバーは「マスタサーバー」と呼ばれ、バックアップサーバーは「複製サーバー」と呼ばれます。マスタサーバーも複製サーバーも NIS+ サーバーソフトウェアを実行し、どちらも NIS+ テーブルを持ちます。

ただし、NIS+ では、NIS の場合とはまったく異なる方法でデータベースが更新されます。NIS が開発された時点では、NIS が格納する情報のほとんどが静的なものと想定されていました。したがって、NIS の変更は手作業で処理し、そのマップ内の情報が変更されるたびにマップを作成しなおし、すべてを伝達させる必要があります。

これに対して NIS+ では、複製サーバーに対して変更分だけの更新ができます。マスタサーバー上のマスタデータベースを変更する必要はありますが、変更内容は複

製サーバーにも自動的に伝達されます。「make」マップを再度作成したり、情報が伝達されるまで何時間も待つ必要はありません。伝達は、3 ～ 4 分で終了します。

情報の管理

NIS+ は、マップやゾーンファイルではなく、「テーブル」に情報を格納します。NIS+ には、図 1–2 に示すように、17 種類の定義済みテーブル (システムテーブル) があります。

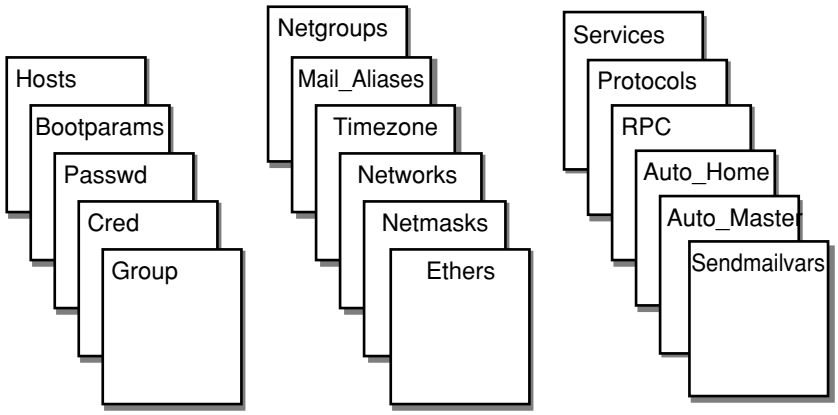

図 1–2　NIS+ の標準テーブル

NIS+ テーブルは ASCII ファイルではなく、NIS+ リレーショナルデータベース内のテーブルです。NIS+ テーブルの内容は、NIS+ のコマンドを使用しなければ表示または編集できません。

NIS+ テーブルには、NIS で使用したマップに比べて大きく改善された機能が 2 つあります。その 1 つは、NIS+ テーブルを、最初の列 (「キー」とも呼ぶ) だけでなく、任意の検索可能な列によって検索できるという機能です。特定の列が検索可能であるかどうかを知るには、テーブルに対して `niscat -o` コマンドを実行してください。コマンドは、そのテーブルの列と属性のリストを返します。この検索機能により、NIS によって使用される `hosts.byname` マップと `hosts.byaddr` マップのような重複するマップを持つ必要性がなくなります。もう 1 つは、NIS+ テーブル内の情報に対して、テーブルレベル、エントリ (行) レベル、列レベルという 3 つのレベルでアクセスを制御できることです。

NIS マップがサーバーのディレクトリ `/var/yp/`*domainname* に置かれるのに対して、NIS+ ディレクトリは `/var/nis/data` に置かれます。NIS+ テーブルはデータベースの中に格納されます。テーブルの情報は、データベースへの要求が出される

と、メモリーに読み込まれます。データを要求された順序でメモリーに保存すると、ディスクへのアクセスを最小限に抑えられるため、要求への応答時間を短縮することができます。

セキュリティ

NIS+ のセキュリティ機能は、名前空間の情報と名前空間そのものの構造を不正なアクセスから保護します。NIS+ のセキュリティ機能は、「認証」と「承認」という 2 つの手段によって行われます。認証とは、NIS+ サーバーが、特定の要求を送信した NIS+ の「主体」(クライアントユーザーまたはクライアントワークステーション) を識別する処理を指します。承認とは、サーバーが、その主体 (クライアントマシンまたはクライアントユーザー) に許可されたアクセス権を識別する処理を指します。

つまり、最高レベルの NIS+ セキュリティ機能がサイトに導入されている場合、名前空間内の情報にアクセスするには認証された NIS+ クライアントでなければならず、その情報にアクセスするための適切なアクセス権を持っていなければなりません。さらに、名前空間へのアクセス要求は、NIS+ のクライアントライブラリルーチンか NIS+ の管理コマンドによって行われた場合にだけ有効になります。また、NIS+ のテーブルと構造を直接編集することはできません。

推奨する移行手順

次に、NIS から NIS+ への移行において推奨する移行手順の概略を示します。

1. 基本的な移行の方針について確認します。
2. NIS+ について理解します。
3. 最終的な NIS+ 名前空間を設計します。
4. セキュリティの方式を選択します。
5. NIS 互換モードの使用方法を決定します。
6. 移行の準備を完了します。
7. 移行を実行します。

この章の以下の部分では、上記の手順の各段階について詳しく説明します。

移行の方針

移行を開始するにあたって、次に示す基本的な方針を確認してください。

移行をすぐに実行するのではなく、別の方法を考慮する

Solaris オペレーティング環境への移行を完全に終えるまで NIS+ へのアップグレードを先延ばしにすることにより、Solaris オペレーティング環境への移行中は移行作業だけに専念できます。NIS+ への移行準備ができるまでは、Solaris オペレーティング環境により、継続して NIS を実行することができます。

処理を簡略化する

いくつかの手順により、移行を簡略にすることができます。これらの手順を実行すると、NIS+ の効果は減少しますが、サーバーの台数は少なくて済み、管理に要する時間も減ります。移行が完了すれば、NIS+ の設定を変更して、サイトの要求に完全に適合させることができます。次にいくつかの推奨事項を示します。

- ドメイン名を変更しない
- 階層を使用しないで、平坦な NIS+ 名前空間を使用する
- NIS 互換機能を使用する
- デフォルトのテーブルとディレクトリ構造を使用する
- Solaris 2.5 以降のリリースを使用する場合は、クライアントの資格を設定しない

1 種類のソフトウェアリリースを使用する

移行に使用する Solaris オペレーティング環境のソフトウェアと NIS+ のバージョンを決定します。各バージョン間には若干の違いがあるため、複数のバージョンを同時に使用すると、移行の処理が不必要に複雑になります。Solaris 製品の 1 バージョンだけを選択して、それに対応するバージョンの NIS+ を使用してください。

現在のリリースは、設定スクリプトなどのほとんどの機能を備えています。通常の操作に必要な Solaris 2.6 のパッチを用意し、すべてのサーバーとクライアントに同じパッチがインストールされていることを確認してください。

クライアントユーザーへの影響を最小限に抑える

クライアントユーザーに関して、考慮するべき点が 2 つあります。1 つは、ユーザーがサービスの変更に気が付かないようにするということです。もう 1 つは、移行作業そのものがユーザーに与える混乱を最小限に抑えるということです。2 番目のポイントについては、ユーザーに移行作業を要求するのではなく、必ず各ドメインの管理者がそのクライアントマシンの NIS+ への移行作業を行うようにすれば解決できます。これにより、正しい手順が実行され、その手順がクライアントマシン全体でも一貫して実行されます。したがって、問題があっても、管理者がただちに処理することができます。

禁止事項

- 現在 NIS によって提供されているネームサービス、または NIS の動作を変更しないこと
- DNS の構造を変更しないこと
- IP ネットワークの形態を変更しないこと
- NIS を使用するアプリケーションを NIS+ にアップグレードしないこと

  NIS+ API への移行は延期します。
- 移行作業の途中では、NIS+ への機能の追加を行わないこと

  機能追加は後で行なってください。

NIS+ について理解する

NIS+ に関する理解を深めておいてください。特に、この章の前半で要約した概念 (このマニュアルの後半で詳しく説明します) については、よく理解しておく必要があります。8ページの「関連マニュアル」でとりあげたマニュアルを参照してください。

NIS+ を理解するための最もよい方法の 1 つは、プロトタイプの名前空間を作成することです。製品を実際に経験するということに優る方法はありません。システム管理者には、業務に支障をきたさないテスト環境での練習が必要です。

注 - プロトタイプのドメインを、実際の NIS+ 名前空間としては使用しないでください。プロトタイプですべてを学んだら、そのプロトタイプは削除して、名前空間の構成上の問題が起こらないようにします。計画をすべて終えたら、新しく実際の名前空間を作成してください。

テストドメインを作成するときは、小規模の管理しやすいドメインを作成してください。テストドメインの作成については、『*Solaris* ネーミングの設定と構成』を参考にしてください。『*Solaris* ネーミングの設定と構成』では、NIS 互換モードを設定した状態、または設定しない状態で、NIS+ セットアップスクリプトを使用して簡単なテストドメインとサブドメインを計画して作成する方法について説明しています。

注 - NIS+ の名前空間を設定する場合、『*Solaris* ネーミングの設定と構成』の Part I で説明した NIS+ スクリプトの使用をお勧めします。この手順では、最初に NIS+ スクリプトを使用して、基本的な NIS+ 名前空間を設定します。続いて NIS+ コマンドセットを使用して、各自のニーズに合わせて名前空間をカスタマイズします。

最終的な NIS+ 名前空間を設計する

第 2 章の指針に従って、最終的な NIS+ 名前を設計します。名前空間の設計中は、NIS からの移行によって生じる制限を気にする必要はありません。これらの制約は、最終的な NIS+ の目的を明確にしてから変更することができます。

セキュリティの方式を選択する

NIS+ のセキュリティは、ユーザーと管理者にとって非常に有益ですが、ユーザーにも管理者にも、より詳しい知識と設定作業が必要になります。 また、計画上の決定をいくつか行う必要もあります。第 3 章では、NIS+ セキュリティの持つ意味と、NIS+ 名前空間でセキュリティを使用する場合に必要な決定事項について説明します。

NIS 互換モードの使用方法を決定する

移行の間は、NIS と NIS+ の名前空間を並行して使用することは事実上避けられません。2 つの名前空間を同時に使用するには、さらに資源を追加する必要があるため、各サイトが二重のサービスを使用する時間、または名前空間内の二重サービスの適用範囲を減らす (たとえば、可能なかぎり多くのドメインを NIS+ に変換するなど) ように努めてください。

第 4 章では、NIS 互換モードに関連する移行の問題を説明し、 NIS から、NIS 互換を経由して、NIS+ へ完全に移行する方法を示します。

移行の準備を完了する

上記で説明した計画上の決定のほかに、第 5 章で説明するように、他にもいくつかの準備を行う必要があります。

移行を実行する

第 6 章では、推奨される一連の手順を示して、それまでに計画した移行を実際に実行します。

第 2 章

NIS+ 名前空間の設計

この章では、サイトで使用する最終的な NIS+ 名前空間を設計するための指針と推奨事項を示します。

管理モデルの目的を明らかにする

名前空間を設計するときは、NIS からの移行によって生じる制限を気にしないでください。NIS+ ドメインは、後で最終的な NIS+ 構成がどのようになるかがわかってから変更することができます。

ドメイン構造など、各サイトで使用する情報管理のモデルを選択します。各サイトでの情報の作成、格納、使用、管理について明確な方針がないと、この節で示す設計の決定を行うことが困難になります。たとえば、作業に必要以上の経費がかかる設計をしてしまう可能性があります。また、要求に合わない名前空間を設計してしまうおそれもあります。一度設定した名前空間の設計の変更には時間と手間がかかります。

名前空間の構造を設計する

NIS+ 名前空間の設計は、いろいろな作業の内で最も重要なものの 1 つです。これは、 NIS+ を一度設定した後にドメイン構造を変更するのは、時間のかかる複雑な作業になるからです。この作業が複雑になるのは、情報、セキュリティ、管理の各方針が名前空間のドメイン構造に組み込まれているからです。ドメインを編成しなおす場合は、情報の再編成、セキュリティの再設定、管理方針の再設計が必要になります。

NIS+ 名前空間の構造を設計する際は、次の点を考慮してください。これらについては、この章の以下の節で説明します。

- 22ページの「ドメインの階層」
- 28ページの「ドメイン名」
- 28ページの「電子メール環境」

ドメインの階層

NIS+ ドメイン階層には、名前空間をより管理しやすい複数の構成要素に分割できる、という利点があります。各構成要素には独自のセキュリティ、情報管理、管理方針を持たせることができます。クライアントの数が 500 を超える場合、あるユーザーグループに異なるセキュリティに方針を設定したい場合、あるいは地理的に分散したサイトがある場合は、階層を使用することをお勧めします。

ドメイン階層の必要がなければ、階層を使用しません。こうすることにより、NIS+ への移行が簡略化されます。すべてのユーザーが同じ NIS ドメイン内にいる場合、これらのユーザーは、完全指定名を使用しなくてもお互いを直接認識することができます。しかし、NIS+ 階層を作成すると、ユーザーは別々のドメインに置かれます。つまり、完全指定名か完全指定パスを使用しないかぎり、あるドメインにいるユーザーは別のドメインにいるユーザーを直接認識することができません。

たとえば、`sales.com.` と `factory.com.` というサブドメインが `.com.` ドメインの下にあるとします。この場合、`sales.com.` ドメインのユーザー `juan` が `factory.com.` ドメインのユーザー `myoko` にメールを送るためには、彼女の名前を `myoko@hostname.factory.com.` (または `myoko@hostname.factory`) と指定する必要があります。この 2 人のユーザーが同じドメインにいたときには、`myoko` と指定するだけで十分でした。リモートログインでもドメイン間の完全指定名が必要です。

テーブル間のパスを使用すると、あるドメインのテーブルと別のドメインのテーブルとの間に接続を設定することができますが、ドメイン階層を使用するメリットはなくなります。また、NIS+ サービスの信頼性も低くなります。これは、クライアントが、各自のホームドメインの利用状況だけでなく、各自のテーブルにパス指定される他のドメインの利用状況にも依存するようになるためです。テーブル間のパスを使用すると、要求への応答時間も長くなります。

ドメインの階層 – Solaris 2.6 以前のリリース

Solaris 2.6 以前のリリースでは、各サブドメインの NIS+ サーバーは、そのドメインではなく、親ドメインに含まれます。ただし、ルートドメインは除きます。サーバーとサブドメインの関係がこのような関係になっていると、サーバーがネームサービスデータをサブドメインから取得できることを想定しているアプリケーションの場合に、問題が発生します。たとえば、サブドメインの NIS+ サーバーが NFS サーバーでもある場合、サーバーはネットグループ情報をサブドメインからではなく、サブドメインの上位ドメインから取り出します。このために、混乱が発生する可能性があります。階層によって問題が発生する可能性がある場合の別の例としては、遠隔ログインするユーザーが自分のワークステーションからでは実行できないコマンドを実行する場合に、この NIS+ サーバーも使用する場合です。ルートドメインが 1 つしかない場合には、NIS+ ルートサーバーは自分がサーバーであるドメイン内にいるので、このような問題は発生しません。

ドメインの階層 – Solaris 7

Solaris 7 では、ドメインの NIS+ サーバーは、自分がサーバーであるドメイン内に存在することができます。したがって、サーバーはクライアントが使用している名前をドメイン名に設定することができます。残りのドメインの階層との機密保護通信を実行できるサーバーの機能には影響を与えません。

