管理者ガイド

iPlanet Messaging Server

リリース 5.1

816-1461-01
2001 年 5 月

目次

第 3 章 メールユーザとメーリングリストを管理する

第 4 章 POP、IMAP、および HTTP サービスを設定する

第 5 章 Messaging Multiplexor

第 6 章 MTA サービスと設定について

第 7 章 書き換え規則を設定する

第 8 章 チャネル定義を設定する

第 9 章 メールのフィルタリングとアクセス制御

第 10 章 メッセージストアを管理する

第 11 章 セキュリティとアクセス制御を設定する

第 12 章 ログ記録とログ解析

このマニュアルについて

このマニュアルでは、iPlanet Messaging Server 5.1 を管理および設定する方法について説明します。iPlanet Messaging Server 5.1 は、インターネットの標準規格を使用して、あらゆるサイズの企業およびメッセージング ホストの電子メール システムにパワフルで柔軟なクロス プラットホーム ソリューションを提供します。

この章には、以下の項目があります。

- 対象読者
- お読みになる前に
- このマニュアルの構成
- マニュアルの表記規則
- 関連情報
- オンラインで本書を入手するには

対象読者

このマニュアルは、iPlanet Messaging Server 5.1 の管理および設定に携わる方たちを対象に書かれています。

お読みになる前に

このマニュアルは、Messaging Server ソフトウェアの設定および管理に携わる方たちを対象としており、以下の予備知識があることを前提に書かれています。

- インターネットおよび WWW (ワールドワイドウェブ)
- iPlanet Administration Server
- iPlanet Directory Server および LDAP
- Netscape Console

このマニュアルの構成

このマニュアルには、以下の各章および付録が含まれています。

- このマニュアルについて (本章)
- 第 1 章 「概要」

  iPlanet Messaging Server の概要について説明します。
- 第 2 章 「一般的なメッセージング機能を設定する」

  サービスの起動および終了、ディレクトリアクセスの設定など、Messaging Server の一般的なタスクについて説明します。
- 第 3 章 「メールユーザとメーリングリストを管理する」

  コンソールのインターフェースを使ってユーザの電子メールアカウントやメーリングリストを作成および管理する方法について説明します。
- 第 4 章 「POP、IMAP、および HTTP サービスを設定する」

  iPlanet コンソールまたはコマンドラインユーティリティを使って、1 つまたは複数のサービスをサーバに設定する方法について説明します。
- 第 5 章 「Messaging Multiplexor」

  複数のメッセージングサーバへの接続点として機能する特殊なメッセージングサーバ「iPlanet Messaging Multiplexor」の概念について説明します。
- 第 6 章 「MTA サービスと設定について」

  お使いのサーバにおける MTA サービス設定に関する概念を説明します。
- 第 7 章 「書き換え規則を設定する」

  MTA 設定ファイル `imta.cnf` に書き換え規則 (アドレスの書き換え) を設定する方法について説明します。
- 第 8 章 「チャネル定義を設定する」

  MTA 設定ファイル `imta.cnf` にチャネル定義を設定する方法について説明します。
- 第 9 章 「メールのフィルタリングとアクセス制御」

  メールサービスに対するアクセス制御の方法およびマッピングテーブルと SSR (Server Side Rules) を使ってメールをフィルタリングする方法について説明します。
- 第 10 章 「メッセージストアを管理する」

  メッセージストアディレクトリのレイアウト、メッセージストアパーティションの設定方法、制限容量や存続期間設定ポリシーの設定等について説明します。
- 第 11 章 「セキュリティとアクセス制御を設定する」

  iPlanet Messaging Server に備わっているセキュリティおよびアクセス制御機能について説明します。

- 第 12 章 「ログ記録とログ解析」

  MTA、メッセージストア、およびメッセージアクセスサービスのサービスログを表示または設定する方法について説明します。

- 付録 A 「SNMP サポート」

  Messaging Server に対する SNMP サポートを有効にする方法について説明します。また、SNMP によって提供される情報のタイプについても簡単に紹介します。

- 用語集

  iPlanet Messaging Server のマニュアルで使われている用語の定義やネーミング規則を提供します。

マニュアルの表記規則

クーリエフォント

クーリエ (courier) フォントは、コンピュータ画面に表示されるテキスト、またはユーザが入力するテキストを表します。また、ファイル名、識別名、機能、および使用例を表す場合にも使用されます。

太字のクーリエフォント

太字のクーリエ (bold courier) フォントは、ユーザが入力するコード例中のユーザが入力するテキストを表します。たとえば、以下のようなものです。

```
./setup
Sun-Netscape Alliance
iPlanet Server Products Installation/Uninstallation
-------------------------------------------------------------------

Welcome to the iPlanet Server Products installation program. This
program will install iPlanet Server Products and the iPlanet Console on
your computer.

It is recommended that you have "root" privilege to install the
software.

Tips for using the installation program:

- Press "Enter" to choose the default and go to the next screen
- Type "Control-B" to go back to the previous screen
- Type "Control-C" to cancel the installation program
```

```
- You can enter multiple items using commas to separate them.
For Example: 1, 2, 3

Would you like to continue with installation? [Yes]:
```

この例は、コマンドラインで **./setup** を入力すると、その結果として後続のテキストが表示されることを意味しています。

斜体フォント

*斜体 (italic) フォント*は、使用中のシステムに特有な情報を使って入力するテキスト (たとえば、変数など) を表します。サーバのパスや名前、およびアカウント ID などに使用します。

たとえば、パス参照は、以下のような形式で表記されています。

server-root/msg-*serverID*/...

この場合、*server-root* はサーバをインストールするディレクトリパスを表し、msg-*serverID* はインストールするときに使用するサーバインスタンスを表します。たとえば、サーバを /usr/iplanet/server5 ディレクトリにインストールし、tango というサーバインスタンスを使用する場合、実際のパスは次のようになります。

```
/usr/iplanet/server5/msg-tango/
```

角括弧

オプションのパラメータは、角括弧 [] で囲まれています。たとえば、setup コマンドの使い方を示す場合は、以下のように記述されます。

./setup [*options*] [*argument*]

以下に示すように setup コマンドだけを実行しても Messaging Server のインストールを開始することはできます。

```
./setup
```

ただし、setup コマンドには、[オプション] や [引数] などの付加的なオプション パラメータも指定できます。たとえば、setup コマンドに -k オプションを指定すると、インストール キャッシュを維持できます。

```
./setup -k
```

コマンドラインプロンプト

このマニュアルの各例では、コマンドラインプロンプト (たとえば、C シェルの %、Korn/Bourne シェルの $ など) が表示されていません。お使いのオペレーティングシステムの環境によって、コマンドラインプロンプトが異なるためです。ただし、特に補足されていないかぎり、コマンドは本書で示すとおりに入力してください。

関連情報

iPlanet Messaging Server 5.1 には、本書の他に、管理者用の補足情報およびエンドユーザや開発者用のマニュアルもあります。Messaging Server に関する各マニュアルの情報については、以下の URL をご利用ください。

```
http://docs.iplanet.com/docs/
```

以下に、利用可能なマニュアルをいくつか紹介します。

- iPlanet Messaging Server 5.1 I インストールガイド
- iPlanet Messaging Server 5.1 リファレンスマニュアル
- iPlanet Messaging Server 5.1 プロビジョニングガイド
- iPlanet Messaging Server 5.1 Schema Reference Manual
- iPlanet Delegated Administrator for Messaging インストールおよび管理ガイド

オンラインで本書を入手するには

『iPlanet Messaging Server 5.1 管理者ガイド』はオンラインで入手することもできます。その場合、本書は PDF または HTML 形式になっています。以下の URL をご利用ください。

```
http://docs.iplanet.com/docs/
```

第 1 章

概要

iPlanet Messaging Server は、大容量のパワフルな標準ベースインターネットメッセージングサーバであり、組織やサービスプロバイダのメッセージングに関するニーズに適切に対応できるよう設計されています。Messaging Server は、標準的な電子メールプロトコルをサポートする数種のモジュラーから構成されており、それぞれのモジュラーは個々に設定することができます。

Messaging Server では、ユーザ、グループ、ドメインに関する情報がセントラル LDAP データベースに保存されます。また、サーバの設定に関する情報は、LDAP データベースまたは一連の設定ファイルに保存されます。

Messaging Server のパッケージには、サーバ設定用のツールやユーザ用のツールがあります。

この章には、以下の項目があります。

- 標準プロトコルのサポート
- ホストドメインのサポート
- ユーザ対応のサポート
- メッセージ統合のサポート
- Web メールのサポート
- パワフルなセキュリティおよびアクセス制御
- 便利なユーザインターフェース
- インストール後のディレクトリ / ファイル構造

標準プロトコルのサポート

- SMTP (Simple Mail Transfer Protocol) サービス : インターネットの基準である SMTP を使用して、内部およびインターネットベースのメールを処理します。
- IMAP4 (Internet Mail Access Protocol) サービス : 多数のユーザが同時に各自のメールボックスにアクセスできます。
- POP3 (Post Office Protocol) サービス : 最も広く使用されているインターネットメールボックスプロトコルによるメールボックスへのアクセスを可能にします。
- HTTP (Hypertext Transfer Protocol) サービス : Web ベースの電子メールをサポートします。iPlanet Messenger Express などの HTTP クライアントからのメールは専用の HTTP サービスに送られ、そこから MTA に転送されます。

ホストドメインのサポート

Messaging Server は、ISP が管理する電子メールドメイン (ホストドメイン) を完全にサポートします。つまり、組織の電子メールシステムが ISP によって運用および維持されている場合でも、Messaging Server を使用することができます。各ドメインは、単一の Messaging Server ホストを他のドメインと共有します。従来の LDAP ベース電子メールシステムでは、ドメインが複数の電子メールサーバホストによってサポートされていましたが、Messaging Server を使用すると、多くのドメインを 1 つのサーバでホストすることができます。各ドメインに対し、ユーザやグループの場所をポイントするための LDAP エントリがあります。

ユーザ対応のサポート

Messaging Server は、ユーザやグループ、ドメインに関する情報をセントラル LDAP データベースに保存します。また、iPlanet Delegated Administrator for Messaging は、コンソールグラフィカルユーザインターフェースや、組織内のユーザ、グループ、ドメインを管理するためのさまざまなコマンドラインユーティリティを備えています。

ユーザ、グループ、ドメインの管理については、以下の各ドキュメントを参照してください。

- 『Messaging Server Provisioning Guide』- LDAP を使って、ドメイン、ユーザ、グループ、管理者のエントリを作成する方法について説明しています。
- 『Messaging Server リファレンスマニュアル』- Delegated Administrator コマンドラインユーティリティを使って、ユーザ、グループ、ドメインを管理する方法について説明しています。

さらに、Delegated Administrator のコンソールインターフェースには、ユーザ用のオンラインヘルプがあります。

メッセージ統合のサポート

iPlanet Messaging Server は、メッセージを統合して保存するためのソリューションを提供しており、電子メール、ボイスメール、ファックスなどのデータをすべて 1 つのメッセージストアに保存できます。

Web メールのサポート

iPlanet Messaging Server の一部である Web 対応電子メールプログラム Messenger Express を使うと、エンドユーザがインターネット接続に HTTP を用いるマシンのブラウザからメールボックスにアクセスすることができます。Messenger Express クライアントから送信したメールは iPlanet Messaging Server の一部である専用 Web サーバに送られ、その後 HTTP サービスによってルーティングまたは配信用にローカル MTA またはリモート MTA に送られます。

パワフルなセキュリティおよびアクセス制御

iPlanet Messaging Server は、以下のセキュリティおよびアクセス制御機能を備えています。

- POP、IMAP、HTTP、または SMTP へのパスワードログインおよび証明書に基づくログインのサポート
- 標準セキュリティプロトコルのサポート：TLS (Transport Layer Security)、SSL (Secure Sockets Layer)、SASL (Simple Authentication and Security Layer)
- アクセス制御インストラクション (ACI) を用いての管理委託
- POP、IMAP、および HTTP へのクライアントアクセスのフィルタ
- MTA へのクライアントアクセスのフィルタ
- マッピングテーブルおよびサーバ側の規則に基づく不特定多数宛てメールのフィルタリング

便利なユーザインターフェース

Messaging Server は、標準的な電子メールプロトコルをサポートする数種のモジュラーから構成されており、各モジュラーは個々に設定することが可能です。

Messaging Server のコマンドラインユーティリティおよびローカルサーバに保存されている一連の設定ファイルを使用して、メッセージ転送エージェント (MTA) を設定できます。また、Messaging Server のコンソールグラフィカルユーザインターフェースおよび一連のコマンドラインユーティリティを使用すると、メッセージストアおよびメッセージアクセスサービスを設定することもできます。

MTA の設定および MTA へのアクセスの設定については、以下の各章を参照してください。

- 第 6 章 「MTA サービスと設定について」
- 第 7 章 「書き換え規則を設定する」
- 第 8 章 「チャネル定義を設定する」
- 第 9 章 「メールのフィルタリングとアクセス制御」
- 第 11 章 「セキュリティとアクセス制御を設定する」

また、『iPlanet Messaging Server リファレンスマニュアル』にも関連情報が記載されています。

メッセージストアの設定およびメッセージストアへのアクセスの設定については、以下の各章を参照してください。

- 第 4 章 「POP、IMAP、および HTTP サービスを設定する」
- 第 10 章 「メッセージストアを管理する」
- 第 11 章 「セキュリティとアクセス制御を設定する」

また、『iPlanet Messaging Server リファレンスマニュアル』にも関連情報が記載されています。

さらに、本書の以下の各章も参照してください。

- 第 2 章 「一般的なメッセージング機能を設定する」- サービスの起動 / 停止、ディレクトリアクセスの設定など、Messaging Server の基本的なタスクについて説明しています。
- 第 5 章 「Messaging Multiplexor」- 複数サーバに対する単一接続ポイントとしての役割を担う特殊なメッセージングサーバ iPlanet Messaging Multiplexor (MMP) について説明しています。

インストール後のディレクトリ / ファイル構造

表 1-1 は、iPlanet Messaging Server をインストールした後のディレクトリやファイルの構成を示しています。ただし、この表は典型的なサーバ管理タスクに関連するディレクトリやファイルのみを示すものであり、完全な表ではありません。

表 1-1　　インストール後のディレクトリ / ファイル構造

ディレクトリ	デフォルトの位置と説明
サーバのルートディレクトリ (*サーバ- ルート*)	/usr/iplanet/server5/ (デフォルト位置)
	特定のサーバグループ (1 つの Administration Server によって管理されているすべてのサーバ) のインストール先ディレクトリ。Messaging Server に加え、他の iPlanet サーバが含まれる場合もあります。
	また、このディレクトリには管理サーバの起動 / 停止に使用するバイナリ実行可能プログラム (start-admin と stop-admin)、および コンソールを起動する startconsole も含まれています。
マニュアルディレクトリ manual	*サーバ- ルート* /manual (変更不可)
	サーバと同時にインストールされるドキュメントのインストール先ディレクトリ。
	manual/en/admin/ には、Administration Server のドキュメントがあります。
	manual/en/msg/ には、Messaging Server のドキュメントがあります。
	manual/en/slapd/ には、Directory Server のドキュメントがあります。
インストールディレクトリ (*インスタンスディレクトリ*)	*サーバ- ルート* /bin/msg/ (変更不可)
	このディレクトリには、インストールした Messaging Server のバイナリ実行可能プログラムの一部も含まれています。
インスタンスディレクトリ (*インスタンスディレクトリ*)	*サーバ- ルート* /msg- *インスタンス名* / (変更不可)
	*インスタンス名*は、インストール時に指定した Messaging Server のインスタンス名を示します (デフォルト設定では、サーバマシンのホスト名になっています)。
	このディレクトリには、Messaging Server のインスタンスを定義する設定ファイルが含まれています。1 台のホストマシンに同じバイナリファイルを共有する複数の Messaging Server インスタンスを作成することも可能です。
	このディレクトリには、configutil、start-msg、stop-msg など、インストールした Messaging Server のバイナリ実行可能プログラムの一部も含まれています。

表 1-1　インストール後のディレクトリ / ファイル構造（続き）

ディレクトリ	デフォルトの位置と説明
設定ディレクトリ config	*インスタンスディレクトリ* /config/ (変更不可)
	local.conf、msg.conf、sslpassword.conf など、一般的な設定ファイルがあります。
	msg.conf ファイル内の各値は、インストール時に設定されます。Messaging Server は、LDAP ホスト名やポート番号などの情報を得るため、起動時にこのファイルを使用します。
MTA ディレクトリ imta	*インスタンスディレクトリ* /imta/ (変更不可)
	MTA の設定に関連するディレクトリがあります (bin、config、db、dl、programs、queue、tmp など)。
MTA 設定ディレクトリ config	*インスタンス ディレクトリ* /imta/config/ (変更不可)
	MTA 設定ファイルがあります (imta.cnf、dispatcher.cnf、job_controller.cnf、aliases、imta_tailor など)。
MTA キューディレクトリ queue	*インスタンスディレクトリ* /imta/queue/ (変更不可)
	メッセージキューサブディレクトリがあります。各チャンネルキュー用に、それぞれ 1 つずつサブディレクトリが割り当てられます (例 : ims-ms、tcp_intranet、tcp_local、autoreply など)。
MTA プログラムディレクトリ programs	*インスタンスディレクトリ* /imta/programs/ (変更不可)
	ユーザメール処理用にサイトから提供された実行可能プログラムがある場合、それらのプログラムはこのディレクトリに含まれます。
MTA データベースディレクトリ db	*インスタンスディレクトリ* /imta/db/ (変更不可)
	MTA によって使用されるデータベースがあります (aliasesdb.db、domaindb.db、profiledb.db、reversedb.db、ssrdb.db)。
メッセージストアディレクトリ store	*インスタンスディレクトリ* /store (変更不可)
	メッセージストアの処理に関連するディレクトリがあります (mboxlist、partition、user)。
	詳細については、215 ページの「メッセージストアディレクトリのレイアウト」を参照してください。

第 2 章

一般的なメッセージング機能を設定する

この章では、サービスの起動および停止、ディレクトリアクセスの設定など、Netscape Console (以下、省略してコンソールという) またはコマンドラインユーティリティを使って実行できる Messaging Server の一般的なタスクについて説明します。個々の Messaging Server サービス (POP、IMAP、HTTP、および SMTP など) に特有なタスクについては、後の章で説明します。この章には、以下の項目があります。

- サーバの基本情報を表示する
- サービスを起動 / 停止する
- グリーティングメッセージを設定する
- 自動返信メッセージ用の言語を設定する
- シングルサインオン (SSO) を使用する
- ディレクトリの検索をカスタマイズする
- 暗号化の設定

注 エンドユーザアカウント情報およびドメイン特有の情報は、主に Delegated Administrator for Messaging のインタフェースを使用して管理します。詳細については、Delegated Administrator の『Delegated Administrator for Messaging インストールおよび管理ガイド』およびオンラインヘルプを参照してください。

サーバの基本情報を表示する

インストールした Messaging Server に関する基本的な情報を確認するには、コンソールを使って情報フォームを表示します。

情報フォームを表示するには :

1 コンソールで、目的の Messaging Server を開きます。

2 左側のパネルにあるサーバのアイコンを選択します。

3 左側のパネルの [環境設定] タブをクリックします。

4 右側のパネルの [情報] タブをクリックします。

情報フォームが表示されます。このフォームには、サーバ名、サーバのルートディレクトリ、インストールディレクトリ、およびインスタンスディレクトリが表示されます。

サービスを起動 / 停止する

サービスを起動 / 停止する方法は、そのサービスが HA 環境にインストールされているかどうかによって異なります。

HA 環境でサービスを起動 / 停止する

Messaging Server を HA 制御下で実行している場合は、個々の Messaging Server サービスを制御するための通常の Messaging Server コマンド (起動、再起動、停止) を使用することはできません。これらのコマンドを使うと、HA 制御は 1 つ以上のサービスが予期しない状況で停止したとみなして、すべての Messaging Server を再起動しようとするか、または他のクラスタノードへフェイルオーバーしようとします。

以下の表に、適切な起動、停止、再起動のコマンドを示します。単一の Messaging Server サービス (たとえば、SMTP) を起動、再起動、停止するための Sun Cluster コマンドはありません。Sun Cluster が認識できる最小単位は、個々のリソースです。Sun Cluster は Messaging Server を 1 つのリソースとして認識しているため、scswitch コマンドを使用すると、すべての Messaging Server サービスに一括して処理が行われます。

表 2-1　Sun Cluster 3.0 環境での起動、停止、再起動

アクション	個々のリソース	リソースグループ全体
起動	`scswitch -e -j <`*リソース*`>`	`sscswitch -Z -g <`*リソースグループ*`>`
再起動	`scswitch -n -j <`*リソース*`>` `scswitch -e -j <`*リソース*`>`	`scswitch -R -g <`*リソースグループ*`>`
停止	`scswitch -n -j <`*リソース*`>`	`scswitch -F -g <`*リソースグループ*`>`

表 2-2　Sun Cluster 2.2 環境での起動、停止、再起動

アクション	個々のデータサービス	すべての登録済みデータサービス
起動	`hareg -y <`*データサービス*`>`	`hareg -Y`
再起動	`hareg -n <`*データサービス*`>` `hareg -y <`*データサービス*`>`	`hareg -N` `hareg -Y`
停止	`hareg -n <`*データサービス*`>`	`hareg -N`

表 2-3　Veritas 1.1 環境での起動、停止、再起動

アクション	個々のリソース	リソースグループ全体
起動	`hares -online <`*リソース*`> -sys <`*システム*`>`	`hagrp -online <`*グループ*`> -sys <`*システム*`>`
再起動	`hares -offline <`*リソース*`> -sys <`*システム*`>` `hares -online <`*リソース*`> -sys <`*システム*`>`	`hagrp -offline <`*グループ*`> -sys <`*システム*`>` `hagrp -online <`*グループ*`> -sys <`*システム*`>`
停止	hares -online < *リソース* > -sys < *システム* >	`hagrp -online <`*グループ*`> -sys <`*システム*`>`

HA 以外の環境でサービスを起動および停止する

サービスは、コンソールまたはコマンドラインを使って起動および停止できます。

必要な操作は、サーバが実際に使用しているサービスを実行するだけです。たとえば、メッセージ転送エージェント (MTA) として、一時的に特定の Messaging Server インスタンスを 1 つだけ使用している場合は、MTA だけを起動できます。また、メンテナンス、修復、セキュリティなどの目的でサーバをシャットダウンする場合には、影響が及ぶサービスだけを停止できます (実行する予定のないサービスは、停止するのではなく無効にしてください)。

注　POP、IMAP、および HTTP の各サービスを起動または停止するには、まずそれらを使用可能な状態にする必要があります。詳細については、60 ページの「サービスを有効または無効にする」を参照してください。

重要 : サーバプロセスがクラッシュすると、他のプロセスがハングします。これは、それらのプロセスがクラッシュしたサーバプロセスによって保持されていたロックを待機しているためです。したがって、サーバプロセスがクラッシュした場合は、すべてのプロセスを停止し、再起動するようにしてください。これには、POP、IMAP、HTTP、MTA の各プロセス、`stored` (メッセージストア) プロセス、および `mboxutil`、`deliver`、`reconstruct`、`readership`、または `upgrade` などの「メッセージの保存」を変更するユーティリティが含まれます。

コンソール - コンソールには、個々のサービスを起動 / 停止したり、各サービスに関するステータス情報を表示するためのフォームがあります。

フォームには、IMAP、POP、SMTP、および HTTP の各サービスに対し、現在の状態 (オンまたはオフ) が表示されます。また、サービスが実行中である場合には、そのサービスが最後に起動した時刻や他のステータス情報も表示されます。

メッセージングサービスを起動またはシャットダウンしたり、そのステータスを表示するには :

1 コンソールで、サービスを起動または停止する Messaging Server を開きます。

2 次のいずれかの方法で、サービスの一般設定フォームを表示します。

   a. [タスク] をクリックし、[サービスの起動 / 停止] をクリックします。

   b. [環境設定] タブをクリックし、左側のパネルの [サービス] フォルダ選択します。その後、右側のパネルで [一般] タブをクリックします。

3 サービスの一般設定フォームが表示されます。

   [プロセスコントロール] フィールドの左側のカラムには、サーバによってサポートされているサービスの一覧があります。また、右側のカラムには、各サービスの基本ステータスが表示されます (オンまたはオフ。オンの場合は、前回起動したときの時刻)。

4 現在実行中のサービスに関するステータス情報を表示するには、[プロセスコントロール] フィールドでそのサービスを選択します。

   [サービスステータス] フィールドに、そのサービスに関するステータス情報が表示されます。

   POP、IMAP、および HTTP の場合、フィールドには、最終接続時間、合計接続数、現在の接続数、最後にサービスを起動してから接続に失敗した回数、最後にサービスを起動してからログインに失敗した回数が表示されます。

   このフィールドの情報を見ることにより、サーバにかかる負荷やそのサービスの信頼性などを把握できます。また、サーバのセキュリティに対する攻撃を調べるのにも役立ちます。

5 サービスを起動するには、[プロセスコントロール] フィールドでそのサービスを選択し、[起動] をクリックします。

6 サービスを停止するには、[プロセスコントロール] フィールドでそのサービスを選択し、[停止] をクリックします。

7 使用可能な状態のサービスをすべて起動または停止するには、[すべて起動] または [すべて停止] ボタンをクリックします。

コマンドライン - start-msg および stop-msg コマンドを使って、任意のメッセージングサービス (pop、imap、http、smtp、store) を起動または停止できます。以下に、その例を示します。

サーバ - ルート /msg- *インスタンス* /start-msg imap
サーバ - ルート /msg- *インスタンス* /stop-msg pop
サーバ - ルート /msg- *インスタンス* /stop-msg smtp

注 start-msg smtp および stop-msg smtp コマンドを実行すると、SMTP サーバだけでなく、すべての MTA サービスが起動および停止します。特定の MTA サービスだけを起動および停止する場合は、imsimta start および imsimta stop コマンドを使用します。詳細については、『Messaging Server リファレンスマニュアル』を参照してください。

グリーティングメッセージを設定する

Messaging Server を使って、新規ユーザに送るグリーティングメッセージを作成できます。

コンソール - コンソールを使って新規ユーザへのグリーティングメッセージを作成するには :

1 コンソールで、新規ユーザへのグリーティングを設定する Messaging Server を開きます。

2 [環境設定] タブを開きます。左側のパネルでサーバのアイコンが強調表示されていない場合は、そのアイコンを選択します。

3 右側のパネルの [その他] タブをクリックします。

4 必要に応じて、新規ユーザへのグリーティングを作成するか、または変更します。

電子メールメッセージと同じように、グリーティングメッセージの書式を設定する必要があります。まずヘッダ (少なくとも件名の行を含めます) を入力し、その後、空白行に続いてメッセージ本文を入力します。

メッセージを作成する際には、メッセージフィールドの上にあるドロップダウンリストを使って言語を指定します。必要に応じて、複数の言語で複数のメッセージを作成することも可能です。サーバは、「自動返信メッセージ用の言語を設定する」の節で説明している情報に基づいて、新規ユーザに適切な言語のメッセージを送信します。

5 [保存] をクリックします。

コマンドライン - コマンドラインを使って新規ユーザへのグリーティングメッセージを作成するには :

configutil -o gen.newuserforms -v *値*

自動返信メッセージ用の言語を設定する

この節では、サーバから送られる通知やメッセージの言語がどのようにして選択されるかについて説明します。また、ユーザが言語を指定する方法やデフォルトのサーバサイト言語を指定する方法についても説明します。

ユーザは、指定した特定の条件が満たされたときにサーバから自動的に送られるメッセージを作成できます。たとえば、すべての受信メールに対して「現在、休暇中です。」というようなメッセージを自動返信する場合です。このようなメッセージを作成するときには、そのメッセージが特定の言語で表示されるように指定できます。つまり、サーバが送信するメッセージをいくつかの異なる言語で作成しておくことが可能なのです。

ユーザは、自分が受け取る自動返信メッセージの言語を指定することもできます。ただし、この機能を使う意味があるのは、目的の言語で作成されたメッセージが準備されている場合だけです。

サーバは、以下の規則に従って特定言語の送信メッセージを選択します。

1 メッセージの送り先であるユーザが言語を選択しており (31 ページの「ユーザの優先言語を選択する」を参照)、その言語で作成されたメッセージが準備されている場合は、その言語のメッセージが送信されます。たとえば、ユーザが日本語を選択しており、日本語で作成されたメッセージが準備されている場合は、日本語のメッセージが送信されます。

2 ユーザが言語を選択していない場合、または言語を選択しているがその言語のメッセージが準備されていない場合は、デフォルトのサーバサイト言語 (31 ページの「サーバサイト言語を設定する」を参照) のメッセージが送信されます。たとえば、デフォルトのサーバサイト言語がスペイン語で、ユーザがフランス語を選択しているのにフランス語版のメッセージが準備されていない場合は、スペイン語版のメッセージが送信されます。

3 ユーザが選択した言語とデフォルトのサーバサイト言語がいずれも準備されているメッセージの言語に一致しない場合に、英語版のメッセージがある場合は、英語版のメッセージが送信されます。たとえば、デフォルトのサーバサイト言語がスペイン語で、ユーザが選択した言語がドイツ語である場合に、フランス語版と英語版のメッセージしか準備されていない場合は、英語版のメッセージが送信されます。

4 メッセージが 1 つの言語でしか作成されなかった場合は、ユーザが選択した言語やサイト言語に関係なく、準備されている言語のメッセージが送信されます。

注 Delegated Administrator のトップレベル管理者はホストドメインのデフォルト言語を設定できます。ただし、Messaging Server が送信メッセージの言語を決定する際に、その設定は使用されません。

ユーザの優先言語を選択する

ユーザは、Delegated Administrator for Messaging のインターフェースを使って優先言語を選択できます。また、メールクライアントの中には、優先言語を指定できるものもあります。Delegated Administrator を使って優先言語を設定した場合、その情報は Directory Server に保存されます。

サーバの管理ドメイン外のユーザにメッセージが送られる場合には、ヘッダに優先言語が指定された受信メッセージに応答するのでない限り、サーバはそれらのユーザの優先言語を判断することができません。これらのヘッダフィールド (`Preferred-Language` または `X-Accept-Language`) は、ユーザのメールクライアントで指定された属性に応じて設定されています。

優先言語に対して複数の設定がある場合、たとえば、Directory Server に保存されている優先言語属性とメールクライアントで指定された優先言語があるような場合には、以下の順序で優先言語が選択されます。

1 元のメッセージの `Preferred-Language` ヘッダ

2 元のメッセージの `X-Accept-Language` ヘッダ

3 送信者の優先言語属性 (LDAP ディレクトリで見つかった場合)

サーバサイト言語を設定する

以下の手順に従って、サーバのデフォルトサイト言語を指定できます。サイト言語は、ユーザの優先言語が設定されていない場合に、どの言語のメッセージを送信するかを決定するために使用されます。

コンソール - コンソールからサイト言語を指定するには :

1 設定を行う Messaging Server を開きます。

2 [環境設定] タブをクリックします。

3 右側のパネルで、[その他] タブをクリックします。

4 [サイト言語] ドロップダウンリストで、使用する言語を選択します。

5 [保存] をクリックします。

コマンドライン - 次に示すように、コマンドラインでサイト言語を指定することもできます。

```
configutil -o gen.sitelanguage -v 値
```

「*値*」には、ローカルでサポートされている以下のいずれかの言語を指定できます。

af	Afrikaans
ca	Catalan
da	Danish
de	German
en	English
es	Spanish
fi	Finnish
fr	French
ga	Irish
gl	Galician
is	Icelandic
it	Italian
ja	Japanese
nl	Dutch
no	Norwegian
pt	Portuguese
sv	Swedish

シングルサインオン (SSO) を使用する

シングルサインオン機能を使うと、1 つのアプリケーションにログインしたユーザが他のアプリケーションも使用できるようになります。たとえば、Messenger Express にログインしたユーザは、認証プロセスを繰り返さなくても Delegated Administrator for Messaging を使用できるようになります。

2 つのアプリケーション間でシングルサインオンを使用するには、各アプリケーションを設定する必要があります。この節では、Messenger Express と Delegated Administrator の間でシングルサインオンを使用できるようにする方法について説明します。35 ページの「Messenger Express と Delegated Administrator for Messaging」を参照してください。

Messenger Express の SSO 設定パラメータ

configutil コマンドを使うと、Messenger Express のシングルサインオン設定パラメータを変更できます。表 2-4 に、それらのパラメータを示します。configutil の詳細については、『Messaging Server リファレンスマニュアル』を参照してください。

表 2-4　Messenger Express のシングルサインオンパラメータ

パラメータ	説明
local.webmail.sso.enable	ログインページが取り込まれたときにクライアントによって与えられた SSO cookie を受け入れ確認する機能、ログイン成功時に SSO cookie を返す機能、他の SSO パートナーからの要求に応答して独自の cookie を確認する機能など、すべてのシングルサインオン機能を有効または無効にします。 ゼロ以外の値に設定した場合、サーバはすべての SSO 機能を実行します。 ゼロに設定した場合、サーバはどの SSO 機能も実行しません。 デフォルト値はゼロです。
local.webmail.sso.prefix	このパラメータの文字列値は、HTTP サーバによって設定された SSO cookie をフォーマットするときのプレフィックスとして使用されます。このプレフィックスの付いた SSO cookie だけがサーバによって認識され、他の SSO cookie はすべて無視されます。 このパラメータの値が null (空白) の場合は、サーバ上のすべての SSO 機能が効果的に使用不可の状態になります。 デフォルト値は null (空白) です。
local.webmail.sso.id	このパラメータの文字列値は、HTTP サーバによって設定された SSO cookie をフォーマットするときのアプリケーション ID 値として使用されます。 デフォルト値は null (空白) です。
local.webmail.sso.cookiedomain	このパラメータの文字列値は、HTTP サーバによって設定されたすべての SSO cookie の cookie ドメイン値を設定するために使用されます。 デフォルトは null (空白) です。

表 2-4　Messenger Express のシングルサインオンパラメータ（続き）

パラメータ	説明
`local.webmail.sso.singlesignoff`	このパラメータの整数値がゼロ以外に設定されている場合は、クライアントがログアウトするときに、local.webmail.sso.prefix の値に一致するプレフィックス値を持つクライアント上の SSO cookie がすべてクリアされます。 ゼロに設定されている場合は、クライアントがログアウトするときに、Messenger Express がその独自の SSO cookie をクリアします。 デフォルト値はゼロです。
`local.sso.`*appid*`.verifyurl`	ピア SSO ホストの確認 URL 値を設定します。*appid* は、処理される SSO cookie を生成するピア SSO ホストのアプリケーション ID です。たとえば、Delegated Administrator の *appid* は `nda45` です。 信頼されている各 PPO ホストに対し、1 つのパラメータが定義されていなければなりません。確認 URL の標準形は次のとおりです。 `http://`*nda-host:port*`/VerifySSO?`

したがって、Messenger Express に対してシングルサインオンを使用するには、以下のように各パラメータを設定します (デフォルトのドメインは eng.siroe.com です)。

```
configutil -o local.webmail.sso.enable -v 1
configutil -o local.webmail.sso.prefix -v ssogrp1
configutil -o local.webmail.sso.id -v msg50
configutil -o local.webmail.sso.cookiedomain -v red.siroe.com
configutil -o local.webmail.sso.singlesignoff -v 1
```

Messenger Express と Delegated Administrator for Messaging

Messenger Express と Delegated Administrator 間でシングルサインオンを使用するには、以下の手順に従って操作します。

1 Directory Server を設定します。
   a. Directory Server でプロキシユーザアカウントのエントリを作成します。
   b. プロキシ認証の ACI (Access Control Instructions) を作成します。
2 Delegated Administrator を設定します。
   a. プロキシユーザ証明書を追加します。
   b. シングルサインオン cookie 情報を追加します。
   c. 関係するサーバの確認 URL を追加します。
3 Enterprise Server サーバを再起動します。

Directory Server を設定するには、`ldapmodify` ユーティリティを使用します。このユーティリティの詳細については、Directory Server のマニュアルを参照してください。

Delegated Administrator を設定するには、以下の設定ファイルを変更します。

DA-サーバ-ルート`/nda/classes/netscape/nda/servlet/resource.properties`

Enterprise-Server-ルート`/https-`*インスタンス名*`/config/servlets.properties`

Enterprise-Server-ルート`/https-`*インスタンス名*`/config/contexts.properties`

手順 1a. プロキシユーザアカウントを作成する

プロキシユーザアカウントは、ユーザがプロキシ認証用に Directory Server にバインドできるようにするためのものです。このアカウントは、Delegated Administrator のベースサフィックス (`osiroot`) 以外のベースサフィックス に (`ldapmodify` ユーティリティを使って) 作成する必要があります。以下に、プロキシユーザアカウント エントリの例を示します (osiroot が o=isp にあると仮定)。

```
dn: uid=proxy, ou=people, o=siroe.com, o=mailga
objectclass: top
objectclass: person
objectclass: organizationalperson
objectclass: inetorgperson
uid: proxy
givenname: Proxy
sn: Auth
cn: Proxy Auth
userpassword: proxypassword
```

手順 1b. プロキシ認証の ACI を作成する

次に、ldapmodify ユーティリティを使って、インストール時に作成したサフィックスの ACI を作成します。

- osiroot - ユーザデータを保存するために入力したサフィックス
- dcroot - ドメイン情報を保存するために入力したサフィックス
- osiroot - 設定情報を保存するために入力したサフィックス (デフォルト : osiroot)

以下に、ACI エントリの例を示します。

```
dn: o=isp
changetype: modify
add: aci
aci: (target="ldap:///o=isp")(targetattr="*")(version 3.0; acl
     "proxy";allow (proxy) userdn="ldap:///uid=proxy, ou=people,
     o=siroe.com, o=mailqa";)
```

手順 2a. resource.properties ファイルにプロキシユーザ証明書を追加する

プロキシ認証用に Delegated Administrator を設定するには、Delegated Administrator の resource-properties ファイルで以下のエントリをコメント解除し、変更を加えます。

LDAPDatabaseInterface-ldapauthdn= *プロキシ - 認証 -DN*

LDAPDatabaseInterface-ldapauthpw= *プロキシ - 認証 - パスワード*

以下に例を示します。

```
LDAPDatabaseInterface-ldapauthdn=uid=proxy, ou=people,o=siroe.com,
o=mailqa
LDAPDatabaseInterface-ldapauthpw=proxypassword
```

手順 2b. シングルサインオン Cookie 情報を追加する

シングルサインオン情報を追加するには、Delegated Administrator のコンテクスト識別子を定義し、そのコンテクストの cookie 名を指定します。

- コンテクスト識別子を定義するには、Enterprise Server の servlets.properties ファイルを編集し、servlet.xxxxx.context=ims50 というテキストが含まれている行をすべてコメント解除します。
- Delegated Administrator 設定でコンテクストの cookie 名を指定するには、以下のエントリを Delegated Administrator の resource.properties ファイルに追加します。

  ```
  NDAAuth-singleSignOnId=ssogrp1-
  NDAAuth-applicationId=nda45
  ```

- Enterprise Server 設定でコンテクストの cookie 名を指定するには、以下のエントリを Enterprise Server の contexts.properties ファイルに追加します。

  ```
  context.ims50.sessionCookie=ssogrp1-nda45
  ```

手順 2c. 関係するサーバの確認 URL を追加する

受け取ったシングルサインオン cookie を確認するには、Delegated Administrator にその連絡先を指定しておく必要があります。関係しているすべてのサーバに対して、確認 URL を指定します。

以下の例では、Messenger Express がインストールされており、そのアプリケーション ID が `msg50` であると仮定しています。Delegated Administrator の `resource.properties` ファイルを編集し、以下のようなエントリを追加します。

```
verificationurl-ssogrp1-msg50=http://<webmail_hostname>:port/
VerifySSO?
```

```
verificationurl-ssogrp1-nda45=http://<nda_hostname>:port/
VerifySSO?
```

手順 3. Enterprise Server を再起動する

手順 1a ～ 2c の説明に従って設定を変更したら、その変更内容が反映されるように Enterprise Server を再起動します。

ディレクトリの検索をカスタマイズする

iPlanet Messaging Server は、iPlanet Directory Server などの LDAP ベースのディレクトリシステムがないと機能しません。Messaging Server および コンソールには、以下の 3 つの目的を果たすためにディレクトリアクセスが必要です。

- Messaging Server を初めてインストールする際には、サーバの環境設定を行います。これらの設定は、中央**設定ディレクトリ**に保存されます。また、インストール時には、そのディレクトリへの接続も設定します。
- メールユーザまたはメールグループ用のアカウント情報を作成または更新すると、その情報は**ユーザディレクトリ**と呼ばれるディレクトリに保存されます。サーバグループの Administration Server はインストール時に設定されており、管理者が「ユーザ」や「グループ」にアクセスする場合に、コンソールが **管理トポロジ**を定義するユーザディレクトリに接続するようにデフォルト設定されています。管理トポロジとは、同じ設定ディレクトリおよびユーザディレクトリを共有する iPlanet サーバのグループのことです。
- メッセージを送り出したりメールをメールボックスに配信するとき、Messaging Server はユーザディレクトリ内で送信者または受信者に関する情報を検索します。デフォルトにより、Messaging Server は Administration Server が使用するのと同じユーザディレクトリ内を検索します。

これらのディレクトリ設定は、以下の方法で変更できます。

- コンソールの Administration Server インターフェースを使うと、設定ディレクトリの接続設定を変更できます (詳細については、『Managing Servers with Netscape コンソール』の「Administration Server」の章を参照してください)。
- コンソールの [ユーザおよびグループ] インターフェースを使うと、ユーザ情報やグループ情報に変更を加えているときに、デフォルトとは別のユーザディレクトリに一時的に接続できます (詳細については、『Netscape Console によるサーバの管理』の「Users and Groups」の章を参照してください)。
- コンソールの Messaging Server インターフェースを使うと、Administration Server で定義されているデフォルトとは別のユーザディレクトリに接続するように Messaging Server を設定できます。これが、この節で説明している設定作業です。

ユーザやグループを検索するのに別のユーザディレクトリに接続するように Messaging Server を再設定するのは、管理者の判断次第です。通常は、サーバの管理ドメインを定義しているユーザディレクトリがドメイン内のすべてのサーバによって使用されます。

注 Messaging Server の検索用にカスタムユーザディレクトリを指定した場合は、コンソールの [ユーザおよびグループ] インターフェースにアクセスして、そのディレクトリのユーザ情報またはグループ情報を変更するときにも同じディレクトリを指定する必要があります。詳細については、第 3 章「メールユーザとメーリングリストを管理する」を参照してください。

コンソール - コンソールを使って Messaging Server の LDAP ユーザ検索設定を変更するには :

1. コンソールを使って、LDAP 接続をカスタマイズする Messaging Server を開きます。
2. [環境設定] タブをクリックします。
3. 左側のパネルで [サービス] フォルダを選択します。
4. 右側のパネルで [LDAP] タブを選択します。[LDAP] フォームが表示されます。

   [LDAP] フォームには、設定ディレクトリとユーザディレクトリの設定が表示されています。ただし、このフォーム内の設定ディレクトリの設定は読み取り専用です。これらの設定の変更方法については、『Netscape Console によるサーバの管理』の「Administration Server」の章を参照してください。
5. ユーザディレクトリの接続設定を変更するには、[メッセージングサーバ固有のディレクトリ設定を使用] ボックスをクリックします。

6 以下に示す情報を入力または変更して、LDAP の環境設定を更新します (**識別名**などの用語の定義やディレクトリの概念については、『Directory Server Administrator's Guide』を参照してください)。

ホスト名 : インストールのユーザ情報を含むディレクトリがあるホストマシンの名前。一般に、これは Messaging Server ホストとは別のものです。ただし、インストールのサイズが非常に小さい場合には同じになる可能性があります。

ポート番号 : Messaging Server がユーザ検索用のディレクトリにアクセスするときに使用するディレクトリホストのポート番号。この番号は、ディレクトリ管理者が定義するもので、必ずしもデフォルトのポート番号 (389) である必要はありません。

ベース DN : 検索ベース - ユーザ検索の開始点を示すディレクトリエントリの識別名。ディレクトリツリー内で検索ベースが目的の情報に近いほど、検索処理は速くなります。ディレクトリツリーに「人びと」や「ユーザ」などのブランチがある場合には、それを開始点にするのが妥当です。

バインド DN : Messaging Server が検索を行うためにディレクトリサーバに接続する際、その Messaging Server を識別するために使われる名前。バインド DN は、ユーザ部分に検索特権が与えられている、ユーザディレクトリ内にあるエントリの識別名でなければなりません。ディレクトリに対して anonymous の検索アクセスを許可する場合は、このエントリを指定しないこともできます。

7 バインド DN に関連して、この Messaging Server を LDAP ディレクトリに対してユーザ検索用に認証するために使用するパスワードを変更するには、バインドパスワード変更のボタンをクリックします。ウィンドウが開くので、そこに新しいパスワードを入力します。

パスワードは、独自のセキュリティポリシーに基づいて決めるようにしてください。最初、パスワードは「パスワードなし」に設定されています。[バインド DN] フィールドには何も指定しないで anonymous アクセスを指定した場合、パスワードは使用されません。

この手順で、サーバの環境設定に保存されているパスワードが更新されますが、LDAP サーバ内のパスワードは変更されません。また、このアカウントは、デフォルトで PAB 検索にも使用されます。パスワードを変更した後、以下の 2 つの操作を行う必要があります。

8 環境設定属性 `local.ugldapbinddn` で指定されているユーザ用のパスワードを変更します。このユーザアカウントは、環境設定属性 `local.ugldapbinddn` で指定されているディレクトリサーバ内にあります。

9 属性 `local.service.pab.ldapbinddn` および `local.service.pab.ldaphost` で指定されているものと同じアカウントが PAB 用に使用されている場合は、`local.service.pab.ldappasswd` に保存されているパスワードも更新する必要があります。

デフォルトのユーザディレクトリに戻るには、[メッセージングサーバ固有のディレクトリ設定を使用] ボックス をオフにします。

コマンドライン - 以下に示すように、コマンドラインでユーザディレクトリの接続設定値を指定することもできます。上記の手順 8 および 9 で説明しているように、LDAP および PAB パスワードも必ず設定するようにしてください。

メッセージングサーバ固有のディレクトリ設定を使用するかどうかを指定するには :

```
configutil -o local.ugldapuselocal -v [ yes | no ]
```

ユーザ検索用の LDAP ホスト名を指定するには :

```
configutil -o local.ugldaphost -v 名前
```

ユーザ検索用の LDAP ポート番号を指定するには :

```
configutil -o local.ugldapport -v 番号
```

ユーザ検索用の LDAP ベース DN を指定するには :

```
configutil -o local.ugldapbasedn -v ベース dn
```

ユーザ検索用の LDAP バインド DN を指定するには :

```
configutil -o local.ugldapbinddn -v バインド dn
```

暗号化の設定

コンソールを使って、Messaging Server の SSL (Secure Sockets Layer) 暗号化および認証を有効にしたり、サーバがすべてのサービスにわたってサポートする特定の符合化方式を選択できます。

この作業は一般的な設定タスクですが、第 11 章「セキュリティとアクセス制御を設定する」の「SSL を有効にする符号化方式を選択する」の節で説明します。この章には、すべてのセキュリティに関する背景情報や Messaging Server のアクセスコントロールに関するトピックが記載されています。

第 3 章

メールユーザとメーリングリストを管理する

この章では、コンソールのインターフェースを使ってユーザの電子メールアカウントやメーリングリストを作成および管理する方法について説明しています。

この章には、以下の項目があります。

- 概要
- メールユーザを管理する
- メーリングリストを管理する

概要

LDAP ユーザディレクトリには、従業員、顧客、その他組織に何らかの関わりを持つ人々に関する詳細な情報を保存しておくことができます。これらの人々は、組織の**ユーザ**として扱われます。

LDAP ディレクトリ内のユーザ情報は、各ユーザエントリのさまざまな属性に基づいて効率的に検索できるようになっています。ユーザエントリに関連付けられている属性には、氏名やその他の ID、部署、職名、勤務地、マネージャ名、直属の上司名、組織内の各部へのアクセス権限などがあります。

組織内に電子メッセージングサービスがある場合は、大部分またはすべてのユーザがメールアカウントを持っているはずです。iPlanet Messaging Server の場合、メールアカウント情報はローカルサーバではなく LDAP ユーザディレクトリの一部であり、各メールアカウントに関する情報はユーザエントリのメール属性としてディレクトリに保存されます。

特定のユーザのメールアカウントに関する情報を表示または変更する場合は、ディレクトリ内にあるそのユーザのメール属性にアクセスします。メール属性には、iPlanet Console (本章後述) または iPlanet Delegated Administrator for Messaging のインターフェースからアクセスできます。また、LDAP ツールを使って直接 LDAP を変更することも可能です。

この章では、iPlanet Console を使ってユーザのメールアカウントやメーリングリストを作成および管理する方法について説明しています。ただし、ユーザ、グループ、およびドメインの管理には、iPlanet Delegated Administrator for Messaging または LDAP ツールの使用をお勧めします。

Delegated Administrator for Messaging は、ユーザ、グループ、ファミリグループ、およびホストドメインの管理を完全にサポートしているため、ユーザやグループの管理を委託したり、ホストドメインごとに管理者を設定することができます。また、Delegated Administrator は GUI インターフェースを備えているため、管理者がユーザやグループを管理したり、エンドユーザが自分のメールアカウントを管理する場合に便利です。さらに、管理者はユーザやグループの管理に Delegated Administrator コマンドラインユーティリティ を使用することもできます。Delegated Administrator の詳細については、『Delegated Administrator Installation and Administration Guide』および Delegated Administrator のオンラインヘルプを参照してください。また、LDAP ツールを使用してユーザ、グループ、ドメインを管理する方法については、『Messaging Server Provisioning Guide』を参照してください。

コンソールを使用する場合は、ユーザディレクトリ内のユーザに対して以下のタスクを実行できます。

- ユーザのメールアカウントにアクセスする
- アカウントのメールアドレス情報を指定する
- アカウントのメール配信方法および属性を定義する
- アカウントのメール転送先アドレスおよび属性を指定する
- アカウントの自動返信方法を指定する

ユーザディレクトリ内のグループに対しては、以下のタスクを実行できます。

- グループのメーリングリストにアクセスする
- メーリングリストのアドレス情報を指定する
- メーリングリストの**電子メール専用**メンバーを指定する
- メーリングリストに掲示されるメッセージの制約を定義する
- メーリングリストのメッセージ拒否通知アクションを定義し、有効にする

これらの各種管理タスクについては、この章の各項でそれぞれ詳しく説明します。ただし、管理タスクを実行するには、まず次項を参考にしてメール管理インターフェースを使用できるようにする必要があります。

メールユーザを管理する

メールユーザにアクセスする

この項では、ユーザのためにメール管理インターフェースを開く方法について説明します。Messaging Server のメールアカウントは、ユーザエントリの属性として、セントラル LDAP ユーザディレクトリ内に保存されているため、メールアカウントを操作するには、ディレクトリ内のユーザエントリにアクセスする必要があります。

新規ユーザを作成する

新規メールアカウントを作成するには、ディレクトリ内で新規ユーザを作成し、そのユーザ用にメールアカウントをインストールします。メールアカウントをインストールしなければ、そのユーザはコンソールのメール管理機能を使用できません (ユーザの作成およびユーザ情報の設定については、『Netscape Console によるサーバの管理』の第 4 章「ユーザとグループの管理」を参照してください)。

新規メールユーザを作成するには :

1 コンソールのメインウィンドウで [ユーザおよびグループ] タブをクリックします。

2 ドロップダウンリストで [新規ユーザ] を選択し、[作成] をクリックします。

3 ユーザが属する組織単位を選択し、[OK] をクリックします。[ユーザの作成] ウィンドウが開きます。

4 ユーザに関する情報を入力します。詳細については、『Netscape Console によるサーバの管理』の第 4 章「ユーザとグループの管理」を参照してください。

5 [ユーザの作成] ウィンドウを開いたままの状態で、[アカウント] タブをクリックします。このユーザアカウントに対して使用できる製品が右のパネルに一覧表示されます。

6 [メールアカウントのインストール] ボックスをクリックします。[ユーザの作成] ウィンドウに [メール] タブが表示されます。

7 [ユーザの作成] ウィンドウの [メール] タブをクリックしてから右のパネルにある任意のタブをクリックします。

8 必要に応じて内容を変更し、[ユーザの作成] ウィンドウの下端にある [OK] をクリックします。

注 必要な作業をすべて完了したことを確認してから [OK] をクリックしてください。

既存のユーザにアクセスする

既存のメールアカウントに変更を加える場合や、既存のユーザにメール機能を与える場合は、ディレクトリ内でそのユーザにアクセスし、メールアカウントの属性を追加または変更します。

既存ユーザのメール情報にアクセスするには :

1 コンソールのメインウィンドウで [ユーザおよびグループ] タブをクリックします。

2 [ユーザおよびグループ] のメインウィンドウで [検索] または [高度な検索] をクリックします。

3 [検索] ウィンドウに検索条件 (例 : ユーザの姓) を入力してユーザディレクトリを検索します。

4 [ユーザおよびグループ] のメインウィンドウに戻り、検索結果の中から任意のユーザを選択して [編集] をクリックします。

5 [エントリの編集] ウィンドウに [メール] タブが表示されない場合は、以下の操作を実行します。

   a. [アカウント] タブをクリックします。インストールされているアカウントが右のパネルに一覧表示されます。

   b. [メールアカウント] チェックボックスをオンにします。[エントリの編集] ウィンドウに [メール] タブが表示されます。

6 [エントリの編集] ウィンドウで [メール] タブをクリックしてから、右のパネルで任意のタブをクリックします。

7 必要に応じて内容を変更し、[エントリの編集] ウィンドウの下端にある [OK] をクリックします。

ユーザの電子メールアドレスを指定する

メールがユーザに正しく配信されるようにするには、ユーザのメールアドレス情報を指定する必要があります。アドレス情報は、Messaging Server ホスト名、ユーザのプライマリ電子メールアドレス、およびその他のアドレスから構成されています。ホスト名とプライマリアドレスは必ず指定する必要がありますが、その他のアドレスは指定しなくてもかまいません。

ユーザのメールアドレス情報を指定するには :

1 コンソールから [ユーザの作成] ウィンドウまたは [エントリの編集] ウィンドウにアクセスします。手順については、42 ページの「メールユーザにアクセスする」を参照してください。

2 [メール] タブをクリックします。

3 [設定] タブが非アクティブになっている場合は、クリックしてアクティブにします。

4 (必須) Messaging Server ホスト名を入力します。

   これは、ユーザのメールを処理する Messaging Server ホストマシン名です。Messaging Server が認識できる完全なドメイン名 (FQDN) を入力してください。

5 (必須) ユーザのプライマリ電子メールアドレスを入力します。

   プライマリアドレスは、ユーザのアドレスとして公開される電子メールアドレスです。RFC 821 に準拠する有効なフォーマットの SMTP アドレスを使用してください。

   送信メールのヘッダ部分に記されるユーザアドレスにホスト名を表示したくない場合は、このフィールドにホスト名を入力しないでください。代わりに、以下に示される手順に従って、ホスト名を含むその他のアドレスを指定します。

6 (オプション) [その他のアドレス] リストにアドレスを入力します。

その他のアドレスとは、基本的にそのユーザのプライマリアドレスのエイリアスに当たるものです。その他のアドレスは、以下の目的に利用できます。

- スペルを間違いやすいアドレスにメールが正しく配信されるようにする (たとえば、プライマリアドレスが「Smythe E」の場合に、その他のアドレスとして「Smith E」と指定します)。
- 送信メールのヘッダにホスト名が表示されないようにする。このためには、プライマリアドレスにはホスト名を含めず、その他のアドレスにホスト名を含める必要があります。たとえば、プライマリアドレスを「jsmith@siroe.com」と指定し、その他のアドレスを「jsmith@sesta.com」と指定します。こうすると、ユーザが送信したメールのヘッダには jsmith@siroe.com と表示されますが、このアドレス宛てのメール (返信を含む) はすべて jsmith@sesta.com に配信されます (ただし、sesta.com が有効なホスト名である場合のみ)。

重複したアドレスを使用しない限り、各ユーザに割り当てられるその他のアドレス数に上限はありません。その他のアドレス宛てに送信されたメッセージはすべてプライマリアドレスに配信されます。

その他のアドレスを追加するには :

a. [その他のアドレス] フィールドの下にある [追加] ボタンをクリックします。

b. [その他のアドレス] ウィンドウでアドレスを入力します (アドレス数に上限はありませんが、一度に複数のアドレスを追加することはできません)。

c. [OK] をクリックして、[その他のアドレス] ウィンドウを閉じます (別のアドレスを追加する場合は、再び [追加] ボタンをクリックして、[その他のアドレス] を表示します)。

7 ユーザのメール情報を変更する作業が完了したら、[エントリの編集] の下端にある [OK] をクリックします。作業を続ける場合は、別のタブをクリックします。

配信オプションを設定する

Messaging Server には 3 種類のメール配信オプションがあり、各ユーザに対しオプションを組み合わせて使用したり、各オプションを有効にしたり、設定を変更したりすることが可能です。配信オプションには、標準 POP/IMAP 配信、プログラム配信、および UNIX 配信 (UNIX ホストのクライアント用) があります。

また、iPlanet Delegated Administrator for Messaging にもエンドユーザ向けの HTML インターフェースがあり、エンドユーザ自身がこれらのオプションを有効にしたり設定できるようになっています。コンソールのインターフェースと Delegated Administrator のインターフェースは共に同じディレクトリ属性を操作するため、どちらか一方のインターフェースを開くと、オプションを設定したのが管理者であるかユーザであるかに関わらず、最新の設定が表示されます。

ユーザの配信オプションを設定するには :

1 コンソールから [ユーザの作成] ウィンドウまたは [エントリの編集] ウィンドウにアクセスします。手順については、42 ページの「メールユーザにアクセスする」を参照してください。

2 [メール] タブをクリックします。

3 [配信] タブをクリックします。

4 1 つまたは複数の配信オプションを選択します。

- POP/IMAP 配信を指定する場合 : 46 ページの「POP/IMAP 配信を指定する」を参照してください。
- プログラム配信を指定する場合 : 46 ページの「プログラム配信を指定する」を参照してください。
- UNIX 配信を指定する場合 : 47 ページの「UNIX 配信を指定する」を参照してください。

5 ユーザのメール情報を変更する作業が完了したら、[エントリの編集] ウィンドウの下端にある [OK] をクリックします。作業を続ける場合は、別のタブをクリックします。

POP/IMAP 配信を指定する

このオプションを選択すると、ユーザの標準 POP3 または IMAP4 メールボックスへの配信が可能になります。POP/IMAP 配信を有効化するには :

1 [配信] タブをクリックします。

2 [POP/IMAP] チェックボックスをオンにし、[プロパティ] ボタンをクリックして [POP/IMAP 配信] ウィンドウを開きます。

3 (オプション) メールの配信先および保存先であるメッセージストアパーティションのニックネーム (パス名または絶対物理パス以外) を入力します。このフィールドに何も入力しないと、現在のプライマリパーティションが使用されます。詳細については、213 ページの「メッセージストアを管理する」を参照してください。

4 (オプション) ユーザに割り当てるメール保存ディスク容量の上限を設定します。デフォルト設定 (221 ページの「メッセージストアの制限容量を設定する」を参照) を使用するか、無制限に設定するか、または任意の容量 (KB/MB) を割り当てることができます。

5 (オプション) 保存可能なメッセージ数の上限を設定します。デフォルト設定 (221 ページの「メッセージストアの制限容量を設定する」を参照) を使用するか、無制限に設定するか、または任意の数を割り当てることができます。

プログラム配信を指定する

このオプションを指定すると、メールがユーザに配信される前に外部アプリケーションに転送されるようになります。

注 この項では、ユーザがプログラム配信オプションを選択できるようにする方法について説明します。ただし、このオプションを使用できるようにするには、まずいくつかの管理タスクを実行して、プログラム配信用のモジュール全体を有効にする必要があります。詳細については、139 ページの「チャネル定義を設定する」を参照してください。

このユーザについてプログラム配信を有効にするには :

1 [配信] タブをクリックします。

2 [Program-Delivery] チェックボックスをオンにし、[プロパティ] ボタンをクリックして [プログラム配信] ウィンドウを開きます。

3 ユーザのメールを処理するための外部アプリケーションコマンドを入力します。

4 [OK] をクリックします。

UNIX 配信を指定する

このオプションを指定すると、ユーザのメール配信方法が UNIX 配信に設定されます。すなわち、メッセージが指定の UNIX メールボックスに配信されるようになります。このオプションは、ユーザの Messaging Server が UNIX ホストマシン上で稼動している場合にのみ選択できます。

UNIX 配信を有効化するには :

1 [配信] タブをクリックします。

2 [UNIX 配信] チェックボックスをオンにします。

注 Messaging Server のユーザが UNIX 配信を使用できるようにするには、通常の UNIX メール管理タスクを実行する必要があります。

転送先アドレスを指定する

Messaging Server のメール転送機能を使用して、ユーザのプライマリアドレスおよびその他のアドレスにメールを転送したり、その他のアドレスのみにメールを転送することができます。

また、iPlanet Delegated Administrator for Messaging にはエンドユーザ向けの HTML インターフェースがあり、ユーザ自身が転送先アドレスを指定できるようになっています。コンソールのインターフェースと Delegated Administrator のインターフェースは共に同じディレクトリ属性を操作するため、どちらか一方のインターフェースを開くと、オプションを設定したのが管理者であるかユーザであるかに関わらず、最新の設定が表示されます。

メール転送先情報を指定するには :

1 コンソールから [ユーザの作成] ウィンドウまたは [エントリの編集] ウィンドウにアクセスします。詳細については、42 ページの「メールユーザにアクセスする」を参照してください。

2 [メール] タブをクリックします。

3 [転送] タブをクリックします。

転送先アドレスがすでに指定されている場合は、[転送先アドレス] フィールドに情報が表示されます。

4 転送先アドレスを追加する場合は、[追加] をクリックします。

5 [転送先アドレス] ウィンドウで転送先アドレスを入力します。

6 [OK] をクリックして [メッセージの転送] タブの [転送先アドレス] フィールドにアドレスを追加し、[転送先アドレス] ウィンドウを閉じます。

7 ユーザのメール情報を変更する作業が完了したら、[エントリの編集] ウィンドウの下端にある [OK] をクリックします。作業を続ける場合は、別のタブをクリックします。

注 同一サーバ上にあり、かつ他の配信方法が設定されていないアカウント間では、互いのアドレスを転送先アドレスに指定しないように注意してください。配信に支障をきたす場合があります。

自動返信を設定する

iPlanet Messaging Server の自動返信機能を使用して、受信したメールに対する返信メッセージが自動的に送られるよう設定できます。自動返信には、エコーモード、Vacation モード、自動返信モードの 3 種類があります。

iPlanet Delegated Administrator for Messaging にはエンド ユーザ向けの HTML インターフェースがあり、ユーザ自身が自動返信の設定を有効にしたり、変更したりできるようになっています。コンソールのインターフェースと Delegated Administrator のインターフェースは共に同じディレクトリ属性を操作するため、どちらか一方のインターフェースを開くと、オプションを設定したのが管理者であるかユーザであるかに関わらず、最新の設定が表示されます。

自動返信サービスを使用できるようにするには :

1 コンソールから [ユーザの作成] ウィンドウまたは [エントリの編集] ウィンドウにアクセスします。詳細については、42 ページの「メールユーザにアクセスする」を参照してください。

2 [メール] タブをクリックします。

3 [自動返信] タブをクリックします

4 以下のいずれかのモードを選択します。

オフ : 自動返信機能を無効にします。

エコー : 受信した各メッセージに対して自動的に返信します。このモードを選択した場合は、[メッセージ] フィールドに任意のメッセージを入力できます。

Vacation : 各差出人から送られた最初のメッセージに対してのみ自動的に返信メッセージが送られます。同一の差出人から複数のメッセージが送られてきた場合は、自動返信の設定がタイムアウトになるまで 2 通目以降のメッセージには返信されません。タイムアウトになると、次のタイムアウトまでの期間に受信した同一差出人からの最初のメッセージに対して、再び自動的に返信メッセージが送られます。このモードを選択した場合は、[Vacation 開始日 / 終了日] オプションを使用し、[返信テキスト] フィールドにメッセージを入力してください。

5 Vacation モードを選択した場合は、自動返信を開始および終了する日時を設定する必要があります。

- [Vacation 開始日 / 終了日] チェックボックスをオンにします。
- [編集] ボタンをクリックし、表示されるカレンダーを使って開始および終了の日時を設定します。

6 タイムアウトを日または時間単位で設定します。

7 エコーモードまたは Vacation モードを選択した場合は、自動返信用の件名およびメッセージを入力する必要があります。

内部からの差出人と外部からの差出人に対して、それぞれ異なるメッセージを設定することができます。内部からの差出人に対してのみ自動返信を設定すると、同じドメイン内の差出人だけにメッセージが送信されます。

また、メッセージテキスト領域の上にあるドロップダウンリストには、複数の使用可能な言語が表示されます。各言語について 1 つずつメッセージを作成できます。

8 ユーザのメール情報を設定する作業が完了したら、[エントリの編集] ウィンドウの下端にある [OK] をクリックします。作業を続ける場合は、別のタブをクリックします。

認可されているサービスを設定する

ユーザがアクセスできるメールサービスを有効にするには :

1 コンソールから [ユーザの作成] ウィンドウまたは [エントリの編集] ウィンドウにアクセスします。詳細については、42 ページの「メールユーザにアクセスする」を参照してください。

2 [メール] タブをクリックします。

3 [認可されているサービス] タブをクリックします。

[認可されているサービス] ウィンドウに、該当ドメインで使用できるサービスが表示されます。

4 目的に合わせて [追加]、[編集]、[削除] ボタンをクリックします。いずれかのボタンをクリックすると、[認証済みサービスの規則を変更] ウィンドウが表示されます。

5 ドロップダウンリストから、規則を指定するサービス (IMAP、POP、SMTP、HTTP、またはすべて) を選択します。

6 [許可] または [拒否] を選択し、規則を適用するドメインを指定します。

7 [OK] をクリックして変更内容を反映させます。

メーリングリストを管理する

メーリングリストにアクセスする

この項では、管理インターフェースからメーリングリストにアクセスする方法について説明します。Messaging Server のメーリングリストは、グループエントリの属性として LDAP ユーザディレクトリに保存されているため、メーリングリストを管理するには、ディレクトリグループにアクセスして修正する必要があります。

新規グループを作成する

新規メーリングリストを作成するには、ディレクトリ内で新規グループを作成し、そのグループ用にメールアカウントをインストールします。メールアカウントをインストールしなければ、そのグループに対してコンソールのメール管理機能を使用することはできません (グループの作成およびグループ情報の設定については、『Netscape Console によるサーバの管理』の第 4 章「ユーザとグループの管理」を参照してください)。

新規メーリングリストを作成するには :

1 コンソールのメインウィンドウで [ユーザおよびグループ] タブをクリックします。

2 ドロップダウンリストから [新規グループ] を選択し、[作成] をクリックします。

3 グループが属する組織単位を選択し、[OK] をクリックします。

4 [グループの作成] ウィンドウで、グループに関する情報を入力します。詳細については、『Netscape Console によるサーバの管理』の第 4 章「ユーザとグループの管理」を参照してください。

注意 : メーリングリストの作成だけを目的とする場合は、[ユーザおよびグループ] タブからメンバーを追加する**必要はありません**。[メールアカウント電子メール専用メンバー] タブを使用できます。

- グループの正規メンバーには、メーリングリストに関する一般的な権限、およびグループ特定のその他の権限が与えられます。正規メンバー (スタティックまたはダイナミック) を追加するには、[メンバー] タブを使用します。
- メーリングリストメンバーには、グループ作成の目的がメーリングリストの使用だけであるかどうかに関わらず、メーリングリストに関する権限しか与えられません。メーリングリストのメンバーは、**電子メール専用メンバー**と呼ばれます。電子メール専用メンバーを追加するには、[メール] タブを使います。

5 [グループの作成] ウィンドウを開いたままの状態で、[アカウント] タブをクリックします。

このグループアカウントに対して使用できる製品のリストが、右パネルに表示されます。

6 [メールアカウント] チェックボックスをオンにします。

[グループの作成] ウィンドウに [メール] タブが表示されます。

7 [グループの作成] ウィンドウの [メール] タブをクリックしてから右パネルのタブをクリックします。

8 必要に応じて内容を変更し、[グループの作成] ウィンドウの下端にある [OK] をクリックします。

エントリが作成され、[グループの作成] ウィンドウが閉じます。

注 メール管理用の各ウィンドウの下端にある [OK] ボタンをクリックすると、メール管理用の各タブを使って設定した情報がすべて有効になります。必要な作業をすべて完了したことを確認してから [OK] をクリックしてください。

既存のグループにアクセスする

既存のメーリングリストに変更を加える場合や、既存のグループにメーリングリスト機能を与える場合は、ディレクトリ内でそのグループにアクセスしてメールアカウントの属性を追加または変更します。

既存のグループのメーリングリスト情報にアクセスするには :

1 コンソールのメインウィンドウで [ユーザおよびグループ] タブをクリックします。

2 [ユーザおよびグループ] のメインウィンドウで [検索] または [高度な検索] をクリックします。

3 ウィンドウに検索条件 (例 : グループ名) を入力してユーザディレクトリの検索を実行します。

4 [ユーザおよびグループ] のメインウィンドウに戻り、検索結果の中から任意のグループを選択して [編集] をクリックします。

5 [エントリの編集] ウィンドウに [メール] タブが表示されない場合は、以下の操作を実行します。

- [アカウント] タブをクリックします。インストールされているアカウントが右のパネルに一覧表示されます。
- [メールアカウント] チェックボックスをオンにします。[エントリの編集] ウィンドウに [メール] タブが表示されます。

6 [エントリの編集] ウィンドウで [メール] タブをクリックしてから、右のパネルで任意のタブをクリックします。

(右のパネルに表示されるタブは、[グループの作成] ウィンドウからアクセスできるタブと同一のものです。)

7 必要に応じて内容を変更し、[エントリの編集] ウィンドウの下端にある [OK] をクリックします。

メーリングリストの設定を指定する

メールがメーリングリストに正しく配信されるようにするためには、リストのメールアドレス情報を指定する必要があります。アドレス情報は、グループのプライマリアドレス、およびプライマリアドレスのエイリアスであるその他のアドレスから構成されます。さらに、メーリングリストの所有者、説明、メンバー、属性、制約、返信に関するアクションなどを指定することも可能です。

メーリングリスト情報を指定するには :

1 コンソール から [グループの作成] ウィンドウまたは [エントリの編集] ウィンドウにアクセスします。手順については、50 ページの「メーリングリストにアクセスする」を参照してください。

2 [メール] タブをクリックします。

3 [設定] タブが非アクティブになっている場合は、クリックしてアクティブにします。

4 (必須) メーリングリストのプライマリ電子メールアドレスを入力します。

プライマリアドレスは、このメーリングリストのアドレスとして公開されるアドレスです。各メーリングリストが複数のプライマリアドレスを持つことはできません。また、プライマリアドレスには RFC 821 に準拠する有効なフォーマットの SMTP アドレスを使用してください。

5 (オプション) メーリングリストのその他のアドレスを指定します。

その他のアドレスとは、グループのプライマリアドレスのエイリアスに当たるものです。その他のアドレスは、以下の目的に利用できます。

- スペルを間違いやすいアドレスにメールが正しく配信されるようにする。
- 送信メールのヘッダにホスト名を表示しないようにする。このためには、プライマリ アドレスにホスト名を含めず、その他のアドレスにホスト名を含めます。

重複したアドレスを使用しない限り、各グループに割り当てられるその他のアドレス数に上限はありません。その他のアドレス宛てに送信されたメッセージはすべてプライマリアドレスに配信されます。

その他のアドレスを追加するには :

a. [その他の電子メールアドレス] フィールドの下にある [追加] ボタンをクリックします。

b. [その他の電子メールアドレス] ウィンドウでアドレスを入力します (アドレス数に上限はありませんが、一度に複数のアドレスを追加することはできません)。

c. [OK] をクリックして、[その他の電子メールアドレス] ウィンドウを閉じます (別のアドレスを追加する場合は、再び [追加] ボタンをクリックして、[その他の電子メールアドレス] ウィンドウを表示します)。

6 (オプション) メーリングリスト宛てに送信されたメッセージが配信不能の場合に、エラーメッセージが送られるようにする場合は、[エラー] フィールドにエラーメッセージの宛先を入力します。

7 (オプション) [メッセージングサーバのホスト名] フィールドにメーリングリストのホストであるマシンのホスト名を入力します。

[プライマリ電子メールアドレス] フィールドにホスト名が含まれている場合は、このフィールドに何も入力しなくてもかまいません。ただし、プライマリ電子メールアドレスでホスト名を省略した場合は、必ずここでホスト名を指定してください。

ユーザ用のメールアカウントの場合とは異なり、メーリングリストのホスト名を指定しないと、そのリストの LDAP エントリにアクセスできるすべてのホストがリストを処理できることになります (ただし、多くの場合は、故意にそのような設定が使われます)。特定ホストのみがリストを処理できるように設定する場合は、ホスト名を指定する必要があります。たとえば、大規模なリストを負荷の小さいサーバで処理するように設定すれば、他のサーバの負荷を軽減できます。

注意 : このウィンドウで一度に複数のホスト名を入力することはできません。複数のホスト名を入力するには、`ldapmodify` コマンドラインユーティリティを使用してください。

8 (オプション) メーリングリストの所有者を入力します。

リスト所有者には、ユーザの追加や削除、設定の変更、リストの削除などの管理権限が与えられます。

メーリングリストの所有者を指定するには、[所有者] タブをクリックして、以下のいずれかの操作を実行します。

- [追加] をクリックし、[リスト所有者の DN を入力] ウィンドウで新しい所有者の識別名 (DN) を入力して (例 : `uid=jsmith, ou=people, o=siroe.com`)、[OK] をクリックします。
- [検索] をクリックして、[ユーザおよびグループを検索] ウィンドウを開き、所有者を検索します。

注意 : このウィンドウで所有者を選択すると、自動的に適切な DN 構文が表示されます。[ユーザおよびグループを検索] ウィンドウの詳細については、『Netscape Console によるサーバの管理』の第 4 章「ユーザとグループの管理」を参照してください。

9 (オプション) メーリングリストに関する説明を入力します。

Messaging Server が使用するためではなく、説明としてテキストや URL を入力するには、以下のいずれかまたは両方の作業を行います。

- メーリングリストの目的や特徴に関する説明を入力します。
- メーリングリストについての情報が記載されている HTML ページの URL を入力します。この情報は参考用であり、Messaging Server が使用するためのものではないことに注意してください。

10 メーリングリスト情報の変更作業が完了したら、[エントリの編集] ウィンドウの下端にある [OK] をクリックします。作業を続ける場合は、別のタブをクリックします。

リストメンバーを指定する

メーリングリストに電子メール専用メンバーを追加するには、以下のいずれかまたは両方の作業を行います。

- 各メンバーを 1 人ずつメーリングリストに追加します。
- ユーザディレクトリにフィルタとしてダイナミック検索条件を適用します。

ここでは、コンソールの [ユーザおよびグループ] インターフェース上で**電子メール専用メンバー**と表示されるメーリングリストメンバーについて説明します。電子メール専用メンバーには、メーリングリストに関する権限のみが与えられます。「正規」メンバーを追加する手順については、『Netscape Console によるサーバの管理』を参照してください。通常、正規メンバーには、電子メール専用メンバーを上回る権限や責任が与えられます。グループの詳細については、『Netscape Console によるサーバの管理』の第 4 章「ユーザとグループの管理」を参照してください。

メンバーのダイナミック検索条件を定義する

ダイナミック検索条件は、ユーザディレクトリ内でメンバーを検索する際にフィルタとして適用される LDAP 検索 URL によって構成されています。グループ宛てにメッセージが届いた場合、このメカニズムによって、静的な名簿ではなくディレクトリ検索に基づいて、どのユーザにメッセージが配信されるかが決定されます。そのため、各メンバーの情報を詳細にたどらなくても、大規模あるいは複雑なグループを作成し、管理することができます。

LDAP 検索フィルタには、必ず LDAP URL 構文のフォーマットを使用してください。LDAP フィルタを構築する方法については、『Netscape Console によるサーバの管理』の第 4 章「ユーザとグループの管理」、iPlanet Directory Server の関連マニュアル、および RFC 1959 を参照してください。

LDAP URL の構文は、以下の要素から構成されています。

```
ldap://hostname:port/base_dn?attributes?scope?filter
```