ドメインの階層を設計する

ドメイン階層について分からない点がある場合は、はじめに『*Solaris* ネーミングの管理』の Part 1 をお読みください。このマニュアルでは、NIS+ のドメイン構造、情報の格納、セキュリティについて説明しています。

ドメイン階層の各構成要素を理解したら、最終的な階層を示す図を作成します。この図は、設定手順を進めるうえで非常に参考になります。少なくとも、次の問題について考慮する必要があります。

- 組織的、または地理的な構造を用いた階層
- 上位ドメインへの接続
- ルートドメインでのクライアントサポート
- ドメインの大きさとドメインの数の比較
- レベルの数
- セキュリティレベル
- 複製サーバーとその数
- 情報管理

ドメインは 1 つのオブジェクトではなく、オブジェクトの集合に対する参照であることを忘れないでください。したがって、ドメインをサポートするサーバーは、実際にはドメインと関連しないでドメインのディレクトリと関連しています。図 2–1 に示すように、ドメインは *domain*、`ctx_dir.`*domain*、`org_dir.`*domain*、`groups_dir.`*domain*、という 4 つのディレクトリからなっています。

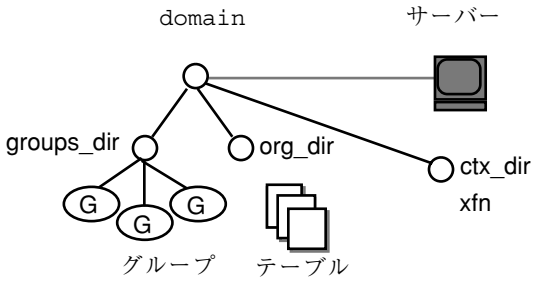

図 2–1　サーバーとドメインの関係

組織的または地理的な構造による階層

NIS+ の主な利点の 1 つに、名前空間をより小さく、より管理しやすい部分に分割できるという機能があります。たとえば、図 2–2 に示す仮の企業である Doc,Inc. の階層にならって、組織の階層を作成することができます。

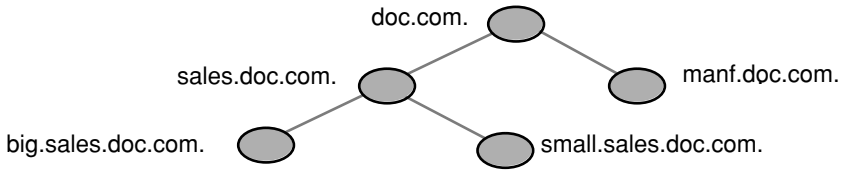

図 2–2　論理的な組織構造による NIS+ 階層の例

図 2–3 に示すように、組織ではなく建物によって階層を構成することもできます。

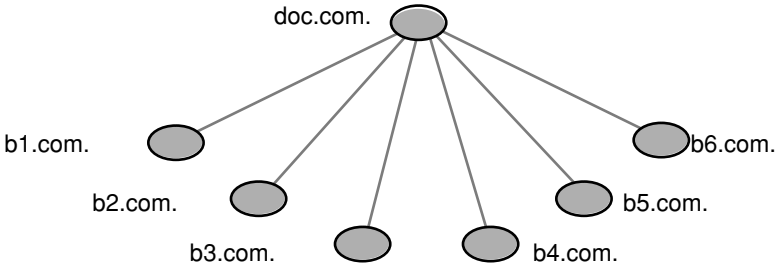

図 2–3　物理的な位置による NIS+ 階層の例

どの構成を選択するかは、主に名前空間の管理方法とクライアントによる名前区間の使用方法によって決まります。たとえば、`factory.com.` ドメインに属するクライアントが Doc,Inc. の建物全体に分散している場合は、名前空間を建物によって構成しないでください。クライアントは他のドメインに常にアクセスしなければならないため、他のドメインへの資格をクライアントに与えなければならず、ルートマスタサーバーとの通信量が増加します。この場合は、組織ごとにクライアントを構成してください。これに対して、建物に基づくドメインは、組織に変更があっても影響を受け付けません。

ネットワークの物理的配置による制限を受けないようにしてください。NIS+ 名前空間は、NIS クライアントをサポートしなければならない場合を除いて、物理的ネットワークに一致する必要はありません。名前空間で必要なドメインの数は、選択した階層の種類によって決まります。

今後の拡張計画を検討します。現在の NIS+ ルートドメインが、将来別の NIS+ ドメインの下に配置されるかどうかを検討してください。現在の設定を変更するには、膨大な作業が必要になります。名前空間での今後のドメインの必要性を見積って、混乱なくそれらのドメインを収容できる構造を設計してください。

上位ドメインへの接続

NIS+ 名前空間をインターネットや DNS のドメインなどの上位ドメインに接続するかどうかを検討します。現在 DNS 階層のもとで NIS を使用している場合は、NIS+ 名前空間に、 NIS ドメインだけを置き換えるか、サイト全体の DNS/NIS 構造を置き換えるかを決めます。

ルートドメインでのクライアントサポート

図 2–2 と図 2–3 に示した Doc,Inc. の 2 つのドメイン階層を例にして説明します。まず、すべてのクライアントを、ルートドメインの下のドメインに配置するかどうかを調べます。また、一部のクライアントをルートドメインに配置するかどうかを調べます。ルートドメインの目的がそのサブドメインのルートとして動作することだけかどうか、あるいはルートドメインがそれ自身のクライアントグループをサポートするかどうかを調べます。 すべてのクライアントをドメインの最下層に配置し、管理に使用するクライアントだけを中間ドメインに配置することができます。たとえば、最初の図でこの計画を実行すると、すべてのクライアントが big.sales.com.、small.sales.com.、factory.com. の各ドメインに配置され、管理に使用されるクライアントだけが wiz.com. ドメインと sales.com. ドメインに配置されます。たとえば、図 2–2 でこの計画を実行すると、すべてのクライアントが `big.sales.com.`、`small.sales.com.`、`factory.com.` の各ドメインに配置され、管理に使用されるクライアントだけが `.com.` ドメインと `sales.com.` ドメインに配置されます。

また、汎用部門のクライアントを上位レベルのドメインに置くこともできます。たとえば、図 2–3 では、`.com.` ドメインは建物によって構成されていて、設備部門のクライアントを `.com.` ドメインに置くことができます。しかし、ルートドメインは、単純で比較的ゆとりのある状態に維持しておく必要があるため、このことはお勧めできません。

ドメインの大きさとドメインの数と比較

現在 NIS+ の実装は、1 つのドメインあたり最大 1000 の NIS+ クライアント、1 つのドメインあたり最大 10 の複製サーバーを設定するように最適化されています。このようなドメインには、通常 10000 のテーブルエントリがあります。この制約は、現在のサーバー発見プロトコルに起因しています。NIS+ クライアントが 1000 を超える場合は、名前空間を異なる複数のドメインに分割して、階層を作成してください。

しかし、階層を作成すると、状況が複雑になって対処しにくくなるおそれがあります。1 つのドメインを大きくした方が、複数の小さいドメインを作成するよりも管理が容易なため、階層ではなくより大きなドメインを作成したいと考えるかもしれません。数の少ない大きいドメインでは、各自が作成するスクリプトを使って、作業をより容易に自動化できるため、それらのドメインのサービスを担当する熟練の管理者が少なくて済み、管理に要する手間と費用を削減することができます。しかし、ドメインを小さくすると性能が向上し、各自のテーブルをより簡単にカスタマイズすることができます。また、小さいドメインでは、管理をより柔軟に行うこともできます。

レベルの数

NIS+ は、複数レベルのドメインを処理するように設計されています。NIS+ は、任意の数のレベルに対応することができますが、レベルの数が多すぎる階層は、管理が困難です。たとえば、オブジェクトの名前は、長くてややこしいものになる場合があります。したがって、1 つのドメインに対するサブドメインの数は 20 までとし、NIS+ 階層のレベルの数は 5 までに制限するようお勧めします。

セキュリティレベル

名前空間は、通常、セキュリティレベル 2 で管理します。ただし、ドメインごとに異なるセキュリティレベルを使用する場合は、ここでそのレベルを指定する必要があります。第 3 章では、セキュリティレベルの詳細を説明しています。

複数の時間帯にまたがるドメイン

地理的に分散した組織では、ドメイン階層を機能のグループによって構成すると、1 つのドメインが複数の時間帯にまたがることがあります。ドメインが複数の時間帯にまたがることが「決して」ないようにしてください。複数の時間帯にまたがるドメインを構成する必要があるときは、複製サーバーの時刻は、マスタサーバーの時刻に合わせられることに注意してください。これにより、データベースの更新は、万国標準時 (グリニッジ標準時) を使って正しく行われます。時刻が重要な他のサービスに複製サーバーが使用されると、このことが問題の原因となるおそれがあります。複数の時間帯にまたがるドメインを動作させるには、 NIS+ をインストールするときに、複製サーバーの `/etc/TIMEZONE` ファイルを、マスタサーバーの時間帯に合わせてローカルに設定する必要があります。複製サーバーがいったん動作を始

めると、時刻が重要なプログラムの中には、万国標準時かローカル時刻のどちらを使用するかによって、正しく作動するものとしないものがでてきます。

情報管理

NIS+ 名前空間の情報の管理は、中央の制約の範囲内でローカルに行うことをお勧めします。情報は、できるかぎりそのホームドメインで管理するべきですが、広域の名前空間レベルで設定された指針または方針に従ってください。これにより、ドメインの独立性を強化する一方で、ドメイン間の整合性を維持することができます。

ドメイン名

名前の長さと複雑さについて検討します。まず、内容がわかりやすい名前を選択します。たとえば、 Sales は BW23A よりも内容をわかりやすく表しています。次に、短い名前を選択します。管理業務をより簡単にするためには、あまり長い名前を付けないでください (例: `administration_services.corporate_headquarters.doc.com.`)。

ドメイン名は、左から右に形成され、ローカルドメインから始まって、ルートドメインで終わります。ルートドメインには、常に少なくとも 2 つのラベルがなければならず、ドットで終了しなければなりません。2 番目のラベルは、“`com.`” などの Internet のドメイン名にすることができます。

サイト内とインターネット全体の電子メールドメインを対象に、このドメイン固有の名前の意味について検討する必要があります。

移行の方式によっては、NIS 上のドメイン名を希望の構造に変更してから、 NIS+ ドメインに移行することもできます。

電子メール環境

NIS が平坦なドメイン空間を持つのに対して、NIS+ はドメイン階層を持つことができるため、NIS+ への移行はメール環境にも影響があります。NIS では、必要な mail ホストは 1 つだけです。NIS+ でドメイン階層を使用すると、名前空間の各ドメインごとに 1 つの mail ホストが必要になります。これは、各ドメインの名前が一意ではなくなるためです。

したがって、ルートドメインにないクライアントの電子メールアドレスが変更される場合があります。一般的に、クライアントの電子メールアドレスは、ドメイン名が変更されるか、または階層に新しいレベルが追加されると変更されます。

以前の Solaris のリリースでは、これらの変更に非常に手間がかかりました。このリリースでは、`sendmail` の拡張機能がいくつか追加され、作業が簡単になっています。さらに、NIS+ には、`sendmailvars` テーブルが追加されています。`sendmail` プログラムは、まず `sendmailvars` テーブル (表 2–5 を参照) を見てから、ローカルな `sendmail.cf` ファイルを調べます。

注 - mail サーバーが、そのサポート対象となるクライアントの NIS+ ドメイン内にあることを確認してください。また、性能上の理由から、 mail サーバーに対して他のドメイン内のテーブルへのパスを指定しないでください。

DNS での新しい mail アドレスの影響について検討してください。DNS の MX レコードを修正しなければならない場合があります。

サーバーの必要条件を決める

各 NIS+ ドメインは、一組の NIS+ サーバーによってサポートされています。各組は、1 つのマスタサーバーと 1 つ以上の複製サーバーを持っています。これらのサーバーは、ドメインのディレクトリ、グループ、テーブルを格納して、ユーザー、管理者、アプリケーションからのアクセス要求に応答します。各ドメインをサポートしているのは、一組のサーバーだけです。一組のサーバーで、複数のドメインをサポートすることができますがお勧めできません。

NIS+ サービスでは、マスターサーバーを少なくとも 1 つ各 NIS+ ドメインに割り当てる必要があります。各ドメインが必要とする複製サーバーの数は、通信量の負荷、ネットワークの構成、NIS クライアントの有無などによって決まります。サーバーメモリーの量、ディスク記憶容量、プロセッサの速度は、クライアントの数とサーバー上に置かれる通信量の負荷によって決まります。

Solaris オペレーティング環境が動作しているワークステーションで、十分な容量のハードディスクさえ備わっていれば、NIS+ サーバーにすることができます。NIS+ のサーバー用、クライアント用のソフトウェアは、どちらも Solaris 製品に含まれています。したがって、Solaris オペレーティング環境がインストールされているワークステーションであれば、サーバーかクライアント、またはこの両方にすることができます。

NIS+ 名前空間をサポートするために必要なサーバーを決定するとき、次の節で説明する要因を考慮する必要があります。

- 30ページの「サポートするドメインの数」
- 31ページの「複製サーバーの数」
- 33ページの「サーバーの速度」
- 34ページの「サーバーメモリーの容量」
- 35ページの「サーバーディスク容量」

サポートするドメインの数

初めに、階層内の各ドメインに 1 つのマスターサーバーを割り当てます。図 2–4 に割り当ての例を示します。

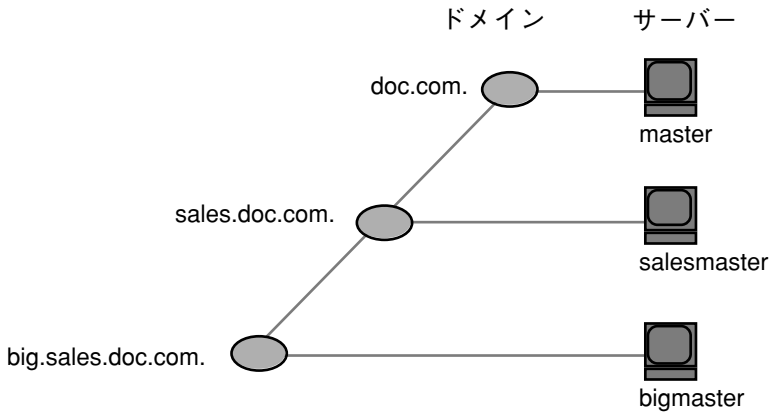

図 2–4　サーバーをドメインに割り当てる

1 つ以上の複製を各ドメインに割り当てます。複製を使うと、マスターサーバーが一時的に使用不可能な場合でも、要求に応答することができます。使用する複製の数については、22ページの「名前空間の構造を設計する」を参照してください。