URL の各オプションには、以下の意味があります。

表 3-1　LDAP URL オプション

オプション	説明
hostname	Directory Server のホスト名 (デフォルト設定は Messaging Server が使用する Directory Server のホスト名)
port	LDAP サーバのポート番号。ポート番号が指定されていない場合は、Messaging Server が使用するデフォルトの標準 LDAP ポートが使用されます。
base_dn	検索ベースとして使用されるディレクトリエントリの識別名。この部分は必ず指定してください。
attributes	検索結果として返される属性。これらの属性は、Messaging Server によって返されます。
scope	検索範囲 :
	「base」を範囲として設定すると、検索ベース (*base_dn*) レベルの情報のみが検索対象になります。
	「one」を範囲として設定すると、検索ベースの 1 つ下のレベルの情報が検索対象になります (検索ベースレベルは含まれません)。
	「sub」を範囲として設定すると、検索ベースおよびその下のレベルにあるすべての情報が検索対象になります。
filter	検索範囲内のエントリに適用されるフィルタ。フィルタが指定されていない場合は、(objectclass=*) が使用されます。

以下は、「Sunnyvale」をメールホストとするユーザをフィルタする LDAP 検索 URL の一例です。

```
ldap:///o=Siroe Corp,c=US??sub?(&(mailHost=sunnyvale.siroe.com)
    (objectClass=inetLocalMailRecipient))
```

この URL は、組織名 Siroe (o=Siroe)、所在地米国 (c=US)、メールホスト名 Sunnyvale (mailHost=sunnyvale) のユーザをフィルタするためのものです。objectClass 属性は、検索対象のエントリの種類を定義するもので、この場合は inetLocalMailRecipient (objectClass=inetLocalMailRecipient) となっています。

コンソールを使用して検索フィルタを作成した場合、グループ名はすべて無視され、検索結果にはユーザ名だけが表示されることに注意してください。これは、グループメンバーでもあるユーザの名前が重複して表示されることを避けるための設定です。コマンドライン設定ユーティリティ (configutil) を使うとこの設定を無効化できますが、コマンドラインの使用はできるだけ避けてください。

次の項で説明しているとおり、検索 URL は、[コンソールのテンプレート] ウィンドウ ([LDAP 検索 URL の作成] ウィンドウ) を使用して作成できます。

メーリングリストにメンバーを追加する

メーリングリストに (電子メール専用) メンバーを追加するには :

1 コンソールから [グループの作成] ウィンドウまたは [エントリの編集] ウィンドウにアクセスします。手順については、50 ページの「メーリングリストにアクセスする」を参照してください。

2 [メール] タブをクリックします。

3 [電子メール専用メンバー] タブをクリックします。

- (オプション) メンバーの検索に LDAP 検索 URL を使用する場合は、[電子メール専用メンバーのダイナミック検索条件] フィールドの下にある [追加] ボタンをクリックし、[ダイナミック検索条件の追加] ウィンドウで以下の作業を行います。
- フィールドに LDAP 検索 URL を入力するか、[構築] タブをクリックして検索 URL のテンプレートである [LDAP 検索 URL の作成] ウィンドウを開きます。
- [OK] をクリックして [電子メール専用メンバーのダイナミック検索条件] フィールドに入力した条件を有効にし、[ダイナミック検索条件の追加] ウィンドウを閉じます。

LDAP 検索 URL の構築については、54 ページの「メンバーのダイナミック検索条件を定義する」を参照してください。

4 (オプション) メーリングリストに個々のメンバーを追加するには、[電子メール専用のメンバー] フィールドの下にある [追加] ボタンをクリックし、[電子メール専用メンバーの追加] ウィンドウで以下の作業を行います。

- フィールドに新規メンバーのプライマリアドレスを入力します。RFC 821 に準拠する有効なフォーマットの SMTP アドレスを入力してください。グループ用に制約を設定する場合は特に、その他のアドレスは指定しないでください。フィールドに複数のアドレスを入力することはできないため、このウィンドウで一度に複数のメンバーを追加することはできません。
- [OK] をクリックしてリストにメンバーを追加し、[電子メール専用メンバーの追加] ウィンドウを閉じます。別のアドレスを入力するには、再び [追加] をクリックして、[電子メール専用メンバーの追加] ウィンドウを開きます。

5 メーリングリスト情報の変更作業が完了したら、[エントリの編集] ウィンドウの下端にある [OK] をクリックします。作業を続ける場合は、別のタブをクリックします。

メッセージ送信に関する制約を定義する

メーリングリスト宛てに送信されるメッセージにさまざまな制約を設けることができます。たとえば、特定のユーザのみにリストへの送信を許可する、差出人の認証を要求する、メッセージの送信元を制限する、メッセージのサイズを制限する、などの制約を設けることができます。制約条件を満たさないメッセージは拒否されます。

注 これらの制約は、リスト宛てに送信されるメッセージを制御するためには便利ですが、高度なセキュリティのアクセス制御を保証するものではありません。

グループに対するメッセージ送信の制約を定義するには :

1 コンソールから [グループの作成] ウィンドウまたは [エントリの編集] ウィンドウにアクセスします。手順については、50 ページの「メーリングリストにアクセスする」を参照してください。

2 [メール] タブをクリックします。

3 [制約] タブをクリックします。

4 (オプション) 以下の中からいずれかのオプションを選び、送信を許可する差出人を定義します。

- **すべて :** 差出人を制限しない場合は、このオプションを選択します (デフォルト設定)。ただし、このオプションを選択した場合は、次の手順で説明している SMTP 認証を選択できなくなることに注意してください。
- **メーリングリストのすべて :** メーリングリストメンバー (電子メール専用メンバー以外のグループメンバーも含む) だけにリストへのメッセージ送信を許可します。
- **次のリストのすべて :** フィールドに記載されたユーザだけにリストへのメッセージ送信を許可します。

[メーリングリストのすべて] を選択した場合、リストにユーザを追加するには、[許可された差出人] フィールドの下にある [追加] をクリックします。または、[検索] をクリックして、[ユーザおよびグループを検索] ウィンドウを開くこともできます。[追加] をクリックすると、[許可された差出人の追加] ウィンドウが開きます。許可を与えたいユーザの電子メールアドレスまたは識別名 (DN) を入力してください。[OK] をクリックすると、[許可された差出人] フィールドにユーザが追加され、ウィンドウが閉じます。上記の手順を繰り返して追加したいユーザをすべて追加します。

[ユーザおよびグループを検索] ウィンドウの詳細については、『Netscape Console によるサーバの管理』を参照してください

5 (オプション) 送信元を制限するために、差出人のドメインを定義します。

- [許可された差出人ドメイン] フィールドの下にある [追加] ボタンをクリックします。
- [許可された差出人ドメインの追加] ウィンドウでドメイン名を入力し、[OK] をクリックしてドメインをリストに追加します。

入力したドメインにサブドメインがある場合は、それらのサブドメインもすべて自動的に含まれることに注意してください。たとえば、`siroe.com` には `sales.siroe.com` が含まれます。

6 (オプション) メッセージサイズの上限を指定します。

サイズをバイト単位で入力してください。

7 メーリングリスト情報の設定作業が完了したら、[エントリの編集] ウィンドウの下端にある [OK] をクリックします。作業を続ける場合は、別のタブをクリックします。

モデレータを定義する

メーリングリストには、1 人または複数のモデレータを追加できます。

モデレータが転送メッセージを受信すると、その処理方法はモデレータによって決められます (モデレータが複数存在する場合は、最初のモデレータが決定することになります)。メッセージは、承認処理のあとリストに転送 (パスワードの指定も可能)、または削除という形で処理されます。

メーリングリストのモデレータを定義するには :

1 コンソールから [グループの作成] ウィンドウまたは [エントリの編集] ウィンドウにアクセスします。手順については、50 ページの「メーリングリストにアクセスする」を参照してください。

2 [メール] タブをクリックします。

3 [モデレータ] タブをクリックします。

4 [モデレータのリスト] フィールドの下の [追加] ボタンをクリックします。

5 [モデレータの追加] ウィンドウで、モデレータのプライマリ電子メールアドレスまたは識別名 (DN) を入力します。個々のアドレスを入力するか、または [検索] をクリックして [ユーザおよびグループを検索] ウィンドウを開き、アドレスを検索することが可能です。ただし、一度に複数のモデレータを追加することはできません。

   [ユーザおよびグループを検索] ウィンドウの詳細については、『Netscape Console によるサーバの管理』を参照してください。

6 [OK] をクリックしてリストにモデレータを追加し、[モデレータの追加] ウィンドウを閉じます (別のアドレスを追加するには、再び [追加] をクリックして [モデレータの追加] ウィンドウを開きます)。

7 メーリングリスト情報の変更作業が完了したら、[エントリの編集] ウィンドウの下端にある [OK] をクリックします。作業を続ける場合は、別のタブをクリックします。

第 4 章

POP、IMAP、および HTTP サービスを設定する

iPlanet Messaging Server は、メールボックスへのクライアントアクセス用に POP3 (Post Office Protocol 3)、IMAP4 (Internet Mail Access Protocol 4)、および HTTP (HyperText Transfer Protocol) をサポートします。IMAP および POP は、ともにインターネット標準のメールボックスプロトコルです。Web 対応の電子メールプログラムである Messenger Express を使用すると、エンドユーザがインターネットに接続したコンピュータ上のブラウザ (HTTP を使用) を介してメールボックスにアクセスできます。

この章では、iPlanet Console またはコマンドラインユーティリティを使って、これらのサービスを使用できるようにサーバを設定する方法について説明します。SMTP (Simple Mail Transfer Protocol) サービスの設定については、第 6 章 「MTA サービスと設定について」を参照してください。

この章には、以下の項目があります。

- 一般的な設定
- ログインの必要条件
- パフォーマンスパラメータ
- クライアントアクセスの制御
- POP サービスを設定する
- IMAP サービスを設定する
- HTTP サービスを設定する

一般的な設定

Messaging Server の POP、IMAP および HTTP サービスに関する一般的な設定には、サービスの有効化 / 無効化、ポート番号の割り当て、および接続したクライアントへ送信するサービスの見出し修正 (オプション) などが含まれます。この項では予備知識としての情報を提供していますが、設定の手順について知りたい場合は、66 ページの「POP サービスを設定する」、68 ページの「IMAP サービスを設定する」、および 70 ページの「HTTP サービスを設定する」を参照してください。

サービスを有効または無効にする

特定の Messaging Server インスタンスが POP、IMAP または HTTP サービスを使用できるかどうかを制御することができます。これはサービスの起動 / 停止とは異なり (26 ページの「サービスを起動 / 停止する」を参照)、POP、IMAP または HTTP が有効になっており、かつ起動していなければなりません。

サービスの有効化は、サービスを起動 / 停止するよりもグローバルなプロセスです。たとえば、[有効化] の設定はシステムを再起動した場合でも維持されますが、以前停止したサービスはシステムを再起動した後にもう一度起動しなければなりません。

使用する予定のないサービスを有効にする必要はありません。たとえば、Messaging Server のインスタンスをメッセージ転送エージェント (MTA) としてのみ使用する場合は、POP、IMAP および HTTP を無効にします。また、POP サービスだけを使用する場合は IMAP および HTTP を無効にし、Web ベースの電子メールだけを使用する場合は POP および IMAP を無効にします。

ポート番号を指定する

各サービスに対して、サーバがサービスの接続に使用するポート番号を指定できます。

- POP サービスを有効にする場合は、サーバが POP 接続に使用するポート番号を指定できます。デフォルトは 110 です。
- IMAP サービスを有効にする場合は、サーバが IMAP 接続に使用するポート番号を指定できます。デフォルトは 143 です。
- HTTP サービスを有効にする場合は、サーバが HTTP 接続に使用するポート番号を指定できます。デフォルトは 80 です。

ただし、たとえば 1 つのホストマシンに複数の IMAP サーバインスタンスがある場合や、同じホストマシンを IMAP サーバおよび Messaging Multiplexor サーバとして使用している場合は、デフォルト以外のポート番号を指定する必要があります。Messaging Multiplexor の詳細については、第 5 章 「Messaging Multiplexor」を参照してください。

ポート番号を指定する際には、以下の点に注意してください。

- ポート番号には、1 から 65535 までの任意の値を指定できます。
- 選択したポートが別のサービス用にすでに使用されていたり、割り当てられていないことを確認してください。

暗号化通信用のポート

Messaging Server は、SSL (Secure Sockets Layer) プロトコルを使用することにより、IMAP および HTTP クライアントの暗号化通信をサポートします。Messaging Server の SSL サポートに関する詳細については、259 ページの「暗号化と証明書に基づく認証を設定する」を参照してください。

SSL を使用した IMAP

「SSL を使用した IMAP」のデフォルトポート番号 (993) を使用するか、または「SSL を使用した IMAP」に別のポートを指定することができます。

現在の IMAP クライアントの多くが個別の IMAP ポートおよび SSL を使用した IMAP ポートを必要としているため、Messaging Server ではオプションとしてそれぞれに個別のポートを使用できます。最近では、同じポートによる IMAP および「SSL を使用した IMAP」の通信が新たな標準となってきています。お使いの Messaging Server に SSL の証明書 (261 ページの「証明書を入手する」を参照) がインストールされていれば、同じポートを使って IMAP および「SSL を使用した IMAP」の通信を行うことができます。

SSL を使用した HTTP

「SSL を使用した HTTP」のデフォルトポート番号 (443) を使用するか、または「SSL を使用した HTTP」に別のポートを指定することができます。

サービスの見出し

クライアントがはじめて Messaging Server の POP または IMAP のポートに接続すると、サーバがクライアントに確認用のテキスト文字列を送信します。このサービスの見出し (通常、クライアントのユーザには表示されません) は、サーバが iPlanet Messaging Server であることを証明するもので、そこにはサーバのバージョン番号が表示されます。一般に、この見出しはクライアントのデバッグや問題を突きとめるために使われます。

接続中のクライアントに異なるメッセージを送信したい場合は、POP または IMAP サービスのデフォルトの見出しを変更できます。

サービスの見出しを設定するには、iPlanet Console または `configutil` ユーティリティを使用します。`configutil` についての構文の詳細については、『Messaging Server リファレンスマニュアル』を参照してください。

ログインの必要条件

ユーザは POP、IMAP、または HTTP サービスにログインしてメールを取り込みます。このユーザによるログインの方法は制御できます。この場合、パスワードに基づくログイン (全サービス)、または証明書に基づくログイン (IMAP または HTTP サービス) のいずれかをユーザに対して許可します。この項では予備知識としての情報を提供していますが、設定の手順について知りたい場合は、66 ページの「POP サービスを設定する」、68 ページの「IMAP サービスを設定する」、70 ページの「HTTP サービスを設定する」を参照してください。

パスワードに基づくログイン

一般的なメッセージングシステムの場合、ユーザはメールクライアントにパスワードを入力して POP、IMAP または HTTP メールボックスにアクセスします。クライアントがサーバにパスワードを送信すると、サーバはそのパスワードを使ってユーザを認証します。ユーザが認証されると、アクセス制御規則に基づき、そのサーバに保存されている特定のメールボックスへのアクセスを許可するかどうかが決定されます。

パスワードログインを認めると、ユーザはパスワードを入力することにより POP、IMAP または HTTP にアクセスできるようになります (POP サービスにおける認証方法は、パスワードに基づくログインのみです)。パスワードは、LDAP ディレクトリに保存されます。パスワードの必要最小文字数などのポリシーは、ディレクトリポリシーによって決まります。

IMAP または HTTP サービスに対してパスワードログインを認めない場合は、パスワードに基づく認証が許可されません。その場合、次の項で説明するように、ユーザは証明書に基づくログインを行わなければなりません。

IMAP および HTTP サービスにおけるパスワード送信のセキュリティを強化するために、サーバに送信する前にパスワードを暗号化するように要求できます。これを行うには、ログインに対する符号化の必要条件を選択します。

- 暗号化の必要がない場合にはゼロを選択します。クライアントポリシーによって、パスワードは平文で、または暗号化されて送信されます。
- ゼロ以外の値を選択すると、クライアントは指定した値を満たすキー長の符号化方式を使って、サーバとの SSL セッションを確立しなければなりません。これにより、クライアントが送信する IMAP または HTTP のユーザパスワードがすべて暗号化されます。

クライアントにおける暗号化のキー長設定がサーバのサポートする最大長より大きい場合、またはサーバにおける暗号化のキー長設定がクライアントのサポートする最大長より大きい場合は、パスワードに基づくログインを行うことができません。さまざまな符号化方式やキー長をサポートするようにサーバを設定する方法については、264 ページの「SSL を有効にする符号化方式を選択する」を参照してください。

証明書に基づくログイン

パスワードに基づくログインのほかに、iPlanet サーバはユーザのデジタル証明書を確認することにより認証を行うことができます。サーバとの SSL セッションを確立する際に、クライアントはパスワードの代わりにユーザの証明書を提示します。証明書の妥当性が確認されると、ユーザが本人であると見なされます。

IMAP または HTTP サービスに対し、証明書に基づくログインを認めるように Messaging Server を設定する方法については、267 ページの「証明書に基づくログインを設定する」を参照してください。

証明書に基づくログインを有効にするために、IMAP または HTTP システムフォームの [パスワードログインの許可] チェックボックスをオフにする必要はありません。チェックボックスが選択されていても (デフォルト)、証明書に基づくログインの設定を行った場合は、パスワードに基づくログインと証明書に基づくログインの両方がサポートされます。その場合、クライアントが SSL セッションを確立し、証明書を提示すると、証明書に基づくログインが使用されます。クライアントが SSL を使用しない場合や、クライアント証明書を提示しない場合には、代わりにパスワードが送信されます。

パフォーマンスパラメータ

Messaging Server の POP、IMAP、および HTTP サービスに対し、いくつかの基本的なパフォーマンスパラメータを設定できます。これらのパラメータを調整すれば、ハードウェアの容量に基づきユーザベースで最も効率的なサービスを実行できます。この項では予備知識としての情報を提供していますが、設定の手順について知りたい場合は、66 ページの「POP サービスを設定する」、68 ページの「IMAP サービスを設定する」、または 70 ページの「HTTP サービスを設定する」を参照してください。

プロセス数

Messaging Server は、作業をいくつかの実行プロセスに分けることができ、それによって効率が上がることがあります。この機能は、特にマルチプロセッササーバマシンにおいて効果があり、サーバプロセス数を調整することにより、ハードウェアプロセッサ間で複数のタスクを効率よく分配できます。

ただし、複数のプロセスにタスクを分散したり、1 つのプロセスから別のプロセスに切り替えたりする際には、パフォーマンスオーバーヘッドが発生します。プロセスが 1 つ追加されるごとに、複数のプロセスを持つ利点が薄れていきます。ほとんどの設定では、サーバマシンの各ハードウェアプロセッサ当たり 1 つのプロセス (最大限 4 つのプロセスまで) を割り当てるのが原則です。用途によっては最適とされる設定が異なることがあるため、この原則はあくまでも参考として把握しておいてください。

注 : プラットフォームによっては、パフォーマンスに影響を与える可能性のある、そのプラットフォーム固有のプロセスに対する制限 (最大ファイルディスクリプタ数など) を緩くするために、プロセス数を増やしたほうがよいこともあります。

POP、IMAP、および HTTP サービスのデフォルトのプロセス数は、1 です。

プロセス当たりの接続数

POP、IMAP、または HTTP サービスが同時に持てるクライアント接続の数が多いほど、クライントにとっては有利になります。空いている接続がないためにクライアントがサービスにアクセスできない場合、別のクライアントが接続を切断するまで待たなければなりません。

一方、各オープン接続がそれぞれメモリリソースを消費し、サーバマシンの入出力サブシステムに負担をかけるため、実際にサーバがサポートできる同時セッションの数には限界があります (サーバのメモリを増やすか入出力を拡大すれば、制限枠を上げることができます)。

IMAP、HTTP および POP には、それぞれ以下のような違いがあります。

- IMAP 接続は、POP 接続や HTTP 接続に比べ、一般的に長く維持できます。メッセージをダウンロードするためにユーザが IMAP に接続すると、接続は通常ユーザが終了するか、タイムアウトになるまで維持されたままです。これに対し、POP 接続や HTTP 接続は、通常 POP または HTTP リクエストが満たされると同時に閉じられます。
- 一般に、IMAP および HTTP 接続は、POP 接続に比べて非常に効率的です。POP 接続の場合は、再接続するたびにユーザの認証を必要とします。これに対し、IMAP 接続の場合は認証が必要なのは 1 回のみで、IMAP セッション (ログインからログアウトまで) が終わるまで接続が維持されます。HTTP 接続は短いですが、1 回の HTTP セッション (ログインからログアウトまで) で複数の接続が許可されているため、ユーザは接続するたびに再び認証を行う必要はありません。そのため、POP 接続は IMAP 接続や HTTP 接続よりも大幅なパフォーマンスオーバーヘッドを生じます。iPlanet Messaging Server は、オープン IMAP 接続 (ただし、アイドル接続) と複数の HTTP 接続によって、オーバーヘッドを減らすように設計されています。

注 HTTP セッションのセキュリティの詳細については、255 ページの「HTTP のセキュリティについて」を参照してください。

したがって、所定の時間とユーザの要求により、Messaging Server は IMAP または HTTP 接続を POP 接続よりも多くサポートできる場合があります。

プロセス当たりの接続数は、IMAP のデフォルトが 4000、HTTP のデフォルトが 6000、POP のデフォルトが 600 です。これらの値は、一般的な設定のサーバマシンが処理できる要求の概略値です。用途によっては最適とされる設定が異なることがあるため、これらのデフォルト値はあくまでも一般的なガイドラインとして参考にしてください。

プロセス当たりのスレッド数

複数のプロセスをサポートするほかに、Messaging Server では複数のスレッドにタスクを分配することにより、さらにパフォーマンスを上げることができます。サーバがスレッドを使うと、処理中のコマンドがほかのコマンドの実行を妨げることがなくなるため、実行の効率性が向上します。コマンドの実行中、必要に応じてスレッドが作成され破棄されます。スレッドは、設定した最大数まで作成できます。

同時に実行されるスレッドがより多いほど、多くのクライアントのリクエストを遅滞なく処理することができ、より多くのクライアントに迅速にサービスを提供できます。ただし、スレッド間のディスパッチがパフォーマンスオーバーヘッドになるため、実際にサーバが使用できるスレッド数には限界があります。

POP、IMAP、および HTTP のプロセス当たりの最大スレッド数は、デフォルトで 250 です。IMAP および HTTP のデフォルトの接続数が POP のデフォルト値より大きいにも関わらず、この数値は同じになります。同じ最大スレッド数で、より多くの IMAP および HTTP 接続が、より少なく、ただし頻度の高い POP 接続と同じくらい効率よく処理されると考えられます。用途によっては最適とされる設定が異なることがありますが、これらのデフォルト値は十分高いため、設定値を大きくする必要はおそらくありません。通常、これらのデフォルト値で十分なパフォーマンスが得られます。

アイドル接続を切断する

応答のないクライアントへの接続に使用されているシステムリソースを回復するために、IMAP4、POP3、および HTTP プロトコルは、一定の時間が過ぎたアイドル接続をサーバが一方的に切断することを許可します。

それぞれのプロトコル仕様により、サーバはアイドル接続を指定されている最小時間オープンにしておくことが要求されます。最低時間のデフォルト値は、POP が 10 分、IMAP が 30 分、HTTP が 3 分です。デフォルト値を増やすことはできますが、減らすことはできません。

POP 接続または IMAP 接続が切断された場合、ユーザは新たに接続するときに再び認証される必要があります。これに対し、HTTP 接続が切断された場合は、HTTP セッションがオープンされたままなので、再認証の必要はありません。HTTP セッションのセキュリティの詳細については、255 ページの「HTTP のセキュリティについて」を参照してください。

POP のアイドル接続は、通常クライアントが応答できない何らかの問題 (クラッシュやハングするなど) により起こります。一方、IMAP のアイドル接続は、正常な状態で起こります。IMAP ユーザが一方的に切断されるのを防ぐため、通常 IMAP クライアントは IMAP サーバに 30 分以下の一定間隔でコマンドを送信します。

HTTP クライアントをログアウトする

HTTP セッションは、複数の接続にわたって維持されます。HTTP クライアントは、接続が切断されてもログアウトされません。ただし、HTTP セッションが指定された時間以上アイドル状態であると、サーバは自動的に HTTP セッションを切断し、クライアントはログアウトされます (デフォルトは 2 時間)。セッションが切断されると、クライアントのセッション ID が無効になり、クライアントは新たにセッションを確立するために、再び認証されなければなりません。HTTP セッションのセキュリティおよびセッション ID の詳細については、255 ページの「HTTP のセキュリティについて」を参照してください。

クライアントアクセスの制御

iPlanet Messaging Server には、POP、IMAP、または HTTP メッセージングサービス (および SMTP) にアクセスできるクライアントを決定するためのアクセス制御機能があります。さまざまな条件に基づき、クライントのアクセスを許可または拒否する柔軟なアクセスフィルタを作成できます。

クライアントアクセスの制御は、iPlanet Messaging Server に備わっている重要なセキュリティ機能です。クライアントアクセスの制御フィルタおよびその使用法の例については、270 ページの「POP、IMAP、および HTTP サービスへの クライアントアクセスを設定する」および 280 ページの「SMTP サービスへのクライアントアクセスを設定する」を参照してください。

POP サービスを設定する

Messaging Server の POP サービスに関する基本的な設定は、`configutil` コマンドまたは iPlanet Console を使って行うことができます。

関連項目 :

- 60 ページの「サービスを有効または無効にする」
- 60 ページの「ポート番号を指定する」
- 64 ページの「プロセス当たりの接続数」
- 65 ページの「アイドル接続を切断する」
- 64 ページの「プロセス当たりのスレッド数」
- 63 ページの「プロセス数」

コンソール - iPlanet Console を使って POP サービスを設定するには :

1. iPlanet Console で、設定する Messaging Server を開きます。
2. [環境設定] タブをクリックし、左側のパネルで [サービス] フォルダを開きます。
3. [POP] を選択します。
4. 右ペインで [システム] タブをクリックします。
5. サービスを有効にするには、[ポートで POP サービスを有効化] チェックボックスをオンにし、ポート番号を指定します。

6 接続の設定を以下のように指定します。

- プロセス当たりの最大ネットワーク接続数を設定します。詳細については、64 ページの「プロセス当たりの接続数」を参照してください。
- 接続の最大アイドル時間を設定します。詳細については、65 ページの「アイドル接続を切断する」を参照してください。

7 プロセス設定を次のように指定します。

- プロセス当たりの最大スレッド数を設定します。詳細については、64 ページの「プロセス当たりのスレッド数」を参照してください。
- 最大プロセス数を設定します。詳細については、63 ページの「プロセス数」を参照してください。

8 必要に応じて、POP サービスの見出しフィールドにサービスの見出しを指定します。

9 [保存] をクリックします。

注 POP サービスの場合は、パスワードに基づくログインが自動的に有効になります。

コマンドライン - 以下に示すように、コマンドラインから POP 属性の値を設定できます。

POP サービスを有効 / 無効にするには :

```
configutil -o service.pop.enable -v [ yes | no ]
```

ポート番号を指定するには :

```
configutil -o service.pop.port -v 番号
```

プロセス当たりの最大ネットワーク接続数を設定するには :

```
configutil -o service.pop.maxsessions -v 数値
```

接続の最大アイドル時間を設定するには :

```
configutil -o service.pop.idletimeout -v 数値
```

プロセス当たりの最大スレッド数を設定するには :

```
configutil -o service.pop.maxthreads -v 数値
```

最大プロセス数を設定するには :

```
configutil -o service.pop.numprocesses -v 数値
```

プロトコルにようこそ見出しを指定するには :

```
configutil -o service.pop.banner -v 見出し
```

IMAP サービスを設定する

Messaging Server の IMAP サービスに関する基本的な設定は、`configutil` コマンドまたは iPlanet Console を使って行うことができます。関連項目：

- 60 ページの「サービスを有効または無効にする」
- 60 ページの「ポート番号を指定する」
- 62 ページの「パスワードに基づくログイン」
- 64 ページの「プロセス当たりの接続数」
- 65 ページの「アイドル接続を切断する」
- 64 ページの「プロセス当たりのスレッド数」
- 63 ページの「プロセス数」

コンソール - iPlanet Console を使って IMAP サービスを設定するには：

1. iPlanet Console で、設定する Messaging Server を開きます。
2. [環境設定] タブをクリックし、左側のパネルで [サービス] フォルダを開きます。
3. [IMAP] を選択します。
4. 右ペインで [システム] タブをクリックします。
5. サービスを有効にするには、[ポートで IMAP サービスを有効化] チェックボックスをオンにし、ポート番号を指定します。
6. 必要に応じて、パスワードに基づくログインを有効にします。
7. 接続の設定を以下のように指定します。
   - プロセス当たりの最大ネットワーク接続数を設定します。詳細については、64 ページの「プロセス当たりの接続数」を参照してください。
   - 接続の最大アイドル時間を設定します。詳細については、65 ページの「アイドル接続を切断する」を参照してください。
8. プロセス設定を次のように指定します。
   - プロセス当たりの最大スレッド数を設定します。詳細については、64 ページの「プロセス当たりのスレッド数」を参照してください。
   - 最大プロセス数を設定します。詳細については、63 ページの「プロセス数」を参照してください。
9. 必要に応じて、IMAP サービスの見出しフィールドにサービスの見出しを指定します。
10. [保存] をクリックします。

コマンドライン - 以下に示すように、コマンドラインを使って IMAP 属性の値を設定できます。

IMAP サービスを有効 / 無効にするには :

```
configutil -o service.imap.enable -v [ yes | no ]
```

ポート番号を指定するには :

```
configutil -o service.imap.port -v 番号
```

「SSL を使用した IMAP」用に別のポートを有効にするには :

```
configutil -o service.imap.enablesslport -v [ yes | no ]
```

「SSL を使用した IMAP」のポート番号を指定するには :

```
configutil -o service.imap.sslport -v 番号
```

IMAP サービスでパスワードログインを有効 / 無効にするには :

```
configutil -o service.http.plaintextmincipher -v
```

値 は、次のいずれかになります。

```
 -1 - パスワードログインを無効にする
 0 - 暗号なしのパスワードログインを有効にする
 40 - パスワードログインを有効にし、暗号の強さを指定する
128 - パスワードログインを有効にし、暗号の強さを指定する
```

プロセス当たりの最大ネットワーク接続数を設定するには :

```
configutil -o service.imap.maxsessions -v 数値
```

接続の最大アイドル時間を設定するには :

```
configutil -o service.imap.idletimeout -v 数値
```

プロセス当たりの最大スレッド数を設定するには :

```
configutil -o service.imap.maxthreads -v 数値
```

最大プロセス数を設定するには :

```
configutil -o service.imap.numprocesses -v 数値
```

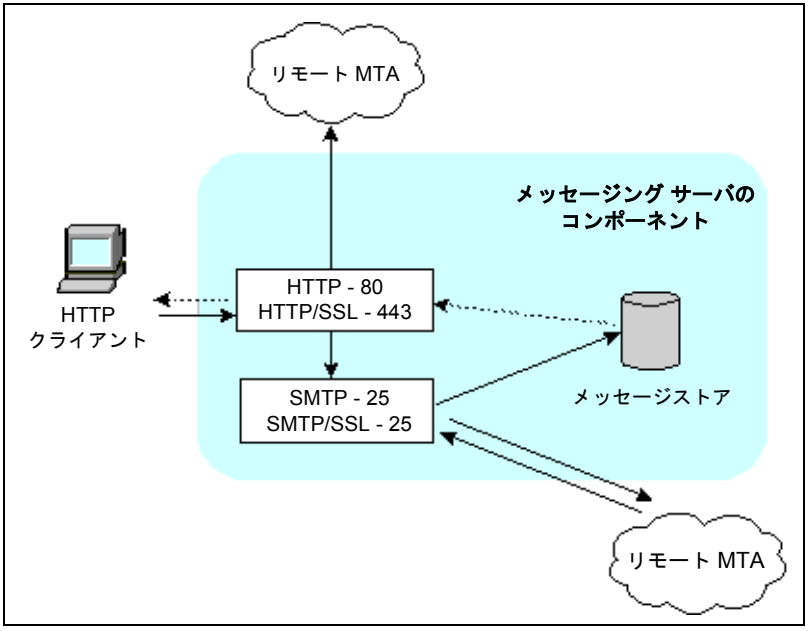
プロトコルにようこそ見出しを指定するには :

```
configutil -o service.imap.banner -v 見出し
```

HTTP サービスを設定する

POP および IMAP クライアントは、ルーティングまたは配信するためにメールを直接 iPlanet Messaging Server の MTA に送信します。これに対し、HTTP クライアントはメールを iPlanet Messaging Server の一部である特殊な Web サーバに送信します。その後、HTTP サービスは、図 4-1 に示すように、ルーティングまたは配信するためにメッセージをローカル MTA またはリモート MTA に送信します。

図 4-1 HTTP サービスのコンポーネント



HTTP 設定のパラメータの多くは、POP および IMAP サービスで提供されるパラメータに似ています。これらには、接続の設定やプロセス設定のパラメータが含まれています。関連項目：

- 60 ページの「サービスを有効または無効にする」
- 60 ページの「ポート番号を指定する」
- 62 ページの「パスワードに基づくログイン」
- 64 ページの「プロセス当たりの接続数」
- 65 ページの「アイドル接続を切断する」
- 65 ページの「HTTP クライアントをログアウトする」
- 64 ページの「プロセス当たりのスレッド数」
- 63 ページの「プロセス数」

パラメータの中には、メッセージ設定や MTA 設定など、HTTP サービスに独特なものもあります。

メッセージ設定 - HTTP クライアントが添付ファイル付きのメッセージを構成すると、添付ファイルはサーバーにアップロードされ、ファイルに保存されます。ルーティングまたは配信するためにメッセージを MTA に送信する前に、HTTP サービスは添付ファイルを取得し、メッセージを構成します。この場合、デフォルトの添付スプールディレクトリを使用するか、または代わりのディレクトリを指定することができます。また、添付ファイルの最大サイズを指定することもできます。

MTA 設定 - デフォルトにより、HTTP サービスはルーティングまたは配信するために、送信 Web メールをローカル MTA に送信します。しかし、サイトがホストサービスで、ほとんどの受信者がローカルホストマシンと同じドメインに入っていないような場合には、メールをリモート MTA に送信するように HTTP サービスを設定できます。Web メールをリモート MTA に送信するには、リモートホスト名およびリモートホストの SMTP ポート番号を指定します。

コンソール - iPlanet Console を使って HTTP サービスを設定するには :

1 iPlanet Console で、設定する Messaging Server を開きます。

2 [環境設定] タブをクリックして、左側のパネルで [サービス] フォルダを開きます。

3 [HTTP] を選択します。

4 右ペインで [システム] タブをクリックします。

5 サービスを有効にするには、[ポートで HTTP サービスを有効化] チェックボックスをオンにし、ポート番号を指定します。

6 必要に応じて、パスワードに基づくログインを有効にします。

7 接続の設定を以下のように指定します。

- プロセス当たりの最大ネットワーク接続数を設定します。詳細については、64 ページの「プロセス当たりの接続数」を参照してください。
- 接続の最大アイドル時間を設定します。詳細については、65 ページの「アイドル接続を切断する」を参照してください。
- クライアントセッションの最大アイドル時間を設定します。詳細については、65 ページの「HTTP クライアントをログアウトする」を参照してください。

8 プロセス設定を次のように指定します。

- プロセス当たりの最大スレッド数を設定します。詳細については、64 ページの「プロセス当たりのスレッド数」を参照してください。
- 最大プロセス数を設定します。詳細については、63 ページの「プロセス数」を参照してください。

9 メッセージ設定を次のように設定します。

- 必要に応じて、添付スプールディレクトリを指定します。
- 必要に応じて、送信メールの最大サイズを指定します。このサイズは base64 でエンコードされたすべての添付ファイルを対象にしていること、および base64 でエンコードするには 33% 増しの容量が必要になることから、注意が必要です。コンソールでの 5M バイトという容量制限を考慮すると、1 つのメッセージと添付ファイルの最大サイズは 3.75M バイト になります。

詳細については、71 ページの「メッセージ設定 -」を参照してください。

10 MTA 設定を次のように設定します。

- 必要に応じて、代わりの MTA ホスト名を指定します。
- 必要に応じて、代わりの MTA ポートを指定します。

詳細については、71 ページの「MTA 設定 -」を参照してください。

11 [保存] をクリックします

コマンドライン - 以下に示すように、コマンドラインを使って HTTP 属性の値を設定できます。

HTTP サービスを有効 / 無効にするには :

```
configutil -o service.http.enable -v [ yes | no ]
```

ポート番号を指定するには :

```
configutil -o service.http.port -v 番号
```

「SSL を使用した HTTP」用に別のポートを有効にするには :

```
configutil -o service.http.enablesslport -v [ yes | no ]
```

「SSL を使用した HTTP」のポート番号を指定するには :

```
configutil -o service.http.sslport -v 番号
```

パスワードログインを有効 / 無効にするには :

```
configutil -o service.http.plaintextmincipher -v 値
```

値 は、次のいずれかになります。

```
 -1 - パスワードログインを無効にする
  0 - 暗号なしのパスワードログインを有効にする
 40 - パスワードログインを有効にし、暗号の強さを指定する
128 - パスワードログインを有効にし、暗号の強さを指定する
```

プロセス当たりの最大ネットワーク接続数を設定するには :

```
configutil -o service.http.maxsessions -v 数値
```

接続の最大アイドル時間を設定するには :

```
configutil -o service.http.idletimeout -v 数値
```

クライアントセッションの最大アイドル時間を設定するには:

```
configutil -o service.http.sessiontimeout -v 数値
```

プロセス当たりの最大スレッド数を設定するには:

```
configutil -o service.http.maxthreads -v 数値
```

最大プロセス数を設定するには:

```
configutil -o service.http.numprocesses -v 数値
```

クライアントの送信メールに対する添付スプールディレクトリを指定するには:

```
configutil -o service.http.spooldir -v ディスパッチ
```

メッセージの最大サイズを指定するには:

```
configutil -o service.http.maxmessagesize -v size
```

size には、メッセージの最大サイズをバイト単位で指定します。このサイズは base64 でエンコードされたすべての添付ファイルを対象にしていること、および base64 でエンコードするには 33% 増しの容量が必要になることから、注意が必要です。コンソールでの 5M バイトという容量制限を考慮すると、1 つのメッセージと添付ファイルの最大サイズは 3.75M バイト になります。

代わりの MTA ホスト名を指定するには:

```
configutil -o service.http.smtphost -v ホスト名
```

代わりの MTA ホスト名のポート番号を指定するには:

```
configutil -o service.http.smtpport -v ポート番号
```

第 5 章

Messaging Multiplexor

この章では、iPlanet Messaging Multiplexor の概念を説明しています。この章には、以下の項があります。

- Messaging Multiplexor の概要
- Messaging Multiplexor を設定する
- Messaging Multiplexor を起動する
- システム構成例

Messaging Multiplexor のインストール手順については、『Messaging Server Installation Guide』を参照してください。また、Messaging Multiplexor の設定パラメータの詳細については、『Messaging Server リファレンスマニュアル』を参照してください。

Messaging Multiplexor の概要

iPlanet Messaging Multiplexor (MMP) は、複数のメッセージングサーバの単一接続ポイントとしての役割を担う特殊なメッセージングサーバです。Messaging Multiplexor を使用すると、大規模なメッセージングサービスプロバイダによる多数の POP メールボックスおよび IMAP メールボックスへの配信が可能になるため、メッセージング容量が増加します。この場合、すべてのユーザが 1 台の Messaging Multiplexor サーバに接続し、そこからそれぞれのメッセージングサーバにリダイレクトされることになります。

多数のユーザにメールサービスを提供する際に、Messaging Multiplexor を使用すると、多数のメッセージングサーバが存在する場合でも、ユーザからはあたかも単一のホストが存在するかのように見える環境を構築できます。

Messaging Multiplexor は iPlanet Messaging Server の一部であり、Messaging Server や他の iPlanet サーバと同時にインストールするか、または Messaging Multiplexor のみを後からインストールすることができます。

Messaging Multiplexor では、以下の操作を行うことができます。

- メールクライアントとの暗号化 (SSL) 通信および非暗号化通信。
- 証明書に基づくクライアント認証。詳細については、79 ページの「証明書に基づくクライアント認証」を参照してください。
- ユーザの事前認証。詳細については、80 ページの「ユーザの事前認証」を参照してください。
- さまざまな IP アドレスでリッスンし、ユーザ ID に自動的にドメイン名を追加する仮想ドメイン。詳細については、80 ページの「仮想ドメイン」を参照してください。
- 複数のマシンに複数の Messaging Multiplexor をインストール (各マシンごとにインストール)。詳細については、『Messaging Server Installation Guide』を参照してください。
- 1 台のサーバに複数の Messaging Multiplexor インスタンスを作成。詳細については、81 ページの「複数の Messaging Multiplexor インスタンス」を参照してください。複数のインスタンスを作成することによって、仮想ドメインを介して処理できないリッスンポートや SSL などの設定が可能になります。
- 高度な LDAP 検索。

Messaging Multiplexor の利点

負荷の大きいメッセージングサーバでは、メッセージストアに必要なディスク容量が非常に大きくなる可能性があります。しかし、ユーザのメールボックスや接続を複数のサーバに振り分ければ、各サーバの容量を増やし、パフォーマンスを向上させることができます。さらに、経済的な面でも、1 台の大きなマルチプロセッササーバマシンを使用するより、複数の小さなサーバマシンを使用した方が効率的な場合があります。

複数のメッセージングサーバを使用する場合は、Messaging Multiplexor をインストールすると非常に便利です。ユーザによるメッセージストアへのアクセスが間接的であること、および複数のメッセージングサーバ間におけるユーザアカウントの再設定が簡単なことから、以下のような利点が生まれます。

- **ユーザ管理の簡易化**

  すべてのユーザを 1 台のサーバ (POP および IMAP 用にそれぞれ Messaging Multiplexor をインストールした場合は 2 台) に接続させることで、メールクライアントを事前設定し、すべてのユーザに均一のログイン情報を提供できます。これにより、管理タスクを簡易化することができ、大量のログイン情報を配布する必要がなくなります。

  また、サーバの負荷が特に大きい場合は、複数の Messaging Multiplexor を使用し、各 Messaging Multiplexor への接続を DNS ラウンドロビンまたはロードバランシングプログラム (Cisco Systems 社の LocalDirector など) によって管理することができます。

  Messaging Multiplexor は LDAP ディレクトリに保存されている情報を使用して各ユーザのサーバを探し出すため、管理者はユーザを簡単に別のサーバに移動でき、ユーザに混乱を生じさせることもありません。管理者は、ユーザのメールボックスをサーバ間で移動し、その後 LDAP ディレクトリ内でそのユーザのエントリを更新できます。ユーザのメールアドレスやメールボックス、またはその他のクライアントプリファレンスを変更する必要はありません。

- **パフォーマンスの向上**

  メッセージストアのサイズが 1 台のマシンで処理しきれないほど大きくなった場合は、一部のメッセージを別のマシンで保存するように設定することで、負荷を調整できます。

  ユーザをクラスごとに異なるマシンに割り当てることも可能です。たとえば、プレミアムユーザをよりパワフルなマシンに割り当てたりします。

  Messaging Multiplexor はバッファリング機能を備えているため、クライアント接続が低速 (モデム接続など) の場合でも、Messaging Server が低速になることはありません。

- **コストの削減**

  Messaging Multiplexor を使用すると複数のサーバを効率的に管理できるため、1 台の大容量サーバマシンを購入する代わりに、複数の小さなサーバマシンを購入して、合計コストを抑えることが可能です。

- **スケーラビリティの向上**

  Messaging Multiplexor を使用すると、システムを簡単に拡張できます。既存のシステムを無駄にすることなく、必要に応じてマシンを追加していくことができます。

- **最小限のユーザ停止時間**

  Messaging Multiplexor を使用すると、大規模なユーザベースを複数の小さなメッセージ保存マシンに振り分けることで、ユーザのダウンタイムを最小限に抑えられます。サーバがダウンしても、影響を受けるのはそのサーバを使用しているユーザだけとなります。

- **セキュリティの向上**

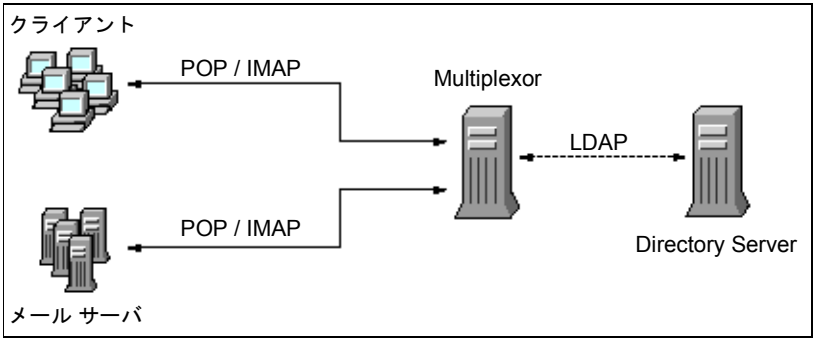
  Messaging Multiplexor をインストールしたサーバをファイアウォールとして使用できます。すべてのクライアント接続をこのサーバからルーティングすることで、外部コンピュータからの内部メッセージ保存マシンへのアクセスを制限できます。Messaging Multiplexor は、クライアントとの暗号化通信および非暗号化通信をサポートしています。

Messaging Multiplexor のしくみ

iPlanet Messaging Multiplexor は、複数のサーバマシンに割り当てられたメールユーザを一括管理するためのマルチスレッドサーバであり、受信したクライアント接続をそれぞれのメールボックスがあるサーバマシンにリダイレクトします。クライアントは直接 Messaging Multiplexor に接続し、Messaging Multiplexor を介して各々のメールボックスがあるサーバにリダイレクトされます。このため、インターネットサービスプロバイダなどが複数のマシンにメッセージストアを割り当てることが可能になり (容量の増加)、ユーザや外部クライアントに対しては、あたかも 1 台のメールホストがすべての処理タスクを担当しているかのような環境を構築できます (能率性の向上およびセキュリティの強化)。

図 5-1 は、Messaging Multiplexor をインストールした場合のシステム構成 (サーバとクライアントの関連) を示しています。

図 5-1 Messaging Multiplexor をインストールした場合のクライアントとサーバ



POP クライアントおよび IMAP クライアントはすべて、Messaging Multiplexor に接続します。Messaging Multiplexor は、接続の許可、LDAP ディレクトリの検索、適切なサーバへのクライアントのリダイレクトなどを行います。従来のメールサーバの場合と同様に、各ユーザには特定の Messaging Server の特定のアドレスおよびメールボックスが割り当てられていますが、すべての接続は Messaging Multiplexor を介してルーティングされます。

ユーザ接続は、以下の手順に基づいて確立されます。

1 ユーザの使用するクライアントマシンが Messaging Multiplexor に接続し、Messaging Multiplexor はその予備認証情報 (ユーザ名) を確認します。

2 Messaging Multiplexor が Directory Server に問い合わせてそのユーザのメールボックスがどの Messaging Server に割り当てられているかを確認します。

3 Messaging Multiplexor が該当する Messaging Server に接続して再認証を行い、接続が継続している間、そのサーバとクライアント間の中継パイプとして動作します。

暗号化 (SSL) オプション

iPlanet Messaging Multiplexor は、サーバとクライアント間の暗号化 (SSL) 通信および非暗号化通信をサポートしています。

SSL モードでは、Messaging Multiplexor がポート 993 をリッスンするようデフォルト設定されています。SSL が有効になっている場合、Messaging Multiplexor IMAP は STARTTLS をサポートします。また、SSL IMAP 接続や SSL POP 接続用に、Messaging Multiplexor がその他のポートをリッスンするように設定することも可能です。

SSL を IMAP サービスまたは POP サービスに対して有効にするには、それぞれ ImapProxyAService.cfg または PopProxyAService.cfg ファイルを編集します。また、各 IMAP サーバまたは POP サーバがセキュアサーバであるかどうかに関わらず、AService.cfg ファイルの default:ServiceList オプションを編集し、ファイル内ですべての IMAP および POP サーバポートを指定する必要があります。

SSL 設定パラメータはコメントアウトされているため、デフォルト設定では SSL が無効になっています。SSL を有効にするには、コメントアウトを外し、パラメータを設定する必要があります。SSL パラメータのリストは、『Messaging Server リファレンスマニュアル』に記載されています。

証明書に基づくクライアント認証

Messaging Multiplexor は、certmap を使用して、クライアントの証明書を Directory Server 内の該当ユーザまたはグループに照らし合わせて認証します。

証明書に基づくクライアント認証を使用できるようにするには、SSL を有効にする必要があります。詳細については、78 ページの「暗号化 (SSL) オプション」を参照してください。

さらに、メッセージストア管理者を設定する必要もあります。メール管理者の ID を使用することもできます、必要に応じて権限の設定を変更できるよう、異なる ID (例 : mmpstore) を設定するようお勧めします。

Messaging Multiplexor は certmap プラグインをサポートしていないことに注意してください。代わりに、certmap.conf ファイルの拡張された DNComps および FilterComps プロパティ値エントリを受け入れます。これらのエントリのフォーマットは、以下のとおりです。

マップ名 :DNComps *FROMATTR=TOATTR*
マップ名 :FilterComps *FROMATTR=TOATTR*

こうすると、証明書の subjectDN の *FROMATTR* 値を使って、*TOATTR*= *値*という要素を含む LDAP クエリを形成。たとえば、証明書の subjectDN が「cn=Pilar Lorca, ou=pilar o=siroe.com」の場合、この証明書を LDAP クエリ「(uid=pilar)」にマップするには、以下の行を使用します。

マップ名 :FilterComps ou=uid

IMAP サービスに対して証明書に基づく認証を有効にするには、以下の手順に従います。

1 メッセージストア管理者の ID を決定します。

メール管理者の ID を使用することもできますが、メッセージストア管理者用に ID を別途作成することをお勧めします (例 : mmpstore)。

2 SSL が有効になっていることを確認します。詳細については、78 ページの「暗号化 (SSL) オプション」を参照してください。

3 certmap.conf ファイルの場所を指定し、Messaging Multiplexor が証明書に基づくクライアント認証を実行するように設定します。

ユーザの事前認証

Messaging Multiplexor には、受信ユーザとしてディレクトリにバインドし、その結果を記録することによってユーザを事前認証するオプションがあります。

注	この機能を有効にすると、サーバのパフォーマンスが低下します。

ログエントリのフォーマットは、以下のとおりです。

日付 時刻 (sid 0x%p) user *名前* pre-authenticated - client IP *アドレス*

*日付*のフォーマットは yyyymmdd、*時刻*のフォーマットは hhmmss です。また、sid はセッションオブジェクトを示し、user *名前* には仮想ドメインが含まれます (存在する場合)。IP アドレスはドットで区切られた 4 つの数字で示されます。

仮想ドメイン

仮想ドメインはさまざまな IP アドレスでリッスンし、ユーザ ID に自動的にドメイン名を追加します。また、仮想ドメインは代替設定を指定するためにも使用できます。

Messaging Multiplexor は IP アドレスをドメイン名にマップできるため、LDAP ディレクトリを検索したり、保存サーバにログインすることができます。サーバの IP アドレスが仮想ドメインマッピングファイルにある場合は、クライアント接続が許可されると、LDAP 検索およびそれに続く再認証のため、ユーザ ID にドメイン名が追加されます。この機能は、ユーザ ID 名領域が重複する複数ドメインをホストする場合に便利です。

仮想ドメインを有効にするには、インスタンスディレクトリ内にある ImapProxyAService.cfg ファイルおよび PopProxyAService.cfg ファイルのいずれかまたは両方が仮想ドメインマッピングファイルを参照するように編集します。

仮想ドメインファイルの各エントリには、以下の構文を使用します。

vdmap *名前 IP アドレス*
名前: *パラメータ 値*

*名前*部分には任意の名前を指定し、*IP アドレス*部分にはドット 4 進表記で指定します。さらに、*パラメータ*および*値*のペアで仮想ドメインを設定します。仮想ドメインの設定パラメータ値を指定すると、これらのパラメータ値はグローバル設定パラメータ値よりも優先されます。

仮想ドメインに指定できる設定パラメータは以下のとおりです。

AuthCacheSize および AuthCacheSizeTTL
AuthService
BindDN および BindPass
CanonicalVirtual
CertMap
CRAMs
DomainDelim
HostedDomains
LdapCacheSize および LdapCacheTTL
LdapURL
MailHostAttrs
PreAuth
ReplayFormat
StoreAdmin および StoreAdminPass
SearchFormat
TCPAccess
VDomain

設定パラメータの詳細については、『Messaging Server リファレンスマニュアル』を参照してください。

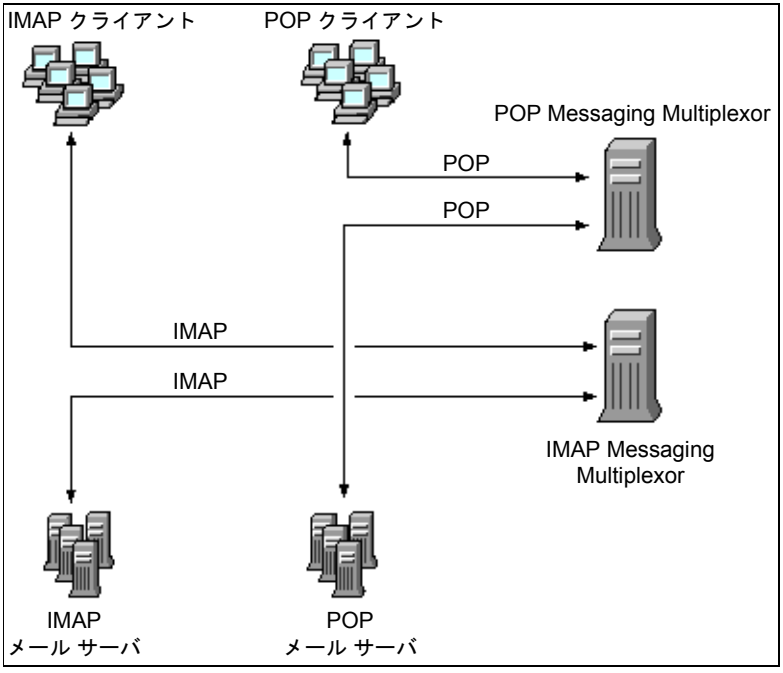
複数の Messaging Multiplexor インスタンス

複数の Messaging Multiplexor インスタンスを作成する場合は、必ずすべてのインスタンスを同一サーバ上に作成する必要があります。つまり、複数のサーバにそれぞれ 1 つずつ Messaging Multiplexor をインストールするか、または 1 台のサーバに複数のインスタンスを作成します。

複数の Messaging Multiplexor インスタンスを使用することで、仮想ドメインでは処理できない設定 (例 : SSL やリッスンポートなど) が可能になります。

また、1 つの Messaging Multiplexor インスタンスが POP プロトコルおよび IMAP プロトコルの両方をサポートするように設定したり (図 5-1 を参照)、各プロトコル用に別々の Messaging Multiplexor インスタンスを作成することも可能です (図 5-2 を参照)。メッセージングサービスを複数のマシンに振り分けることで、各マシンのパフォーマンスを最大限に引き上げることができます。

図 5-2 各プロトコル用に別々の Messaging Multiplexor インスタンスを作成した場合



複数の Messaging Multiplexor インスタンスを作成する手順については、『Messaging Server Installation Guide』を参照してください。

Messaging Multiplexor を設定する

Messaging Multiplexor を設定するには、表 5-1 に示す Messaging Multiplexor 設定ファイルの設定パラメータを手作業で編集する必要があります。

表 5-1　Messaging Multiplexor 設定ファイル

ファイル	説明
PopProxyAService.cfg	POP サービス用の環境変数を指定する設定ファイル。
ImapProxyAService.cfg	IMAP サービス用の環境変数を指定する設定ファイル。
AService.cfg	起動するサービス、および POP サービスと IMAP サービスが共有するオプションを指定する設定ファイル。

Messaging Multiplexor 設定ファイルは、*サーバ- ルート* /mmp- *ホスト名* ディレクトリに保存されています。*サーバ- ルート*部分には Messaging Server をインストールしたディレクトリ、mmp- *ホスト名*部分には Messaging Multiplexor インスタンスにちなんで付けられたサブディレクトリ名を指定します。たとえば、tarpit というマシンのデフォルト位置に Messaging Multiplexor をインストールした場合、設定ファイルは /usr/iplanet/server5/mmp-tarpit に保存されます。

また、パラメータの例を挙げると、LogDir パラメータおよび LogLevel パラメータは、3 つの設定ファイルすべての中で使用されています。これらのパラメータは、ImapProxyAService.cfg ファイルでは IMAP 関連イベントのロギングパラメータを設定するために、また、PopProxyAService.cfg ファイルではロギングパラメータを設定するために使われています。stored -d オプションを使ってデータベースに一貫性を持たせることができない場合には、以下に示す手順を上から順番に実行してください。

すべてのサーバを停止します。

server-root/msg-instance/store/mboxlist 内のすべてのファイルを削除します。

サーバプロセスを再起動します。

reconstruct -m を実行して、POP 関連イベントのスプール area.meters の内容から新規のメールボックスデータベースを作成します。ただし、AService.cfg ファイルの LogDir および LogLevel は、POP サービスまたは IMAP サービスの起動に失敗した場合など、MMP 全般に関する問題を記録するために使用されています。

Messaging Multiplexor 設定パラメータの詳細については、『Messaging Server リファレンスマニュアル』を参照してください。

Messaging Multiplexor を起動する

UNIX システム

UNIX システムで Messaging Multiplexor を起動するには、*サーバ- ルート* /mmp- *ホスト名* ディレクトリにある AService.rc スクリプトを以下のように指定して実行します。

./AService.rc [*オプション*]

AService.rc スクリプトのオプションパラメータについては、表 5-2 を参照してください。

表 5-2　AService.rc スクリプトのオプション パラメータ

オプション	説明
start	Messaging Multiplexor を起動します (すでに別のインスタンスが起動している場合を含む)。
stop	最後に起動した Messaging Multiplexor を停止します。
restart	最後に起動した Messaging Multiplexor を停止し、新たにインスタンスを起動します。
reload	アクティブな接続に影響を与えることなく、稼働中の Messaging Multiplexor の設定を再び読み込みます。

Windows NT システム

Windows NT で Messaging Multiplexor のインスタンスを起動するには、Windows NT コントロールパネルの [サービス] で [開始] をクリックします。また、[停止] をクリックすると MMP を停止できます。以下の表 5-3 は、サービスのオプションとその説明をまとめたものです。

表 5-3　Windows NT MMP サービスのオプション

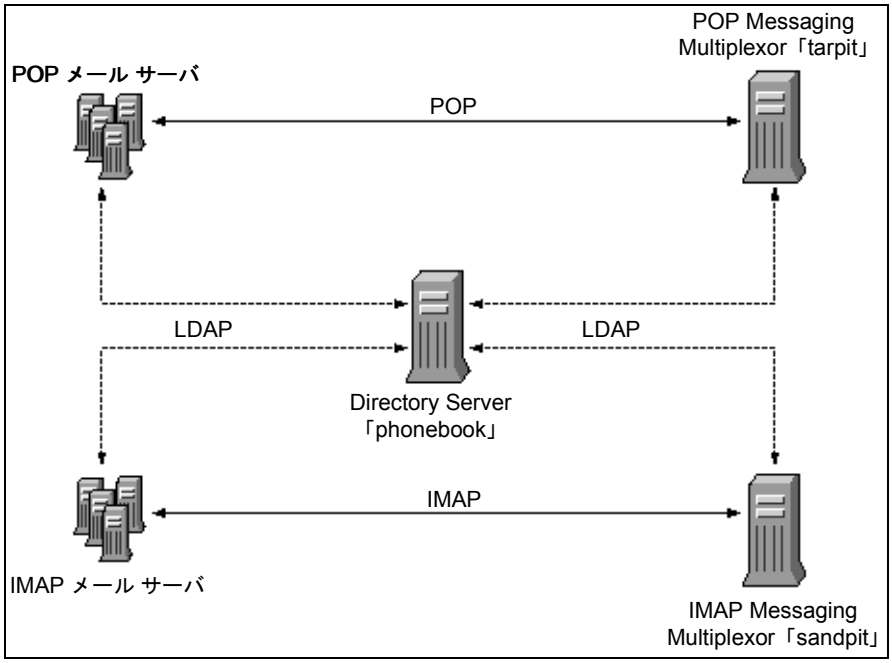
オプション	説明
start	コントロールパネルで MMP を起動するか (すでに実行中の場合も含む)、コマンドラインで AService.exe start コマンドを実行する
stop	コントロールパネルで最後に起動した MMP を停止するか、コマンドラインで AService.exe stop コマンドを実行する
restart	Windows NT で再起動するために、最後に起動した MMP を停止し、MMP を起動する
reload	MMP を再読み込みするために、mmp-instance ディレクトリに移動し、コマンドラインで AService.exe refresh コマンドを実行する

システム構成例

架空の企業である Siroe Corporation には、Messaging Multiplexor をインストールしたマシンが 2 台あり、各マシンがそれぞれ複数のサーバをサポートするよう設定されているとします。POP ユーザおよび IMAP ユーザのメールボックスは、複数の Messaging Server マシンに振り分けられており、各マシンは POP 専用または IMAP 専用として設定されています (IMAP サーババイナリを削除すると POP サービスへのクライアントアクセスのみを制限でき、同様に、POP サーババイナリを削除すると IMAP サービスへのクライアントアクセスのみを制限できます)。また、各 Messaging Multiplexor は、POP または IMAP のいずれかのみをサポートするように設定されています。LDAP ディレクトリサービスは、専用のマシンに別途インストールされています。

図 5-3 に、このシステム構成を示します。

図 5-3 複数 の Messaging Multiplexor が複数のサーバをサポートしている場合



IMAP 設定の例

図 5-3 の IMAP Messaging Multiplexor は、2 つのプロセッサを持つ `sandpit` にインストールされ、IMAP 接続の標準ポート (143) をリッスンするように設定されています。この Messaging Multiplexor は LDAP サーバ `phonebook` からユーザのメールボックス情報を得て、クライアントを適切な IMAP サーバにルーティングします。また、IMAP 機能文字列の無効化、仮想ドメインファイルの提供、SSL 通信のサポートなどのタスクも行います。

この Messaging Multiplexor の ImapProxyAService.cfg 設定ファイルの内容は、以下のとおりです。

```
default:LdapUrl             ldap://phonebook/o=Siroe.com
default:LogDir              /usr/iplanet/server5/mmp-sandpit/log
default:LogLevel            5
default:BindDN              "cn=Directory Manager"
default:BindPass            secret
default:BacksidePort        143
default:Timeout             1800
default:Capability          "IMAP4 IMAP4rev1 ACL QUOTA LITERAL+ NAMESPACE UIDPLUS
CHILDREN LANGUAGE XSENDER X-NETSCAPE XSERVERINFO AUTH=PLAIN"
default:SearchFormat        (uid=%s)
default:SSLEnable           yes
default:SSLPorts            993
default:SSLSecmodFile       /usr/iplanet/server5/mmp-sandpit/secmod.db
default:SSLCertFile         /usr/iplanet/server5/mmp-sandpit/cert7.db
default:SSLKeyFile          /usr/iplanet/server5/mmp-sandpit/key3.db
default:SSLKeyPasswdFile    ""
default:SSLCipherSpecs      all
default:SSLCertNicknames    Siroe.com Server-Cert
default:SSLCacheDir         /usr/iplanet/server5/mmp-sandpit
default:SSLBacksidePort     993
default:VirtualDomainFile   /usr/iplanet/server5/mmp-sandpit/vdmap.cfg
default:VirtualDomainDelim  @
default:ServerDownAlert     "your IMAP server appears to be temporarily out of
service"
default:MailHostAttrs       mailHost
default:PreAuth             no
default:CRAMs               no
default:AuthCacheSize       10000
default:AuthCacheTTL        900
default:AuthService         no
default:AuthServiceTTL      0
default:BGMax               10000
default:BGPenalty           2
default:BGMaxBadness        60
default:BGDecay             900
default:BGLinear            no
default:BGExcluded          /usr/iplanet/server5/mmp-sandpit/bgexcl.cfg
default:ConnLimits          0.0.0.0|0.0.0.0:20
default:LdapCacheSize       10000
default:LdapCacheTTL        900
default:HostedDomains       yes
default:DefaultDomain       Siroe.com
```

POP 設定の例

図 5-3 の POP Messaging Multiplexor は、4 つのプロセッサを持つ tarpit マシンにインストールされ、POP 接続の標準ポート (110) をリッスンするように設定されています。この Messaging Multiplexor は、LDAP サーバ phonebook からユーザのメールボックス情報を得て、クライアントを適切な POP サーバにルーティングし、スプーフメッセージ ファイルを提供します。

この Messaging Multiplexor の PopProxyAService.cfg 設定ファイルの内容は、以下のとおりです。

```
default:LdapUrl             ldap://phonebook/o=Siroe.com
default:LogDir              /usr/iplanet/server5/mmp-tarpit/log
default:LogLevel            5
default:BindDN              "cn=Directory Manager"
default:BindPass            password
default:BacksidePort        110
default:Timeout             1800
default:Capability          "IMAP4 IMAP4rev1 ACL QUOTA LITERAL+ NAMESPACE UIDPLUS
CHILDREN LANGUAGE XSENDER X-NETSCAPE XSERVERINFO AUTH=PLAIN"
default:SearchFormat        (uid=%s)
default:SSLEnable           no
default:VirtualDomainFile   /usr/iplanet/server5/mmp-tarpit/vdmap.cfg
default:VirtualDomainDelim  @
default:MailHostAttrs       mailHost
default:PreAuth             no
default:CRAMs               no
default:AuthCacheSize       10000
default:AuthCacheTTL        900
default:AuthService         no
default:AuthServiceTTL      0
default:BGMax               10000
default:BGPenalty           2
default:BGMaxBadness        60
default:BGDecay             900
default:BGLinear            no
default:BGExcluded          /usr/iplanet/server5/mmp-tarpit/bgexcl.cfg
default:ConnLimits          0.0.0.0|0.0.0.0:20
default:LdapCacheSize       10000
default:LdapCacheTTL        900
default:HostedDomains       yes
default:DefaultDomain       Siroe.com
```

第 6 章

MTA サービスと設定について

この章では、サーバにおける MTA サービスの設定に関する概念を説明します。この章には、以下の項目があります。

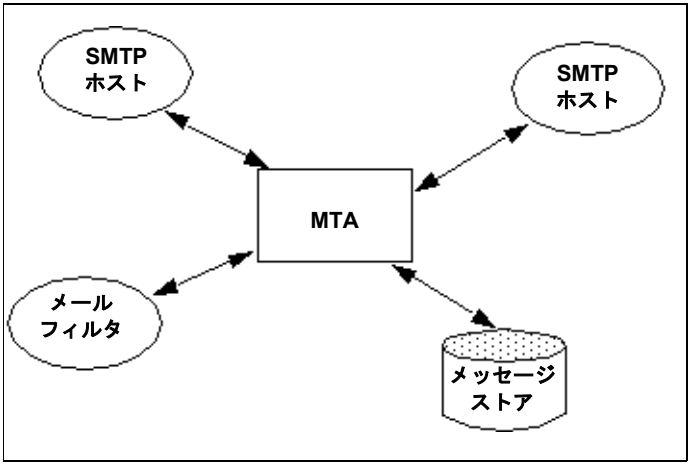
- メッセージ転送エージェント (MTA)
- チャネル
- 書き換え規則
- ジョブコントローラ
- ディスパッチャ
- MTA 設定ファイル
- その他の MTA 設定ファイル
- エイリアス
- コマンドラインユーティリティ
- MTA ディレクトリキャッシュ
- SMTP セキュリティとアクセス制御
- ログファイル

メッセージ転送エージェント (MTA)

Messaging Server の MTA は、インターネット標準に基づいた保存および転送用メッセージングシステムです。メッセージ転送エージェント (MTA) は、メッセージが適切な受取人に配信されるように、メッセージのルーティング方法を決定します。図 6-1 に示すように、MTA は以下の操作を行います。

- 別の SMTP ホストにメッセージをルーティングします。
- ローカルメッセージストアにメッセージを配信します。
- メッセージ処理プログラム (メールをフィルタするなど) にメッセージを配信します。

図 6-1　　MTA のルーティングと配信



チャネル

チャネルとは、メッセージを処理するための基本的な MTA コンポーネントです。チャネルは、別のコンピュータシステムまたはシステムグループとの接続を表します。実際のハードウェア接続やソフトウェアトランスポート (またはその両方) は、チャネルによって大きく異なることがあります。

チャネルには、以下のような機能があります。

- メッセージをリモートシステムに送信し、その後でメッセージをキューから削除します。
- リモートシステムからメッセージを受信し、適切なチャネルキューに保存します。
- メッセージをローカルのメッセージストアに配信します。
- メッセージを特殊処理プログラムに配信します。

メッセージは、MTA に入るときにチャネルによってキュー内に配置され、MTA から出るときに取り出されます。通常、メッセージは 1 つのチャネルを介して入り、別のチャネルを介して送り出されます。チャネルは、メッセージを取り出して処理したり、または別の MTA チャネルのキューに配置したりします。

チャネルは、プライマリ MTA 設定ファイル `imta.cnf` で定義します。また、MTA オプションファイル `option.dat` でチャネルのグローバルオプションを設定したり、チャネルオプションファイルで特定のチャネルを設定することもできます。

MTA 設定ファイルの詳細については、95 ページの「MTA 設定ファイル」を参照してください。オプションファイルの詳細については、101 ページの「オプションファイル」および 98 ページの「TCP/IP チャネルオプションファイル」を参照してください。チャネルの設定の詳細については、第 8 章 「チャネル定義を設定する」を参照してください。

マスタープログラムとスレーブプログラム

通常、チャネルには 2 つのプログラムがあります。マスターおよびスレーブと呼ばれるプログラムです。リモートシステムへの送信を開始するチャネルプログラムが「マスタープログラム」で、リモートシステムから開始された送信を受け取るプログラムが「スレーブプログラム」です。

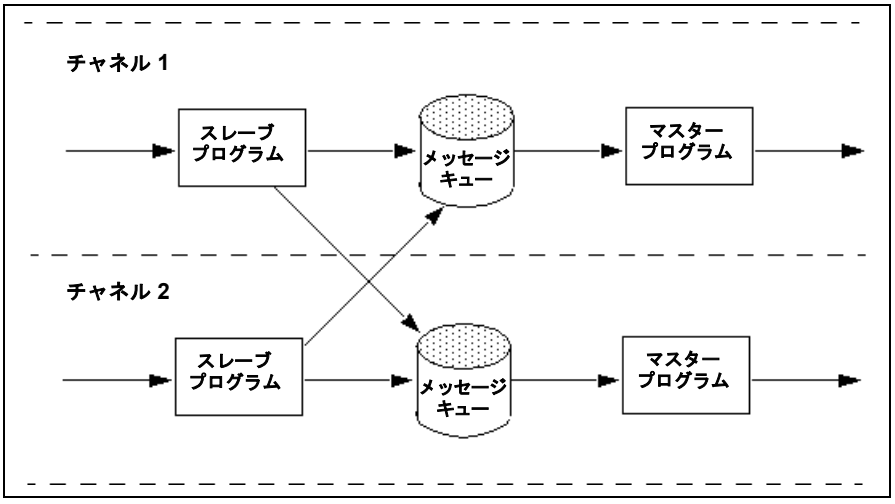
たとえば、SMTP チャネルには、メッセージを送信するマスタープログラムと、メッセージを受信するスレーブプログラムがあります。これらは、それぞれ SMTP クライアントおよびサーバに相当します。

- 通常、マスタープログラムは、MTA が発した送信接続を管理します。マスターチャネルプログラムには、以下のような機能があります。
  - ローカルの処理リクエストに応えて起動します。
  - チャネルメッセージからメッセージを取り出します。
  - 宛先フォーマットが、待機中のメッセージのフォーマットと異なる場合は、必要な変換をアドレス、ヘッダ、および内容に対して行います。
  - メッセージのネットワーク転送を開始します。
- 通常、スレーブプログラムは、MTA が外部リクエストに対して応答するための受信接続を受け入れます。スレーブチャネルプログラムには、以下のような機能があります。
  - 外部イベントまたはローカルリクエストに応えて起動します。
  - メッセージをチャネルキューに入れます。ターゲットチャネルは、エンベロープアドレスを書き換え規則に照会することにより決定されます (書き換え規則の詳細については、この章で後述しています)。

たとえば、図 6-2 では、チャネル 1 とチャネル 2 の 2 つのチャネルプログラムが示されています。チャネル 1 のスレーブプログラムが、リモートシステムからメッセージを受信したと仮定します。スレーブプログラムは、アドレスを確認して必要な書き換え規則を適用し、書き換えられたアドレスに基づいてメッセージを適切なチャネルメッセージキューに入れます。

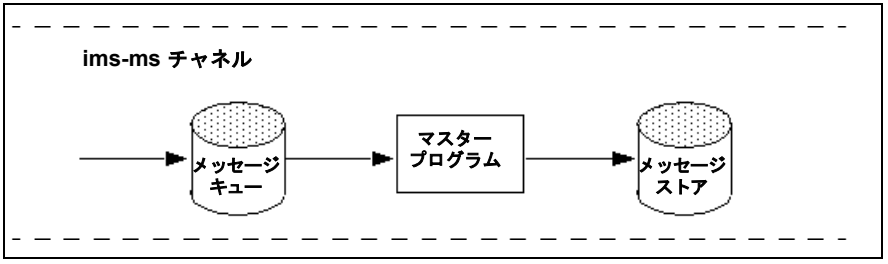
スレーブプログラムは、メッセージをそのチャネル内のメッセージキューに、または別のチャネルのメッセージキューに入れることができます。マスタープログラムは、キュー内で待機しているメッセージを取り出し、メッセージのネットワーク転送を開始します。ただし、マスタープログラムは、その独自のチャネルキュー内にあるメッセージしか取り出せません。

図 6-2　　マスタープログラムとスレーブプログラム



通常、1 つのチャネルにはマスタープログラムとスレーブプログラムの両方がありますが、スレーブプログラム**または**マスタープログラムだけのチャネルもあります。たとえば、Messaging Server で提供される `ims-ms` チャネルには、マスタープログラムしかありません。このチャネルで行われる操作は、図 6-3 で示すように、メッセージを取り出してローカルメッセージストアに送信するだけです。

図 6-3　　ims-ms チャネル



チャネルメッセージキュー

すべてのチャネルには、関連付けられたメッセージキューがあります。メッセージがメッセージングシステムに入ると、スレーブプログラムによってメッセージを入れるキューが決められます。キューに入れられたメッセージは、チャネルキューディレクトリのメッセージファイル内に保存されます。これらのディレクトリは、デフォルトで以下の場所に保存されます : `/` *サーバ- インスタンス* `/imta/queue/` *チャネル* `/*`

書き換え規則

書き換え規則には、以下の目的があります。

- アドレスを正しい形式、または目的の形式に書き換える方法を指定する。
- アドレスを書き換えた後にメッセージをキューに入れるためのチャネルを決定する。

各書き換え規則には、それぞれパターンとテンプレートがあります。パターンは、アドレスのドメイン名を検索する文字列であり、テンプレートは一致したパターンに基づいてアドレスを書き換える方法を示すものです。アドレスが書き換えられた後、メッセージはその受取人に配信するために、宛先チャネルに入れられます。

書き換え規則の設定方法については、95 ページの「MTA 設定ファイル」および第 7 章「書き換え規則を設定する」を参照してください。

ジョブコントローラ

ジョブコントローラは、メッセージを配信するためのチャネルジョブを作成および管理します。これらのチャネルジョブは、ジョブコントローラ内の処理プール内で実行されます。

メッセージがチャネルキューに入れられるたびに、ジョブコントローラはメッセージを配信するためのジョブが実行されていることを確認します。これには、新規ジョブプロセスを開始したり、スレッドを追加したり、または単にジョブがすでに実行されていることを確認するなどの操作が含まれます。チャネルまたはプールのジョブ制限に達したためにジョブを開始できない場合、ジョブコントローラは別のジョブが終了するのを待ち、ジョブ制限を超えていないことを確認してからジョブを開始します。

ジョブコントローラは、起動時に設定ファイルを読み込みます。設定ファイルには、一般的なパラメータ、返信ジョブスケジューリング、パージジョブスケジューリング、プール定義、およびチャネル処理情報が指定されています。この設定情報は、*サーバ_ルート*/msg-*インスタンス*/imta/config/ ディレクトリの job_controller.cnf に保存されています。

ジョブコントローラの設定の詳細については、102 ページの「ジョブコントローラファイル」および 159 ページの「メッセージの処理と配信を設定する」を参照してください。

ジョブコントローラを起動するには、次のコマンドを実行します。

```
imsimta start job_controller
```

ジョブコントローラを停止するには、次のコマンドを実行します

```
imsimta stop job_controller
```

ジョブコントローラを再起動するには、次のコマンドを実行します。

```
imsimta restart job_controller
```

ジョブコントローラを再起動すると、動作中のジョブコントローラが終了し、新規のジョブコントローラが起動します。

ディスパッチャ

ディスパッチャとは、指定のサービスにおける責任を共有するための複数のマルチスレッドサーバを許可するマルチスレッド接続ディスパッチエージェントのことです。ディスパッチャを使用すると、複数のマルチスレッド SMTP サーバを同時実行できるようになります。また、それぞれのサーバで複数のアクティブな接続が可能になります。