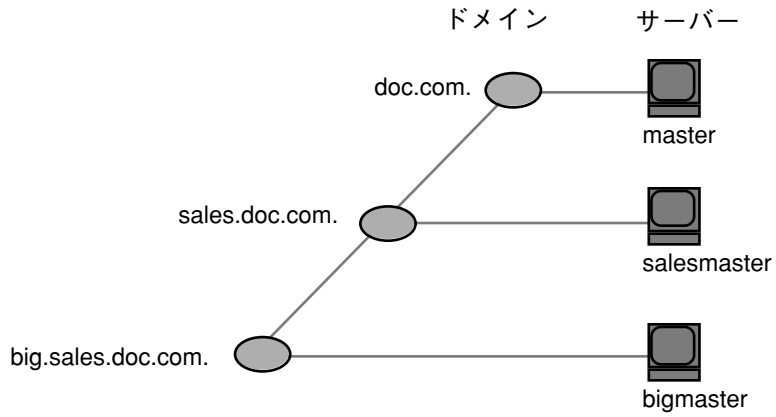

図 2–5　ドメインへの複製サーバーの追加

複製サーバーの数

ドメインに最適なサーバーの数 (マスターと複製) は、数多くの要因によって決まります。

- NIS+ はローカルサブネット上の同時通信に依存しないため、NIS+ マスターサーバーが必要とする複製の数は NIS サーバーよりも少なくなります。
- すべてのドメインには少なくとも 1 つの複製サーバーがなければなりません。その理由は、マスターサーバーが一時的に使用不可能になったときに NIS+ サービスが破壊されないようにするためです。
- ドメインには 10 以上の複製があってはなりません。その理由は、情報更新が多くの複製に伝わるときにネットワークの通信量とサーバーの負荷が増加するためです。
- クライアントの種類。クライアントワークステーションが古くて遅いと、新しくて高速のマシンより必要な複製の数が少なくなります。
- 設計するドメイン階層が広域ネットワーク (WAN) リンクをまたがる場合、WAN リンクの両側に複製を置くと安全に実行できるようになります。この場合、リンクの 1 つの側にマスターサーバーと 1 つ以上の複製を設置して、他の側にも 1 つ以上の複製を設置するようにします。こうすると、WAN リンクが一時的に使用不可能になった場合でも、リンクの片側にいるクライアントは NIS+ サービスを継続して使用することができます (しかし、サーバーを WAN の両側に置くと、物理的配置によってではなくグループ機能別に構成されている名前空間の構造が変化します。その原因は、複製は地理的に異なったドメインで、物理的に常駐するためです)。

多くのサイトが分散されている組織では、各サイトは独自のサブドメインを必要とする場合もあります。サブドメインマスターは、さらにレベルの高いドメインに配置されます。その結果、ポイントツーポイントのリンク間では非常に多くの通信量が発生します。地域的な複製を作成すると、要求への応答を早くすることができ、さらにリンク両端でのポイントツーポイントの通信量を少なくすることもできます。

- ドメイン内のサブネット数。できれば、1 つの複製を各サブネット上に置きます (ただし、ドメイン全体で 10 以上の複製を使わないでください)。Solaris 1.x NIS クライアントがない場合または、NIS クライアントをサポートするために NIS+ サーバーを NIS 互換モードで使う場合、これらの場合以外には、すべてのサブネットに複製を配置する必要はありません。NIS クライアントは、同じサブネット上にないサーバーにアクセスしません。唯一の例外は Solaris オペレーティング環境の NIS クライアントであり、`ypinit`(1M) を使って NIS サーバーのリストを指定することができます。この場合、ネットマスク数は正しく設定しなければなりません。

- ユーザーと管理者がルックアップを実行する方法。`niscat` *table* | `grep` *name* コマンドは、`nismatch` *name table* コマンドが使用するものよりもはるかに多くのサーバー資源を使用します。

- サーバーの種類。新しくて高速なサーバーは、古くて遅いマシンが実行するサービスよりも高速で、より効率的なサービスを行うことができます。したがって、サーバーが強力になるほど、必要とするサーバーが少なくなります。

- クライアントの数。ドメイン内のクライアントの数が多くなるほど、必要とする複製サーバーの数も多くなります。ドメイン内のクライアントの数は 1000 以下になるようにしてみてください。 NIS+ クライアントは 、 NIS クライアントよりもサーバー上での負荷が大きくなります。非常に多くのクライアントがほんのわずかのサーバーからサービスを提供されると、ネットワークの性能に影響を与えることになります。

  次の 表 2–1 は、応答時間を長くしないで一連のサーバーが処理できるビジークライアントのピーク数を示しています。この結果を作成したベンチマークテストでは、クライアントは、 NIS+ サービスを集中的に利用するように設計されています。各クライアントは、通常のドメインが経験する平均的な負荷ではなく、ピーク負荷をシミュレートするため、多くの NIS+ コールを行いました。したがって、表 2–1 に示した数字は応答時間を長くしないでピーク負荷 (平均負荷ではなく) に適合するように設定された構成を示しています。

表 2–1 サーバーの構成と NIS+ クライアントの数

サーバーと複製の構成	ビジークライアントのピーク数
Master: SS5-110	120
Master: SS5-110 Replica: SS10-40	220
Master: SS5-110 Replica: SS10-40 Replica: SS20-50	580
Master: Ultra-167	420
Master: Ultra-167 Replica: SS10-40	840

表の数字は、クライアントが NIS+ サービスを広範囲に使用した場合、約 100 から 400 のクライアントごとに余分な複製を追加する必要があることを示しています。複製が SS5 の場合、 100 のクライアントごとに新しい複製を 1 つ追加する必要があり、複製が Ultra の場合 400 のクライアントごとに新しい複製を追加する必要があります。この数字は、必要性に応じて調整します。

各種のマシンを使わないでドメインあたりの複製の数を十分なものにする 1 つの方法は、マルチホームのサーバーを作成することです。マルチホームサーバーとは、複数のイーサネットまたはネットワークインタフェースを持っているマシンをいいます。マルチホームサーバーは、1 つのドメイン内にある複数のサブネットにサービスを提供することができます (マスターあるいは複製サーバーに複数のドメインを設定することもできますが、これはお勧めできません)。

サーバーの速度

サーバーの速度が早いほど、 NIS+ の性能は向上します (しかし、その場合 NIS+ サーバーは SMP マルチスレッドハードウェアを有効に利用することはできません)。NIS+ サーバーは、平均的なクライアントと同等かそれ以上に強力にする必要があります。新しいクライアントのサーバーとして古いマシンを使うことはお勧めできません。

サーバーの速度以外に、その他の多くの要因が NIS+ の性能に影響を与えます。ユーザーおよびホストの数と種類、実行しているアプリケーションの種類、ネットワークトポロジ、負荷の密度、その他の要因すべてが NIS+ の性能に影響します。したがって、 2 つの異なるネットワークにおいて、同じサーバーハードウェアからまったく同じ性能を期待することはできません。

表 2–2 に示したベンチマーク数字は、比較のためにだけ示してあります。ネットワーク上の性能は、この数字とは違うこともあります。下に示したベンチマークの数字は、10000 エントリという標準的なテーブルサイズのテストネットワークに基づいています。表 2–2 を参照してください。

表 2–2 ハードウェア速度と NIS+ 動作の比較

マシン	秒当たりの整合動作数	秒当たりの追加動作数
SS5-110	400	6
SS20-50	440	6
PPro-200	760	13
Ultra-167	800	11
Ultra-200	1270	8

サーバーメモリーの容量

サーバーの絶対最低メモリー必要量は 32M バイトですが、中から大規模ドメインのサーバーは少なくとも 64M バイトを装備した方が良いでしょう。

理想的には、 NIS+ サーバーは、 有効な NIS+ テーブルすべての検索可能カラムのエントリすべてを RAM 内に一度に保存できるほど十分なメモリーが必要です。要するに、最適なサーバーメモリーは、すべてのNIS+ テーブルが必要とするの合計メモリー必要量になります。

分かりやすくするため、表 2–3 は検索可能カラムが 5 つある netgroup テーブルのメモリー必要量を示し、表 2–4 は `passwd` 、 `host` および `cred` テーブルのおおよそのメモリー必要量を示しています。

表 2–3 `netgroups` テーブルに必要なサーバーメモリー

エントリの数	サーバーメモリー使用量 (M バイト)
6000	4.2
60000	39.1
120000	78.1
180000	117.9

表 2–3　netgroups テーブルに必要なサーバーメモリー　続く

エントリの数	サーバーメモリー使用量 (M バイト)
240000	156.7
300000	199.2

表 2–4　passwd テーブルに必要なおおよそのメモリー

エントリの数	サーバーメモリー使用量 (M バイト)
6000	3.7
60000	31.7
120000	63.2
180000	94.9
240000	125.8
300000	159.0
1000000	526.2

他のテーブルには、検索可能な各カラムに対してエントリ当たりの平均バイト数に予測エントリ数を掛けると、メモリーサイズを予測することができます。たとえば、エントリが 10000 で検索可能カラムが 2 のテーブルがあるとします。最初のカラムでのエントリ当たりの平均バイト数は 9 で、 2 番目のカラムでのエントリ当たり平均バイト数は 37 です。したがって、計算結果は、 (10000 × 9) + (10000 × 37) = 46000 になります。

注 - cred テーブルのエントリ数を予測するときは、ユーザーのローカル資格証明書に 1 つ、DES 資格証明書に 1 つずつ、すべてのユーザーが 2 つのエントリを持つことを忘れないでください。各マシンが使用するエントリは 1 つだけです。

標準的な NIS+ テーブルのそれぞれにある検索可能カラムの数については、37ページの「NIS+ 標準テーブル」を参照してください。

サーバーディスク容量

必要なディスク容量は、次の 4 つの要因によって決まります。

- Solaris オペレーティング環境のソフトウェアが使用するディスク容量

- /var/nis (および /var/yp 互換モードで使用する場合) のディスク容量
- メモリーの容量
- NIS+ サーバー処理に必要なスワップ空間

Solaris オペレーティング環境のソフトウェアは、インストールした量によって、220M バイトを超えるディスク容量を必要とすることがあります。正確な数字については、Solaris のインストールガイドを参照してください。また、サーバーが使用する他のソフトウェアの使用するディスク容量も計算に入れる必要があります。NIS+ ソフトウェア自体は、Solaris 2.4 配布の一部であるため、余分なディスク容量を使用しません。

NIS+ のディレクトリ、グループ、テーブル、クライアント情報は、/var/nis に格納されています。この /var/nis ディレクトリは、1 つのクライアントごとにおよそ 5K バイトのディスク容量を使用します。たとえば、名前空間に 1000 のクライアントがあると、/var/nis には、およそ 5M バイトのディスク容量が必要になります。ただし、同じく /var/nis に格納されるトランザクションのログが大量になる場合があるため、クライアントごとにディスク容量を追加する必要があるかもしれません。この場合は 10〜15M バイトの容量を追加するようお勧めします。つまり、1000 のクライアントがあるときは、15〜20M バイトを /var/nis に割り当ててください。トランザクションのログに対して定期的にチェックポイントを実行する場合、この数字を減らすことができます。 /var/nis には独立したパーティションを設けることをお勧めします。パーティションが独立していることにより、オペレーティングシステムのアップグレードを行う際、その作業が容易になります。

NIS+ を NIS と並行して使用するときは、/var/yp に対して、/var/nis に割り当てている量と同じ容量を割り当てて、NIS から転送する NIS マップを格納してください。

さらに、サーバーの通常のスワップ空間の所要量に加えて、rpc.nisd のサイズの 2 倍のスワップ空間も必要になります。システム上で rpc.nisd が使用しているメモリーの量を確認するには、 nisstat コマンドを実行します。詳細は、rpc.nisd マニュアルページを参照してください。この空間のほとんどは、コールバック操作中や、 nisping–C によってディレクトリに対しチェックポイントを実行するか、複製サーバーが作成されるときに使用されます。これは、このような手続き中には、NIS+ サーバープロセス全体がフォークされるためです。使用するスワップ空間が、64M バイト未満になることはありません。

テーブルの構成を決める

NIS+ テーブルには、単純なテキストファイルやマップにはない、いくつかの機能があります。これらのテーブルは、列エントリ構造を持ち、検索パスを受け付けます。また、これらのテーブルをリンクして、いくつかの異なる方法で構成することもできます。さらに、独自のカスタム NIS+ テーブルを作成することもできます。各自のドメイン用にテーブル構成を選択するときは、以下の節の内容を検討してください。

- 37ページの「NIS+ テーブルと NIS マップとの違い」
- 42ページの「カスタム NIS+ テーブルの使用」
- 43ページの「テーブル間の接続」

NIS+ テーブルと NIS マップとの違い

NIS+ テーブルは、様々な点で NIS マップと異なりますが、次の 2 つの相違点は、名前空間を設計する場合に念頭においておく必要があります。

- NIS+ が使用する標準テーブルの数は NIS よりも少ない
- NIS+ テーブルは、SunOS 4.x リリースでの NIS マップとは異なる方法で、`/etc` 内のファイルと相互運用される

NIS+ 標準テーブル

17 の標準 NIS+ テーブルを検討して、各サイトの必要に応じたものかどうかを確認してください。これらのテーブルは、表 2–5 に示してあります。表 2–6 は、 NIS マップと NIS+ テーブルの対応を示しています。

関連するテーブルの同期化については心配する必要はありません。NIS+ テーブルには、基本的に NIS マップと同じ情報が格納されます。ただし、NIS+ テーブルでは、類似の情報が 1 つのテーブルに統合されます (たとえば、NIS+ の hosts テーブルには、NIS マップの `hosts.byaddr` と `hosts.byname` と同じ情報が格納されます)。NIS+ テーブルでは、 NIS マップで使用されていた対のキー値の代わりに、列と行が使用されます (『*Solaris* ネーミングの設定と構成』を参照)。キー値のテーブルには、2 つの列があり、最初の列はキー、2 番目の列は値になります。したがって、ホスト情報などの情報を変更するときは、その情報を、`hosts` テーブルなど 1

か所で変更するだけですみます。関連するマップ全体の情報の整合性の維持について注意する必要はなくなりました。

オートマウンタテーブルの新しい名前は次のとおりです。

- `auto_home` (旧名 : `auto.home`)
- `auto_master` (旧名 : `auto.master`)

NIS+ では、ドットを使ってディレクトリを区切るため、ドットは下線に変更されました。テーブル名にドットを使用すると、NIS+ は名前の変換を誤ります。同じ理由で、マシン名にドットを使用することはできません。ドットを含むマシン名は、かならず他の名前に変更してください。たとえば、`sales.alpha` というマシン名は使用できません。`sales_alpha`、`salesalpha` などのドットを含まない任意の名前に変更してください。

NIS から NIS+ への移行を行うには、NIS 自動マウンタマップのドットを下線に変更する必要があります。また、クライアントのオートマウンタ構成ファイルでも、同じ処理が必要です。表 2–5 を参照してください。

表 2–5 NIS+ テーブル

NIS+ テーブル	テーブル内の情報
`hosts`	ドメイン内にあるすべてのワークステーションのネットワークアドレスとホスト名
`bootparams`	ドメイン内にあるすべてのディスクレスクライアントのルート、スワップ、ダンプの各パーティションの位置
`passwd`	ドメイン内のすべてのユーザーに関するパスワード情報
`cred`	ドメインに属する主体の資格
`group`	ドメイン内のすべての UNIX ® グループのグループパスワード、グループ ID、メンバー
`netgroup`	ドメイン内のワークステーションとユーザーが属するネットグループ
`mail_aliases`	ドメイン内のユーザーの mail 別名に関する情報
`timezone`	ドメインの時間帯
`networks`	ドメイン内のネットワークとその標準的な名前

表 2–5　NIS+ テーブル　続く

NIS+ テーブル	テーブル内の情報
netmasks	ドメイン内のネットワークとそれに関連するネットマスク
ethers	ドメイン内にあるすべてのネットワークのイーネットアドレス
services	ドメインで使用される IP サービスの名前とそのポート番号
protocols	ドメインで使用される IP プロトコルのリスト
rpc	ドメインで使用できる RPC サービスの RPC プログラム番号
auto_home	ドメイン内のすべてのユーザーホームディレクトリの位置
auto_master	オートマウンタマップ情報
sendmailvars	mail ドメインを格納

表 2–6　NIS マップと NIS+ テーブルの対応表

NIS マップ	NIS+ テーブル	注
auto.home	auto_home	
auto.master	auto_master	
bootparams	bootparams	
ethers.byaddr	ethers	
ethers.byname	ethers	
group.bygid	group	NIS+ グループとは異なる
group.byname	group	NIS+ グループとは異なる
hosts.byaddr	hosts	

表 **2–6**　NIS マップと NIS+ テーブルの対応表　続く

NIS マップ	**NIS+** テーブル	注
hosts.byname	hosts	
mail.aliases	mail_aliases	
mail.byaddr	mail_aliases	
netgroup	netgroup	
netgroup.byhost	netgroup	
netgroup.byuser	netgroup	
netid.byname	cred	
netmasks.byaddr	netmasks	
networks.byaddr	networks	
networks.byname	networks	
passwd.byname	passwd	
passwd.byuid	passwd	
protocols.byname	protocols	
protocols.bynumber	protocols	
publickey.byname	cred	
rpc.bynumber	rpc	
services.byname	services	
ypservers		必要なし

NIS+ には、NIS テーブルと対応しない sendmailvars という新しいテーブルが 1 つあります。この sendmailvars テーブルには、sendmail で使用される mail ドメインが格納されます。

NIS+ テーブルは、NIS とは異なる方法で /etc 内のファイルと相互運用される

NIS および他のネットワーク情報サービスが SunOS 4.x 環境の /etc 内のファイルとの間で行う相互運用は、+/- 構文を使用して /etc 内のファイルによって管理されていました。NIS+、NIS、DNS、および他のネットワーク情報サービスが、Solaris オペレーティング環境の /etc 内のファイルと相互運用を行う方法は、ネームサービススイッチによって決まります。ネームサービススイッチは構成ファイルで、/etc/nsswitch.conf という名前ですべての Solaris オペレーティング環境のクライアントに格納されています。すべての Solaris オペレーティング環境クライアントにある構成ファイルの nsswitch.conf は、そのクライアントの情報源を指定します。これは、 /etc 内のファイル、DNS ゾーンファイル (ホストだけ)、NIS マップ、または NIS+ テーブルなどです。この NIS+ クライアントの nsswitch.conf 構成ファイルの例は、例 2–1 の簡易説明です。

例 2–1 簡易化されたネームサービススイッチファイルの例

```
passwd: files
group: compat
group_compat: nisplus
hosts: nisplus dns [NOTFOUND=return] files
services: nisplus [NOTFOUND=return] files
networks: nisplus [NOTFOUND=return] files
protocols: nisplus [NOTFOUND=return] files
rpc: nisplus [NOTFOUND=return] files
ethers: nisplus [NOTFOUND=return] files
netmasks: nisplus [NOTFOUND=return] files
bootparams: nisplus [NOTFOUND=return] files
publickey: nisplus
netgroup: nisplus
```

(続く)

```
automount: files nisplus

aliases: files nisplus
```

つまり、ほとんどのタイプの情報で、情報源はまず NIS+ テーブルであり、次に /etc 内のファイルということになります。passwd および group エントリの場合、ネットワーク情報のソースは、ネットワークファイルか、または /etc 内のファイルおよび /etc ファイルの +/- エントリによって表された NIS+ テーブルのいずれかとなります。

3 種類のスイッチ構成ファイルから選択するか、または独自のスイッチ構成ファイルを作成することができます。方法については、『*Solaris* ネーミングの管理』を参照してください。

カスタム NIS+ テーブルの使用

どの標準以外の NIS マップを使用するか、またその使用目的を決定してください。NIS+ に変換できるか、あるいは NIS+ 標準マップと置き換えられるかを検討します。

アプリケーションの中には、NIS マップに依存するものがあります。これらのアプリケーションが、NIS+ でも同様に機能するか、また混合環境で正しく機能できるかを検討します。

NIS+ でカスタムテーブルを作成するには、nistbladm を使用します。テーブル名にはドットを使用できないことを忘れないでください。

NIS+ を使用して、独自の NIS マップをサポートできるようにしたい場合は、2 つの列を使用するキー値テーブルを作成する必要があります。最初の列はキー、2 番目の列は値を示します。このテーブルを作成して、NIS+ サーバーを NIS 互換モードで実行すると、NIS クライアントは機能の変更に気がつきません。

テーブル間の接続

NIS+ テーブルには、そのホームドメインの資源とサービスに関する情報だけが含まれています。したがってクライアントは、別のドメインに格納された情報を検索する際には、そのドメインの名前を指定しなければなりません。この「転送」を自動化するには、ローカルテーブルをリモートテーブルに接続してください。NIS+ テーブルは、次の 2 つの方法で接続することができます。

- パスを使用する方法
- リンクを使用する方法

NIS+ 名前空間で NIS クライアントを使用するときは、パスとリンクを使用してはいけません。NIS クライアントは、パスまたはリンクでは、正しい情報を検索することができません。

パス

他のドメインのクライアントが、特定の NIS+ テーブル内の情報を頻繁に要求する場合は、そのローカル NIS+ テーブルから他のドメインのテーブルへのパスを設定することを検討してみてください。図 2–6 を参照してください。

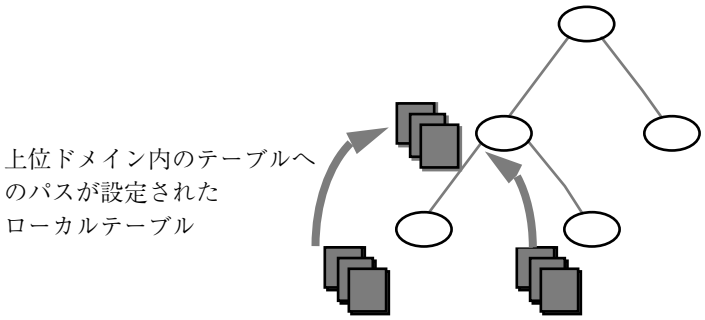

図 2–6　上位ドメイン内のテーブルへのパスを設定する

このようなパスがもたらす主な利点は 2 つあります。まず、下位ドメインのクライアントが、別のテーブルを明示的に検索しなくてもすみます。さらに、上位ドメインの管理者があるテーブルで変更を行い、その変更を他のドメインのクライアントに見えるようにすることができます。ただし、このようなパスを設定すると、性能が低下します。特に検索がうまくいかないと、性能に影響が出ます。これは、NIS+ サービスで、1 つのテーブルではなく 2 つのテーブルを検索しなければならないためです。パスを使用すると、テーブル検索も、他のドメインの利用状況に依存することになります。この依存によって、ドメインの実質の利用度が低下する可

能性があります。このような理由から、パスは、他に問題を解決する手段がない場合に限って使用するようにしてください。

mailhost (mail ホスト) は、別名として使用されることが多いため、特定の mailhost に関する情報を検索する必要がある時は、検索パスに完全指定名 (たとえば、`mailhost.sales.com.` など) を使用する必要があることに注意してください。そうしないと、 NIS+ は、検索したすべてのドメインで見つかった mailhost をすべて返します。

パスをローカルテーブルに設定するには、`nistbladm` コマンドに `–p` オプションを付けて使用します。テーブルのパスを変更するには、テーブルオブジェクトへの変更アクセス権がなければなりません。テーブルの検索パスを調べるには、`niscat -o` コマンドを使用してください (テーブルへの読み取りアクセス権が必要です)。

リンク

テーブル間にリンクを設定すると、パスと同様の効果が生じますが、リンクでは 1 つのテーブル、つまりリモートテーブルの検索だけが行われる点が異なります。検索パスでは、 NIS+ はまずローカルテーブルを検索し、うまくいかなかった場合にのみリモートテーブルを検索します。リンクでは、検索は、リモートテーブルに対して直接行われます。実際には、リモートテーブルがローカルテーブルと置き換わります。リンクを設定すると、下位ドメインが、独自のテーブルを管理しなくても、上位ドメインの情報を使用することができます。

リンクを作成するには、`nisln` コマンドを使用してください。また、テーブルオブジェクトに対する変更権が必要です。

パスを使用するか、またはドメイン内の NIS+ テーブルをリンクするかを決定するのは、容易ではありません。この決定を行う際の基本的な方針をいくつか、次に示しておきます。

- すべてのドメインに、すべての標準テーブルへのアクセス権がなければなりません。
- 内容の更新が多く、またアクセス頻度が高いデータは、階層の下位に位置していなければなりません。このようなデータは、最も使用頻度の高い場所の近くに置くようにしてください。
- いくつかのドメインが使用するデータは、階層内の上位に位置していなければなりません。ただし、それらのドメインを独立した状態にしておく必要がある場合は除きます。

- データの格納場所が階層の下位であればあるほど、自立的な管理は容易になります。
- NIS+ クライアントだけが、パスおよびリンクで接続されたテーブルを見ることができます。NIS クライアントは、これらのテーブルを見ることができません。

図 2–7 は、以上の方針をまとめたものです。

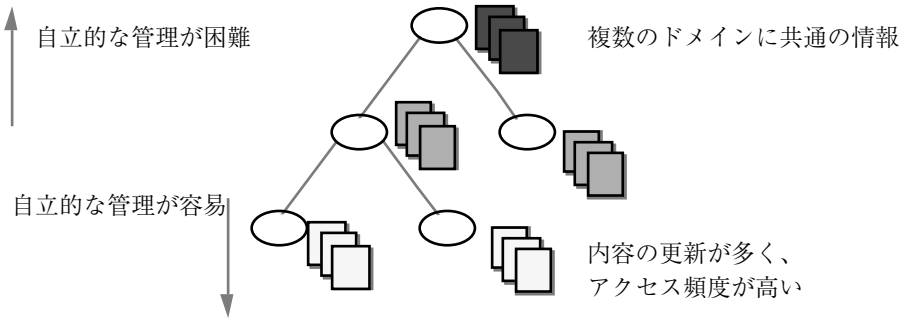

図 2–7　NIS+ 階層での情報の配布

ユーザー名とホスト名の重複の解決

NIS+ は、要求が実行された場合に、その主体が人間なのかワークステーションなのかを区別できません。したがって、すべてのユーザー名は、同一の名前空間におけるマシン名と違うものでなければなりません。すなわち、一定の名前空間においては、ユーザーがマシン名と同じユーザー名を持つことができず、またユーザー ID と同じマシン名を付けることもできません。

たとえば、NIS 環境ではローカルマシンの名前が `irina` の場合も、ユーザーは `irina` というログイン名を使用できます。このユーザーのネットワークアドレスは、`irina@irina` となります。これは、NIS+ 環境では成立しません。サイトを NIS+ に変換する場合、ユーザーがログイン名を変更するか、あるいはユーザーのマシン名を変更する必要があります。同一のユーザー名とマシン名が存在する場合、その名前を持つマシンが同じ名前のユーザーに属していない場合でも問題となります。次に示す例は、NIS+ では無効となる重複した名前の例です。

- 同一名前空間における `jane@jane`
- 同一名前空間における `patna@peshawar` と `rani@patna`

この問題の一番の解決方法は、/etc 内のファイルすべてと NIS マップ をチェックしてから、 NIS+ テーブルを生成することです。重複している名前を見つけた場合は、ログイン名ではなくマシン名を変更し、後でマシンの元の名前の別名を作成してください。

第 3 章

NIS+ セキュリティ基準の選択

この章では、名前空間のセキュリティに関する選択を行うための一般的な指針と推奨事項を示します。

NIS+ セキュリティの影響について理解する

NIS+ には、NIS にはなかったセキュリティが備わっているため、さらに多くの管理作業が必要になります。`chkey`、`keylogin`、または `keylogout` の手順の実行に慣れていないユーザーにも、より多くの作業が要求されることがあります。さらに、NIS+ によって提供される保護は、完璧に安全というものではありません。十分な計算能力と知識があれば、Diffie-Hellman 公開鍵暗号システムを破ることができます。

192 ビットを超える Diffie-Hellman 鍵を使用すると、NIS+ セキュリティが大幅に向上します。ただし、鍵が長くなるにつれて認証に必要な時間が長くなるため、性能が低下する可能性があります。

注 - nisauthconf を使用して、この種類の Diffie-Hellman 鍵を設定します。長い鍵の使用については、nisauthconf(1M) を参照してください。

また、キーサーバープロセスによって格納された秘密鍵は、資格を持つ、ルート以外のユーザーがログアウトしても、そのユーザーが keylogout によってログアウトしないかぎり、自動的に削除されません。セキュリティは、ユーザーが keylogout(1) によってログアウトしたとしても、完全ではありません。これは、セッションキーが、その期限が切れるか、または再初期化されるまで、有効なためです (詳細については keylogout(1) のマニュアルページを参照してください)。ルートキーは、keylogin –r によって作成されて、/etc/.rootkey に格納されますが、これは .rootkey ファイルが明示的に削除されるまで残ります。スーパーユーザーは keylogout(1) を使用することができません。しかしそれでも、NIS+ は、NIS よりもはるかに安全です。

NIS+ セキュリティがユーザーに与える影響

NIS+ セキュリティを使用すると、NIS+ から取得する情報の信頼性が向上し、情報への不正なアクセスを防げるため、ユーザーにとって有益です。ただし、NIS+ セキュリティを使用するには、ユーザーは、セキュリティに関する若干の知識を習得して、2 ～ 3 の管理手順を実行しなければなりません。

NIS+ ではネットワークログインが必要ですが、ユーザーがさらにキーログインを実行する必要はありません。これは、クライアントが正しく設定されていれば、login コマンドにより、そのクライアントのネットワーク鍵が自動的に取得されるためです。クライアントは、そのログインパスワードと SecureRPC パスワードが同じであれば、正しく設定されます。ユーザー root の秘密鍵は、通常、/etc/.rootkey ファイルで入手することができます (潜在的なセキュリティの問題として前述しました)。NIS+ ユーザーのパスワードと資格が、passwd コマンドによって変更されると、そのユーザーの資格情報も自動的に変更されます。

- NIS+ マシンのローカルの root パスワードを変更するには、passwd コマンドを実行します。
- root の資格を変更するには、chkey コマンドを実行します。

ただし、ユーザーがそのネットワークパスワードだけでなく、ローカルの /etc/passwd ファイルのパスワードも管理できて、これらのパスワードがネットワークパスワードと異なる場合、ユーザーは login を実行するたびに keylogin

を実行しなければなりません。この理由は、『*Solaris* ネーミングの管理』のセキュリティに関する章に説明されています。

NIS+ セキュリティがシステム管理者に与える影響

Solaris オペレーティング環境は、認証のための DES 暗号機構を備えているため、セキュリティ保護操作を必要とするシステム管理者は、別に暗号キットを購入する必要がありません。ただし、システム管理者は、ユーザーに、`passwd` コマンドと `passwd -r` コマンドを使用する方法と、これらのコマンドをいつ使用するかを指示する必要があります。

また、セキュリティを強化した NIS+ 名前空間の設定は、通常の名前空間の設定よりも複雑です。この複雑さは、名前空間の設定に必要なステップが多いことだけではなく、すべての NIS+ 主体に対するユーザーの資格とマシンの資格を作成して管理しなければならないということに原因があります。管理者は、`passwd` テーブルと`hosts` テーブルから不要なアカウント情報を削除するのと同様に、不要な資格を削除する必要があります。また、管理者は、サーバーの公開鍵が変更された場合、`nisupdkeys` を使用して、名前空間全体の鍵も変更しなければなりません。さらに管理者は、他のドメインからこのドメインへのリモートログインを望んだり、NIS+ への認証されたアクセスを望むユーザーに対して、LOCAL 資格を追加しなければなりません。