ディスパッチャは、その設定に一覧されている TCP ポートの中心的なレシーバとして機能します。定義された各サービスに対して、ディスパッチャは 1 つまたは複数の SMTP サーバプロセスを作成し、確立された接続を処理します。

通常、ディスパッチャが定義された TCP ポートの接続を受信すると、ディスパッチャはそのポートにおけるサービスのワーカープロセスのプールを確認し、その接続用に最適なワーカープロセスを選択します。適当なワーカープロセスがない場合、ディスパッチャは、この接続および後続の接続を処理するための新しいワーカープロセスを作成します。また、ディスパッチャは、今後の受信接続を予測して、新しいワーカープロセスを作成することもできます。ディスパッチャのさまざまなサービスを制御するための設定オプションがいくつかあります。これらの設定オプションは特に、ワーカープロセス数、および各ワーカープロセスが処理できる接続の数を制御するのに使用されます。

サーバプロセスの作成と有効期限

ディスパッチャ内の自動ハウスキーピング機能により、新規サーバプロセスの作成や、古いまたはアイドル状態のサーバプロセスの有効期限を制御することができます。ディスパッチャの動作を制御する基本的なオプションは、MIN_PROCS および MAX_PROCS です。MIN_PROCS は、受信接続用に一定のサーバプロセス数を待機させることにより、確実に一定レベルのサービスを提供します。一方、MAX_PROCS は、指定したサービスに対して同時にアクティブにできるサーバプロセス数の上限を設定します。

すでに処理可能な最大数の接続を処理しているため、またはプロセスの終了がスケジュールされているために、動作中のサーバプロセスが接続を受け入れられないことがあります。ディスパッチャは、今後の接続に役立つよう追加のプロセスを作成することができます。

MIN_CONNS および MAX_CONNS オプションを使うと、サーバプロセス間で接続を分配することができます。MIN_CONNS はサーバプロセスが「十分にビジー」であることを示す接続数を指定し、MAX_CONNS はサーバプロセスが「最高にビジー」な状態となる場合の接続数を指定するものです。

通常、現在のサーバプロセス数が MIN_PROCS 未満である場合、または既存のサーバプロセスがすべて「十分にビジー」(各サーバプロセスに対し、現在アクティブな接続の数が MIN_CONNS 以上である) な場合、ディスパッチャは新しいサーバプロセスを作成します。

たとえば UNIX システムの kill コマンドによってサーバプロセスが突然終了した場合、ディスパッチャは新しい接続ごとに新規サーバプロセスを作成します。

ディスパッチャの設定の詳細については、99 ページの「ディスパッチャ設定ファイル」を参照してください。

ディスパッチャを制御する

ディスパッチャは、必要に応じて、さまざまなサービスに対するサーバプロセスを起動および終了する単一の常駐プロセスです。

ディスパッチャを起動するには、次のコマンドを実行します。

```
imsimta start dispatcher
```

このコマンドは、ディスパッチャの設定で管理されている MTA のコンポーネントを起動するのに以前使われていた、他の `imsimta start` コマンドすべてを取り込み、無効にします。特に、`imsimta start smtp` は使用しないでください。無効になったコマンドを実行しようとすると、警告メッセージが表示されます。

ディスパッチャを終了するには、次のコマンドを実行します。

```
imsimta stop dispatcher
```

ディスパッチャを終了するときにサーバプロセスがどのように処理されるかは、その基礎となっている TCP/IP パッケージによって決まります。MTA の設定またはオプションを変更した場合は、新規の設定またはオプションを有効にするために、必ずディスパッチャを再起動してください。

ディスパッチャを再起動するには、次のコマンドを実行します。

```
imsimta restart dispatcher
```

ディスパッチャを再起動すると、実行中のディスパッチャが終了すると同時に新しいディスパッチャが起動します。

MTA 設定ファイル

最も重要な MTA 設定ファイル名は、`imta.cnf` です。デフォルトにより、このファイルは次の場所に保存されています。*サーバ - インスタンス* `/imta/config/imta.cnf`。このファイルには、サーバのすべてのチャネル定義、およびルーティング用でアドレスを書き換える際の書き換え規則が含まれています。書き換えられた宛先アドレスに関連付けられたチャネルが、宛先チャネルとなります。

この節では、MTA 設定ファイルについて簡単に説明します。MTA 設定ファイルに含まれている書き換え規則およびチャネル定義の設定については、第 7 章 「書き換え規則を設定する」および第 8 章 「チャネル定義を設定する」を参照してください。

MTA 設定ファイルを変更することにより、サイトで使用されるチャネルを確立し、書き換え規則を介してどのチャネルがどのようなアドレスを処理するかを決定することができます。設定ファイルは、送信方法 (チャネル) およびトランスポートルート (書き換え規則) を指定し、アドレスのタイプを適切なチャネルに関連付けることにより電子メールシステムの体系を確立するためのファイルです。

次の imta.cnf 設定ファイルの例は、書き換え規則を使って適切なチャネルにメッセージをルーティングする方法を示しています。わかりやすくするために、ドメイン名は使用していません。書き換え規則は設定ファイルの前半部分にあり、その後にチャネル定義が続いています。

図 6-4 簡単な MTA 設定ファイルの例

```
! test.cnf - An example configuration file. (1)
!
! This is only an example of a configuration file. It serves
! no useful purpose and should not be used in a real system.
!
a     $U@a-daemon (2)
b     $U@b-daemon
c     $U%c@b-daemon
d     $U%d@a-daemon
               (3)
l              (4)
local-host

a_channel defragment charset7 usascii (5)
a-daemon

b_channel noreverse notices 1 2 3
b-daemon
```

以下に、上記設定ファイルの主な項目 (カッコで括られた番号付き) について説明します。

1 感嘆符 (!) は、コメント行を表します。感嘆符は最初のカラムに表示されていなければなりません。その他の場所で表示される感嘆符は、**文字として**解釈されます。

2 書き換え規則は設定ファイルの前半部分にあります。書き換え規則に空白行を入れることはできません。コメント行 (最初のカラムに感嘆符が付いている) を入れることはできます。

3 設定ファイル内で最初に現れる空白行は、書き換え規則の終わりとチャネル定義の始まりを表します。

4 UNIX の場合、最初のチャネル定義ブロックは常に l チャネル (「L」の小文字で指定された UNIX ローカルチャネル) です。各チャネル定義ブロックは、空白行で区切られています (defaults チャネルは例外。このチャネルは l チャネルより先に表示されます)。

表 6-1 に、上記設定ファイルによるメッセージのルーティングおよびキュー処理を示します。

表 6-1　　アドレスと関連チャネル

アドレス	チャネル (キュー)
u@a	a_channel
u@b	b_channel
u@c	b_channel
u@d	a_channel

その他の MTA 設定ファイル

imta.cnf ファイルの他にも、iPlanet Messaging Server には MTA サービスを設定するのに役立ついくつかの設定ファイルがあります。表 6-2 に、これらの設定ファイルの要約を示します。

表 6-2　　MTA 設定ファイル

ファイル	説明
自動返信オプションファイル	autoreply プログラムによって使用されるオプション。 / *サーバ-インスタンス* /imta/config/autoreply_option
エイリアスファイル (必須)	ディレクトリにないエイリアスを実行します。 / *サーバ- インスタンス* /imta/config/aliases
TCP/IP チャネルオプションファイル	チャネル固有のオプションを設定します。 / *サーバ- インスタンス* /imta/config/ *チャネル* _option
変換ファイル	変換チャネルがメッセージ本体部分の変換を制御するのに使用します。 / *サーバ- インスタンス* /imta/config/conversions
Dirsync オプションファイル (必須)	dirsync プログラムによって使用されるオプション。 / *サーバ- インスタンス* /imta/config/dirsync.opt
ディスパッチャ設定ファイル (必須)	ディスパッチャ用の設定ファイル。 / *サーバ- インスタンス* /imta/config/dispatcher.cnf
MTA 設定ファイル (必須)	アドレスの書き換え、ルーティング、およびチャネル定義に使用します。 / *サーバ- インスタンス* /imta/config/imta.cnf
マッピングファイル (必須)	マッピングテーブルのリポジトリ。 / *サーバ- インスタンス* /imta/config/mappings

表 6-2　MTA 設定ファイル（続き）

ファイル	説明
オプションファイル	グローバルな MTA オプションのファイル。 / *サーバ- インスタンス* /imta/config/option.dat
テイラーファイル (必須)	場所といくつかの調整パラメータを指定するファイル。 / *サーバ- インスタンス* /imta/config/imta_tailor
ジョブコントローラファイル (必須)	ジョブコントローラによって使用する設定ファイル。 /*サーバインスタンス*/imta/config/job_controller.cnf

自動返信オプションファイル

自動返信ファイル autoreply_option は、自動返信または Vacation プログラムのオプションを設定します。このファイルの構文の詳細については、『Messaging Server リファレンスマニュアル』を参照してください。

エイリアスファイル

エイリアスファイル aliases は、ディレクトリにないエイリアスを設定します。その例として、ルートのアドレスが挙げられます。このファイルで設定したエイリアスがディレクトリにもある場合は、ファイル内の設定が無視されます。エイリアスおよび aliases ファイルの詳細については、105 ページの「エイリアス」を参照してください。

aliases ファイルに変更を加えた場合は、必ず MTA を再起動してください。

TCP/IP チャネルオプションファイル

TCP/IP チャネルオプションファイルは、TCP/IP チャネルのさまざまな特性を制御します。チャネルオプションファイルは、MTA 設定ディレクトリに保存する必要があります。ファイルには *x*_option という名前を付けてください。ファイル名の *x* はチャネル名となります。たとえば、次のようになります。/ *サーバ - インスタンス* /config/imta/tcp_local_option

オプションファイルは、1 つまたは複数のキーワードと 1 つの関連する値により構成されています。たとえば、DISABLE_EXPAND キーワードをオプションファイルに入れ、値を 1 に設定すると、サーバの SMTP EXPN コマンドを無効にすることができます。

その他のオプションファイルキーワードを使って、以下の設定を行うことができます。

- メッセージ当たりの受取人の人数制限を設定する (ALLOW_RECIPIENTS_PER_TRANSACTION)
- 接続当たりのメッセージ数の制限を設定する (ALLOW_TRANSACTIONS_PER_SESSION)
- MTA ログファイルに記録される情報のタイプを制御する (LOG_CONNECTION、LOG_TRANSPORTINFO)
- クライアントチャネルプログラムが許可する同時送信接続の最大数を指定する (MAX_CLIENT_THREADS)

すべてのチャネルオプションキーワードおよび構文の詳細については、『Messaging Server リファレンスマニュアル』を参照してください。

変換ファイル

変換ファイル `conversions` は、MTA を介して送受信されるメッセージの変換チャネルにおける変換方法を指定します。変換には、いずれの MTA 通信のサブセットでも選択することができます。また、変換処理を行うには、いずれのプログラムまたはコマンドのセットでも使用することができます。MTA は変換ファイルに基づいて、それぞれのメッセージ本文に対する適切な変換を選択します。

このファイルの構文の詳細については、『Messaging Server リファレンスマニュアル』を参照してください。

Dirsync オプションファイル

Dirsync オプションファイル `dirsync.opt` は、コマンドラインで設定できない `dirsync` プログラムのオプションを設定します。

このファイルの構文の詳細については、『Messaging Server リファレンスマニュアル』を参照してください。

ディスパッチャ設定ファイル

ディスパッチャ設定ファイル `dispatcher.cnf` は、ディスパッチャの設定情報を指定します。インスール時に作成されたデフォルトの設定ファイルをそのまま使用することができます。ただし、セキュリティやパフォーマンスなどの理由でデフォルトの設定ファイルを変更する場合には、`dispatcher.cnf` ファイルを変更します。

ディスパッチャ設定ファイルのフォーマットは、その他の MTA 設定ファイルに似ています。オプションを指定する行は、次の形式に従います。

option=value

option はオプション名で、*value* はオプションを設定する文字列または整数となります。*option* が整数の *value* を認める場合は、*b%v* という形式の記数法を使って基数を指定できます。*b* は基数 10 で表される基数となり、*v* は基数 *b* が表している実際の値となります。このようなオプション仕様は、下記のオプション設定が適用されるサービスに応じてセクション別にグループ分けされます。これには、次の形式の行を使用します。

[SERVICE=*service-name*]

service-name はサービス名です。このようなセクションタグの前に記述されている最初のオプション仕様は、すべてのセクションに適用されます。

以下に、ディスパッチャ設定ファイル (dispatcher.cnf) の例を示します。

```
! The first set of options, listed without a [SERVICE=xxx]
! header, are the default options that will be applied to all
! services.
!
MIN_PROCS=0
MAX_PROCS=5
MIN_CONNS=5
MAX_CONNS=20
MAX_LIFE_TIME=86400
MAX_LIFE_CONNS=100
MAX_SHUTDOWN=2
!
! Define the services available to Dispatcher
!
[SERVICE=SMTP]
PORT=25
IMAGE= サーバ - ルート /msg- インスタンス /imta/lib/tcp_smtp_server
LOGFILE= サーバ - ルート /msg- インスタンス /imta/log/tcp_smtp_server.log
```

このファイルのパラメータの詳細については、『Messaging Server リファレンスマニュアル』を参照してください。

マッピングファイル

マッピングファイル mappings は、MTA が入力文字列を出力文字列にマップする方法を定義します。

MTA コンポーネントの多くは、テーブル検索に基づいた情報を使用します。一般に、このタイプのテーブルは、入力文字列を出力文字列に変える (マップする) のに使用されます。このようなテーブルは、マッピングテーブルと呼ばれ、通常 2 つのカラムで構成されます。1 つ目 (左側) のカラムには入力文字列が、2 つ目 (右側) のカラムにはその入力文字列に関連付けられた出力文字列が並んでいます。MTA データベースのほとんどは、このタイプのマッピングテーブルです。ただし、MTA データベースファイルには、ワイルドカード検索機能はありません。データベース全体でワイルドカードに一致するものを検索するのは非効率的だからです。

マッピングファイルによって、MTA が複数のマッピングテーブルをサポートできるようになります。さらに、完全なワイルドカード機能もあり、複数の手順や反復マッピング方法にも対応しています。このアプローチは、データベースを使用する場合に比べてさらに多くの処理を必要とします。特に、エントリ数が多い場合などはなおさらです。ただし、それに付随して柔軟性が増すため、同等のデータベースにおけるエントリのほとんどを必要としなくなり、全体的にオーバーヘッドが少なくなります。

imsimta test -mapping コマンドを使ってマッピングテーブルをテストすることができます。マッピングファイルの構文および test -mapping コマンドの詳細については、『Messaging Server リファレンスマニュアル』を参照してください。

オプションファイル

オプションファイル option.dat は、チャネル オプションとは逆に、グローバルな MTA オプションを指定します。

オプションファイルを使って、MTA 全体に適用されるさまざまなパラメータのデフォルト値を無効にすることができます。特に、設定ファイルやエイリアスファイルが読み込まれるさまざまなテーブルのサイズを確立するのに使用できます。また、MTA が受信するメッセージのサイズを制御したり、MTA 設定で許可するチャネル数を指定したり、許可する書き換え規則の数を設定するなどの操作を行うことができます。

オプションファイルの構文の詳細については、『Messaging Server リファレンスマニュアル』を参照してください。

テイラーファイル

テイラーファイル imta_tailor は、さまざまな MTA コンポーネントの場所を設定します。MTA が正常に機能するには、imta_tailor ファイルが常に *サーバ - インスタンス* /imta/config ディレクトリ内になければなりません。

このファイルを編集して特定のインストールにその変更を反映させることはできますが、その際には注意が必要です。このファイルを変更した場合は、必ず MTA を再起動してください。MTA が停止しているときに変更を行うのが望ましい方法です。

注	特に必要でない限り、このファイルを変更することは避けてください。

このファイルの構文の詳細については、『Messaging Server リファレンスマニュアル』を参照してください。

ジョブコントローラファイル

ジョブコントローラファイル job_controller.cnf は、チャネル処理の情報を指定します。このファイルには、以下の目的があります。

- さまざまなプールを定義する。
- すべてのチャネルに対し、マスタープログラム名とスレーブプログラム名を指定します (該当する場合)。

imta.cnf ファイルで、pool *キーワード*を使ってプロセスプール (job_controller.cnf で定義) の名前を指定できます。たとえば、次のサンプルファイル job_controller.cnf の要素は、プール MY_POOL を定義します。

```
[POOL=MY_POOL]
job_limit = 12
```

次のサンプルファイル imta.cnf の要素は、チャネル定義ブロック内でプール MY_POOL を指定します。

```
channel_x pool MY_POOL
channel_x-daemon
```

デフォルトのプール設定に関連付けられたパラメータを変更したり、プールを追加する場合には、job_controller.cnf ファイルを編集してから、ジョブコントローラを終了して再起動してください。

新しい設定を使用して新規のジョブコントローラプロセスが作成され、それ以降のリクエストを受信するようになります。古いジョブコントローラプロセスは、キューに入っているリクエストをすべて処理し終了します。

ジョブコントローラ設定ファイルの最初のプールは、プール名が指定されていないリクエストのすべてに使用されます。MTA 設定 (imta.cnf) で定義されている MTA チャネルは、後にプール名が続く pool チャネルキーワードを使って、特定のプールに処理リクエストを送ることができます。このプール名は、ジョブコントローラ設定のプールの名前と一致しなければなりません。ジョブコントローラがリクエストされたプール名を認識できない場合、そのリクエストは無視されます。

最初の設定には、DEFAULT、LOCAL_POOL、IMS_POOL、SMTP_POOL のプールが定義されています。

使用例

通常、特定のチャネルの処理を別のチャネルの処理と区別したい場合には、ジョブコントローラ設定に付加的なプール定義を追加します。また、異なる特性を持つプールを使用することもできます。たとえば、チャネルが処理できる同時リクエスト数を制御する必要があるとします。これを行うには、ジョブ制限を持つ新規プールを作成し、pool チャネルキーワードを使ってチャネルをより適切なプールに割り当てます。

プール定義に加え、ジョブコントローラ設定ファイルには、各チャネルのリクエストを処理するのに必要な MTA チャネルとコマンドのテーブルが含まれています。リクエストには「マスター」と「スレーブ」と呼ばれる 2 つのタイプがあります。通常、チャネルの MTA メッセージキューにメッセージが入れられると、チャネルマスタープログラムが起動します。マスタープログラムは、メッセージをキューから取り出します。

スレーブプログラムは起動すると、チャネルをポーリングし、そのチャンネル内の受信メッセージを受け取ります。マスタープログラムはほぼすべての MTA チャネルにありますが、スレーブプログラムは MTA チャネルにはほとんどなく、すなわち必要とされません。たとえば、TCP/IP を使用した SMTP を処理するチャネルではスレーブプログラムを使用しません。すべての SMTP サーバからのリクエストに対して、ネットワークサービスである SMTP サーバが受信 SMTP メッセージを受け取るためです。SMTP チャネルのマスタープログラムは、MTA の SMTP クライアントです。

チャネルに関連付けられた宛先のシステムが一度に複数のメッセージを処理できない場合は、ジョブ制限が 1 である新しいタイプのプールを作成する必要があります。

```
[POOL=single_job]
job_limit=1
```

一方、宛先のシステムが十分に並行処理できる場合は、ジョブ制限の値の設定を増やすことができます。

図 6-5 に、ジョブコントローラ設定ファイルの例を示します。

図 6-5　　UNIX のジョブコントローラ設定ファイルの例

```
!MTA Job Controller configuration file
!
!Global defaults
tcp_port=27442(1)
secret=never mind
return_job=サーバ_ルート/bin/msg/imta/bin/return.sh
return_time=00:30/24:00
purge_job=サーバ_ルート/bin/msg/imta/bin/purge
purge_argv=-num=5
slave_command=NULL(2)
max_life_age=3600(3)
!
!
!Pool definitions
!
[POOL=DEFAULT](4)
job_limit=10(5)
!
[POOL=LOCAL_POOL]
job_limit=10
!
[POOL=IMS_POOL]
job_limit=1
!
[POOL=SMTP_POOL]
job_limit=1
!
!Channel definitions
!
!
[CHANNEL=l](6)
master_command=サーバ_ルート/bin/msg/imta/bin/l_master
!
[CHANNEL=ims-ms]
master_command=サーバ_ルート/bin/msg/imta/bin/ims_master
!
[CHANNEL=tcp_*](7)
anon_host=0
master_command=サーバ_ルート/bin/msg/imta/bin/tcp_smtp_client
```

以下に、上記例の主な項目 (丸括弧付き表示された) について説明します。

1 このグローバルオプションは、ジョブコントローラがリクエストをリッスンする TCP ポート番号を定義します。

2 後続の [CHANNEL] セクションのデフォルト SLAVE_COMMAND を設定します。

3 後続の [CHANNEL] セクションのデフォルト MAX_LIFE_AGE を設定します。

4 この [POOL] セクションは、DEFAULT という名前のプールを定義します。

5 このプールの JOB_LIMIT を 10 に設定します。

6 この [CHANNEL] セクションは、l という名前のチャネル (UNIX ローカルチャネル) に適用されます。このセクションに必要な定義は、ジョブコントローラがこのチャネルを実行するのに発行する master_command のみです。このチャネル名にはワイルドカードが含まれていないため、チャネル名は完全に一致しなければなりません。

7 この [CHANNEL] セクションは、tcp_* で始まるすべてのチャネル名に適用されます。このチャネル名にはワイルドカードが含まれているため、tcp_ で始まるすべてのチャネルに一致します。

ジョブコントローラファイルの構文の詳細については、『Messaging Server リファレンスマニュアル』を参照してください。

エイリアス

MTA には、必ずしも実際のユーザに対応するとは限らない、ローカルシステムに関連付けられたメールボックス名をサポートする機能である「エイリアス」があります。エイリアスは、メーリングリストの作成、メールの転送、およびユーザの別名の設定に役立ちます。

エイリアスを適用できるのは、l チャネルまたは aliaslocal キーワードの付いたすべてのチャネルに一致するアドレスだけです。MTA のメッセージ送信ロジックが l チャネルまたは aliaslocal キーワードの付いたすべてのチャネルに一致するアドレスを識別するたびに、アドレスに指定されているメールボックス (たとえば、ユーザ名) がエイリアスデータベースまたはエイリアスファイル内の各エントリと照合されます。一致するエントリが見つかると、エイリアスアドレスは変換値またはエイリアスで指定された値に置き換えられます。エイリアスは、追加エイリアスまたは実際のアドレスによる任意の組み合わせに変換できます。実際のアドレスが l チャネルや aliaslocal キーワードの付いたすべてのチャネルに一致する必要はありません。したがって、エイリアスは、リモートシステムにメールを転送するのに使用することができます。

本当にチャネルに一致すると見なされるアドレスは Envelope To アドレスのみであるため、エイリアスは Envelope To アドレスにしか適用されません。MTA は、アドレスの書き換えが完了した後にのみエイリアスの変換および拡張を行います。エイリアスによって生成された変換値は、完全に新しいアドレスとして扱われ、最初から処理されます。

エイリアスデータベース

MTA はディレクトリ内の情報を使用し、エイリアスデータベースを作成します。このエイリアスデータベースは、標準のエイリアスファイルが参照されるたびに参照されます。ただし、エイリアスデータベースのエントリが調べられるのは、標準のエイリアスファイルが使用される前です。すなわち、デーベースは、エイリアスファイルが使用される前に実行される、一種のアドレス書き換え機能として動作します。エイリアスデータベースにユーザおよび配信リストのエントリを作成するためのディレクトリ属性については、『iPlanet Messaging Server 5.1 Provisioning Guide』を参照してください。

注　データベースには固有のフォーマットがあるので、データベースを直接編集することは避け、必要な変更はディレクトリ内で行うようにしてください。

エイリアスファイル

aliases ファイルは、ディレクトリで設定されていないエイリアスを設定するのに使用します。よい例として、Postmaster エイリアスが挙げられます。このファイルで設定したエイリアスがディレクトリにもある場合、このファイルの設定は無視されます。変更を有効にするには、MTA を再起動する必要があります。感嘆符で始まる行は、コメント行として解釈されるため、無視されます。また、空白行も無視されます。

このファイルでは、一行に入力できる文字数が 252 文字に制限されています。バックスラッシュ (\) を継続文字として使用すれば、1 つの論理行を複数の行に分割することができます。

ファイルフォーマットは以下のとおりです。

```
user@domain: <address> (ホストドメインのユーザ用)

user@domain: <address> (非ホストドメインのユーザ用。例 : default-domain)
```

以下に例を示します。

```
! A /var/mail/ user
inetmail@siroe.com: inetmail@native-daemon

! A message store user
ms_testuser@siroe.com: mstestuser@ims-ms-daemon
```

エイリアスファイルに他のファイルを含める

プライマリ aliases ファイルには、他のファイルを含めることができます。次の行は、MTA に file-spec ファイルを読み込むように指示するためのものです。

```
<file-spec
```

ファイル仕様は、完全なパスを指定したものでなければなりません。また、そのファイルには、プライマリ aliases ファイルと同じ保護が設定されている必要があります (たとえば誰でも読み込み可能であることなど)。

含まれているファイルの内容は、aliases ファイル内の参照ポイントに挿入されます。含めたファイルへのリファレンスをそのファイルの実際の内容に置き換えることによっても、同様の効果が得られます。含まれたファイルのフォーマットは、プライマリ aliases ファイルとまったく同じになります。さらに、含まれたファイルに他のファイルを含めることも可能です。ファイルには 3 段階までの入れ子レベルが許可されています。

コマンドラインユーティリティ

iPlanet Messaging Server には、MTA のさまざまなメンテナンス、テスト、管理タスクを行うためのコマンドラインユーティリティが備わっています。たとえば、MTA の設定、エイリアス、マッピング、セキュリティ、システム全体のフィルタ、およびオプションファイルをコンパイルするには、imsimta cnbuild コマンドを使用します。また、MTA ディレクトリキャッシュを再作成または更新するには、imsimta dirsync コマンドを使用します。MTA コマンドラインユーティリティの詳細については、『Messaging Server リファレンスマニュアル』を参照してください。

MTA ディレクトリキャッシュ

MTA は、処理する各メッセージに対し、サポートするユーザ、グループ (メーリングリスト、ファミリアカウント、組織)、およびドメインに関する情報にアクセスする必要があります。この情報は、LDAP ディレクトリサービスに保存されています。MTA は、メッセージを処理するごとにディレクトリサービスのクエリを行うのではなく、ディレクトリ情報をキャッシュに保存します。つまり、ディレクトリ情報のスナップショットを保存するのです。その後、MTA はこのキャッシュ内のディレクトリ情報にアクセスします。

ディレクトリサービスに保存されたディレクトリ情報は、常に更新されます。このため、MTA のディレクトリキャッシュもディレクトリサービス内のディレクトリ情報に合わせて定期的に更新 (つまり、同期) する必要があります。Messaging Server では、2 種類の同期方法を利用できます。

- **完全同期** - 既存のキャッシュが新しいキャッシュに置き換えられ、ディレクトリサービスにあるユーザおよびグループのエントリを使って完全に再構築されます。同期後、MTA 設定ファイルが再構築され、自動的に MTA が再起動します。
- **インクリメンタル同期** - 既存のキャッシュが、前回の完全同期またはインクリメンタル同期以降に作成されたユーザおよびグループのエントリを使って更新されます。MTA は再起動しません。

デフォルトでは、毎日午前 2 時に完全同期が行われ、また 10 分ごとにインクリメンタル同期が行われます。

表 6-3 に、完全同期またはインクリメンタル同期が行われるディレクトリエントリを示します。

表 6-3　　MTA ディレクトリキャッシュの更新

MTA ディレクトリキャッシュの更新	完全同期	インクリメンタル同期
追加した新規のユーザエントリ	○	○
修正したユーザエントリの更新	○	○
* 削除したユーザエントリの破棄	○	X
既存の配信リストに追加した新規メンバー	○	○
既存の配信リストから削除したメンバーの破棄	○	○
追加した新規の配信リスト	○	○
* 削除した配信リストの破棄	○	X

* 削除したエントリに対してインクリメンタル同期を実行するには、そのエントリのステータスに削除済みのマークが付いている必要があります。インクリメンタル同期の実行後、MTA はそのユーザまたはグループが存在しないと見なします。実際にディレクトリを削除する作業は、インクリメンタル同期の後に行ってください。

通常、ディレクトリの同期は自動的に行われます。ただし、必要に応じて、`imsimta dirsync` コマンドを使って MTA ディレクトリキャッシュを再作成または更新することができます。`imsimta dirsync` コマンドの詳細については、『Messaging Server リファレンスマニュアル』を参照してください。

同期設定パラメータ

表 6-4 に、ディレクトリ同期設定のパラメータを示します。

表 6-4　　ディレクトリ同期設定のパラメータ

パラメータ	説明
local.imta. ldsearchtimeout	ユーザおよびメーリングリストの情報を検索する際の LDAP 検索のタイムアウトを指定します。デフォルトでは、タイムアウトはありません。
local.imta. hostnamealiase	LDAP エントリがローカルであるかどうかを確認する目的でそのエントリの mailhost または mailRoutingHosts 属性をチェックする際に、dirsync プロセスは local.hostname パラメータを使って比較を行います。さらに、local.imta.hostnamealiases パラメータにより、カンマで区切られたホスト名エイリアスのリストが提供されます。dirsync プロセスは、これらの 2 つのパラメータで提供されるすべてのホスト名を使って、エントリがローカルであるかどうかを調べます。
local.imta. mailaliases	デフォルトでは、mail および mailAlternateAdress という LDAP 属性しかルーティング可能なメールアドレスとして見なされません。その代わり、local.imta.mailaliases パラメータにより、カンマで区切られた LDAP 属性のリストが提供されます。このリストはデフォルトの属性を上書きします。たとえば、メッセージをルーティングする際に、MTA は次の 4 つの属性を考慮します。 local.imta.mailaliases=mail,mailAlternateAdres, rfc822mailbox,rfc822mailalias
local.imta. ugfilter	このパラメータは、ユーザやメーリングリストの情報を検索する際に、dirsync が使用する LDAP 検索フィルタを設定します。 デフォルトのフィルタは次のとおりです。 (objectClass=inetLocalMailRecipient) たとえば、inetLocalMailRecipient および myispSubscriber オブジェクトクラスの LDAP エントリだけを考慮する場合には、このパラメータを次のように設定します。 local.imta.ugfilter= (&(objectClass=inetLocalMailRecipient) (objectClass=myispSubscriber)) 注意 : インクリメンタル同期の場合は、このフィルタにタイムスタンプフィルタが追加されます。このため、カスタムフィルタを ( ) で括る必要があります。
local.imta. statssamplesize	このパラメータを設定すると、標準出力として、最初からのユーザ / メーリングリストエントリおよび平均率 (エントリ数 / 秒) を要約して印刷するように dirsync に指示が出されます。ユーザおよびメーリングリストは、同期が完了したかどうかに関わらず数えられます。

表 6-4　ディレクトリ同期設定のパラメータ（続き）

パラメータ	説明
local.imta.reverseenabled	リバースデータベースの生成をトリガします。デフォルト値は、Yes です。実際にリバースデータベースが使用される方法は、USE_REVERSE_DATABASE オプションで制御されます。
local.imta.ssrenabled	SSR (Server Side Rule) データベースの生成をトリガします。デフォルト値は、Yes です。SSR データベースが使用される方法は、ssr チャネルキーワードで制御されます。
local.imta.vanityenabled	バニティドメイン (msgVanityDomain ユーザ LDAP 属性) が有効であるかどうかを制御します。デフォルト値は Yes です。
local.imta.catchallenabled	キャッチオールアドレス (@domain 形式の mail または mailAlternateAddress) が有効であるかどうかを制御します。デフォルト値は Yes です。
local.imta.scope	このパラメータは、どのエントリを同期するかを dirsync に知らせます。 mailhost 属性がローカルホストであるユーザおよびメーリングリストのエントリだけをキャッシュする場合 : 値 = "local"。 mailhost 属性に関わらず、ユーザおよびメーリングリストのエントリをキャッシュする場合 : 値 = "domains"。これはパラメータがない場合のデフォルト値です。 ドメイン、ユーザ、またはメーリングリストをキャッシュしない場合 : 値 = "nobody"。

SMTP セキュリティとアクセス制御

SMTP セキュリティとアクセス制御の詳細については、第 9 章 「メールのフィルタリングとアクセス制御」および第 11 章 「セキュリティとアクセス制御を設定する」を参照してください。

ログファイル

MTA 専用のログファイルはすべて、MTA ログディレクトリ (*サーバ - インスタンス* /log/imta/) に保存されます。このディレクトリには、MTA を介したメッセージ通信のログファイル、および特定のマスタープログラムまたはスレーブプログラムの情報を記述したログファイルがあります。

MTA ログファイルの詳細については、第 12 章「ログ記録とログ解析」を参照してください。

第 7 章

書き換え規則を設定する

この章では、imta.cnf ファイル内で書き換え規則を設定する方法について説明します。この章へ進む前に、第 6 章 「MTA サービスと設定について」をお読みください。

この章には、以下の項目があります。

- 書き換え規則の構造
- 書き換え規則のパターンとタグ
- 書き換え規則のテンプレート
- MTA がアドレスに書き換え規則を適用する方法
- テンプレートの置換シーケンスと書き換え規則 コントロールシーケンス
- 多数の書き換え規則を扱う
- 書き換え規則をテストする
- 書き換え規則の例

Messaging Server のアドレス書き換え機能は、アドレスのホストまたはドメイン部分を操作および変更するのに欠かせない重要な機能です。Messaging Server には、エイリアス、アドレス置き換えデータベース、および特殊化されたマッピングテーブルといった他の機能もあります。ただし、アドレス操作を実行する可能性がある場合には、常に書き換え規則を使用するようにしてください。それにより、最高のパフォーマンスを得ることができます。

注　imta.cnf ファイル内の書き換え規則を変更する場合は、imsimta start コマンドを使って起動するときに設定データを 1 回だけ読み込むようなプログラムまたはチャネルを再起動する必要があります (例、SMTP サーバ)。コンパイルされた設定を使用する場合は、設定を再コンパイルした後にプログラムを再起動する必要があります。

設定情報のコンパイルおよびプログラムの再起動については、『Messaging Server リファレンスマニュアル』を参照してください。

書き換え規則の構造

書き換え規則は MTA 設定ファイル (imta.cnf) の前半部分にあり、各規則が 1 行ごとに記述されています。規則間にコメントを記述することは可能ですが、空白行を挿入することはできません。書き換え規則の最後には空白行が挿入され、その後にチャネルの定義が続きます。図 7-1 に、設定ファイル内の書き換え規則を示します。

図 7-1 設定ファイルの例 - 書き換え規則

```
! test.cnf  - 設定ファイルの例。
!
! これは、単に設定ファイルの例です。
! 実際のシステムで使用するためのものではありません。
!
a      $U@a-host
b      $U@b-host
c      $U%c@b-daemon
d      $U%d@a-daemon

! 以下、チャネルの定義が続きます。
```

書き換え規則は、2 つの部分から構成されています。最初にパターン、その後に同等の文字列またはテンプレートを指定します。これらの 2 つの部分は空白文字を挿入して区切る必要があります。ただし、パターンやテンプレート自体に空白文字を使用することはできません。書き換え規則の構造は、次のとおりです。

```
パターン  テンプレート
```

パターン

検索の対象となるドメイン名内の文字列です。図 6-1 の例では、a、b、c、d がパターンです。

パターンがアドレスのドメイン部分に一致すると、その書き換え規則がアドレスに適用されます。パターンの後には空白文字を挿入して、テンプレート部分を区別できるようにします。パターンの構文については、113 ページの「書き換え規則のパターンとタグ」を参照してください。

テンプレート

以下のいずれかの形式を使って指定します。テンプレートの構文については、117 ページの「書き換え規則のテンプレート」を参照してください。

UserTemplate%*DomainTemplate*@*ChannelTag*[*コントロール*]

UserTemplate@*ChannelTag*[*コントロール*]

UserTemplate%*DomainTemplate*[*コントロール*]

UserTemplate@*DomainTemplate*@*ChannelTag*[*コントロール*]

UserTemplate@*DomainTemplate*@*SourceRoute*@*ChannelTag*[*コントロール*]

UserTemplate	アドレスのユーザ部分をどのように書き換えるかを指定します。元のアドレスの一部またはデータベース検索の結果を表すために置換シーケンスを使用することもできます。置換シーケンスは、アドレスを書き換える際に、それが表す本来の文字列に置き換えられます。図 6-1 では、$U という置換シーケンスが使用されています。詳細については、124 ページの「テンプレートの置換シーケンスと書き換え規則 コントロールシーケンス」を参照してください。
DomainTemplate	アドレスのドメイン部分をどのように書き換えるかを指定します。*UserTemplate* と同様に、*DomainTemplate* にも置換シーケンスを含めることができます。
ChannelTag	このメッセージの送信先チャネルです (すべてのチャネル定義に、チャネルタグとチャネル名を含める必要があります。一般に、チャネルタグは書き換え規則とそのチャネル定義に記述されます)。
コントロール	コントロールを使って、規則の適用度を制限できます。コントロールシーケンスの中には、規則の前に置くものと、規則の後に置くものとがあります。コントロールの詳細については、124 ページの「テンプレートの置換シーケンスと書き換え規則 コントロールシーケンス」を参照してください。

書き換え規則のパターンとタグ

一般に、書き換え規則のパターンは、特定のホスト名 (そのホスト名だけに一致) またはサブドメインパターン (サブドメイン全体における任意のホスト / ドメインに一致) のいずれかで構成されます。

たとえば、次の書き換え規則のパターンには、特定のホスト名が含まれています。このパターンは、この指定したホスト名だけに一致します。

```
host.siroe.com
```

次の書き換え規則のパターンには、サブドメインパターンが含まれています。このパターンは、サブドメイン全体における任意のホストまたはドメインに一致します。

```
.siroe.com
```

ただし、このパターンは siroe.com というホスト名には一致しません。siroe.com も対象に含める場合は、siroe.com という別のパターンが必要です。

MTA は、特定のホスト名に一致するものからホスト / ドメイン名を書き換えていき、より不特定のパターンへと処理を進めます。つまり、特定のパターンは、不特定のパターンよりも優先して使用されることになります。たとえば、設定ファイルに、以下の書き換え規則パターンが記述されているとします。

```
hosta.subnet.siroe.com
.subnet.siroe.com
.siroe.com
```

この場合、まず jdoe@hosta.subnet.siroe.com というアドレスが hosta.subnet.siroe.com という書き換え規則パターンに一致します。その後、jdoe@hostb.subnet.siroe.com というアドレスが .subnet.siroe.com という書き換え規則パターンに一致し、次に jdoe@hostc.siroe.com というアドレスが .siroe.com という書き換え規則パターンに一致します。

特に、サブドメインの書き換え規則パターンを含む書き換え規則は、インターネットのサイトでよく使用されます。一般に、そのようなサイトでは、内部のホストやサブネット用に多数の書き換え規則が用意され、最上位のインターネットドメインに対する書き換え規則が internet.rules (*サーバ-インスタンス*/imta/config/internet.rules) ファイル内の設定に含められます。

インターネット宛先 (より特定の書き換え規則を通じて処理されたインターネットホスト宛先を除く) へのメッセージが正しく書き換えられ、送信 TCP/IP チャネルに送られるようにするには、imta.cnf ファイルに以下の内容を含めます。

- 最上位のインターネットドメインに一致するパターンを含んだ書き換え規則
- そのようなパターンに一致するアドレスを書き換える、送信 TCP/IP チャネルに対するテンプレート

```
!    Ascension Island
.AC                                        $U%$H$D@TCP-DAEMON
. [ 簡潔にするため
.    テキストを
.             省略 ]
!    Zimbabwe
.ZW                                        $U%$H$D@TCP-DAEMON
```

同様に、IP ドメインリテラルの場合も階層に基づいて照合が行われます。ただし、左から右ではなく、右から左へ照合が行われます。たとえば、次のパターンは [1.2.3.4] という IP リテラルにのみ一致します。

```
[1.2.3.4]
```

次のパターンは 1.2.3.0 サブネット内の任意の IP リテラルに一致します。

```
[1.2.3.]
```

ホスト / サブドメイン名を使った一般的な書き換え規則パターンのほかに、特殊なパターンを使用することもできます。これらの特殊なパターンについては、表 7-1 およびその後の説明を参照してください。

表 7-1　書き換え規則の特殊パターン

パターン	説明 / 使用方法
$%	パーセントハック規則。A%B 形式の任意のホスト / ドメイン仕様に一致します。
$!	bang-style 規則。B!A 形式の任意のホスト / ドメイン仕様に一致します。
[]	IP リテラル全一致規則。任意の IP ドメインリテラルに一致します。
.	任意のホスト / ドメイン仕様に一致します。たとえば、joe@[129.165.12.11]

これらの特殊パターンに加え、Messaging Server には、書き換え規則のパターン内で使われる**タグ**の概念もあります。これらのタグは、アドレスが複数回にわたって書き換えられる場合に使用されます。その場合、それぞれの書き換えを区別する必要があります。この区別は、直前に行われた書き換えに基づき、どの書き換え規則がアドレスに一致するかを制御することによって行います。詳細については、116 ページの「タグ付き書き換え規則セット」を参照してください。

パーセントハックに一致する規則

MTA が A%B 形式のアドレスを書き換えようとして失敗した場合は、そのアドレスが A%B@localhost として扱われる前に、もう 1 つの規則が適用されます (これらのアドレス形式の詳細については、117 ページの「書き換え規則のテンプレート」を参照してください)。この規則が**パーセントハック規則**です。パターンは $% で、これが変わることはありません。この規則は、パーセント記号を含むローカル部分が他のすべての方法 (後で説明する全一致規則を含む) で書き換えに失敗した場合にのみアクティブになります。

パーセントハック規則は、パーセントハックアドレスに何らかの特別な意味を持たせる場合に便利です。

bang-style (UUCP) アドレスに一致する規則

MTA が B!A 形式のアドレスを書き換えようとして失敗した場合は、そのアドレスが B!A@localhost 形式のアドレスとして扱われる前に、もう 1 つの規則が適用されます。この規則が *bang-style* 規則です。パターンは $! で、これが変わることはありません。この規則は、感嘆符を含むローカル部分が他のすべての方法 (後で説明するデフォルトの規則を含む) で書き換えに失敗した場合にのみアクティブになります。

bang-style 規則を使用すると、UUCP スタイルのアドレスが UUCP システムおよびルーティングに関する総合的な情報を備えたシステムを経由するように書き換えることができます。

任意のアドレスに一致する規則

特殊パターン「.」(ドット文字) は、他に一致する規則がない場合に、任意のホスト / ドメイン仕様に一致します。ただし、そのホスト / ドメイン仕様は、チャネルテーブル内で見つからないものに限ります。つまり、「.」規則は、アドレスの書き換えに失敗する前の最後の手段として使用されます。

注	置換シーケンスについては、全一致規則が一致し、そのテンプレートが展開される場合、$H はホストのフルネームに展開し、$D はドット文字 1 個「.」に展開します。したがって、全一致規則のテンプレートでは、$D の使用が制限されます。

タグ付き書き換え規則セット

書き換えプロセスを実行するにあたり、別の規則セットを追加するとうまくいく場合があります。別の規則セットを追加するには、書き換え規則タグを使用します。現在のタグは、設定ファイルまたはドメインデータベースでパターンが検索される前に、各パターンの前に付けられます。タグは、書き換え規則テンプレート内の $T という代替文字列を使って一致する書き換え規則により変更することができます (後述の説明を参照)。

タグは、1 つのアドレスから抽出されたすべてのホストに対し、連続して適用されます。そのため、タグを使用した場合は、別の規則を指定する際にそれが正しいタグ値から始まるように注意してください。一般に、タグは特殊な目的でしか使用しないため、このことが問題になることはほとんどありません。アドレスの書き換えが完了すると、タグはデフォルトのタグ (空白文字列) にリセットされます。

規則により、すべてのタグ値には、その最後に縦棒 (|) が付けられます。この文字は通常のアドレスには使用されないため、パターンの残りの部分とタグとを区別することができます。

書き換え規則のテンプレート

以下の節では、書き換え規則のテンプレートについて詳説します。表 7-2 に、テンプレートの各形式を示します。

表 7-2　書き換え規則のテンプレート形式

テンプレート	使用方法
A%B	A は新しいユーザ / メールボックス名になり、B は新しいホスト / ドメイン仕様になります。繰り返して書き換えます。
A@B	A%B@B として扱われます。
A%B@C	A は新しいユーザ / メールボックス名になり、B は新しいホスト / ドメイン仕様になります。ホスト C に関連したチャネルに送ります。
A@B@C	A@B@C@C として扱われます。
A@B@C@D	A は新しいユーザ / メールボックス名になり、B は新しいホスト / ドメイン名になります。C をソースルートとして挿入し、ホスト D に関連したチャネルに送ります。

よく使われる書き換えテンプレート : A%B@C または A@B

以下に示すテンプレート形式は、最もよく使われるものです。規則は、アドレスのユーザ部分とドメイン部分に適用されます。その後、新しいアドレスがメッセージを特定のチャネル (*ChannelTag* で指定されたチャネル) へ送るために使用されます。

UserTemplate%*DomainTemplate*@*ChannelTag*[*コントロール*]

以下に示すテンプレート形式は、上記のテンプレートと実質的に同じものです。ただし、この形式は、*DomainTemplate* と *ChannelTag* が同じ場合にしか使用できません。

UserTemplate@*ChannelTag*[*コントロール*]

繰り返し書き換えテンプレート : A%B

以下に示すテンプレート形式は、繰り返して適用する必要がある規則に使用されます。いったん規則が適用された後、その新しいアドレスに対して書き換えプロセス全体が繰り返されます (他の書き換え規則形式の場合は、いずれも規則が適用されたに書き換えプロセスが終了します)。

UserTemplate%*DomainTemplate*[*コントロール*]

たとえば、以下に示す規則を使うと、.removable というドメイン名で終わるすべてのアドレスから .removable が削除されます。

```
.removable      $U%$H
```

繰り返し規則を使用する場合には、「規則ループ」が生じないよう特別な注意が必要です。そのため、特に必要がない限り、繰り返し書き換え規則の使用を控えるようお勧めします。繰り返し規則を使用する際には、imsimta test -rewrite コマンドを使って規則をテストするとよいでしょう。test -rewrite コマンドの詳細については、『Messaging Server リファレンスマニュアル』を参照してください。

指定ルート書き換えテンプレート : A@B@C@D または A@B@C

以下に示すテンプレート形式は、一般によく使われる形式 *UserTemplate*%*DomainTemplate*@*ChannelTag* (最初の区切り文字が異なります) と同じように機能します。ただし、*ChannelTag* はソースルートとしてアドレスに挿入されています。メッセージは *ChannelTag* に送られます。

UserTemplate@*DomainTemplate*@*Source-Route*
@*ChannelTag*[*コントロール*]

書き換えられたアドレスは @*route*:*user*@*domain* となります。また、次のテンプレートも使用できます。

UserTemplate@*DomainTemplate*@*ChannelTag*[*コントロール*]

たとえば、以下に示す規則を使うと、jdoe@com1 というアドレスが @siroe.com:jdoe@com1 というソースルートアドレスに書き換えられます。チャネルタグは siroe.com になります。

```
com1 $U@com1@siroe.com
```

書き換え規則テンプレートにおける大文字と小文字の区別

書き換え規則内のパターンとは異なり、テンプレートでは大文字と小文字が区別されます。この機能は、大文字と小文字を区別するメールシステムへのインターフェースを提供するような書き換え規則を使用する場合に必要となります。アドレスから抽出された部分の代わりに使われる $U や $D などの置換シーケンスでも、大文字と小文字が区別され、元のアドレスと同じ状態が維持されます。

UNIX システムでメールボックスを小文字にする場合など、代替部分に特定の大文字 / 小文字が使われるようにするには、テンプレートに特殊な置換シーケンスを使用します。たとえば、$\ は後に続く代替部分を小文字にし、$^ は後に続く代替部分を大文字にします。また、$_ は元と同じ状態を保ちます。

たとえば、以下の規則を使うと、unix.siroe.com のアドレスに対するメールボックスを小文字にすることができます。

```
unix.siroe.com    $\$U$_%unix.siroe.com
```

MTA がアドレスに書き換え規則を適用する方法

以下に、MTA が指定アドレスに書き換え規則を適用する手順について説明します。

1 アドレスから最初のホスト仕様またはドメイン仕様を抽出します。

アドレスには、次のように 1 つ以上のホスト名またはドメイン名が指定されている場合があります。

```
jdoe%hostname@siroe.com.
```

2 最初のホスト名またはドメイン名を識別した後、そのホスト名またはドメイン名に一致するパターンが含まれている書き換え規則を検索します。

3 一致する書き換え規則が見つかると、その規則のテンプレート部分に従ってアドレスを書き換えます。

4 最後に、チャンネルタグと各チャネルに関連するホスト名とを比較します。

一致するものが見つかると、MTA は関連するチャネルへのメッセージをキューに入れます。一致するものが見つからない場合、書き換えプロセスは失敗に終わります。一致するチャネルがローカルチャネルの場合は、エイリアスデータベースやエイリアスファイルを検索することによって、さらにアドレスの書き換えが実行される場合があります。

これらの動作の詳細については、後続の節を参照してください。

注 既存のどのチャネルにも属さないチャネルタグを使用すると、この規則に一致するアドレスを持つメッセージが戻ってきます。すなわち、一致するメッセージが配信不能となります。

動作 1 最初のホスト / ドメイン仕様を抽出する

アドレスの書き換えプロセスは、アドレスから最初のホストまたはドメイン仕様を抽出することから始まります (以下の説明をより理解するために、RFC 822 アドレス規則について把握しておくことをお勧めします)。アドレス内のホスト / ドメイン仕様が検索される順序は、以下のとおりです。

1 ソースルートのホスト (左から右へ読み取り)

2 単価記号 (@) の右側にあるホスト

3 最後のパーセント記号 (%) の右側にあるホスト

4 最初の感嘆符 (!) の左側にあるホスト

最後の 2 項目の順序は、アドレスの書き換えを行っているチャネルで bangoverpercent キーワードが有効になっているかどうかによって入れ替わります。すなわち、メッセージをキューに入れようとしているチャネルが bangoverpercent チャネルキーワードでマークされているかどうかによって順序が異なります。

表 7-3 に、アドレスと最初に抽出されるホスト名の例を示します。

表 7-3　　アドレスと抽出されるホスト名

アドレス	最初のホストドメイン仕様	コメント
user@a	a	「短形式」のドメイン名。
user@a.b.c	a.b.c	「完全修飾」のドメイン名 (FQDN)。
user@[0.1.2.3]	[0.1.2.3]	ドメインリテラル。
@a:user@b.c.d	a	短形式のドメイン名をともなった「ルート」と呼ばれるソースルートアドレス。
@a.b.c:user@d.e.f	a.b.c	ソースルートアドレス ; ルート部分は完全形。
@[0.1.2.3]:user@d.e.f	[0.1.2.3]	ソースルートアドレス ; ルート部分はドメインリテラル。
@a,@b,@c:user@d.e.f	a	a -> b-> c ルーティングをともなったソースルートアドレス。
@a,@[0.1.2.3]:user@b	a	ルート部分にドメインリテラルをともなったソースルートアドレス。
user%A@B	B	この非標準形のルーティングは「パーセントハック」と呼ばれます。
user%A	A	
user%A%B	B	
user%%A%B	B	
A!user	A	「bang-style」のアドレス。UUCP によく使われます。
A!user@B	B	
A!user%B@C	C	
A!user%B	B	nobangoverpercent キーワードが有効な場合 (デフォルト)。
A!user%B	A	bangoverpercent キーワードが有効な場合。

RFC 822 には、アドレスにおける感嘆符 (!) およびパーセント記号 (%) の解釈が含まれていません。パーセント記号は慣例上 単価記号 (@) と同じように解釈されます (単価記号 @ がない場合)。この規則は Messaging Server MTA で採用されています。

パーセント記号をローカルユーザ名の一部として扱うために、繰り返しパーセント記号の解釈が使用されます。これは、外部メールシステムのアドレスを処理するような場合に便利です。感嘆符の解釈は、RFC 976 の「bang-style」アドレス規則に従います。この解釈により、Messaging Server MTA で UUCP アドレスを使用することが可能になります。

これらの解釈の順序については、RFC 822 または RFC 976 のどちらにも指定されていません。そのため、bangoverpercent および nobangoverpercent キーワードを使って、書き換えを行うチャネルによって解釈が適用される順序を制御します。デフォルト設定がより標準的ですが、状況によっては代わりの設定を使った方が便利な場合もあります。

注 アドレス内に感嘆符 (!) やパーセント記号 (%) を使用することはお勧めしません。

動作 2 書き換え規則を検索する

アドレスから最初のホストまたはドメイン仕様が抽出されると、MTA は書き換え規則を調べてその仕様の処理方法を明らかにします。ホスト / ドメイン仕様は、各規則のパターン部分 (各規則の左側) と比較されます。その場合、大文字と小文字の区別はありません。大文字と小文字の区別がないことは、RFC 822 で定められています。MTA では、特に大文字と小文字を区別しませんが、可能な限り元の状態が維持されます。

ホスト / ドメイン仕様がどのパターンにも一致しない場合は、ホスト / ドメイン仕様の最初の部分 (最初のドット文字より前の部分、通常はホスト名) がアスタリスク (*) に置き換えられ、その新しいホスト / ドメイン仕様が検索されます。ただし、その場合、検索対象となるのは設定ファイル内の書き込み規則だけで、ドメインデータベースは調べられません。

この試行が失敗に終わると、最初の部分が削除され、プロセスが繰り返されます。この試行も失敗に終わると、次の部分 (通常はサブドメイン) が削除され、再び検索が行われます。最初にアスタリスクを含めて検索が行われ、その後アスタリスクを含めずに検索が行われます。アスタリスクを含んだ検索が行われるのは設定ファイル内の書き換え規則テーブルだけで、ドメインデータベースは調べられません。このプロセスは、一致する規則が見つかるか、またはホスト / ドメイン仕様全体がなくなるまで続けられます。このようなプロセスを使用することにより、より目的に近いドメインを最初に見つけ出し、次により特化したドメインを検索することができます。

このマッチングプロセスのアルゴリズムは、以下のとおりです。

- ホスト / ドメイン仕様が比較文字列 spec_1 および spec_2 の最初の値として使用されます (たとえば、spec_1 = spec_2 = a.b.c)。
- 比較文字列 spec_1 が設定ファイル内にある各書き換え規則のパターン部分と比較されます。一致するものが見つからない場合は、次にドメインデータベース内が調べられます。このマッチングプロセスは、一致するものが見つかった時点で終了します。
- 一致するものが見つからなかった場合は、spec_2 の最も左側の部分 (アスタリスク以外) がアスタリスクに変換されます。たとえば、a.b.c という spec_2 は *.b.c に、*.b.c という spec_2 は *.*.c に変換されます。このマッチングプロセスは、一致するものが見つかった時点で終了します。
- 一致するものが見つからなかった場合は、比較文字列 spec_1 の最初の部分 (先頭のアスタリスクを含む) が削除されます。spec_1 が 1 つの部分だけからなる場合 (たとえば、.c または c) は、ドット文字 1 個に置き換えられます。削除後の新しい spec_1 文字列の長さがゼロでない場合は、動作 1 に戻ります。削除後の新しい文字列の長さがゼロの場合 (たとえば、削除前の文字列が「.」だった場合) は、検索プロセスが失敗に終り、マッチングプロセスが終了します。

たとえば、dan@sc.cs.siroe.edu というアドレスを書き換える場合、MTA は以下に示すパターンを上から順番に検索します。

```
sc.cs.siroe.edu
*.cs.siroe.edu
.cs.siroe.edu
*.*.siroe.edu
.siroe.edu
*.*.*.edu
.edu
*.*.*.*
.
```

動作 3 テンプレートに従ってアドレスを書き換える

ホスト / ドメイン仕様が書き換え規則に一致すると、そのホスト / ドメイン仕様は規則のテンプレート部分を使って書き換えられます。テンプレートには、次の 3 つの仕様があります。

1 アドレスの新しいユーザ名。

2 アドレスの新しいホスト / ドメイン仕様。

3 メッセージの送信先である既存の MTA チャネルが指定されたチャネル。

動作 4 書き換えプロセスを終了する

ホスト / ドメイン仕様が書き換えられると、次の 2 つの動作のうちどちらかが行われます。

- チャネルタグがローカルチャネルまたは routelocal チャネルキーワードでマークされているチャネルのどちらにも関連付けられていない場合、またはアドレス内に他のホスト / ドメイン仕様がない場合は、書き換え後の指定が抽出された元の指定に置き換えられ、書き換えプロセスが終了します。
- チャネルタグがローカルチャネルまたは routelocal でマークされたチャネルに一致し、かつアドレス内に他のホスト / ドメイン仕様がある場合は、書き換え後のアドレスが破棄され、アドレスから元 (最初) のホスト / ドメイン仕様が削除されます。そして、そのアドレスから新しいホスト / ドメイン仕様が抽出され、プロセス全体が繰り返されます。書き換えプロセスは、すべてのホスト / ドメイン仕様がなくなるか、あるいは非ローカルチャネルまたは非ルートローカルチャネルを介したルートが見つかるまで続けられます。MTA がソースルーティングをサポートできるのは、この反復メカニズムがあるからです。実際、ローカルシステムまたはルートローカルシステムを介した不必要なルートは、このプロセスによってアドレスから削除されます。

書き換え規則に一致しなかった場合

ホスト / ドメイン仕様がどの書き換え規則にも一致せず、デフォルトの規則もない場合には、「そのまま」の仕様が使われます。たとえば、元の仕様が新しい仕様およびルーティングシステムになります。アドレスに無意味なホスト / ドメイン仕様が含まれている場合、その仕様は、ルーティングシステムが任意のチャネルに関連付けられたどのシステム名にも一致しないときに検出され、メッセージが戻されます。

書き換え後の構文チェック

書き換え規則が適用された後のアドレスに対し、構文チェックは行われません。これは意図的なものです。構文チェックを行わないようにすることで、書き換え規則を使ってアドレスを RFC 822 に準拠しない形式に変換することができます。ただし、設定ファイル内に間違いがあると、MTA から送り出されるメッセージに不正なアドレスが含まれる可能性もあります。

ドメインリテラルの処理

ドメインリテラルは、特に書き換えプロセス中に処理されます。アドレスのドメイン部分にあるドメインリテラルが書き換え規則のパターンに一致しない場合、そのリテラルは、角括弧で囲まれ、ドット文字で区切られた文字列の集まりとして解釈されます。そして、最も右側にある文字列が削除され、検索が繰り返されます。それでも一致するものが見つからない場合は、角括弧だけが残るまで次々に文字列が削除されていきます。空白の角括弧を使った検索も失敗に終わった場合は、ドメインリテラル全体が削除され、ドメインアドレスの次の部分について書き換え処理が実行されます (次の部分が存在する場合)。ドメインリテラルの内部処理では、アスタリスクが使用されません。ドメインリテラル全体がアスタリスクに置き換えられた場合は、アスタリスクの数とドメインリテラル内の要素の数とが一致します。

通常のホスト / ドメイン仕様の場合と同じように、ドメインリテラルの場合も指定した内容に最も近いものから順に検索が行われます。そして、パターンに一致した最初の規則を使って、ホスト / ドメイン仕様の書き換えが行われます。規則リスト内に同じパターンが 2 つある場合は、先に記述されている方の規則が適用されます。

たとえば、`dan@[128.6.3.40]` というアドレスを書き換えるとします。この場合、まず `[128.6.3.40]` の検索が行われ、その後 `[128.6.3.]`、`[128.6.]`、`[128.]`、`[]`、`[*.*.*.*]`、そして最後に全一致規則「.」という順に検索が実行されます。

ドメインリテラルとドメイン名が組み合わさっている場合は、検索試行の回数がかなり多くなります。この方法は一般的ではないため、この方法を使用することはお勧めしません。たとえば、dan@[1.2].a.[3.4].b というアドレスの場合は、以下に示す検索が実行されます。

```
[1.2].a.[3.4].b
[1.].a.[3.4].b
[].a.[3.4].b
[*.*].a.[3.4].b
.a.[3.4].b
[*.*].*.[3.4].b
.[3.4].b
[*.*].*.[3.].b
.[3.].b
[*.*].*.[].b
.[].b
[*.*].*.[*.*].b
.b
[*.*].*.[*.*].*
.
```

テンプレートの置換シーケンスと書き換え規則 コントロールシーケンス

置換シーケンスは、書き換え後のアドレスに文字列を挿入することにより、ユーザ名またはアドレスを書き換えるために使用します。挿入される文字列は、使用している置換シーケンスによって決まります。

たとえば、以下のテンプレートでは、$U が置換シーケンスです。この置換シーケンスを使用することにより、書き換えられるアドレスの**ユーザ名**部分がテンプレートの出力に挿入されます。したがって、このテンプレートによって jdoe@mailhost.siroe.com が書き換えられる場合、その出力は jdoe@siroe.com となります。つまり、$U が元のアドレスの **ユーザ名**部分に置き換えられます。

```
$U@siroe.com
```

コントロールシーケンスは、書き換え規則を適用するうえで、さらに条件を加えるためのものです。すなわち、書き換え規則のパターン部分がホスト / ドメイン仕様に一致しなければならないだけでなく、書き換えるアドレスの他の要素がコントロールシーケンスの条件を満たしていなければなりません。たとえば、$E コントロールシーケンスは、書き換えるアドレスがエンベロープアドレスでなければならないことを意味します。また、$F コントロールシーケンスは、そのアドレスが前方を探すアドレスでなければならないことを意味します。以下の書き換え規則は、user@siroe.com 形式の (書き換え) エンベロープ「To:」アドレスにのみ適用されます。

```
siroe.com $U@mail.siroe.com$E$F
```

ホスト / ドメイン仕様は書き換え規則のパターン部分に一致するが、テンプレート内のコントロールシーケンスに指定されている条件がすべて満たされない場合、その書き換え規則は失敗に終わり、他の適用可能な規則が検索されます。

表 7-4 に、テンプレートの置換シーケンスおよびコントロールシーケンスを示します。

表 7-4　テンプレートの置換シーケンスとコントロールシーケンス

置換シーケンス	置き換える内容
$D	一致したドメイン仕様の部分。
$H	ホスト / ドメイン仕様の不一致部分。パターン内のドットの左側。
$L	ドメインリテラルの不一致部分。パターンリテラル内のドットの右側。
$U	元のアドレスのユーザ名。
$0U	元のアドレスのローカル部分 (ユーザ名)。サブアドレスは含まれません。
$1U	元のアドレスのローカル部分 (ユーザ名) にあるサブアドレス (存在する場合のみ)。
$$	ドル記号 ($) を挿入します。
$%	パーセント記号 (%) を挿入します。
$@	単価記号 (@) を挿入します。
$\	小文字にします。
$^	大文字にします。
$_	元の大文字 / 小文字を使用します。
$W	ランダムに選択される固有文字列の代替。
$]...[	LDAP クエリの URL 検索。
$ (テキスト)	一般データベースの代替。検索に失敗すると、規則も失敗します。
${...}	指定マッピングを与えられた文字列に適用します。
$[...]	カスタマ提供のルーチンを起動します。結果の代替。
$&*n*	一致しなかった (またはワイルドカードを使った) ホストの *n* 番目の部分。0 から始まり、左から右へ数えます。
$!*n*	一致しなかった (またはワイルドカードを使った) ホストの *n* 番目の部分。0 から始まり、右から左へ数えます。
$**n*	一致したパターンの *n* 番目の部分。0 から始まり、左から右へ数えます。
$#*n*	一致したパターンの *n* 番目の部分。0 から始まり、右から左へ数えます。

表 7-4　テンプレートの置換シーケンスとコントロールシーケンス（続き）

置換シーケンス	置き換える内容
$*n*D	一致したドメイン仕様の一部。左側の 0 から n 番目までの部分が残されます。
$*n*H	一致しなかったホスト / ドメイン仕様の一部。左側の 0 から n 番目までの部分が残されます。
コントロールシーケンス	**書き換え規則における効果**
$E	エンベロープアドレスにのみ適用されます。
$B	ヘッダ / 本文アドレスにのみ適用されます。
$F	前方を探すアドレス (例、To:) にのみ適用されます。
$R	後方を探すアドレス (例、From:) にのみ適用されます。
$M *channel*	*channel* がアドレスを書き換える場合にのみ適用されます。
$N *channel*	*channel* がアドレスを書き換える場合は適用されません。
$Q *channel*	*channel* へ送る場合に適用されます。
$C *channel*	*channel* へ送る場合は適用されません。
$S	ホストがソースルートからのものである場合に適用されます。
$A	ホストが 単価記号 @ の右側にある場合に適用されます。
$P	ホストがパーセント記号の右側にある場合に適用されます。
$X	ホストが感嘆符の左側にある場合に適用されます。
$T*newtag*	書き換え規則タグを newtag に設定します。
$?*errmsg*	書き換えに失敗した場合、デフォルトのエラーメッセージの代わりに errmsg を返します。

ユーザ名とサブアドレスの代替：$U、$0U、$1U

テンプレート内にある $U はすべて、元のアドレスから抽出されたユーザ名 (RFC 822「ローカル部」) に置き換えられます。この場合、a."b" 形式のアドレスは "a.b" に置き換えられます。現在行われているインターネットの標準化では、RFC 822 における古い構文の使用は推奨されません。今後、より新しい構文の使用が中心になると考えられます。

テンプレート内にある $0U はすべて、元のアドレスのユーザ名に置き換えられます。ただし、サブアドレスおよびサブアドレスを示す文字 (+) は含まれません。テンプレート内にある $1U はすべて、元のアドレスのサブアドレスおよびサブアドレスを示す文字 (+) に置き換えられます (それらが存在する場合のみ)。$0U と $1U はユーザ名を互いに補う関係にあります。すなわち、$0U$1U と $U とは同じものです。

ホスト / ドメインと IP リテラルの代替 : $D、$H、$nD、$nH、$L

$H はすべて、規則に一致しなかったホスト / ドメイン仕様の部分に置き換えられます。また、$D はすべて、規則に一致したホスト / ドメイン仕様の部分に置き換えられます。$nH および $nD は、通常の $H または $D の部分から左側の 0 から n 番目までの部分を残す変形体です。すなわち、$nH または $nD を使用すると、通常 $H または $D で得られる部分から左端の 1 から n 番目までの部分が省略されます。$0H と $H、および $0D と $D はそれぞれ同じものです。

たとえば、jdoe@host.siroe.com というアドレスが以下の規則に一致したとします。

```
host.siroe.com    $U%$1D@TCP-DAEMON
```

この規則が適用されると、出力チャネルに TCP-DAEMON を使用する jdoe@siroe.com というアドレスが得られます。$D は一致したドメイン全体 (つまり host.siroe.com) に置き換えられる置換シーケンスですが、この例で使われている $1D は一致したドメインから部分 1 (siroe) を省略した部分 (siroe.com) に置き換えられます。

$L は、書き換え規則に一致しなかったドメインリテラルの部分に置き換えられます。

リテラル文字の代替 : $$、$%、$@

通常、$、%、および @ 文字は書き換え規則テンプレートのメタ文字です。これらの文字を挿入する場合は、その文字の前にドル記号 $ を付けます。すなわち、$$ は単一のドル記号 $ に、$% は単一のパーセント記号 % (この場合、パーセントはテンプレートのフィールド区切り文字として解釈されません) に、$@ は単一の単価記号 @ (同様に、フィールド区切り文字として解釈されません) に展開されます。

LDAP クエリ URL の代替 : $]...[

$]ldap-url[形式の置換シーケンスは LDAP クエリ URL として解釈され、LDAP クエリの結果に置き換えられます。標準の LDAP URL では、ホストとポートが省略されます。その代わり、ホストとポートは、msg.conf ファイル (local.ldaphost および local.ldapport 属性) で指定されています。

すなわち、LDAP URL は、以下のように指定されます。ここで、角括弧 [ ] は URL のオプション部分を表しています。

```
ldap:///dn[?attributes[?scope?filter]]
```

dn は検索ベースを指定する名前で、この部分は必須です。URL のオプションである属性 (attributes)、範囲 (scope)、フィルタ (filter) は、戻される情報を指定するためのものです。書き換え規則の場合、戻される情報を指定するための属性として望ましいのは mailRoutingSystem 属性 (または同様の属性) です。範囲は、任意のベース (デフォルト)、one、または sub にすることができます。また、フィルタには、mailDomain の値が書き換えられるドメインに一致するオブジェクトを戻すようなリクエストを指定するとよいでしょう。

LDAP ディレクトリスキーマに mailRoutingSystem および mailDomain 属性が含まれている場合、指定アドレスの送り先となるシステムを決定する書き換え規則は、たとえば次のようになります。この例で、作成された LDAP クエリ内の LDAP URL 置換シーケンス $D は、現在のドメイン名に置き換えられます。

```
.siroe.com \    $U%$H$D@$]ldap:///o=siroe.com?mailRoutingSystem?sub?
\
   (mailDomain=$D)[
```

この例で使われているバックスラッシュは、書き換え規則の 1 行が次の行に続いていることを示すためのものです。表 7-5 に、LDAP URL 置換シーケンスを示します。

表 7-5　　LDAP URL 置換シーケンス

置換シーケンス	説明
$$	$ 文字
$~ *アカウント*	ユーザアカウントのホームディレクトリ
$A	アドレス
$D	ドメイン名
$H	ホスト名 (完全なドメイン名の最初の部分)
$L	~ または _ などの特別な先頭文字を除くユーザ名
$S	サブアドレス
$U	ユーザ名

一般データベースの代替：$(...)

$(テキスト) 形式の置換シーケンスは、特殊な方法で処理されます。テキスト部分は、特殊な一般データベースにアクセスするためのキーとして使われます。このデータベースは、/imta/config/imta_tailor ファイル内の IMTA_GENERAL_DATABASE オプションで指定されているファイル (通常、/imta/db/generaldb.db ファイル) で構成されています。

このデータベースは、imta crdb ユーティリティを使って作成されます。「テキスト文字列」がデータベース内のエントリに一致すると、データベース内の対応するテンプレートがその文字列に置き換えられます。「テキスト文字列」がデータベース内のどのエントリにも一致しなかった場合は、書き換えプロセスが失敗に終わります。つまり、最初から何も一致しなかったのと同じ状態に戻ります。置き換えがうまくいくと、次にデータベースから抽出されたテンプレートに別の置換シーケンスが含まれていないかどうかが調べられます。ただし、抽出されたテンプレート内に別の $(テキスト) を含めることは禁じられています。参照ループが発生する可能性があるからです。

例として、次の書き換え規則に jdoe@siroe.siroenet というアドレスが一致した場合を考えてみましょう。

```
.SIROENET $($H)
```

まず、一般データベースで siroe というテキスト文字列が検索され、その結果 (見つかった場合) が書き換え規則のテンプレートとして用いられます。ここで、siroe の検索結果を $u%eng.siroe.com@siroenet とします。この場合、テンプレートの出力は jdoe@eng.siroe.com (すなわち、ユーザ名 = jdoe、ホスト / ドメイン仕様 = eng.siroe.com) になり、ルーティングシステムは siroenet になります。

一般データベースは、正しい操作を行うために誰でも読み取り可能でなければなりません。

指定マッピングの適用 : ${...}

${mapping,argument} 形式の置換シーケンスは、MTA マッピングファイルでマッピングを検索し、見つかったマッピングを適用するのに使用します。mapping フィールドにはマッピングテーブルの名前を指定し、argument フィールドにはマッピングへ渡す文字列を指定します。この置換シーケンスを使用するには、指定したマッピングが存在し、かつその出力に $Y フラグが設定されていなければなりません。マッピングが存在しなかったり、$Y フラグが設定されていない場合、書き換えは失敗に終わります。問題なく処置が行われた場合は、マッピングの結果がテンプレート内の同じ位置にマージされた後、再び展開されます。

このメカニズムにより、様々な方法で MTA 書き換えプロセスを展開することができます。たとえば、アドレスのユーザ名部分を選択しながら分析したり変更することができます。通常の MTA 書き換えプロセスに、このような機能はありません。

カスタマ指定ルーチンの代替 : $[...]