NIS+ セキュリティが移行の計画に与える影響

NIS+ セキュリティの利点と管理上の要件をよく理解したら、NIS+ セキュリティを、移行中または移行後のどちらで実装するかを決める必要があります。NIS 互換モードで、ドメイン内のサーバーの一部またはすべてを操作している場合でも、完全な NIS+ セキュリティを使用するようお勧めします (ドメイン内のすべてのサーバーが同じ NIS 互換モードを使用しているのが、望ましい状態です)。ただし、これには管理の手間が非常にかかります。簡単な方法としては、NIS 互換セキュリティによって NIS+ サーバーと名前空間を設定し、NIS+ クライアントの資格は作成しないことです。ただし、管理者とサーバーには、やはり資格が必要です。NIS+ クライアントは、NIS クライアントとともに、未認証カテゴリに割り当てられます。これにより、学習と設定の作業は軽減されますが、次のような欠点があります。

- ユーザーは、NIS+ テーブルを更新できなくなります ただし、ログインパスワードの変更は可能です (ただし Solaris 2.5 以降のリリースの場合だけ)。

- ユーザーは、ネームサービス情報が、認証されたNIS+ サーバーのものかどうかを確認できなくなります。

資格を選択する

NIS+ には、LOCAL と DES という 2 つの種類の資格があります。

注 - このマニュアルでは、「DES 資格」という用語は、拡張 640 ビット Diffie-Hellman 鍵と、オリジナルの 192 ビット Diffie-Hellman (デフォルト) 鍵の長さについて使用します。 `cred` テーブルでは、拡張鍵は `DES` キーワードではなく、`DH640-0` のような着信先を使用します。長い鍵の使用については、`nisauthconf`(1M) を参照してください。

どの NIS+ 主体も、これらの資格のうち少なくとも 1 つを必要とします。名前空間がセキュリティレベル 2 (デフォルト) で管理されているときは、すべての NIS+ 主体 (クライアント) は、そのホームドメインに、DES 資格がなければなりません。また、すべてのユーザー (ワークステーションではなく) は、そのホームドメインと、ログインアクセスが必要な他のすべてのドメインに、LOCAL 資格がなければなりません。

名前空間の資格の必要を調べるには、次のことを検討してください。

- 主体の種類
- 資格の種類

NIS+ の主体になれるのは、ユーザーか、クライアントワークステーション上のスーパーユーザーです。図 3–1 を参照してください。

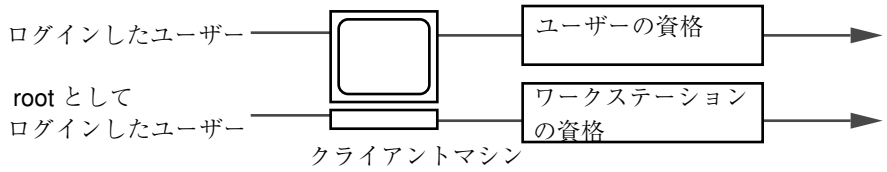

図 3–1　NIS+ の主体

作成する必要がある資格を決めたら、その資格の対象となる主体の種類を確認してください。たとえば、NIS+ クライアントを `nisclient` によって設定した場合は、ワークステーションとユーザーの両方に資格を作成することになります。ユー

ザーの資格を作成しないと、そのユーザーには、未認証クラスに許可されたアクセス権しか与えられません。意図してそのように名前空間を設定している場合は、この設定は十分正しく機能します。しかし、未認証クラスにアクセス権を何も与えていないと、ユーザーはその名前空間を使用することができません。

セキュリティレベルを選択する

NIS+ はセキュリティレベル 2 で実行されるように設計されており、このレベルがデフォルトです。セキュリティレベルの 0 および 1 は、テストとデバッグの目的にのみ用意されています。実際にユーザーが存在しているネットワーク (operational network) は、レベル 2 以外で運用しないでください。NIS+ のセキュリティレベルの詳細については、『*Solaris* ネーミングの管理』を参照してください。

パスワード有効期限の基準、原則、および規則を確立する

パスワードの有効期限は、ユーザーに対し定期的にパスワードを変更させる仕組みです。パスワードの有効期限については、次の設定が可能です。

- 次にパスワードを変更するまでに使用可能な日数を指定
- パスワードが変更 (設定) されてから、次の変更が可能になるまでの日数を指定
- パスワードが有効期限に達する前の一定の日数、警告メッセージを表示するよう指定
- アカウントが使用可能な最大日数の指定

  そのアカウントに対し、ログインのないままその日数が経過すると、ユーザーのパスワードはロックされます。

さまざまな最大日数や期間に到達していても、それまでにすでにログインしているユーザーは、上記の機能には影響されないことを覚えておいてください。これらのユーザーは、通常どおりに作業を継続できます。パスワード有効期限に関する制限と動作は、ユーザーがログインした場合、または次の操作のうちの 1 つを実行した場合のみ実行されます。

- `login`

- `rlogin`
- `telnet`
- `ftp`

パスワード有効期限のパラメータは、ユーザー単位を基本として適用されます。また、ユーザーごとに異なるパスワード有効期限を設定できます。さらに、個別に有効期限を設定したユーザー以外のすべてのユーザーに適用される、一般的なデフォルトのパスワード有効期限パラメータを設定できます。

NIS+ の名前空間を計画する場合、実装したいパスワード有効期限の機能と指定したいデフォルト値を決定してください。パスワードの有効期限についての詳細は、『*Solaris* ネーミングの管理』のパスワードに関連する章を参照してください。

NIS+ グループの計画

NIS+ は、NIS にはない新しい種類のグループをネームサービス管理に導入します。NIS+ グループは、NIS+ アクセス権を一度にいくつかの NIS+ 主体に与える手段としてだけ使用します。またこれは、NIS+ の承認にだけ使用します。

NIS+ グループは、アクセス権が基準を置いている、4 つの承認クラスのうちの 1 つです。4 つの承認クラスは次のとおりです。

- 所有者

  NIS+ のオブジェクトにはすべて、単独のユーザーである所有者が 1 人存在します。所有者は、通常オブジェクトの作成者ですが、所有権を他のユーザーへ移すことができます。

- グループ

  ユーザーの集合に所定の NIS+ のアクセス権を与える目的で付けられたグループ名の元に集められたユーザーの集合です。

- その他

  認証されたすべてのユーザー、すなわち有効な DES 資格を持つユーザーのことです。定義によれば、オブジェクトの所有者およびオブジェクトのグループのメンバーは、それぞれの資格が有効である限り、その他クラスの一部でもあります。

- 未認証

有効な DES 資格を持たないユーザーのことです。他のクラスのメンバーの資格が、無効である、失われている、破損している、または見つからないのいずれかの場合、そのユーザーは未認証クラスに分類されます。

NIS+ スクリプトにより、アクセス権を与える目的で作成されたデフォルトのグループ名は、*admin* グループです。また、別の名前を付けて別のグループを作成することも、別のグループに別の NIS+ オブジェクトを割り当てることもできます。

あるオブジェクトグループのメンバーユーザーには、そのオブジェクトに特定の変更を行うアクセス権のような特権があります。たとえば、admin グループに何人かの見習い管理者を追加し、`passwd` テーブルと `hosts` テーブルだけを変更できるが、他のテーブルは変更できないようにすることができます。admin グループを使用すると、管理作業を、階層全体のスーパーユーザーだけに行わせるのではなく、多数のユーザーに分散させることができます。NIS+ admin グループには、NIS 互換モードでドメインを管理している場合でも、そのメンバーのために作成された資格がなければなりません。これは、認証を受けたユーザーだけが、NIS+ テーブルを変更するアクセス権を持つためです。

必要な資格の種類を確認したら、名前空間に必要なアクセス権を選択する必要があります。この作業を容易にするには、まずいくつの管理用のグループが必要かを決めます。複数のグループに異なる権利を割り当てたい場合は、独立したグループを使用すると便利です。通常、グループはドメイン別に作成します。各ドメインには、admin グループが 1 つだけなければなりません。

NIS+ グループとディレクトリへのアクセス権の計画

主体をグループに配置したあと、名前空間のオブジェクトによって、他のカテゴリの主体 (未認証、所有者、グループ、その他) だけでなく、これらのグループに許可されるアクセス権の種類を決めます。これらの割り当てを事前に決めておくと、一貫性のあるセキュリティの方針を確立するうえで役立ちます。

表 3–1 に示すように、NIS+ では名前空間の各オブジェクトに対してデフォルトのアクセス権を提供します。

表 3–1　NIS+ オブジェクトへのデフォルトのアクセス権

オブジェクト	未認証	所有者	グループ	その他
ルートディレクトリオブジェクト	r---	rmcd	rmcd	r---
ルート以外のディレクトリオブジェクト	r---	rmcd	rmcd	r---
groups_dir ディレクトリオブジェクト	r---	rmcd	rmcd	r---
org_dir ディレクトリオブジェクト	r---	rmcd	rmcd	r---
NIS+ グループ	----	rmcd	r---	r---
NIS+ テーブル	*varies*	*varies*	*varies*	*varies*

デフォルトのアクセス権を使用するか、または独自のアクセス権を割り当てることができます。独自のアクセス権を割り当てるときは、名前空間内のオブジェクトがどのようにアクセスされるかをよく考える必要があります。未認証クラスは、NIS+ クライアントからのすべての要求から構成されており、その要求は認証されていてもいなくても構わない、ということに注意してください。その他のクラスは、NIS+ クライアントからの認証を受けているすべての要求から構成されます。したがって、認証されていない要求に対し、名前空間へのアクセス権を与えたくなければ、未認証クラスへのアクセス権を割り当てず、その他のクラスだけを割り当てます。一方で、いくつかのクライアントが、たとえばアプリケーションを通して、認証されていない読み取り要求を出すことが予測されるときは、未認証クラスに読み取り権を割り当てる必要があります。NIS クライアントを NIS 互換モードでサポートしたい場合は、未認証クラスに読み取り権を割り当てなければなりません。

また、各種の名前空間オブジェクトが、最初に指定した NIS+ グループに割り当てる権利についても検討してください。名前空間の管理方法によって、利用できるアクセス権の一部またはすべてを、このグループに割り当てることができます。マスタサーバー上のユーザー root を、admin グループの所有者にすることをお勧めします。admin グループには、ルートドメインのオブジェクトに対する作成権と削除権が必要です。1 人の管理者にだけ、ルートドメインを作成、変更させたい場合は、その管理者だけを admin グループに所属するようにしてください。グループには、いつでもメンバーを追加することができます。設定を行う管理者が何人かいる場合は、

その管理者をすべてグループに追加して、そのグループにすべての権利を割り当ててください。その方が、所有者を切り替えたり元に戻したりするよりも簡単です。

オブジェクトの所有者にはすべての権利が与えられていなければなりません。ただし、グループにすべての権利が与えられていれば、このことはさほど重要ではありません。すべての権利を所有者にだけ与えると、名前空間のセキュリティ保護はより安全なものになります。しかし、管理グループにすべての権利を与えた方が管理は容易です。

NIS+ テーブルのアクセス権の計画

NIS+ テーブル以外の NIS+ オブジェクトは主に構造として存在するものですが、NIS+ テーブルは、種類の異なるオブジェクトであり、情報を伝えるものです。NIS+ テーブルへのアクセスは、すべての NIS+ 主体と、これらの主体に代わって実行されるアプリケーションで必要とされます。このため、NIS+ へのアクセス要件は若干異なります。

表 3–2 は、NIS+ テーブルに割り当てられるデフォルトのアクセス権を示しています。列が、テーブルの権利以外の権利を持つ場合は、それらの権利も示しています。テーブルとエントリのレベルの権利は、`nischmod` コマンドによって変更することができます。また、列レベルの権利は、`nistbladm -u` コマンドによって変更することができます。57ページの「暗号化されているパスワードフィールドの保護」には、テーブル権利を変更して異なる要求に応える方法の一例を示してあります。

表 3–2 NIS+ テーブルと列のデフォルトのアクセス権

テーブル / 列	未認証	所有者	グループ	その他
hosts テーブル	`r---`	`rmcd`	`rmcd`	`r---`
bootparams テーブル	`r---`	`rmcd`	`rmcd`	`r---`
passwd テーブル	`----`	`rmcd`	`rmcd`	`r---`
ユーザー名 (name) 列	`r---`	`----`	`----`	`----`
パスワード (passwd) 列	`----`	`-m--`	`----`	`----`

表 3–2　NIS+ テーブルと列のデフォルトのアクセス権　続く

テーブル / 列	未認証	所有者	グループ	その他
ユーザー ID (uid) 列	r---	----	----	----
グループ ID (gid) 列	r---	----	----	----
GCOS (gcos) 列	r---	-m--	----	----
ホームディレクトリ (home) 列	r---	----	----	----
ログインシェル (shell) 列	r---	----	----	----
シャドー (shadow) 列	----	----	----	----
group テーブル	----	rmcd	rmcd	r---
名前 (name) 列	r---	----	----	----
パスワード (passwd) 列	----	-m--	----	----
グループ ID (gid) 列	r---	----	----	----
メンバ (members) 列	r---	-m--	----	----
cred テーブル	r---	rmcd	rmcd	r---
cname 列	----	----	----	----
auth_type 列	----	----	----	----
auth_name 列	----	----	----	----
public_data 列	----	-m--	----	----
private_data 列	----	-m--	----	----
networks テーブル	r---	rmcd	rmcd	r---

表 3–2 NIS+ テーブルと列のデフォルトのアクセス権 続く

テーブル / 列	未認証	所有者	グループ	その他
netmasks テーブル	r---	rmcd	rmcd	r---
ethers テーブル	r---	rmcd	rmcd	r---
services テーブル	r---	rmcd	rmcd	r---
protocols テーブル	r---	rmcd	rmcd	r---
rpc テーブル	r---	rmcd	rmcd	r---
auto_home テーブル	r---	rmcd	rmcd	r---
auto_master テーブル		rmcd	rmcd	r---

注 - NIS 互換ドメインは、テーブルオブジェクトレベルの passwd テーブルに、未認証クラスの読み取り権を与えます。

暗号化されているパスワードフィールドの保護

表 3–2 を見るとわかるように、passwd テーブルを除くすべてのテーブルで、未認証クラスに読み取り権が与えられています。NIS+ テーブルは、未認証クラスの読み取りアクセス権を与えます。これは、NIS+ テーブルにアクセスする必要がある多くのアプリケーションが、認証されていないクライアントとして実行されるためです。ただし、passwd テーブルに対して同じことを行うと、暗号化されているパスワードの列が、認証されていないクライアントに公開されてしまいます。

表 3–2 に示す構成は、NIS 互換ドメインに対するデフォルトのアクセス権です。NIS 互換ドメインは、passwd 列に、未認証クラスの読み取りアクセス権を与えなければなりません。これは、NIS クライアントが認証されておらず、未認証クラスの読み取りアクセス権を与えないと、その passwd 列にアクセスできないためです。したがって、NIS 互換ドメインでは、パスワードが暗号化されていても、復号