$[*image*,*routine*,*argument*] 形式の置換シーケンスは、カスタマ指定ルーチンを検索し、呼び出すのに使用します。UNIX において、MTA は dlopen および dlsym を使って動的に共有ライブラリイメージから指定したルーチンをロードし、呼び出します。そのとき、そのルーチンは以下の引数をともなった関数として呼び出されます。

```
status := routine (argument, arglength, result, reslength)
```

argument および *result* は、252 バイトの文字列バッファです。UNIX 上で、*argument* と *result* は文字列へのポインタ (例、C 言語の char*) として渡されます。*arglength* と *reslength* は、参照によって渡される符号付の long 型整数です。入力時、*argument* には書き込み規則テンプレートからの引数文字列が含まれ、*arglength* にはその文字列の長さが含まれます。値を返すときには、*result* に結果文字列が入り、*reslength* にその長さが入ります。そして、結果的に得られた文字列が書き換え規則テンプレート内の "$[*image,routine,argument*]" に置き換わります。routine の値として 0 が返された場合には書き換え規則が有効になり、-1 が返された場合には書き換え規則が失敗に終わります。

このメカニズムによって、書き換えプロセスの複雑な展開が可能になります。たとえば、あるタイプの名前サービスに対して呼び出しを実行し、その結果を使って名前を変化させることができます。前方を探すアドレス (例、To: アドレス) のディレクトリサービス検索を siroe.com というホストに対して実行する場合には、以下のような書き込み規則を使用します。$F を使うことによって、この規則が前方を探すアドレスにのみ適用されるようになります。$F の詳細については、132 ページの「方向および位置に固有の書き換え規則 ($B、$E、$F、$R)」を参照してください。

```
siroe.com $F$[LOOKUP_IMAGE,LOOKUP,$U]
```

jdoe@siroe.com という前方を探すアドレスがこの規則に一致すると、メモリ内に LOOKUP_IMAGE (UNIX の共有ライブラリ) がロードされ、jdoe を引数パラメータとしてともなった LOOKUP ルーチンが呼び出されます。その後、LOOKUP ルーチンは、結果パラメータ内の John.Doe%eng.siroe.com などの別の名前と書き換え規則が適用されたことを示す値 (-1) を返します。結果文字列内のパーセント記号 (117 ページの「繰り返し書き換えテンプレート : A%B」を参照) は、書き換えプロセスを繰り返すためのものです。この場合、書き換え元のアドレスには John.Doe@eng.siroe.com が使用されます。

UNIX システムでは、サイト提供の共有ライブラリイメージが誰でも読み取り可能でなければなりません。

注 この機能は、Messaging Server の機能をシステム全体に拡張するためのもので、一般ユーザが使用するものではありません。

単一フィールドの代替 : $&、$!、$*、$#

単一フィールド置換シーケンスは、書き換えるホスト / ドメイン仕様からサブドメイン部分を抽出するためのものです。表 7-6 に、使用可能な単一フィールド置換シーケンスを一覧します。

表 7-6 単一フィールドの置換シーケンス

コントロールシーケンス	使用目的
$&n	ホスト仕様 (ワイルドカードに一致しなかった / 一致した部分) 内の n 番目の要素を表します (n=0,1,2,..,9,)。要素はドット文字で区切られており、最も左にあるものが「要素 0」となります。要求された要素が存在しない場合は、書き換えが失敗に終わります。
$!n	ホスト仕様 (ワイルドカードに一致しなかった / 一致した部分) 内の n 番目の要素を表します (n=0,1,2,..,9,)。要素はドット文字で区切られており、最も右にあるものが「要素 0」となります。要求された要素が存在しない場合は、書き換えが失敗に終わります。
$*n	ドメイン仕様 (パターンで指定されているテキストに一致した部分) 内の n 番目の要素を表します (n=0,1,2,...,9,)。要素はドット文字で区切られており、最も左にあるものが「要素 0」となります。要求された要素が存在しない場合は、書き換えが失敗に終わります。
$#n	ドメイン仕様 (パターンで指定されているテキストに一致した部分) 内の n 番目の要素を表します (n=0,1,2,...,9,)。要素はドット文字で区切られており、最も右にあるものが「要素 0」となります。要求された要素が存在しない場合は、書き換えが失敗に終わります。

jdoe@eng.siroe.com というアドレスが次の書き換え規則に一致したとします。

```
*.SIROE.COM     $U%$&0.siroe.com@mailhub.siroe.com
```

この場合、テンプレートからは「mailhub.siroe.com をルーティングシステムとして使った jdoe@eng.siroe.com 」という結果が得られます。

固有文字列の代替

$W コントロールシーケンスは、大文字の英数字からなる繰り返し不可能な固有のテキスト文字列に挿入します。$W は、繰り返されないアドレス情報を作成するような場合に便利です。

ソースチャネル固有の書き換え規則 ($M、$N)

特定のチャネルに関してのみ動作する書き換え規則を作成することができます。これは、短形式の名前に 2 つの意味が含まれるような場合に便利です。

1 名前が 1 つのチャネルに届くメッセージ内にある場合。

2 名前が別のチャネルに届くメッセージ内にある場合。

ソースチャネル固有の書き換えは、使用中のチャネルプログラムおよび rules / norules チャネルキーワードに関連しています。書き換えを実行する MTA コンポーネントに関連付けられたチャネルに norules が指定されている場合、チャネル固有の書き換え規則チェックは行われません。そのチャネルに rules 指定されている場合は、チャネル固有の書き換え規則チェックが行われます。デフォルトは rules キーワードです。

ソースチャネル固有の書き換えは、指定されたアドレスに一致するチャネルとは関係がありません。このタイプの書き換えは、書き換えを実行する MTA コンポーネントとそのコンポーネントのチャネルテーブルエントリにのみ依存します。

チャネル固有の書き換え規則チェックは、規則のテンプレート部分に $N または $M コントロールシーケンスがある場合に実行されます。$N または $M の直後から単価記号 (@)、パーセント記号 (%)、または後続の $N、$M、$Q、$C、$T、または $? までの間にある文字がチャネル名として解釈されます。

たとえば、$M*channel* を使用したときに *channel* が現在書き換えを行っているチャネルでない場合は、規則が適用されません。また、$N*channel* を使用したときに *channel* が書き換えを行っている場合も、規則が適用されません。複数の $M および $N 句を指定することもできます。複数個の $M 句を使用した場合は、そのうちの 1 つでも一致すれば、規則が適用されます。複数の $N 句を使用している場合は、そのうちの 1 つでも一致すれば、規則の適用は失敗に終わります。

宛先チャネル固有の書き換え規則 ($C、$Q)

メッセージをキューに入れる依存する書き換え規則を作成することができます。これは、あるホストに対して名前が 2 つあるような場合に便利です。つまり、1 つのホストグループに認識されている名前と、別のホストグループに認識されている名前とが異なる場合です。異なるチャネルを使って各グループにメールを送ることにより、各グループに知られている名前を使ってホストを参照するようにアドレスを書き換えることができます。

宛先チャネル固有の書き換えは、メッセージを取り出して処理するチャネルとそのチャネルに関する rules/norules キーワードに関連しています。宛先チャネルに norules が指定されている場合、チャネル固有の書き換え規則チェックは行われません。宛先チャネルに rules が指定されている場合は、チャネル固有の書き換え規則チェックが行われます。デフォルトのキーワードは rules です。

宛先チャネル固有の書き換えは、指定されたアドレスに一致するチャネルとは関係がありません。このタイプの書き換えは、メッセージのエンベロープ To: アドレスにのみ依存します。メッセージがキューに入ると、まずそのエンベロープ To: アドレスが書き換えられ、メッセージの送り先チャネルが決定されます。エンベロープ To: アドレスの書き換え中、$C および $Q コントロールシーケンスはすべて無視されます。エンベロープ To: アドレスが書き換えられて宛先チャネルが決まると、その後、メッセージに関連する他のアドレスが書き換えられるときに、$C および $Q コントロールシーケンスが考慮されます。

宛先チャネル固有の書き換え規則チェックは、規則のテンプレート部分に $C または $Q コントロールシーケンスがあると実行されます。$C または $Q の直後から単価記号 (@)、パーセント記号 (%)、または後続の $N、$M、$C、$Q、$T、または $? までの間にある文字がチャネル名として解釈されます。

たとえば、$Q*channel* を使用したときに *channel* が宛先でない場合は、規則が適用されません。また、$C*channel* を使用したときに *channel* が宛先である場合にも、規則は適用されません。複数の $Q および $C 句を指定することもできます。複数の $Q 句を指定した場合は、そのうちの 1 つでも一致すれば、規則が適用されます。複数の $C 句を指定した場合は、そのうちの 1 つでも一致すれば、規則の適用は失敗に終わります。

方向および位置に固有の書き換え規則 ($B、$E、$F、$R)

エンベロープアドレスにのみ適用される書き換え規則、またはヘッダアドレスにのみ適用される書き換え規則を指定したい場合があります。$E コントロールシーケンスを使うと、書き換えるアドレスがエンベロープアドレスでない場合、書き換えを実行することができなくなります。$B コントロールシーケンスを使うと、書き換えるアドレスがメッセージのヘッダまたは本文からのものでない場合、書き換えを実行することができなくなります。これらのシーケンスはこのような効果を得る目的でのみ使用され、書き換え規則テンプレート内の任意の場所に含めることができます。

アドレスは、方向によって分類することもできます。前方を探すアドレスは、To:、Cc:、Resent-to:、または宛先を参照する他のヘッダ行またはエンベロープ行に関して生じるアドレスです。また、後方を探すアドレスは、From:、Sender:、または Resent-From: といったソースを参照するものです。$F コントロールシーケンスを使うと、前方を探すアドレスである場合に書き換え規則が適用されます。$R コントロールシーケンスを使うと、後方を探すアドレスである場合に書き換え規則が適用されます。

ホスト名の位置に固有の書き換え ($A、$P、$S、$X)

アドレス内のホスト名の位置に基づいて適用されるような規則を必要とする場合があります。アドレス内のホスト名は、以下の位置にくることが考えられます。

- ソースルート内
- 単価記号 (@) の右側
- ローカル部分のパーセント記号 (%) の右側
- ローカル部分の感嘆符 (!) の左側

通常ホスト名は、それがどこに位置するかに関係なく、同じように処理されます。ただし、特別な処理を必要とする場合もあります。

アドレス内のホスト名の位置に基づいてマッチング動作を制御するには、以下の 4 つのコントロールシーケンスを使用できます。

- 規則をソースルートから抽出されたホストに一致させるには、$S を使用します。
- 規則を単価記号 @ の右側にあるホストに一致させるには、$A を使用します。
- 規則を % 記号の右側にあるホストに一致させるには、$P を使用します。
- 規則を 感嘆符 (!) の左側にあるホストに一致させるには、$X を使用します。

ホスト名が指定した位置にない場合は、規則の適用が失敗に終わります。これらのシーケンスは、1 つの書き換え規則内で組み合わせることもできます。たとえば、$S と $A を指定すると、規則はソースルート内のホスト名または単価記号 @ の右側にあるホスト名のいずれかに一致します。これらのシーケンスをすべて指定したのと、どれも指定しないのとは同じことです。すなわち、規則はホスト名の位置に関係なく一致します。

現在のタグ値の変更 ($T)

現在の書き換え規則タグを変更するには、$T コントロールシーケンスを使用します。書き換え規則タグはすべての書き換え規則パターンの先頭に付けられ、その後、設定ファイルやドメインデータベースで書き換え規則パターンの検索が行われます。$T の直後から単価記号 @、パーセント記号 %、$N、$M、$Q、$C、$T、または $? までの間のテキストが新しいタグとして扱われます。

タグは、特定のコンポーネントが検出されたときにアドレスの特性全体が変わるような、特殊なアドレス形式を処理する場合に便利です。たとえば、internet という特別なホスト名が見つかったときに、そのホスト名をアドレスから削除し、削除後のアドレスを強制的に TCP-DAEMON チャネルにマッチングするとします。

これは、以下のような規則を使って実行できます (ローカルホストの正式な名前を localhost とします)。

```
internet                $S$U@localhost$Tmtcp-force|

mtcp-force|.            $U%$H@TCP-DAEMON
```

最初の規則は、ソースルート内で internet という特別なホスト名が見つかった場合、そのホスト名に一致します。その後、ローカルチャネルと internet とのマッチングが行われ、アドレスから internet が削除されます。そして、書き換えタグが設定されます。書き換えプロセスは続けられますが、タグに対して通常の規則が一致することはありません。最後に、デフォルトの規則がタグとともに試され、2 番目の規則に移ります。この規則では、他の条件に関係なく、アドレスが強制的に TCP-DAEMON チャネルに対してマッチングされます。

書き換えに関連するエラーメッセージの制御 ($?)

MTA には、書き換えとチャネルの照合に失敗したときに表示されるデフォルトのエラーメッセージがあります。これらのメッセージは、特定の条件下で変更することができます。たとえば、誰かが Ethernet ルータボックスにメールを送信しようとした場合などは、「不正なホスト / ドメインが指定されています」というより「ルータがメールを受け入れられません」というメッセージを表示した方がより適切です。

特殊なコントロールシーケンスを使って、規則の適用に失敗した場合に印刷されるエラーメッセージを変更することができます。エラーメッセージを指定するには、$? シーケンスを使用します。$? の直後から単価記号 @、% 記号、$N、$M、$Q、$C、$T、または $? までの間のテキストがエラーメッセージのテキストとして扱われます。このエラーメッセージは、書き換えの結果がどのチャネルにも一致しなかった場合に印刷されます。エラーメッセージの設定は記憶され、書き換えプロセスを通じて有効となります。

$? を含む規則も他の規則と同じように動作します。特別なケースとして、$? だけを含む規則には注意してください。この場合、アドレスのメールボックスまたはホスト部分は変更されずに書き換えプロセスが終了し、ホストがチャネルテーブル内で検索されます。この検索は失敗に終り、その結果としてエラーメッセージが返されます。

たとえば、MTA 設定ファイル内に、次に示すような最終的な書き換え規則があるとします。

```
. $?Unrecognized address; contact postmaster@siroe.com
```

この例で、認識されないホスト / ドメイン仕様は、その失敗のプロセスにおいて、「Unrecognized address; contact postmaster@siroe.com」というエラーメッセージを生成します。

多数の書き換え規則を扱う

MTA は常に imta.cnf ファイルからすべての書き換え規則を読み取り、メモリ内のハッシュテーブルにそれらの規則を保存します。コンパイルした設定を使用すると、情報が必要になるたびに設定ファイルを読み取るという作業を省くことができます。この場合でも、メモリ内にすべての書き込み規則を保存するためにハッシュテーブルが使われます。この方法は、書き換え規則があまり多くない場合に適しています。サイトによっては 10,000 個以上の書き換え規則が必要になる場合もあります。このような場合には、かなり多くのメモリを費やさなければなりません。

MTA では、補助的なインデックス付きデータファイルに多数の書き換え規則を保存するオプションの機能を使って、この問題を解決することができます。通常の設定ファイルが読み取られるたびに、MTA はドメインデータベースがあるかどうかを調べます。データベースがある場合は、設定ファイルの規則が照合に失敗するたびにそのデータベースが開かれ、その内容が調べられます。ドメインデータベースが調べられるのは、指定された規則が設定ファイル内に見つからなかったときだけです。そのため、規則はいつでも設定ファイルに追加することができ、それによってデータベース内の規則が無効になります。特に設定を変更しない限り、ドメインデータベースは、ホストドメインに関連する書き換え規則を保存するために使用されます。IMTA_DOMAIN_DATABASE 属性は imta_tailor ファイルに保存されています。このデータベースのデフォルトの場所は *サーバ - インスタンス* /imta/db/domaindb.db です。

注 このファイルは手作業で編集しないでください。Directory Server でホストドメインが Directory Server で作成されると、dirsync プロセスが既存のドメインデータベースを上書きします。そのため、カスタム編集した内容は失われてしまいます。

書き換え規則をテストする

書き換え規則をテストするには imsimta test -rewrite コマンドを使用します。-noimage 修飾子を使うと、新しい設定をコンパイルする前に、設定ファイルに加えた変更内容をテストすることができます。

このユーティリティと -debug 修飾子を使って少数のアドレスを書き換えると便利かもしれません。この場合、ステップバイステップ形式でアドレスの書き換えが行われます。たとえば、以下のコマンドを実行します。

```
% imsimta test -rewrite -debug joe@siroe.com
```

imsimta test -rewrite ユーティリティの詳細については、『Messaging Server リファレンスマニュアル』を参照してください。

書き換え規則の例

以下に、書き換え規則の例とそれらの規則によってサンプルアドレスがどのうように書き換えられるかを示します。

SC.CS.SIROE.EDU システムの設定ファイルに、図 7-2 に示す書き換え規則が含まれているとします。

図 7-2　　書き換え規則の例

```
sc                      $U@sc.cs.siroe.edu
sc1                     $U@sc1.cs.siroe.edu
sc2                     $U@sc2.cs.siroe.edu
*                       $U%$&0.cs.siroe.edu
*.cs                    $U%$&0.cs.siroe.edu
*.cs.siroe              $U%$&0.cs.siroe.edu
*.cs.siroe.edu          $U%$&0.cs.siroe.edu@ds.adm.siroe.edu
sc.cs.siroe.edu         $U@$D
sc1.cs.siroe.edu        $U@$D
sc2.cs.siroe.edu        $U@$D
sd.cs.siroe.edu         $U@sd.cs.siroe.edu
.siroe.edu              $U%$H.siroe.edu@cds.adm.siroe.edu
.edu                    $U@$H$D@gate.adm.siroe.edu
[]                      $U@[$L]@gate.adm.siroe.edu
```

表 7-7 に、サンプルアドレスとそれらの書き換え結果およびルートを示します。

表 7-7　　サンプルアドレスと書き換え結果

最初のアドレス	書き換え後	ルート
user@sc	user@sc.cs.siroe.edu	sc.cs.siroe.edu
user@sc1	user@sc1.cs.siroe.edu	sc1.cs.siroe.edu
user@sc2	user@sc2.cs.siroe.edu	sc2.cs.siroe.edu
user@sc.cs	user@sc.cs.siroe.edu	sc.cs.siroe.edu
user@sc1.cs	user@sc1.cs.siroe.edu	sc1.cs.siroe.edu
user@sc2.cs	user@sc2.cs.siroe.edu	sc2.cs.siroe.edu
user@sc.cs.siroe	user@sc.cs.siroe.edu	sc.cs.siroe.edu
user@sc1.cs.siroe	user@sc1.cs.siroe.edu	sc1.cs.siroe.edu
user@sc2.cs.siroe	user@sc2.cs.siroe.edu	sc2.cs.siroe.edu
user@sc.cs.siroe.edu	user@sc.cs.siroe.edu	sc.cs.siroe.edu
user@sc1.cs.siroe.edu	user@sc1.cs.siroe.edu	sc1.cs.siroe.edu

表 7-7　サンプルアドレスと書き換え結果（続き）

最初のアドレス	書き換え後	ルート
user@sc2.cs.siroe.edu	user@sc2.cs.siroe.edu	sc2.cs.siroe.edu
user@sd.cs.siroe.edu	user@sd.cs.siroe.edu	sd.cs.siroe.edu
user@aa.cs.siroe.edu	user@aa.cs.siroe.edu	ds.adm.siroe.edu
user@a.eng.siroe.edu	user@a.eng.siroe.edu	cds.adm.siroe.edu
user@a.cs.sesta.edu	user@a.cs.sesta.edu	gate.adm.siroe.edu —route inserted
user@b.cs.sesta.edu	user@b.cs.sesta.edu	gate.adm.siroe.edu —route inserted
user@[1.2.3.4]	user@[1.2.3.4]	gate.adm.siroe.edu —route inserted

基本的に、これらの書き換え規則の内容は次のとおりです : ホスト名が短形式の名前 (sc、sc1、または sc2) の 1 つである場合、またはフルネーム (sc.cs.siroe.edu など) の 1 つである場合は、その名前をフルネームに展開し、私たちに送る。cs.cmu.edu を 1 つの部分からなる短形式の名前に追加し、もう一度試行する。.cs が後に続く 1 つの部分を .cs.siroe.edu が後に続く 1 つの部分に変換し、もう一度試行する。また、.cs.siroe も .cs.siroe.edu に変換し、もう一度試行する。

名前が sd.cs.siroe.edu (私たちが直接接続するシステム) である場合は、それを書き換え、そこに送る。ホスト名が .cs.siroe.edu サブドメイン内の他のものである場合は、それを ds.cs.siroe.edu (.cs.siroe.edu サブドメインのゲートウェイ) に送る。ホスト名が .siroe.edu サブドメイン内の他のものである場合は、それを cds.adm.siroe.edu (.siroe.edu サブドメインのゲートウェイ) に送る。ホスト名が .edu 最上位レベル内の他のものである場合は、それを gate.adm.siroe.edu (メッセージを適切な宛先に送ることが可能) に送る。ドメインリテラルが使用されている場合は、それも gate.adm.siroe.edu に送る。

上記の例のように、書き換え規則によってアドレスのユーザ名 (またはメールボックス) 部分が変更されることはほとんどありません。アドレスのユーザ名部分を変更する機能は、MTA が RFC 822 に準拠しないメールソフトウェア (ホスト / ドメイン仕様をアドレスのユーザ名部分に詰め込む必要があるメールソフトウェア) へのインターフェースとして使われる場合に使用されます。この機能を使用する際には、十分な配慮が必要です。

第 8 章

チャネル定義を設定する

この章では、MTA 設定ファイル imta.cnf でチャネル定義を設定する方法について説明します。

この章を読む前に第 6 章 「MTA サービスと設定について」の内容を理解しておくことをお勧めします。imta.cnf ファイルの書き換え規則の設定については、第 7 章 「書き換え規則を設定する」を参照してください。

この章には、以下の項目があります。

- チャネルの構造
- 既定のチャネル
- SMTP チャネルを設定する
- メッセージの処理と配信を設定する
- Postmaster 宛てのメッセージを設定する
- チャネルオプションを設定する
- チャネルのデフォルトを設定する
- チャネルのログを設定する
- チャネルのデバッグを設定する
- プログラム配信を設定する
- hold チャネルを使用する
- conversion チャネルを使用する
- 変換を理解する

注　imta.cnf ファイル内のチャネルの定義を変更する場合は、imsimta start コマンドを使って起動するときに設定データを 1 回だけ読み込むようなプログラムまたはチャネルを起動する必要があります (例、SMTP サーバ)。コンパイルした設定を使用する場合は、設定を再コンパイルした後にプログラムを再起動する必要があります。

設定情報のコンパイルおよびプログラムの起動については、『Messaging Server リファレンスマニュアル』を参照してください。

チャネルの構造

チャネル定義は MTA 設定ファイルの後半部分、すなわち書き換え規則の後に記述されています。ファイル内の最初の空白行が書き換え規則の終了およびチャネル定義の開始を示しています。

チャネル定義には、チャネル名、そのチャネルの設定を定義するキーワードリスト (オプション)、および、および特有のチャネルタグ (書き換え規則で使用される、メッセージをチャネルにルーティングするためのタグ) がこの順番で含まれています。それぞれのチャネル定義の間は 1 行の空白行によって区切られています。そのため、1 つのチャネル定義の中にコメント行を含めることはできますが、空白行を含めることはできません。

```
[ 空白行 ]
! チャネル定義の例
チャネル名  キーワード1  キーワード2
チャネル - タグ
[ 空白行 ]
```

チャネル定義は、まとめてチャネル ホストテーブルと呼ばれます。また、チャネルホストテーブルに含まれる個々のチャネル定義は、チャネルブロックと呼ばれます。図 8-1 に、3 つのチャネルブロックを含むチャネルホストテーブルの一例を示します。

図 8-1 簡単な設定ファイルの例 - チャネル定義

```
! test.cnf - 設定ファイルの例。
!
! 書き換え規則
      .
      .
      .

! チャネル定義開始
! 第 1 チャネルブロック
l
local-host

! 第 2 チャネルブロック
a_channel defragment charset7 usascii
a-daemon

! 第 3 チャネルブロック
b_channel noreverse notices 1 2 3
b-daemon
```

チャネルホストテーブルは、Messaging Server が使用できるチャネルおよび各チャネルに関連付けられたシステムを定義するものです。

UNIX システムでは、第 1 チャネルブロックは常にローカルチャネル `l` の説明です (ただし、`defaults` チャネルは例外で、ローカルチャネルの前にくることがあります)。ローカルチャネルは、ルーティングの決定および UNIX メールツールを使用して送られたメールの配信に使用されます。

既定のチャネル

チャネルによっては iPlanet Messaging Server をインストールした時点ですでに定義されているものもあります。表 8-1 は、これらの既定チャネルのリストです。

表 8-1　既定のチャネル

チャネル	説明
l	**UNIX のみ。**ルーティングの決定および UNIX メールツールを使用したメールの送信に使われます。
ims-ms	メールをローカルストアに配信します。
native	**UNIX のみ。**メールを /var/mail に配信します (Messaging Server は /var/mail へのアクセスをサポートしていません。ユーザが /var/mail ストアのメールにアクセスするには、UNIX ツールを使う必要があります)。
pipe	サイト提供のプログラムやスクリプトを介してメールを配信するために使用されます。このパイプチャネルによって実行されるコマンドは、管理者が imsimta プログラムのインターフェースを通じて管理します。詳細については、169 ページの「プログラム配信を設定する」を参照してください。
tcp_local tcp_intranet tcp_auth tcp_submit tcp_tas	TCP/IP の上位プロトコルとして SMTP を実装します。マルチスレッド TCP SMTP チャネルには、ディスパッチャ制御下のマルチスレッド SMTP サーバが含まれます。送信された SMTP メールは、必要に応じてジョブコントローラの制御下で動作し、チャネル プログラム tcp_smtp_client によって処理されます。 tcp_local はリモート SMTP ホストからのメールを受信します。メールを送信する場合は、smarhost/ ファイアウォール設定が使われているかどうかによって、直接リモート SMTP ホストに送るか、またはスマートホストファイアウォールシステムに送ります。 tcp_intranet はイントラネット内のメールを送受信します。 tcp_auth は tcp_local のスイッチチャネルとして使用されます。認証されたユーザは、リレーブロックの制約を回避するため tcp_auth チャネルに移されます。 tcp_submit は、送信されたメッセージ (通常の場合はユーザエージェントからのメッセージ) を予約されている送信ポート 587 で受け入れます (RFC 2476 を参照)。 tcp_tas は Unified Messaging を使用するサイト用の特殊なチャネルです。
reprocess process	遅延メッセージのオフライン処理に使用されるチャネルです。通常、reprocess チャネルはソースまたは宛先チャネルとして公にされません。process チャネルは、他の MTA チャネルと同様、公にされます。
defragment	断片化された MIME メッセージの修復方法を提供します。
conversion	MTA を通じて配信されるメッセージを本文部分ごとに変換します。

表 8-1　既定のチャネル（続き）

チャネル	説明
bitbucket	破棄するメッセージに使用されます。
inactive/deleted	ディレクトリ内でのステータスが非アクティブまたは削除済みになっているユーザへのメッセージの処理に使用されます。通常、受信したメッセージを差出人に送り返し、カスタム返送メッセージを送ります。
hold	ユーザへのメッセージを保留します。たとえば、ユーザがあるメールサーバから別のサーバに移行された場合などに便利です。
autoreply	自動返信および vacation 通知のリクエストを処理するために使用されます。

SMTP チャネルを設定する

インストールの種類によっては、Messaging Server のインストール時に数種の SMTP チャネルが提供されます (tcp_local、tcp_intranet、tcp_submit、tcp_auth、および tcp_tas)。また、これらのチャネルの定義を変更したり、新規チャネルを作成することも可能です。

この節には、以下の項があります。

- SMTP コマンドとプロトコルのサポート
- TCP/IP 接続と DNS 検索のサポート
- SMTP 認証と SASL
- TLS (Transport Layer Security)
- チャネル動作のタイプ

SMTP コマンドとプロトコルのサポート

SMTP チャネルが EHLO、ETRN、VRFY などの SMTP コマンドをサポートするように指定することができます。また、チャネルが DNS ドメイン認証をサポートするかどうかや、どの文字を改行記号として受け入れるかなどを指定することも可能です。この項では、以下の内容について説明します。

- チャネルプロトコル選択と改行記号
- EHLO コマンドのサポート
- ETRN コマンドのサポート
- VRFY コマンドのサポート
- DNS ドメイン確認
- 文字セットのラベルと 8 ビットデータ
- プロトコルストリーミング

表 8-2 に、この項で説明されているキーワードのリストを示します。

表 8-2　　SMTP コマンドとプロトコルに関連するキーワード

チャネルキーワード	説明
プロトコル選択と改行記号	**チャネルが SMTP プロトコルをサポートするかどうか、および改行記号として受け入れる文字シーケンスを指定**
smtp	SMTP プロトコルをサポートします。smtp はすべての SMTP チャネルに必須のキーワードです (このキーワードは smtp_crorlf と同じものです)。
nosmtp	SMTP プロトコルをサポートしません。デフォルト設定では、このキーワードが使用されています。
smtp_cr	キャリッジリターン (CR) で改行し、ラインフィード (LF) が後に続いていない行を受け入れます。
smtp_crlf	キャリッジリターン (CR) + ラインフィード (LF) シーケンスで改行している行だけを受け入れます。
smtp_lf	キャリッジリターン (CR) がなく、ラインフィード (LF) だけで改行している行を受け入れます。
smtp_crorlf	キャリッジリターン (CR) のみ、ラインフィード (LF) のみ、またはその両方 (CRLF) で改行しているすべての行を受け入れます。
EHLO キーワード	**チャネルによる EHLO コマンドの処理方法を指定**
ehlo	最初から接続に SMTP EHLO コマンドを使用します。
checkehlo	応答の見出しを確認して、EHLO と HELO のどちらか使用するかを決定します。
noehlo	EHLO コマンドを使用しません。
ETRN キーワード	**チャネルによる ETRN コマンド (キュー処理のリクエスト) の処理方法を指定**
allowetrn	ETRN コマンドに従います。
blocketrn	ETRN コマンドをブロックします。
domainetrn	ドメインを指定している ETRN コマンドのみに従います。
silentetrn	チャネル情報をエコーせずに ETRN コマンドに従います。
sendetrn	ETRN コマンドを発行します。
nosendetrn	ETRN コマンドを発行しません。
VRFY キーワード	**チャネルによる VRFY コマンドの処理方法を指定**
domainvrfy	完全なアドレスを使用して VRFY コマンドを発行します。
localvrfy	ローカルアドレスを使用して VRFY コマンドを発行します。

表 8-2　SMTP コマンドとプロトコルに関連するキーワード（続き）

チャネルキーワード	説明
novrfy	VRFY コマンドを発行しません。
vrfyallow	VRFY コマンドに対して有益な情報を含む応答を返します。
vrfydefault	チャネルの HIDE_VERIFY オプションの設定に従い、VRFY コマンドに対してデフォルトの応答を返します。
vrfyhide	SMTP VRFY コマンドに対してあいまいな応答を返します。
DNS ドメイン確認	**チャネルが DNS ドメイン確認を行うかどうかを指定**
mailfromdnsverify	MAIL FROM: コマンドに使用されているドメインが DNS に存在するかどうかを確認します。
nomailfromdnsverify	MAIL FROM: コマンドに使用されているドメインが DNS に存在するかどうかを確認しません。
文字セットと 8 ビットデータ	**チャネルによる 8 ビットデータの処理方法を指定** **注意：これらのキーワードは主に SMTP チャネルで使用されますが、その他のチャネルで使用されることもあります。**
charset7	7 ビットのテキストメッセージに関連付けるデフォルトの文字セット。
charset8	8 ビットのテキストメッセージに関連付けるデフォルトの文字セット。
charsetesc	エスケープ文字を含む 7 ビットのテキストメッセージに関連付けるデフォルトの文字セット。
eightbit	チャネルが 8 ビット文字をサポートするように指定します。
eightnegotiate	チャネルが 8 ビット伝送の使用のネゴシエーションを行うように指定します (可能な場合)。
eightstrict	チャネルがネゴシエーションが行われていない 8 ビットデータを含むメッセージを拒否するように指定します。
sevenbit	チャネルが 8 ビット文字をサポートしないように指定します。8 ビット文字はエンコードされなければなりません。
プロトコルストリーミング streaming	**チャネルが使用するプロトコルストリーミングの程度を指定**

チャネルプロトコル選択と改行記号

smtp および nosmtp キーワードは、チャネルが SMTP プロトコルをサポートするかどうかを指定するものです。smtp (またはその変形) は、すべての SMTP チャネルに対して必須のキーワードです。

smtp_crlf、smtp_cr、smtp_crorlf、および smtp_lf は、MTA が改行記号として受け入れる文字シーケンスの種類を指定するために、SMTP チャネルに対して使用されます。smtp_crlf キーワードを使用すると、キャリッジリターン (CR) + ラインフィーダ (LF) のシーケンスのみが改行記号として認識されます。smtp_lf または smtp キーワードを使用すると、LF のみのターミネータが受け入れられます。また、smtp_cr を使用すると、CR のみのターミネータが受け入れられます。これらのオプションは、受信データにしか適用されません。

SMTP では 改行記号として CRLF が要求されるため、MTA は常に CRLF シーケンスを作成します。各種の smtp キーワードは、MTA がその他の改行記号を受け入れるかどうかを指定するだけのものです。たとえば、MTA が規定通りの SMTP メッセージだけを受け入れ、非標準的な改行記号を含むメッセージを拒否するように指定するには、stmp_crlf を使います。

EHLO コマンドのサポート

SMTP プロトコルは、その他のコマンドの使用のネゴシエーションを行うことができるよう拡張されています (RFC 1869)。これを利用するには、RFC 821 規定の HELO コマンドの代わりに、新しい EHLO コマンドを使用します。EHLO コマンドを受け取った 拡張 SMTP サーバはサポートする拡張内容のリストを返します。拡張をサポートしないサーバにこのコマンドを発行した場合は、不明なコマンドエラーのメッセージが返され、エラーメッセージを受け取ったクライアントは折り返し HELO コマンドを送ります。

このフォールバックは、サーバが拡張されているかどうかに関わらず機能します。ただし、サーバが RFC 821 に準拠した SMTP を実装していない場合は、問題が発生する可能性があります。特に、認識できないコマンドを受け取ると接続を遮断してしまうサーバもあります。

EHLO コマンドを受け取ったサーバが接続を遮断した場合、SMTP クライアントは HELO コマンドを発行して再接続を試みます。ただし、EHLO を受け取ったリモートサーバが接続を遮断するだけでなく、その他の問題を併発する場合は、クライアントが再接続できないこともあります。

ehlo、noehlo、および checkehlo チャネルキーワードは、このような情況に対処するためのキーワードです。ehlo キーワードは、MTA が最初の接続試行に EHLO コマンドを使用するように指定します。noehlo キーワードは EHLO コマンドの使用をすべて無効にします。checkehlo キーワードは、リモート SMTP サーバによって返された見出しに「ESMTP」文字列が含まれているかどうかを確認し、含まれている場合には EHLO を使用し、含まれていない場合には HELO を使用するように指示します。デフォルトでは、最初の接続試行に対する応答の見出しに「fire away」文字列が含まれている場合は HELO を使用し、それ以外の場合は EHLO を使用するように設定されています。このデフォルト設定は ehlo キーワードと checkehlo キーワードの中間的な効果を得るものであり、この設定を指定するためのキーワードは存在しないことに注意してください。

ETRN コマンドのサポート

RFC 1985 で規定されている ETRN コマンドは SMTP サービスの拡張を可能にするものです。このコマンドによって SMTP サーバがクライアントとの通信に基づいてメッセージキューの処理を開始し、指定のホストにメッセージを配信できるようになります。

SMTP クライアントは ETRN を使用して、自分宛てのメッセージキューの処理を開始するようリモート SMTP サーバにリクエストできます。つまり、ETRN は SMTP クライアントがメッセージを受信できるようにリモート SMTP システムを「ポーリング」するためのコマンドです。これは、一過性の接続しか持たないシステム間 (たとえば、ダイアルアップ以外の方法ではインターネットに接続できないサイト用に二次的な MX ホストとして設定されているサイトなど) に対して有用です。このコマンドを有効にすることで、ダイアルアップ接続を行うリモートサーバもメール配信のリクエストを送ることができるようになります。

SMTP クライアントは、SMTP ETRN コマンド行でメッセージの送信先となるシステム名 (通常、その SMTP クライアントシステムの名前) を指定します。リモート SMTP サーバが ETRN コマンドをサポートする場合、サーバは指定のシステムに別途接続し、そのシステム宛てのメッセージの配信を開始するためのプロセスがトリガされます。

ETRN コマンドに応答する

allowetrn、blocketrn、domainetrn、および silentetrn キーワードは、SMTP クライアントが ETRN コマンドを発行して MTA キュー内のメッセージを配信するようリクエストした際に、MTA がどのように対応するかを指定するキーワードです。

デフォルト設定では allowetrn キーワードが有効になっているため、MTA はすべての ETRN コマンドに従います。MTA が ETRN コマンドを拒否するように指定するには、チャネル定義に blocketrn キーワードを使用します。

MTA がすべての ETRN コマンドに従い、かつドメインによって確認されたチャネル名をエコーしないように指定するには、silentetrn キーワードを使用します。ETRN コマンドがドメインを指定している場合にのみ MTA がそのコマンドに従うように指定するには、domainetrn キーワードを使用します。また、このキーワードを使用すると、MTA はドメインによって確認されたチャネル名をエコーしません。

ETRN コマンドを発行する

sendetrn および nosendetrn チャネルキーワードは、MTA が SMTP 接続開始時に ETRN コマンドを送るかどうかを指定するキーワードです。デフォルト設定では nosendetrn が有効になっているため、MTA は ETRN コマンドを送りません。リモート SMTP サーバが ETRN コマンドをサポートする場合にのみ MTA が ETRN を発行するように指定するには、sendetrn キーワードを使用します。sendetrn キーワードの後ろには、メッセージの配信先となるシステムの名前を記述する必要があります。

VRFY コマンドのサポート

VRFY コマンドは、SMTP クライアントが 特定のユーザ名に宛てられたメールが存在するかどうかを確認するよう SMTP サーバにリクエストするためのコマンドです。VRFY コマンドは、RFC 821 で規定されています。

サーバは、ユーザがローカルであるかどうか、メールが転送されるかどうかなどの情報を返します。250 という応答はユーザ名がローカルであることを意味し、251 はローカルではないがメッセージの転送は可能であることを意味します。サーバの応答には、メールボックス名が含まれます。

VRFY コマンドを発行する

通常、SMTP ダイアログの一部として VRFY コマンドを発行する必要はありません。SMTP RCPT TO コマンドに VRFY コマンドと同じ効果があり、必要に応じて適切なエラーを返すためです。ただし、サーバによっては、RCPT TO コマンドを受け取った場合はコマンドが指定するアドレスをいったん受理してから返送し、VRFY コマンドを受け取った場合はより広範なチェックを実行するものもあります。

デフォルト設定では novrfy キーワードが有効になっているため、MTA は VRFY コマンドを発行しません。

MTA が SMTP VRFY コマンドを発行するように指定するには、チャネル定義に domainvrfy または localvrfy キーワードを挿入します。domainvrfy キーワードを使用すると、完全なアドレス (user@host) を引数とする VRFY コマンドが発行されます。localvrfy キーワードを使用すると、アドレスのローカル部分 (user) だけを引数とする VRFY コマンドが発行されます。

VRFY コマンドに応答する

vrfyallow、vrfydefault、および vrfyhide キーワードは、SMTP クライアントから SMTP VRFY コマンドを受け取った SMTP サーバがどのように対応するかを指定するキーワードです。

MTA が詳細な情報を含む応答を返すように指定するには、vrfyallow キーワードを使用します。HIDE_VERIFY=1 チャネルオプションが指定されていない限り MTA が詳細な情報を含む応答を返すよう指定するには、vrfydefault キーワードを使用します。MTA があいまいな応答を返すよう指定するには、vrfyhide キーワードを使用します。これらのキーワードを使用すると、VRFY コマンドに対する応答をチャネルごとに制御できます。一方、HIDE_VERIFY オプションは、1 つの SMTP サーバを介して処理されるすべての受信 TCP/IP チャネルに適用されます。

DNS ドメイン確認

mailfromdnsverify を受信 TCP/IP チャネルに対して設定すると、MTA は SMTP MAIL FROM コマンドで指定されているドメインのエントリが DNS に存在するかどうかを確認し、エントリが存在しない場合にはメッセージを拒否します。デフォルト設定では nomailfromdnsverify が有効になっているため、この確認は行われません。ただし、返信用アドレスに対して DNS 確認を行うと、許可されるべきメッセージも拒否されてしまう可能性があることに注意してください (たとえば、正規のサイトでもそのドメイン名がまだ登録されていない場合や、DNS が適切に動作していない場合など)。これは、RFC 1123 の「Requirements for Internet Hosts (インターネットホストの必要条件)」で規定されている電子メール受信の心得に反する行為です。ただし、存在しないドメインから不特定多数宛てのメール (UBE) が送られる場合は、この確認を行った方がよい場合もあります。

文字セットのラベルと 8 ビットデータ

文字セットのラベル

charset7、charset8、および charsetesc チャネルキーワードは、文字セットのラベルが欠如しているメッセージヘッダに文字セット名を挿入するメカニズムをチャネルごとに提供するキーワードです。これらのキーワードを使用する場合は、単一の文字セット名を引数として指定する必要があります。文字セット名が正しいかどうかの確認は行われません。文字セットの変換は、MTA テーブルディレクトリ内の文字セット定義ファイル charsets.txt で定義されている文字セットに対してのみ可能であることに注意してください。できるだけこのファイルで定義されている名前を使用することをお勧めします。

メッセージに含まれるのが 7 ビットデータのみの場合は charset7 を、8 ビットデータが含まれる場合は charset8 を使用します。charsetesc は、メッセージに 7 ビットデータおよびエスケープ文字が含まれる場合に使用します。適切なキーワードが指定されていない場合は、Content-type: ヘッダ行に文字セット名が挿入されません。

これらの文字セット指定が既存のラベルより優先されることはありません。メッセージにすでに文字セットラベルが含まれている場合やメッセージがテキストでない場合、これらのキーワードは効果をもたらしません。

charsetesc キーワードは、特に日本語や韓国語の文字セットを使用し、エスケープ文字を含むラベルなしのメッセージを受信するチャネルに便利です。

8 ビットデータ

127 (10 進) 以上の序数値を持つ文字の使用は制限される場合があります。特に、SMTP サーバの中には、高ビットを切り捨てるために 8 ビット領域の文字を含むメッセージの文字化けの原因となるものもあります。

Messaging Server は、そのようなメッセージを自動的にエンコードし、8 ビットデータがメッセージに直接表示されないようにする機能を備えています。特定のチャネルのキューに入れられるすべてのメッセージにエンコードを適用するには、sevenbit キーワードを使用します。そのような制約がない場合は、eightbit を使用します。

リモート SMTP サーバが 8 ビットをサポートすると明示していない限り、SMTP プロトコルは 8 ビットを許可しません。ただし、拡張 SMTP などの場合は、8 ビット文字の転送が可能かどうかのネゴシエーションを行って決定することもあります。ネゴシエートが失敗した場合に備えて、eightnegotiate キーワードを使用し、チャネルがメッセージをエンコードするよう指定しておくことを強くお勧めします。デフォルト設定ではすべてのチャネルに対してこのキーワードが有効になっているため、ネゴシエーションをサポートしないチャネルは 8 ビットデータの転送が可能であるという仮定のもとに動作します。

Messaging Server がネゴシエーションされていない 8 ビットデータを含むメッセージをすべて拒否するように設定するには、eightstrict キーワードを使用します。

プロトコルストリーミング

メールプロトコルによっては、ストリーミングをサポートするものもあります。ストリーミングがサポートされている場合は、MTA が一度に複数のリクエストを発行し、それぞれに対する応答をバッチで受け取ることができます。`streaming` は、チャネルに関連付けられたプロトコルのストリーミングの程度を制御するキーワードです。このキーワードには整数値のパラメータが必要です。パラメータの解釈は、プロトコルによって異なります。

現時点で MTA がサポートしているのは SMTP チャネル上の試験的なストリーミングだけです。この機能は試験的なもので、将来のリリースで変更される可能性があります。

ストリーミング値の範囲は 0 から 3 までです。値が 0 の場合はストリーミングが指定されず、値が 1 の場合は RCPT TO コマンドグループがストリーミングされ、2 の場合は MAIL FROM/RCPT TO が、3 の場合は HELO/MAIL FROM/RCPT TO または RSET/MAIL FROM/RCPT TO がストリーミングされます。デフォルト値は 0 です。

SMTP 実装ソフトの中には、このストリーミングを必ずしも適切に処理できないものもあります。特に、sendmail は 1 以上のストリーミングレベルを処理できないと言われています。一方、iPlanet Messaging Server はすべてのストリーミングレベルに適切に対応しています。

TCP/IP 接続と DNS 検索のサポート

サーバによる TCP/IP 接続およびアドレス検索の処理方法を指定することができます。この項では、以下の内容について説明します。

- TCP/IP ポート番号とインターフェースアドレス
- チャネル接続情報のキャッシング
- DNS 検索
- IDENT 検索
- TCP/IP MX レコードのサポート
- ネームサーバ検索
- 最後のホスト
- メール受信用代替チャネル
- ターゲットホストの選択

表 8-3 に、この項で説明されている TCP/IP 接続および DNS 検索に関連するキーワードのリストを示します。

表 8-3　TCP/IP 接続と DNS 検索に関連するキーワード

チャネル キーワード	説明
ポート選択とインターフェースアドレス	**SMTP 接続のデフォルトポート番号およびインターフェースアドレスを指定**
port	SMTP 接続用のデフォルトポート番号を指定します。標準ポートは 25 です。
interfaceaddress	指定された TCP/IP インターフェースアドレスにバインドします。
キャッシュキーワード	**接続情報のキャッシュ方法を指定**
cacheeverything	すべての接続情報をキャッシュします。
cachefailures	接続失敗に関する情報だけをキャッシュします。
cachesuccesses	接続成功に関する情報だけをキャッシュします。
nocache	接続情報をキャッシュしません。
DNS 検索	**受信した SMTP 接続に対する DNS 検索の処理方法を指定**
forwardcheckdelete	リバース DNS 検索が実行された場合、返された名前をフォワード検索して IP 番号が最初のものに一致するかどうかを確認します。一致しなかった場合、名前は削除され、IP アドレスが使用されます。
forwardchecknone	リバース DNS 検索の後にフォワード検索を実行しません。
forwardchecktag	リバース検索が実行された場合、返された名前をフォワード検索して IP 番号が最初のものに一致するかどうかを確認し、一致しなければ名前に「*」を付けます。
IDENT 検索 / リバース DNS 検索	**受信した SMTP 接続に対する IDENT 検索および リバース DNS 検索の処理方法を指定**
identnone	IDENT 検索を実行せず、IP からホスト名への変換を実行し、Received: ヘッダにホスト名と IP アドレスを含めます。
identnonelimited	IDENT 検索を実行せず、IP からホスト名への変換を実行し (ただしチャネルの切り替えを行う際にはホスト名を使用しない)、Received: ヘッダにホスト名と IP アドレスを含めます。
identnonenumeric	IDENT 検索および IP からホスト名への変換を実行しません。
identnonesymbolic	IDENT 検索を実行せず、IP からホスト名への変換を実行し、Received: ヘッダにホスト名だけを含めます。
identtcp	受信した SMTP 接続に対して IDENT 検索を実行し、IP からホスト名への変換を実行し、Received: ヘッダにホスト名と IP アドレスを含めます。

表 8-3　TCP/IP 接続と DNS 検索に関連するキーワード（続き）

チャネル キーワード	説明
identtcplimited	受信した SMTP 接続に対して IDENT 検索を実行し、IP からホスト名への変換を実行し (ただしチャネルの切り替えを行う際にはホスト名を使用しない)、Received: ヘッダにホスト名と IP アドレスを含めます。
indenttcpnumeric	受信した SMTP 接続に対して IDENT 検索を実行し、IP からホスト名への変換を実行しません。
identtcpsymbolic	受信した SMTP 接続に対して IDENT 検索を実行し、IP からホスト名への変換を実行し、Received: ヘッダにホスト名だけを含めます。
MX レコードのサポートと TCP/IP ネームサーバ	**チャネルが MX レコード検索をサポートするかどうか、およびサポートする場合にはどのように処理するかを指定**
mx	TCP/IP ネットワークおよびソフトウェアが MX レコード検索をサポートするように指定します。
nomx	TCP/IP ネットワークが MX 検索をサポートしないように指定します。
defaultmx	ネットワークから MX 検索を実行するかどうかをチャネルが決定するように指定します。
randommx	MX 検索を実行し、返されたエントリを同等の優先順位でランダム化します。
nonrandomemx	MX 検索を実行しますが、返されたエントリを同等の優先順位でランダム化しません。
nameservers	TCP/IP スタックが選択したネームサーバの代わりに照合するネームサーバのリストを指定します。nameservers には、空白文字で区切られたネームサーバの IP アドレスのリストが必要です。
defaultnameservers	TCP/IP スタックが選択したネームサーバを照合します。
lastresort	最後のホストを指定します。
switch キーワード	**メールを受信する代替チャネルのリストを制御**
allowswitchchannel	switchchannel チャネルからこのチャネルへの切り替えを許可します。
noswitchchannel	サーバチャネルの使用を継続し、送信元ホストに関連付けられているチャネルに切り替えをしません。また、他のチャネルからこのチャネルへの切り替えを許可しません。
switchchannel	サーバチャネルから送信元のホストに関連付けられたチャネルに切り替えます。
tlsswitchchannel	TLS のネゴシエートが成功した場合に、他のチャネルに切り替えます。
saslswitchchannel	SASL 認証が成功した場合に他のチャネルへ切り替えます。
ターゲットホストの選択とメッセージコピーの保存	**ターゲットホストシステムとメッセージコピーの保存方法を指定**

表 8-3　TCP/IP 接続と DNS 検索に関連するキーワード（続き）

チャネル キーワード	説明
daemon	エンベロープアドレスに関わらず特定のホストシステムに接続します。
single	チャネル上の各宛先アドレス用にメッセージのコピーが 1 つずつ作成されるように指定します。
single_sys	各宛先システム用にメッセージのコピーを 1 つずつ作成します。

TCP/IP ポート番号とインターフェースアドレス

通常、TCP/IP 上に実装された SMTP チャネルは、ポート 25 に接続してメッセージを送信します。SMTP 実装 TCP/IP チャネルがその他のポートを使用するように指定するには、port キーワードを使用します。このキーワードは、PORT ディスパッチャオプション (SMTP 接続を受け入れるために MTA がリッスンするポートを制御するオプション) を補足するものです。

interfaceaddress キーワードは、TCP/IP チャネルが送信時にソースアドレスとしてバインドするアドレスを制御します。つまり、複数のインターフェースアドレスが存在するシステム上で、MTA が SMTP メッセージを送信する際にどのアドレスをソース IP アドレスとして使用するかを制御するキーワードです。このキーワードは、INTERFACE_ADDRESS ディスパッチャオプション (接続およびメッセージを受け入れるために TCP/IP チャネルがリッスンするインターフェースアドレスを制御するオプション) を補足するものです。

チャネル接続情報のキャッシング

SMTP プロトコルを使用するチャネルは、過去の接続試行の履歴を含むキャッシュを管理しています。このキャッシュは、アクセスできないホストに繰り返し接続しようとして時間を浪費し、他のメッセージの配信が遅延されることを回避するために使用されます。このキャッシュは送信 SMTP チャネルが動作中の間のみ維持され、動作が終了するたびに削除されます。

通常、キャッシュには、成功した接続試行と失敗した接続試行の両方に関する情報が記録されます (成功した試行は、その後失敗する試行を相殺するために記録されます。すなわち、一度接続に成功したホストがその後失敗しても、初めての試行する接続や以前失敗した接続ほど次の接続試行が遅れることはありません)。

ただし、MTA が使用するキャッシング方法がすべての情況において適切であるとは限りません。そこで、チャネルキーワードを使用して MTA キャッシュを調整します。

cacheeverything キーワードは、すべての形式のキャッシングを有効にします。デフォルト設定ではこのキーワードが使用されます。nocache キーワードは、すべてのキャッシングを無効にします。

cachefailures キーワードは、失敗した接続のキャッシングだけを有効にします。このキーワードを使用すると、次の試行は cacheeverything を使用した場合より多くの制約を受けることになります。cachesuccesses は成功した接続だけをキャッシュします。このキーワードは、SMTP チャネルに対する nocache キーワードと同等のものです。

DNS 検索

forwardchecknone、forwardchecktag、および forwardcheckdelete チャネルキーワードは、リバース DNS 検索の影響を修正します。これらのキーワードは、MTA が リバース DNS 検索によって検出された IP 名のフォワード検索を実行するかどうか、および実行する場合にはフォワード検索の結果が最初の IP 番号と一致しなかった場合にどのように対処するかを制御します。

デフォルト設定では forwardchecknone キーワードが有効になっているため、フォワード検索は実行されません。forwardchecktag キーワードは、リバース検索が行われる度にフォワード検索を実行し、検出された番号が最初の接続の番号と一致しない場合は IP 名にアスタリスク (*) を付けるように指定します。forwardcheckdelete キーワードは、リバース検索が行われる度にフォワード検索を実行し、その結果が最初の接続の IP アドレスと一致しなかった場合はリバース検索によって検出された名前を無視 (削除) して最初の IP アドレスを使用するように指定します。

注　複数の IP アドレスに「一般的な」IP 名が使用されているサイトの場合、フォワード検索の結果が最初の IP アドレスと一致しないのは比較的頻繁に見られる現象です。

IDENT 検索

IDENT キーワードは、MTA が IDENT プロトコルを使用して接続や検索を処理する方法を制御します。IDENT プロトコルは、RFC 1413 で規定されています。

identtcp、identtcpsymbolic、および identtcpnumeric キーワードは、MTA が接続や検索に IDENT プロトコルを使用するように指定するものです。IDENT プロトコルを使用して得た情報 (通常、SMTP 接続を使用しているユーザの ID) は、以下のようにメッセージの Received: ヘッダに挿入されます。

- identtcp は 受信した IP 番号に呼応するホスト名 (リバース DNS 検索で検出された名前) および IP 番号そのものを挿入します。
- identtcpsymbolic は、受信した IP 番号に呼応するホスト名 (リバース DNS 検索で検出された名前) を挿入します。ただし、IP 番号は Received: ヘッダには含まれません。
- identtcpnumeric は、受信した IP 番号を挿入します。リバース DNS 検索は実行されません。

注　identtcp、identtcpsymbolic、または identtcpnumeric による IDENT 検索が役に立つのは、リモートシステムで IDENT サーバが稼動している場合です。

IDENT 検索の試行でパフォーマンスヒットが発生する場合があります。そうすると、ルータは認識できないポートへの接続試行を次第に「ブラックホール化」するようになります。IDENT 検索でこのような情況が発生した場合は、接続がタイムアウトするまで MTA には応答が返されません (通常、このタイムアウトは TCP/IP スタックが制御するもので、1、2 分ほどかかります)。

別のパフォーマンス因子として、identtcp、indenttcplimited、または identtcpsymbolic と identtcpnumeric とを比較する方法もあります。identtcp、identtcplimited または identtcpsymbolic によって リバース DNS 検索が実行された場合に、よりユーザフレンドリーなホスト名を返すにはより長時間が必要になります。

identnone キーワードは IDENT 検索を無効にしますが、IP からホスト名への変換は行われます。メッセージの Received: ヘッダには IP 番号とホスト名が共に含まれます。デフォルト設定では、このキーワードが使用されます。

identnonesymbolic キーワードは IDENT 検索を無効にしますが、IP からホスト名への変換は行われます。メッセージの Received: ヘッダにはホスト名だけが含まれます。

identnonenumeric キーワードは IDENT 検索を無効にし、リバース DNS 検索の IP 番号からホスト名への変換を禁止します。また、Received: ヘッダにユーザフレンドリーではないホスト名を使用するため、パフォーマンスの向上につながる可能性もあります。

identtcplimited および identnonelimited キーワードは、IDENT 検索、リバース DNS 検索、Received: ヘッダに表示する情報などに関し、identtcp および identnone と同様の効果をもたらします。ただし、異なる点として、identtcplimited および identnonelimited の場合は、switchchannel キーワードの影響で、リバース DNS 検索によってホスト名が検出されたかどうかに関わらず常に IP リテラルアドレスがチャネルスイッチのベースとして使用されます。

TCP/IP MX レコードのサポート

TCP/IP ネットワークには、MX (メール転送) レコードの使用をサポートするものとしないものとがあります。MTA システムの接続先であるネットワークから提供される MX レコードだけを使用するように設定できる TCP/IP チャネルプログラムもあります。mx、nomx、defaultmx、randommx、および nonrandommx キーワードは、MX レコードのサポートを制御するためのものです。

randommx キーワードは、MX 検索を実行し、同等の優先順位を持つ MX レコード値を順不同で処理するように指定します。nonrandommx キーワードは、MX 検索を実行し、同等の優先順位を持つ MX レコード値を受信した通りの順番で処理するように指定します。

現在のところ、mx キーワードは nonrandommx キーワードと同じものですが、将来のリリースでは randommx と同じになるように変更される可能性もあります。nomx キーワードは MX 検索を無効にします。defaultmx キーワードは、ネットワークが MX レコードをサポートする場合に mx を使用するように指定します。MX 検索をサポートするチャネルではすべて defaultmx キーワードがデフォルトとして設定されています。

ネームサーバ検索

ネームサーバ検索が実行される際、TCP/IP スタックが選択したネームサーバの代わりに nameservers チャネルキーワードを使ってネームサーバのリストを指定することができます。nameservers キーワードには、空白文字で区切られたネームサーバの IP アドレスのリストが必要です。以下の例を参照してください。

```
nameservers 1.2.3.1 1.2.3.2
```

デフォルト設定では defaultnameservers が有効になっているため、TCP/IP スタックの選択によるネームサーバが使用されます。

UNIX でネームサーバ検索を禁止するには、nsswitch.conf ファイルを編集します。NT の場合は、TCP/IP 設定を変更します。

最後のホスト

lastresort キーワードは、「最後のホスト」つまり他のホストへの接続試行がすべて失敗した場合に最終的な接続先となるホストを指定します。このキーワードは、事実上の最終手段的 MX レコードとして動作します。このキーワードは、SMTP チャネルに対してのみ効果があります。

メール受信用代替チャネル

次の各キーワードは、メール受信用代替チャネルの選択を制御するものです :switchchannel、allowswitchchannel、および noswitchchannel。

MTA がリモートシステムの受信接続を許可するには、どのチャネルで接続を確立するかを決定する必要があります。通常、使用するチャネルは転送形式に基づいて決定されます。たとえば、リモートシステムが TCP/IP の上位プロトコルとして SMTP を実装している場合は、自動的に tcp_local チャネルで接続が確立されます。

ただし、異なる性質を持つ複数の送信チャネルが複数のシステムに対して同時に使用される場合は、受信接続と送信接続がそれぞれ異なるチャネルで行われるため、対応するチャネルの性質がリモートシステムに関連付けられません。

この問題は、switchchannel キーワードを使用することにより解決できます。サーバが最初に使用するチャネルに switchchannel を指定すると、送信元ホストの IP アドレスがチャネルテーブルに照合され、一致した場合はソースチャネルがそれに合わせて切り替えられます。一致するものがない場合、または最初のデフォルト受信チャネルに一致するものが検出された場合は、MTA が リバース DNS 検索によって検出したホスト名に一致するエントリを見つけようと試みる場合もあります。ソースチャネルは switchchannel または allowswitchchannel にマークされているチャネルに切り替えられます (デフォルト)。noswitchchannel キーワードは、チャネルの切り替えを行わないよう指定します。

デフォルトでは、サーバが関連付けられているチャネル以外のチャネルに switchchannel を使用しても効果はありません。現在のところ、switchchannel を使用できるのは SMTP チャネルに対してのみですが、いずれにしても SMTP チャネル以外に switchchannel を使用すべきではありません。

ターゲットホストの選択

daemon キーワードは、SMTP チャネル上でターゲットホストの選択を制御するために使用します。

通常、ホストへの接続に使用されているチャネルは、メッセージのエンベロープアドレスに表示されます。daemon キーワードは、エンベロープアドレスにどのチャネルが表示されているかに関わらず、チャネルがファイヤウォールやメールハブシステムなど特定のリモートシステムに接続するように設定します。実際のリモートシステム名は、以下の例に示すように daemon キーワードの直後に記述します。

```
tcp_firewall smtp mx daemon firewall.acme.com
TCP-DAEMON
```

daemon キーワードの後ろの引数が完全なドメイン名ではない場合、引数は無視され、チャネルは正規ホストに接続します。ファイヤウォールやゲートウェイシステムを正規ホストにする場合は、以下の例に示すように daemon キーワードの引数を router として指定します。

```
tcp_firewall smtp mx daemon router
firewall.acme.com
TCP-DAEMON
```

また、関連するキーワードとして、single および single_sys があります。single キーワードは、チャネルの各宛先アドレス用にメッセージのコピーを 1 つずつ作成するように指定します。single_sys キーワードは、各宛先システム用にメッセージのコピーを 1 つずつ作成します。どのキーワードを使用しても、メッセージがキューに入れられる各チャネルごとに最低 1 つずつメッセージのコピーが作成されることに注意してください。

SMTP 認証と SASL

Messaging Server が SASL (Simple Authentication and Security Layer) を使用した SMTP サーバの認証をサポートするかどうかを指定できます。SASL については、RFC 2222 で規定されています。SASL、SMTP 認証、およびセキュリティの詳細については、第 11 章「セキュリティとアクセス制御を設定する」を参照してください。

表 8-4 に、この項で説明している SASL に関連するキーワードのリストを示します。

表 8-4　　SASL を使用した SMTP 認証

キーワード	説明
maysaslserver	SMTP サーバが SASL 認証をサポートするように指定します。クライアントは SASL 認証を使用して接続試行を行うことができます。
mustsaslserver	SMTP サーバが SASL 認証をサポートするように指定します。クライアントは必ず SASL 認証を使用する必要があります。リモートクライアントが認証に成功しない限り、SMTP サーバはメッセージを受け入れません。
nosasl	SASL 認証の許可および試行を禁止します。このキーワードは nosaslserver を包括するため、SASL 認証の使用はすべて禁止されます。デフォルト設定では、このキーワードが使用されます。
nosaslserver	SMTP サーバが SASL 認証を許可しないように指定します。
saslswitchchannel	クライアントが SASL の使用に成功した場合、その受信接続は指定のチャネルに切り替えられます。このキーワードを使用する場合は、切り替え先のチャネルを指定する必要があります。

TLS (Transport Layer Security)

maytls、maytlsclient、maytlsserver、musttls、musttlsclient、musttlsserver、notls、notlsclient、notlsserver、および tlsswitchchannel チャネルキーワードは、TCP/IP チャネルなどの SMTP ベースのチャネルが SMTP プロトコルを使用するときに TLS をどのように処理するかを設定するためのキーワードです。

デフォルト設定では notls が有効になっているため、TLS は許可または試行されません。このキーワードは notlsclient (MTA SMTP クライアントは送信接続に TLS を使用しない。送信接続時に STARTTLS コマンドは発行されない) および notlsserver (MTA SMTP サーバは TLS 使用の接続を許可しない。SMTP サーバもコマンド自体も STARTTLS 拡張に通知しない) を包括しています。

maytls が設定されている場合、MTA は TLS 使用の接続を受け入れ、送信接続にも TLS を使用しようと試みます。このキーワードは、maytlsclient (MTA SMTP クライアントは TLS をサポートする。SMTP サーバにメッセージを送信する際に TLS を使用する) および maytlsserver (MTA SMTP サーバが STARTTLS 拡張をサポートすることを通知し、メッセージを受信する際に TLS を使用する) を包括しています。

musttls キーワードは、MTA が送受信接続に必ず TLS を使用するように指定します。TLS 使用のネゴシエーションを行うことができなかったリモートシステムとの電子メールの交換は許可されません。このキーワードは、musttlsclient (MTA SMTP クライアントはメッセージの送信に必ず TLS を使用し、TLS の使用のネゴシエーションが成功しない。SMTP サーバにメッセージを送らない。MTA 発行の STARTTLS コマンドは必ず成功しなければならない) および musttlsserver (MTA SMTP サーバが STARTTLS 拡張をサポートすることを通知し、TLS 使用のメッセージを受け入れる。TLS の使用のネゴシエーションが成功しないクライアントからのメッセージは拒否される) を包括しています。

tlsswitchchannel キーワードは、クライアントが TSL 使用のネゴシエートに成功した場合、受信した接続を指定のチャネルに切り替えるためのキーワードです。このキーワードには、切り替え先のチャネルを指定する必要があります。

チャネル動作のタイプ

Messaging Server は、RFC 2476 規定のメッセージ 送信プロトコルをサポートしています。チャネルを送信専用に設定するには、submit キーワードを使用します。これは、送信専用のポートで動作する SMTP サーバなどの TCP/IP チャネルに対して便利なキーワードです。RFC 2476 は送信専用としてポート 587 を規定しています。

メッセージの処理と配信を設定する

サーバが特定の条件に基づいてメッセージの配信を試みるように指定できます。また、サービスジョブの処理制限や、新しい SMTP チャネルスレッドを作成するタイミングなど、ジョブ処理に関するパラメータを指定することも可能です。この項では、以下の内容について説明します。

- メッセージの配信
- チャネル実行ジョブの処理プール
- サービスジョブの制限
- SMTP チャネルスレッド
- 複数アドレスの拡張
- 配信不能メッセージに対する通知発行のタイミング

表 8-5 に、この項で説明しているキーワードのリストを示します。

表 8-5　　メッセージの処理と配信に関連するキーワード

キーワード	定義
即時配信	**メッセージの即時配信に関する設定を定義**
immnonurgent	優先度に関わらず、送信後すべてのメッセージの配信を即座に開始します。
遅延配信	**遅延ジョブの配信に関する設定を定義**
backoff	遅延メッセージ配信の試行頻度を指定します。他の backoff キーワードが使用されていない限り、このキーワードが優先度に関わらずすべてのメッセージに適用されます。デフォルトでは、次のように設定されています : サーバは 1 時間後、2 時間後、4 時間後に 1 回ずつ配信できないメッセージの配信を再試行し、それ以降は 4 時間おきに 3 回、そしてそれ以降は 8 時間おきに再試行します。
nonurgentbackoff	優先度が低いメッセージの配信試行頻度を指定します。
normalbackoff	優先度が標準であるメッセージの配信試行頻度を指定します。
urgentbackoff	優先度が高いメッセージの配信試行頻度を指定します。
サイズに基づくメッセージの優先度	**サイズに基づいてメッセージの優先度を定義**
nonurgentblocklimit	指定値以上のサイズを持つメッセージの優先度を「低」以下 (2 番目の優先度) に設定します。該当するメッセージは次の定期ジョブまで処理されません。
normalblocklimit	指定値以上のサイズを持つメッセージの優先度を「低」に設定します。

表 8-5　メッセージの処理と配信に関連するキーワード（続き）

キーワード	定義
urgentblocklimit	指定値以上のサイズを持つメッセージの優先度を「標準」に設定します。
チャネル実行ジョブの処理プール	**異なる優先度を持つメッセージを処理するプールおよびジョブの遅延を指定**
pool	チャネルが動作するプールを指定します。
after	チャネルが動作するまでの遅延時間を指定します。
サービスジョブの制限	**サービスジョブ数、および 1 つのジョブで処理できるメッセージファイル数を指定**
maxjobs	1 つのチャネルに対して同時実行できるジョブの数を指定します。
filesperjob	1 つのジョブで処理できるキューエントリの数を指定します。
SMTP チャネルスレッド threaddepth	マルチスレッド SMTP クライアントに対して新しいスレッドをトリガするために必要なメッセージ数を指定します。
複数アドレス拡張	**複数の宛先アドレスを持つメッセージの処理方法を定義**
expandlimit	指定値以上の宛先アドレスを持つメッセージを受信した場合に、「オフライン」でメッセージを処理します。
expandchannel	expandlimit の適用による遅延拡張を実行するチャネルを指定します。
holdlimit	指定値以上の宛先アドレスを持つメッセージを受信した場合に、そのメッセージを保留します。
配信不能メッセージに対する通知	**配信できないメッセージに対して通知を送るタイミングを指定**
notices	メッセージを配信できない場合に通知を送り、そのメッセージを返送するまでの時間を指定します。
nonurgentnotices	優先度が低いメッセージを配信できない場合に通知を送り、そのメッセージを返送するまでの時間を指定します。
normalnotices	優先度が標準のメッセージを配信できない場合に通知を送り、そのメッセージを返送するまでの時間を指定します。
urgentnotices	優先度が高いメッセージを配信できない場合に通知を送り、そのメッセージを返送するまでの時間を指定します。

メッセージの配信

メッセージがチャネルのキューに入る度に、ジョブコントローラはメッセージが確実に配信されるよう新しいジョブプロセスの開始、スレッドの追加、ジョブ実行の確認などを行います。チャネルやプールのジョブ数が制限に達しているために新しいジョブを開始できない場合は、実行中のジョブが終了するのを待って、ジョブ数が制限以下になったら新しいジョブを開始します。チャネルのジョブ数制限は maxjobs チャネルキーワードによって決定され、プールのジョブ数制限は JOB_LIMIT プールオプションによって決定されます。

Messaging Server はすべてのメッセージの即時配信を試みます。最初の試行でメッセージを配信できない場合は、該当する backoff キーワードに基づいて配信遅延時間が決定されます。遅延メッセージは backoff キーワードが指定する時間が経過したときに配信され、必要に応じてメッセージを処理するチャネルジョブが開始されます。

チャネルジョブを作成および管理するのはジョブコントローラであり、チャネルジョブはジョブコントローラの処理プール内で実行されます。プールの詳細については、161 ページの「チャネル実行ジョブの処理プール」を参照してください。

ジョブコントローラのメモリ内における処理中メッセージおよび処理待ちメッセージに関するデータの構造は、ディスクの MTA キュー領域に保存されているメッセージファイル全体の構造を反映しています。ただし、ディスク上のメッセージファイルのバックログがジョブコントローラのメモリ内データ構造のサイズ制限を超過するほど大きくなると、ジョブコントローラはディスク上のメッセージファイルの一部だけをトラックし、トラックしているメッセージだけを処理するようになります。メッセージを配信してメモリに余裕ができると、ジョブコントローラは MTA キュー領域をスキャンしてメモリ内の保存情報をリフレッシュし、メッセージのリストを更新し、ディスクから読み込んだメッセージの処理を開始します。ジョブコントローラは自動的に MTA キュー領域のスキャンを実行します。

メッセージのバックログが頻繁に発生する場合は、MAX_MESSAGES オプションを使用してジョブコントローラを調整します。MAX_MESSAGES オプションの値を大きくするとジョブコントローラはより多くのメモリを使用できるようになるため、メッセージのバックログによるジョブコントローラのメモリ内キャッシュのオーバーフローを回避できます。このため、ジョブコントローラが MTA キューディレクトリをスキャンするのに必要な時間を短縮できます。ただし、ジョブコントローラがメモリ内キャッシュを再構築する必要がある場合は、キャッシュのサイズが大きいために比較的長時間かかることに注意してください。また、ジョブコントローラは起動 (または再起動) する度に MTA キューディレクトリをスキャンします。メッセージのバックログが大きい場合は、バックログが小さい場合に比べて、ジョブコントローラの起動 (または再起動) にも時間がかかることに注意してください。

チャネル実行ジョブの処理プール

複数のチャネルが 1 つのプール内で動作するように設定すると、複数のチャネルが同じプールのリソースを共有できるようになります。特定のチャネル専用に指定されているプール内で他のチャネルが動作するように設定することも可能です。各プール内のメッセージは優先度に基づいて自動的に適切な処理キューに割り当てられ、優先度の高い順に処理されます。詳細については、163 ページの「サイズに基づくメッセージの優先度」を参照してください。

pool キーワードを使用すると、ジョブが作成されるプールをチャネルごとに指定できます。pool キーワードの後ろには、カレントチャネルの配信ジョブのプール先となるプール名を指定する必要があります。プール名の文字数の上限は 12 文字です。

サービスジョブを遅らせるには、after キーワードを使います。after キーワードの後ろには、遅延時間の長さを記述する必要があります。遅延時間に符号なし整数を使用すると、その値はデルタタイム値、つまりメッセージの遅延配信時間までの秒数として認識されます。

サービスジョブの制限

メッセージがチャネルのキューに入る度に、ジョブコントローラはメッセージが確実に配信されるよう新しいジョブプロセスの開始、スレッドの追加、ジョブ実行の確認などを行います。しかし、1 つのサービスジョブではすべてのメッセージを手際よく配信できない場合もあります。

メッセージ配信のために開始されるプロセスやスレッドの数には、妥当な制限があります。このプロセスやスレッド数の上限は、プロセッサの数、ディスクの速度、接続の性質などによって決定されます。MTA 設定ファイルでは、以下のものを制御することができます。

- 1 つのチャネルに対して開始できるプロセス数の上限 (maxjobs チャネルキーワード)
- 1 つのチャネルセットに対して開始できるプロセス数の上限 (ジョブコントローラ設定ファイルの該当するプールセクションに設定されている JOB_LIMIT パラメータ)
- 新しいスレッドまたはプロセスを開始する前に受信したキュー内のメッセージ数 (threaddepth チャネルキーワード)
- チャネルによっては、特定の配信プログラム内で実行するスレッド数の上限 (チャネルオプションファイル内の max_client_threads パラメータ)

1 つのチャネルに対して開始されるプロセス数の上限は、そのチャネルに対して設定されている maxjobs、またはチャネルが動作しているプールに対して設定されている JOB_LIMIT の最小値に当たります。

処理すべきメッセージがある場合、ジョブコントローラは以下の基準に基づいて新しいプロセスを開始します。

- チャネルに対してプロセスが実行されておらず、プールのジョブ数が制限に達していない場合は、新しいプロセスを開始します。
- チャネルプログラムがシングルスレッドの場合、またはスレッド数が制限に達していて threaddepth で指定されている以上のバックログがあり、かつチャネルとプールのジョブ数が共に制限に達していない場合は、新しいプロセスを開始します。
- チャネルプログラムがマルチスレッドで、スレッド数が制限に達しておらず、かつ threaddepth で指定されている以上のバックログがある場合は、新しいスレッドが開始されます。

特に、SMTP チャネルに対しては、異なるホスト宛てのメッセージがキューに入るにつれて新しいスレッドやプロセスが開始されます。処理すべきメッセージがある場合ジョブコントローラは、SMTP チャネルに対し、以下の基準に基づいて新しいプロセスを開始します。

- SMTP チャネルに対して実行されているプロセスがなく、プールのジョブ数が制限に達していない場合は、新しいプロセスが開始されます。
- スレッド数が制限に達しており (MAX_CLIENT_THREADS)、サービス待ち状態のホスト宛てのメッセージがキューに入り、かつチャネルのジョブ数 (maxjobs) およびプールのジョブ数 (JOB_LIMIT) が共に制限に達していない場合は、新しいプロセスが開始されます。
- スレッド数が制限に達しておらず、サービス待ち状態のホスト宛てのメッセージがキューに入った場合は、新しいスレッドが開始されます。
- スレッド数が制限に達しておらず、メッセージがキューに入ったためにそのホスト宛てのメッセージのバックログが threaddepth で指定されている以上の数になった場合は、新しいスレッドが開始されます。

詳細については、164 ページの「SMTP チャネルスレッド」を参照してください。

filesperjob キーワードを使うと、MTA に追加のサービスジョブを作成するよう指示することもできます。このキーワードには、正の整数を 1 つパラメータとして設定する必要があります。この整数は、複数のサービスジョブを作成するため関連するにチャネルが受け取らなくてはならないキューエントリ (ファイル) の数を指定します。パラメータに 0 またはそれ以下の値を設定すると、サービスジョブは 1 つしか作成されません。キーワードが設定されていない場合は、パラメータの値が 0 であると認識されます。また、実際に作成されるサービスジョブの数は、チャネルが受け取ったキューエントリの合計数によって決定されます。

filesperjob キーワードは、実際のキューエントリ (ファイル) 数を指定値で割って作成するジョブ数を算出します。各メッセージのキューエントリ数は、single や single_sys キーワード、メーリングリストのヘッダ修正アクション、そのほかさまざまな要素によって決定されます。

maxjobs キーワードは、同時実行可能な合計ジョブ数を制限します。maxjobs キーワードの後ろには、整数値を指定する必要があります。算出されたサービスジョブ数がこの値より大きい場合には、maxjobs ジョブだけが作成されます。maxjobs が使用されていない場合のデフォルト値は 100 に設定されています。通常、maxjobs には、そのチャネルが使用するプールまたはサービスプールで同時実行が可能な合計ジョブ数と同じ値、またはそれ以下の値を使用します。

サイズに基づくメッセージの優先度

urgentblocklimit、normalblocklimit、および nonurgentblocklimit キーワードは、サイズに基づいてメッセージの優先度を下げるように MTA に指定するためのものです。これらのキーワードは、ジョブコントローラがメッセージ処理時に適用する優先度に影響を及ぼします。

SMTP チャネルスレッド

マルチスレッドの SMTP クライアントは、メッセージを宛先ごとにそれぞれ異なるスレッドに割り当てるため、送信メッセージを並べ替えます。threaddepth キーワードは、マルチスレッドの SMTP クライアントが 1 つのスレッドに割り当てられるメッセージの数を制限し、それ以上のメッセージがある場合には別のスレッドに割り当てるよう指定します。通常、同じ宛先へのメッセージはすべて 1 つのスレッドによって処理されますが、このキーワードが設定されている場合はそれらのメッセージが複数のスレッドによって処理されるようになります。

threaddepth キーワードは、チャネルの接続先の SMTP サーバが複数の接続を同時に処理できる場合に、デーモン ルータ TCP/IP チャネル (ある特定の SMTP サーバに接続する TCP/IP チャネル) 上でマルチスレッドを確立する際に便利です。

チャネルに対するバックログが threaddepth で指定されている以上の数に達すると、ジョブコントローラはより多くのリソースをそのチャネルのキューにあるメッセージの処理に割り当てようとします。チャネルがマルチスレッドの場合、ジョブコントローラはメッセージを処理するジョブがそのチャネルに対して新しくスレッドを開始するように指示し、すべてのジョブのスレッド数がそのチャネルの制限に達している場合 (tcp_* チャネルの MAX_CLIENT_THREADS オプション) は、新しいプロセスを開始するように指示します。シングル スレッドのチャネルに対しては、新しいプロセスを開始するように指示します。ただし、チャネルのジョブ数 (maxjobs) またはプールのジョブ数 (JOB_LIMIT) が制限に達している場合、新しいジョブは開始されません。

複数アドレスの拡張

大部分のチャネルは複数の宛先アドレスを持つメッセージを受け入れますが、1 つのメッセージに複数の宛先アドレスが指定されていると、配信処理に遅延 (オンライン遅延) が生じます。遅延時間が長いとネットワークがタイムアウトが発生し、メッセージの重複送信やその他の問題が発生する可能性があります。

MTA は、1 つのメッセージに特定数以上のアドレスが指定されている場合に配信を遅らせて処理 (オフライン処理) することができます。この方法によって、オンライン遅延を大きく軽減することが可能です。処理のオーバーヘッドを遅らせることはできますが、遅延を完全に回避することは不可能です。

この機能を有効にするには、たとえば一般的な reprocessing チャネルと expandlimit キーワードを使用します。expandlimit キーワードには、オフライン処理を開始するまでにチャネルから受け入れることのできるメッセージのアドレス週の上限を示す整数の引き数をとります。expandlimit キーワードが設定されていない場合、オフライン処理は行われません。引数の値を 0 にすると、そのチャネルで受信したすべてのメッセージがオフラインで処理されます。

expandlimit キーワードは、ローカルチャネルおよび reprocessing チャネルには使用できません。使用すると、予測できない事態が発生する可能性があります。

オフライン処理を行うチャネルを指定するには、expandchannel キーワードを使用します。特に設定を変更しない限り、expandchannel が設定されていない場合は reprocessing チャネルが使用されますが、特別な目的のためにはその他の reprocessing チャネルまたは processing チャネルを設定することもできます。expandchannel を使ってオフライン処理を行うチャネルを指定する場合、reprocessing チャネルまたは processing チャネル以外のチャネルを使用することはできません。その他のチャネルを使用すると、予測できない事態が発生する可能性があります。

expandlimit を適切に機能させるには、reprocessing チャネル (またはオフライン処理を実行するその他のチャネル) を MTA 設定ファイルに追加する必要があります。ただし、MTA 設定ユーティリティによって生成された設定ファイルを使用しているのであれば、その必要はありません。

非常に多くの宛先アドレスが指定されているのは、不特定多数宛てメールの特徴です。holdlimit キーワードは、MTA が特定数以上の宛先アドレスを持つメッセージを受信した場合、そのメッセージを .HELD メッセージとして reprocess チャネル (または expandchannel キーワードが指定するチャネル) のキューに入れるように指示します。メッセージは MTA postmaster が手動で介入するまで reprocess キュー内で未処理のまま待機します。

配信不能メッセージに対する通知発行のタイミング

notices、nonurgentnotices、normalnotices、および urgentnotices キーワードは、配信できないメッセージをチャネルキュー内に保持する時間の長さを制御するものです。Messaging Server は、差出人に繰り返し配信不能の警告メッセージを送ることができます。それでもメッセージを宛先に配信できない場合、Messaging Server はそのメッセージを差出人に返送します。

メッセージの優先度に基づいて異なる返送方法を適用するには、nonurgentnotices、normalnotices、または urgentnotices キーワードを使用します。これらのキーワードが設定されていない場合は、notices キーワードがすべてのメッセージに適用されます。

キーワードの後ろには、同じ間隔で増加する最高 5 つの整数値を指定できます。これらの値はメッセージが受信されてから警告メッセージが発行されるまでの時間を示すもので、MTA オプションファイル内で RETURN_UNITS が 0 に設定されている場合やオプションが設定されていない場合は、日単位として認識されます。RETURN_UNITS が 1 に設定されている場合は、時間単位として認識されます。

指定された最終時間に達してもメッセージを配信できない場合、そのメッセージは差出人に返送されます。それまでは、キーワードで指定した時間になる度に警告メッセージが送られます。特に設定を変更しない限り、notices キーワードが設定されていない場合は notices 設定が使用されます。notices 設定もない場合は、メッセージを受信してから 3 日後 (または 3 時間後)、6 日後 (または 6 時間後)、9 日後 (または 9 時間後)、12 日目（または 12 時間後）に警告メッセージが送られ、その後もメッセージキューに残っているメッセージが差出人に返送されます。

notices キーワードの構文に、ドット文字やカンマを使用する必要はありません。たとえば、デフォルトの返送ポリシーは以下のように設定されています。

```
notices 3 6 9 12
```

全チャネルの通知発行のタイミングを一括して変更するには、MTA 設定ファイルのチャネルブロックセクションの冒頭に defaults チャネルブロックを追加するか、ローカルチャネルに notices 設定を追加するのが最も簡単な方法です。たとえば、以下のコマンドを使用すると、すべてのチャネルの通知発行タイミングを指定する defaults チャネルを追加できます。

```
defaults notices 1 3 6 9 12
```

defaults チャネルは、MTA 設定ファイル内にある最初の空白行の直後に記述します。

Postmaster 宛てのメッセージを設定する

長期間にわたってサービスが支障を来たしている場合や、アドレスが不正確な場合には、チャネルプログラムがメッセージを配信できないことがあります。その場合、MTA チャネルプログラムは、配信不能の理由を説明する文章と共に、メッセージを差出人に返送します。

メッセージの返送に加えて、MTA は配信できないメッセージに関する詳細な情報を記載した警告メッセージを送ることがあります。通常、この警告メッセージは notices チャネルキーワードが指定するタイムアウトに基づいて送られますが、配信試行に失敗したときに送られることもあります。通知には、問題点の説明と配信試行を継続する時間枠が記載されます。また、多くの場合、該当するメッセージのヘッダと最初の数行も含まれます。

さらに、配信できないメッセージおよび警告メッセージのコピーをすべてローカル postmaster に送るように設定することも可能です。ただし、この設定を使用すると、メッセージの配信不能情況や各種キューの状態を監視するには便利ですが、postmaster 宛てのメッセージが非常に多くなる可能性があります。

表 8-6 に示すキーワードを使用して、postmaster 宛てのメッセージを制御することができます。

表 8-6　　Postmaster 宛てのメッセージに関連するキーワード

キーワード	説明
返送メッセージ	**返送メッセージに関する通知の処理方法を指定**
sendpost	postmaster にすべての配信不能メッセージのコピーを送ります。
copysendpost	メッセージの差出人アドレス部分が空白になっていない場合は postmaster に通知のコピーを送り、差出人アドレスが空白の場合は配信不能メッセージのコピーを送ります。ただし、そのメッセージがもともと返送されたものである場合や通知である場合、メッセージのコピーは送られません。
errsendpost	差出人に通知を送ることができない場合にのみ postmaster に配信不能メッセージのコピーを送ります。nosendpost が設定されている場合、配信不能メッセージのコピーは送られません。
nosendpost	配信不能メッセージのコピーを postmaster に送りません。
警告メッセージ	**警告メッセージの処理方法を指定**

表 8-6　Postmaster 宛てのメッセージに関連するキーワード（続き）

キーワード	説明
warnpost	警告メッセージのコピーを postmaster に送ります。デフォルトでは、キーワードが設定されていない場合は警告メッセージのコピーが postmaster に送られるように設定されています。ただし、Warnings-to: ヘッダやエンベロープの From: アドレスが完全に空白になっている場合は送られません。
copywarnpost	配信不能メッセージの差出人アドレスが空白になっていない限り、postmaster に警告メッセージのコピーを送ります。
errwarnpost	差出人に警告メッセージを送ることができない場合に postmaster に通知のコピーを送ります。
nowarnpost	postmaster に警告メッセージのコピーを送りません。
返送メッセージの内容	**postmaster にメッセージ全体を送るか、ヘッダだけを送るかを指定**
postheadonly	postmaster にヘッダだけを送ります。メッセージ全体を送らないことで、ユーザのプライバシーを尊重できます。ただし、postmaster やシステム管理者は一般に root システム権限を使用してメッセージの内容を読むことができるため、このキーワードを使用してもメッセージのセキュリティを完全に保証することにはなりません。
postheadbody	メッセージのヘッダおよび内容を送ります。

チャネルオプションを設定する

TCP/IP チャネルオプションファイルは、TCP/IP チャネルのさまざまな性質を制御するものです。チャネルオプションファイルは、*x*_option (*x* 部分は該当チャネル名) という名前で MTA 設定ディレクトリ内に保存されていなければなりません。以下に例を示します : */ サーバ- インスタンス* /imta/config/tcp_local_option。

オプションファイルは、1 つまたは複数のキーワードとその関連値によって構成されています。たとえば、サーバのメーリング リスト拡張を無効にするには、オプションファイルに DISABLE_EXPAND キーワードを追加し、値を 1 に設定します。

また、その他のオプションファイルキーワードを使用すると、以下の制御を行うことができます。

- メッセージあたりの宛先数を制限する (ALLOW_RECIPIENTS_PER_TRANSACTION)
- セッションあたりのメッセージ数を制限する (ALLOW_TRANSACTIONS_PER_SESSION)
- MTA ログファイルに記録される情報の内容を微調整する (LOG_CONNECTION, LOG_TRANPORTINFO)
- クライアントチャネルプログラムが許可できる同時送信接続数を指定する (MAX_CLIENT_THREADS)

チャネルオプションキーワードと構文の詳細については、『Messaging Server リファレンスマニュアル』を参照してください。

チャネルのデフォルトを設定する

設定ファイルにはさまざまなチャネルキーワードが繰り返し記述されていることがありますが、このような設定を管理するには時間がかかり、エラーの原因にもなります。複数のチャネルに対してまとめてデフォルトのキーワードを指定すると、設定を簡素化することができます。

たとえば、以下の行を設定ファイルに追加すると、行中で指定したキーワードがそれ以降のすべてのチャネルブロックに適用されます。

```
defaults キーワード1 キーワード2 キーワード3 ...
```

defaults 行はチャネルを特定せずにデフォルトのキーワードを変更するための特殊なチャネルブロックだと考えられます。また、defaults 行に他のチャネルブロック情報を指定する必要はありません (指定しても無視されます)。

1 つのファイルに使用できる defaults 行の数に上限はありません。複数の defaults 行を指定した場合、ファイルの下へ行くほど (後で追加した行ほど) 優先度が高くなります。

設定ファイル内のある位置 (たとえば、外部ファイルのチャネルブロックの独立したセクションの冒頭など) 以降には無条件に defaults 行が適用されないように設定しておく方がよい場合もあります。そのためには、nodefaults 行を使用します。たとえば、以下の行を設定ファイルに挿入すると、それ以前の部分で defaults を使って指定した設定がすべて無効になり、defaults を使用していないのと同じ状態に戻ります。

```
nodefaults
```

他のチャネルブロックと同様に、defaults や nodefaults チャネルブロックを使用する場合も、ブロック間の区切りには空白行を使用します。設定ファイル内でローカルチャネルの前に記述できるチャネルブロックは、defaults と nodefaults のみです。ただし、他のチャネルブロックと同様、書き換え規則の前に記述することはできません。

チャネルのログを設定する

MTA は、メッセージがキューに出し入れされる度にログを作成することができます。logging および nologging キーワードは、チャネルごとのメッセージログの作成を制御します。デフォルト設定では、すべてのチャネルに対してログが作成されます。特定のチャネルに対してログの作成を無効にするには、チャネル定義で logging の代わりに nologging キーワードを設定します。

ログの詳細については、第 12 章 「ログ記録とログ解析」を参照してください。

チャネルのデバッグを設定する

チャネルプログラムによっては、デバッグ目的のためにより詳細な診断出力を生成するオプションコードがあるものもあります。このチャネルごとのデバッグ出力を有効にするためのチャネルキーワードには 2 種類あります。master_debug キーワードはマスタープログラムのデバッグ出力を有効にし、slave_debug キーワードはスレーブプログラムのデバッグ出力を有効にします。デフォルト設定では nomaster_debug および noslave_debug が有効になっているため、デバッグ出力は生成されません。

デバッグを有効にすると、デバッグ出力は各チャネルプログラムに関連付けられているログファイルに記述されます。ログファイルの場所はプログラムによって異なりますが、通常はログディレクトリにあります。マスタープログラムのログファイルの名前は、概して *x*_master.log (*x* はチャネル名) という形式になっています。スレーブプログラムのログファイル名の形式は、*x*_slave.log です。

プログラム配信を設定する

ユーザによっては、受信メールをメールボックスではなく メールソートプログラムや Vacation Notice などの自動返信エージェントに配信して欲しいと望む人もいます。pipe チャネルはサイト提供のユーザごとのプログラムを使用してメッセージを配信します。

プログラム配信を有効化するには、まず pipe チャネルが呼び出せるプログラムを登録する必要があります。そのためには、imsimta program ユーティリティを使用して、pipe チャネルから呼び出し可能なコマンドとして登録したものにそれぞれ特有の名前を付けます。これによってエンドユーザが mailprogramdeliveryinfo LDAP 属性の値としてプログラム名を指定できるようになります。

たとえば、UNIX の myprocmail コマンドをユーザが呼び出せるプログラムとして追加するには、imsimta program ユーティリティを使用して以下の例のようにこのコマンドを登録します。この例では、-d *ユーザ名* という引数を使用して procmail プログラムをユーザとして実行する myprocmail プログラムが登録されます。

```
imsimta program -a -m myprocmail -p procmail -g "-d %s" -e user
```

programs ディレクトリ (*サーバ- インスタンス* /imta/programs) に実行可能ファイルが存在し、「others」に対して実行権が設定されていることを確認してください。

ユーザがプログラムにアクセスするためには、そのユーザの LDAP エントリに以下の属性および値が含まれている必要があります。

```
maildeliveryoption: program
mailprogramdeliveryinfo: myprocmail
```

imsimta program ユーティリティの詳細については、『Messaging Server リファレンスマニュアル』を参照してください。

その他の配信プログラムを使用する場合は、そのプログラムが以下の終了コードおよびコマンド行の引数に関する条件を満たしていることを確認してください。

終了コード条件 : pipe チャネルが呼び出す配信プログラムは、チャネルがメッセージをキューから出すか、後で処理するために配信するか、または返送するかを判断できるように、適切なエラーコードを返すものでなくてはなりません。

サブプロセスが終了コード 0 (EX_OK) で終了した場合は、メッセージが適切に配信されたと認識され、MTA のキューから削除されます。終了コード 71、74、75、または 79 (EX_OSERR、EX_IOERR、EX_TEMPFAIL、または EX_DB) で終了した場合は、一時的なエラーが発生したと見なされ、メッセージの配信は延期されます。その他のコードが返されると、メッセージは配信不能として差出人に返送されます。終了コードは、システムヘッダファイル sysexits.h 内で定義されています。

コマンド行の引数 : 可変引数 (%s) を含め、配信プログラムが使用できる引数の数に上限はありません。可変引数は、ユーザが実行するプログラムの場合はユーザ名を、postmaster「inetmail」が実行するプログラムの場合はユーザ名 + ドメイン名を示します。たとえば、以下のコマンド行は procmail プログラムを使用してメールを受取人に配信します。

```
/usr/lib/procmail -d %s
```

hold チャネルを使用する

hold チャネルは、一時的に受信不能になっている宛先へのメッセージを保留するためのチャネルです。一時的な受信不能の原因としては、ユーザ名が変更されている最中であったり、メールボックスが別のホストやドメインに移行されている最中であることが考えられます。原因は他にもありますが、この 2 つが最も一般的なものです。

hold チャネルにメッセージを保留するには、以下の 2 通りの方法があります。

- ユーザの maildeliveryoption 値の 1 つを hold にします。その他の maildeliveryoption 値はすべて無視され (maildeliveryoption は複数値を持つ属性)、そのユーザへのメッセージは hold チャネルにルーティングされます。
- hold_slave プログラムを実行します。このプログラムは、その他のすべてのチャネルをチェックし、引数が指定する宛先に一致する宛先を持つすべてのメッセージを hold チャネルに移します。

他のチャネルとは異なり、hold チャネルのマスタープログラムは自動的に起動するように設定されていません。hold チャネルのキュー内のメッセージは、管理者が hold_master プログラムを呼び出すまでそのままの状態で待機します。

ユーザを移行するには、まず imadmin modify user を使用して maildeliveryoption を hold に設定することによって、そのユーザが移行中であることを示す必要があります。次に、hold_slave を呼び出し、その他のチャネルのキュー内にあるメッセージを hold チャネルのキューに移してから通常の移行ステップを実行します。移行ステップをすべて完了したら maildeliveryoption=hold を削除し、hold_master を呼び出して適切なチャネルのキューにメッセージを入れます。

conversion チャネルを使用する

conversion チャネルは、MTA を通して配信されるメッセージを本文部分ごとに変換します。MTA トラフィックのサブセットはいずれも変換可能であり、変換プロセスには任意のプログラムやコマンドを使用できます (MTA のネイティブ変換機能には限界があるため、外部コンバータを呼び出す能力が重要になります)。各本文部分の変換には、特殊な conversion チャネル設定が使われます。

変換処理のトラフィックを選択する

変換処理は標準的な MTA チャネルプログラムを使用して実行されますが、このチャネルがアドレスまたは MTA の書き換え規則内で直接指定されていることはあまりありません。MTA は、MTA マッピングファイル (*サーバ _ ルート* /msg- *インスタンス* /imta/config/mappings) 内の CONVERSIONS マッピングテーブルを使って conversion チャネルへのアクセスを制御します。

MTA は、以下の形式の文字列を使って CONVERSIONS マッピングテーブル (存在する場合) をプローブしながら各メッセージを処理します。

IN-CHAN= *ソース - チャネル* ;OUT-CHAN= *宛先 - チャネル* ;CONVERT

*ソース - チャネル*はメッセージの送信元であるチャネル、*宛先 - チャネル*はメッセージの送信先であるチャネルを示します。プローブの結果として返される値は Yes または No という文字列です。Yes の場合、MTA はメッセージを宛先チャネルではなく conversion チャネルに送ります。No の場合および一致するものがない場合は、メッセージは通常の宛先チャネルのキューに送られます。

たとえば、tcp_intranet チャネル以外のチャネルから送られたメッセージのうち、変換処理を必要とするものに対しては、以下のマッピングが適切です。

```
CONVERSIONS

  IN-CHAN=tcp_intranet;OUT-CHAN=tcp_intranet;CONVERT NO
  IN-CHAN=*;OUT-CHAN=tcp_intranet;CONVERT YES
```

conversion チャネルの設定

MTA 設定ファイル (imta.cnf) 内 の conversion チャネルの設定は、デフォルトで実行されます。user@conversion . *ローカルホスト名* または user@conversion という形式のアドレスは、CONVERSIONS マッピングの内容に関わらず、すべて conversion チャネルを通してルーティングされます。

変換の制御

conversion チャネルが実行する変換は、MTA 変換ファイル内で定義されている規則によって制御されます。このファイルは、MTA テイラーファイル内の IMTA_CONVERSION_FILE オプションによって指定されているものであり、デフォルト設定では *サーバ_ルート*/msg-*インスタンス*/imta/conversions です。

MTA 変換ファイルは MIME Content-Type パラメータに準拠する形式のエントリを含むテキストファイルです。各エントリは 1 つまたは複数のグループ化された行から構成され、各行には 1 つまたは複数の name= 値 ; パラメータ句が含まれています。引用規則は Content-Type ヘッダ行のパラメータに関する MIME の様式に準拠します。最終行以外のすべての行には、その末尾にセミコロン (;) が付けられます。一行 (物理行) に入力できる文字数の上限は 252 文字です。論理行を複数の物理行に分割するには、バックスラッシュ (\) 継続文字が使われます。エントリは、セミコロンで終了していない行や空白行が 1 行以上挿入されている所で終了します。たとえば、ims-ms チャネルに送られるメッセージの application/wordperfect5.1 部分を架空のコンバータ「convert」で MS Word に変換するように指定するエントリは、以下のようになります。

```
out-chan=l; in-type=application; in-subtype=wordperfect5.1;
  out-type=application; out-subtype=ddif; out-mode=block;
  command="/usr/bin/convert -in=wordp -out=msword
<$INPUT_FILE>$OUTPUT_FILE"
```

変換を理解する

MTA が行う変換には大きく分けて 2 つのカテゴリがあり、各カテゴリはそれぞれ対応するマッピングテーブルおよび MTA の conversions ファイルによって制御されます。

最初のカテゴリは MTA が内部で実行する文字セット、フォーマット、およびラベルの変換です。この種の変換は CHARSET-CONVERSION マッピングテーブルによって制御されます。

もう 1 つのカテゴリは、ドキュメントコンバータなどの外部サードパーティプログラムおよびサイトで提供するプロシージャに基づいて行うメッセージ添付ファイルの変換です。この種の変換は CONVERSIONS マッピングテーブルによって制御されます。変換を必要とするメッセージは MTA の conversion チャネルに送られ、conversion チャネルによってサイト指定の外部変換プロシージャが実行されます。

MTA の conversions ファイルは、CONVERSION テーブルによってトリガされる外部変換の詳細、および CHARSET-CONVERSION テーブルによってトリガされる内部変換の詳細を指定するために使用されます。

文字セット変換とメッセージフォーマット変換のマッピング

Messaging Server の基本的なマッピングテーブルの 1 つに、文字セット変換テーブルがあります。CHARSET-CONVERSION という名のこのテーブルは、チャネル間における文字セット変換やメッセージフォーマット変換の種類を指定するために使用されます。

多くのシステムでは、文字セットおよびメッセージフォーマットの変換は不必要なため、このテーブルが使われることはありません。しかし、文字セット変換の必要が生じる場合もあります。

CHARSET-CONVERSION マッピングテーブルは、メッセージフォーマットを変換するためにも使用され、多数の非 MIME フォーマットを MIME に変換することができます。MIME エンコーディングおよび構造に変更を加えることもできます。これらのオプションは、MIME または MIME のサブセットだけをサポートするシステムにメッセージを送る際に使用されます。また、MIME フォーマットから非 MIME フォーマットへの変換が可能な場合もあります。

MTA は 2 通りの方法によって CHARSET-CONVERSION マッピングテーブルをプローブします。1 回目のプローブは、MTA がメッセージフォーマットを変換すべきか、また変換する場合はどのフォーマット オプションを使用すべきかを決定するために実行されます (フォーマット変換が指定されていない場合、特定の文字セットへの変換に関するチェックは行われません)。このプローブには、以下のような形式の入力文字列が使用されます。

IN-CHAN=*イン - チャネル*;OUT-CHAN=*アウト - チャネル*;CONVERT

*イン - チャネル*はソースチャネル (メッセージの送信元)、*アウト - チャネル*は宛先チャネル (メッセージの送信先) を示します。一致するものが見つかった場合は、カンマで区切られたキーワードのリストが返されます。キーワードについては、表 8-7 を参照してください。

表 8-7　CHARSET-CONVERSION マッピングテーブルに関連するキーワード

キーワード	説明
Always	conversion チャネルが中継地点である場合も変換を実行します。
Appledouble	Appledouble フォーマット以外の MacMIME フォーマットを Appledouble フォーマットに変換します。
Applesingle	Applesingle フォーマット以外の MacMIME フォーマットを Applesingle フォーマットに変換します。
BASE64	MIME エンコードを BASE64 に切り替えます。
Binhex	Binhex フォーマット以外の MacMIME フォーマット、または Macintosh タイプおよびクリエータ情報を含む部分を Binhex フォーマットに変換します。
Block	message/rfc822 本文部分 (転送メッセージ) をメッセージ内容部分とヘッダ部分に「フラット化」します。
Bottom	message/rfc822 本文部分 (転送メッセージ) をメッセージ内容部分とヘッダ部分に「フラット化」します。

表 8-7　CHARSET-CONVERSION マッピングテーブルに関連するキーワード（続き）

キーワード	説明
Delete	message/rfc822 本文部分 (転送メッセージ) をメッセージ内容部分に「フラット化」し、転送ヘッダを削除します。
Level	重複する multipart レベルをメッセージから削除します。
Macbinary	Macbinary フォーマット以外の MacMIME フォーマット、または Macintosh のタイプやクリエータ情報を含む部分を Macbinary フォーマットに変換します。
No	変換を無効にします。
QUOTED-PRINTABLE	MIME エンコードを QUOTED-PRINTABLE に切り替えます。
Record,Text	テキスト / プレーン部分を 80 バイトのところで折り返します。
Record,Text= n	テキスト / プレーン部分を n バイトのところで折り返します。
RFC1154	メッセージを RFC 1154 フォーマットに変換します。
Top	メッセージ /rfc822 本文部分 (転送メッセージ) をヘッダ部分とメッセージ内容部分に「フラット化」します。
UUENCODE	MIME エンコードを X-UUENCODE に切り替えます。
Yes	変換を有効にします。

文字セットの変換

プローブを行い、メッセージフォーマットを変換する必要があると判断した場合、MTA はメッセージにおける各部分のチェックを開始します。テキスト部分はすべて検出され、その文字セットのパラメータは 2 回目のプローブに使用されます。ただし、変換が必要であると判断されるまで 2 回目のプローブは行われません。2 回目のプローブを行うための入力文字列は以下のとおりです。

IN-CHAN= *チャネル (入力)*;OUT-CHAN= *チャネル (出力)*;IN-CHARSET= *文字セット (入力)*

チャネル (入力) と *チャネル (出力)* の部分は前述の例と同じです。*文字セット* (入力) は該当する部分の文字セット名を示します。この 2 回目のプローブで一致するものがない場合、文字セットの変換は行われません (ただし、フォーマットの変換、たとえば MIME 構造への変換などは、最初のプローブで一致したキーワードに基づいて行われます)。一致するものが見つかった場合は、以下の文字列が返されます。

OUT-CHARSET= *文字セット (出力)*

この場合、文字セット（入力）は*文字セット(出力)*が示す文字セットに変換されます。これらの文字セットは、MTA テーブルディレクトリに含まれる文字セット定義テーブル charsets.txt 内で定義されているものでなくてはなりません。文字セットがこのファイル内で適切に定義されていないと、変換は行われません。しかし、このファイルの中には現在最も利用度の高い数百種の文字セットが定義されているため、特に心配する必要はないでしょう。charsets.txt ファイルの詳細については、imsimta chbuild (UNIX および NT) ユーティリティの説明を参照してください。

すべての条件が満たされると、MTA は文字セットマッピングを作成し、変換を実行します。変換されたメッセージ部分のラベルは、変換後の文字セット名に変更されます。

メッセージフォーマットの変換

前述したように、CHARSET-CONVERSION マッピングテーブルは MIME フォーマットと数種のメーカー独自のメールフォーマット間における添付ファイルの変換にも関わりがあります。

以下の各項では、CHARSET-CONVERSION マッピングテーブルによって可能なその他のメッセージフォーマット変換の例を紹介します。

非 MIME バイナリ添付ファイルの変換

メッセージの処理にかかわるチャネルで CHARSET-CONVERSION が有効になっている場合、MIME 以外非標準のフォーマットを使用しているメッセージ、たとえば Microsoft Mail (MSMAIL) SMTP ゲートウェイからのメッセージは、自動的に MIME フォーマットに変換されます。tcp_local チャネルが存在する場合は通常、このチャネルが Microsoft Mail SMTP ゲートウェイからのメッセージを受信します。以下の例は、ローカルユーザ宛てのメッセージのフォーマット変換を有効にするものです。

```
CHARSET-CONVERSION

   IN-CHAN=tcp_local;OUT-CHAN=ims-ms;CONVERT          Yes
```

すべてのチャネルに対してフォーマット変換を有効にするには、OUT-CHAN=ims-ms を OUT-CHAN=* に変更します。ただし、こうすると tcp_local チャネルからのメールがすべてチェックされることになるため、特定のチャネルに限定する場合より、処理時間が長くなる可能性があります。

さらに、このように無差別な変換を設定すると、エンベロープおよび関連する転送情報部分のみを変換すべきメッセージ (たとえばシステムを通過するだけのメッセージなど) に対してまで広範な変換処理を行うことになりかねません。

MIME を Microsoft Mail SMTP ゲートウェイが理解できるフォーマットに変換するには、MTA 設定ファイルで Microsoft Mail SMTP ゲートウェイ専用のチャネル (tcp_msmail など) を設定し、マッピングファイルに以下の内容を追加します。

```
CHARSET-CONVERSION

   IN-CHAN=*;OUT-CHAN=tcp_msmail;CONVERT         RFC1154
```

MIME ヘッダラベルの変換

ユーザエージェントやゲートウェイによっては、より正確な MIME ヘッダを作成するために十分な情報があるにも関わらず、比較的無益な MIME ヘッダを作成するものもあります。最も良い方法はそのようなエージェントやゲートウェイの設定を適切に変更することですが、それが不可能な場合には有用な MIME ヘッダを構築するように MTA を設定します。

最初のプローブの際に CHARSET-CONVERSION マッピングテーブルが Yes または Always キーワードを返した場合、MTA は conversions ファイルが存在するかどうかを確認します。ファイルが存在する場合、MTA はそのファイルをチェックして RELABEL=1 という記述があるかどうかを確認し、ある場合はそのエントリの指定に従って MIME ラベルを変換します。

たとえば、以下のような CHARSET-CONVERSION テーブルと MTA conversions ファイルのエントリの組み合わせなら、メッセージは tcp_local チャネルから ims-ms チャネルにルーティングされます。さらに、受信時の MIME ラベルが application/octet-stream でファイル名パラメータの拡張子が ps または msw の場合には、それぞれ application/postscript または application/msword という新しいラベルが付けられます (このより正確なラベルは、もともとユーザエージェントやゲートウェイがメッセージに付けておくべきものです)。

CHARSET CONVERSION テーブル

```
CHARSET-CONVERSION

   IN-CHAN=tcp_local;OUT-CHAN=mr_local;CONVERT            Yes
```

MTA CONVERSIONS ファイル エントリ

```
out-chan=ims-ms; in-type=application; in-subtype=octet-stream;
  in-parameter-name-0=name; in-parameter-value-0=*.ps;
  out-type=application; out-subtype=postscript;
     parameter-copy-0=*; relabel=1

out-chan=ims-ms; in-type=application; in-subtype=octet-stream;
  in-parameter-name-0=name; in-parameter-value-0=*.msw;
  out-type=application; out-subtype=msword;
     parameter-copy-0=* relabel=1
```

MacMIME フォーマットの変換

Macintosh ファイルには、Macintosh 特有の情報を含むリソースフォークと、他のプラットフォームで使用できるデータを含むデータフォークの 2 つの部分があります。さらに、Macintosh ファイルの転送には一般に 4 種類の異なるフォーマットが使用されるため、Macintosh ファイルを転送するにはより複雑な処理が必要となります。Applesingle、Binhex、および Macbinary フォーマットは、Macintosh リソースフォークと Macintosh データフォークを 1 つにエンコードしたものから成り立っています。Appledouble フォーマットの場合は、リソースコードとデータフォークがそれぞれ独立した部分として存在しています。このため、Macintosh 以外のプラットフォームでは、リソースフォーク部分を無視してデータフォーク部分のみを使用できる Appledouble が最も便利です。逆に、Macintosh への送信には、他の 3 種類のフォーマットが便利です。

MTA は、これらの Macintosh フォーマット間の変換を実行することができます。MTA は CHARSET-CONVERSION キーワードである Appledouble、Applesingle、Binhex、および Macbinary によって MacMIME フォーマット部分をそれぞれ multipart/appledouble、application/applefile、application/mac-binhex40、または application/macbinary の MIME フォーマットに変換します。さらに、Binhex および Macbinary キーワードは、MIME Content-type: ヘッダに X-MAC-TYPE および X-MAC-CREATOR パラメータを含む特定の非 MacMIME フォーマットへの変換もリクエストします。CHARSET-CONVERSION キーワードの Block は、MTA に対し、MacMIME フォーマット部分のデータフォークのみを抽出し、リソースフォークを破棄するようリクエストします (ただし、このキーワードを使用すると一部の情報が失われるため、Appledouble キーワードの使用をお勧めします)。

たとえば、以下の CHARSET-CONVERSION テーブルは ims-ms チャネルにメッセージを配信する場合に Appledouble フォーマットへの変換を MTA に指示します。

```
CHARSET-CONVERSION

  IN-CHAN=*;OUT-CHAN=l;CONVERT            Appledouble
```

この場合、すでに MacMIME フォーマットが使用されている部分のみが Appledouble フォーマットに変換されます。

Appledouble または Block フォーマットへの変換には、オリジナルの Macintosh ファイルに含まれる Macintosh クリエータおよびタイプ情報に基づいて Appledouble または Block フォーマットの部分のデータフォークに付ける MIME ラベルを指定するために、MAC-TO-MIME-CONTENT-TYPES マッピングテーブルが使用されることもあります。このテーブルのプローブには、「フォーマット | タイプ | クリエータ | ファイル名」形式が使用されます。フォーマットの値には SINGLE、BINHEX、MACBINARY のどれかが指定され、タイプの値には Macintosh タイプ情報 (16 進)、クリエータの値には Macintosh クリエータ情報 (16 進)、そしてファイル名の値には実際のファイル名が指定されます。

たとえば、ims-ms チャネルにメッセージを送る場合に Appledouble フォーマットに変換し、MACBINARY または BINHEX 部分から MS Word または PostScript に変換されたドキュメントに特定の MIME ラベルを付けるには、以下のテーブルが適切です。

```
CHARSET-CONVERSION

  IN-CHAN=*;OUT-CHAN=ims-ms;CONVERT   Appledouble

MAC-TO-MIME-CONTENT-TYPES

! PostScript
    MACBINARY|45505346|76677264|*     APPLICATION/POSTSCRIPT$Y
    BINHEX|45505346|76677264|*        APPLICATION/POSTSCRIPT$Y
! Microsoft Word
    MACBINARY|5744424E|4D535744|*     APPLICATION/MSWORD$Y
    BINHEX|5744424E|4D535744|*        APPLICATION/MSWORD$Y
```

マッピングエントリのテンプレート (右側) に $Y フラグが設定されていない場合、指定したラベルは付けられません。MTA テーブル ディレクトリ内の mac_mappings.sample ファイルには、その他の種類の添付ファイルに関するサンプル エントリが記載されています。

MacMIME 以外のフォーマットが使用されている部分を Binhex または Macbinary フォーマットに変換するには、X-MAC-TYPE および X-MAC-CREATOR MIME Content-type: パラメータ値が必要です。通常これらのパラメータ値を持たない部分にそれを強要するために MIME ラベルの変換を実行することも可能です。

サービス変換

MTA の変換サービス機能をサイト提供のプロシージャと一緒に使用すると、新しい形式のメッセージを作成することができます。前述の CHARSET-CONVERSION や conversion チャネルの場合は個別の MIME メッセージ部分を操作しますが、変換サービスはすべての MIME メッセージ部分 (MIME ヘッダと内容) および MIME メッセージ全体を操作します。また、他の CHARSET-CONVERSION 操作や conversion チャネルの操作とは異なり、変換サービスは独自で MIME 逆アセンブリ、デコード、再エンコード、および再アセンブリを行います。

他の CHARSET-CONVERSION 操作と同様に、変換サービスは CHARSET-CONVERSION マッピング テーブルを通じて有効化されます。CHARSET-CONVESION マッピングテーブルを最初にプローブした結果が Yes または Always キーワードの場合、MTA は conversions ファイルが存在するかどうかをチェックします。conversions ファイルが存在する場合は、ファイル内に SERVICE-COMMAND を指定するエントリがあるかどうかを確認し、ある場合はそれを実行します。conversions ファイルのエントリの形式は以下のとおりです。

```
in-chan=channel-pattern;
  in-type=type-pattern; in-subtype=subtype-pattern;
  service-command=command
```

ここでコマンド文字列に注目してください。これは、たとえばドキュメントコンバータを呼び出すなどのサービス変換を行うために必要なコマンドです。このコマンドが実行されると、変換を必要とするメッセージを含む入力ファイルが処理され、新しいメッセージテキストを含む出力ファイルが生成されます。UNIX では、コマンドが成功した場合には 0、失敗した場合にはその他の値で終了する必要があります。

入力ファイル名、出力ファイル名、メッセージのエンベロープ受取人アドレスを含むファイルの名前などを伝達するためには、環境変数が使われます。これらの 3 つの環境変数は以下のとおりです。

- INPUT_FILE - 処理する入力ファイルの名前
- OUTPUT_FILE - 生成する出力ファイルの名前
- INFO_FILE - エンベロープ受取人アドレスを含むファイルの名前

これらの環境変数の値は、通常の方法でコマンド行に代入することができます。UNIX では、変数名の前に「$」記号を挿入します。

第 9 章

メールのフィルタリングとアクセス制御

この章では、メールサービスへのアクセス制御方法、およびマッピングテーブルと SSR（サーバ側規則）を使ったメールのフィルタリング方法について説明します。

システムレベルで特定の差出人または宛先のメールを拒否したり、特定のユーザ間のメッセージトラフィックに複雑な規制を設けたり、あるいはユーザ自身が受信メッセージのフィルタリング（メッセージヘッダの内容に基づくメッセージ拒否など）を設定したいことがあります。

エンベロープレベルの制御が望ましい場合には、マッピングテーブルを使ってメールをフィルタリングできます。ヘッダベースの制御が望ましい場合、またはユーザによる独自の制御設定には、サーバ側規則を使った一般的なメールのフィルタリングアプローチが適切です。

この章は、以下の 2 つの部分から構成されています。

第 1 部 マッピングテーブル

第 2 部 メールボックスフィルタ

第 1 部 マッピングテーブル

第 1 部には、以下の節があります。

- マッピングテーブルを使ってアクセスを制御する
- アクセス制御はいつ適用されるのか
- アクセス制御マッピングをテストする
- SMTP リレーを追加する
- SMTP リレーブロッキングを設定する
- 多数のアクセスエントリを処理する
- マッピングテーブルのフラグ

マッピングテーブルを使ってアクセスを制御する

メールサービスへのアクセスを制御するには、マッピングテーブルを使用します。マッピングテーブルを使用することにより、誰がメールを送信または受信できるのか、あるいは送受信できるのかを制御することができます。マッピングファイルの一般的な情報および使用方法については、『Messaging Server リファレンスマニュアル』を参照してください。

表 9-1 に、この項で説明しているマッピングテーブルの一覧を示します。

表 9-1　　マッピングテーブル

マッピングテーブル	説明
SEND_ACCESS	エンベロープの From アドレス、エンベロープの To アドレス、ソースチャネルと宛先チャネルに基づいて受信接続をブロックする場合に使用します。書き換え、エイリアス展開などの処理が行われてから To アドレスを調べます。 183 ページの「SEND_ACCESS テーブルと ORIG_SEND_ACCESS テーブル」を参照。
ORIG_SEND_ACCESS	エンベロープの From アドレス、エンベロープの To アドレス、ソースチャネルと宛先チャネルに基づいて受信接続をブロックする場合に使用します。書き換えの後、エイリアス展開の前に To アドレスを調べます。 183 ページの「SEND_ACCESS テーブルと ORIG_SEND_ACCESS テーブル」を参照。
MAIL_ACCESS	SEND_ACCESS テーブルと PORT_ACCESS テーブルを組み合せた情報に基づいて受信接続をブロックする場合に使用します。SEND_ACCESS のチャネルとアドレス、および PORT_ACCESS の IP アドレスとポート番号に関する情報が基準となります。 185 ページの「MAIL_ACCESS マッピングテーブルと ORIG_MAIL_ACCESS マッピングテーブル」を参照。
ORIG_MAIL_ACCESS	ORIG_SEND_ACCESS テーブルと PORT_ACCESS テーブルを組み合せた情報に基づいて受信接続をブロックする場合に使用します。ORIG_SEND_ACCESS のチャネルとアドレス、および PORT_ACCESS の IP アドレスとポート番号に関する情報が基準となります。 185 ページの「MAIL_ACCESS マッピングテーブルと ORIG_MAIL_ACCESS マッピングテーブル」を参照。
FROM_ACCESS	エンベロープの From アドレスに基づいてメールをフィルタリングする場合に使用します。To アドレスとは無関係に処理を行うときにこのテーブルを使用します。 187 ページの「FROM_ACCESS マッピングテーブル」を参照。
PORT_ACCESS	IP 番号に基づいて受信接続をブロックする場合に使用します。 189 ページの「PORT_ACCESS マッピングテーブル」を参照。

最も一般的なのは、MAIL_ACCESS および ORIG_MAIL_ACCESS によるマッピングで、SEND_ACCESS および ORIG_SEND_ACCESS に使用できるアドレスおよびチャネル情報のほか、IP アドレスやポート番号などの PORT_ACCESS マッピングテーブルを介して得られるような情報も得ることができます。

SEND_ACCESS テーブルと ORIG_SEND_ACCESS テーブル

誰がメールを送信または受信できるのか、あるいは送受信できるのかを制御するには、SEND_ACCESS と ORIG_SEND_ACCESS のマッピングテーブルを使用します。アクセスチェックは、メッセージエンベロープの From アドレスおよびエンベロープの To アドレス、あるいはメッセージがどのチャネルから入ってきたか、そしてどのチャネルから出て行くのかという情報に基づいて行われます。

SEND_ACCESS または ORIG_SEND_ACCESS のマッピングテーブルが存在する場合、MTA を通過するメッセージの各受信者を調べるために、MTA は以下のフォーマットの文字列が記述されているテーブルを走査します（縦棒文字「|」の用法に注意してください）。

src-channel|*from-address*|*dst-channel*|*to-address*

src-channel はメッセージをキューに入れるチャネル、*from-address* はメッセージの作成者アドレス、*dst-channel* はキューに入れられたメッセージの宛先となるチャンネル、*to-address* はメッセージの宛先アドレスです。これらの 4 つのフィールド内でアスタリスクを使用すると、そのフィールドの情報（チャネルやアドレスなど）が任意のデータと一致するようになります。

この場合のアドレスは、エンベロープの From アドレスとエンベロープの To アドレスを指しています。SEND_ACCESS の場合は、書き換えやエイリアス展開などの処理が行われた後で、エンベロープの To アドレスが調べられます。ORIG_SEND_ACCESS の場合には、書き換えの後、エイリアス展開の前に、メッセージ作成者により指定されたエンベロープの To アドレスが調べられます。

検索文字列のパターン（テーブルの左側にあるエントリ）が一致すると、そのマッピングの結果出力が調べられます。出力に「$Y」または「$y」フラグが含まれている場合は、その特定の To アドレスに対してメッセージをキューに入れることが許可されます。一方、出力にフラグ「$N」、「$n」、「$F」、あるいは「$f」が含まれている場合には、その特定のアドレスに対してメッセージをキューに入れることが拒否されます。拒否された場合には、オプションの拒否通知テキストをマッピング出力に与えることができます。その文字列は、MTA が発行する拒否通知エラーメッセージに含まれることになります。$N、$n、$F、$f フラグ以外に文字列が出力されない場合は、デフォルトの拒否通知テキストが使用されます。その他のフラグの説明については、204 ページの「マッピングテーブルのフラグ」を参照してください。

次の例は、mail や Pine などの UNIX ユーザエージェントから送られてきたメール、ローカル l チャネルからの入力、および TCP/IP などのチャネルからメッセージをインターネットに出力するケースを示すものです。postmaster 以外のローカルユーザは、インターネットからメールを受信できても送信は許可されていないと仮定します。そのような制御を行う 1 つの手段として、図 9-1 に示している SEND_ACCESS マッピングテーブルの使用があります。このマッピングテーブルの例では、ローカルのホスト名が sesta.com であると想定しています。チャネル名「tcp_*」ではワイルドカードを使って任意の TCP/IP チャネル名 （たとえば tcp_local）と一致するようにしています。

拒否通知メッセージでは、メッセージ内の空白文字の引用符としてドル記号が使われています。ドル記号を使用しないと、拒否通知メッセージが「Internet postings are not permitted.」とならずに「Internet」だけで終ってしまいます。この例では、ローカルのポスティングに関する他のソース （PC ベースのメールシステムであるのか、または POP または IMAP クライアントであるのかなど）は無視されていることに注意してください。

図 9-1 SEND_ACCESS マッピングテーブル

```
SEND_ACCESS

  *|postmaster@sesta.com|*|*     $Y
  *|*|*|postmaster@sesta.com     $Y
  l|*@sesta.com|tcp_*|*          $NInternet$ postings$ are$ not$ \
    permitted
```

注 MTA による拒否通知エラーテキストが、メッセージの差出人であるユーザに対して実際に提示されるかどうかは、メッセージの送信を試行するクライアントに依存します。受信 SMTP メッセージを拒否するために SEND_ACCESS を使用した場合、オプションの拒否通知テキストを含む SMTP 拒否通知コードを MTA が発行することはほとんどありません。その情報に基づいてバウンスメッセージを構築し、オリジナルの差出人に戻すかどうかは、送信 SMTP クライアントによって決まります。

MAIL_ACCESS マッピングテーブルと ORIG_MAIL_ACCESS マッピングテーブル

MAIL_ACCESS マッピングテーブルは、SEND_ACCESS マッピングテーブルと PORT_ACCESS マッピングテーブルのスーパーセットです。つまり、SEND_ACCESS のチャネルとアドレス、および PORT_ACCESS の IP アドレスとポート番号の情報を組み合せたものです。同様に、ORIG_MAIL_ACCESS マッピングテーブルは、ORIG_SEND_ACCESS マッピングテーブルと PORT_ACCESS マッピングテーブルのスーパーセットです。MAIL_ACCESS のプローブ文字列フォーマットは以下のとおりです。

port-access-probe-info|*app-info*|*submit-type*|*send_access-probe-info*

同様に、ORIG_MAIL_ACCESS のプローブ文字列フォーマットは以下のとおりです。

port-access-probe-info|*app-info*|*submit-type*|*orig_send_access-probe-info*

上記の *port-access-probe-info* は、受信 SMTP メッセージの場合、PORT_ACCESS マッピングテーブルプローブに通常含まれているすべての情報から成ります。それ以外の場合は空白です。*app-info* は、SMTP 経由で送信されたメッセージの場合は通常 SMTP となり、それ以外の場合は空白です。*submit-type* は、MAIL、SEND、SAML、あるいは SOML のいずれかであり、メッセージが Messaging Server に送られてきた方法に対応します。通常、この値は、メッセージとして送信されたことを表す MAIL です。SEND、SAML、または SOML は、ブロードキャストリクエスト（あるいはブロードキャストとメッセージを組み合せたリクエスト）が SMTP サーバに送信された場合の値です。MAIL_ACCESS マッピングの *send-access-probe-info* は、SEND_ACCESS マッピングテーブル プローブに通常含まれているすべての情報から成ります。同様に、ORIG_MAIL_ACCESS マッピングの *orig-send-access-probe-info* は、ORIG_SEND_ACCESS マッピングテーブルプローブに通常含まれているすべての情報から成ります。

受信 TCP/IP 接続情報が、チャネルおよびアドレスの情報と同じマッピングテーブルにあると、特定の IP アドレスからのメッセージにどのエンベロープの From アドレスを表示させるのかなど、何らかの制御を課す場合に便利です。また、電子メールの偽造を規制したり、ユーザに対し POP および IMAP クライアントの From アドレス設定を正しく行うように奨励する効果もあります。

たとえば、IP アドレスが 1.2.3.1 および 1.2.3.2 から送信されたメッセージに対してのみエンベロープの From アドレスに vip@siroe.com を表示し、1.2.0.0 サブネット内のシステムから送信されるメッセージにはエンベロープの From アドレスに siroe.com を表示するようなサイトでは、図 9-2 に示す MAIL_ACCESS マッピング テーブルを使用します。

図 9-2　　MAIL_ACCESS マッピングテーブル

```
MAIL_ACCESS

  ! Entries for vip's two systems
  !
  TCP|*|25|1.2.3.1|*|SMTP|MAIL|tcp_*|vip@siroe.com|*|*  $Y
  TCP|*|25|1.2.3.2|*|SMTP|MAIL|tcp_*|vip@siroe.com|*|*  $Y
  !
  ! Disallow attempts to use vip's From: address from other
  ! systems
  !
  TCP|*|25|*|*|SMTP|MAIL|tcp_*|vip@siroe.com|*|*  \
      $N500$ Not$ authorized$ to$ use$ this$ From:$ address
  !
  ! Allow sending from within our subnet with siroe.com From:
  ! addresses
  !
  TCP|*|25|1.2.*.*|*|SMTP|MAIL|tcp_*|*@siroe.com|*|*  $Y
  !
  ! Allow notifications through
  !
  TCP|*|25|1.2.*.*|*|SMTP|MAIL|tcp_*||*|*  $Y
  !
  ! Block sending from within our subnet with non-siroe.com
  ! addresses
  !
  TCP|*|25|1.2.*.*|*|SMTP|MAIL|tcp_*|*|*|*  \
      $NOnly$ siroe.com$ From:$ addresses$ authorized
```

FROM_ACCESS マッピングテーブル

FROM_ACCESS マッピングテーブルは、誰がメールを送信できるのか、また誰が From アドレスを認証アドレスに書き換えることができるのかを制御するのに使用します。

FROM_ACCESS マッピングテーブルの入力プローブ文字列は、MAIL_ACCESS マッピングテーブルのものと似ています。違いは、宛先チャネルとアドレスがなく、場合によっては認証済み差出人情報があることです。したがって、FROM_ACCESS マッピングテーブルが存在する場合は、メッセージが送信されるたびに Messaging Server によって以下のフォーマットで文字列が記述されているテーブルの走査が行われます（縦棒文字「|」の用法に注意してください）。

port-access-probe-info|*app-info*|*submit-type*|*src-channel*|*from-address*|*auth-from*

この場合の *port-access-probe-info* は、受信 SMTP メッセージの場合、PORT_ACCESS マッピングテーブルプローブに通常含まれているすべての情報から成ります。それ以外の場合は空白です。*app-info* は、SMTP 経由で送信されたメッセージの場合は通常 SMTP となり、それ以外の場合は空白です。*submit-type* は、MAIL、SEND、SAML、あるいは SOML のいずれかであり、メッセージが MTA に送られてきた方法に対応します。通常、この値は、メッセージとして送信されたことを表す MAIL です。SEND、SAML、または SOML は、ブロードキャストリクエスト（あるいはブロードキャストとメッセージを組み合せたリクエスト）が SMTP サーバに送信された場合の値です。*src-channel* はメッセージを発する（メッセージをキューに入れる）チャネル、*from-address* はメッセージの作成者アドレスです。*auth-from* は認証済み作成者アドレスですが、その情報がない場合には空白になります。

プローブ文字列のパターン（テーブルの左側にあるエントリ）が一致した場合には、そのマッピングの結果出力が調べられます。出力に「$Y」または「$y」フラグが含まれている場合には、その特定の To アドレスに対しメッセージをキューに入れることが許可されます。出力に「$N」、「$n」、「$F」、あるいは「$f」フラグが含まれている場合には、その特定のアドレスに対しメッセージをキューに入れることが拒否されます。拒否された際には、オプションの拒否通知テキストをマッピング出力に与えることができます。その文字列は、Messaging Server が発行する拒否通知エラーメッセージに含まれることになります。$N、$n、$F、$f フラグ以外に文字列が出力されない場合は、デフォルトの拒否通知テキストが使用されます。その他のフラグの説明については、204 ページの「マッピングテーブルのフラグ」を参照してください。

FROM_ACCESS は、作成者の情報に基づいてメッセージの送信を許可するかどうかを決定できるだけでなく、エンベロープの From アドレスを $J フラグで変更したり、authrewrite チャネルキーワードの効果を $K フラグで変更（受理したメッセージに Sender: ヘッダアドレスを追加）できます。たとえば、以下のマッピングテーブルを使用し、エンベロープの From アドレスを最初のものから認証アドレスに置き換えることができます。

```
FROM_ACCESS

  *|SMTP|*|tcp_local|*|        $Y
  *|SMTP|*|tcp_local|*|*       $Y$J$3
```

特定のソースチャネルの authrewrite をゼロ以外の値に設定する効果を変更するために FROM_ACCESS マッピングテーブルを使用する場合、認証アドレスが文字どおりである限り FROM_ACCESS を使用する必要はありません。

たとえば、tcp_local チャネルに authrewrite 2 を設定する場合は、authrewrite だけでこの効果（文字どおりの認証済みアドレス）を得るのに十分なため、次の FROM_ACCESS マッピングテーブルは不要です。

```
FROM_ACCESS

  *|SMTP|*|tcp_local|*|      $Y
  *|SMTP|*|tcp_local|*|*     $Y$K$3
```

しかし、FROM_ACCESS の本来の目的は、図 9-3 に示すように、より複雑で微妙な変更を行うことにあります。受信メッセージに Sender: ヘッダ行を追加（SMTP AUTH 認証済み送信者アドレスを表示）したいのであれば、authrewrite キーワードだけでも十分です。ただし、SMTP AUTH 認証済み送信者アドレスがエンベロープの From アドレスと異なる場合にのみ、受信メッセージに Sender: ヘッダ行を強制的に追加したいとします（つまり、アドレスが一致した場合には、Sender: ヘッダ行を追加しません）。さらに、エンベロープの From はオプションのサブアドレス情報を含むため、SMTP AUTH およびエンベロープの From アドレスが相違することはほとんどないと考えられます。

図 9-3 FROM_ACCESS マッピングテーブル

```
FROM_ACCESS

  ! If no authenticated address is available, do nothing
  *|SMTP|*|tcp_local|*|              $Y
  ! If authenticated address matches envelope From:, do nothing
  *|SMTP|*|tcp_local|*|$2*          $Y
  ! If authenticated address matches envelope From: sans
  ! subaddress, do nothing
  *|SMTP|*|tcp_local|*+*@*|$2*@$4*  $Y
  ! Fall though to...
  ! ...authenticated address present, but didn't match, so force
  ! Sender: header
  *|SMTP|*|tcp_local|*|*            $Y$K$3
```

PORT_ACCESS マッピングテーブル

ディスパッチャは、IP アドレスおよびポート番号に基づいて、受信接続を許可するかどうかを選択できます。ディスパッチャは、起動時に PORT_ACCESS という名前のマッピングテーブルを探します。このファイルが見つかると、ディスパッチャは接続情報を以下のようにフォーマットします。

TCP| *サーバ - アドレス* | *サーバ - ポート* | *クライアント - アドレス* | *クライアント - ポート*

ディスパッチャは、すべての PORT_ACCESS マッピングエントリを照合します。マッピングの結果に「$N」または「$F」が含まれている場合には、接続を即座に終了します。それ以外の場合は、接続を許可します。「$N」または「$F」の後に拒否通知メッセージが続くことがあります。メッセージがある場合には、接続を断つ前にそのメッセージが送り返されます。メッセージが送り返される前に、その文字列には CRLF ターミネータが追加されることに注意してください。

「$<」フラグにオプションの文字列が続いており、マッピングプローブが一致しなかった場合は、Messaging Server が文字列を syslog （UNIX）またはイベントログ （NT）に送ります。「$>」フラグにオプションの文字列が続いており、アクセスが拒否された場合は、Messaging Server が文字列を syslog （UNIX）またはイベントログ （NT）に送ります。LOG_CONNECTION MTA オプションのビット 1 が設定されており、かつ「$N」フラグが設定されて接続が拒否されている場合は、「$T」フラグを指定することにより「T」エントリが接続ログに書き込まれるようになります。LOG_CONNECTION MTA オプションのビット 4 が設定されている場合は、サイトが提供するテキストを PORT_ACCESS エントリに提供し、「C」接続ログエントリに含めることが可能です。そのようなテキストを指定するには、エントリの右側に縦棒「|」を 2 つと適切なテキストを挿入します。表 9-2 に、使用可能なフラグを示します。

表 9-2　PORT_ACCESS マッピングフラグ

フラグ	説明
$Y	アクセスを許可します。
フラグと引数 （引数の読み取り順序 +）	
$< 文字列	プローブが一致する場合、文字列を syslog （UNIX）またはイベントログ （NT）に送ります。
$> 文字列	アクセスが拒否された場合、文字列を syslog （UNIX）またはイベントログ （NT）に送ります。
$N 文字列	アクセスを拒否し、オプションのエラーテキスト文字列を送ります。
$F 文字列	「$N 文字列」と同じ。アクセスを拒否し、オプションのエラーテキスト文字列を送ります。
$T テキスト	LOG_CONNECTION MTA オプションのビット 1 が設定されており、かつ「$N」フラグが設定されて接続が拒否されている場合、「$T」フラグを指定することにより、「T」エントリが接続ログに書き込まれるようになります。オプションのテキスト （2 つの縦棒「|」に続けて挿入）は、接続ログエントリに含めることができます。

+ 複数のフラグと引数を使用する場合には、引数を縦棒「|」で区切り、この表に示されている順序で引数を配置してください。

たとえば、次のマッピングは、単一のネットワークからポート 25 （標準の SMTP ポート）への SMTP 接続だけを許可します。説明テキストは送らずに特定のホストを拒否します。

```
PORT_ACCESS

  TCP|*|25|192.123.10.70|*  $N500
  TCP|*|25|192.123.10.*|*   $Y
  TCP|*|25|*|*              $N500$ Bzzzt$ thank$ you$ for$ \
     playing.
```

PORT_ACCESS マッピングテーブルを変更した場合は、その変更内容を適用するために、ディスパッチャを再起動する必要があります。コンパイルした MTA 設定ファイルを使用している場合は、変更内容を適用するために、先に設定ファイルをリコンパイルしてください。

PORT_ACCESS マッピングテーブルは、特に IP ベースの拒否通知を処理するためのものです。電子メールアドレスレベルでの一般的な制御には、SEND_ACCESS または MAIL_ACCESS マッピングテーブルが適しています。

MTA への IP アドレス接続を制限する

PORT_ACCESS マッピングテーブルで conn_throttle.so 共有ライブラリを使用すると、特定の IP アドレスが MTA に接続する頻度を制限できます。特定の IP アドレスによる接続の制限は、サービス拒否攻撃などによる不正な接続を防ぐ場合などに便利です。

conn_throttle.so は PORT_ACCESS マッピングテーブルで使用されるライブラリで、特定の IP アドレスからの過度の MTA 接続を制限するためのものです。以下に示すように、設定オプションはすべて、接続スロットル共有ライブラリ (conn_throttle.so) に対するパラメータとして指定します。

$[<*server-root*>/lib/conn_throttle.so,throttle,IP-address,max-rate]

IP-address は、ピリオドで区切られた数字によるリモートシステムのアドレスです。max-rate は、この IP アドレスに対して許可される 1 分当たりの最大接続数です。

throttle の代わりに throttle_p をルーチン名として使用すると、ペナルティが適用されます。throttle_p を使用すると、過去に過度の接続があった場合、接続が拒否されます。たとえば、最大接続数が 100 で、1 分間に 250 の接続が試みられた場合、最初の 100 個の接続が終わってから次の 1 分が始まるまでの間だけでなく、次の 1 分間もサイトへの接続がブロックされます。つまり、1 分が経過するごとに、その 1 分間に試行された接続数と 1 分当たりの許容最大接続数とが比較され、試行接続数が許容最大接続数より大きいと判断された場合、そのリモートシステムはブロックされます。

指定した IP アドレスの接続が 1 分当たりの最大接続数を超えなかった場合、共有ライブラリのコールアウトに失敗します。

1 分当たりの最大接続数を超過した場合、共有ライブラリのコールアウトは成功しますが、値は返されません。この動作は $C と $E の組み合わせによって制御されます。以下に、その例を示します。

```
PORT_ACCESS

  TCP|*|25|*|*    \
$C$[<server-root>/lib/conn_throttle.so,throttle,$1,10]    \
$N421$ Connection$ not$ accepted$ at$ this$ time$E
```

説明 :

$C は、次のテーブルエントリからマッピングプロセスを続行させます。つまり、現在のエントリの出力文字列を、マッピングプロセスの新しい入力文字列として使用します。

`$[<server-root>/lib/conn_throttle.so,throttle,$1,10]` はライブラリの呼び出しで、`throttle` はライブラリルーチン、`$1` はサーバの IP アドレス、10 は 1 分当たりの接続数のしきい値です。

$N421$ Connection$ not$ accepted$ at$ this$ time は、アクセスを拒否して、「現在接続は受け付けられません」という旨のメッセージとともに 421 SMTP コード (一時的な接続拒否) を返します。

$E は、マッピングプロセスをその時点で終了させます。また、現在のエントリからの出力文字列をマッピングプロセスの最終結果として使用します。

アクセス制御はいつ適用されるのか

Messaging Server は、可能な限り早い段階でアクセス制御マッピングを調べます。実際にどの時点で行われるかは、使用する電子メールプロトコルによって異なります。これは、必要な情報をいつ読み取れるのかという点に依存しているためです。

SMTP プロトコルの場合、`FROM_ACCESS` による拒否は、送信側が受信者情報やメッセージデータを送信する前に、MAIL FROM: コマンドへの応答として行われます。`SEND_ACCESS` あるいは `MAIL_ACCESS` による拒否は、送信側がメッセージデータを送信する前に、RCPT TO: コマンドへの応答として行われます。SMTP メッセージが拒否された場合は、Messaging Server がメッセージデータを受信せずメッセージデータを確認しないため、そのような拒否を処理するためのオーバーヘッドが最小になります。

複数のアクセス制御マッピングテーブルが存在する場合、Messaging Server はそれらをすべて調べます。したがって、`FROM_ACCESS`、`SEND_ACCESS`、`ORIG_SEND_ACCESS`、`MAIL_ACCESS`、および `ORIG_MAIL_ACCESS` のすべてのマッピングテーブルが使用されることがあります。

アクセス制御マッピングをテストする

imsimta test -rewrite ユーティリティ (特に -from、-source_channel、および -destination_channel オプション) は、アクセス制御マッピングのテストに役立ちます。例として、図 9-4 に、サンプルの SEND_ACCESS マッピングテーブルとその結果としてのプローブを示します。

図 9-4　　サンプルの SEND_ACCESS マッピングテーブルおよびプローブ

マッピングテーブル

```
SEND_ACCESS

  tcp_local|friendly@siroe.com|l|User@sesta.com     $Y
  tcp_local|unwelcome@varrius.com|l|User@sesta.com  $NGo$ away!
```

プローブ

```
$ TEST/REWRITE/FROM="friendly@siroe.com" -
_$  /SOURCE=tcp_local/DESTINATION=l User@sesta.com
...
Submitted address list:
  l
    User (SESTA.COM) *NOTIFY FAILURES* *NOTIFY DELAYS* Submitted
notifications list:


$ TEST/REWRITE/FROM="unwelcome@varrius.com" -
_$  /SOURCE=tcp_local/DESTINATION=l User@sesta.com
...
Submitted address list:
Address list error -- 5.7.1 Go away! User@sesta.com

Submitted notifications list:
```

SMTP リレーを追加する

iPlanet Messaging Server は、デフォルトで、試行された SMTP リレーをブロックするように設定されています。つまり、認証されていない外部ソースから外部アドレスへのメッセージの送信は拒否されます (外部システムとは、サーバがあるホスト以外のシステムのことです)。他のシステムはすべて外部システムとみなされることから、SMTP リレーをブロックするこのデフォルト設定はかなり厳しいものだと言えます。

IMAP クライアントと POP クライアントが システムの SMTP サーバを経由して外部アドレス宛てのメッセージを送信しようとしても、SMTP AUTH (SASL) を使って認証を受けていない場合は、そのメッセージ送信は拒否されます。このため、自分の内部システムや内部サブネットが外部システムとみなされないように (そこからのリレーが必ず許可されるように)、設定を変更した方がよいでしょう。

どのシステムとサブネットを内部とみなすかは、通常 INTERNAL_IP マッピングテーブルで制御されます。このテーブルは *<instance-root>*`/imta/config/mappings` ファイルにあります。

たとえば、IP アドレスが 123.45.67.89 の iPlanet Messaging Server システムの場合、デフォルトの INTERNAL_IP マッピングテーブルは次のようになります。

```
INTERNAL_IP

   $(123.45.67.89/32)   $Y
   127.0.0.1   $Y
   *   $N
```

ここでは、$(IP-pattern/signicant-prefix-bits) 構文を使った 1 つ目のエントリは、32 ビットの 123.45.67.89 すべてに一致する IP アドレスが、内部として一致および認識されるように指定しています。2 番目のエントリは、ループバック IP アドレス 127.0.0.1 を内部として認識します。最後のエントリは、その他のすべての IP アドレスを外部として認識されるように指定しています。すべてのエントリの先頭には、少なくとも 1 つの空白文字が必要です。

最後の $N エントリの前に別の IP アドレスを指定して、エントリを追加することもできます。これらのエントリには、必ず左側に IP アドレスまたはサブネット (サブネットの指定には $(.../...) 構文を使用) を指定し、右側に $Y を入力します。また、既存の $(.../...) エントリを編集して、より広範囲のサブネットを受け入れるようにすることもできます。

たとえば、このサンプルのサイトがクラス C ネットワークで、すべての 123.45.67.0 サブネットを保持している場合は、アドレス照合に使用されるビット数を変更して 1 つ目のエントリを変更する必要があります。次に示すマッピングテーブルでは、32 ビットが 24 ビットに変更されています。これにより、クラス C ネットワークのすべてのクライアントが、SMTP リレーサーバを介してメールをリレーできるようになります。

```
INTERNAL_IP

   $(123.45.67.89/24)   $Y
   127.0.0.1   $Y
   *   $N
```

また、サイトが 123.45.67.80 ～ 123.45.67.99 の範囲の IP アドレスだけを保持している場合は、次のようにします。

```
INTERNAL_IP

! Match IP addresses in the range 123.45.67.80-123.45.67.95
   $(123.45.67.80/28)   $Y
! Match IP addresses in the range 123.45.67.96-123.45.67.99
   $(123.45.67.96/30)   $Y
   127.0.0.1   $Y
   *   $N
```

IP アドレスが特定の $(.../...) テストの条件に一致するかどうかを検査するには、*<InstanceRoot>*/imsimta test -match ユーティリティが便利です。このユーティリティは、さまざまな IP アドレス入力に対して、INTERNAL_IP マッピングテーブルが望ましい結果を返すかどうかを検査したいときに役立ちます。

INTERNAL_IP マッピングテーブルを編集したら、必ず *<InstanceRoot>*/imsimta restart コマンド (コンパイルされた設定で実行しない場合) または *<InstanceRoot>*/imsimta refresh コマンド (コンパイルされた設定で実行する場合) を実行して、変更が適用されるようにします。

ファイルのマッピングと一般的なマッピングテーブルの形式および imsimta コマンドラインユーティリティの詳細については、『iPlanet Messaging Server リファレンスマニュアル』を参照してください。

外部サイトの SMTP リレーを許可する

前の項で説明したように、内部 IP アドレスはすべて INTERNAL_IP マッピングテーブルに追加しなければなりません。同一組織内または信用できるシステムやサイトがあり、そこからの SMTP リレーを許可したい場合は、そのシステムやサイトを自分の内部 IP アドレスとともに INTERNAL_IP マッピングテーブルに指定する方法が最も簡単です。

ただし、これらを実際の内部システムやサイトと区別したい場合 (たとえば、ログや他の制御目的のために 実際の内部システムと、リレーを許可する外部システムを区別したい場合) は、別の方法でシステムを設定することもできます。

1 つのアプローチとして、これらの外部システムからメッセージを受信する特別のチャネルを設定する方法があります。この設定を行うには、既存の *tcp_internal* チャネルに類似した *tcp_friendly* チャネルを *tcp_friendly-daemon* という正式のホスト名を使って作成します。また、リレーを許可する外部システムの IP アドレスをリストした、INTERNAL_IP マッピングテーブルに似た FRIENDLY_IP マッピングテーブルを作成します。そして、現在の書き換え規則のすぐ後に新しい書き換え規則を追加します。現在の書き換え規則は次のようになっています。

```
! Do mapping lookup for internal IP addresses []
$E$R${INTERNAL_IP,$L}$U%[$L]@tcp_intranet-daemon
```

次の新しい書き換え規則を追加します。

```
! Do mapping lookup for "friendly", non-internal IP addresses []
$E$R${FRIENDLY_IP,$L}$U%[$L]@tcp_friendly-daemon
```

もう 1 つのアプローチとして、ORIG_SEND_ACCESS マッピングテーブルの最後にある $N エントリの前に、次の形式の新しいエントリを追加する方法があります。

```
  tcp_local|*@siroe.com|tcp_local|*    $Y
```

siroe.com は外部アドレスのドメインです。また、次に示すように、ORIG_MAIL_ACCESS マッピングテーブルにエントリを追加します。

```
ORIG_MAIL_ACCESS

   TCP|*|25|$(match-siroe.com-IP-addresses)|*|SMTP|MAIL|     \
tcp_local|*@siroe.com|tcp_local|*     $Y
   TCP|*|*|*|*|SMTP|MAIL|tcp_local|*|tcp_local|*    $N
```

$(...) の IP アドレス構文は、前の項で説明した構文と同じです。ORIG_SEND_ACCESS の検査は、アドレスに問題がない限り成功します。ここでは、より厳密な検査、つまり IP アドレスが siroe.com の IP アドレスに一致した場合にのみ成功する ORIG_MAIL_ACCESS 検査を行います。

SMTP リレーブロッキングを設定する

アクセス制御マップを使うことによって、Messaging Server システムが SMTP メールのリレーに利用されるのを防ぐことができます。たとえば、あなたのメールシステムを利用して何百、何千ものインターネットメールボックスにジャンクメールをリレーしようとする不正操作を阻止できます。

Messaging Server のデフォルトでは、ローカルの POP ユーザおよび IMAP ユーザによるリレーを含むすべての SMTP リレー操作が防止されます。

不正なリレーをブロックする一方、正しいローカルユーザによるリレーを許可するには、2 つのクラスのユーザを識別するように Messaging Server を設定する必要があります。たとえば、POP または IMAP を使用するローカルユーザの場合、SMTP リレー操作は Messaging Server に依存しています。

SMTP リレーを阻止するには、以下のいずれかの操作を行う必要があります。

- 内部メールと外部メールを識別する
- 認証ユーザのメールを識別する
- メールのリレーを防止する

内部のホストとクライアントによる SMTP リレーを可能にするには、INTERVAL_IP マッピングテーブルに内部 IP アドレスまたはサブネットを追加します。

内部メールと外部メールを識別する

メールのリレーアクティビティをブロックするためには、まず、メールが同じサイトで発信された内部メールなのか、あるいはインターネットからシステムを経由して再びインターネットに戻っていく外部メールなのかを識別できなければなりません。そして、前述のクラスを許可し、後述のクラスをブロックする必要があります。この識別は、インバウンドの SMTP チャネルに switchchannel キーワードを使うことで実現できます。通常、このチャネルは tcp_local です。

switchchannel キーワードは、SMTP サーバが受信 SMTP 接続の実際の IP アドレスを調べるようにするものです。この IP アドレスは、Messaging Server によって、ドメイン内の SMTP 接続とドメイン外の接続とを識別するために書き換え規則と共に使用されます。その後、この情報は、内部と外部のメッセージトラフィックを分離するために使用されます。

以下の手順では、サーバが内部と外部のメッセージトラフィックを識別できるように MTA 設定を変更する方法について説明します。

1 設定ファイルで、ローカルストアチャネルを見つけます。次の例のように、ローカルチャネルの直前に defaults チャネルを追加し、noswitchchannel キーワードを挿入します。

```
! final rewrite rules
defaults noswitchchannel
! Local store
ims-ms ...
```

既に設定ファイルの該当位置に defaults チャネルがある場合は、そこにキーワード noswitchchannel だけを挿入します。

2 受信 TCP/IP チャネルを変更し、switchchannel および remotehost キーワードを指定します。例：

```
tcp_local smtp single_sys mx switchchannel remotehost
TCP-DAEMON
```

3 受信 TCP/IP チャネル定義の後に、同様の新しいチャネルを別の名前で追加します。以下に例を示します。

```
tcp_internal smtp single_sys mx allowswitchchannel routelocal
TCP-INTERNAL
```

routelocal チャネルキーワードは、ソースルートアドレスを短絡的に書き換えるために使用されます。これにより、明示されたソースルートアドレスを経由した内部 SMTP ホストのループによるリレー試行がブロックされます。

4 ドメインのルートホストと IP アドレスの書き換え規則を tcp_internal チャネルに追加します。たとえば、ドメイン名が sesta.com で、ドメインの IP 番号が [a.b.subnet] の範囲である場合は、設定ファイルの冒頭に以下の書き換え規則を追加します。

```
.sesta.com      $U%$H$D@TCP-INTERNAL
[a.b.]           $U%[a.b.$L]@TCP-INTERNAL$E$R
```

このように設定を変更すると、ドメイン内で生成された SMTP メールは tcp_internal チャネルから入ってくるようになります。それ以外の SMTP メールは、tcp_local チャネルから入ってきます。したがって、メールが入ってくるチャネルに基づいて内部と外部のメールを識別できます。

さて、この設定はどのように機能するのでしょうか。ここで最も重要な要素は switchchannel キーワードです。手順 2 で、このキーワードが tcp_local チャネルに適用されています。このキーワードにより、SMTP サーバにメッセージが入ってくると、サーバが受信接続のソース IP アドレスを調べるようになります。サーバは、受信接続のリテラル IP アドレスのリバースポインティングのエンベロープ書き換えを試行し、関連するチャネルを探します。その書き換えがローカルホストと一致する場合は、手順 4 で追加した書き換え規則に従って、手順 3 で追加された tcp_internal チャネルに書き換えられます。

tcp_internal チャネルは allowswitchchannel キーワードでマークされているため、メッセージは tcp_internal チャネルに切り替えられて、そのチャネルから入ってきます。外部ソースから入ってくるメッセージの IP アドレスは内部ソースに対応しません。その場合、リバースポインティングのエンベロープ書き換えは、tcp_local チャネルあるいはその他のチャネルに対して書き換えを行います。ただし、tcp_internal チャネルに対する書き換えは行われません。それ以外のチャネルは手順 1 で noswitchchannel とマークされているため、メッセージは別のチャネルに切り替えられず、tcp_local チャネルのまま処理されます。

注　「tcp_local」という文字列を使用するマッピングテーブルまたは変換ファイルのエントリは、必要に応じて「tcp_*」または「tcp_internal」に変更する必要があるかもしれません。

認証ユーザのメールを識別する

サイトには、物理的にネットワークの一部ではない「ローカル」のクライアントユーザが存在することがあります。これらのユーザがメールを送信すると、メッセージの送信は外部 IP アドレス（任意のインターネットサービスプロバイダ (ISP) など）から入ってきます。ユーザが SASL 認証を処理できるメールクライアントを使用している場合には、外部接続と認証接続とを識別できます。その結果に基づいて、認証ユーザによる送信を許可し、認証されていないユーザによるリレー送信試行を拒否できます。認証されているかどうかに基づく接続の識別は、インバウンドの SMTP チャネル（通常、tcp_local チャネル）に saslswitchchannel キーワードを使うことで実現できます。

saslswitchchannel キーワードはチャネルの切り替え先を示す引数をとり、SMTP の差出人が認証されると、送信メッセージが指定した切り替え先チャネルから入ってくるようになります。

認証ユーザによる送信であるかどうかを識別するには、以下のようにします。

1 設定ファイルに新しい TCP/IP チャネル定義を別の名前で追加します。以下に例を示します。

```
tcp_auth smtp single_sys mx mustsaslserver noswitchchannel
TCP-INTERNAL
```

このチャネルでは、通常のチャネル切り替えは行われません。それよりも前のデフォルト行で、noswitchchannel が明示あるいは暗黙に指定されているはずです。このチャネルには mustsaslserver が必要です。

2 次の例のように、maysaslserver と saslswitchchannel tcp_auth を追加することにより、tcp_local チャネルを変更します。

```
tcp_local smtp mx single_sys maysaslserver saslswitchchannel
tcp_auth \
switchchannel
|TCP-DAEMON
```

この設定では、ローカルのパスワードによって認証が可能なユーザが送信した SMTP メールは tcp_auth チャネルから入ってくるようになります。認証されていない SMTP メールが内部ホストから送信された場合、そのメールは tcp_internal から入ってきます。それ以外の SMTP メールすべては、tcp_local から入ってきます。

メールのリレーを防止する

次の例では、無許可のユーザが送信した SMTP メールのリレーをシステムが中継しないように設定しています。まず、ローカルユーザによる SMTP メールのリレーは許可することを念頭におきます。たとえば、POP ユーザおよび IMAP ユーザは、メールの送信に Messaging Server を使います。ローカルユーザには、メッセージが内部 IP アドレスから入ってくる物理的なローカルユーザのほか、ローカルユーザとして認証され得るリモートユーザも含まれます。

サーバにおけるリレーを阻止しなければならないのは、不特定多数のインターネット利用者からのメッセージです。次に説明する設定では、これらのユーザクラスを識別して特定のクラスだけをブロックできます。特に、tcp_local チャネルから入り、同一のチャネルから出るメールをブロックします。そのためには、ORIG_SEND_ACCESS マッピング テーブルを使用します。

ORIG_SEND_ACCESS マッピングテーブルは、ソースチャネルと宛先チャネルに基づいてトラフィックをブロックするために使用できます。ここでは、tcp_local チャネルから入り、同一チャネルから出るトラフィックをブロックします。これは、次の ORIG_SEND_ACCESS マッピングテーブルで実現できます。

```
ORIG_SEND_ACCESS

   tcp_local|*|tcp_local|*        $NRelaying$ not$ permitted
```

この例では、メッセージが tcp_local チャネルから入り、同一のチャネルから出ることは許可されないことを示しています。つまり、このエントリを使用すると、外部からのメールを SMTP サーバで中継してインターネットに転送する処理を禁じることができます。

SEND_ACCESS マッピングテーブルではなく ORIG_SEND_ACCESS マッピングテーブルを使用するのは、ims-ms チャネルに元々一致するアドレスにブロックを適用するのではないからです （アドレスは、エイリアスまたはメーリングリストの定義を介して展開し、外部アドレスとなることがあるためです）。SEND_ACCESS マッピングテーブルでは、外部の利用者が外部ユーザに展開するメーリング リストにメールを送信したり、外部アドレスにメッセージを転送するユーザにメールを送信できるようにするのは困難です。

SMTP ポートへのローカルホスト送信を許可する

ここでは、前述の SMTP リレーブロック手法をさらに追求します。

特定のサイトでは、クライアントが動作しているシステムから SMTP ポートへの送信を禁止したいことがあります。たとえば、正当な手段でそのような処理が行われない場合は、その送信をブロックすることで、偽造電子メールの経路を遮断できます。

しかし、他のサイトでは、システムの SMTP ポートに TCP/IP 接続を確立することによりメッセージの送信を許可している場合があるかもしれません。たとえば、サードパーティによるメーリングリストエクスパンション （Messaging Server 独自のメーリングリストエクスパンション以外）の中には、そのような方法で機能するものがあります。

さらに、そのような応用では設定を簡素化するために、システムのドメイン名ではなく、LOCALHOST や [127.0.0.1] などのようなループバック名やアドレスを使って接続することがあります。基礎となる TCP/IP パッケージによっては、受信接続が、システムで特定されているドメイン名や IP アドレスから入ってくるのではなく、LOCALHOST や [127.0.0.1] から入ってくるように見えることもあります。

単に内部と外部の接続を識別する方法 (前述) では、ホストシステム上のクライアントからの SMTP 送信は tcp_local チャネルから入ってくるようになります。したがって、tcp_local から tcp_local へのメッセージトラフィックが禁止されると、そのような方法でメッセージを送信しようとするユーザやアプリケーションは外部アドレス宛にメッセージを送信できなくなります。

そのような送信を「内部」送信として処理するには （たとえば、SMTP リレーブロッキングが適用されたにもかかわらず、サードパーティによるメーリングリストアプリケーションの実行を許可する場合）、さらに設定を追加しなければなりません。

MTA 設定ファイルの冒頭に、ローカルホスト名 （基礎となる TCP/IP パッケージが接続ソースのどこを見るかによって異なるが、LOCALHOST または [127.0.0.1]）の書き換え規則を以下の形式で追加します。

```
localhostname           $E$R$U%localhostname@TCP-INTERNAL
[localhostipnumber]     $E$R$U%localhostname@TCP-INTERNAL
LOCALHOST               $E$R$U%localhostname@TCP-INTERNAL
[127.0.0.1]             $E$R$U%localhostname@TCP-INTERNAL
```

localhostname は ims-ms チャネルの正式なホスト名です。

これらの書き換え規則内の「$E」および「$R」コントロールシーケンスは、エンベロープの From: アドレス書き換えの効果を制限するもので、ローカルシステム宛のアドレスには標準の書き換え規則が適用されることを意味します。しかし、switchchannel 書き換えもこれらの規則を使用するため、メッセージをシステムからそのシステム自体の SMTP ポートに送る内部送信が可能となります。