化されやすい状態にあります。パスワードを、所有者以外には読めないようにしておくと、より安全になります。

標準の NIS+ ドメイン (NIS 互換ではない) には、さらに別のレベルのセキュリティがあります。 `nissetup` によって提供されるデフォルトの構成では、列ごとに制御する方法で、`passwd` 列を未認証ユーザーから保護しますが、`passwd` テーブルの残りの部分に対するアクセス権は与えられます。テーブルレベルでは、未認証の主体に読み取りアクセス権はありません。列レベルでは、`passwd` 列を除くすべての列への読み取りアクセス権があります。

エントリ所有者が、パスワード列に対するアクセス権を取得する方法について説明します。エントリ所有者は、各自のエントリに対する読み取り権と変更権の両方を持ちます。エントリ所有者は、その他のクラスのメンバーになることによって、読み取り権を取得します (テーブルレベルでは、その他のクラスに読み取り権があることに注意してください)。また、エントリ所有者は、列レベルでの明示的な割り当てによって、変更権を取得します。

テーブルの所有者とエントリの所有者は、同じ NIS+ 主体であることはほとんどなく、また同じである必要もないことに注意してください。したがって、所有者にテーブルレベルの読み取り権があっても、特定のエントリの所有者に読み取り権があるということではありません。

前に述べたように、これは、Solaris 2.3 以降のデフォルト設定です。テーブル、エントリ、列それぞれのレベルでのセキュリティの詳細については、『*Solaris* ネーミングの管理』を参照してください。

第 4 章

NIS 互換モードの使用方法

この章では、 NIS 互換モードについての概略を説明し、さらに NIS 互換モードで NIS+ を実行するときに発生する問題についても詳しく説明します。

NIS 互換モード

NIS と平行して NIS+ を実行するかどうか、実行する場合にはその方法、および停止する時を決定するのは、おそらくユーザーが直面する最も難しい移行問題の 1 つでしょう。 NIS+ には、 NIS といっしょに使用できる機能がいくつかありますが、中でも NIS 互換モードという機能があります。

NIS 互換モードを使用する計画がある場合、 NIS 互換モードで利用できる基本的な利点を考えておく必要があります。 NIS クライアントにはまったく変更を行う必要はありません。基本的な欠点は、完全な NIS+ セキュリティと階層を利用できないことと、クライアントのドメイン名を変更する必要があることです。

図 4–1 は、NIS だけの名前空間から、NIS と NIS+ の両方の要求に応じる名前空間に変換する方法を示しています。

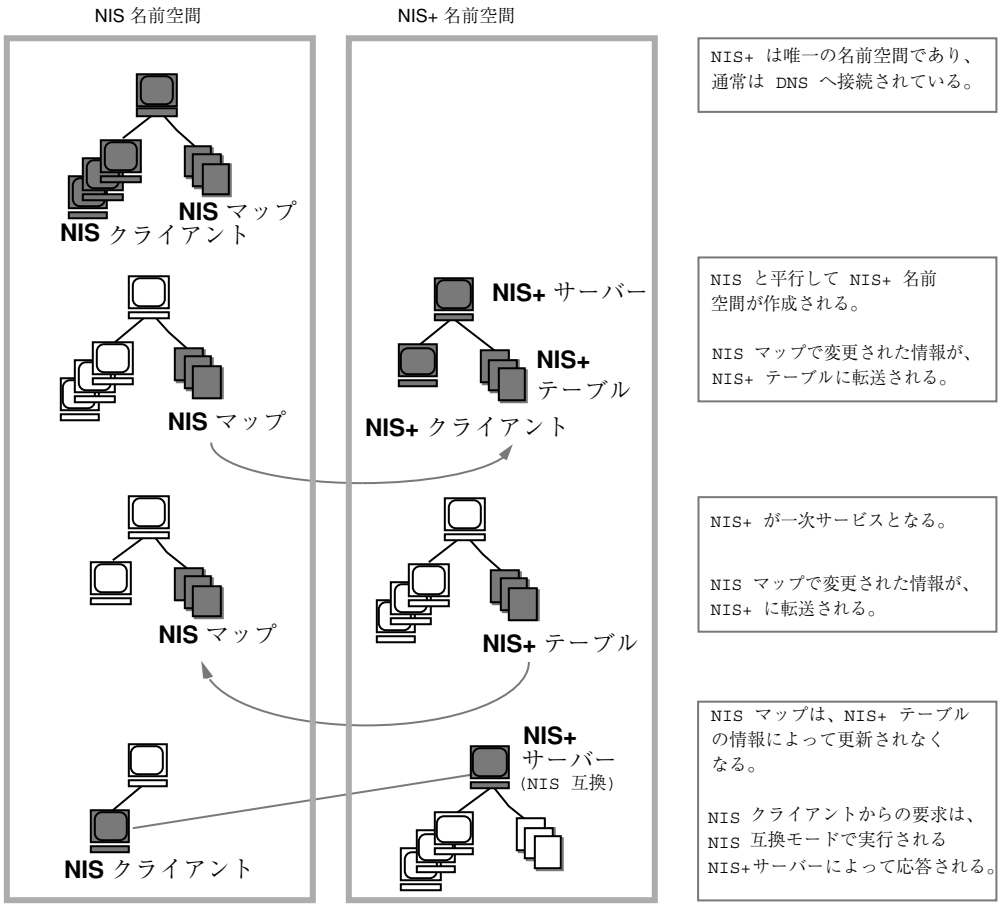

図 4–1　図 4-1 NIS　互換モードへの移行

NIS 互換になるドメインを選ぶ

NIS クライアントのリストを作成して、それらを最終的な NIS+ ドメインにグループ化してください。NIS 互換モードで管理される NIS+ ドメインの名前が、その NIS クライアントの元の NIS ドメインと異なる場合は、NIS クライアントのドメイ

ン名を、NIS 互換の NIS+ サーバーによってサポートされる NIS+ ドメインの名前に変更しなければなりません。

まず、NIS は間違いなく一次サービスです。情報共有の複雑さに慣れれば、NIS+ を一次サービスに移行する計画を立てることもできます。NIS+ ユーザーは、主な NIS ドメインと新しい NIS+ ドメインを切り替える機能を必要とする場合があります。`nisclient` スクリプトを使用すると、バックアップファイルが作成されるとき、この切り替えを行うことができます。

NIS 互換サーバーの構成を決める

NIS+ サーバーの要件を考慮した上で、各自の NIS サーバーについて判断を行います。最終的に、それらのサーバーを NIS+ サービスに使用する場合は、それらを NIS+ で推奨されるものに変更します。どの NIS サーバーを使用してどの NIS+ ドメインを、またどの機能 (マスタか複製か) でサポートするかを明らかにします。NIS+ サーバーは、それらがサポートするドメインよりも上位のドメインに属することを忘れないでください (ルートドメインサーバーは例外です)。NIS+ サーバーは、そのサービス対象となるドメインに属さないため、ドメインに依存する情報を必要とする他のサービスに、そのマシンを使用することはできません。

可能であれば、NIS+ サーバーマシンは、NIS+ にだけ使用するようにしてください。この構成では、DNS ネームサービス、ブートサーバー、ホームディレクトリ、NFS サーバーなどの他のネットワークサービスを、NIS+ ではないサーバーマシンに転送しなければならない可能性があります。

サイトの多くで、NIS サーバーは、NFS サーバー、計算サーバー、`rlogin` サーバー、mailhost サーバーなど、複数の役割を果たします。NIS サーバーは、そのクライアントと同じ情報を使用してその名前を解決するため、他のサービスも提供することができます。22ページの「ドメインの階層」で説明したように、ルートドメインを除くすべての NIS+ サーバーが、それがサービスを提供するドメインよりも上位のドメインに存在します。したがって、NIS+ サーバー上ではネームサービスを利用しなければならないサービスを実行しないようにするか、あるいは `nsswitch.conf` のファイルのような他の手段を使用して、これと同じ情報を取得してください。この問題は、階層がない場合には起こりません。この場合、NIS+ ルートサーバーは、そのサービス対象のドメイン内に存在します。NIS+ サーバーの資源の要件は、NIS サーバーの要件よりも大きいため、NIS+ とともに他のサービスを実行しないようにしてください。

Solaris 以外のマシンがネットワーク上にある場合は、NIS 互換モードで NIS+ サーバーを引続き使用することも、このようなマシンをすべて独自のドメインに移動させることもできます。Solaris 以外のマシンをすべて、1 つのサブネットに移動すると、NIS 互換クライアントの場合と同様に、同じサブネットに NIS+ サーバーがなければならないという制約をなくすことができます。これにより、ドメインに必要な複製サーバーの数が減ります。

サービス間で情報を転送する方法を決める

情報を同期させるには、一方の名前空間がもう一方の名前空間に従属する関係になるようにしてください。まず、NIS 名前空間を「主」とします。この場合、NIS マップを変更すると、次にその変更内容を「従」である NIS+ テーブルに反映します。したがって、NIS 名前空間がマスタデータベースになります。

NIS 互換モードの NIS+ サーバーは、標準の NIS マップをサポートします。これらのマップの完全なリストは、`ypfiles`(4) のマニュアルページの注意事項の節にあります。ただし、マップのサポートにはいくつかの制約があります。NIS+ サーバーは、ネットグループマップに対する `ypmatch` 要求には応じますが、逆マップに対する要求には応じません。また、`ypcat` などのネットグループマップの表示要求をサポートしません。`passwd.adjunct` マップもサポートしません。

最終的には NIS+ 名前空間が「主」になります。この場合は、NIS+ テーブルで変更を行って、それを NIS マップにコピーします。

NIS+ コマンドの `nisaddent` と NIS+ スクリプトの `nispopulate` を使用すると、表 4–1 に示すように、NIS マップと NIS+ テーブルの間で、情報を転送することができます。

表 4–1　passwd テーブルでの情報変更のためのコマンド

NIS+ コマンド	説明
/usr/lib/nis/nisaddent -y	ypxfr を実行して、NIS サーバーからローカルディスクへマップを転送した後で、NIS マップから NIS+ テーブルへ情報を転送する。標準以外の NIS マップは、情報がキーと値のペアになっていれば、NIS+ テーブルに転送できる。複数列のマップは転送されない
/usr/lib/nis/nisaddent -d	NIS+ テーブルからファイルへ情報をコピーする。この情報は、標準 NIS ユーティリティを使って、さらに NIS マップに転送することができる
/usr/lib/nis/nispopulate -Y	NIS マップから NIS+ テーブルへ情報を転送する

Solaris 2.5 より前のリリースの NIS+ のバージョンでは、ユーザーのパスワード情報が /etc 内のファイル、NIS マップ、NIS+ テーブルのどこに格納されているかによって、別々のパスワードコマンド (passwd、yppasswd、nispasswd) を使用して、パスワード関連の処理を行う必要がありました。Solaris 2.5 からは、パスワード関連の処理をすべて passwd または passwd −r nisplus のコマンドで自動的に行うとともに、ユーザーの nsswitch.conf ファイルの passwd エントリによって管理することになりました。

NIS+ または NIS 互換のネットワーク上に、passwd コマンドとパスワードの有効期限を正しく設定するには、各マシン上の nsswitch.conf ファイルの passwd エントリが正しくなければなりません。このエントリによって、passwd コマンドがパスワード情報を取得する場所と更新する場所が決まります。

次の 5 つのパスワードエントリ構成のみが使用できます。

例 4–1　nsswitch.conf ファイルにおける使用可能な passwd エントリ

```
passwd:files

passwd: files nis

passwd: files nisplus

passwd: compat
```

(続く)

```
passwd_compat: nisplus
```

注意 - 使用しているネットワークのワークステーション上に存在するすべての nsswitch.conf ファイルは、必ず上記の passwd 構成のうちの 1 つを使用していなければなりません。別の方法で、passwd エントリを構成した場合、ユーザーがログインできない可能性があります。

DNS 転送を実装する方法を決める

NIS サーバーは、Solaris 1.x の NIS クライアントからの DNS 要求を転送することができます。 NIS 互換モードで実行される NIS+ サーバーにも、DNS 転送機能がありますが、Solaris 2.3 以降のリリースからしか使用できません (この機能は、パッチ#101022-06 を使用すれば、Solaris 2.2 でも使用できます)。このため、Solaris 2 または Solaris 7 オペレーティング環境で動作している NIS クライアントは、/etc/nsswitch.conf ファイルと /etc/resolv.conf ファイルをローカルに設定しておく必要があります。

NIS 互換モードで実行される Solaris 2.0 または 2.1 のサーバーによってサポートされている Solaris 1.X NIS クライアントは、DNS 転送を利用することができません。これらのサーバーは、Solaris 2.3 以降のリリースにアップグレードする必要があります。

DNS ドメインの区分を再度作成するときは、新しい DNS ゾーンファイルを定義しなければなりません。ただし、クライアントによっては、/etc/resolv.conf ファイルの変更が必要な場合があります。クライアントが DNS クライアントでもある場合は、そのネームサービススイッチ構成ファイルを設定して、NIS+ テーブルだけでなく、DNS ゾーンファイルまたは NIS マップのホスト情報を検索することができます。

NIS+ クライアントの DNS 転送

NIS+ クライアントは、NIS クライアントのような暗黙の DNS 転送機能を持ちません。そのかわり、ネームサービススイッチを使用することができます。NIS+ クライアントに DNS 機能を与えるには、その hosts エントリを次のように変更してください。

```
hosts: nisplus dns [NOTFOUND=return] files
```

Solaris 2 または Solaris 7 オペレーティング環境の NIS クライアントの DNS 転送

NIS クライアントが、*NIS* 互換の NIS+ サーバーの DNS 転送機能を使用している場合、そのクライアントの nsswitch.conf ファイルは、hosts エントリに次の構文があってはいけません。

```
hosts: nis dns files
```

DNS 転送では、ホスト要求が DNS に自動的に転送されるため、この構文があると、NIS+ サーバーとネームサービススイッチの両方が、不必要な要求を DNS サーバーに転送してしまいます。この結果、性能が低下します。

Solaris 1、Solaris 2、Solaris 7 における NIS コマンドと NIS+ コマンドの比較

この節で示す表を見ると、Solaris 1 オペレーティング環境の NIS コマンド、Solaris 2 または Solaris 7 オペレーティング環境の NISコマンド、およびそれに対応する NIS+ コマンドの間の違いがわかります。

- 表 4–2 は、Solaris 2 および Solaris 7 でサポートされている NIS コマンドを示しています。
- 表 4–3 と表 4–4 は、Solaris 2 および Solaris 7 の NIS クライアントとサーバーのコマンドに対応する NIS+ コマンドを示しています。

- 表 4–5 には、NIS アプリケーションプログラマ用のインタフェース関数と、それに対応する NIS+ API が示されています。詳細については、該当するマニュアルページを参照してください。

Solaris 2 および Solaris 7 でサポートされている NIS コマンド

Solaris 2 および Solaris 7 では、一部の NIS コマンドだけがサポートされています。NIS サーバーコマンドは、Solaris 2 および Solaris 7 では提供されません。NIS クライアントコマンドだけがこのリリースに含まれています。これらの NIS コマンドが実行されるかどうかも、Solaris 2 または Solaris 7 の NIS クライアントが、NIS サーバーまたは NIS 互換モードの NIS+ サーバーにサービスを要求するかどうかによって決まります。NIS クライアントは、NIS 互換モードで実行されている NIS+ サーバーに更新を依頼することができません。たとえば、このようなクライアントは、chkey、newkey の各コマンドを実行することができません。表 4–2 は、Solaris 2 および Solaris 7 でサポートされている NIS コマンドの一覧です。