SMTP リレーブロッキングに対する RBL 検査を含む DNS 検索を使用する

iPlanet Messaging Server には、配信および転送するために受け入れたすべてのメールが、有効な DNS 名を持つアドレスから送信されたものであるかどうかを確認するさまざまな方法があります。最も簡単な方法は、tcp_local チャネルに mailfromdnsverify チャネルキーワードを割り当てることです。

また iPlanet Messaging Server には、dns_verify というプログラムが用意されています。このプログラムは、配信や転送のために受け入れたすべてのメールが有効な DNS 名を持つアドレスから送信されたものであるかどうかを、次に示す ORIG_MAIL_ACCESS の規則を使って確認します。

```
ORIG_MAIL_ACCESS

  TCP|*|*|*|*|SMTP|MAIL|*|*@*|*|*     \
     $[<server-root>/bin/msg/imta/lib/dns_verify,      \
    dns_verify,$6|$$y|$$NInvalid$ host:$ $$6$ -$ %e]
```

上の例に示されている改行は、このようなマッピングエントリの構文では非常に重要な意味を持ちます。バックスラッシュ (または円記号) は、その行が次の行に続いていることを意味しています。

もう 1 つの UBE 対策として、dns_verify イメージを使用して、着信した接続が RBL (Realtime Blackhole List)、MAPS (Mail Abuse Prevention System)、DUL (Dial-up User List)、ORBS (Open Relay Behavior-modification System) などのリストに対して有効かどうか検査することもできます。また、新しい mailfromdnsverify キーワードのように、dns_verify コールアウトを行わなくてもこれらの検査を実行できる簡単な方法があります。それは dispatcher.cnf ファイルで DNS_VERIFY_DOMAIN オプションを使用する方法です。たとえば、[SERVICE=SMTP] セクションで、オプションのインスタンスを検査対象のリストに設定します。

```
[SERVICE=SMTP]
PORT=25
! ...rest of normal options...
DNS_VERIFY_DOMAIN=rbl.maps.vix.com
DNS_VERIFY_DOMAIN=dul.maps.vix.com
!...etc...
```

この方法の短所は、内部ユーザからのメッセージを含む、通常の SMTP 受信メッセージすべてに対して検査が行われるということです。このため効率が下がり、インターネット接続が切断された場合に問題が発生することがあります。この他の方法として、PORT_ACCESS マッピングテーブル、または ORIG_MAIL_ACCESS マッピングテーブルから dns_verify をコールアウトする方法があります。PORT_ACCESS マッピングテーブルでは、先頭から数えていくつかのエントリでは、ローカルの内部 IP アドレスまたはメッセージ送信者の検査を行わないようにし、それ以降のエントリではすべての項目について検査を行うようにすることができます。また、ORIG_MAIL_ACCESS マッピングテーブルでは、tcp_local チャネルに着信したメッセージのみを検査することにした場合、内部システムまたはクライアントからのメッセージに対する検査を省略することになります。以下に、dns_verify へのエントリポイントを使用した例を示します。

```
PORT_ACCESS

! Allow internal connections in unconditionally
  *|*|*|*|*  $C$|INTERNAL_IP;$3|$Y$E
! Check other connections against RBL list
  TCP|*|25|*|*    \
      $C$[<server-root>/bin/msg/imta/lib/dns_verify,  \
dns_verify_domain_port,$1,rbl.maps.vix.com]EXTERNAL$E


ORIG_MAIL_ACCESS

  TCP|*|25|*|*|SMTP|*|tcp_local|*@*|*|*    \
      $C$[<server-root>/bin/msg/imta/lib/dns_verif,     \
      dns_verify_domain,$1,rbl.maps.vix.com]$E
```

多数のアクセスエントリを処理する

マッピングテーブルに非常に多くのエントリを使用するサイトでは、マッピングテーブルを組織化し、特定の参照に対して一般的なデータベースを呼び出す一般的なワイルドカードエントリを利用するとよいでしょう。特定の参照に対し、2 ～ 3 件のマッピングテーブルエントリから一般的なデータベースを呼び出すほうが、数多くのエントリを直接マッピングテーブルで処理するよりもはるかに効率的です。

その一例として、誰がインターネットの電子メールを送信または受信できるのかをユーザごとに制御するサイトがあります。そのような制御は、ORIG_SEND_ACCESS などのアクセスマッピングテーブルを使って簡単に適用できます。この場合、一般的なデータベースに特定の情報（たとえば特定のアドレスなど）をまとめて保存し、マッピングテーブルのエントリで呼び出すように設定すれば、効率と性能がかなり向上します。

たとえば、図 9-5 のマッピングテーブルを見てください。

図 9-5　　ORIG_SEND_ACCESS マッピングテーブル

```
ORIG_SEND_ACCESS

  ! Users allowed to send to Internet
  !
  *|adam@siroe.com|*|tcp_local    $Y
  *|betty@siroe.com|*|tcp_local   $Y
  ! ...etc...
  !
  ! Users not allowed to send to Internet
  !
  *|norman@siroe.com|*|tcp_local  $NInternet$ access$ not$
      permitted
  *|opal@siroe.com|*|tcp_local    $NInternet$ access$ not$
      permitted
  ! ...etc...
  !
  ! Users allowed to receive from the Internet
  !
  tcp_*|*|*|adam@siroe.com        $Y
  tcp_*|*|*|betty@siroe.com       $Y
  ! ...etc...
  !
  ! Users not allowed to receive from the Internet
  !
  tcp_*|*|*|norman@siroe.com      $NInternet$ e-mail$ not$
      accepted
  tcp_*|*|*|opal@siroe.com        $NInternet$ e-mail$ not$
      accepted
  ! ...etc...
```

このように、ユーザごとに個々のエントリを記述したマッピングテーブルを使用するのではなく、より効率的な設定（何百、何千件ものユーザを効率的に処理できる設定）を次の図 9-6 に示します。この図には、一般的なデータベースエントリと ORIG_SEND_ACCESS マッピングテーブルが示されています。

図 9-6 データベースエントリとマッピングテーブルの例

データベースエントリ

```
SEND|adam@domain.com    $Y
SEND|betty@domain.com   $Y
! ...etc...
SEND|norman@domain.com  $NInternet$ access$ not$ permitted
SEND|opal@domain.com    $NInternet$ access$ not$ permitted
! ...etc...
RECV|adam@domain.com    $Y
RECV|betty@domain.com   $Y
! ...etc...
RECV|norman@domain.com  $NInternet$ e-mail$ not$ accepted
RECV|opal@domain.com    $NInternet$ e-mail$ not$ accepted
```

マッピングテーブル

```
ORIG_SEND_ACCESS

  ! Check if may send to Internet
  !
  *|*|*|tcp_local       $C${SEND|$1}$E
  !
  ! Check if may receive from Internet
  !
  tcp_*|*|*|*           $C${RECV|$3}$E
```

この例では、一般的なデータベースの左側に記述した文字列「SEND|」および「RECV|」を使用（マッピングテーブルで生成される一般的なデータベースプローブ）することにより、2 種類のプローブを区別しています。一般的なデータベースプローブを「$C」および「$E」フラグで囲むのは、マッピングテーブルから一般的なデータベースを呼び出すコールアウトに特有の方法です。

この例では、単純なマッピングテーブルプローブが一般的なデータベースのエントリを参照するケースを示しています。より複雑なプローブのマッピングテーブルでも一般的なデータベースの使用による効果を得ることができます。

マッピングテーブルのフラグ

表 9-3 に、SEND_ACCESS、ORIG_SEND_ACCESS、MAIL_ACCESS、ORIG_MAIL_ACCESS、および FROM_ACCESS のマッピングテーブルに関連するアクセスマッピングフラグを示します。PORT_ACCESS マッピングテーブルでは、少し異なるフラグがサポートされています（表 9-2 を参照）。

表 9-3　　アクセスマッピングフラグ

フラグ	説明
$B	ビットバケットにメッセージをリダイレクトします。
$H	.HELD ファイルとしてメッセージを保留します。
$Y	アクセスを許可します。
フラグと引数（引数の読み取り順序 +）	
$J アドレス	元のエンベロープ From: アドレスを指定のアドレスに置換します。*
$K アドレス	元の Sender: アドレスを指定のアドレスに置換します。* ++
$I ユーザ	識別子	特定のユーザのグループ ID を調べます。
$< 文字列	プローブが一致する場合に、文字列を システムログ （UNIX）またはイベント ログ （NT）に送ります。+++
$> 文字列	アクセスが拒否された場合に、文字列を システムログ （UNIX）またはイベントログ （NT）に送ります。+++
$D 遅延	応答を遅らせます （100 分の 1 秒）。正の値はトランザクションの各コマンドごとに遅らせ、負の値は、アドレスの引き渡し時（FROM_ACCESS テーブルの SMTP MAIL FROM: コマンド、その他のテーブルの SMTP RCPT TO: コマンド）にのみ遅らせます。
$T タグ	タグを前に付けます。
$A ヘッダ	メッセージにヘッダ行を追加します。
$X エラーコード	メッセージを拒否した場合に、指定したエラーコードを含む拡張 SMTP エラーコードを発行します。
$N 文字列	アクセスを拒否し、オプションのエラーテキスト文字列を渡します。
$F 文字列	$N 文字列と同じで、アクセスを拒否し、オプションのエラーテキスト文字列を渡します。

* FROM_ACCESS テーブルでのみ使用できます。

+ 引数を伴うフラグを複数個使用する場合は、引数を縦棒文字「|」で区切り、この表に示されている順序で配置します。

++「$K」フラグを FROM_ACCESS マッピング テーブルで有効にするには、ソース チャネルに authrewrite キーワードが含まれていなければなりません。

+++ 問題のある差出人によるサービス アタックを防ぐには「$D」フラグを使用するとよいでしょう。特に、$> エントリまたはアクセスを拒否する $< エントリで「$D」フラグを使用します。

第 2 部 メールボックスフィルタ

第 2 部には、以下の項目があります。

- 概要
- ユーザ単位のフィルタを作成する
- チャネルレベルのフィルタを作成する
- MTA 全体のフィルタを作成する
- ユーザフィルタをデバッグする

概要

フィルタは、メールメッセージに適用する 1 つまたは複数の条件から構成されています。Messaging Server フィルタはサーバに保存され、サーバによって評価されます。そのため、それらは SSR （サーバ側規則）と呼ばれることもあります。Messaging Server のフィルタは、Sieve Internet Draft の Draft 9 である Sieve フィルタリング言語に基づいています。

管理者は、チャネルレベルのフィルタと MTA 全体のフィルタを作成し、不正メールの配信を防止できます。また、フィルタテンプレートを作成し、Delegated Administrator for Messaging のインターフェースを介してエンドユーザが利用できるようにすることも可能です。エンドユーザは、テンプレートを利用して個人用のメールボックスフィルタを構築し、受け取りたくないメールメッセージの受信を拒否できます。

サーバは、次の優先順位に従ってフィルタを適用します。

1 ユーザ単位のフィルタ

   個人用メールボックスフィルタにメッセージの許可あるいは拒否が定義されている場合は、メッセージに対してそのフィルタ処理が行われます。しかし、受取人がメールボックスフィルタを設定していない場合、またはユーザのメールボックスフィルタが適用されないメッセージの場合は、Messaging Server によってチャネルレベルのフィルタが適用されます。

2 チャネルレベルのフィルタ

   チャネルレベルのフィルタにメッセージの許可あるいは拒否が定義されている場合は、メッセージに対してそのフィルタ処理が行われます。それ以外の場合は、Messaging Server によって MTA 全体のフィルタが適用されます (該当する場合)。

3 MTA 全体のフィルタ

デフォルト設定を使用した場合、それぞれのユーザはメールボックスフィルタを所有していません。ユーザが 委任管理者 のインターフェースを使用して 1 つまたは複数のフィルタを作成すると、それらのフィルタがディレクトリに保存され、ディレクトリの同期処理時に MTA によって読み取られます。

ユーザ単位のフィルタを作成する

ユーザ単位のフィルタは、特定ユーザのメールボックスに送信されるメッセージに適用されます。管理者は、フィルタテンプレートを作成し、Delegated Administrator for Messaging のインターフェースを介してそのテンプレートをエンド ユーザに提供できます。エンドユーザはテンプレートを利用して個人用サーバフィルタを構築し、メールボックスへのメールメッセージ配信を制御できます。つまり、特定のメールメッセージの受信を拒否したり、メールをリダイレクトしたり、あるいはメールボックスフォルダに入れるメッセージをフィルタリングすることができます。

フィルタテンプレートは、Sieve スクリプトのハードコード要素をプロンプトや入力フィールドに置換することで、Sieve スクリプトを一般化したものです。Java servlet は、Sieve テンプレートを解析し、ブラウザで UI ページを生成するために使用されます。エンドユーザが入力フィールドに値を入力すると、Servlet によってそれらの値が読み取られ、ユーザのディレクトリプロフィール エントリ内の Sieve スクリプトに保存されます。プロンプトおよび入力フィールドは、Delegated Administrator のインターフェースを介してエンドユーザに提示されます。

Delegated Administrator には、サンプルのテンプレートセットが用意されています。これらのテンプレートファイルは、次のディレクトリにあります。

```
nda-path/nda/nda/default/lang/templates/enduser/ssr/*.txt
```

フィルタテンプレートは、Sieve 言語を使って変更したり新規作成することができます。新規のフィルタテンプレートを作成した場合は、それを前述の ssr ディレクトリにテキスト形式で保存しなければなりません。そのファイルが誰でも読み取り可能であることを確認し、以下の例に示すように、フィルタテンプレートに LDAP エントリを追加します。

```
dn: cn=Subject Discard,cn=ssrconf,cn=en,
              cn=domainConfiguration,ou=config,o=isp
objectclass: top
objectclass: nsValueItem
cn: Subject Discard
nsvaluetype: nsValueCIS
nsvaluecis: ../templates/enduser/ssr/subject-discard.txt
```

図 9-7 に、テンプレートの例を示します。

図 9-7 Sieve テンプレートの例

```
#RULE: $Template="File To Folder"
require "fileinto";
if header :contains # Q1
    # Q2
{
    fileinto # Q3
    ;
}

#PRE: "This rule files messages into a folder."
#PRE: "Choose the header line to search on"
#PRE: "And specify the phrase you wish to search for"
#Q1: header "If the header line"
#Q2: value "Contains the phrase"
#Q3: folder "Then file into the folder"
```

上記の例で、Q1、Q2、および Q3 は入力される値のプレースフォルダであり、UI がその値を見つけて置換します。各トークンは、その入力値の質問とデータタイプをマッピングします。

データタイプおよび関連する質問は、各トークンごとのコメント行に定義されています。それらは、*トークン*: *データ*- *タイプ*- *変数*の形式で定義され、続いて、引用符に囲まれた文字列に実際の質問が含まれています。上記の例で、`header value`、および `folder` は、いずれも、ドロップダウンリスト、編集ボックス、あるいはその他の要素を示すデータタイプです。これらのデータタイプ変数は、UI に対し、どのタイプの情報をユーザから取得するのかを指示するものです。

テンプレートが解析されると、ダイアログが生成され、図 9-8 の例のようにエンドユーザに表示されます。この例で、角括弧はドロップダウンリストを表しています。

図 9-8 テンプレート出力の例

```
+-------------------------------------------------------------+
| Template: File To Folder Name: _________________            |
+-------------------------------------------------------------+
|           This rule files messages to a folder              |
|           Choose the header line to search on               |
|       And specify the phrase you wish to search for         |
|                                                             |
|   If the header line: [From       ]                         |
|   Contains the phrase: ____________________________         |
|   Then file into the folder: _________________              |
+-------------------------------------------------------------+
```

ユーザがデータを入力すると、その規則がユーザの mailSieveRuleSource 属性に保存されます。

テンプレートの構文には、以下の規則があります。

- #RULE 行は、その他の行よりも前に記述され、$Template を定義する必要があります。
- #PRE で始まるコメント行は、GUI ページの入力フィールドよりも前に表示されます。

  #PRE 文は、二重引用符で囲まれていなければなりません。
- #POST で始まるコメント行は、GUI ページの最後に表示されます。

  #POST 文は、二重引用符で囲まれていなければなりません。
- その他のコメント行は、GUI ページには表示されません。
- トークンは ASCII 文字列で、大文字と小文字の区別はありません。トークンに空白を挿入することはできません。
- データタイプ変数は、コメント行のトークン文字列の後に記述します。大文字と小文字の区別はありません。
- 実際の質問は、データタイプ変数のすぐ後のコメント行に定義されており、二重引用符で囲まれています。

Sieve テンプレートでは、以下のデータタイプ変数がサポートされています。

- `header` - GUI に表示される際には、リストボックスが使用され、次の値が表示されます：`Subject`、`To`、`From`。

  Sieve 規則がユーザエントリに保存されると、`Subject` の値が Subject、Comments、Keywords に展開され、`From` の値は From、Sender、Resent-from、Resent-sender、Return-path に、さらに `To` の値は To、Cc、Bcc、Resent-to、Resent-cc、Reset-bcc に展開されます。

- `value` - テキストフィールドを使って値を示します。
- `address` - テキストフィールドを使って値を示します。アドレスの構文が RFC 822 のメールアドレス形式に準拠しているかどうかが調べられます。
- `folder` - テキストフィールドを使って値を示します。
- `size` - ユーザは「キロバイト」または「メガバイト」の中から選択するか、または任意の数値を指定できます。
- `message` - テキストフィールドを使って値を示します。

チャネルレベルのフィルタを作成する

チャネルレベルのフィルタは、チャネルのキューに入った各メッセージに適用されます。この種のフィルタの一般的な用途は、特定のチャネルから入ってくるメッセージをブロックすることです。

チャネルレベルのフィルタを作成するする手順を以下に示します。

1. Sieve を使ってフィルタを記述します。
2. フィルタを、以下のディレクトリのファイルに保存します。

   `msg-`*インスタンス*`/imta/config/`*file*`.filter`

   ファイルは誰でも読み取り可能で、MTA の uid によって所有されていなければなりません。

3. 以下のチャネル設定を定義します。

   `destinationfilter file:IMTA_TABLE:`*file*`.filter`

4. 設定をリコンパイルし、ディスパッチャを再起動します。

   注意 : フィルタファイルへの変更を有効にするのに、リコンパイルやディスパッチャの再起動は不要です。

`destinationfilter` チャネルキーワードは、対象チャネルのキューに入るメッセージのフィルタリングを有効にします。`sourcefilter` チャネルキーワードは、対象チャネルからキューに入るメッセージのフィルタリングを有効にします。これらのキーワードには、それぞれパラメータが 1 つ必要です。このパラメータは、そのチャネルに関連付けられたチャネル フィルタファイルへのパスを指定するものです。

destinationfilter チャネルキーワードの構文は以下のとおりです。

```
destinationfilter URL-パターン
```

sourcefilter チャネルキーワードの構文は以下のとおりです。

```
sourcefilter URL-パターン
```

URL-パターン は、対象チャネルのフィルタファイルへのパスを示す URL です。次の例で、*チャネル名* はチャネルの名前です。

```
destinationfilter file:///imta/config/チャネル名.filter
```

filter チャネルキーワードは、対象チャネルにおけるメッセージのフィルタリングを有効にします。このキーワードには、パラメータが 1 つ必要です。このパラメータは、そのチャネルを介してメールを受信するエンベロープの各受取人に関連付けられたチャネルフィルタファイルへのパスを指定するものです。

filter チャネルキーワードの構文は以下のとおりです。

```
filter URL-パターン
```

URL-パターン は、特殊な置換シーケンスを処理した後の URL で、指定した受信者アドレスに対するフィルタファイルへのパスを示します。*URL-パターン* には、特殊な置換シーケンスを含めることができます。このシーケンスは、受信者アドレス local-part@host.domain から派生する文字列に置き換えられます。表 9-4 に、これらの置換シーケンスを示します。

fileinto キーワードは、メールボックスフィルタの fileinto 演算子が適用されたときにアドレスをどのように変更するのかを指定するものです。次の例では、フォルダ名をサブアドレスとして元のアドレスに挿入して、元のサブアドレスを置き換えるように指定しています。

```
fileinto $U+$S@$D
```

表 9-4　　置換シーケンス

シーケンス	代替文字列
$$	$ 文字に置き換えます。
$A, $a	アドレス (local-part@ host.domain) に置き換えます。
$D, $d	ホストドメインに置き換えます。
$H, $h	ホストに置き換えます。
$L, $l	ローカル部分に置き換えます。
$U, $u	下線 (_) やチルド (~) のプレフィックス、およびサブアドレスのポストフィックスを除くローカル部分に置き換えます。
$~	アドレスのローカル部分に関連付けられたホームディレクトリに対するファイルパスに置き換えます。

MTA 全体のフィルタを作成する

MTA 全体のフィルタは、MTA のキューに入るすべてのメッセージに適用されます。この種のフィルタの一般的な用途は、メッセージの宛先とは関係なく、ダイレクトメールや受信したくないメッセージをブロックすることです。

1 Sieve を使ってフィルタを記述します。

2 フィルタを、次のファイルに保存します。

`msg-`*インスタンス*`/imta/config/imta.filter`

このフィルタファイルは、誰でも読み取り可能でなければなりません。このファイルは自動的に使用されます。

3 設定をリコンパイルし、ディスパッチャを再起動します。

コンパイルした設定を使用する場合、MTA 全体のフィルタファイルはコンパイルされた設定内に組み込まれています。

FILTER_DISCARD チャネルから破棄メッセージをルーティングする

デフォルトでは、メールボックスフィルタで破棄されたメッセージは、システムから即座に破棄（削除）されます。しかし、ユーザが最初にメールボックスフィルタを設定した場合（設定が間違っている場合）、またはデバッグを目的とする場合には、削除処理を遅らせると便利です。

メールボックスフィルタによる破棄メッセージをシステム内に一時保存し、それを後で削除できるようにするには、次の例に示すように、まず MTA 設定に `filter_discard` チャネルを追加し、`notices` チャネルキーワードでメッセージを削除するまでの保存期間 （通常は日数）を記述します。

```
filter_discard notices 7
FILTER-DISCARD
```

次に MTA オプションファイルで `FILTER_DISCARD=2` オプションを設定します。`filter_discard` キュー内のメッセージは、ユーザの個人用ゴミ箱フォルダの延長と考えることができます。したがって、`filter_discard` キュー内のメッセージに対して警告メッセージが送られたり、バウンスやリターンの要求に応じてメッセージが差出人に戻されることもありません。これらのメッセージは、final notices 値の期限となるか、`imsimta return` などのユーティリティを使ってバウンスを要求することによって、システムから削除されるだけです。

ユーザフィルタをデバッグする

以下の情報は、システムのユーザフィルタに関して問題が発生した場合に役に立ちます。

dirsync プロセスは、ユーザフィルタに関する MTA の SSR データベース情報を更新します。短いフィルタは、データベース内に保存されます。長いフィルタの場合は、データベースに LDAP dn が保存されます。dirsync プロセスによってデータベースが更新されるまで、ユーザフィルタの変更内容は認識されません。

フィルタに関する問題を解決するには、以下の手順に従ってください。

- imta.cnf ファイル内で、ims-ms チャネルが次のようにマークされていることを確認します。

  ```
  filter ssrd:$a fileinto $u+$s@$d
  ```

- dirsync プロセスが configutil コマンドを使ってフィルタ情報を同期するようになっていることを確認します。

  configutil -l -o service.imta.ssrenabled -v true

  ```
  OK SET
  ```

  configutil | fgrep ssr

  service.imta.ssrenabled = true

- ファイルをテストするには、imsimta test コマンドを使用します。

  imsimta test -rewrite -debug -filter user@domain

  出力で、以下の情報を探します。

  ```
  mmc_open_url called to open ssrd:user@ims-ms
     URL with quotes stripped: ssrd:user@ims-ms
  Determined to be an SSRD URL.
     Identifier: user@ims-ms-daemon
  Filter successfully obtained.
  ```

- フィルタの構文に問題がある場合は、以下の情報を探します。

  ```
  Error parsing filter expression:...
  ```

- フィルタに問題がない場合は、test コマンドによって、出力の最後にフィルタが表示されます。

- フィルタに問題がある場合は、test コマンドによって、出力の最後に次の情報が表示されます。

  ```
  Address list error -- 4.7.1 Filter syntax error: user@siroe.com
  ```

  また、次に示すように、SMTP RCPT TO コマンドによって一時的なエラー応答コードが返されます。

  ```
  RCPT TO:<user@siroe.com>
  452 4.7.1 Filter syntax error
  ```

- ユーザアドレスの最終的な書き換え形式が分かっている場合には、imsimta test -url コマンドを使って MTA がそのユーザ用に使っているフィルタを確認できます。

  imsimta test -url ssrd:user@ims-ms-daemon

  imsimta test -rewrite コマンドを使用すると、ユーザアドレスの最終的な書き換え形式を見つけることができます。

第 10 章

メッセージストアを管理する

この章では、メッセージストアおよびメッセージストア管理のインターフェースについて説明します。この章には、以下の節があります。

- 概要
- メッセージストアディレクトリのレイアウト
- ストアのメッセージクリーンアップ方法
- ストアへの管理者アクセスを指定する
- メッセージストア制限容量の概要
- メッセージストアの制限容量を設定する
- 存続期間決定ポリシーを指定する
- メッセージストアのパーティションを設定する
- メンテナンスと復元のプロシージャを実行する
- メッセージストアをバックアップ、リストアする

概要

メッセージストアには、特定の Messaging Server インスタンスに対するユーザメールボックスがあり、そのサイズは、メールボックス、フォルダ、およびログファイルの数が増えるに従って大きくなります。メッセージストアのサイズを制御するには、各メールボックスのサイズ (ディスク容量) を制限する、各メールボックスに保存できるメッセージの合計数を制限する、ストア内におけるメッセージの存続期間を設定するなどの方法があります。

システムを使用するユーザの数が増えるにつれ、必要なディスク容量も増加します。サーバがサポートするユーザ数によっては、複数の物理ディスクが必要な場合もあります。また、ユーザベースが非常に大きい場合は、それぞれ異なるメッセージストアを持つ複数の Messaging Server インスタンスが存在している場合もあります。同様に、複数のホストドメインがある場合は、1 つのサーバインスタンスを 1 つの大きなドメイン専用に設定する必要が生じることもあります。このような設定では、ドメインごとにストア管理者を割り当てることができます。

iPlanet Messaging Server には、iPlanet Console のインターフェースのほかに、メッセージストア管理用の一連のコマンドラインユーティリティが備わっています。表 10-1 は、これらのコマンドラインユーティリティの説明です。ユーティリティの使い方については、231 ページの「メンテナンスと復元のプロシージャを実行する」および『Messaging Server リファレンスマニュアル』を参照してください。

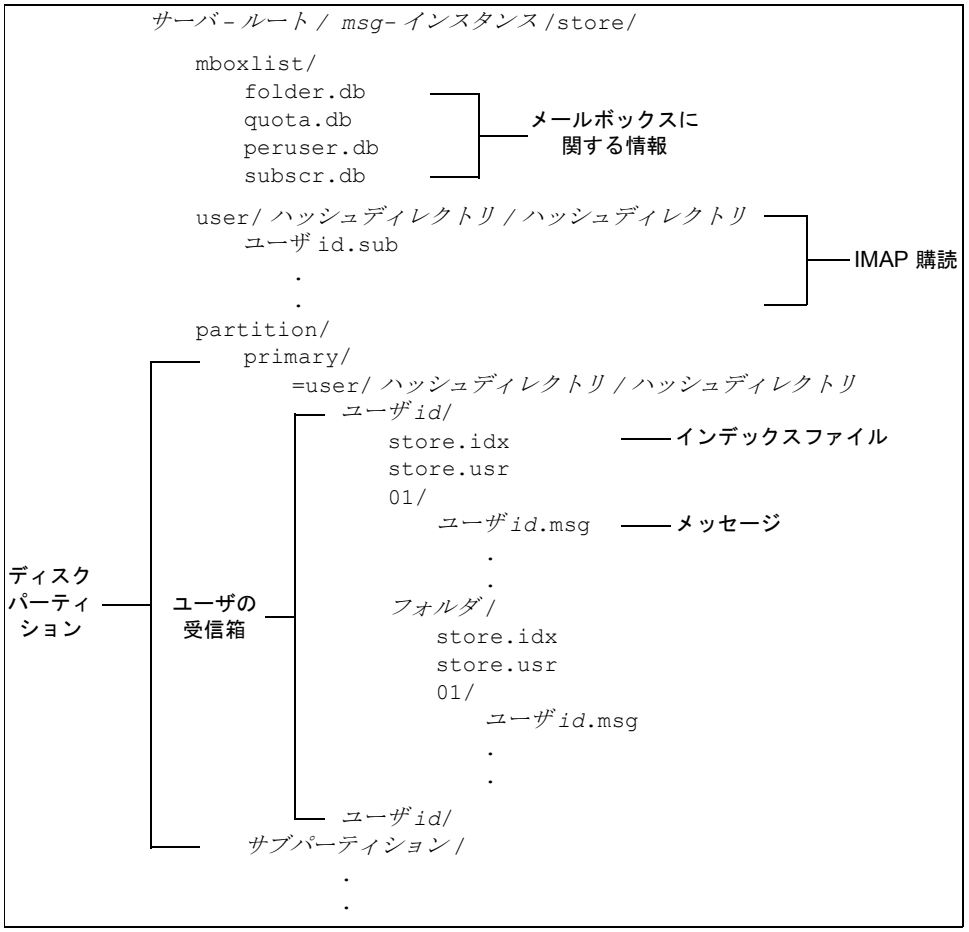
表 10-1　メッセージストアに関するコマンドラインユーティリティ

ユーティリティ	説明
`configutil`	ストアの設定パラメータを指定および変更します。
`hashdir`	特定のユーザのメッセージストアを含むディレクトリを検出します。
`mboxutil`	メールボックスの表示、作成、削除、名前の変更、移動、およびディスク容量使用状況の報告を行います。
`MoveUser`	ユーザアカウントをメッセージングサーバ間で移動します。
`readership`	共有 IMAP フォルダの読者に関する情報を収集します。
`reconstruct`	損傷があるか、または壊れたメールボックスを再構築します。
`stored`	バックグラウンドタスクおよび日常的なタスクを実行し、ディスクから保存されているメッセージを消去します。
`imsbackup`	ディスクに保存されているメッセージのバックアップを作成します。
`imsrestore`	バックアップされたメッセージをリストアします。

メッセージストアディレクトリのレイアウト

図 10-1 は、1 つのサーバインスタンスにおけるメッセージストアディレクトリのレイアウトを示しています。メッセージストアは、メールボックスの内容に迅速にアクセスできるように設計されています。各ディレクトリの詳細については、表 10-2 を参照してください。

図 10-1 メッセージストアディレクトリのレイアウト



ディレクトリパスは、たとえば以下のようになります。

サーバ - ルート /msg- *インスタンス* /store/partition/primary/=user/53/53/=mack1

表 10-2　メッセージストアディレクトリの説明

場所	内容 / 説明
サーバ - ルート /msg- *インスタンス* /store/	メッセージストアの最上位ディレクトリ。このディレクトリの中には mboxlist、user、および partition サブディレクトリがあります。
.../store/mboxlist/	サーバ上のメールボックスおよびその制限容量に関する情報を保存するデータベース (Berkley DB) があります。
	folder.db ファイルには、メールボックスが保存されているパーティションの名前、ACL、および store.idx ファイルの部分的な情報のコピーが含まれています。folder.db には、各メールボックスにつき 1 つずつエントリが作成されます。
	quota.db ファイルには、ディスクの制限容量および使用状況に関する情報が含まれています。quota.db2 ファイルには、各ユーザにつき 1 つずつエントリが作成されます。
	peruser.db には、ユーザごとのフラグに関する情報が含まれています。これらのフラグは、各ユーザがメッセージを開封または削除したことを示します。
	subscr.db には、ユーザ購読に関する情報が含まれています。
.../store/user/	各ユーザが購読する IMAP フォルダに関する情報が含まれています。各ユーザに関する情報は、*ユーザid*.sub ファイルに保存されます。これらのファイルは迅速に検索できるようハッシュ構造になっています。特定のユーザのファイルが含まれているディレクトリを探すには、hashdir ユーティリティを使用します。
.../store/partition/	デフォルトの primary パーティションがあります。このディレクトリには、管理者が定義したサブパーティションを追加することもできます。
/ *サブパーティション* /=user/	パーティションのサブディレクトリに含まれるすべてのユーザメールボックスが含まれています。メールボックスは迅速に検索できるようにハッシュ構造で保存されています。ある特定のユーザのメールボックスが含まれているディレクトリを探すには、hashdir ユーティリティを使います。

表 10-2　メッセージストアディレクトリの説明（続き）

場所	内容 / 説明
/=user/ *ハッシュディレクトリ* / *ハッシュディレクトリ* / *ユーザid*/	*ユーザ id* が示すユーザの最上位メールフォルダ。デフォルトドメインの場合、*ユーザid* 部分は*ユーザid* のみとなり、ホストドメインの場合、*ユーザ id* 部分は*ユーザid@ ドメイン*となります。メッセージはこのメールフォルダに配信されます。
/ *ユーザid*/ *フォルダ*	ユーザ定義のフォルダです。
/ *ユーザid*/store.idx	/ *ユーザ id*/ ディレクトリに保存されているメッセージに関する情報を提供するインデックスです。このファイルには、メッセージ数、メールボックスに対して設定されているディスク容量の制限、メールボックスがメッセージを受け取った最終時刻、メッセージフラグ、ヘッダや MIME 構造を含む可変長の情報、各メッセージのサイズなどの情報が含まれています。また、各ユーザの mboxlist 情報のバックアップコピーやディスク制限容量情報のバックアップコピーも含まれています。
/ *ユーザid*/store.usr	フォルダにアクセスしたユーザのリストがあります。リストされている各ユーザについて、フォルダへの最終アクセス時間、開封したメッセージのリスト、およびユーザが削除したメッセージのリストなどが含まれています。
/ *ユーザid*/store.exp	図 10-2 には示されていません。消去されたがディスクには残っているメッセージファイルのリストがあります。このファイルは、消去されたメッセージがある場合にのみ表示されます。
/ *ユーザid*/store.sub	図 10-2 には示されていません。ユーザ購読に関する情報が含まれています。
/ *ユーザid*/*nn*/	*メッセージ id*.msg のフォーマットでメッセージを保存するハッシュディレクトリ。*nn* は 00 から 99 までのいずれかの数字を示します。 たとえば、1 から 99 までのメッセージは 00 ディレクトリに保存され、100 から 199 までのメッセージは 01 ディレクトリに、9990 から 9999 までのメッセージは 99 ディレクトリに、10000 から 10099 までのメッセージは 00 ディレクトリに、それぞれ保存されます。

ストアのメッセージクリーンアップ方法

ストアでは、以下の 3 つの段階を経てメッセージのクリーンアップが行われます。

1 **削除 :** 削除するメッセージにクライアントがマークを付けます。この時点でクライアントは、このマークを外すことによってメッセージをリストアできます。

2 **消去 :** マークが付いているメッセージをクライアント (または指定した存続期間決定ポリシー) がメールボックスから消去します。いったん消去されたメッセージをクライアントがリストアすることはできませんが、この時点ではまだメッセージはディスクに残っています (同じメールボックスに接続している別のクライアントがメッセージを入手することは可能です)。

3 **クリーンアップ :** `stored` ユーティリティによって、消去後 1 時間以上経ったメッセージがディスクからすべてクリーンアップされます。

ストアへの管理者アクセスを指定する

メッセージストア管理者は、ユーザのメールボックスを表示またはモニタしたり、メッセージストアへのアクセスを制御することができます。ストア管理者はすべてのサービス (POP、IMAP、HTTP、SMTP) へのプロキシ認証特権を持つため、あらゆるユーザ特権を使って任意のサービスに対する認証を受けることができます。これらの特権により、ストア管理者はストア管理ユーティリティを実行できます。たとえば、`MoveUser` を使用して、ユーザのアカウントやメールボックスをシステム間で移動できます。

この節では、Messaging Server のメッセージストアへのアクセス特権を制御する方法について説明します。

注 他のユーザがストアにアクセスする管理者特権を持っている場合もあります。たとえば、サイトが Delegated Administration (DA) 製品を使用している場合、最上位の DA 管理者はデフォルト設定によってメールシステム内にあるすべてのメッセージングサーバのストアにアクセスする特権が与えられています。また、DA ドメイン管理者は、デフォルト設定によってそのドメインのストアにアクセスする特権が与えられています。DA 管理者の詳細については、『Messaging Server Provisioning Guide』および DA 関連のマニュアルを参照してください。

管理者は以下のタスクを実行できます。

- 管理者を追加する
- 管理者エントリを変更する
- 管理者エントリを削除する

管理者によるストアへのアクセスを制御するには、`configutil` コマンドまたはコンソールを使用します。

コンソールを使用する場合は以下の手順に従います。

1 コンソールで、設定する Messaging Server を開きます。

2 [環境設定] タブをクリックし、左ペインで [メッセージの保存] を選択します。

3 右ペインで [管理者] タブをクリックします。

管理者を追加する

コンソール - コンソールを使用して管理者エントリを追加するには、以下の手順に従います。

1 [管理者] タブをクリックします。

このタブには既存の管理者 ID のリストが表示されます。

2 [管理者 UID] ウィンドウの横にある [追加] ボタンをクリックします。

3 [管理者 UID] フィールドに、追加する管理者のユーザ ID を入力します。

iPlanet Directory Server が認識できるユーザ ID を使用してください。

4 [OK] をクリックして [管理者] タブに表示されるリストに管理者 ID を追加します。

5 [管理者] タブの [保存] をクリックして、変更した管理者リストを保存します

コマンドライン - コマンドラインユーティリティを使用して管理者エントリを追加するには、以下の手順に従います。

```
configutil -o store.admins -v "adminlist"
```

adminlist はカンマ区切りの管理者 ID リストです。複数の管理者を指定する場合は、リストを引用符で囲む必要があります。

管理者エントリを変更する

コンソール - コンソールを使用して既存のメッセージストア管理者 UID リストを変更するには、以下の手順に従います。

1 [管理者] タブをクリックします。

2 [管理者 UID] ウィンドウの横にある [編集] ボタンをクリックします。

3 [管理者 UID] フィールドの内容を必要に応じて変更します。

4 [OK] をクリックして変更内容を有効にし、[管理者の編集] ウィンドウを閉じます。

5 [管理者] タブの [保存] をクリックして、変更したリストを保存します。

コマンドライン - コマンドラインユーティリティを使用して既存のメッセージストア管理者 UID リストのエントリを変更するには、以下の手順に従います。

```
configutil -o store.admins -v "adminlist"
```

管理者エントリを削除する

コンソール - コンソールを使用してメッセージストア管理者 UID リストからエントリを削除するには、以下の手順に従います。

1 [管理者] タブをクリックします。

2 [管理者 UID] リストで、削除するエントリを選択します。

3 [削除] をクリックして選択したエントリを削除します。

4 [保存] をクリックして変更した管理者リストを保存します。

コマンドライン - コマンドラインユーティリティを使用してメッセージストア管理者を削除するには、以下の手順に従います。

```
configutil -o store.admins -v "adminlist"
```

メッセージストア制限容量の概要

この節では、以下の内容について説明します。

- ユーザに対する容量の制限
- ドメインとファミリグループに対する容量の制限
- テレフォニアプリケーションサーバに関する例外

ユーザに対する容量の制限

メッセージストアのサイズを制限するには、各ユーザメールボックスのサイズを制限します。そのためには、以下のような方法があります。

- ディスク容量 : 各ユーザが使用できるディスク容量を制限します。ディスク容量に関する制限は、ユーザが持つメールフォルダやメッセージの数に関わらず、そのユーザのすべてのメッセージの合計サイズに対して適用されます。ディスクの総容量に限りがある場合は、各ユーザが使用できるディスク容量を制限すると良いでしょう。
- メッセージ容量 : 各ユーザメールボックスに保存できるメッセージの数を制限します。

制限容量に関する情報は、LDAP 属性および設定変数として保存されます。制限が有効になっている場合、Messaging Server はメッセージをストアに追加する前に、制限容量を超えていないことを確認するために、制限容量キャッシュおよび設定ファイルをチェックします。また、制限に関する通知が有効になっている場合は、ユーザのディスク使用容量が制限に達すると、そのユーザにエラーメッセージが送られます。使用容量が制限容量に近づきつつあるユーザに対して警告メッセージを送るようにサーバを設定することも可能です。

特定の制限容量をデフォルトとして全ユーザに対して設定するか、またはユーザごとに制限を設定することができます。Messaging Server は、使用容量が制限容量を超過しているかどうかを判断する際、まず該当するユーザに対して制限が設定されているかどうかをチェックし、設定されていない場合は、全ユーザに対して設定されているデフォルトの制限容量をチェックします。

ユーザメッセージの合計サイズまたは合計数が制限容量を超過している場合、そのユーザ宛てのメッセージは、次のいずれかの状況になるまでメッセージキュー内に維持されます。(1) ユーザのメッセージの合計サイズまたは合計数が制限以下になった場合、サーバはユーザにメッセージを配信します。(2) 未配信のメッセージが指定猶予期間以上キュー内に維持されており、かつユーザのメールボックスが依然として制限容量を超過している場合、メッセージはサーバによって返送されます。

注	制限容量に達していないアカウントに対して配信する場合は、メッセージサイズのチェックは行われません。あるメッセージが配信されたことによってアカウントが制限以上の容量に達しても、ユーザはそのメッセージを受信できます。ただし、その次のメッセージはキュー内で待機することになります。

メッセージがユーザまたはメンテナンスポリシー (存続期間決定ポリシーなど) によって削除および消去されると、ディスク容量に余裕ができます。

ドメインとファミリグループに対する容量の制限

特定のドメインやドメイン内のファミリグループに対してディスク制限容量を設定することもできます。これらの制限は強制的なものではありませんが、ディスク使用容量を確認するのに便利です。詳細については、『Delegated Administrator User's Guide』を参照してください。

テレフォニアプリケーションサーバに関する例外

統合化されたメッセージング要件をサポートするために、Messaging Server はメッセージストアによって課された制限容量を無効にし、テレフォニアプリケーションサーバ (TAS) など、ある種のエージェントを通して送られたメッセージを配信できます。TAS が受け取ったメッセージは特別な MTA チャネルにルーティングされ、制限容量に関わらずストアに配信されます。TAS チャネルを設定する方法については、第 8 章「チャネル定義を設定する」を参照してください。

メッセージストアの制限容量を設定する

すべてのユーザに対してデフォルトの制限容量を設定するには、iPlanet Console または `configutil` コマンドを使用します。また、ユーザ、ファミリグループ、ドメインなどに対して個別に容量を制限することも可能です。

このマニュアルでは、制限容量のデフォルトを設定する方法について説明します。ユーザ、ファミリグループ、ドメインなどに対して個別に容量を制限する方法については、『Delegated Administrator's User Guide』を参照してください。

この節では、以下のタスクについて説明します。

- ユーザに対するデフォルトの制限容量を設定する
- 制限容量と通知を有効にする
- 猶予期間を設定する

iPlanet Console を使用する場合 :

1 iPlanet Console で、設定する Messaging Server を開きます。

2 [環境設定] タブをクリックし、左ペインの [メッセージの保存] を選択します。

3 右ペインの [制限容量] タブをクリックします。

ユーザに対するデフォルトの制限容量を設定する

制限容量のデフォルト設定は、個別に制限容量を設定されていないすべてのユーザに適用されます。個別に設定されている場合は、その設定がデフォルト設定に優先します。

コンソール - コンソールを使用してデフォルトの制限容量を設定するには、以下の手順に従います。

1 [制限容量] タブをクリックします。

2 ユーザに対するデフォルトの制限容量を設定するには、[デフォルトのユーザディスク制限容量] フィールドで以下のいずれかのオプションを選択します。

無制限 : ユーザが使用できるディスク容量を制限しない場合は、このオプションを選択します。

サイズ制限 : ユーザが使用できるディスク容量を特定のサイズに制限するには、このオプションを選択します。ボタンの横にあるフィールドに数値を入力し、ドロップダウンリストで [メガバイト] または [キロバイト] を選択します。

3 メールボックスに保存できるメッセージの数を指定するには、[デフォルトのユーザメッセージ制限容量] ボックスに数値を入力します。

4 [保存] をクリックします。

コマンドライン - ディスク容量を特定のサイズに設定するには、以下の手順に従います。

```
configutil -o store.defaultmailboxquota -v [ -1 | 数値 ]
```

-1 は無制限を示し、*数値* は制限する場合のバイト数を示します。

メッセージの合計数に対してデフォルトの制限容量を設定するには、以下の手順に従います。

```
configutil -o store.defaultmessagequota -v [ -1 | 数値 ]
```

-1 は無制限を示し、*数値* は制限する場合のバイト数を示します。

制限容量と通知を有効にする

制限容量と通知はそれぞれ有効または無効にできます。サーバの動作は、表 10-3 に示される設定変数に基づいて決定されます。

表 10-3　制限容量と通知

	制限オン	制限オフ
通知オン	メッセージは指定の猶予期間保留され、時効になった時点で拒否されます。メールボックスには追加されません。 IMAP SELECT、IMAP APPEND、SMTP sendmail メカニズムおよび配信コマンドはエラーメッセージを表示します。	メッセージはストアに配信され、メールボックスに追加されます。 IMAP SELECT、IMAP APPEND、SMTP sendmail メカニズムおよび配信コマンドはエラーメッセージを表示しません。
通知オフ	メッセージは指定の猶予期間保留され、時効になった時点で拒否されます。メールボックスには追加されません。 IMAP SELECT コマンド、配信コマンド、および SMTP sendmail メカニズムはエラーメッセージを表示しません。 IMAP APPEND コマンドはエラーメッセージを表示します。	メッセージはストアに配信され、メールボックスに追加されます。 IMAP SELECT、IMAP APPEND、SMTP sendmail メカニズム、および配信コマンドはエラーメッセージを表示しません。

制限容量を有効にする

コンソール - コンソールを使用して制限容量を有効にするには、以下の手順に従います。

1　[制限容量] タブをクリックします。

2　[制限容量実施の有効化] チェックボックスをオンにします。

このボックスはトグルとして機能します。制限を無効にするには、このチェックボックスをオフにします。

3　[保存] をクリックします。

コマンド ライン - コマンドラインユーティリティを使用して制限容量を有効にするには、以下の手順に従います。

```
configutil -o store.quotaenforcement -v [ yes | no]
```

no と指定すると制限容量は有効になりません。

制限容量に関する通知を有効にする

コンソール - コンソールを使用して制限容量に関する通知を有効にするには、以下の手順に従います。

1 [制限容量] タブをクリックします。

2 [制限容量有効化の通知] チェックボックスをオンにします。

このボックスはトグルとして機能します。通知を無効にするには、このチェックボックスをオフにします。

3 [保存] をクリックします。

コマンドライン - コマンドラインユーティリティを使用して制限容量に関する通知を有効にするには、以下の手順に従います。

```
configutil -o store.quotanotification -v [ yes | no ]
configutil -o store.quotaexceededmsg -v message
```

上記のコマンドで *message*（メッセージ）が設定されないと、制限容量に関する警告メッセージはユーザに送信されません。

制限容量に関する警告メッセージを定義する

制限容量を超過したユーザに対して送る警告メッセージは、以下の方法で定義できます。警告メッセージはユーザのメールボックスに配信されます。

コンソール - コンソールを使用して制限容量に関する警告メッセージを定義するには :

1 [制限容量] タブをクリックします。

2 ドロップダウンリストから使用する言語を選択します。

3 ドロップダウンリストの下にあるメッセージテキストフィールドに、警告メッセージを入力します。

4 [保存] をクリックします。

コマンドライン - コマンドラインユーティリティを使用して制限容量に関する警告メッセージを定義するには :

```
configutil -o store.quotaexceededmsg -v メッセージ
```

メッセージには必ず RFC 822 準拠のフォーマットを使用してください。

警告メッセージ発行の頻度を指定するには :

```
configutil -o store.quotaexceedmsginterval -v 数値
```

*数値*は日数を示します。たとえば、3 と指定すると、警告は 3 日ごとに送られます。

制限容量に関する警告のしきい値を指定する

制限容量のしきい値を設定することで、IMAP ユーザが制限容量に達する前に警告メッセージを送ることができます。ユーザのディスク使用容量が指定したしきい値を超過すると、サーバがユーザに警告メッセージを発行します。

クライアントが IMAP ALERT メカニズムをサポートしている場合は、IMAP ユーザがメールボックスを選択する度に画面にメッセージが表示されます (メッセージは IMAP ログにも記録されます)。

コンソール - コンソールを使用して制限容量のしきい値を指定するには :

1 [制限容量] タブをクリックします。

2 [制限容量の警告のしきい値] フィールドに、警告のしきい値とする数値を入力します。

この数値は、許可されている制限容量に対するパーセント値を示します。たとえば、この値を 90 パーセントに指定すると、ユーザのディスク使用容量が制限容量の 90 パーセントに達したときに警告が発行されます。デフォルトは 90 パーセントに設定されています。この機能を無効にするには、100 パーセントに指定します。

3 [保存] をクリックします。

コマンドライン - コマンドラインユーティリティを使用して制限容量のしきい値を指定するには :

```
configutil -o store.quotawarn -v 数値
```

数値 は、許可されている制限容量に対するパーセント値を示します。

猶予期間を設定する

ユーザメールボックスのサイズまたはメッセージ数が制限を超過すると、サーバは指定した期間 (猶予期間) そのメールボックス宛てのメッセージをキュー内に保持し、その後返送を開始します。メッセージは、以下のいずれかの状況になるまでキュー内で待機します。

- メールボックスのサイズまたはメッセージ数が制限以下になった場合 (サーバはメッセージをメールボックスに配信します)。
- 猶予期間を過ぎてもメールボックスのサイズまたはメッセージ数が制限を超過している場合 (サーバはメッセージを返送します)。
- メッセージが指定した最大時間以上にわたってキュー内に保持されていた場合。

コンソール - コンソールを使用してキューにメッセージを保管する猶予期間を設定するには、以下の手順に従います。

1 [制限容量] タブをクリックします。

2 [制限容量超過時の猶予期間] フィールドに数値を入力します。

3 ドロップダウンリストで [日] または [時間] を選択します。

4 [保存] をクリックします。

コマンドライン - コマンドラインユーティリティを使用して猶予期間を設定するには :

```
configutil -o store.quotagraceperiod -v 数値
```

数値 は時間数を示します。

存続期間決定ポリシーを指定する

存続期間決定ポリシーは、サーバディスクの使用を制御するもう 1 つの手段です。このポリシーを設定することで、メッセージがメールボックスに保持される期間を制御できます。ディスクの総容量に限りがある場合は、存続期間決定ポリシーを設定してストアからメッセージを削除することをお勧めします。ただし、メッセージがストアから削除される際、ユーザに対する警告は発行されません。存続期間決定ポリシーを設定する場合は、ユーザに前もって通知しておく必要があります。

存続期間規則は、以下の条件に基づいて作成できます。

- メールボックス内のメッセージ数
- メールボックスの合計サイズ
- メッセージがメールボックスに保持される日数
- メールボックスのサイズが指定値を超過している場合に、超過分のメッセージがメールボックスに保持される日数

1 つのメールボックスに対して複数の規則を適用した場合、期間に関する規則はすべて有効と見なされますが、最も厳しい条件のものが最優先されます。たとえば、あるメールボックスに対して次の 2 つの規則が設定されているとします。1 つはメールボックスに保存できるメッセージの数を 1000 件と規定し、もう 1 つは 500 件と規定しています。この場合期間が過ぎると、サーバはメールボックスに 500 件を残し、それ以外のメッセージをすべて削除します。また、別の例として、1 つの規則は合計 10 万バイト分のメッセージを 3 日間維持すると規定し、もう 1 つの規則は合計 1000 バイト分のメッセージを 12 日間維持すると規定しています。この場合、サーバは 10 万バイト分のメッセージを 3 日間保持します。3 日間にわたってメールボックスに保持されるメッセージ以外、すなわち超過分はすべて削除されます。特定のメールボックスに特定の規則を適用するには、exclusive パラメータを使用します。

コンソール - コンソールを使用して新規規則を作成するには :

1 iPlanet Console で、設定する Messaging Server を開きます。

2 [環境設定] タブをクリックし、左ペインの [メッセージの保存] を選択します。

3 右ペインの [存続期間] タブをクリックします。

4 [追加] をクリックして [規則の追加] ウィンドウを開きます。

5 作成する規則の名前を入力します。

6 規則を適用するターゲットフォルダを選択します。

パス名、ファイル名、または部分的な文字列を入力できます。以下の IMAP ワイルドカードを使用することもできます。

* - どのような組み合わせの文字にも一致します。
% - スラッシュを除き、どのような組み合わせの文字にも一致します。

新しい規則は、指定したパターンに一致するフォルダにのみ適用されます。

7 新しく作成した規則だけをターゲットフォルダに適用するには、[除外] ボックスをオンにします。

8 フォルダサイズに基づいて規則を作成するには、以下の操作を実行します。

- [メッセージの件数] フィールドに、フォルダが古いメッセージを削除することなく保持できるメッセージ数の上限を入力します。
- [フォルダサイズ] フィールドにフォルダサイズを入力し、ドロップダウンリストで [キロバイト] または [メガバイト] を選択します。

フォルダサイズが指定値を超過すると、サイズが指定値以下になるまで超過分のメッセージは古い順に削除されます。

9 メッセージの存続期間に基づいて規則を作成するには、[日数] フィールドにフォルダがメッセージを保持する期間を数値で入力します。

10 メッセージサイズに基づいて規則を作成するには、以下の操作を実行します。

- [メッセージサイズの制限] フィールドにフォルダが保持できるメッセージサイズの上限を入力し、ドロップダウンリストで [キロバイト] または [メガバイト] を選択します。
- [猶予期間] フィールドに、超過分のメッセージがフォルダ内に残る期間を数値で入力します。

猶予期間が過ぎると、サーバは超過分のメッセージを削除します。

11 [OK] をクリックして新しい規則を存続期間規則のリストに追加し、[追加] ウィンドウを閉じます。

12 [保存] をクリックして、存続期間規則のリストを保存します。

コマンドライン - コマンドラインユーティリティを使って新規規則を作成する場合は、以下のコマンドを使用します。*名前* は規則名を示します。

規則を適用するターゲットフォルダを指定するには :

```
configutil -o store.expirerule.名前.folderpattern -v パターン
```

たとえば、パターン部分を `user/*` と指定するとすべてのフォルダに規則が適用され、`user/%@siroe.com/*` と指定すると `siroe.com` ドメイン内のすべてのユーザのすべてのフォルダに、`user/%/Trash` と指定すると全ユーザのごみ箱フォルダにそれぞれ規則が適用されます。

ターゲットフォルダに他の規則が適用されないように設定するには :

```
configutil -o store.expirerule.名前.exclusive -v [ yes | no ]
```

古いメッセージを削除することなく、フォルダに保持できるメッセージの数の上限を指定するには:

```
configutil -o store.expirerule.名前.messagecount -v 数値
```

フォルダサイズを指定するには :

```
configutil -o store.expirerule.名前.foldersizebytes -v 数値
```

数値 はバイト数を示します。

メッセージの存続期間を指定するには:

```
configutil -o store.expirerule.名前.messagedays -v 数値
```

*数値*は日数を示します。

メッセージサイズを指定するには:

```
configutil -o store.expirerule.名前.messagesize -v 数値
```

*数値*はバイト数を示します。

超過分のメッセージをフォルダに保持する期間を指定するには:

```
configutil -o store.expirerule.名前.messagesizedays -v 数値
```

*数値*は日数を示します。

メッセージストアのパーティションを設定する

特に設定を変更しない限り、すべてのユーザメールボックスは msg-*インスタンス*/store/partition/ ディレクトリに保存されます。partition ディレクトリは論理ディレクトリであり、1 つまたは複数のサブパーティションが含まれることもあります。サブパーティションを単数または複数の物理ドライブにマッピングすることも可能です。インストール時、partition ディレクトリには primary パーティションというサブパーティションが 1 つだけ作成されます。

partition ディレクトリには、必要に応じてパーティションを追加できます。たとえば、以下に示すように、1 つのディスクにパーティションを追加してユーザを整理できます。

```
msg-インスタンス/store/partition/mkting/
msg-インスタンス/store/partition/eng/
msg-インスタンス/store/partition/sales/
```

必要なディスク容量が増加するに従い、これらのパーティションをそれぞれ異なる物理ディスクドライブにマップする必要が生じることもあります。

各ディスクにそれぞれメールボックス数を制限しておくことをお勧めします。メールボックスを複数のディスクに分散することで、配信に必要な時間を短縮できます (ただし、SMTP の承認レートが速くなるとは限りません)。各ディスクに割り当てられるメールボックスの数は、ディスクの総容量と各ユーザに与えるディスク容量によって変化します。たとえば、ユーザあたりのディスク容量を少なくすると、各ディスクに割り当てられるメールボックスの数は増加します。

メッセージストアに複数のディスクが必要な場合は、RAID (Redundant Array of Inexpensive Disks) 技術を利用して管理を簡素化できます。RAID 技術を使用すると、複数のディスクにデータが分散している場合でも、あたかも 1 つの論理ディスクを使用しているかのように全ディスクを管理できます。また、RAID 技術は、障害復旧用にメッセージストアのバックアップを作成するために利用することもできます。

注　より迅速なディスクアクセスを実現するためには、メッセージストアとメッセージキューをそれぞれ異なるディスクに配置する必要があります。

パーティションを追加する

パーティションを追加する際には、ディスク上のパーティション保存場所 (絶対物理パス) と論理名 (パーティションニックネーム) を指定します。

パーティションニックネームを使用すると、物理パスにかかわらず、ユーザを論理パーティション名にマップできます。パーティションニックネームは、ユーザアカウントを設定する際や、ユーザにメッセージストアを割り当てる際に使用できます。ニックネームには英数字を使用します (ただし、大文字は使用できません)。

パーティションを作成および管理するには、物理パスに指定されている場所への書き込み特権が与えられているユーザ ID を使用する必要があります。

注　　パーティションを追加したら、サーバをいったん停止してから再起動することにより、設定情報を更新してください。

コンソール - コンソールを使用してストアにパーティションを追加するには :

1. iPlanet Console で、設定する Messaging Server を開きます。
2. [環境設定] タブをクリックし、左ペインの [メッセージの保存] を選択します。
3. 右ペインの [パーティション] タブをクリックします。
4. [追加] ボタンをクリックします。
5. パーティションのニックネームを入力します。

   これはパーティションの論理名です。
6. パーティションのパスを入力します。

   これはパーティションの絶対パス名です。
7. このパーティションをデフォルトとして指定するには、[デフォルトのパーティションにする] ボックスをオンにします。
8. [OK] をクリックしてパーティション設定エントリを有効にし、ウィンドウを閉じます。
9. [保存] をクリックしてパーティションリストを保存します。

コマンドライン - コマンドラインユーティリティを使用してストアにパーティションを追加するには :

```
configutil -o store.partition.ニックネーム.path -v パス
```

*ニックネーム*はパーティションの論理名を示し、*パス*はパーティション保存場所の絶対パス名を示します。

デフォルトプライマリ パーティションのパスを指定するには :

```
configutil -o store.partition.primary.path -v パス
```

メールボックスを別のディスクパーティションに移動する

特に設定を変更しない限り、メールボックスは primary パーティション内に作成されます。このパーティションの容量が一杯になると、メッセージを保存することができなくなります。この問題には、次のような対応策があります。

- ユーザのメールボックスのサイズを小さくする
- 容量管理ソフトウェアを使用している場合、別のディスクを追加する
- 別のパーティションを作成し (229 ページの「パーティションを追加する」)、メールボックスを新しいパーティションに移動する

可能な限り、容量管理ソフトを使用して、システムにディスク容量を追加する方法をお勧めします。これは、ユーザへの影響を最も少なく抑えられるためです。しかし、次の手順に従って、メールボックスを別のパーティションに移動することもできます。

1 移行プロセス中は、ユーザがメールボックスに接続されていない状態にします。

ユーザに通知を出して、メールボックスの移動作業を行う前にログオフし、作業期間中にログオンしないように指示します。または、ユーザがログオフした後、POP、IMAP、および HTTP のサービスを使用できないように mailAllowedServiceAccess 属性を設定します。詳細は、次の URL を参照してください。

```
http://docs.iplanet.com/docs/manuals/messaging/ims50/pg/users.htm#19110
```

注 mailAllowedServiceAccess を設定して POP、IMAP、HTTP へのアクセスを拒否しても、ユーザがすでにメールボックスに接続している場合に、その接続が切断されることはありません。このため、メールボックスを移動する前に、すべての接続が切断されていることを確認してください。

2 次のコマンドを使用して、ユーザのメールボックスを移動します。

```
mboxutil -r user/<userid>/INBOX user/<userid>/INBOX <oartition_name>
```

userid はユーザ ID、*partition_name* はパーティション名を示します。

例:

```
mboxutil -r user/ofanning/INBOX user/ofanning/INBOX secondary
```

3 移動したユーザの LDAP エントリ内の mailMessageStore 属性を、新しいパーティションの名前に設定します。

例:mailMessageStore: secondary

4 ユーザにメッセージストアへの接続が再開されたことを通知します。必要に応じて、POP、IMAP、および HTTP サービスを使用できるように mailAllowedServiceAccess 属性を変更します。

メンテナンスと復元のプロシージャを実行する

この項では、メッセージストアのメンテナンスタスクおよび復元タスクに使用するユーティリティについて説明します。サーバからの警告などを見逃さないよう、常に postmaster メールを読むようにしてください。また、サーバのパフォーマンスを確認するために、ログファイル内の情報をモニタすることもできます。ログファイルの詳細については、第 12 章「ログ記録とログ解析」を参照してください。

この項では、以下の事項について説明します。

- メールボックスを管理する
- 制限容量をモニタする
- ディスク容量をモニタする
- stored ユーティリティを使用する
- メールボックスやメールボックスデータベースを修復する
- ユーザのアカウントを移動する

メールボックスを管理する

この節では、メールボックスの管理およびモニタに使用する `mboxutil`、`hashdir`、および `readership` ユーティリティについて説明します。

mboxutil ユーティリティ

`mboxutil` コマンドは、メールボックスの典型的なメンテナンスタスクに使用します。これには、以下のタスクが含まれます。

- メールボックスのリストを表示する
- メールボックスを作成する
- メールボックスを削除する
- メールボックスの名前を変更する
- メールボックスをパーティション間で移動する

また、`mboxutil` コマンドを使って、制限容量に関する情報を表示することもできます。詳細については、234 ページの「制限容量をモニタする」を参照してください。

表 10-4 に、mboxutil コマンドのオプションを示します。構文や使用条件の詳細については、『Messaging Server リファレンスマニュアル』を参照してください。

表 10-4　mboxutil のオプション

オプション	説明
-a	ユーザに対して設定されているすべての制限容量に関する情報を表示します。
-c *メールボックス*	指定したメールボックスを作成します。
-d *メールボックス*	指定したメールボックスを削除します。
-g *グループ*	指定したグループに対して設定されている制限容量に関する情報を表示します。
-k *mailbox コマンド*	指定したメールボックスをフォルダレベルでロックし、指定したコマンドを実行し、コマンド終了後にロックを解除します。
-l	サーバ上にあるすべてのメールボックスのリストを表示します。
-p *パターン*	-l オプションと併用した場合、*パターン*に一致するメールボックス名だけを表示します。IMAP ワイルドカードを使用することも可能です。
-q *ドメイン*	指定したドメインに対して設定されている制限容量に関する情報を表示します。
-r *古い名前 新しい名前* [*パーティション*]	メールボックス名を*古い名前*から*新しい名前*に変更します。フォルダをあるパーティションから別のパーティションに移動するには、*パーティション*オプションを使用して移動先のパーティションを指定する必要があります。 このオプションは、ユーザの名前を変更するために使用できます。たとえば、`mboxutil -r user/user1/INBOX user/user2/INBOX` と指定すると、user1 のメールとメールボックスはすべて user2 に移動し、新しいメッセージが新しい INBOX に表示されるようになります (user2 が既に存在する場合は、この操作は失敗します)。
-u *ユーザ*	メッセージストア現在のサイズ、制限容量 (設定されている場合)、ディスク制限容量に対する使用容量の割合などのユーザ情報を表示します。
-x	-l オプションと併用すると、メールボックスのパスおよびアクセス制御に関する情報も表示できます。

メールボックス命名規則

メールボックスに名前を付ける際には、必ず user/ *ユーザid*/ *メールボックス*というフォーマットを使用してください。*ユーザid* はメールボックスの所有者であるユーザを示し、*メールボックス*はメールボックス名を示します。ホストドメインの場合、*ユーザid* は *ユーザid@ドメイン*のフォーマットで指定します。

たとえば、以下のコマンドを使用すると、ユーザ ID が crowe というユーザのために INBOX という名前のメールボックスを作成できます。INBOX は crowe 宛てのメールが配信されるデフォルトのメールボックスです。

```
mboxutil -c user/crowe/INBOX
```

重要： INBOX というメールボックス名は、各ユーザのデフォルトメールボックス名として予約されています。INBOX は、大文字と小文字が区別されない唯一のフォルダ名です。その他のフォルダ名の場合は、すべて大文字と小文字が区別されます。

例

全ユーザの全メールボックスのリストを表示するには：

```
mboxutil -l
```

パスおよび ACL 情報と共に全メールボックスのリストを表示するには：

```
mboxutil -l -x
```

ユーザ daphne のデフォルトメールボックス INBOX を作成するには：

```
mboxutil -c user/daphne/INBOX
```

ユーザ delilah のメールフォルダ projx を削除するには：

```
mboxutil -d user/delilah/projx
```

ユーザ druscilla のデフォルトメールボックス INBOX および*その他のすべてのメールフォルダ*を削除するには：

```
mboxutil -d user/druscilla/INBOX
```

ユーザ desdemona のメールフォルダ memos の名前を memos-april に変更するには：

```
mboxutil -r user/desdemona/memos user/desdemona/memos-april
```

ユーザ dulcinea のメールフォルダ legal をロックするには：

```
mboxutil -k user/dulcinea/legal コマンド
```

*コマンド*はフォルダがロック中に実行されるコマンドです。

ユーザ dimitria のメールアカウントを別のパーティションに移動するには：

```
mboxutil -r user/dimitria/INBOX user/dimitria/INBOX パーティション
```

*パーティション*は移動先パーティションの名前です。

ユーザ dimitria のメールフォルダ personal を別のパーティションに移動するには：

```
mboxutil -r user/dimitria/personal user/dimitria/personal パーティション
```

hashdir ユーティリティ

メッセージストア内のメールボックスは、迅速な検索が行えるようにハッシュ構造で保存されています。したがって、特定のユーザのメールボックスのあるディレクトリを探すには、hashdir ユーティリティを使います。

このユーティリティは、特定のアカウントに割り当てられているメッセージストアを含むディレクトリを検出し、メッセージストアへの相対パス (例 : d1/a7/) を報告します。このパスは、ユーザ ID に基づくディレクトリレベルの 1 つ上のディレクトリレベルへの相対パスであり、パス情報は標準出力に送られます。

たとえば、ユーザ crowe のメールボックスへの相対パスを検索するには、以下のように指定します。

```
hashdir crowe
```

readership ユーティリティ

readership ユーティリティは、メールボックスの所有者以外のユーザで共有 IMAP フォルダ内のメッセージを読み込んだユーザの数を報告します。

IMAP フォルダの所有者が、他のユーザにフォルダ内のメッセージを読み込む許可を与えることがあります。所有者以外のユーザがアクセスできるフォルダは、**共有フォルダ**と呼ばれます。管理者は readership ユーティリティを使って、所有者以外に何人のユーザが共有フォルダにアクセスしたかをチェックできます。

このユーティリティはすべてのメールボックスをスキャンし、各共有フォルダについて 1 行ずつ情報を出力します。出力行には、共有フォルダにアクセスしたユーザ数およびメールボックス名が表示され、ユーザ数とメールボックス名の間は空白文字によって区切られています。

ユーザ数は、特定の期間に共有フォルダにアクセスした識別可能な ID を持つユーザの数を示します。個人のメールボックスへのアクセスはこの数に含まれません。個人のメールボックスは、所有者以外にアクセスしたユーザがいない限り報告されません。

たとえば、過去 15 日間に共有 IMAP フォルダにアクセスしたユーザの総数を調べるには、以下のように指定します。

```
readership -d 15
```

制限容量をモニタする

mboxutil ユーティリティを使用して、ユーザのディスク使用状況および制限容量の上限をモニタできます。mboxutil ユーティリティは、設定されている制限容量の上限のリストを生成し、ユーザのディスク使用状況に関する情報を提供します。各情報は、キロバイト単位で表示されます。

ユーザに対して設定されている制限容量に関する情報をすべて表示するには、以下の手順に従います。

```
mboxutil -a
```

crowe というユーザに対して設定されている制限容量に関する情報を表示するには:

```
mboxutil -u crowe
```

siroe.com ドメインに対して設定されている制限容量に関する情報を表示するには:

```
mboxutil -q siroe.com
```

ディスク容量をモニタする

システムがディスク使用容量をモニタする頻度、および警告を発行する条件を指定できます。ディスク使用容量のモニタおよび通知発行を設定するには、configutil コマンドを使用して警告に関する属性を設定します。属性の詳細については、表 10-5 を参照してください。

表 10-5　　警告に関するディスク容量属性

ディスク容量属性	デフォルト値
alarm.diskavail.msgalarmstatinterval	3600 秒
alarm.diskavail.msgalarmthreshold	10 パーセント
alarm.diskavail.msgalarmwarninginterval	24 時間

システムが 600 秒ごとにディスク使用容量をモニタするように設定するには:

```
configutil -o alarm.diskavail.msgalarmstatinterval -v 600
```

使用可能なディスク容量が 20 パーセント以下になったらサーバが警告を発行するように設定するには:

```
configutil -o alarm.diskavail.msgalarmthreshold -v 20
```

警告に関する属性を設定する方法については、『Messaging Server リファレンスマニュアル』を参照してください。

stored ユーティリティを使用する

stored ユーティリティは、サーバに対して以下のモニタタスクおよびメンテナンスタスクを実行します。

- バックグラウンドタスクおよび日常的なメッセージングタスク
- デッドロックの検出およびデッドロックしたデータベーストランザクションのロールバック
- 起動時における一時ファイルのクリーンアップ
- 存続期間決定ポリシーの実施
- サーバの状態、ディスク容量、サービスへの応答時間などの周期的なモニタ
- 必要に応じた警告の発行

stored ユーティリティは、自動的に毎日午後 11 時にクリーンアップや有効期限関連の操作を実行します。これらの操作の頻度を高くすることも可能です。

また、stored ユーティリティは、メールボックスデータベースやログファイルのバックアップ作成にも使用できます。バックアップを作成しておくと、データベースが壊れても再構築することなく復元できます。データベースのバックアップを作成するには、configutil コマンドを使用し、以下のパラメータ値を指定します。

```
configutil -o local.store.snapshotinterval -v 数値
```

数値 は stored がデータベースのバックアップを作成する頻度を指定するための値であり、分単位の間隔を示します。

```
configutil -o local.store.snapshotpath -v パス
```

*パス*はバックアップコピーの場所を示します。

表 10-6 に、stored オプションの一覧を示します。また、その下には一般的な使用例が記されています。構文や使用条件の詳細については、『Messaging Server リファレンスマニュアル』を参照してください。

表 10-6　stored オプション

オプション	説明
-c	消去されたメッセージをディスクからクリーンアップします。1 回だけ実行して終了します。-c オプションは繰り返し実行されるものではないため、-1 オプションを指定する必要はありません。
-d	デーモンとして動作し、システムチェック、警告の有効化、デッドロックの検出、およびデータベースの修復を行います。
-1	1 回だけ実行して終了します。
-n	トライアルモードでしか実行できません。メッセージ存続期間のカウントやクリーンアップは行いません。1 回だけ実行して終了します。
-v	詳細モード出力を行います。
-v -v	さらなる詳細モード出力。

有効期限ポリシーをテストするには :

```
stored -n
```

存続期間のチェックやクリーンアップを 1 回だけ実行するには :

```
stored -l -v
```

自動クリーンアップや有効期限関連操作の時刻を変更するには (configutil ユーティリティを使用) :

```
configutil -o store.expirestart -v 21
```

たとえばメールボックスリストデータベースが壊れた場合など、stored ユーティリティを再起動する必要が生じることもあります。UNIX で stored を再起動するには、コマンドラインで以下のように指定します。

サーバ - ルート /msg- *インスタンス* /stop-msg store
サーバ - ルート /msg- *インスタンス* /start-msg store

サーバデーモンがクラッシュした場合は、すべてのデーモンを停止し、stored を含むすべてのデーモンを再起動する必要があります。

メールボックスやメールボックスデータベースを修復する

メールボックスが損傷した場合は、reconstruct ユーティリティを使って、メールボックスまたはメールボックスデータベースを再構築し、矛盾を修正できます。

reconstruct ユーティリティは、メールボックスまたはマスターメールボックスファイルを再構築し、矛盾を修正するためのユーティリティです。このユーティリティを使うと、メッセージストア内のデータ損傷がどのようなものであっても、ほぼ確実に復元できます。ただし、トランザクションの完遂や不完全なトランザクションのロールバックなど、低レベルのデータベース修復は stored -d で実行されることに注意してください。

表 10-7 に、reconstruct の各オプションを示します。構文や使用条件の詳細については、『Messaging Server リファレンスマニュアル』を参照してください。

表 10-7　reconstruct のオプション

オプション	説明
-f	整合性チェックを行わず再構築を強行します。また、このオプションは、整合性チェックを実行し、問題がなかった場合に再構築を強行する場合にも使用できます。
-m	高レベルの整合性チェックおよびメールボックスデータベースの修復を行います。スプール領域のすべてのメールボックスをチェックし、必要に応じてメールボックスデータベースのエントリを追加または削除します。エントリの追加 / 削除を行った場合は、データベースが再構築時にチェックポイントされるようにするには、このオプションと stored -d を併用します。
-n	整合性チェックを行いますが、問題が検知された場合でも修復は行いません。このオプションは主にデバッグ目的で使用するものですが、ストアをチェックするために使用することも可能です。
-o	孤立したアカウント、つまり 対応するエントリが LDAP にないメールボックスがメッセージングサーバホストに存在するかどうかをチェックします。たとえば、-o オプションは、LDAP から削除されたか、または別のサーバホストに移されたユーザの受信箱を検出します。孤立したアカウントがあると、reconstruct は標準出力に以下のコマンドを書き込みます。 mboxutil -d user/ *ユーザ id*/INBOX

表 10-7　**reconstruct のオプション**（続き）

オプション	説明
-o -d *ファイル名*	-d　*ファイル名*が -o オプションと併用されている場合、reconstruct は指定したファイルに mboxutil -d コマンドを書き込みます。孤立したアカウントを削除するためにこのファイルをスクリプトファイルにすることも可能です。
-p *パーティション*	パーティション名を指定します。このオプションは、最初の reconstruct に使用できます。
-q	制限容量サブシステム内の矛盾 (制限容量ルートが不正確なメールボックスや、使用容量に関する報告が不正確な制限容量ルートなど) を修正します。-q オプションは、他のサーバプロセスが実行中の場合でも実行できます。
-r [*メールボックス*]	整合性チェックを行い、必要に応じて指定したメールボックス (1 つまたは複数) のパーティション領域を修復します。-r オプションは、必要に応じて指定メールボックス内のサブメールボックスの修復も行います。メールボックス引数を指定せずに -r オプションを使用すると、ユーティリティは必要に応じてデータベース内の全メールボックスのスプール領域を修復します。

メールボックスを再構築する

メールボックスを再構築するには、-r オプションを使用します。このオプションは、以下のような場合に使用してください。

- メールボックスにアクセスすると「システム入出力エラー」または「メールボックスのフォーマットが不正です」という旨のエラーが表示される場合。
- メールボックスにアクセスするとサーバがクラッシュする場合。
- スプールディレクトリにファイルが追加された場合、またはディレクトリからファイルが削除された場合。

5.0 リリースでは、reconstruct -r は整合性チェックを実行し、結果を報告し、問題が検出された場合にのみ再構築を実行します。したがって、このリリースでは、reconstruct ユーティリティのパフォーマンスが向上していると言えます。

reconstruct は、以下の例のように使用できます。

daphne というユーザのメールボックスに対してスプール領域を再構築するには :

```
reconstruct -r user/daphne
```

メールボックスデータベースにリストされているすべてのメールボックスに対してスプール領域を再構築するには :

```
reconstruct -r
```

ただし、メッセージストアの規模が大きいと、メールボックスデータベースにリストされているすべてのメールボックスに対してスプール領域を再構築するのに非常に長い時間がかかります (240 ページの「reconstruct のパフォーマンス」を参照してください)。万一の場合に備える最善の方法として、メッセージストア用に複数のディスクを使用することもできます。この方法を利用すると、1 つのディスクに問題が発生しても、メッセージストア全体が影響を受けることはありません。したがって、ディスクが損傷した場合でも、-p オプションを以下のように使用して、ストアを部分的に再構築するだけで済みます。

```
reconstruct -r -p サブパーティション
```