表 4–2　Solaris 2 および Solaris 7 オペレーティング環境でサポートされる NIS コマンド

コマンドの種類	**Solaris 2** および **7** でサポートされる **NIS** コマンド	**Solaris 2** および **7** でサポートされない **NIS** コマンド
ユーティリティ	`ypinit ypxfr ypcat ypmatch yppasswd ypset ypwhich`	`yppush yppoll ypchsh ypchfn ypmake`
デーモン	ypbind	`ypserv ypxfrd rpc.ypupdated rpc.yppasswdd`
NIS API	`yp_get_default_domain()`	`yp_order() yp_update()`
	`yp_bind()`	
	`yp_unbind()`	
	`yp_match()`	
	`yp_first`	
	`yp_next()`	
	`yp_all()`	
	`yp_master()`	
	`yperr_string()`	
	`ypprot_err()`	

クライアントコマンドとサーバーコマンドの対応

この節で示す 2 つの表には、NIS コマンドと、それに相当する NIS+ コマンドを示してあります。これらのコマンドは、2 つのカテゴリに分けられます。表 4–3 では、ネームサービスクライアントからネームサービスサーバーへのコマンドを示しています。 表 4–4 では、ネームサービスサーバーからネームサービスサーバーへのコマンドを示しています。

対応するクライアントコマンド

表 4–3 では、ネームクライアントからネームサーバーへのコマンドを示しています。これらのコマンドを、ネームサービスのクライアントマシン上で入力してネームサービスサーバーの情報を要求します。表の 1 列目のコマンドは、Solaris 1 の NIS サーバーに接続されている、 Solaris 1、Solaris 2 または Solaris 7 の NIS クライアントで実行されます。表の 2 列目のコマンドは、 NIS 互換モードで実行されている Solaris 2 または Solaris 7 の NIS+ サーバーに接続されている、 Solaris 1、Solaris 2 または Solaris 7の NIS クライアント上で実行されます。表の 3 列目のコマンドは、 Solaris 1 または Solaris 7 の NIS+ サーバーに接続されている、Solaris 2 または Solaris 7 の NIS+ クライアント上でのみ実行されます。1 つの行に示されたコマンドは、ほぼ同じ機能を持ちます。「なし」は、対応するコマンドがないことを示しています。

表 4–3 NIS クライアントコマンドと対応する NIS+ コマンド

SunOS 4.*x* NIS サーバー	**NIS** 互換モードの **NIS+** サーバー	**NIS+** サーバー
`ypwhich -m`	`ypwhich -m`	`niscat -o org_dir`
`ypcat`	`ypcat`	`niscat`
`ypwhich`	`ypwhich`	なし
`ypmatch`	`ypmatch`	`nismatch/ nisgrep`
`yppasswd`	`passwd`	`passwd`
`ypbind`	`ypbind`	なし
`yppoll`	なし	なし
`ypset`	`ypset`	なし
なし	`ypinit -c`	`nisclient -c`

以下の点に注意してください。

- Solaris 2.5 では、passwd コマンドは NIS または NIS+ の状態に関係なく使用できます。以前 nispasswd および yppasswd コマンドによって実行していた機能は、このリリースでは passwd コマンドに含まれました。
- ypinit –c コマンドは、Solaris 2 または Solaris 7 の NIS クライアント上でのみ使用できます。
- ypcat コマンドは、netgroup テーブルに対する照会ではサポートされません。NIS クライアントの要求は、応答が返される前に時間切れになります。これは、このテーブルの形式が、netgroup NIS マップの形式と大幅に異なるためです。

対応するサーバーコマンド

表 4–4 では、ネームサーバーからネームサーバーへのコマンドを示しています。NIS サーバーコマンドは、Solaris 2 または Solaris 7 に含まれていないため、NIS+ サーバーにも NIS 互換モードの NIS+ サーバーにも使用できません。また、NIS サーバーは、NIS+ サーバーに変更を依頼することができません。この逆もできません。このテーブルの 3 番目の列には、最初の列の NIS サーバーコマンドに対応する NIS+ サーバーコマンドが示されています。NIS 互換モードはクライアントコマンドだけを参照するため、NIS 互換モードのサーバーには同じ機能を提供するコマンドはありません。

表 4–4 NIS サーバーコマンドと対応する NIS+ コマンド

SunOS 4.*x* NIS サーバー	**NIS** 互換モードの **NIS+** サーバー	**NIS+** サーバー
ypxfr	なし	なし
makedbm	なし	nisaddent
ypinit -m ypinit -s	なし	nisserver
ypserv	rpc.nisd -Y	rpc.nisd
ypserv -d	rpc.nisd -Y -B	DNS 転送は不要、/etc/nsswitch.conf を使用すること
ypxfrd	なし	なし
rpc.ypupdated	なし	なし

表 4–4　NIS サーバーコマンドと対応する NIS+ コマンド　続く

SunOS 4.*x* NIS サーバー	**NIS** 互換モードの **NIS+** サーバー	**NIS+** サーバー
`rpc.yppasswd`	`rpc.nispasswdd`	`rpc.nispasswdd`
`yppush`	なし	`nisping`
`ypmake`	なし	`nissetup`、`nisaddent`
`ypxfr`	なし	なし

NIS と NIS+ の API 関数の対応

サイトを完全に NIS+ に移行するには、ネームサービスを変更するだけでなく、すべてのアプリケーションを NIS+ に移植する必要があります。NIS の呼び出しを行う、サイトの内部で作成されたアプリケーションはすべて、NIS+ の呼び出しを実行するように変更しなければなりません。そうしないと、常に NIS 互換モードで NIS+ サーバーを実行しなければならず、このモードの欠点をすべて抱えることになります。サイトの外部で作成されたアプリケーションでは、必要な変更が行われるまで、NIS 互換モードで名前空間を管理しなければならないことがあります。

表 4–5 では、NIS API 機能と、それに対応する NIS+ API 機能を示しています。

表 4–5　NIS の API の関数と NIS+ の API の関数の対応

NIS API の関数	**NIS API** の関数
`yp_get_default_domain()`	`nis_local_directory()`
`ypbind()`	なし
`ypunbind()`	なし
`ypmatch()`	`nis_list()`
`yp_first()`	`nis_first_entry()`

表 4–5　NIS の API の関数と NIS+ の API の関数の対応　続く

NIS API の関数	NIS API の関数
yp_next()	nis_next_entry()
yp_all()	nis_list()
yp_master()	nis_lookup()
yperr_string()	nis_perror() nis_sperrno()
ypprot_err()	nis_perror() nis_sperrno()
yp_order()	なし
yp_update()	nis_add_entry()、nis_remove_entry()、nis_modify_entry()

NIS 互換モードのプロトコルサポート

表 4–6 は、NIS 互換モードで動作する NIS+ サーバー によってサポートされる NIS プロトコルについて示しています。

表 4–6　NIS+ サーバーによる NIS プロトコルのサポート

NIS プロトコル	互換性についての説明
NIS クライアント V2 プロトコル	サポートしている
NIS サーバー間プロトコル (NIS server-to-server プロトコル)	サポートしていない

表 **4–6** NIS+ サーバーによる NIS プロトコルのサポート 続く

NIS プロトコル	互換性についての説明
NIS クライアント更新プロトコル	`yppasswd`プロトコルをサポートしている
NIS クライアント V1 プロトコル	`YPPROC_NULL`、`YPPROC_DOMAIN`、`YPPROC_DOMAIN_NONACK` を 除き、サポートしていない

第 5 章

移行の準備

この章では、移行を始める前に実行しなければならないいくつかの作業について説明します。

他のシステムに対する NIS+ の影響を調べる

システム管理者を教育するだけでなく、サイトで NIS+ を紹介し、テストを行い、NIS+ に習熟できるような教育を行なってください。また、NIS+ への移行によって

影響を受ける他のシステムやアプリケーションの NIS への依存関係を調べてください。

たとえば、アプリケーションの中には、NIS マップの一部に依存するものがあります。これらのアプリケーションが標準 NIS+ テーブルまたはカスタム NIS+ テーブルのどちらで機能するか、また、それらのアクセスの必要性によりセキュリティ計画全体にどのような影響が及ぶかを調べてください。

さらに、サイトで使用される標準以外の NIS マップはどれか、また、それらのマップを NIS+ テーブルに変換するかあるいは標準以外の NIS+ テーブルを作成して、情報を格納できるかを調べてください。アクセス権をチェックする必要もあります

各サイトで、NIS に依存する、ローカルで作成したアプリケーションを使用するかどうかも調べます。また、`yp_match()` 関数の呼び出しが埋め込まれているかどうかなど、直接 NIS を呼び出すコマンドやアプリケーションがあるかどうかも調べる必要があります (詳細については、70ページの「NIS と NIS+ の API 関数の対応」を参照してください)。

名前空間でユーザー名とホスト名が重複していないかチェックしてください (詳細については、45ページの「ユーザー名とホスト名の重複の解決」を参照してください)。

NIS+ への移行がネットワークのインストール手順に与える影響も調べます。もし影響があれば、必要な変更を分析してください。 NIS+ のサイト管理作業に対する影響を調べると、発生する可能性がある障害を事前に明らかにすることができます。

システム管理者の教育

18ページの「NIS+ について理解する」 で説明した紹介と教育プログラムのもう 1 つの目的として、各サイトの管理者に NIS+ の概念を理解してもらい、作業手順に慣れる機会を与えるということがあります。教室での学習だけでは不十分です。システム管理者には、業務に支障をきたさない環境で作業する機会が必要です。この教育には、次の内容が含まれます。

- NIS+ の正しい概念と管理を教えるコース
- 基本的な NIS+ の障害追跡情報とその実習
- 各サイトの実装方針と計画に関する情報

ユーザーへの事前の連絡

NIS+ へのクライアントの移行を実際に開始するかなり前から、ユーザーに事前に移行についての連絡を行なってください。実装の計画を伝え、詳細を入手する方法を提供してください。第 1 章 で説明したように、移行の主な目的の 1 つは、クライアントに対する移行の影響を最小限に抑えるということですが、当然ユーザーは新しい変更に気づく場合があります。このような場合には、電子メールで通知を送って、情報セミナーの開催を知らせ、ユーザーが質問を送信できる電子メールの別名または個人名を指定してください。

必要な変換ツールとプロセスを明らかにする

移行のツールを作成または入手して、実装に利用してください。各サイトですでに自動化ツールを使用して、個々のシステムやネットワークサービスを管理している場合は、それらを移植して、移行に使用するバージョンの Solaris ソフトウェアや NIS+ で動作するようにしてください (17ページの「1 種類のソフトウェアリリースを使用する」を参照)。次に、スクリプトを作成する際の推奨事項を示します。

- NIS+ へユーザーを移行させるためのスクリプト - `nisclient` シェルスクリプトに追加を行う
- ユーザーの NIS+ 環境を確認するチェックスクリプト
- バックアップ、復元スクリプト
- 日常的な NIS+ 管理の `crontab` エントリ
- 障害通知手順

このようなスクリプトを作成すると、ドメイン全体で一貫した移行を行い、移行の効率をあげて、問題を減らすことができます。また、名前空間全体のすべてのクライアントで使用できるような `nsswitch.conf` といった一連の標準構成ファイルとオプションを用意する必要もあります。

移行に使用される管理用のグループを明らかにする

移行の際に調べた管理資源に対応する名前空間の設計 (51ページの「パスワード有効期限の基準、原則、および規則を確立する」 を参照) の一部として、NIS+ グループが作成されたことを確認してください。NIS+ 名前空間の日常的な操作に使用されるもの以外の NIS+ グループを、移行に使用することもできます。リモートの管理者の援助が至急必要な場合には、グループにこれらの管理者を追加してください。

グループのメンバーに正しい資格があり、名前空間オブジェクトがグループに正しいアクセス権を承認していることを確認してください。また、その適切なグループが、適切な名前空間オブジェクトのグループ所有者として識別されることを確認してください。

表 5–1 は、NIS+ グループで使用できるコマンドとグループアクセス権をまとめたものです。

表 5–1 グループ用の NIS+ コマンド

コマンド	説明
`nisgrpadm`	グループを作成または削除し、メンバーを追加、変更、一覧表示、削除する
`niscat -o`	NIS+ グループのオブジェクト属性値を表示する
`nissetup`	ドメインのグループが格納されているディレクトリの基本構造を作成する
`nisls`	ディレクトリの内容を一覧表示する
`NIS_GROUP`	シェルで設定されている `nisdefaults` の値を上書きする環境変数
`nischmod`	オブジェクトのアクセス権を変更する
`nischown`	NIS+ オブジェクトの所有者を変更する
`nischgrp`	NIS+ オブジェクトのグループ所有者を変更する

表 5–1　グループ用の NIS+ コマンド　続く

コマンド	説明
`nistbladm -u`	NIS+ テーブルの列へのアクセス権を変更する
`nisdefaults`	現在の NIS+ のデフォルトを表示、または変更する

ドメインの所有者を決める

ドメイン階層の機能を十分利用するには、ドメインの所有権を、それらのドメインをサポートしている組織に分散させてください。これにより、ルートドメインの管理者が、ローカルレベルの基本的な作業を行わなくてもすむようになります。 誰が何を所有しているのかがわかれば、管理用のグループを作成するための指針を用意して、オブジェクトへのアクセス権を設定することができます。

NIS+ ドメインの所有権と DNS ドメインの所有権をどのように調整するかを検討してください。次のいくつかの指針を示します。

- DNS ドメイン構造の管理には、サイトの最上位レベルの管理用のグループの作業を含みます。
- これと同じ管理用のグループが、最上位のレベルの NIS+ ドメインを所有します。
- 下位レベルの DNS ドメインと NIS+ ドメインの管理責任は、上位レベル管理グループによって、個々のサイトに委任されます。NIS+ ドメインが、DNS ドメインと同じ設計で作成される場合 (たとえば地理的に構成されるなど)、この委任は説明しやすいものになります。

資源の利用度を調べる

実装にどの管理資源が必要かを調べます。これらの資源は、通常の NIS+ の操作に必要な資源をはるかに超えます。移行を行うときに、NIS+ と NIS の互換性が必要な期間が長期に及ぶ場合は、さらに資源が必要になります。

名前空間の設計を実装する作業だけでなく、多くのクライアントを移行して、特殊な要求や問題を処理する作業についても検討してください。このとき、NIS+ の習得にかなり時間がかかることを考慮に入れておいてください。NIS+ でサポート作業を行う場合、NIS で作業していたときとくらべて、しばらくの間、管理者の作業効率がやや低下する場合があります。このため、通常の教育だけでなく、実習経験をともなう上級コースの研修を受けることも検討してください。

さらに、移行が完了した後でも、管理者は、NIS+ をサポートするための毎日の作業に慣れるまでに若干の時間を要します。

ハードウェア資源についても検討してください。NIS サーバーは、経路指定、印刷、ファイル管理などの他のネットワークサービスをサポートするために使用されることがよくあります。NIS+ サーバーにかかる可能性のある負荷を考えて、専用の NIS+ サーバーを使用する必要があります。このように負荷を分散すると、障害追跡と性能監視が簡単になるため、移行が簡略化されます。もちろん、システムを追加するとコストがかかります。必要なサーバーの数と、その構成方法については、第 2 章に説明があります。