引数として指定されているメールボックスが primary パーティションにある場合にのみ再構築を実行するには :

```
reconstruct -p primary mbox1 mbox2 mbox3
```

primary パーティション内のすべてのメールボックスを再構築する必要がある場合には :

```
reconstruct -r -p primary
```

整合性チェックを省略してフォルダの再構築を強行するには、-f オプションを使用します。ユーザフォルダ daphne の再構築を強行するには :

```
reconstruct -f -r user/daphne
```

修復を行わず、全メールボックスのチェックだけを実行するには (-n オプションを使用) :

```
reconstruct -r -n
```

メールボックスをチェック / 修復する

メールボックスデータベースの高レベルな整合性チェックおよび修復を実行するには :

```
reconstruct -m
```

-m オプションは、以下のような場合に使用します。

- ストアスプール領域から 1 つ以上のディレクトリが削除されたため、メールボックスデータベースのエントリを削除する必要がある場合。
- ストアスプール領域に 1 つ以上のディレクトリがリストアされたため、メールボックスデータベースのエントリを追加する必要がある場合。
- stored -d オプションではデータベースの整合性を修復できない場合。

  stored -d オプションでデータベースの整合性を修復できない場合は、以下の手順を順番に実行します。

  - すべてのサーバを停止します。
  - *サーバルート*/msg-*インスタンス*/store/mboxlist ディレクトリからすべてのファイルを削除します。
  - サーバプロセスを再起動します。
  - reconstruct -m を使用し、スプール領域の内容に基づいて新しいメールボックス データベースを構築します。

孤立したアカウントを削除する

孤立したアカウント (対応するエントリが LDAP に存在しないメールボックス) を検索するには :

```
reconstruct -o
```

コマンド出力 :

```
reconstruct: Start checking for orphaned mailboxes
mboxutil -d user/test/annie/INBOX
mboxutil -d user/test/oliver/INBOX
reconstruct: Found 2 orphaned mailbox(es)
reconstruct: Done checking for orphaned mailboxes
```

孤立したメールボックスの削除に使用するスクリプトファイルに変換できる、孤立したメールボックスのリストを含む orphans.cmd という名前のファイルを作成するには :

```
reconstruct -o -d orphans.cmd
```

コマンド出力 :

```
reconstruct: Start checking for orphaned mailboxes
reconstruct: Found 2 orphaned mailbox(es)
reconstruct: Done checking for orphaned mailboxes
```

reconstruct のパフォーマンス

reconstruct があるタスクを完了するために必要な時間は、以下の要素に左右されます。

- 実行するタスクおよび選択されたオプションの種類
- ディスクパフォーマンス
- reconstruct -m の実行時に存在しているフォルダの数
- reconstruct -r の実行時に存在しているメッセージの数
- メッセージストア全体のサイズ
- システムが他にどのようなプロセスを実行しているか、およびシステムがどの程度ビジーであるか
- POP、IMAP、HTTP、または SMTP アクティビティが進行中であるかどうか

reconstruct -r オプションは最初の整合性チェックを実行します。再構築するフォルダの数によっては、このチェックで reconstruct のパフォーマンスが向上することもあります。

たとえば、ユーザ数が 2400、メッセージストアのサイズが 85 GB、サーバが POP、IMAP、または SMTP アクティビティを実行中という状況で実験した場合、以下のような結果が報告されています。

- reconstruct -m を完了するのに必要な時間 : 1 時間
- reconstruct -r -f を完了するのに必要な時間 : 18 時間

注 サーバで POP、IMAP、HTTP、または SMTP アクティビティが進行中でなければ、reconstruct の操作に必要な時間は大きく短縮される可能性があります。

ユーザのアカウントを移動する

MoveUser ユーティリティは、ユーザのアカウントをメッセージングサーバ間で移動するためのユーティリティです。ユーザアカウントを移動する場合は、ユーザのメールボックスおよびそこに含まれるメッセージも同じサーバに移動する必要があります。また、MoveUser は、メールボックスの移動に加え、mailhost 新しい名およびメッセージストアパスを反映するために Directory Server のエントリを更新します。

MoveUser ユーティリティを使用するには、MoveUser コマンドに -a オプションを含め、認証を受ける必要があります。正当なメッセージストア管理者であれば誰でも MoveUser コマンドを実行できます。ユーザにストア管理者特権を与えるには以下の方法があります。

- 特定の Messaging Server に対するメッセージストア管理特権を与えるには、iPlanet Console を使用します。詳細については、218 ページの「ストアへの管理者アクセスを指定する」を参照してください。
- DA トップレベル管理者は、自動的にメールシステム全体のメッセージストア管理特権を与えられます。
- DA ドメイン管理者は、自動的にドメインのメッセージストア管理特権を与えられます。

表 10-8 に、MoveUser の各オプションを示します。また、その後にはオプションの使用例が記されています。構文や使用条件の詳細については、『Messaging Server リファレンスマニュアル』を参照してください。

表 10-8　MoveUser のオプション

オプション	説明
-a *デスティネーションプロキシユーザ*	デスティネーションメッセージングサーバのプロキシ認証ユーザ。
-A	LDAP エントリに他の電子メールアドレスを追加しません。
-d *デスティネーションメールホスト*	デスティネーションメッセージングサーバ
-D *バインド dn*	*dn* を指定した *ldapURL* にバインドします。
-F	メールボックスの移動に成功した場合に、ソースメッセージングサーバからメッセージを削除します。このオプションを指定しなかった場合、メッセージはソースメッセージングサーバに残ります。
-h	指定したコマンドに関するヘルプを表示します。
-l *ldapURL*	Directory Server との接続を確立するための URL。
-L	Messaging Server のライセンスを追加します (まだ設定されていない場合)。
-m *デスティネーションメールドロップ*	デスティネーションメッセージングサーバのメッセージストアパス。指定されていない場合は、デフォルトが使用されます。
-n *メッセージ数*	一度に削除するメッセージの数。
-o *ソースメールドロップ*	ソースメッセージングサーバのメッセージストアパス。指定されていない場合は、デフォルトが使用されます。
-p *ソースプロキシパスワード*	ソースメッセージングサーバのプロキシ認証パスワード。
-s *ソースメールホスト*	ソースメッセージングサーバ。
-S	各ユーザ用に新しいメッセージストアパスを設定しません。
-u *ユーザ id*	削除するメールボックスの所有者であるユーザの ID。-l オプションとは併用できません。
-U *新規ユーザ id*	メールボックスの移動先となる新しい (名前変更後の) ユーザ ID。
-v *デスティネーションプロキシパスワード*	デスティネーションメッセージングサーバのプロキシ認証パスワード。
-w *バインドパスワード*	-D オプションが指定する *バインド dn* のバインディングパスワード。
-x *ソースプロキシユーザ*	ソースメッセージングサーバのプロキシ認証ユーザ。

Directory Server siroe.com のアカウント情報に基づいて、すべてのユーザを host1 から host2 に移動するには:

```
MoveUser -l \
  "ldap://siroe.com:389/o=Siroe.com???\
  (mailhost=host1.domain.com)" \
  -D "cn=Directory Manager" -w パスワード -s host1 -x admin \
  -p パスワード -d host2 -a admin -v パスワード
```

Directory Server siroe.com のアカウント情報に基づいて、1 人のユーザを、ポート 150 を使用する host1 から host2 に移動するには:

```
MoveUser -l \
  "ldap://siroe.com:389/o=Siroe.com???(uid= ユーザ id)" \
  -D "cn=Directory Manager" -w パスワード -s host1:150 -x admin \
  -p パスワード -d host2 -a admin -v パスワード
```

Directory Server server1.siroe.com のアカウント情報に基づいて、ID が「s」で始まるすべてのユーザを host1 から host2 に移動するには:

```
MoveUser -l \
  "ldap://server1.siroe.com:389/o=Siroe.com???(uid=s*)" \
  -D "cn=Directory Manager" -w パスワード -s host1 -x admin \
  -p パスワード -d host2 -a admin -v パスワード
```

admin というユーザ ID がコマンドライン中で指定されている場合に、そのユーザのメールボックスを host1 から host2 に移動するには:

```
MoveUser -u uid \
  -s host1 -x admin -p パスワード \
  -d host2 -a admin -v パスワード
```

host1 のユーザ aldonza を host2 に移動し、ID を dulcinea に変更するには:

```
MoveUser -u aldonza -U dulcinea \
  -s host1 -x admin -p パスワード \
  -d host2 -a admin -v パスワード
```

メッセージストアをバックアップ、リストアする

バックアップおよびリストアは、最も一般的でかつ重要な管理タスクです。以下のような問題が発生した場合にデータの損失を避けられるよう、メッセージストアのバックアップ / リストアポリシーを準備しておく必要があります。

- システムクラッシュ
- ハードウェアの故障
- 誤ってメッセージやメールボックスを削除してしまった場合
- システムの再インストールまたはアップグレード時に問題が発生した場合
- 天災 (地震、火事、台風など)

また、ユーザを移動する場合にもデータをバックアップしておく必要があります。

Messaging Server には、メッセージストアのバックアップおよびリストアに使用できるコマンドラインユーティリティが備わっています。また、Messaging Server は Legato Networker との統合ソリューションも提供しています。

Messaging Server に備わっているのは、単一コピーバックアップのプロシージャです。ある特定のメッセージが何個のユーザフォルダに含まれているかということには関係なく、最初に検出されたファイルだけがバックアップされます。2 つ目以降のメッセージコピーは、最初のメッセージファイル名へのリンクとしてバックアップされます。`backup` ユーティリティは、メッセージファイルのデバイスと i ノードをインデックスとして使用し、全メッセージのハッシュテーブルを保守します。ただし、この方法はデータのリストアに影響を及ぼすので注意してください。詳細については、247 ページの「部分的リストアを行う場合の注意事項」を参照してください。

この項では、以下の事項について説明します。

バックアップポリシーを作成する

バックアップポリシーを決定する際には、以下の要素を考慮する必要があります。

- ピーク時の負荷
- フルバックアップとインクリメンタルバックアップ
- 並列バックアップと直列バックアップ

ピーク時の負荷

システムのバックアップを計画する際には、時間的な負荷量の増減を考慮する必要があります。たとえば、午前 2 時などの早朝の時間帯にバックアップをスケジュールするのが良いでしょう。

フルバックアップとインクリメンタルバックアップ

インクリメンタルバックアップはストアをスキャンして変更があったデータのみをバックアップする方法で、フルバックアップはメッセージストア全体をバックアップする方法です。フルバックアップとインクリメンタルバックアップをそれぞれどの程度の頻度で実行するかを決定する必要があります。インクリメンタルバックアップは日常的なメンテナンスプロシージャの一環として実行すると良いでしょう。フルバックアップはデータを移動する場合などに適しています。

並列バックアップと直列バックアップ

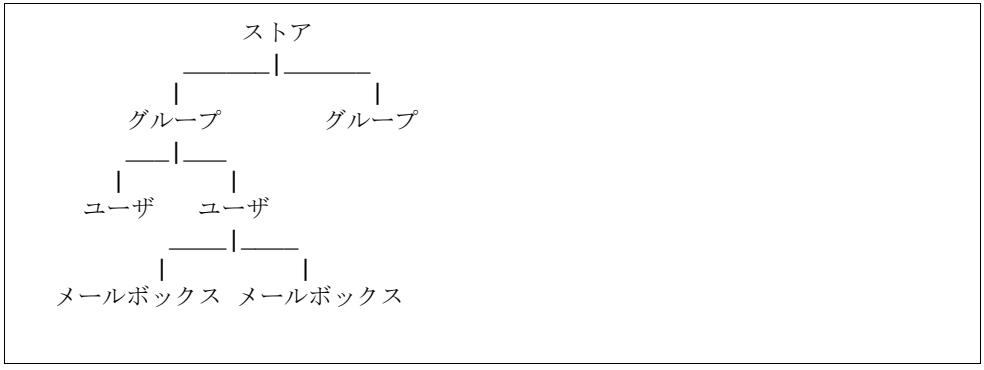
ユーザデータが複数のディスクに保存されている場合は、並列的にユーザグループのデータをバックアップできます。システムリソースによっては、このような並列バックアップを行うことでバックアップ全体に必要な時間を短縮できる場合もあります。しかし、サーバのパフォーマンスに影響を与えたくない場合は、直列バックアップを選択した方が良いでしょう。バックアップ方法は、システム負荷、ハードウェア設定、使用可能なテープドライブの数など、さまざまな要素を考慮して決定するようにしてください。

バックアップグループを作成する

ユーザをグループに分けることで、より効果的なバックアップ管理が可能になります。たとえば、グループごとにバックアップセッションをスケジュールしたり、複数のグループを同時にバックアップすることができます。

たとえばユーザメッセージが前述の例のようにユーザの姓に基づいて保存されている場合、姓の頭文字が A から F までのユーザを 1 つのバックアップグループとして認識させて、頭文字が G から M までのユーザは別のバックアップグループとして認識させることができます。

メッセージストアを論理的に表すと、次の図のようになります。



ユーザをグループに分けることで、より優れたバックアップ管理が可能になります。たとえば、グループごとにバックアップセッションをスケジュールしたり、複数のグループを同時にバックアップすることができます。バックアップグループの作成方法については、245 ページの「バックアップグループを作成する」を参照してください。

バックアップグループを作成するには、グループ定義を保存するための設定ファイルを作成する必要があります。このファイルには backup-groups.conf という名前を付け、以下のディレクトリに保存します。

サーバルート /msg- *インスタンス* /config/backup-groups.conf

このファイルのフォーマットは以下のとおりです。

```
グループ= 定義
グループ= 定義
.
.
.
```

たとえば、ユーザ ID の頭文字に基づいてユーザをグループ化するには、以下の定義を使用します。

```
groupA=a*
groupB=b*
groupC=c*
```

バックアップオブジェクトの名前は、以下のように、メッセージストアの論理構造に従って付けられます。

/ *サーバ* / *グループ* / *ユーザ* / *メールボックス*

「*サーバ*」は、メッセージストアのインスタンス名です （例、siroe）。

Messaging Server には、backup-groups 設定ファイルを作成せずに使用できるデフォルトのバックアップグループが 1 つあります。ALL という名前のこのグループには、すべてのユーザが含まれています。

Messaging Server バックアップ / リストアユーティリティ

Messaging Server には、データをバックアップおよびリストアするための imsbackup および imsrestore ユーティリティが備わっています。

imsbackup ユーティリティおよび imsrestore ユーティリティは、一般的なバックアップを行うために提供されているものではありません。これらのユーティリティには、Legato Networker などの多目的ツールが持つ高度な機能はありません。たとえば、テープ自動チェンジャサポート機能には制限があり、1 つのストアの内容を同時に複数のデバイスに書き込むことはできません。総合的なバックアップは、Legato Networker などのツールに対するプラグインを介して行われます。Legato Networker の使用方法については、249 ページの「Legato Networker を使用する」を参照してください。

imsbackup ユーティリティ

imsbackup を使用すると、メッセージストアの内容を部分的に選択し、磁気テープ、UNIX パイプ、ファイルなど、さまざまなシリアルデバイスに書き込むことができます。作成したバックアップの一部または全体をリストアするには、imsrestore ユーティリティを使用します。imsbackup の出力を imsrestore にパイプすることも可能です。

バックアップを行うには、imsbackup コマンドを使用します。以下の例では、user1 が backupfile にバックアップされます。

```
imsbackup -f backupfile /mystore/ALL/user1
```

このコマンドは、20 というデフォルトのブロッキングファクタを使用します。imsbackup コマンドの構文の詳細については、『Messaging Server リファレンスマニュアル』を参照してください。

imsrestore ユーティリティ

バックアップデバイスからメッセージをリストアするには、imsrestore コマンドを使用します。以下の例では、backupfile ファイルから user1 のメッセージがリストアされます。

```
imsrestore -f backupfile /mystore/ALL/user1
```

imsbackup コマンドの構文の詳細については、『Messaging Server リファレンス マニュアル』を参照してください。

部分的リストアを行う場合の注意事項

単一コピーバックアッププロシージャに従ってバックアップしたメッセージをリストアする際には、以下の事項に注意してください。

- **フルリストア :** フルリストアの場合、リンクされたメッセージはリンク先メッセージと同じ i ノード をポイントします。
- **部分的バックアップ / リストア :** 部分的バックアップおよびリストアでは、メッセージストアの単一コピー特性が維持されないことがあります。

以下のように 3 人のユーザ A、B、C に属するメッセージがあると仮定します。

A/INBOX/1
B/INBOX/1
C/INBOX/1

例 1 : システムは以下のように部分的バックアップおよびフルリストアを実行します。

1 ユーザ B および C をバックアップします。

2 ユーザ B および C を削除します。

3 手順 1 で作成したバックアップデータをリストアします。

この例で、B/INBOX/1 および C/INBOX/1 には新しい i ノード 番号が割り当てられ、メッセージデータはディスクの新しい場所に書き込まれます。また、リストアされるのは最初のメッセージだけであり、2 つ目のメッセージは最初のメッセージへのハードリンクです。

例 2 : システムは以下のようにフルバックアップおよび部分的リストアを実行します。

1 フルバックアップを行います。

2 ユーザ A を削除します。

3 ユーザ A をリストアします。

A/INBOX/1 には新しい i ノード 番号が割り当てられます。

例 3 : この例では、部分的リストアを繰り返し試みる必要が生じることがあります。

1 フルバックアップを行います。

B/INBOX/1 および C/INBOX/1 は A/INBOX/1 へのリンクとしてバックアップされます。

2 ユーザ A および B を削除します。

3 ユーザ B をリストアします。

管理者に A/INBOX をリストアするよう指示が出されます。

4 ユーザ A および B をリストアします。

5 ユーザ A を削除します (オプション)。

注 部分的リストアの際に、すべてのメッセージが確実にリストアされるようにしたい場合は、`imsbackup` コマンドに `-i` オプションを使用します。`-i` オプションは、各メッセージを必要に応じて複数回バックアップします。このオプションは、POP 環境で最も便利なものです。

Legato Networker を使用する

Messaging Server には、Legato Networker などのサードパーティバックアップツール用のインターフェースを提供するバックアップ API があります。物理メッセージストアの構造およびデータフォーマットは、バックアップ API 内でカプセル化されます。バックアップ API はメッセージストアと直接通信を行い、バックアップサービスにメッセージストアの論理ビューを提供します。バックアップサービスは、このメッセージストアの論理ビューを利用してバックアップオブジェクトを保存および取得します。

Messaging Server では、Legato Networker の `save` および `recover` コマンドで呼び出せるアプリケーション特有モジュール (ASM) を使って、メッセージストアデータのバックアップおよびリストアを実行できます。ASM は Messaging Server `imsbackup` および `imsrestore` ユーティリティを呼び出します。

注　この項では、Messaging Server のメッセージストアと Legato Networker を併用する方法について説明します。Legato Networker のインターフェースについては、Legato に付属のマニュアルを参照してください。

Legato Networker を使ってデータをバックアップする

Legato Networker を使って Messaging Server メッセージストアをバックアップするには、Legato のインターフェースを呼び出す前に以下の手順を実行します。

1. `/usr/lib/nsr/imsasm` から *サーバルート*`/msg-`*インスタンス*`/bin/imsasm` へのシンボリックリンクを作成します。
2. Sun または Legato から `nsrfile` バイナリファイルのコピーを入手し、以下のディレクトリにコピーします。

   `/usr/lib/nsr/nsrfile`

3. グループごとにユーザをバックアップする場合は、以下の手順を実行します。

   a. 245 ページの「バックアップグループを作成する」の説明に従ってバックアップグループファイルを作成します。

   b. `mkbackupdir.sh` を実行して設定を確認します。

      サーバルート`/msg-`*インスタンス*`/backup` ディレクトリの構造を確認します。ディレクトリは、図 10-2 に示されているような構造になっていなければなりません。

   `backup-groups.conf` ファイルを指定しないと、すべてのユーザを含むデフォルトのバックアップグループ `ALL` が使用されます。

4 savegroup が mkbackupdir.sh スクリプトを呼び出せるように、/nsr/res/ ディレクトリに res ファイルを作成します。図 10-3 を参照してください。

NOTE Legato Networker には、saveset の名前に 64 文字という制限があります。デフォルトでは、mkbackupdir.sh によって、*serverRoot*/msg-*instance*/backup ディレクトリ内にストアイメージが作成されます。このディレクトリの名前とメールボックスの論理名 (例、siroe/groupA/fred) が 64 文字を超える場合には、mkbackupdir.sh -p を実行する必要があります。たとえば、次のコマンドを実行すると、"/" ディレクトリ内にバックアップイメージが作成されます。

```
mkbackupdir.sh -p /
```

図 10-2 に、バックアップグループディレクトリ構造の一例を示します。

図 10-2 バックアップグループディレクトリ構造

```
siroe-groupA-a1
            -a2
     -groupB-b1
            -b2
     -groupC-c1
            -c2
```

図 10-3 は nsr ディレクトリに含まれる IMS.res という名前のサンプル res ファイルです。

図 10-3 サンプル res ファイル

```
type: savepnpc
precmd: "echo mkbackupdir started",
   "/usr/siroe/server5/msg-siroe/bin/mkbackupdir.sh"
pstcmd: "echo imsbackup Completed";
timeout: "12:00 pm";
```

次に、以下の手順に従って Legato Networker のインターフェースを使用します。

1 必要に応じて Messaging Server の savegroup を作成します。

a. nwadmin を実行します。

b. Customize (カスタマイズ) | Group (グループ) | Create (作成) を選択します。

2 savepnpc をバックアップコマンドとして使用し、バックアップクライアントを作成します。

a. mkbackupdir によって作成されたディレクトリに saveset を設定します。

単一セッションのバックアップには *サーバルート* /msg- *インスタンス* /backup を使用します。

並列バックアップには *サーバルート* /msg- *インスタンス* /backup/ *サーバ* / *グループ* を使用します。

245 ページの「バックアップグループを作成する」の説明に従って、あらかじめ *グループ* を作成しておく必要があります。

また、parallelism をバックアップセッションの回数に設定しなければなりません。

詳細については、251 ページの「例 - Networker にバックアップクライアントを作成する」を参照してください。

3 Group Control (グループ制御) | Start (開始) を選択してバックアップ設定をテストします。

例 - Networker にバックアップクライアントを作成する Networker にバックアップクライアントを作成するには、nwadmin から Client (クライアント) | Client Setup (クライアントセットアップ) | Create (作成) を選択します。

```
Name: siroe
Group: IMS
Savesets:/usr/siroe/server5/msg-siroe/backup/siroe/groupA
   /usr/siroe/server5/msg-siroe/backup/siroe/groupB
   /usr/siroe/server5/msg-gotmail/backup/gotmail/groupC
         .
         .
Backup Command:savepnpc
Parallelism: 4
```

Legato Networker を使用してデータをリストアする

データのリストアには、Legato Networker の `nwrecover` インターフェースまたは `recover` コマンドラインユーティリティを使用できます。a1 というユーザの INBOX をリストアするには:

```
recover -a -f -s siroe
/usr/siroe/server5/msg-siroe/backup/siroe/groupA/a1/INBOX
```

メッセージストア全体をリストアするには:

```
recover -a -f -s siroe /usr/siroe/server5/msg-siroe/backup/siroe
```

第 11 章

セキュリティとアクセス制御を設定する

iPlanet Messaging Server には、広範囲にわたる柔軟なセキュリティ機能があります。これらの機能により、メッセージが中断されないようにしたり、不正侵入者がユーザや管理者を装ってシステムにアクセスすることを防ぐことができます。また、指定したユーザだけがメッセージシステム内の特定部分にアクセスできるように設定することも可能です。

Messaging Server のセキュリティアーキテクチャは iPlanet サーバのセキュリティアーキテクチャの一部であり、最大限の共同利用性および整合性が得られるように業界規格と公開プロトコルに基づいて構築されています。したがって、Messaging Server のセキュリティポリシーを実施するためには、本章だけでなく、他のマニュアルも参照して理解を深めておく必要があります。特に、『Netscape Console によるサーバの管理』に記載されている情報は、Messaging Server のセキュリティを設定するために必要な情報が記載されています。

この章には、以下の項目があります。

- サーバのセキュリティについて
- HTTP のセキュリティについて
- 認証機構を設定する
- ユーザパスワードログイン
- 暗号化と証明書に基づく認証を設定する
- Messaging Server への管理者アクセスを設定する
- POP、IMAP、および HTTP サービスへの クライアントアクセスを設定する
- SMTP サービスへのクライアントアクセスを設定する

サーバのセキュリティについて

サーバのセキュリティは、広範囲に及ぶさまざまな観点から考慮することができます。通常、企業のメッセージングシステムに欠かせない重要な条件として、承認されたユーザだけがサーバにアクセスできること、パスワードや個人情報が安全であること、ユーザが他のユーザを装って通信を行わないこと、必要に応じて通信の機密性が保たれることが挙げられます。

サーバのセキュリティはさまざまな方法によって危険にさらされる可能性があるため、それらに対するアプローチも多種多様です。この章では、暗号化、認証、およびアクセス制御に注目し、以下に挙げる Messaging Server のセキュリティ関連トピックについて説明します。

- **ユーザ ID とパスワードログイン :** ユーザは、IMAP、POP、HTTP、または SMTP にログインするためにユーザ ID とパスワードを入力する必要があります。また、メッセージの受信者に送信者認証を送る場合は、SMTP パスワードログインを使用します。
- **暗号化と認証 :** TLS および SSL プロトコルを使って通信を暗号化し、クライアントを認証できるようにサーバをセットアップします。
- **管理者アクセス制御 :** Netscape Console のアクセス制御機能を使って、Messaging Server や個々のタスクへのアクセスを委託します。
- **TCP クライアントアクセス制御 :** フィルタリング技術を使って、どのクライアントがサーバの POP、IMAP、HTTP、および SMTP サービスに接続できるかを制御します。

Messaging Server に関連するすべてのセキュリティ / アクセス問題が本章で取り上げられているわけではありません。本章以外で説明されているセキュリティ関連のトピックには、以下のものがあります。

- **物理的なセキュリティ :** サーバマシンを物理的に保護する設備がなければ、ソフトウェアのセキュリティも無意味になります。
- **メッセージの暗号化 (S/MIME):** Secure Multipurpose Internet Mail Extensions (S/MIME) があると、送信者はメッセージを暗号化してから送信することができ、また、受信者は受け取った暗号化メッセージを保存することができます。暗号化メッセージは、受信者がそれらを読むときに復号化されます。S/MIME を使用するのに、Messaging Server に関する特別な設定や作業は必要ありません。S/MIME はクライアントに依存するからです。S/MIME の設定方法については、お使いのクライアントに付属のマニュアルを参照してください。注意 : Messenger Express クライアントのインターフェースは、電子メールメッセージの暗号化をサポートしていません。
- **メッセージストアへのアクセス :** Messaging Server では、複数のメッセージストア管理者を定義することができます。これらの管理者は、メールボックスを表示および監視したり、メールボックスへのアクセスを制御することができます。詳細については、第 10 章 「メッセージストアを管理する」を参照してください。
- **エンドユーザアカウントの設定 :** エンドユーザアカウント情報は、主に Delegated Administrator 製品を使って管理されます。詳細については、Delegated Administrator のマニュアルを参照してください。また、エンドユーザアカウントは、コンソールのインターフェースを使って管理することもできます。詳細については、第 3 章 「メールユーザとメーリングリストを管理する」を参照してください。
- **UBE (unsolicited bulk email) のフィルタリング :** 第 9 章 「メールのフィルタリングとアクセス制御」を参照してください。

iPlanet では、さまざまセキュリティに関するトピックを提供できるように数多くの文書を用意しております。本章に記載されているトピックの背景、およびその他のセキュリティ関連情報については、iPlanet の Web サイトをご覧ください (http://docs.iplanet.com)。

HTTP のセキュリティについて

Messaging Server でサポートされている HTTP プロトコル用のセキュリティ機能は、IMAP プロトコル用のセキュリティ機能と同じものです。つまり、ユーザ ID/ パスワードによる認証とクライアント証明書による認証の両方がサポートされています。ただし、HTTP プロトコルと IMAP プロトコルとでは、クライアントとサーバ間におけるネットワーク接続の処理方法にいくつかの相違点があります。

POP、IMAP、または SMTP クライアントが Messaging Server にログインすると、接続が確立され、セッションが開始されます。この接続は、セッション間、すなわちログインしてからログアウトするまで維持されます。新しい接続を確立すると、クライアントはサーバに対して再び認証を行う必要があります。

HTTP クライアントが Messaging Server にログインすると、サーバからクライアントに固有のセッション ID が与えられます。クライアントは、このセッション ID を使って、同一セッション中に複数の接続を確立することができます。HTTP クライアントは接続を確立するたびに認証を行う必要はありません。クライアントが再び認証を行わなければならないのは、セッションが切断された場合とクライアントが新規のセッションを開始する場合だけです。ただし、HTTP セッションが指定された時間以上アイドル状態になると、サーバは自動的に HTTP セッションを切断し、クライアントは強制的にログアウトされます (デフォルトは 2 時間)。

HTTP セッションの接続は安全です。以下に、その理由を挙げます。

- セッション ID は、特定の IP アドレスにバインドされています。したがって、セッション ID が他のホストによって使用されることはありません。
- 各セッション ID には、タイムアウト値が関連付けられています。つまり、セッション ID が指定された時間を超えて使用されなかった場合、そのセッション ID は無効になります。
- 開いているすべてのセッションに対するセッション ID のデータベースがサーバに保管されます。そのため、クライアントが ID を偽造することは不可能です。
- セッション ID は、cookie ファイルではなく URL 内に保管されます。

設定パラメータを指定して接続パフォーマンスを向上させる方法については、第 4 章「POP、IMAP、および HTTP サービスを設定する」を参照してください。

認証機構を設定する

認証機構は、クライアントが不正なものでないことをサーバに証明するための一手段です。Messaging Server は SASL (Simple Authentication and Security Layer) プロトコルにより定義されている認証メソッドをサポートしており、また、証明書に基づく認証も使用できます。SASL による認証機構については、本章で説明しています。証明書に基づく認証については、259 ページの「暗号化と証明書に基づく認証を設定する」を参照してください。

Messaging Server では、パスワードに基づく認証を実施するにあたり、以下の SASL 認証メソッドがサポートされています。

- **PLAIN** - ユーザのテキスト形式パスワードがネットワークを介して渡されます。そのため、パスワードが盗まれる可能性があります。

  この問題は、SSL を使用することにより解消できます。詳細については、259 ページの「暗号化と証明書に基づく認証を設定する」を参照してください。

- **DIGEST-MD5** - RFC 2831 で定義されている HTTP ダイジェスト認証に基づくチャレンジ / レスポンス型認証機構。ただし、Messaging Multiplexor では、DIGEST-MD5 がサポートされていません。
- **CRAM-MD5** - APOP と同様のチャレンジ / レスポンス型認証機構。ただし、この機構は、APOP とは異なり、他のプロトコルにも使用できます。RFC 2195 で定義されています。
- **APOP** - POP3 専用のチャレンジ / レスポンス型認証機構。RFC 1939 で定義されています。

チャレンジ / レスポンス型の認証機構では、サーバからクライアントにチャレンジ文字列が送られます。その後、クライアントは、そのチャレンジのハッシュとユーザのパスワードを用いて応答します。クライアントの応答がサーバのハッシュに一致すると、そのユーザは認証されます。このハッシュには可逆性がないため、ネットワークを介して送信されるときにユーザのパスワードが危険にさらされることはありません。

注　POP、IMAP、および SMTP サービスでは、すべての SASL 機構がサポートされています。HTTP サービスでは、プレーンパスワードによる機構しかサポートされていません。

プレーンテキストパスワードへのアクセスを設定する

CRAM-MD5、DIGEST-MD5、または APOP SASL 認証メソッドでは、ユーザのプレーンテキストパスワードに対するアクセスが要求されます。そのため、以下の操作を行う必要があります。

1. パスワードが平文で保存されるように Directory Server を設定します。
2. Messaging Server を設定して Directory Server が平文のパスワードを使用していることを伝えます。

Directory Server を設定する

CRAM-MD5、DIGEST-MD5、または APOP 機構を使用するには、パスワードが平文で保存されるように Directory Server を設定する必要があります。以下の手順に従います。

1 コンソールで、設定対象の Directory Server を開きます。

2 [環境設定] タブをクリックします。

3 左側のパネルで [データベース] を開きます。

4 右ペインで [パスワード] をクリックします。

5 パスワード暗号化用のドロップダウンリストで [クリアテキスト] を選択します。

Messaging Server を設定する

次に、Messaging Server の設定を変更して、Directory Server が平文のパスワードを取り込めることを Messaging Server に知らせます。これにより、Messaging Server で APOP、CRAM-MD5、および DIGEST-MD5 を使用できるようになります。

```
configutil -o sasl.default.ldap.has_plain_passwords -v 1
```

SASL 機構を無効にする場合は、値を 0 または空白 (" ") に設定します。

注 既存のユーザは、パスワードを再設定または移行するまで APOP、CRAM-MD5、または DIGESt-MD5 を使用できません (次の「ユーザを移行する」の項を参照)。

ユーザを移行する

ユーザの移行に関する情報を指定するには、`configutil` を使用します。たとえば、ユーザパスワードが変わる場合や、適切なエントリがない機構を使ってクライアントが認証を試みようとする場合です。

```
configutil -o sasl.default.transition_criteria -v 値
```

「値」には、以下のいずれかを指定できます。

- `CHANGE` - ユーザ パスワードが変わると、サーバはテキスト形式のパスワードを受け入れるように移行します (デフォルト)。
- `CLIENT` - クライアントが適切なエントリのない機構を使用しようとすると、サーバはテキスト形式のパスワードを使って認証を行うようクライアントに指示を出します。その後、サーバは、同じパスワード値を使って目的のエントリを作成します。
- `PLAIN` - ユーザがテキスト形式のパスワードを使用すると、サーバはテキスト形式のパスワードを受け入れるように移行します。

ユーザを無事に移行するには、Messaging Server にユーザパスワード属性への書き込みアクセス権を与えるよう、Directory Server の ACI を設定する必要があります。以下の手順に従います。

1 コンソールで、設定対象の Directory Server を開きます。

2 [ディレクトリ] タブをクリックします。

3 ユーザ / グループツリーのベースサフィックスを選択します。

4 [オブジェクト] メニューの [アクセス権限] を選択します。

5 「Messaging Server エンドユーザ管理者書き込みアクセス権」に対する ACI を選択 (ダブルクリック) します。

6 [ACI の属性] をクリックします。

7 既存の属性のリストに `userpassword` 属性を追加します。

8 [OK] をクリックします。

ユーザパスワードログイン

Messaging Server にログインする際には、最初にパスワードの入力が求められます。これは、認可されていないユーザによるアクセスを防ぐために設けられた最初の防御手段です。Messaging Server では、IMAP、POP、HTTP、および SMTP の各サービスに対し、パスワードに基づくログインがサポートされています。

IMAP、POP、HTTP のパスワードログイン

特に設定を変更しない限り、ユーザーは Messaging Server からメッセージを取り込むためにパスワードを入力する必要があります。パスワードログインは、POP、IMAP、HTTP の各サービスごとに有効または無効にすることができます。POP、IMAP、HTTP サービスのパスワードログインの詳細については、62 ページの「パスワードに基づくログイン」を参照してください。

ユーザのクライアントソフトウェアからサーバにユーザパスワードが転送される際、パスワードは平文または暗号文 (POP の場合は例外) のいずれかの形態をとります。クライアントとサーバの両方が SSL を使用できるように設定されており、かつ必要な強度の暗号化機能 (264 ページの「SSL を有効にする符号化方式を選択する」を参照) がサポートされている場合には、暗号化が実行されます。

ユーザ ID とパスワードは、LDAP ユーザディレクトリに保管されています。最小長などのパスワードに関するセキュリティ条件は、ディレクトリポリシーの必要条件によってできまり、Messaging Server の管理に含まれません。

証明書に基づくログインは、パスワードに基づくログインに代わるものです。証明書に基づくログインについては、SSL の説明とともに本章で後述しています。267 ページの「証明書に基づくログインを設定する」を参照してください。

チャレンジ / レスポンス型の SASL 機構は、テキスト形式のパスワードを使ったログインに代わるものです。

SMTP のパスワードログイン

デフォルトでは、Messaging Server の SMTP サービスに接続してメッセージを送信するのに、ユーザはパスワードを入力する必要がありません。しかし、認証 SMTP 機能を有効にするために、パスワードを使って SMTP サービスにログインできるように設定することも可能です。

認証 SMTP は、クライアントがサーバに対して認証を行うことを可能にする、SMTP プロトコルの拡張機能です。メッセージの送信時に認証が行われます。認証 SMTP を使用する主な目的は、ローカルユーザが外出先から (または各自のホーム ISP を使用して) メールを送信 (リレー) するときに、他のユーザが悪用できるようなオープンリレーの発生を防ぐことです。クライアントは、AUTH コマンドを使ってサーバに対する認証を行います。

SMTP のパスワードログイン、すなわち 認証 SMTP を有効にする方法については、157 ページの「SMTP 認証と SASL」を参照してください。

認証 SMTP は、SSL 暗号化機能といっしょに (または SSL 暗号化機能を使わずに) 使用することができます。

暗号化と証明書に基づく認証を設定する

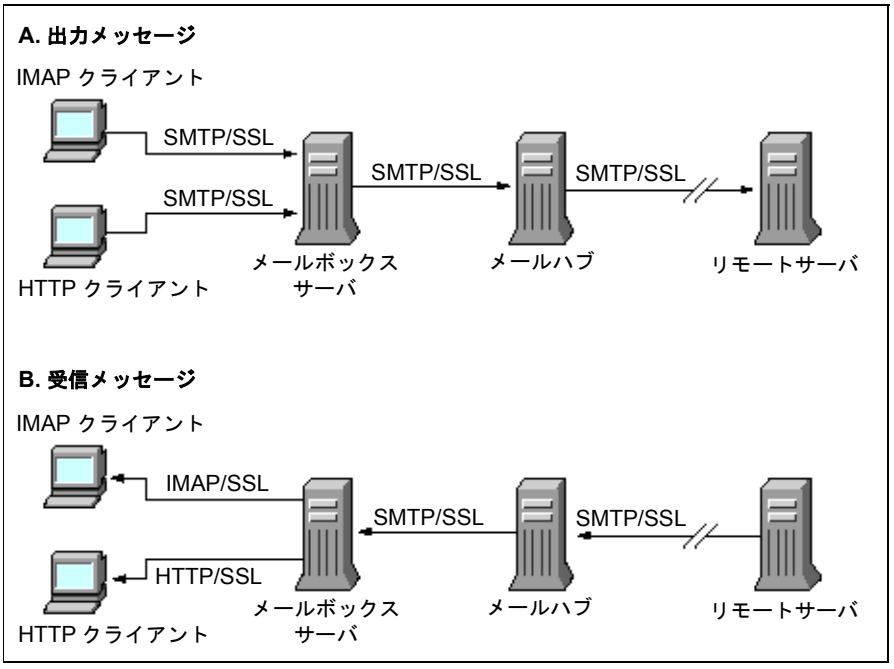
iPlanet Messaging Server は、暗号化通信およびクライアント / サーバ間の証明書に基づく認証を行うために TLS (Transport Layer Security) プロトコルを使用します。このプロトコルは、SSL (Secure Sockets Layer) を標準化したものとして知られています。iPlanet Messaging Server では、SSL バージョン 3.0 および 3.1 がサポートされています。TLS には、SSL との完全な互換性があり、必要な SSL 機能がすべて含まれています。

SSL に関する背景情報については、「Introduction to SSL」(『Netscape Console によるサーバの管理』の付録) を参照してください。SSL は、公開鍵暗号方式の概念に基づいています。この概念は、「Introduction to Public-Key Cryptography」(『Netscape Console によるサーバの管理』の付録) で説明されています。

Messaging Server とクライアント間、およびそのサーバと他のサーバ間におけるメッセージ送信が暗号化されるのであれば、通信上のプライバシーが朗詠する危険性はまずありません。また、接続しているクライアントが認証されたものである場合には、それらのクライアントを装って (スプーフして) 侵入者が介入してくる危険性もありません。

SSL は、IMAP4、HTTP、および SMTP のアプリケーション層の下で、プロトコル層の役割を果たします。SMTP と SMTP/SSL は同一のポートを使用しますが、HTTP と HTTP/SSL にはそれぞれ別のポートが必要です。IMAP と IMAP/SSL の場合は、同一のポートを使用することも別のポートを使用することも可能です。図 11-1 に示すように、SSL は、送信メッセージと受信メッセージの両方においてメッセージ通信の特定の段階で動作します。

図 11-1　　Messaging Server の暗号化通信



SSL はホップ間 (hop-to-hop) の暗号化を提供しますが、各中間サーバではメッセージが暗号化されません。クライアントが S/MIME をサポートするためには、エンド間 (end-to-end) の暗号化が必要です。

注　　通信メッセージに対して暗号化を有効にするには、チャネル定義に `maytls` や `musttls` などの `tls` チャネルキーワードを含める必要があります。詳細については、『Messaging Server リファレンスマニュアル』を参照してください。

SSL 接続を設定する際にオーバーヘッドが大きくなると、サーバのパフォーマンスが下がる可能性があります。メッセージングシステムの設計およびパフォーマンス分析の段階で、セキュリティニーズとパフォーマンスのバランスをとる必要があります。

注 SSL はすべての iPlanet サーバでサポートされており、SSL を設定するための コンソールインターフェースはどのサーバの場合でもほとんど同じです。そのため、本章で説明しているタスクの一部は、『Netscape Console によるサーバの管理』の SSL に関する章でより詳しく説明されています。本章では、これらのタスクについて、その要約だけを説明します。

証明書を入手する

SSL を使用する目的が暗号化または認証のいずれであっても、お使いの Messaging Server のサーバ証明書を入手する必要があります。この証明書は、お使いのサーバをクライアントや他のサーバと区別するために使用されます。

内部モジュールと外部モジュールを管理する

サーバ証明書によって、キーペアの所有権および有効性が確立されます。キーペアとは、データの暗号化および暗号解除に使用される数値のことです。お使いのサーバの証明書とキーペアは、そのサーバのアイデンティティを表すもので、サーバ内部または取り外し可能な外部ハードウェアカード (スマートカード) の証明書データベース内に保管されます。

iPlanet サーバは、PKCS (Public-Key Cryptography System) #11 API に準拠するモジュールを使って、キーと証明書のデータベースにアクセスします。通常、ハードウェアデバイスの PKCS #11 モジュールは、そのデバイスの販売元から入手することができます。このモジュールを Messaging Server にインストールしないと、Messaging Server はそのデバイスを使用することができません。システムには「Netscape Internal PKCS # 11 Module」が既にインストールされていますが、これはサーバ内部の証明書データベースを使用する単一の内部ソフトウェアトークンです。

サーバの証明書設定には、証明書とそのキーを格納するためのデータベースを作成する作業と PKCS #11 モジュールをインストールする作業とが関与します。外部のハードウェア トークンを使用しない場合は、サーバ上に内部データベースを作成し、デフォルトの内部モジュール (Messaging Server の一部) を使用します。外部トークンを使用する場合は、ハードウェアスマートカードリーダーを接続し、その PKCS #11 モジュールをインストールします。

PKCS #11 モジュールは、それが外部モジュールまたは内部モジュールのいずれであっても、コンソールを使って管理できます。PKCS #11 モジュールをインストールするには :

1 カードウェアカードリーダーを Messaging Server ホストマシンに接続し、ドライバをインストールします。

2 コンソールの [PKCS #11 の管理] インターフェースを使って、インストールしたドライバに対する PKCS #11 モジュールをインストールします。

詳細については、『Netscape Console によるサーバの管理』の SSL に関する章を参照してください。

ハードウェア暗号化アクセラレータをインストールする 暗号化用に SSL を使用する場合は、ハードウェア暗号化アクセラレータをインストールすることにより、メッセージの暗号化および復号化におけるパフォーマンスを上げることができます。一般に、暗号化アクセラレータは、サーバマシンに常設されたハードウェアボードとソフトウェアドライバから成ります。iPlanet Messaging Server では、PKCS #11 API に従うアクセラレータモジュールがサポートされています (これらは独自のキーを持たないハードウェアトークンです。つまり、キーの保管には内部データベースが使用されます)。提供された指示に従って、まず、ハードウェアとドライバをインストールして、アクセラレータをインストールします。その後、PKCS #11 モジュールをインストールして、ハードウェア証明書トークンのインストールを完了します。

サーバ証明書を要求する

サーバ証明書を要求するには、iPlanet Console でサーバ証明書を要求し、[証明書セットアップウィザード] を実行します。このウィザードは、[コンソール] メニューまたは Messaging Server の [暗号化] タブからアクセスすることができます。証明書セットアップウィザードを使って、以下のタスクを実行します。

1 証明書要求を作成します。

2 電子メールで、認証局 (CA) に要求を送ります。認証局から証明書が発行されます。

認証局 (CA) から電子メールによる応答を受け取ったら、その内容をテキスト形式でファイルに保存し、証明書セットアップウィザードを使って証明書をインストールします。

詳細については、『Netscape Console によるサーバの管理』の SSL に関する章を参照してください。

証明書をインストールする

証明書の要求とインストールは、それぞれ別のプロセスを意味します。証明書の要求に対して認証局 (CA) から電子メールによる応答を受け取ったら、その内容をテキスト形式でファイルに保存し、証明書セットアップウィザードを使って証明書をインストールします。

1 既に入手した証明書をインストールしようとしていることをウィザードに知らせます。

2 指示に従って、証明書のテキストをフィールド内に貼り付けます。

詳細については、『Netscape Console によるサーバの管理』の SSL に関する章を参照してください。

注 CA 証明書 (以下に説明) をインストールするには、このプロセスを実行する必要があります。クライアントによって提示された証明書が信頼できるものであるかどうかをサーバが CA 証明書を使用して判断します。

認証済み認証局の証明書をインストールする

証明書セットアップウィザードを使って、認証局の証明書 (CA 証明書) もインストールします。CA 証明書とは、認証局自体のアイデンティティを確証するためのものです。サーバは、クライアントや他のサーバを認証する過程でこれらの CA 証明書を使用します。

たとえば、パスワードに基づく認証 (267 ページの「証明書に基づくログインを設定する」) に加え、証明書に基づく認証も使用するように設定した場合は、クライアントによって提示される可能性のある証明書の発行元認証局のうち、信頼できるすべての認証局の CA 証明書をインストールする必要があります。これらの認証局は、自社の内部組織であったり、または民間機関、政府機関、他の企業などの外部組織である場合があります (CA 証明書の使用については、『Netscape Console によるサーバの管理』の「Introduction to Cryptography」を参照してください)。

Messaging Server には、いくつかの民間認証局に対する CA 証明書が既に備わっています。他の民間認証局の CA 証明書を追加する場合や、自分の所属する企業が (iPlanet Certificate Server を使って) 社内で使用するための独自の認証局を開発している場合には、さらに CA 証明書を入手し、インストールする必要があります。

注 Messaging Server により自動的に提供される CA 証明書は、最初はクライアント証明書に対し「認証済み (信頼できる)」になっていません。したがって、これらの認証局から発行されるクライアント証明書を「認証済み」として扱いたい場合には、信頼設定を編集する必要があります。詳細については、263 ページの「証明書と認証済み CA を管理する」を参照してください。

新しい CA 証明書を要求してインストールするには、以下の操作を行います。

1. Web ページを通じて、または電子メールを利用して認証局に連絡し、その CA 証明書をダウンロードします。
2. 受け取った証明書のテキストをテキスト形式でファイルに保存します。
3. 前項で説明したように、証明書セットアップウィザードを使って証明書をインストールします。

詳細については、『Netscape Console によるサーバの管理』の SSL に関する章を参照してください。

証明書と認証済み CA を管理する

サーバには、信頼できる認証局の証明書を必要な数だけインストールすることができます。これらの証明書は、クライアント認証を行うために使用されることになります

コンソールでサーバを選択してから [コンソール] メニューの [証明書の管理] コマンドを選択すると、Messaging Server にインストールされている証明書の信頼設定を表示または編集したり、任意の証明書を削除することができます。詳細については、『Netscape Console によるサーバの管理』の SSL に関する章を参照してください。

パスワードファイルを作成する

どの iPlanet サーバの場合でも、証明書セットアップウィザードを使って証明書を要求すると、キーペアが作成されます (このキーペアは、後で内部モジュールのデータベースまたはスマートカード内にある外部データベースのいずれかに保存されることになります)。その後、このプライベートキーを暗号化するために使われるパスワードを入力するよう求められます。後でキーを復号化するときには、同じパスワードを使用しなければなりません。パスワードはどこにも記録されないので忘れないようにしてください。

一般に、SSL を使用している iPlanet サーバの場合は、起動時に管理者がキーペアの復号化用パスワードを入力するようになっています。ただし、Messaging Server の場合は、何度もパスワードを入力しなくても済むように (少なくとも 3 つのサーバプロセスで必要とされます)、また、重要度の低いサーバの再起動を簡素化するために、パスワードはパスワードファイルから読み取られます。

パスワードファイルの名前は `sslpassword.conf` で、このファイルは *サーバ- インスタンス* `/config/` ディレクトリに保存されています。ファイル内の各エントリは、次のフォーマットで 1 行ずつ記述されています。

`moduleName:password`

ここで、*moduleName* は使用される (内部または外部) PKCS #11 モジュールの名前で、*password* はそのモジュールのキーペアを暗号化するためのパスワードです。パスワードは、平文 (暗号化されない) で保存されます。

Messaging Server には、デフォルトのパスワードファイルがあります。このファイルには、以下に示すエントリが 1 つだけ含まれています (内部モジュールおよびデフォルトのパスワード用)。

```
Internal (Software) Token:netscape!
```

内部証明書をインストールするときにデフォルト以外のパスワードを指定した場合は、パスワードファイル内の行 (上記参照) を編集して、指定したパスワードを反映させる必要があります。外部モジュールをインストールした場合は、ファイルに新しい行を追加し、そこにモジュール名とそのパスワードを記述する必要があります。

注意　管理者はサーバの起動時にモジュールのパスワードを入力するように求められません。そのため、管理者によるアクセスが適切に制御されていること、およびサーバホスト マシンおよびそのバックアップの物理的なセキュリティが確保されていることが重要なポイントとなります。

SSL を有効にする符号化方式を選択する

SSL を有効にし、Messaging Server がクライアントとの暗号化通信に使用する符号化方式を選択するには、コンソールを使用します。

符号化方式の概要

「符号化方式」とは、暗号化プロセスでデータを暗号化および復号化するためのアルゴリズムのことです。符号化方式の中には、強度の高低があります。つまり、承認されていない人が符号を解読しようとした場合、強度が高いほど解読が困難であることを意味します。

符号化方式は、キー (長い数値) をデータに適用することによって動作します。一般に、暗号化に使用するキーが長いほど、適切な復号キーなしで、データを復号することは難しくなります。

クライアントが Messaging Server と SSL 接続を開始するとき、クライアントはサーバに対して、暗号化に使用したい符号化方式とキー長を伝えます。暗号化通信では、両者が同じ符号化方式を使用していなければなりません。一般に使用される符号化方式とキーの組み合わせには数多くのタイプがあります。そのため、サーバは暗号化のサポートに対して柔軟でなければなりません。iPlanet Messaging Server では、符号化方式とキー長の組み合わせとして 6 つまでのタイプをサポートしています。

表 11.1 に、Messaging Server が SSL 3.0 を使ってサポートできる符号化方式の一覧を示します。この表は、各タイプについて簡単に説明したものです。詳細については、『Netscape Console によるサーバの管理』の「Introduction to SSL」を参照してください。

表 11-1　Messaging Server の SSL 符号化方式

符号化方式	説明
RC4 (128 ビットの暗号化)、MD5 メッセージ認証	最も高速の符号化方式 (RSA)。この符号化方式と暗号化キーの組み合わせは、高レベルの強度を提供します。
Triple DES (168 ビットの暗号化)、SHA メッセージ認証	やや低速の符号化方式 (米国政府標準)。この符号化方式と暗号化キーの組み合わせは、最高レベルの強度を提供します。
DES (56 ビットの暗号化)、SHA メッセージ認証	やや低速の符号化方式 (米国政府標準)。この符号化方式と暗号化キーの組み合わせは、中間レベルの強度を提供します。
RC4 (40 ビットの暗号化)、MD5 メッセージ認証	最高速の符号化方式 (RSA)。この符号化方式と暗号化キーの組み合わせは、低レベルの強度を提供します。
RC2 (40 ビットの暗号化)、MD5 メッセージ認証	やや低速の符号化方式 (RSA)。この符号化方式と暗号化キーの組み合わせは、低レベルの強度を提供します。
暗号化なし、MD5 メッセージ認証のみ	暗号化なし。認証用のメッセージダイジェストのみ。

特定の符号化方式を使わないようにする特別な理由がない限り、上記すべての符号化方式をサポートするようにしてください。ただし、特定の暗号化方式の使用が制限されている国もあるので注意が必要です。また、米国輸出規制が緩和される前に開発されたクライアントソフトウェアの中には、強度の高い暗号化を使用できないものもあります。40 ビットの符号化方式を使った場合、軽い攻撃を防ぐことはできるかもしれませんが、あまり安全だとは言えません。意図的な攻撃は防ぐことができません。

コンソール - コンソールを使って SSL を有効にし、符号化方式を選択するには、以下の手順で操作します。

1 コンソールで、符号化方式の設定を変更する Messaging Server を開きます。

2 左側のパネルの [環境設定] タブをクリックし、[サービス] フォルダを開きます。

3 右ペインの [暗号化] タブをクリックします。

4 [SSL の利用] チェックボックスをオンにして、サーバの SSL を有効にします。

5 RSA による符号化方式を使用可能にする場合は、[RSA] チェックボックスをオンにします。

6 [トークン] ドロップダウンリストで、使用するトークンを選択します。

7 [証明書] ドロップダウンリストで、使用する証明書を選択します。

8 [符号化方式のプリファレンス] をクリックして、使用可能な符号化方式のリストを開きます。

9 ボックスをクリックしてサポートする符号化方式 (複数可) を選択します。

SSL を無効にするには、[SSL の利用] チェックボックスをオフにします。

注 送信メッセージに対して SSL 暗号化を有効にするには、チャネル定義に `maytls` や `musttls` などの `tls` チャネルキーワードを含める必要があります。詳細については、『Messaging Server リファレンスマニュアル』を参照してください。

コマンドライン - コマンドラインを使って SSL を有効にし、符号化方式を選択することもできます。

SSL を有効 / 無効にするには :

```
configutil -o nsserversecurity -v [ on | off ]
```

RSA 符号化方式を有効 / 無効にするには :

```
configutil -o encryption.rsa.nssslactivation -v [ on | off ]
```

トークンを指定するには :

```
configutil -o encryption.rsa.nsssltoken -v トークン名
```

証明書を指定するには :

```
configutil -o encryption.rsa.nssslpersonalityssl -v 証明書名
```

RSA 符号化方式を有効にした場合は、トークンと証明書を指定する必要があります。

符号化方式のプリファレンスを選択するには :

```
configutil -o encryption.nsssl3ciphers -v cipherlist
```

ここで、*cipherlist* はコンマで区切られた符号化方式リストを指します。

証明書に基づくログインを設定する

パスワードに基づくログインに加え、iPlanet サーバでは、デジタル証明書の確認によるユーザ認証をサポートしています。証明書に基づく認証の場合、クライアントはサーバとの SSL セッションを確立し、ユーザの証明書をサーバに提出します。その後、サーバによって、提出された証明書が信頼できるものであるかどうかを評価します。証明書の信頼性が確認されると、そのユーザは本人であると見なされます。

証明書に基づくログインを行えるように Messaging Server を設定するには、以下の手順に従います。

1 お使いのサーバに対するサーバ証明書を入手します（詳細については、261 ページの「証明書を入手する」を参照してください）。

2 証明書セットアップウィザードを実行して、信頼できる認証局の証明書をインストールします。これにより、サーバは、これらの認証局から証明書を発行されたユーザを認証できるようになります（詳細については、263 ページの「認証済み認証局の証明書をインストールする」を参照してください）。

   サーバのデータベース内に信頼できる認証局が少なくとも 1 つある場合、そのサーバは接続した各クライアントに対してクライアント証明書を要求するようになります。

3 SSL を有効にします（詳細については、264 ページの「SSL を有効にする符号化方式を選択する」を参照してください）。

4 （オプション）サーバが提出された証明書の情報に基づいて LDAP ユーザディレクトリを適切に検索するように、サーバの `certmap.conf` ファイルを編集します。

   ユーザの証明書の電子メールアドレスがユーザのディレクトリエントリ内にある電子メールアドレスに一致する場合、`certmap.conf` ファイルを編集する必要はありません。また、検索を最適化したり、提出された証明書をユーザエントリ内の証明書と照合する必要もありません。

   `certmap.conf` のフォーマットおよび可能な変更については、『Netscape Console によるサーバの管理』の SSL に関する章を参照してください。

上記の手順を実行した後に、ユーザが IMAP または HTTP にログインできるようにクライアントが SSL セッションを確立すると、Messaging Server はクライアントに対してユーザの証明書を要求します。クライアントによって提出された証明書がサーバで既に認証されている認証局から発行されたものである場合、およびその証明書におけるアイデンティティがユーザディレクトリ内のエントリに一致する場合は、そのユーザが認証され、アクセスが許可されます（そのユーザを規制しているアクセス制御規則によります）。

証明書に基づくログインを有効にするためにパスワードに基づくログインを無効する必要はありません。パスワードに基づくログインが許可されている場合（デフォルトの状態）に、この節で説明しているタスクを実行すると、パスワードに基づくログインと証明書に基づくログインの両方がサポートされます。その場合、クライアントが SSL セッションを確立し、証明書を提示すると、証明書に基づくログインが使用されます。クライアントが SSL を使用しない場合、または証明書を提示しなかった場合は、パスワードが要求されます。

証明書に基づく認証を利用できるように iPlanet サーバおよびクライアントを設定する方法については、『Single Sign-On Deployment Guide』を参照してください。

Messaging Server への管理者アクセスを設定する

この節では、サーバ管理者による Messaging Server へのアクセスを制御する方法について説明します。特定の Messaging Server および Messaging Server タスクへの管理上のアクセスは、委託サーバ管理に関連して起こります。

「委託サーバ管理」とは、ある管理者が他の管理者に対し個々のサーバおよびサーバ機能へのアクセスを提供することができる機能を意味する用語で、この機能はほとんどの iPlanet サーバに備わっています。この章では、委託サーバ管理のタスクについて簡単に説明します。詳細については、『Netscape Console によるサーバの管理』の委託サーバ管理に関する章、および『Messaging Server Provisioning Guide』の「Provisioning Messaging Server Administrators」を参照してください。『Provisioning Guide』では、サーバ管理者 (Messaging Server を設定できる管理者)、および iDA 管理者 (システム内のユーザおよびグループを追加、変更、削除できる管理者) について説明しています。

委託管理の階層

ネットワーク上に最初の iPlanet サーバをインストールすると、LDAP ユーザディレクトリに「設定管理者グループ」と呼ばれるグループが、インストールプログラムによって自動的に作成されます。特に設定を変更しない限り、設定管理者グループのメンバーには、ネットワーク上のすべてのホストおよびサーバに対する無制限のアクセスが与えられます。

設定管理者グループは、以下に説明するようなアクセス階層の最上位に位置します。このアクセス階層は、Messaging Server の委託管理を実行するうえで利用されます。

1. **設定管理者 :** iPlanet サーバのネットワークにおける「スーパーユーザ」。すべてのリソースに対する完全なアクセス権があります。
2. **サーバ管理者 :** ドメイン管理者は、各タイプのサーバを管理するためのグループを作成することがあります。たとえば、管理ドメイン内またはネットワーク全体にあるすべての Messaging Server を管理するために「メッセージング管理者」グループを作成したりします。このグループのメンバーには、その管理ドメイン内のすべての Messaging Server に対するアクセス権があります (他のサーバに対するアクセス権はありません)。
3. **タスク管理者 :** 上記の管理者はいずれも、単一または複数の Messaging Server に対する制限付きアクセス権を持つグループを作成したり、またはそのようなアクセス権を持つ個人ユーザを指定することができます。このようなタスク管理者は、特定の制限されたサーバタスク (サーバの起動や停止、特定のサービスのログへのアクセス) だけを実行することが許可されます。

コンソールの便利なインターフェースを使用して、管理者が以下のタスクを実行できるように設定できます。

- グループまたは個人に特定の Messaging Server に対するアクセス権を与えます。次項の「サーバ全体に対するアクセスを与える」を参照してください。
- そのアクセスを特定の Messaging Server における特定のタスクに制限します。269 ページの「アクセスを特定のタスクに制限する」を参照してください。

サーバ全体に対するアクセスを与える

ユーザまたはグループに特定の Messaging Server に対するアクセス権を与えるには、以下の手順に従います。

1 対象となる Messaging Server へのアクセス権を持つ管理者としてコンソールにログインします。

2 [コンソール] ウィンドウで、そのサーバを選択します。

[コンソール] メニューから [オブジェクト]—[アクセス権の設定] を選択します。

3 そのサーバへのアクセス権を持つユーザおよびグループのリストを編集します。

詳細については、『Netscape Console によるサーバの管理』の委託サーバ管理に関する章を参照してください。

特定の Messaging Server へのアクセス権を持つユーザおよびグループのリストを設定したら、以下で説明する ACI を使って、そのリスト内の特定の人物またはグループに特定のサーバタスクを委託することができます。

アクセスを特定のタスクに制限する

一般に、管理者はサーバに接続して 1 つ以上の管理タスクを実行します。コンソールの Messaging Server タスクフォームには、通常行われる管理タスクがリストされています。

デフォルト設定を使用する場合、「特定の Messaging Server へのアクセス」とは、そのサーバのすべてのタスクにアクセスできることを意味します。ただし、タスクフォーム内の各タスクには、一連のアクセス制御インストラクション (ACI) をつけることができます。サーバは、接続しているユーザ (サーバ全体に対するアクセス権を既に持っているユーザ) にタスクへのアクセス権を与える前に、これらの ACI を調べます。実際、タスクフォームには、そのユーザがアクセス権を持っているタスクのみが表示されます。

Messaging Server へのアクセス権がある場合は、アクセス権を持っている任意のタスクに関する ACI を作成または編集することで、そのタスクに対して他のユーザやグループが持っているアクセス権を制限することができます。

接続しているユーザまたはグループに対し、タスクへのアクセス権を制限するには :

1 対象となる Messaging Server へのアクセス権を持っている管理者として コンソールにログインします。

2 サーバを開き、そのサーバのタスクフォームからタスクを選択します。タスクを選択するには、「タスク」テキストをクリックします。

3 [編集] メニューの [アクセス権の設定] を選択し、ユーザまたはグループにアクセスを与えるためのアクセス規則のリストを編集します。

4 必要に応じて、他のタスクに同じ手順を繰り返します。

詳細については、『Netscape Console によるサーバの管理』の委託サーバ管理に関する章を参照してください。

ACI およびその作成方法については、『Netscape Console によるサーバの管理』の委託サーバ管理に関する章で詳しく説明しています。

POP、IMAP、および HTTP サービスへの クライアントアクセスを設定する

Messaging Server には、IMAP、POP、および HTTP の各サービスに対して高性能なアクセス制御機能があります。これにより、クライアントによるサーバへのアクセスを広範囲に細かく制御することができます。

大企業またはインターネット サービスプロバイダ用にメッセージングサービスを管理する場合は、これらの機能が、システムからスパム (大量メール送信) や DNS スプーフを除外したり、ネットワークの一般的なセキュリティを強化するのに役立ちます。一方的に送られてくる大量の不要電子メールを制御する方法については、第 9 章 「メールのフィルタリングとアクセス制御」を参照してください。

注　システムにとって、IP アドレスによるアクセス制御がそれほど**重要でない**場合は、この項で説明しているフィルタを作成する必要はありません。最小限のアクセス制御だけを設定する方法については、276 ページの「大部分のアクセスを許可」を参照してください。

クライアントアクセスフィルタのしくみ

Messaging Server のアクセス制御機能は、TCP デーモンと同じポートで応答をリッスンするプログラムです。つまり、アクセスフィルタを使用してクライアントのアイデンティティを確認し、クライアントがフィルタリングプロセスを通過した場合には、そのデーモンへのアクセスがクライアントに与えられます。

そのプロセスの一部として、Messaging Server の TCP クライアントアクセス制御システムは、必要に応じて、以下のようなソケットのエンドポイントアドレスの解析を行います。

- 両エンドポイントのリバース DNS 検索 (名前に基づくアクセス制御を行うため)
- 両エンドポイントのフォワード DNS 検索 (DNS スプーフィングを検出するため)
- `Identd` コールバック (クライアントエンドのユーザがクライアントホストに対して認識されているかどうかを調べるため)

システムは、この情報を「フィルタ」と呼ばれるアクセス制御文と比較することにより、アクセスの許可または拒否を決定します。各サービスには、アクセスを制御するために、それぞれ別の ALLOW フィルタ / DENY フィルタのセットがあります。ALLOW フィルタは明示的にアクセスを与えるもので、DENY フィルタは明示的にアクセスを禁止します。

クライアントがサービスへのアクセスを要求すると、アクセス制御システムは、そのクライアントのアドレスまたは名前情報をそのサービスのフィルタと比較します。その際、以下の条件を使って、順番に比較作業が行われます。

- 検索は、最初の一致項目が見つかった時点で終了します。ALLOW フィルタは DENY フィルタより先に処理されるため、ALLOW フィルタが優先されることになります。
- クライアント情報がそのサービスの ALLOW フィルタに一致した場合は、アクセスが許可されます。
- クライアント情報がそのサービスの DENY フィルタに一致した場合は、アクセスが拒否されます。
- ALLOW フィルタと DENY フィルタのどちらにも一致しなかった場合は、アクセスが許可されます。ただし、DENY フィルタがなく、ALLOW フィルタだけしかない場合は、その ALLOW フィルタに一致しない限り、アクセスは許可されません。

フィルタの構文にはとても柔軟性があり、簡単でわかりやすい方法を用いて、さまざまなアクセス制御ポリシーを実装することができます。ALLOW フィルタと DENY フィルタは自由に組み合わせて使うことができます。ただし、ほとんどのアクセスを許可するようなフィルタ、またはほとんどのアクセスを拒否するようなフィルタを使用してポリシーを自由に作成することが多いと思われます。

以下の節では、フィルタの構文について詳しく説明するほか、いくつかの使用例も紹介します。アクセスフィルタの作成手順については、278 ページの「各サービスのアクセスフィルタを作成する」を参照してください。

フィルタの構文

フィルタ文は、サービス情報とクライアント情報から構成されます。サービス情報には、サービスの名前、ホストの名前、ホストアドレスなど含めることができます。一方、クライアント情報には、ホスト名、ホストアドレス、ユーザ名などを含めることができます。サービス情報およびクライアント情報では、共にワイルドカード名やパターンを使用できます。

以下に、フィルタの最も簡単な形式を示します。

```
service: hostSpec
```

ここで、*service* はサービスの名前 (`smtp`、`pop`、`imap`、または `http` など)、*hostSpec* はアクセスを要求しているクライアントを表すホスト名、IP アドレス、またはワイルドカード名 / パターンです。フィルタが処理されるときに、アクセスを要求しているクライアントは *hostSpec* に一致すると、*service* で指定されているサービスへのアクセスが (フィルタのタイプに応じて) 許可または拒否されます。以下の例を見てください。

```
imap: roberts.newyork.siroe.com

pop: ALL

http: ALL
```

これらが ALLOW フィルタとして使われる場合は、最初の文によって roberts.newyork.siroe.com というホストに IMAP サービスへのアクセスが許可されます。また、次の 2 つの文によって、すべてのクライアントにそれぞれ POP サービスおよび HTTP サービスへのアクセスが許可されます。これらが DENY フィルタとして使われる場合は、同様のクライアントに対し、上記サービスへのアクセスが拒否されることになります。ALL などのワイルドカード名の詳細については、273 ページの「ワイルドカード名」を参照してください。

フィルタのサービス情報およびクライアント情報は、場合によってさらに複雑になることがあります。以下に、より一般的な形式を示します。

serviceSpec: *clientSpec*

ここで、*serviceSpec* は *service* または *service@hostSpec* のどちらかとなり、*clientSpec* は*ホスト仕様*または *user@ hostSpec* のどちらかとなります。この「 *user*」はアクセスを要求しているクライアントに関連付けられたユーザ名 (またはワイルドカード名) です。以下に、2 つの例を挙げます。

```
pop@mailServer1.siroe.com: ALL
```

```
imap: srashad@xyz.europe.siroe.com
```

これらを DENY フィルタとして考えてみましょう。最初のフィルタでは、すべてのクライアントに対し、mailServer1.siroe.com というホスト上の SMTP サービスへのアクセスが拒否されます。また、2 番目のフィルタでは、xyz.europe.siroe.com というホストの srashad というユーザに対し、IMAP サービスへのアクセスが拒否されます。サーバおよびクライアントの拡張設定の使い方については、275 ページの「サーバホスト仕様」および 275 ページの「クライアントのユーザ名仕様」を参照してください。

フィルタを最も一般的な形式で表すと、以下のようになります。

serviceList: *clientList*

ここで、*serviceList* は 1 つ以上の *serviceSpec* エントリから成り、*clientList* は 1 つ以上の *clientSpec* エントリから成ります。また、*serviceList* および *clientList* の各エントリは、空白やカンマで区切ります。

この場合、フィルタが処理されているときに、アクセスを要求しているクライアントが *clientList* 内の任意の *clientSpec* エントリに一致すると、*serviceList* で指定されているすべてのサービスに対するアクセスが (フィルタのタイプの応じて) 許可または拒否されます。以下に、その例を挙げます。

```
pop, imap, http: .europe.siroe.com .newyork.siroe.com
```

これが ALLOW フィルタであるとすると、europe.siroe.com ドメインまたは newyork.siroe.com ドメイン内のすべてのクライアントに POP、IMAP、および HTTP サービスへのアクセスが許可されます。ドメインやサブネットを指定するための先行ドットや他のパターンの使い方については、274 ページの「ワイルドカードパターン」を参照してください。

ワイルドカード名

以下のワイルドカード名を使って、サービス名、ホストの名前やアドレス、またはユーザ名を表すことができます。

表 11-2　　ワイルドカード名

ワイルドカード名	説明
ALL	ユニバーサルなワイルドカード。すべての名前に一致します。
LOCAL	すべてのローカルホストに一致します (ドット文字のない名前を持つホスト)。ただし、正規の名前のみを使っているシステムの場合は、ローカルホストにもドットが含まれるため、このワイルドカードには一致しません。
UNKNOWN	名前が不明なすべてのユーザ、または名前やアドレスが不明なすべてのホストに一致します。 このワイルドカードは、注意して使用してください。 一時的な DNS サーバ問題が発生した場合など、ホスト名が使用できなくなることがあります。このような場合、UNKNOWN を使用しているすべてのフィルタはすべてのクライアントホストに一致してしまいます。 ソフトウェアが通信先のネットワークタイプを識別できない場合は、ネットワークアドレスを使用できません。そのような場合、UNKNOWN を使用しているフィルタは、そのネットワーク上にあるすべてのクライアントホストに一致してしまいます。
KNOWN	名前が認識されているすべてのユーザ、または名前**および**アドレスが認識されているすべてのホストに一致します。 このワイルドカードは、注意して使用してください。 一時的な DNS サーバ問題が発生した場合など、ホスト名が使用できなくなることがあります。このような場合、KNOWN を使用しているフィルタはどのクライアントホストにも一致しません。 ソフトウェアが通信先のネットワークタイプを識別できない場合は、ネットワークアドレスを使用できません。そのような場合、KNOWN を使用しているフィルタは、そのネットワーク上のどのクライアントホストにも一致しません。
DNSSPOOFER	DNS 名がその IP アドレスに一致しないホストに一致します。

ワイルドカードパターン

サービスまたはクライアントアドレスには、以下のパターンを使用できます。

- ドット文字 (.) から始まる文字列。ホスト名の末尾部分が指定したパターンに一致する場合、そのホスト名は一致します。たとえば、.siroe.com というワイルドカードパターンは、siroe.com というドメイン内のすべてのホストに一致します。
- ドット文字 (.) で終わる文字列。ホストアドレスの先頭の数値フィールドが指定したパターンに一致する場合、そのホストアドレスは一致します。たとえば、123.45. というワイルドカード パターンは、123.45.0.0 サブネット内にある任意のホストのアドレスに一致します。
- n.n.n.n/m.m.m.m 形式の文字列。このワイルドカードパターンは「*ネット / マスク*」のペアと解釈されます。*ネット*がアドレスと *マスク*のビット AND に等しい場合、そのホストアドレスは一致します。たとえば、123.45.67.0/255.255.255.128 というパターンは 123.45.67.0 ～ 123.45.67.127 の範囲に含まれるすべてのアドレスに一致します。

EXCEPT 演算子

アクセス制御システムでは、1 つの演算子がサポートされています。EXCEPT 演算子を使うと、*serviceList* または *clientList* のいずれかに複数のエントリがある場合に、名前やパターンの一致に関する例外を指定することができます。以下に、その形式を示します。

list1 EXCEPT *list2*

この文では、*list1* に当てはまるものがすべて一致します。ただし、そのうち *list2* に当てはまるものは**除外**されます。

以下に、その例を挙げます。

```
ALL: ALL EXCEPT isserver.siroe.com
```

これを DENY フィルタとして使うと、isserver.siroe.com というホストマシン上のクライアントを除くすべてのクライアントに対し、すべてのサービスへのアクセスが拒否されます。

EXCEPT 句はネスティングすることも可能です。次の形式を見てください。

list1 EXCEPT *list2* EXCEPT *list3*

これは、以下の形式と同じように解釈されます。

list1 EXCEPT (*list2* EXCEPT *list3*)

サーバホスト仕様

serviceSpec エントリにサーバホストの名前またはアドレス情報を含めることにより、要求されている特定のサービスをさらに識別することができます。この場合、エントリは以下の形式で表します。

service@hostSpec

この機能は、Messaging Server ホストマシンが異なるインターネットホスト名を持つ複数のインターネットアドレス用に設定されている場合に便利です。サービスプロバイダは、この機能を使うことによって、異なるアクセス制御規則を持つ複数のドメインを 1 個のサーバインスタンスでホストすることができます。

クライアントのユーザ名仕様

RFC 1413 で定義されている identd サービスをサポートするクライアントホストマシンの場合は、フィルタの *clientSpec* エントリ内にクライアントのユーザ名を含めることにより、サービスを要求している特定のクライアントを識別することができます。この場合、エントリは次の形式で表します。

user@hostSpec

ここで、「*user*」_ はクライアントの identd サービス (またはワイルドカード名) によって返されるユーザ名です。

フィルタにクライアントユーザ名を指定すると、場合によっては効果がありますが、以下の事項に注意してください。

- identd サービスは認証ではありません。したがって、クライアントシステムが安全なものでない場合、そこから返されるクライアントユーザ名を信頼することはできません。一般には、特定のユーザ名を使用せずに、ALL、KNOWN、または UNKNOWN などのワイルドカードだけを使用するようにします。
- ユーザ名検索には時間がかかります。すべてのユーザについて検索を実行すると、identd をサポートしていないクライアントによるアクセスが遅くなることがあります。この問題は、ユーザ名検索を選択的に行うことにより解消できます。たとえば、次の例を見てください。

  serviceList: @xyzcorp.com ALL@ALL

  このフィルタを使うと、ユーザ検索を実行することなく、xyzcorp.com ドメイン内のユーザが一致します。そして、その他のすべてのシステムについては、ユーザ名検索が実行されます。

ユーザ名検索の機能は、クライアントホストにおける非承認ユーザからの攻撃を防ぐのに役立つ場合があります。たとえば、TCP/IP 実装では、不正侵入者が rsh (リモートシェルサービス) を使って信頼されているクライアントユーザを装うことができます。クライアントホストが ident サービスをサポートしている場合は、ユーザ名検索を使ってそのような攻撃を検出することができます。その例と説明については、277 ページの「指定ユーザだけにアクセスを許可する」を参照してください。

フィルタの例

この節では、さまざまなアクセス制御のアプローチ例を紹介します。これらの例を参照するにあたり、ALLOW フィルタが DENY フィルタより先に処理されること、一致する項目が見つかった時点で検索が終了すること、および一致する項目が見つからなかった場合にはアクセスが許可されることに留意してください。

これらの例では、IP アドレスではなく、ホスト名とドメイン名を使用しています。フィルタにアドレス情報やネットマスク情報を含めておくと、ネームサービスにエラーが発生した場合の信頼性を高めることができます。