これらのサーバーは、NIS サーバーの他に必要であることを忘れないでください。NIS サーバーは、移行が完了すると、必要なくなるか、あるいは他の用途で使用される場合がありますが、 NIS+ サーバーは引き続き使用されます。

ログイン名とホスト名の衝突を解決する

NIS+ 認証では、ワークステーションとユーザーが、1 つのドメイン内で同じ名前を使用することはできません。たとえば、joe@joe は使用できません。NIS+ は、ホストの資格とログイン名の資格を区別しないため、1 つの名前に 1 種類の資格を使用するだけですみます。名前空間に重複した名前があり、何らかの理由でその重複したホスト名を維持しなければならないときは、次のように変更してください。つまり、ユーザーログイン名をそのままにして、重複したホスト名を別名に指定します。ホストに新しい名前を作成して、古い名前を新しい名前の別名として使用します。無効な名前の組み合わせの例については、45ページの「ユーザー名とホスト名の重複の解決」 を参照してください。

名前の衝突を解決してから実装を開始する必要がありますが、通常の NIS+ 操作中、新しいワークステーションとユーザーの名前を常時チェックする計画をたてる必要もあります。これには、`nisclient` スクリプトを使用してクライアントの資格を作成すると、名前の比較が行われます。

すべての情報源となるファイルを調べる

/etc 内のファイルと NIS マップをすべて調べて、空のフィールドやこわれているデータがないかを確認してから、NIS+ を構成してください。NIS+ テーブルの生成スクリプトとコマンドは、データファイルに空のフィールドや余分な文字があると、正常に実行されない場合があります。空フィールドを埋めるか、またはデータを修正してから、作業を開始してください。NIS+ スクリプトをそのまま実行してデータを破壊する危険をおかすよりも、問題のあるユーザーやマシン名を /etc 内のファイルや NIS マップから削除してから、 NIS+ スクリプトを実行して、NIS+ のインストール後にそれらを戻すことをお勧めします。

ホスト名から “.” を削除する

NIS+ では、マシン名とドメインの区切りや親ドメインとサブドメインとの区切りにドット (ピリオド) を使用するため、ドットを含むマシン名 (ホスト名) を付けることはできません。NIS+ へ移行するにあたって、ホスト名からドットを必ず削除する必要があります。ドットの代わりにハイフン (-) を使用できます。たとえば、sales.alpha というマシン名を付けることはできません。この名前は、sales-alpha に置き換えることができます (使用可能なホスト名の詳細については、hosts のマニュアルページを参照してください)。

NIS マップ名から “.” を削除する

第 2 章で説明したように、NIS+ のオートマウンタテーブルでは、その名前とファイル内容の “.” が下線で置き換えられています。この変更は、移行中に使用する NIS マップの名前に対しても行う必要があります。この変更を行わないと、NIS+ は、名前の “.” を、オブジェクト名のドメインレベルを区別するピリオドと混同します。

注 - オートマウンタだけでなく、すべての NIS マップの「.」を必ず下線に変換してください。ただし、標準以外の NIS マップの名前をドットから下線に変更した場合、標準以外のマップを使用するアプリケーションを、NIS+ 構文を認識するように変更しないと、そのアプリケーションに障害が生じるおそれがあります。

既存の NIS 名前空間を文書化する

現在の構成を文書化しておくと、移行を開始する開始点を明確にすることができます。次の項目のリストを作成してください。

- 現在のすべての NIS ドメインとネットワークの名前と位置
- 現在のすべての NIS サーバー (マスタとスレーブの両方) のホスト名と位置
- 現在のすべての NIS サーバーの構成

  次のものが含まれます。

  - ホスト名
  - CPU の種類
  - メモリーサイズ
  - 使用可能なディスク容量
  - root アクセス権を持つ管理者の名前

- 標準以外の NIS マップ

NIS クライアントのリストと、最終的な NIS+ ドメインを対応させてください。これらは、Solaris オペレーティング環境にアップグレードする必要があります。

NIS サーバーの移行計画を作成する

NIS サーバーについてよく考慮します。移行が完了した後でも NIS サーバーを他の用途に使用することができますが、「両方」のサービスにサーバーを必要とする段階があることを忘れないでください。したがって、既存の NIS サーバーを使って、すべての NIS+ サーバーの必要を満たす計画を立てることはできません。

NIS サーバーの詳しい移行計画を作成して、NIS+ に使用される NIS サーバーと、その移行時期を明らかにしておくと役立ちます。NIS から NIS+ への移行の初期段階では、NIS サーバーを NIS+ サーバーとして使用しないでください。第 6 章で説明するように、名前空間全体に対する作業を調べてからクライアントを NIS+ に移行すると、大抵の場合安定した実装を行うことができます。

NIS サーバーを NIS+ ドメインに割り当てて、各サーバーの役割 (マスタまたは複製) を明らかにしてください。NIS+ サービスへの移行を計画しているサーバーを指

定したら、それらを NIS+ の要件に合わせてアップグレードしてください (34ページの「サーバーメモリーの容量」を参照)。

第 6 章

移行の実施

この章では、NIS+ 名前空間の設定に必要な作業を、いくつかの段階に分けて説明します。

移行の実施

前の章で説明した作業を実行すれば、手のかかる仕事はほとんど終わったことになります。ここでしなければならないことは、設計した名前空間の設定と、クライアントの追加だけです。この章では、これらの処理を行う方法について説明します。これらの手順を実行するにあたっては、移行前の準備作業すべてが完了していて、各サイトのユーザーが移行の計画を了解していることを確認してください。

NIS+ ドメインを DNS ドメインと並行して使用する場合は、各 DNS ドメインに 1 つの NIS+ サブドメインを設定します。最初の DNS ドメインに完全な NIS+ 名前空間を設定して、すべてが正しく動作していることを確認したら、別の NIS+ 名前空間を並行して設定することができます。

第 1 段階 - NIS+ 名前空間を設定する

ドメインを NIS 互換モードで管理している場合でも、完全な DES 認証を備えた名前空間を設定してください。『*Solaris* ネーミングの設定と構成』に記載された NIS+ スクリプトを使用して、名前空間を設定します。基本的な手順の詳細については、『*Solaris* ネーミングの管理』を参照してください。そして、次の手順に従ってください。

1. ルートドメインを設定します。

   NIS 互換モードでルートドメインを管理する場合は、`nisserver` を使用します (セットアップスクリプトを使用しない場合は、`rpc.nisd` および `nissetup` に `–y` フラグを付けて使用してください)。

2. ルートドメインテーブルを生成します。

   NIS マップまたはテキストファイルから、 `nispopulate` を使用して、情報を転送することができます。もちろん、 `nistbladm` や `nisaddent` を使用して、同時に複数のエントリを作成することもできます。

3. ルートドメインのクライアントを設定します。

   ルートドメインに 2、3 のクライアントを設定して、その操作を正しくテストできるようにします。完全な DES 認証を使用してください。これらのクライアントコンピュータの中には、後でルートの複製サーバーに変換されたり、ルートドメインをサポートする管理者のワークステーションとして機能するものがあります。NIS+ サーバーは、個人用のワークステーションにはなりません。

4. サイト固有の **NIS+** テーブルを作成、または変換します。

   新しい NIS+ ルートドメインにサイト固有のカスタム NIS+ テーブルが必要な場合は、 `nisaddent` を使用してそれらのテーブルを作成し、 `nistbladm` を使用して、それらのテーブルに NIS データを転送します。

5. ルートドメインのグループに管理者を追加します。

   管理者には、LOCAL 資格と DES 資格が必要です (`nisaddcred` を使用します)。管理者のワークステーションは、ルートドメインのクライアントでなければなりません。また、管理者のルート識別情報は、DES 資格を持つ NIS+ クライアントでなければなりません。

6. 必要に応じて、sendmailvars テーブルを変更します。

   新しいドメイン構造の結果、電子メール環境が変更された場合は、新しいエントリを使って、ルートドメインの sendmailvars テーブルを生成します。

7. ルートドメインの複製サーバーを設定します。

   まず、クライアントをサーバーに変換します (NIS 互換のために rpc.nisd に –Y オプションを使用し、DNS 転送が必要な場合は –B も使用します)。次に、nisserver –R. を使って、それらのサーバーをルートドメインに関連づけます。

   NIS 互換の場合は、 rpc.nisd に –Y オプションを使用して実行します。そして、 /etc/init.d/rpc ファイルを編集して、EMULYP 行からコメント記号 (#) を削除します。DNS 転送の場合は、rpc.nisd に –B オプションを使用します。

8. ルートドメインの動作をテストします。

   一連のインストール固有のテストルーチンを作成して、NIS+ に切り替えた後に、クライアントの機能を確認します。これにより、移行処理の効率が向上して、問題が減ります。このドメインをおよそ 1 週間操作してから、他のユーザーを NIS+ に移行してください。

9. 名前空間の残りを設定します。

   これ以上クライアントを NIS+ に移行しないで処理を進め、ルートドメインの下にある他のドメインをすべて設定します。これには、マスタサーバーと複製サーバーの設定も含まれます。新しい各ドメインを、ルートドメインの場合と同様に完全にテストして、構成とスクリプトが正しく機能することを確認します。

10. 名前空間の動作をテストします。

    保守、バックアップ、復元などのすべての操作手順をテストします。名前空間内のすべてのドメイン間での情報共有処理をテストします。NIS+ 全体の操作環境を検査し終わるまでは、第 2 段階に進まないでください。

11. **NIS+** ドメインのセキュリティ構成をカスタマイズします。

    これは、すべてが正しく機能していれば必要ありません。ただし、不正なアクセスから保護したい情報がある場合は、NIS+ テーブルのデフォルトアクセス権を変更して、 NIS クライアントであっても、それらの情報にアクセスできないようにすることができます。また、NIS+ グループのメンバーの関係と NIS+ の構成オブジェクトのアクセス権を再構成して、管理責任を割り当てることもできます。

第 2 段階 - NIS+ 名前空間を他の名前空間に接続する

1. ルートドメインを **DNS** 名前空間に接続します **(**任意**)**。

   NIS+ クライアントは、ネームサービススイッチを使って、Internet に接続することができます。ワークステーションが DNS クライアントでもある場合、そのネームサービススイッチ構成ファイルを設定して、NIS+ テーブルや NIS マップだけでなく、DNS ゾーンファイル内の情報を検索することもできます。

   各クライアントの `/etc/nsswitch.conf` ファイルと `/etc/resolv.conf` ファイルを正しく構成してください。 `/etc/nsswitch.conf` ファイルは、クライアントのネー ムサービススイッチ構成ファイルです。 `/etc/resolv.conf` には、クライアントの DNS の IP アドレスを列挙します。これは『*Solaris* ネーミングの設定と構成』で説明されています。

2. **NIS+** と **DNS** の共同操作をテストします。

   情報への要求を複数の名前空間の間で、問題なく渡せることを確認します。

3. **NIS+** を **NIS** と並行して操作している場合は、情報の転送をテストします。

   `nispopulate` スクリプトを使用して、NIS から NIS+ へ情報を転送します。NIS+ から NIS へデータを転送するには、 `nisaddent -d` を実行後、 `ypmake`を実行します (詳細についてはマニュアルページを参照してください)。 スクリプトを使用して、この処理を自動化します。テーブル、特に `hosts` テーブルと `passwd` テーブルを同期させる方針を設定します。NIS 環境と NIS+ 環境の間で整合性を維持するために使用するツールをテストします。NIS+ テーブルを実際の情報源にする時期を決めます。

4. **DNS** と **NIS** の両方との **NIS+** の操作をテストします。

   3 つの名前空間をすべて一緒にテストして、追加した接続に問題がないことを確認します。

第 3 段階 - NIS+ 名前空間を十分に稼働させる

1. クライアントを **NIS+** に移行します。

   一度に 1 つのワークグループのクライアントを移行して、1 つのサブネット内のワークグループをすべて移行してから、他のサブネットでの移行を行います。このように、1 つのサブネット内のクライアントをすべて移行したら、そのサブネット上の NIS サービスを削除することができます。各クライアントを移行したら、検査スクリプトを実行して、移行が正しく行われたことを確認します。この検査スクリプトは、ユーザーに対して、問題とその問題の報告に役立つサポート形態を通知します。実際に必要は手順は、サイトによって異なります。

   `nisclient` スクリプトを使用して、NIS クライアントを NIS+ クライアントに移行します。クライアントの DNS 構成を変更する必要がある場合は、独自のスクリプトを作成して、その処理を自動化しなければなりません。

   `/usr/local` のような共有の、マウントされるディレクトリがサイトにあれば、時間を節約することができます。このディレクトリにスクリプトを置いて、移行時に、このスクリプトをスーパーユーザーとして実行するよう依頼する電子メールをクライアントに送ることができます。

2. クライアントの移行中、移行の状況を監視します。

   計画と突き合わせて進行状況を追跡し、計画段階では予測できなかった重大な問題がないかを監視します。状況を通知して、関係するグループがそれを追跡できるようにします。

3. **NIS** サーバーを削除します。

   サブネット上のすべてのクライアントが NIS+ に移行されたら、NIS サーバーを削除します。特定のサブネットに、NIS サービスを必要とするクライアントがある場合は、NIS+ サーバーの NIS 互換モード機能を使用します。NIS サーバーをそのままにしないでください。

4. **NIS+** の性能を評価します。

   実装が完了したら、NIS+ が正しく機能しているかどうかをテストします。

5. **NIS+** 環境を最適化します。

   性能の評価結果に基づいて、必要であれば NIS+ の環境を変更します。このような改善には、選択した複製サーバーを負荷の高いドメインに追加するような簡単

なものや、ドメインのグループの NIS+ 情報の記憶領域を再編成したりすることが含まれます。

6. 新しいドメインを整理します。

   移行の際に、処理の簡便化のため、古いドメインの名前を変更しなかった場合は、それらをここで新しい NIS+ の命名方式に合わせて変更します。たとえば、物理的な位置を表す名前を持つドメインをいくつか残し、その一方で組織的な階層へ移行した場合は、物理的な位置を表す名前を組織を表す名前に変更します。

第 4 段階 - NIS 互換ドメインを移行する

1. 最後の **NIS** クライアントを **NIS+** に移行します。

   NIS 互換の NIS+ ドメインが、できるだけ早く不要になるようにします。最後の NIS クライアントを NIS+ に移行すると、NIS+ のセキュリティ機能を利用できるようになります。ネットワーク上で Solaris 以外のコンピュータを実行している場合は、NIS 互換の NIS+ ドメインを削除することはできません。

2. セキュリティ構成を調整します。

   NIS クライアントがなくなったら、NIS+ サーバーを標準モードで再起動して、NIS+ テーブルに対して `nischmod` を実行し、アクセス権レベルを変更して、NIS 互換によって生じたセキュリティの不備を削除することができます。NIS+ 主体に以前に資格を作成しなかった場合は、ここで資格を作成してください。認証されていない主体のアクセスは制限してください。

3. その他の評価とプログラムの改善を行います。

   操作手順を評価して、改善できるものがないかを調べます。特に、問題回復に使用される手順を調べてください。新しい NIS+ リリースと機能強化の可能性について検討します。また、新しい NIS+ テーブルを必要とする可能性がある Solaris の構成要素の開発を調査します。さらに、NIS+ 管理作業をより効率的に実行できるようにする自動化ツールを探します。最後に、社内の開発担当者と協力して、NIS+ API を利用できるように援助してください。

   これで NIS+ への移行は完了です。

索引

H

K

L

M

N

Y

あ

い

え

お

か

き

く

す

せ

そ

た

て

と

な