大部分のアクセスを拒否する

この例では、デフォルトでアクセスが拒否されます。そのため、明示的に認可されたホストだけがアクセスを許可されます。

デフォルトのポリシー (アクセスなし) は、次に示す 1 つの単純な DENY フィルタを使って実装されます。

```
ALL: ALL
```

このフィルタは、ALLOW フィルタによって明示的にアクセスを許可されていないすべてのクライアントに対し、すべてのサービスを拒否するものです。この場合の ALLOW フィルタは、たとえば次のようなものです。

```
ALL: LOCAL @netgroup1

ALL: .siroe.com EXCEPT externalserver.siroe.com
```

最初の規則では、ローカルドメイン内のすべてのホスト (すなわち、ホスト名にドットがないすべてのホスト) からのアクセス、および netgroup1 というグループのメンバーからのアクセスを許可しています。2 番目の規則では、externalserver.siroe.com ホストを除く siroe.com ドメイン内のすべてのホストからのアクセスを許可するために、先行ドットのワイルドカードパターンを使用しています。

大部分のアクセスを許可

この例では、デフォルトでアクセスが許可されます。そのため、明示的に指定されたホストだけがアクセスを拒否されます。

デフォルトのポリシー (アクセス許可) により、ALLOW フィルタは特に必要ありません。つまり、DENY フィルタ内にアクセスを拒否するクライアントを明示的に指定すればよいのです。以下に、その例を示します。

```
ALL: externalserver.siroe1.com, .siroe.asia.com

ALL EXCEPT pop: contractor.siroe1.com, .siroe.com
```

最初のフィルタでは、特定のホストおよびドメインに対するすべてのサービスを拒否しています。2 番目のフィルタでは、特定のホストおよびドメインからのアクセスを POP だけに限定しています。

指定ユーザだけにアクセスを許可する

以下に示す DENY フィルタを使うと、クライアントホストの identd サービスで既に認識されているユーザをすべて除外することができます。

```
ALL: UNKWOWN@ALL
```

つまり、このフィルタを使うと、すべてのドメインにおける不明なユーザ全員に対し、すべてのサービスが拒否されます。

「UNKNOWN@*host*」の「*clientSpec*」エントリを使うと、さらに特定化した DENY フィルタを作成できます。アクセス制御システムは、「*host*」からの要求を受け取ると、「*host*」上の ident サービスを使ってそのホストが実際に要求を送ったかどうか、およびその要求を送ったユーザの名前を調べます。要求を送ったユーザが不明な場合、そのユーザは不正侵入者である可能性があります (ただし、クライアントのホストが identd サービスをサポートしていない場合は、すべての要求者が UNKNOWN@*host* フィルタに一致してしまうので注意してください)。

ALLOW フィルタで使用するユーザ名検索は、あまり当てになりません。たとえば、「KNOWN@*host*」の「*clientSpec*」エントリを使って ALLOW フィルタを作成したとします。しかし、不正侵入者はクライアント接続と ident 検索の両方をスプーフィングできるため、「KNOWN@*host*」フィルタの一致がスプーフィングのないことの確実な証拠にはなりません。さらに、クライアントシステムが信頼できるものでない場合には、ident によって偽の情報が返されることもあります。

詳細については、275 ページの「クライアントのユーザ名仕様」を参照してください。

スプーフィングされたドメインへのアクセスを拒否する

フィルタに DNSSPOOFER ワイルドカード名を使用することにより、ホスト名スプーフィングを検出することができます。DNSSPOOFER を指定すると、アクセス制御システムによって正方向または逆方向の DNS 検索が実行され、クライアントにより提示されたホスト名がその実際の IP アドレスと一致するかどうかが調べられます。以下に、DENY フィルタの例を示します。

```
ALL: DNSSPOOFER
```

このフィルタでは、IP アドレスがその DNS ホスト名に一致しないすべてのリモート ホストに対し、すべてのサービスを拒否しています。

仮想ドメインへのアクセスを制御する

メッセージングシステムで仮想ドメインを使用しており、1 つのサーバインスタンスが複数の IP アドレスおよびドメイン名に関連付けられている場合は、ALLOW フィルタと DENY フィルタを組み合わせて使って各仮想ドメインへのアクセスを制御することができます。たとえば、以下に示すような ALLOW フィルタを使用できます。

```
ALL@msgServer.siroe1.com: @.siroe1.com

ALL@msgServer.siroe2.com: @.siroe2.com

...
```

この場合、たとえば次のような DENY フィルタを使用できます。

```
ALL: ALL
```

各 ALLOW フィルタでは、domain*N* 内のホストだけが msgServer.siroe*N*.com に対応する IP アドレスを持つサービスに接続できるように指定されています。他の接続はすべて拒否されます。

特定のユーザを拒否する

1 人のユーザに対し、特別にアクセスを拒否する場合は、以下のような DENY フィルタを使用します。

```
ALL: 対象ユーザ@ALL
```

もちろん、このフィルタを使った場合でも、そのユーザが別のユーザ名を使ってアクセスすることを防ぐことはできません。

各サービスのアクセスフィルタを作成する

IMAP、POP、HTTP の各サービスに対して、ALLOW フィルタおよび DENY フィルタを作成することができます。

コンソール - コンソールを使ってフィルタを作成するには、以下の手順に従います。

1. コンソールで、アクセスフィルタを作成する対象となる Messaging Server を開きます。
2. [環境設定] タブをクリックします。
3. 左側のパネルで [サービス] フォルダを開き、そのフォルダの下にある IMAP、POP、または HTTP を選択します。
4. 右ペインの [アクセス] タブをクリックします。

   [許可] フィールドおよび [拒否] フィールドにそれぞれ、そのサービスの既存の ALLOW フィルタおよび DENY フィルタが表示されます。フィールドの各行がそれぞれ 1 つのフィルタに相当します。どちらか一方のフィールドに対し、以下の操作を実行できます。

   - [追加] をクリックして新規のフィルタを作成できます。[ALLOW フィルタ] ウィンドウまたは DENY フィルタウィンドウが開くので、そこに新しいフィルタのテキストを入力し、[OK] をクリックします。
   - フィルタを選択して [編集] をクリックすると、そのフィルタを編集できます。[ALLOW フィルタ] ウィンドウまたは DENY フィルタウィンドウが開くので、そこに表示されたフィルタのテキストを編集し、[OK] をクリックします。
   - フィルタを選択して [削除] をクリックすると、そのフィルタを削除できます。

ALLOW フィルタまたは DENY フィルタの順序を変更する必要がある場合は、フィルタが目的の順序に並ぶまで [削除] 操作と [追加] 操作を繰り返します。

フィルタの構文とその例については、271 ページの「フィルタの構文」を参照してください。また、その他の例については、276 ページの「フィルタの例」を参照してください。

コマンドライン - コマンドラインを使って ALLOW フィルタや DENY フィルタを指定することもできます。以下に、その例を示します。

各サービスに対して ALLOW フィルタを作成または編集するには :

```
configutil -o service.service.domainallowed -v filter
```

ここで、*service* は pop、imap、または http のいずれかであり、*filter* は 271 ページの「フィルタの構文」で説明している構文の規則に従います。

各サービスに対して DENY フィルタを作成または編集するには :

```
configutil -o service.service.domainnotallowed -v filter
```

ここで、*service* は pop、imap、または http のいずれかであり、*filter* は 271 ページの「フィルタの構文」で説明している構文の規則に従います。

HTTP プロキシ認証のアクセスフィルタを作成する

ストア管理者は誰でも、任意のサービスに対してプロキシ認証を行うことができます (ストア管理者の詳細については、218 ページの「ストアへの管理者アクセスを指定する」を参照してください)。HTTP サービスに限っては、任意のエンドユーザがサービスに対してプロキシ認証を行うことができます。ただし、そのエンドユーザのクライアントホストに、プロキシ認証アクセスフィルタを通じたアクセスが許可されていなければなりません。

プロキシ認証では、ポータルサイトなどの他のサービスがユーザを認証したり、HTTP ログインサービスに認証資格を渡すことができます。たとえば、1 つのポータルサイトにいくつかのサービスがあり、そのうちの 1 つが Messenger Express の Web ベース電子メールだとします。HTTP プロキシ認証機能を使うと、エンドユーザはポータルサービスに対して一度だけ認証を行うことになります。すなわち、電子メールにアクセスするのに再び認証を行う必要はありません。ただし、ポータルサイトは、ログインサーバをクライアントとサービス間のインターフェースとして機能するように設定しておく必要があります。Messenger Express の認証用にログインサーバを設定する際には、iPlanet 製の Messenger Express 認証 SDK を利用できます。

この節では、ALLOW フィルタを使って IP アドレスによる HTTP プロキシ認証を許可する方法について説明します。ログインサーバの設定方法や Messenger Express 認証 SDK の使い方については、iPlanet までご連絡ください。

コンソール - HTTP サービスに対するプロキシ認証用の ALLOW フィルタを作成するには :

1 コンソールで、ALLOW フィルタを作成する対象となる Messaging Server を開きます。

2 [環境設定] タブをクリックします。

3 左側のパネルで [サービス] フォルダを開き、そのフォルダの下にある HTTP を選択します。

4 右ペインの [プロキシ] タブをクリックします。

[許可] フィールドには、プロキシ認証用の既存 ALLOW フィルタが表示されています。

5 新規のフィルタを作成する場合は、[追加] をクリックします。

[ALLOW フィルタ] ウィンドウが開きます。ウィンドウに新しいフィルタのテキストを入力し、[OK] をクリックします。

6 既存のフィルタを編集する場合は、[編集] をクリックします。

[ALLOW フィルタ] ウィンドウが開きます。ウィンドウに表示されているフィルタのテキストを編集し、[OK] をクリックします。

7 既存のフィルタを削除する場合は、[許可] フィールドでフィルタを選択し、[削除] をクリックします。

8 [プロキシ] タブでの変更作業が終わったら、[保存] をクリックします。

ALLOW フィルタの構文については、271 ページの「フィルタの構文」を参照してください。

コマンドライン - コマンドラインを使って、HTTP サービスに対するプロキシ認証用の ALLOW フィルタを指定することもできます。以下に、その例を示します。

```
configutil -o service.service.proxydomainallowed -v filter
```

ここで、*filter* は 271 ページの「フィルタの構文」で説明している構文の規則に従います。

SMTP サービスへのクライアントアクセスを設定する

SMTP サービスへのクライアントアクセスの設定については、第 9 章 「メールのフィルタリングとアクセス制御」を参照してください。

第 12 章

ログ記録とログ解析

iPlanet Messaging Server では、ログファイルを作成して、管理に関連したサーバのイベント、サーバでサポートされているプロトコル （SMTP、POP、IMAP、HTTP）を使った通信関連のイベント、およびサーバで処理されるその他のプロセスに関連するイベントを記録できます。そのログファイルを調べれば、サーバのアクションをさまざまな観点から監視できます。

MTA は他のサービスとは異なるログ機構を使用しているため、iPlanet Console を使ってログサービスを設定したりログを表示することはできません。設定ファイルに情報を定義することで、MTA のログ設定を行います。この章は、以下のように 3 部構成になっています。第 1 部では概要について、第 2 部ではメッセージストアおよび管理のログ、第 3 部では MTA サービスのログについて説明します。

第 1 部 概要

第 2 部 サービスログ （メッセージストアおよび管理サーバ）

第 3 部 サービスログ （MTA）

第 1 部 概要

Messaging Server ログファイルの作成と管理に関するポリシーはカスタマイズできます。この章では、ログファイルの種類と構造、およびログファイルの管理と表示方法について説明します。

サービスとログファイル

Messaging Server は、サポートしている主なプロトコルやサービスごとに一連のログファイルを作成します。ログファイルの各タイプは、個別にカスタマイズしたり表示することができます。表 12-1 に、ログ記録が可能なサービスのリストとそれぞれのログファイルに関する説明を示します。

表 12-1　　サービスとログファイル

サービス	ログファイルの説明
Admin	Administration Server を介した iPlanet Console と Messaging Server（主に複数の CGI プロセス）間の通信に関連するログイベントが記録されます。
SMTP	SMTP アクティビティに関連するログイベントが記録されます。
IMAP	サーバの IMAP4 アクティビティに関連するイベントが記録されます。
POP	サーバの POP3 アクティビティに関連するログイベントが記録されます。
HTTP	サーバの HTTP アクティビティに関連するログイベントが記録されます。
Default	サーバのその他のアクティビティ（コマンドラインユーティリティやその他のプロセスなど）に関連するログイベントが記録されます。

サードパーティ製のツールを使ってログを解析する

iPlanet Messaging Server ではサポートされていないログ解析やレポート生成を行うには、別のツールを利用する必要があります。ログファイルは、テキストエディタや標準のシステムツールで操作できます。

正規表現による構文解析をサポートするスクリプタブルなテキストエディタを利用すると、この章で説明しているような特定の条件に基づくログエントリの検索や抽出を実施できます。さらに、その結果を並べ替えたり、集計や統計を行うこともできます。

UNIX 環境では、UNIX の `syslog` ファイルを操作するために開発された既存のレポート生成ツールを変更して使用することも可能です。パブリックドメインの `syslog` 操作ツールを使用する場合は、日付 / 時刻フォーマットのほか、Messaging Server のログエントリにある `syslog` エントリにはない *facility* と *logLevel* の 2 つの特殊コンポーネントの変更が必要な場合があります。

第 2 部 サービスログ （メッセージストアおよび管理サーバ）

ここでは、POP、IMAP、HTTP、Admin、および Default の各サービスに関するログについて説明します （表 12-1 を参照）。

これらのサービスの場合には、iPlanet Console を使ってログの設定と表示ができます。設定内容は、どのイベントを記録するか、何件まで記録するかという点に影響します。これらの設定とその他の特徴を利用して、ログファイルの解析時にログイベントの検索条件を微調整できます。

第 2 部には、以下の項目があります。

- ログの特徴
- ログファイルのフォーマット
- ログオプションを定義、設定する
- ログを検索、表示する

ログの特徴

ここでは、メッセージストアおよび管理サービスに関するログの特徴（ ログレベル、ログイベントのカテゴリ、ログのファイル名規則、ログファイルのディレクトリ）について説明します。

ログレベル

ログのレベル（優先順位）設定では、ログのアクティビティをどれだけ詳細に行うのか（詳細度）を定義します。レベル (重要度) が高いほど、ログの詳細度は低くなります。優先順位の高いイベントだけがログに記録されるためです。一方、レベルを下げると、ログは詳細なものとなり、より多くのイベントがログファイルに記録されます。

ログレベルは、POP、IMAP、HTTP、Admin、および Default の各サービスごとに個別に設定できます。ログレベルを設定することで、ログイベントを検索するときにフィルタリングが可能になります。表 12-2 に、設定可能なレベルを示します。これらのログレベルは、UNIX の `syslog` 機構で定義されるレベルのサブセットです。

表 12-2　ストアサービスと管理サービスのログレベル

レベル	説明
Critical	最も詳細度の低いログが作成されます。メールボックスや実行に必要なライブラリにサーバがアクセスできない場合など、サーバに重大な問題や致命的な状態が発生したときにイベントがログに記録されます。
Error	クライアントあるいは別のサーバへの接続に失敗した場合など、エラー状態が発生したときにイベントがログに記録されます。
Warning	サーバがクライアントから送られたデータを解釈できない場合など、警告状態が発生したときにイベントがログに記録されます。
Notice	ユーザがログインに失敗したり、セッションを終了した場合など、通知 （通常の状態における重要なイベント）が発生したときにイベントがログに記録されます。
Informational	ユーザがログオンやログオフを行ったり、あるいはメールボックスを作成したり名前を変更した場合など、重要なアクションが行われたときにイベントがログに記録されます。
Debugging	最も詳細度の高いログファイルが作成されます。デバッグを行う場合に役立ちます。各プロセスあるいはタスク内の個々のステップごとにイベントがログに記録されるため、問題箇所を正確に突き止めることができます。

特定のログレベルを選択すると、そのレベルのイベントおよびそれ以上のレベルの （詳細度の低い）イベントがログに記録されます。デフォルトのログレベルは、`Notice` に設定されています。

注　低レベルの （より詳細な）ログを指定するほど、ログファイルがより多くのディスク容量を使用するようになります。そのガイドラインににについては、287 ページの「ログオプションを定義、設定する」を参照してください。

ログイベントのカテゴリ

サポートされているサービスあるいはプロトコル内で、Messaging Server はイベントが発生する機構すなわち機能上の領域に基づいてログイベントをさらに分類します。ログファイルに記録された各イベントには、そのイベントを生成した機構の名前が記されています。これらのカテゴリは、イベントを検索する際のフィルタリングに利用できます。表 12-3 に、Messaging Server がログ処理用に認識するカテゴリのリストを示します。

表 12-3　ログイベントの発生場所のカテゴリ

機構	説明
General	プロトコルあるいはサービスに関連するアクション全般。
LDAP	LDAP ディレクトリデータベースにアクセスする Messaging Server に関連するアクション。
Network	ネットワークの接続に関するアクション（ソケットエラーなど）。
Account	ユーザのアカウントに関連するアクション（ユーザのログインなど）。
Protocol	プロトコル固有のコマンドに関連するプロトコルレベルのアクション（POP、IMAP、HTTP 機能によって返されるエラーなど）。
Stats	サーバの統計データ収集に関連するアクション。
Store	メッセージストアに関連する低レベルのアクション（読み込み / 書き込みエラーなど）。

ログを検索する際のフィルタリングにカテゴリを使用する例については、291 ページの「ログを検索、表示する」を参照してください。

メッセージストアおよび管理に関連するログファイルの名前

POP、IMAP、HTTP、Admin、および Default サービスのログファイルには、同一のネーミング規則が適用されます。各ログファイルのファイル名は、以下の形式に従います。

```
service.sequenceNum.timeStamp
```

表 12-4 に、メッセージストアに関連するログファイルのネーミング規則を示します。

表 12-4　ストアおよび管理に関連するログファイルのネーミング規則

構成要素	定義
service	ログの対象であるサービス：POP、IMAP、HTTP、Admin、Default
sequenceNum	ログファイルディレクトリ内に作成されたログファイルの順番を表す整数値。新しいログファイルほど、この値が大きくなります。このシーケンスの値がロールオーバーすることはなく、値はサーバのインストール時に始まり、そのサーバを使用している限り常に増え続けます。
timeStamp	ファイルが作成された日付と時刻を表す整数値。この値は UNIX 標準の時刻形式で表されます。つまり、1970 年 1 月 1 日零時以降の秒数です。

たとえば、imap.63.915107696 という名前のログファイルは、IMAP ログファイルのディレクトリで 63 番目に作成されたログファイルであり、作成日および作成時刻が 1998 年 12 月 31 日 12:34:56 PM であることを表します。

拡張可能なシーケンス番号とタイムスタンプを組み合わせることによって、解析するファイルのローテーション、期間、および選択における柔軟性が増します。詳細については、287 ページの「ログオプションを定義、設定する」を参照してください。

ログファイルのディレクトリ

ログされる各サービスごとにディレクトリが 1 つ割り当てられ、ログファイルはそこに保存されます。IMAP ログファイルや POP ログファイルなど、各サービスのログファイルは、それぞれのディレクトリ内に一緒に保存されます。各ディレクトリの場所、そのディレクトリ内に保存できるログファイルの数、ファイルの最大サイズは、設定できます。

すべてのログファイルを保存するのに十分な容量があることを確認してください。ログレベルが低いほど、(詳細度が高くなるほど) ログファイルのサイズは大きくなり易くなります。

すべてのログファイルディレクトリのバックアップが行われ、ディレクトリが過負荷状態にならないように、ログレベル、ログローテーション、ログ有効期間、およびサーバのバックアップポリシーを正しく設定することが重要です。詳細については、287 ページの「ログオプションを定義、設定する」を参照してください。

ログファイルのフォーマット

Messaging Server によって作成されたメッセージストアログファイルと管理サービスログファイルのコンテンツフォーマットはすべて同じです。ログファイルは、複数のテキスト行から構成されており、各行にイベントが 1 つ記述されています。サポートされている各サービスに対するすべてのイベントは、通常以下のようなフォーマットで記述されています。

日付時刻 ホスト名 プロセス名 [pid]: カテゴリ ログレベル : イベントメッセージ

表 12-5 に、ログファイルの構成要素を示します。このイベント記述フォーマットは、日付 / 時刻フォーマットが異なることと、さらに別の 2 つの構成要素（*カテゴリ*と*ログレベル*）があることを除き、UNIX の syslog 機構で定義されているものと同じです。

表 12-5　　ストアログファイルと管理ログファイルの構成要素

構成要素	定義
日付時刻	イベントが記録された日付および時刻。*dd/mm/yyyy hh:mm:ss* の形式で表記されます。タイムゾーンフィールドは GMT を基準とした +/-*hhmm* の形式で表記されます。以下に例を示します。 02/Jan/1999:13:08:21 -0700
ホスト名	サーバが実行されているホストマシンの名前。以下に例を示します。showshoe **注意 :** ホストに複数の Messaging Server インスタンスがある場合には、プロセス ID（pid）を使ってログイベントのインスタンスを区別できます。

表 12-5　ストアログファイルと管理ログファイルの構成要素（続き）

構成要素	定義
プロセス名	イベントを生成したプロセスの名前。例：cgi_store
pid	イベントを生成したプロセスのプロセス ID。例：18753
カテゴリ	イベントが属するカテゴリ。例：General（285 ページの「表 12-3」を参照）
ログレベル	イベントのログレベル。例：Notice（284 ページの「表 12-2」を参照）
イベントメッセージ	イベント固有のメッセージ（任意の長さのメッセージ）。例：Log created (894305624)

以下に、iPlanet Console を使って表示した 3 つのログイベントの例を示します。

```
02/May/1998:17:37:32 -0700 showshoe cgi_store[18753]:
General Notice:
    Log created (894155852)

04/May/1998:11:07:44 -0400 xyzmail cgi_service[343]: General Error:
    function=getserverhello|port=2500|error=failed to connect

03/Dec/1998:06:54:32 +0200 SiroePost imapd[232]: Account Notice:
    close [127.0.0.1] [unauthenticated] 1998/12/3 6:54:32
    0:00:00 0 115 0
```

IMAP および POP のイベントエントリの末尾は、3 つの数値である場合があります。上の例では「0 115 0」となっています。最初の数値はクライアントによって送信されたバイト数、2 番目の数値はサーバによって送信されたバイト数、3 番目の数値は選択されたメールボックスの数 (POP の場合は常に 1) を表しています。

[ログビューア] ウィンドウにログファイルを表示する場合は、ログレベルやカテゴリ、あるいはプロセス ID などのイベント固有の構成要素を検索し、表示するイベントを制限できます。詳細については、291 ページの「ログを検索、表示する」を参照してください。

各ログエントリのイベントメッセージは、ログに記録されるイベントのタイプに特有のフォーマットで表記されます。つまり、各サービスごとに、イベントメッセージに含まれるコンテンツが定義されます。ほとんどのイベントメッセージは簡単で明白なものですが、中には複雑なものもあります。

ログオプションを定義、設定する

メッセージストアと管理サービスのログ設定は、管理業務のニーズに合わせて定義できます。ここでは、最適な設定およびポリシーを決定するために役立つ情報、およびそれらの適用方法について説明します。

柔軟性のあるログ構造

ログファイルの名前形式（*サービス*.*シーケンス番号*.*タイムスタンプ*）は、柔軟性のあるログローテーションとバックアップポリシーの設定に役立ちます。異なるサービスのイベントは、それぞれ別のファイルに記録されるため、問題箇所の素早い検出が可能になります。また、ファイル名中のシーケンス番号は常に増え続け、タイムスタンプは常に固有のものであるため、指定したシーケンス番号の限界に達しても、新しいログファイルが古いログファイルを自動的に上書きしてしまうことはありません。古いログファイルの上書きや削除が行われるのは、ログファイルの保存期間や最大ファイル数、あるいは合計ログ容量など、より柔軟性のある制限がその限界に達したときにだけです。

Messaging Server では、管理やバックアップの作業を簡素化できるように、ログファイルの自動ローテーションがサポートされています。後続のログイベントを記録するために，手作業で記録中のログファイルを回収して新しいログファイルを作成する必要はありません。ディレクトリ内にあるファイルはすべて (記録中のログファイル以外)、サーバを停止させたり、新しいログファイルの開始を手作業で指定することなく、いつでもバックアップを作成できます。

ログポリシーの設定では、各サービスごとに、合計保存容量、最大ログファイル数、個々のファイルサイズ、ログファイルの最長保存期間、ログファイルのローテーション頻度といったオプションを設定できます。

適切なオプションを判断する

複数の制限を設定する必要があることと、それらの中にはログファイルのローテーションや削除を発生させるものがあることを理解しておいてください。最初に限界に達する制限が制御の中心となります。たとえば、ログファイルの最大サイズを 3.5 MB に設定し、新規のログを毎日作成するように設定したとします。しかし、24 時間以内に 3.5 MB 以上のデータが記録される場合は、指定期間内に複数のログファイルが作成されることになります。したがって、最大ログファイル数が 10 個、最長有効期間が 8 日に設定されている場合でも、8 日に達する前に 10 個のファイルが作成され、指定期間まで達しない可能性があります。

以下に、適切なオプションを判断する際に役立つ一般的な設定を示します。これは Messaging Server 管理ログのデフォルトです。

ディレクトリ内の最大ログファイル数 : 10
最大ログファイルサイズ : 2 MB
全ログファイルを対象とする合計最大サイズ : 20 MB
最小空きディスク容量 : 5 MB
ログロールオーバー期間 : 1 日
最長有効期間 : 7 日
ログレベル : Notice

この設定の場合、サーバ管理ログのデータは 1 日あたり 2 MB 記録され、バックアップは毎週作成されます。また、管理ログの保存に割り当てられている合計容量は 25 MB 以上です (ログレベルの詳細度を上げると、この設定では不十分になる可能性があります)。

POP、IMAP、HTTP のログの場合も、同様の設定から始めてみるとよいでしょう。すべてのサービスに上記のデフォルト値と同じ容量のログが必要だとすると、最初にログを保存するために 150 MB のディスク容量が必要になります（ここに示した設定はあくまでも一般例であるため、実際の条件とは異なる場合があります)。

ログオプションを設定する

メッセージストアのログ設定を制御するオプションは、iPlanet Console あるいはコマンドラインを使って指定できます。

これらのオプションの最適な設定は、ログデータが集積される頻度によって異なります。1 MB の保存領域には、約 4,000 ～ 10,000 件のログエントリを記録できます。適度に使用されているサーバでは、ログレベルが低い場合 （Notice など）、1 週間あたり数百メガバイトのログデータが記録されます。以下の設定方法を参考にしてください。

- 使用可能な保存領域の上限に合わせてログレベルを設定します。つまり、使用可能な保存領域の上限に基づき、ログデータの集積頻度を考慮してログレベルを判断します。
- 検索処理に影響が出ないように、ログファイルのサイズを設定します。ローテーションスケジュールと合計保存領域の上限を考慮して調整します。ログエントリが集積される頻度に基づいて、ローテーションが自動的に発生するまでに集積されるデータのサイズより少し多めに最大値を設定します。最大ファイルサイズと最大ファイル数を掛け合わせることによって得られる値が、合計保存領域の上限とほぼ等しくなります。

  たとえば、IMAP ログローテーションを毎日、1 日あたりに集積される IMAP ログデータが 3 MB、IMAP ログの合計保存領域の上限が 25 MB である場合、IMAP ログファイル の最大サイズは 3.5 MB に設定します （この例では、データ集積頻度が高く、すべてのログファイルが最大サイズおよび最大ファイル数に達するほど速いスピードでデータが集積される場合、ログデータが失われる可能性があります）。
- サーバのバックアップが毎週で IMAP ログローテーションが毎日である場合、最大 IMAP ログファイル数を約 10 （個々のログファイルのサイズの上限を越える場合のローテーション頻度を考慮）、および有効期間を 7 ～ 8 日に設定します。
- 使用するハードウェアの容量とサーバのバックアップスケジュールに基づいて、合計保存領域の上限を設定します。データの集積頻度を予測し、サーバのバックアップ周期を超えないように保存容量の上限値を少し多めに設定します。

  たとえば、1 日あたりに集積される IMAP ログデータが平均 3 MB、サーバのバックアップが毎週である場合、IMAP ログの保存領域限度は 25 ～ 30 MB に設定します（十分な保存領域があると仮定した場合）。
- 安全性を確保するため、ログファイルを保存するボリュームに、最小空きディスク容量を設定します。ログファイルサイズ以外の要因でボリュームがいっぱいになることがあった場合、いっぱいになったディスクにログデータを書き込もうとすることが原因でエラーが発生する前に古いファイルが削除されます。

ログ情報は、サーバによるログファイルではなく、syslog 機構に送るよう選択することもできます。ログ情報を syslog に送るには、`syslogfacility` オプションを以下のように設定します。

```
configutil -o logfile. サービス.syslogfacility -v 値
```

この場合の *サービス* には `admin`、`pop`、`imap`、あるいは `http` を、*値* には `user`、`mail`、`daemon`、`local0` ～ `local7`、または none を指定します。

値が設定されると、設定値に対応する syslog 機構のログにメッセージが記録され、その他のすべてのログファイルサービスオプションが無視されます。オプションが設定されていないか、あるいは値が none の場合には、Messaging Server のログファイルが使用されます。

コンソール - iPlanet Console を使ってログオプションを設定するには、以下の手順に従います。

1 ログファイルオプションを設定する Messaging Server を開きます。

2 [環境設定] タブをクリックし、左側のパネルで [ログファイル] フォルダを開き、サービス （IMAP、HTTP、Admin など）のログファイルを選択します。

3 [詳細レベル] ドロップダウンリストからログレベルを選択します。

4 [ログファイルのディレクトリパス] フィールドに、ログファイルの保存先となるディレクトリの名前を入力します。

5 [各ログのファイルサイズ] フィールドに、ログファイルの最大サイズを入力します。

6 [新規ログエントリの作成] フィールドに、ログローテーションスケジュールの値を入力します。

7 [ディレクトリ当たりのログ数] および [ログが次の日付よりも古い場合] フィールドに、最大ログファイル数と期限を示す値を入力し、バックアップスケジュールとの兼ね合いを調整します。

8 [ログサイズの合計が次の値を超えたとき] フィールドに、合計保存領域の上限を入力します。

9 [残りディスク容量が次の値以下になった場合] フィールドに、確保しておく空きディスク容量の最小値を入力します。

コマンドライン - コマンドラインでログオプションを設定するには、以下の例のように configutil コマンドを使用します。

ログレベルを設定するには、以下の手順に従います。

```
configutil -o logfile.サービス.loglevel -v レベル
```

「*サービス*」には、admin、pop、imap、または http のいずれかを、「*レベル*」には、Nolog、Critical、Error、Warning、Notice, Information、または、Debug のいずれかを指定します。

ログファイルのディレクトリパスを指定するには :

```
configutil -o logfile.サービス.logdir -v ディレクトリパス
```

各ログの最大ファイル サイズを指定するには、以下の手順に従います。

```
configutil -o logfile.サービス.maxlogfilesize -v サイズ
```

「*サイズ*」には、バイト数を指定します。

ログのローテーションスケジュールを指定するには、以下の手順に従います。

```
configutil -o logfile.サービス.rollovertime -v 数値
```

「*数値*」には秒数を指定します。

ディレクトリ内の最大ログファイル数を指定するには、以下の手順に従います。

`configutil -o logfile.`*サービス*`.maxlogfiles -v` *数値*

保存容量の限度を指定するには、以下の手順に従います。

`configutil -o logfile.`*サービス*`.maxlogsize -v` *数値*

「*数値*」にはバイト数を指定します。

確保しておく空きディスク容量の最小値を指定するには、以下の手順に従います。

`configutil -o logfile.`*サービス*`.minfreediskspace -v` *数値*

「*数値*」にはバイト数を指定します。

ログの存続期間を指定するには、以下の手順に従います。

`configutil -o logfile.`*サービス*`.expirytime -v` *数値*

「*数値*」には秒数を指定します。

ログを検索、表示する

iPlanet Console には、メッセージストアおよび管理に関するログデータを表示するための基本的なインターフェースがあります。個々のログファイルを選択したり、それらのファイル内で柔軟にフィルタリングを行って、ログエントリを検索することができます。

ログファイルは、サービスごとに分かれており、それぞれ作成順に表示されます。検索するログファイルを選択し、検索パラメータを指定して個々のイベントの検索対象を限定できます。

検索パラメータ

以下に、表示するログデータを特定するための検索パラメータを示します。

- **期間** : イベントを読み取る期間の開始と終了を指定するか、または検索する日数（現時点からさかのぼる日数）を指定します。サーバがクラッシュしたり、その他のイベントが発生した時点までの一定期間のログイベントを調べる場合に使用します。また、記録中のログファイルで今日のイベントだけを見る場合は、期間を 1 日に指定することもできます。
- **ログレベル** : ログレベルを指定できます （283 ページの「ログレベル」を参照）。特定の問題を検出するために該当するレベルを選択します。たとえば、サーバがダウンした原因を調べるためには Critical を、失敗したプロトコルコールを検出するためには Error を選択します。
- **機能** : 機能を指定できます （284 ページの「ログイベントのカテゴリ」を参照）。問題が含まれている機能領域が分かっている場合には、特定の機能を選択できます。たとえば、サーバのクラッシュにディスクエラーが関連していると思われる場合は Store を、IMAP プロトコルコマンドに問題があると思われる場合には Protocol を選択します。

- **テキスト検索パターン：** テキスト検索パターンを指定して検索対象を絞ることができます。イベントの構成要素を含めることができます（286 ページの「ログファイルのフォーマット」を参照）。イベント時刻、プロセス名、プロセス ID、イベントメッセージの一部 (リモートホスト名、関数名、エラー番号など) のイベント構成要素をワイルドカードなどで表現して目的のイベントを指定できます。

  検索パターンには、以下の特殊文字およびワイルドカード文字を使用できます。

  * 任意の文字セット （例：*.com）
  ? 任意の 1 文字（例： 199?）
  [*nnn*] 中の一連の文字 *nnn*（例：[aeiou]）
  [^*nnn*] 一連の文字 *nnn* 以外の任意の文字 （例：[^aeiou]）
  [*n-m*] 範囲 *n-m* 内 の任意の文字 （例：[A-Z]）
  [^*n-m*] 範囲 *n-m* 外の任意の文字 （例：[^0-9]）
  \ エスケープ文字：*、?、[、または] の前に配置してリテラルとして使用

注意：検索では、大文字と小文字が区別されます。

ログを表示する際にログレベルと機能を組み合せた検索を行う場合は、以下のオプションを含めることができます。

- 潜在的なセキュリティ違反を調べる際に役立つエラーログを表示するには、Account 機能 （および Notice ログレベル）を指定します。
- 接続に関する問題を調べるときには、Network 機能 （およびすべてのログレベル）を指定します。
- サーバの機能に関する基本的な問題を調べるときには、すべての機能 （および Critical ログレベル）を指定します。

検索を指定し、結果を表示する

指定したサービスに固有のログイベントを検索するには、以下の手順に従います。

1 iPlanet Console で、ログファイルの対象となる Messaging Server を開きます。

2 以下のいずれかの方法で、指定したサービスログの [コンテンツ] タブを表示します。

   - [タスク] タブをクリックし、[< サービス > ログの表示] をクリックします。この場合の < サービス > は、ログに記録されているサービスの名前 （IMAP や Admin など）です。
   - [環境設定] タブをクリックし、左側のパネルで該当サービス（IMAP や Admin など）のログファイルフォルダを選択します。右側のパネルで [コンテンツ] タブをクリックします。

3 ログされたサービスの [コンテンツ] タブが表示されます。

4 [ログファイル名] フィールドで、調べたいログファイルを選択します。

5 [選択したログの表示] ボタンをクリックし、[ログビューア] ウィンドウを開きます。

6 [ログビューア] ウィンドウで、検索パラメータを指定します （前述の「検索パラメータ」を参照）。

7 [更新] をクリックして検索を実行し、[ログエントリ] フィールドに結果を表示します。

第 3 部 サービスログ （MTA）

MTA には、各メッセージがキューに入ったりキューから取り出されるときに、それらのメッセージをログに記録する機能が備わっています。チャネルごとにログに記録することも、またはすべてのチャネルにおけるメッセージアクティビティをログに記録することもできます。初期設定では、すべてのチャネルでログが無効になっています。

ログ機能を有効にすると、メッセージが MTA チャネルを通過するたびに `mail.log*` ファイルにエントリが追加されます。これらのログエントリは、MTA（あるいは特定チャネル）を通過するメッセージの件数を調べたり、メッセージが送信あるいは配信されたかどうか、いつ送信あるいは配信されたのかなどを調べるときに役に立ちます。

特定の MTA チャネルを通過したメッセージの件数について統計を得るだけであれば、該当する MTA チャネルについてのみ logging チャネルキーワードを有効にするとよいでしょう。ほとんどのサイトでは、すべての MTA チャネルについてログ機能を有効にしています。特に、問題の原因を追求する際には、問題分析の最初のステップとして特定のチャネルにメッセージが送られているかどうかを調べることができるように、すべてのチャネルについてのログが有効になっていると便利です。

注意 ログ機能が有効になっている場合は、`mail.log` が大きくなりつづけるため、そのままにしておくと使用可能なディスク容量がなくなってしまいます。このファイルのサイズを監視し、定期的に不要なコンテンツを削除するようにしてください。ファイル自体を削除することもできます。その場合は、必要に応じて新しいファイルが作成されます。

MTA のログ機能を有効にする

目的のチャネルについてログ機能を有効にするには、以下の例のように、MTA 設定ファイルのチャネル定義に `logging` キーワードを追加します。

チャネル名 キーワード1 キーワード2 `logging`

すべてのチャネルについてメッセージアクティビティをログファイルに記録する場合には、defaults チャネルブロックを MTA 設定ファイルのチャネルブロックセクションの冒頭に追加します。例：

```
defaults logging

l defragment charset7 us-ascii charset8 iso-8859-01
siroe.com
```

`defaults` チャネルは、MTA 設定ファイルの最初の空白行のすぐ後にあるはずです。`defaults logging` 行の前後には、それぞれ空白行が必要です。

メッセージがキューに入ったりキューから取り出されるたびに、そのメッセージに関するログが記録されます。ログエントリはすべて、MTA ログディレクトリ内の mail.log_current ファイルに記 3 録されます (MTA ログディレクトリ : msg- *インスタンス* /log/imta/mail.log_current)。

毎晩深夜に実行されるメッセージリターンジョブでは、まず既存の mail.log_yesterday が mail.log というログファイルに追加されます。その後、現在の mail.log_current ファイルが mail.log_yesterday というファイル名に変更され、新規の mail.log_current ファイルが作成されます。connection.log* ファイルについても同様の処理が行われます。

LOG_MESSAGES_SYSLOG オプションを設定して、MTA ログメッセージを syslog に送ることもできます。

その他の MTA ログオプションを指定する

ログ機能を有効にしたときに与えられる基本的な設定のほかにも、MTA オプションファイルでさまざまな MTA オプション LOG_* を設定することにより、オプションの情報フィールドを含めることができます。オプションファイルの詳細については、『Messaging Server リファレンスマニュアル』を参照してください。

- LOG_MESSAGE_ID : エントリとメッセージの関連性を示すことができます。
- LOG_FILENAME : 特定のメッセージファイルの配信を何回試みたのかを即座に把握できるようになります。また、複数の受信者宛に MTA がいつメッセージを分割し、メッセージファイルをディスクにコピーしたのかを調べる際にも役立ちます。
- LOG_CONNECTION が TCP/IP 接続およびメッセージトラフィックのログを記録できます。接続に関するログエントリは、mail.log* ファイルに記録されるようにデフォルトで設定されていますが、connection.log* ファイルに記録することもできます (SEPARATE_CONNECTION_LOG を参照)。
- SEPARATE_CONNECTION_LOG : 接続に関するログエントリを connection.log ファイルに記します。
- LOG_PROCESS : LOG_CONNECTION といっしょに使用することで、接続エントリとメッセージエントリとの関連性をプロセス ID によって示すことができます。
- LOG_USERNAME : メールをキューに入れるプロセスに関連付けられているユーザ名を mail.log ファイルに保存するかどうかを制御します。SASL （SMTP AUTH） を使用している SMTP 送信の場合は、ユーザ名フィールドが認証ユーザ名となります （先頭にアスタリスク「*」が付きます)。

MTA ログエントリのフォーマット

MTA ログファイルは、ASCII テキストとして記述されます。デフォルトでは、図 12-1 に示すように、各ログファイルエントリに 8 個または 9 個のフィールドが含まれます。

図 12-1　　MTA ログエントリのフォーマット

```
19-Jan-1998 19:16:57.64 l tcp_local E 1 adam@sesta.com
 rfc822;marlowe@siroe.com marlowe@siroe.com
```

ログエントリには以下の情報が含まれています。

1　エントリが記録された日付および時刻。

2　ソースチャネルのチャネル名 （上記の例では l）。

3　宛先チャネルのチャネル名 （上記の例では tcp_local）。SMTP チャネルの場合は、LOG_CONNECTION が有効になっているとき、プラス記号「+」が SMTP サーバの受信、マイナス記号「-」が SMTP クライアント経由の送信を表します。

4　エントリのタイプ（上記の例では E）。表 12-6 を参照。

5　メッセージのサイズ（上記の例では 1）。デフォルトでは、キロバイト単位に設定されていますが、MTA オプションファイルで BLOCK_SIZE キーワードを使って単位を変更することもできます。

6　エンベロープ From: アドレス（上記の例では adam@sesta.com）。通知メッセージのように、エンベロープの From: アドレスが空白のメッセージの場合、このフィールドは空白になります。

7　オリジナルのエンベロープ To: アドレス （上記の例では marlowe@siroe.com）。

8　アクティブな (現在の) エンベロープ To: アドレス（上記の例では marlowe@siroe.com）。

9　配信ステータス （SMTP チャネルのみ）。

表 12-6 に、ログエントリの各コードを示します。

表 12-6　　ログエントリのコード

エントリ	説明
D	キューからの取り出しに成功
DA	SASL （認証）に関し、キューからの取り出しに成功
DS	TLS （セキュリティ）に関し、キューからの取り出しに成功
DSA	TLS および SASL （セキュリティと認証）に関し、キューからの取り出しに成功
E	キューに送信
EA	SASL （認証）に関し、キューへの送信に成功
ES	TLS （セキュリティ）に関し、キューへの送信に成功
ESA	TLS および SASL （セキュリティと認証）に関し、キューへの送信に成功
J	キューへの送信試行で拒否（スレーブチャネルプログラムによる拒否）
Q	キューからの取り出しで一時的な失敗
R	キューからの取り出し試行で受信者アドレスの拒否 （マスターチャネルプログラムによる拒否）、または失敗 / バウンスメッセージの生成
W	未配信メッセージに関する警告メッセージの生成
Z	数人の受信者に対して送信できたが、この受信者に対しては一時的に失敗 (全受信者宛のオリジナルのメッセージファイルはキューから取り出され、失敗した受信者宛の新しいメッセージがキューに入ります)
SMTP チャネルの LOG_CONNECTION + / - エントリ	
C	接続終了
O	接続開始
X	接続拒否
Y	接続が確立される前、試行に失敗
I	ETRN コマンド受信

LOG_CONNECTION、LOG_FILENAME、LOG_MESSAGE_ID、LOG_NOTARY、LOG_PROCESS、および LOG_USERNAME がすべて有効になっている場合、フォーマットは、図 12-2 のようになります。以下の例ではログエントリ行は改行されて表示されていますが、実際のログエントリは 1 行に記述されます。

図 12-2 その他のフィールドを含むログフォーマット

```
19-Jan-1998 13:13:27.10 HOSTA   2e2d.2.1 tcp_local   l
 E 1 service@siroe.com rfc822;adam@sesta.com
 adam 276 /imta/queue/l/ZZ01IWFY9ELGWM00094D.00
 <01IWFVYLGTS499EC9Y@siroe.com> inetmail
 siroe.com (siroe.com [192.160.253.66])
```

前述の説明に含まれていないフィールドは、以下のとおりです。

1 チャネルプロセスを実行しているノードの名前 （上記の例では HOSTA）。

2 プロセス ID （16 進数）、およびその後に続くドット文字 （ドット）とカウント。マルチスレッドのチャネルエントリ （tcp_* チャネルエントリなど）の場合は、プロセス ID とカウントの間にスレッド ID が挿入されます。上記の例では 2e2d.2.1 がプロセス ID です。

3 メッセージの NOTARY （配信受け取りリクエスト）フラグ。整数値で表記 （上記の例では 276）。

4 MTA キュー領域内のファイル名 （上記の例では /imta/queue/l/ZZ01IWFY9ELGWM00094D.00）。

5 メッセージ ID （上記の例では <01IWFVYLGTS499EC9Y@siroe.com>）。

6 実行プロセスの名前 （上記の例では inetmail）。UNIX における SMTP サーバなどのディスパッチャプロセスの場合は、通常 inetmail （SASL が使用されない場合）。

7 接続情報 （上記の例では siroe.com (siroe.com [192.160.253.66]）。接続情報は、送信システム、チャネル名（送信側システムが HELO/EHLO 行に示す名前など）、あるいは (他の種類のチャネルに対する) チャネルの正式なホスト名から構成されています。TCP/IP チャネルの場合は、送信側システムの正式な名前です。ident* チャネルキーワードを使用して、DNS 逆参照により報告されるシンボリック名や IP アドレスを括弧内に示すこともできます （154 ページの「IDENT 検索」を参照）。この例では、DNS から見つかった名前と IP アドレスの両方を表示するように選択するキーワードの 1 つ (たとえば、デフォルトの identnone キーワード) が使用されていると仮定しています。

MTA ログファイルを管理する

毎晩深夜に実行されるメッセージリターンジョブでは、まず既存の mail.log_yesterday が mail.log という集積ログファイルに追加されます。その後、現在の mail.log_current ファイルの名前が mail.log_yesterday に変更され、新しい mail.log_current ファイルが作成されます。また、connection.log* ファイルについても同様の処理が行われます。

MTA は、自動的にロールオーバーを行って現在のファイルを維持しますが、エントリが累積される mail.log ファイルでは、ファイルのバックアップ、切り捨て、ファイルの削除などのタスクのポリシーを決めて管理する必要があります。

ログファイルの管理方法を考えるときには、MTA の定期的なリターンジョブが、サイトから提供された *サーバ- インスタンス* /imta/bin/daily_cleanup プロシージャを実行する （該当プロシージャがある場合）ことに注意してください。したがって、サイトによっては、古い mail.log ファイルの名前を 1 週間に 1 回 （または 1 月に 1 回）変更するなど、独自のクリーンアッププロシージャを適用することがあります。

MTA メッセージログの例

MTA メッセージファイルにログされるフィールドのフォーマットおよびフィールドのリストは、設定したオプションによって異なります。ここでは、いくつかの典型的な例を見ながらログエントリについて解説します。その他のオプションのフィールドについては、294 ページの「その他の MTA ログオプションを指定する」を参照してください。

注	ここでは、ログファイルエントリの例が複数行にわたって表示されていることがありますが、実際のログファイルエントリは常に 1 行に記述されます。

ログファイルを見直す際、システムでは通常一度に多くのメッセージが処理されていることに留意してください。したがって、特定のメッセージに関連するエントリは、同時に処理された他のメッセージに関連するエントリの中にあります。基本的なログ情報を見ることにより、何件のメッセージが MTA を通過したのかを把握できます。

同じのメッセージに関する特定のエントリをそのメッセージの同じ受信者に関連付けたい場合は、LOG_MESSAGE_ID を有効にします。MTA キュー領域内の特定のメッセージと特定のファイルを関連付けたり、キューからの取り出しに成功していない特定のメッセージの配信試行が何度行われたかをエントリを見て調べたりする場合には、LOG_FILENAME を有効にします。また、SMTP メッセージ （TCP/IP チャネルを経由して処理されるメッセージ）の場合は、リモートシステムとの TCP 接続とメッセージ送信を関連付けるには、LOG_PROCESS と何らかのレベルの LOG_CONNECTION を有効にします。

図 12-3 に、ローカルユーザが TCP/IP チャネルからインターネットなどにメッセージを送信した場合の基本的なログエントリの例を示します。この例では、LOG_CONNECTION が有効になっています。(1) と (2) の行は 1 つのエントリで、実際のログファイルでは 1 行に記述されます。同様に、(3) ～ (7) の行も 1 つのエントリで、実際のログファイルでは 1 行に記述されます。

図 12-3 ログ : ローカルユーザが送信メッセージを送った場合

```
19-Jan-1998 19:16:57.64 l            tcp_local    E 1 (1)
 adam@sesta.com rfc822;marlowe@siroe.com marlowe@siroe.com (2)

19-Jan-1998 19:17:01.16 tcp_local                 D 1 (3)
 adam@sesta.com rfc822;marlowe@siroe.com marlowe@siroe.com (4)
 dns;thor.siroe.com
 (TCP|206.184.139.12|2788|192.160.253.66|25) (5)
 (THOR.SIROE.COM -- Server ESMTP [iMS V5.0 #8694]) (6)
 smtp;250 2.1.5 marlowe@siroe.com and options OK. (7)
```

1 この行は、ブロックメッセージ (1) をチャネル l から tcp_local チャネルのキューに入れた (E) ときの日付と時刻を示します。

2 この部分は、実際にはログファイルの行 (1) の後に続く部分です。ここでは、印刷上の理由から改行されています。エンベロープ From: アドレス (adam@sesta.com)、およびエンベロープ To: アドレスの元のバージョンと現在のバージョン (marlowe@siroe.com) を示しています。

3 ブロックメッセージ (1) を tcp_local チャネルのキューから取り出した (D) ときの日付と時刻を示します。つまり、tcp_local チャネルからリモートの SMTP サーバにメッセージが送信されたことを示します。

4 エンベロープ From: アドレス、元のエンベロープ To: アドレス、および現在のエンベロープ To: アドレスを示しています。

5 接続先のシステムは DNS で thor.siroe.com という名前であること、ローカルの送信システムの IP アドレスは 206.184.139.12 で、ポート 2788 から送信していること、およびリモート送信先システムの IP アドレスは 192.160.253.66 で、その接続ポートは 25 であることを示します。

6 リモート SMTP サーバの SMTP バナー行を示します。

7 このアドレスに対して返された SMTP ステータスコードを示しています。250 は 基本的な SMTP 成功コードです。また、このリモート SMTP サーバは拡張 SMTP ステータスコードとその他のテキストを返しています。

図 12-4 に示すログエントリは 図 12-3 の例に似ていますが、LOG_FILENAME=1 および LOG_MESSAGE_ID=1 を設定したことによって、その他の情報 （ファイル名とメッセージ ID） も示されています。(1) と (2) を参照してください。特に、メッセージ ID は、エントリとメッセージの関連を示すために使用されます。

図 12-4 ログ : オプションのログフィールドを含めた場合

```
19-Jan-1998 19:16:57.64 l            tcp_local    E 1
 adam@sesta.com rfc822;marlowe@siroe.com marlowe@siroe.com
 /imta/queue/tcp_local/ZZ01ISKLSKLZLI90N15M.00
   <01ISKLSKC2QC90N15M@sesta.com> (1)

19-Jan-1998 19:17:01.16 tcp_local                 D 1
 adam@sesta.com rfc822;marlowe@siroe.com marlowe@siroe.com
 /imta/queue/tcp_local/Z01ISKLSKLZLI90N15M.00
   <01ISKLSKC2QC90N15M@sesta.com> (2)
 dns;thor.siroe.com (TCP|206.184.139.12|2788|192.160.253.66|25)
 (THOR.SIROE.COM -- Server ESMTP [iMS V5.0 #8694])
 smtp;250 2.1.5 marlowe@siroe.com and options OK.
```

図 12-5 は、LOG_FILENAME=1、LOG_MESSAGE_ID=1、および LOG_CONNECTION=1 を有効にして、複数の受信者にメッセージを送信した例を示しています。この場合、ユーザ adam@sesta.com が MTA メーリングリスト test-list@sesta.com に送信したメッセージは、bob@sesta.com、carol@varrius.com、および david@varrius.com に展開されています。各受信者の元のエンベロープ To: アドレスは、test-list@sesta.com ですが、現在のエンベロープ To: アドレスは、それぞれの受信者のアドレスになっていることに注意してください。2 つのファイル （チャネル l と送信チャネル tcp_local） がありますが、メッセージ ID は同一です。

図 12-5 ログ : リスト宛に送信した場合

```
19-Jan-1998 20:01:44.10 l            l            E 1
 adam@sesta.com rfc822;test-list@sesta.com bob
 imta/queue/l/ZZ01ISKND3DE1K90N15M.00
 <01ISKND2H8MS90N15M@sesta.com>

19-Jan-1998 20:01:44.81 l            tcp_local    E 1
 adam@sesta.com rfc822;test-list@sesta.com carol@varrius.com
 imta/queue/tcp_local/ZZ01ISKND2WS1I90N15M.00
 <01ISKND2H8MS90N15M@sesta.com>

19-Jan-1998 20:01:44.81 l            tcp_local    E 1
 adam@sesta.com rfc822;test-list@sesta.com david@varrius.com
 imta/queue/tcp_local/ZZ01ISKND2WS1I90N15M.00
 <01ISKND2H8MS90N15M@sesta.com>

19-Jan-1998 20:01:50.69 l                         D 1
 adam@sesta.com rfc822;test-list@sesta.com bob
 imta/queue/l/ZZ01ISKND3DE1K90N15M.00
 <01ISKND2H8MS90N15M@sesta.com>

19-Jan-1998 20:01:57.36 tcp_local                 D 1
 adam@sesta.com rfc822;test-list@sesta.com carol@varrius.com
 imta/queue/tcp_local/ZZ01ISKND2WS1I90N15M.00
 <01ISKND2H8MS90N15M@sesta.com>
 dns;gw.varrius.com (TCP|206.184.139.12|2788|192.160.253.66|25)
 (gw.varrius.com -- SMTP Sendmail)
 smtp;250 OK.

19-Jan-1998 20:02:06.14 tcp_local                 D 1
 adam@sesta.com rfc822;test-list@sesta.com david@varrius.com
 imta/queue/tcp_local/ZZ01ISKND2WS1I90N15M.00
 <01ISKND2H8MS90N15M@sesta.com>
 dns;gw.varrius.com (TCP|206.184.139.12|2788|192.160.253.66|25)
 (gw.varrius.com -- SMTP Sendmail)
 smtp;250 OK.
```

図 12-6 は、存在しないドメイン（very.bogus.com）宛にメッセージを送信しようとした場合の例です。つまり、MTA の書き換え規則によって「存在しない」と判断されないドメイン名で、かつ送信 TCP/IP チャネルに対して一致するドメイン名を使った場合です。この例では、LOG_FILENAME=1 と LOG_MESSAGE_ID=1 という MTA オプションが設定されていると仮定しています。

TCP/IP チャネルが DNS のドメイン名を調べると、DNS はそのような名前は存在しないという旨のエラーを返します。(5) の拒否エントリ (R) のように、DNS は (6) エラーを返し、ドメイン名が不正であることを示します (6)。

メッセージが発行された後でアドレスが拒否されたため、MTA はオリジナルの送信者宛にバウンスメッセージを生成します。MTA は、この新しい拒否メッセージをキューに入れ、オリジナルの送信者 (1) に送り、オリジナルの送信メッセージを削除する前にそのコピーを postmaster (4) に送信します （(5) の R エントリ）。

例の (2) および (8) に示すように、バウンスメッセージなどの通知メッセージのエンベロープ From: アドレスは空白であるため、エンベロープ From: フィールドも空白になります。MTA で生成されたバウンスメッセージが最初のキューに入れられることにより、オリジナルメッセージのメッセージ ID の後に新規通知メッセージのメッセージ ID が示されます (3)。（この情報は、MTA が常に利用できるわけではありません。この情報がログ用に得られる場合には、失敗した送信メッセージに対応するログエントリを通知メッセージに関連付けることができます。）この通知メッセージは、プロセスチャネルのキューに入れられた後、適切な宛先チャネルのキューに送られます (7)。

図 12-6　　ログ : 存在しないドメインに送信しようとした場合

```
19-JAN-1998 20:49:04 l            tcp_local    E 1
 adam@sesta.com rfc822;user@very.bogus.com user@very.bogus.com
 imta/queue/tcp_local/ZZ01ISKP0S0LVQ94DU0K.00
 <01ISKP0RYMAS94DU0K@SESTA.COM>

19-JAN-1998 20:49:33 tcp_local    process      E 1 (1)
 rfc822;adam@sesta.com adam@sesta.com  (2)
 imta/queue/process/ZZ01ISKP0S0LVQ94DTZB.00
 <01ISKP22MW8894DTAS@SESTA.COM>,<01ISKP0RYMAS94DU0K@SESTA.COM> (3)

19-JAN-1998 20:49:33 tcp_local    process      E 1 (4)
 rfc822;postmaster@sesta.com postmaster@sesta.com
 imta/queue/process/ZZ01ISKP0S0LVQ94DTZB.00
 <01ISKP22MW8894DTAS@SESTA.COM>,<01ISKP0RYMAS94DU0K@SESTA.COM>

19-JAN-1998 20:50:07 tcp_local                 R 1 (5)
 adam@sesta.com rfc822;user@very.bogus.com user@very.bogus.com
 imta/queue/tcp_local/ZZ01ISKP0S0LVQ94DU0K.00
 <01ISKP0RYMAS94DU0K@SESTA.COM>
 Illegal host/domain name found (6)

19-JAN-1998 20:50:08 process      l            E 3 (7)
 rfc822;adam@sesta.com adam (8)
 imta/queue/l/ZZ01ISKP23BUQS94DTYL.00
 <01ISKP22MW8894DTAS@SESTA.COM>

19-JAN-1998 20:50:08 process      l            E 3
 rfc822;postmaster@sesta.com postmaster
 imta/queue/l/ZZ01ISKP23BUQS94DTYL.00
 <01ISKP22MW8894DTAS@SESTA.COM>

19-JAN-1998 20:50:12 l                         D 3
 rfc822;adam@sesta.com adam
 imta/queue/l/ZZ01ISKP23BUQS94DTYL.00
 <01ISKP22MW8894DTAS@SESTA.COM>

19-JAN-1998 20:50:12 l                         D 3
 rfc822;postmaster@sesta.com postmaster
 imta/queue/l/ZZ01ISKP23BUQS94DTYL.00
 <01ISKP22MW8894DTAS@SIROE.COM>
```

図 12-7 は、メッセージがリモートシステムの不正アドレス宛に送信された場合の例を示しています。この例では、LOG_FILENAME=1 と LOG_MESSAGE_ID=1 という MTA オプション設定、および LOG_BANNER=1 と LOG_TRANSPORTINFO=1 というチャネル オプション設定を使用していると仮定しています。(1) の拒否エントリ (R) を見てください。図 12-6 の拒否エントリとは異なり、この拒否エントリにはリモートシステムとの接続が示されています。また、リモート SMTP サーバが発行した SMTP エラーコードも示されています (2)、(3)。(2) に示されている情報は、LOG_BANNER=1 と LOG_TRANSPORTINFO=1 というチャネル オプション設定によるものです。

図 12-7 ログ : 存在しないリモート ユーザ宛に送信した場合

```
20-JAN-1998 13:11:05 l            tcp_local    E 1
 adam@sesta.com rfc822;nonesuch@siroe.com nonesuch@siroe.com
 imta/queue/tcp_local/ZZ01ISLNBB1JOE94DUWH.00
 <01ISLNBAWV3094DUWH@sesta.com>

20-JAN-1998 13:11:08 tcp_local    process      E 1
 rfc822;adam@sesta.com adam@sesta.com
 imta/queue/process/ZZ01ISLNBB1JOE94DSGB.00
 <01ISLNBFKIDS94DUJ8@sesta.com>,<01ISLNBAWV3094DUWH@sesta.com>

20-JAN-1998 13:11:08 tcp_local    process      E 1
 rfc822;postmaster@sesta.com postmaster@sesta.com
 imta/queue/process/ZZ01ISLNBB1JOE94DSGB.00
 <01ISLNBFKIDS94DUJ8@sesta.com>,<01ISLNBAWV3094DUWH@sesta.com>

20-JAN-1998 13:11:11 tcp_local                 R 1   (1)
 adam@sesta.com rfc822;nonesuch@siroe.com nonesuch@siroe.com
 imta/queue/tcp_local/ZZ01ISLNBB1JOE94DUWH.00
 <01ISLNBAWV3094DUWH@sesta.com>
 dns;thor.siroe.com
 (TCP|206.184.139.12|2788|192.160.253.66|25)          (2)
 (THOR.SIROE.COM -- Server ESMTP [iMS V5.0 #8694])
 smtp; 553 unknown or illegal user: nonesuch@siroe.com   (3)

20-JAN-1998 13:11:12 process      l            E 3
 rfc822;adam@sesta.com adam
 imta/queue/l/ZZ01ISLNBGND1094DQDP.00
 <01ISLNBFKIDS94DUJ8@sesta.com>

20-JAN-1998 13:11:12 process      l            E 3
 rfc822;postmaster@sesta.com postmaster
 imta/queue/l/ZZ01ISLNBGND1094DQDP.00
 <01ISLNBFKIDS94DUJ8@sesta.com>

20-JAN-1998 13:11:13 l                         D 3
 rfc822;adam@sesta.com adam@sesta.com
 imta/queue/l/ZZ01ISLNBGND1094DQDP.00
 <01ISLNBFKIDS94DUJ8@sesta.com>

20-JAN-1998 13:11:13 l                         D 3
 rfc822;postmaster@sesta.com postmaster@sesta.com
 imta/queue/l/ZZ01ISLNBGND1094DQDP.00
 <01ISLNBFKIDS94DUJ8@sesta.com>
```

図 12-8 は、MTA がリモート側のメッセージ送信試行を拒否した場合のログファイルエントリを示しています。 この例では、LOG_* オプションが有効になっていないものと仮定しているため、ログエントリには基本的なフィールドしか記述されていません。LOG_CONNECTION オプションを有効にすると、J エントリなどに他の情報フィールドが追加されます。この例は、以下の ORIG_SEND_ACCESS マッピングを使って SMTP リレーブロッキング （195 ページの「SMTP リレーブロッキングを設定する」を参照）が設定された MTA に対するものです。

```
ORIG_SEND_ACCESS

! ...numerous entries omitted...
!
    tcp_local|*|tcp_local|*   $NRelaying$ not$ permitted
```

alan@very.bogus.com は内部アドレスではありません。したがって、リモートユーザ harold@varrius.com が MTA システムを介したリレーを利用してメッセージをリモートユーザ alan@very.bogus.com に送信しようとしても拒否されます。

図 12-8 ログ : リモート側のメッセージ送信試行が拒否された場合

```
28-May-1998 12:02:23 tcp_local                J 0      (1)
 harold@varrius.com rfc822; alan@very.bogus.com         (2)
 550 5.7.1 Relaying not permitted: alan@very.bogus.com  (3)
```

1 このログは、MTA がリモート側のメッセージ送信を拒否したときの日付と時刻を示します。拒否は J レコードで表されています。MTA チャネルのメッセージ送信が拒否されたことは 図 12-6 および 図 12-7 に示されているように、R レコードで表されます。

2 試行されたエンベロープ From: アドレス および To: アドレスが示されています。この場合、オリジナルの To: 情報がなかったため、そのフィールドは空白になっています。

3 このエントリには、MTA がリモート （送信者） 側宛に発行した SMTP エラーメッセージが含まれています。

図 12-9 に、一回目の試行でメッセージを配信できなかったために、MTA が何度も配信試行を行う場合のログファイル エントリの例を示します。この例では、LOG_FILENAME=1 および LOG_MESSAGE_ID=1 オプションが設定されているものと仮定しています。

図 12-9　　ログ : 複数回の配信試行が行われた場合

```
15-Jan-1998 10:31:05.18 tcp_internal   tcp_local  E 3 (1)
 adam@hosta.sesta.com rfc822;user@some.org user@some.org
 imta/queue/tcp_local/ZZ01IS3D2ZP7FQ9UN54R.00
 <01IRUD7SVA3Q9UN2D4@sesta.com>

15-Jan-1998 10:31:10.37 tcp_local                Q 3 (2)
 adam@hosta.sesta.com rfc822;user@some.org user@some.org
 imta/queue/tcp_local/ZZ01IS3D2ZP7FQ9UN54R.00        (3)
 <01IRUD7SVA3Q9UN2D4@sesta.com>
 TCP active open: Failed connect()    Error: no route to host (4)

 ...several hours worth of entries...

15-Jan-1998 12:45:39.48 tcp_local                Q 3 (5)
 adam@hosta.sesta.com rfc822;user@some.org user@some.org
 imta/queue/tcp_local/ZY01IS3D2ZP7FQ9UN54R.00        (6)
 <01IRUD7SVA3Q9UN2D4@sesta.com>
 TCP active open: Failed connect()    Error: no route to host

 ...several hours worth of entries...

15-Jan-1998 16:45:24.72 tcp_local                Q 3
 adam@hosta.sesta.com rfc822;user@some.org user@some.org
 imta/queue/tcp_local/ZX01IS67NY4RRK9UN7GP.00        (7)
 <01IRUD7SVA3Q9UN2D4@sesta.com>
 TCP active open: Failed connect() Error: connection refused (8)

 ...several hours worth of entries...

15-Jan-1998 20:45:51.55 tcp_local                D 3 (9)
 adam@hosta.sesta.com rfc822;user@some.org user@some.org
 imta/queue/tcp_local/ZX01IS67NY4RRK9UN7GP.00
 <01IRUD7SVA3Q9UN2D4@sesta.com>
 dns;host.some.org (TCP|206.184.139.12|2788|192.1.1.1|25)
 (All set, fire away)
 smtp; 250 Ok
```

1 メッセージが tcp_internal チャネルに入ります。これは、おそらく POP クライアントまたは MAP クライアント、あるいは SMTP リレーとして MTA を使った組織内の別のホストからきたものです。MTA は、そのメッセージを出力用の tcp_local チャネルのキューに入れます。

2 一回目の配信試行に失敗しています (Q エントリ)。

3 これが一回目の配信試行であることは ZZ* ファイル名からわかります。

4 この配信試行は、TCP/IP パッケージがリモート側へのルートを見つけられなかったために失敗しています。図 12-6 とは異なり、DNS は宛先ドメイン名 some.org の存在を否定していません。ホストへのルートがないことを示すエラーにより、送信側と受信側の間にネットワークに関連する問題があったことが示されています。

5 MTA の定期的なジョブ実行により配信の再試行が行われ、再び失敗しています。

6 ファイル名が ZY* となり、2 回目の試行であることを示しています。

7 ファイル名が ZX* となり、3 回目の試行であることを示しています。

8 定期的なジョブ実行により配信の再試行が行われ、再び失敗しています。ただし、ここでは、TCP/IP パッケージがリモートの SMTP サーバに接続できなかったことが示されているのではなく、リモートの SMTP サーバが接続を受け入れなかったことが示されています。（リモート側におけるネットワーク問題は解消されたが、SMTP サーバをまだ立ち上げていない、あるいはその SMTP サーバのメッセージ処理が追いつかないなどの理由で、MTA の接続試行が受け入れられなかったことが考えられます。）

9 メッセージがキューから取り出されました。

図 12-10 に、メッセージが変換チャネルを通過した場合の例を示します。このサイトには、以下のような CONVERSIONS マッピングテーブルがあるものとします。

```
CONVERSIONS

  IN-CHAN=tcp_local;OUT-CHAN=l;CONVERT  Yes
```

この例では、LOG_FILENAME=1 および LOG_MESSAGE_ID=1 オプションが設定されているものと仮定します。

図 12-10　　ログ : 変換チャネルを介して送られた受信 SMTP メッセージ

```
04-Feb-1998 00:06:26.72 tcp_local    conversion   E 9 (1)
 amy@siroe.edu rfc822;bert@sesta.com bert@sesta.com
 imta/queue/conversion/ZZ01IT5UAMZ4QW98518O.00
 <01IT5UALL14498518O@siroe.edu>

04-Feb-1998 00:06:29.06 conversion   l            E 9 (2)
 amy@siroe.edu rfc822;bert@sesta.com bert
 imta/queue/l/ZZ01IT5UAOXLDW98509E.00
 <01IT5STUMUFO984Z8L@siroe.edu>

04-Feb-1998 00:06:29.31 conversion                D 9 (3)
 amy@siroe.edu rfc822;bert@sesta.com bert
 imta/queue/conversion/ZZ01IT5UAMZ4QW98518O.00
 <01IT5UALL14498518O@siroe.edu>

04-Feb-1998 00:06:32.62 l                         D 9 (4)
 amy@siroe.edu rfc822;bert@siroe.com bert
 imta/queue/l/ZZ01IT5UAOXLDW98509E.00
 <01IT5STUMUFO984Z8L@siroe.edu>
```

1　外部ユーザ amy@siroe.edu からのメッセージが届きました。このメッセージは、チャネル l から受信者 bert@sesta.com に渡されるものです。しかし、CONVERSIONS マッピングエントリによって、このメッセージは、直接チャネル l に送られず、最初に変換チャネルのキューに入ります。

2　変換チャネルが実行され、メッセージがチャネル l のキューに入ります。

3　変換チャネルにより、メッセージがキューから取り出されています （古いメッセージファイルを削除）。

4　最後に、チャネル l のキューからメッセージが取り出されています （配信）。

図 12-11 は、接続に関するログ機能が有効 (LOG_CONNECTION=3) になっているときの送信メッセージのログ出力例を示しています。この例では、LOG_PROCESS=1、LOG_MESSAGE_ID=1、および LOG_FILENAME=1 オプションが設定されているものとします。この例は、ユーザ adam@sesta.com が 1 つのメッセージ （各メッセージコピーのメッセージ ID は同じであることに注意） を bobby@hosta.sesta.com、carl@hosta.sesta.com、および dave@hostb.sesta.com の 3 人の受信者宛に送信した場合を示しています。また、ここでは、メッセージが single_sys チャネルキーワードで示された tcp_local チャネルから送信されると仮定しています。したがって、(1)、(2)、(3) に示されているように、各ホスト名のそれぞれの受信者について、別のメッセージファイルがディスクに作成されます。bobby@hosta.sesta.com と carl@hosta.sesta.com の受信者は同じメッセージファイルに保存されますが、dave@hostb.sesta.com の受信者は別のメッセージファイルに保存されます。

図 12-11　　ログ : 送信接続ログ

```
19-Feb-1998 10:52:05.41 1e488.0 l            tcp_local    E 1
 adam@sesta.com rfc822;bobby@hosta.sesta.com bobby@hosta.sesta.com
 imta/queue/tcp_local/ZZ01ITRF7BO388000FCN.00  (1)
  <01ITRF7BDHS6000FCN@SESTA.COM>

19-Feb-1998 10:52:05.41 1e488.0 l            tcp_local    E 1
 adam@sesta.com rfc822;carl@hosta.sesta.com carl@hosta.sesta.com
 imta/queue/tcp_local/ZZ01ITRF7BO388000FCN.00  (2)
  <01ITRF7BDHS6000FCN@SESTA.COM>

19-Feb-1998 10:52:05.74 1e488.1 l            tcp_local    E 1
 adam@sesta.com rfc822;dave@hostb.sesta.com dave@hostb.sesta.com
 imta/queue/tcp_local/ZZ01ITRF7C11FU000FCN.00  (3)
  <01ITRF7BDHS6000FCN@SESTA.COM>

19-Feb-1998 10:52:10.79 1f625.2.0 tcp_local    -            O (4)
 TCP|206.184.139.12|5900|206.184.139.66|25
 SMTP/hostb.sesta.com/mailhub.sesta.com         (5)

19-Feb-1998 10:52:10.87 1f625.3.0 tcp_local    -            O (6)
 TCP|206.184.139.12|5901|206.184.139.70|25
 SMTP/hosta.sesta.com/hosta.sesta.com           (7)

19-Feb-1998 10:52:12.28 1f625.3.1 tcp_local                 D 1
 adam@sesta.com rfc822;bobby@hosta.sesta.com bobby@hosta.sesta.com
 imta/queue/tcp_local/ZZ01ITRF7BO388000FCN.00
  <01ITRF7BDHS6000FCN@SESTA.COM>
 hosta.sesta.com dns;hosta.sesta.com            (8)
 (TCP|206.184.139.12|5901|206.184.139.70|25)
 (hosta.sesta.com -- Server ESMTP [iMS V5.0 #8790])
 (TCP|206.184.139.12|5901|206.184.139.70|25)
 smtp;250 2.1.5 bobby@hosta.sesta.com and options OK.

19-Feb-1998 10:52:12.28 1f625.3.1 tcp_local                  D 1
 adam@sesta.com rfc822;carl@hosta.sesta.com carl@hosta.sesta.com
 imta/queue/tcp_local/ZZ01ITRF7BO388000FCN.00
  <01ITRF7BDHS6000FCN@SESTA.COM>
 hosta.sesta.com dns;hosta.sesta.com
 (TCP|206.184.139.12|5901|206.184.139.70|25)
 (hosta.sesta.com -- Server ESMTP [iMS V5.0 #8790])
 (TCP|206.184.139.12|5901|206.184.139.70|25)
 smtp;250 2.1.5 carl@hosta.sesta.com and options OK.

19-Feb-1998 10:52:12.40 1f625.3.2 tcp_local     -            C (9)
 TCP|206.184.139.12|5901|206.184.139.70|25
 SMTP/hosta.sesta.com/hosta.sesta.com

19-Feb-1998 10:52:13.01 1f625.2.1 tcp_local                  D 1
 adam@sesta.com rfc822;dave@hostb.sesta.com dave@hostb.sesta.com
 imta/queue/tcp_local/ZZ01ITRF7C11FU000FCN.00
  <01ITRF7BDHS6000FCN@SESTA.COM>
 mailhub.sesta.com dns;mailhub.sesta.com
 (TCP|206.184.139.12|5900|206.184.139.66|25)
 (MAILHUB.SESTA.COM -- Server ESMTP [iMS V5.0 #8694])
 (TCP|206.184.139.12|5900|206.184.139.66|25)
```

```
 smtp;250 2.1.5 dave@hostb.sesta.com and options OK.

19-Feb-1998 10:52:13.05 1f625.2.2 tcp_local     -            C (10)
 TCP|206.184.139.12|5900|206.184.139.66|25
 SMTP/hostb.sesta.com/mailhub.sesta.com
```

1 1 人目の受信者へのメッセージがキューに入れられます。

2 続いて、2 人目の受信者へのメッセージがキューに入れられます。

3 最後に 3 人目の受信者へのメッセージがキューに入れられます。

4 LOG_CONNECTION=3 が設定されているため、MTA によってこのエントリが書き込まれています。マイナス記号「-」は、このエントリが送信接続であることを示しています。「O」は、このエントリが接続開始に対応したものであることを示しています。接続開始の処理はスレッド 2 とスレッド 3 によって実行されていますが、これらの接続に対するマルチスレッド TCP/IP チャネルには同一のプロセスが使用されているため、プロセス ID「1f625」が同一であることに注意してください。

5 2 つの異なるリモートシステムに接続するために、マルチスレッド SMTP クライアントがそれぞれの接続を開いています。最初はこのエントリで、2 つ目は (7) に示されています。このエントリには、送信側と受信側の IP 番号とポート番号、および最初のホスト名と DNS 検索で見つかったホスト名の両方が表示されます。SMTP/ *最初のホスト* /*dns- ホスト* の部分には、最初のホスト名と DNS MX レコード検索を実行した後のホスト名が表示されています。mailhub.sesta.com は、hostb.sesta.com の MX サーバであることがわかります。

6 マルチスレッド SMTP クライアントが、別のスレッドで 2 つ目のシステムとの接続を開いています （プロセスは同じ）。

7 2 つの異なるリモートシステムに接続するために、マルチスレッド SMTP クライアントがそれぞれの接続を開きます。2 つ目がこのエントリで、最初の接続は上記の 5 に示されています。このエントリには、送信側と受信側の IP 番号とポート番号、および最初のホスト名と DNS 検索で見つかったホスト名の両方が表示されています。この例では、hosta.sesta.com というシステムがメールを直接受信することがわかります。

8 この例に示されているように、特定の接続エントリのほか、LOG_CONNECTION=3 によって接続に関連する情報が標準のメッセージエントリに含まれます。

9 このエントリは、LOG_CONNECTION=3 の設定によって書き込まれます。キューからメッセージ （上記の例では bobby と carl のメッセージ）が取り出され、接続が終了しています。C は接続の終了を表しています。

10 このエントリは、LOG_CONNECTION=3 の設定によって書き込まれます。キューからメッセージ（上記の例では dave のメッセージ）が取り出され、接続が終了しています。C は接続の終了を表しています。

図 12-12 は、接続に関するログが有効 (LOG_CONNECTION=3) になっているときの受信 SMTP メッセージのログ出力例を示しています。

図 12-12 ログ : 受信接続ログ

```
19-Feb-1998 17:02:08.70 tcp_local    +            O    (1)
 TCP|206.184.139.12|25|192.160.253.66|1244 SMTP         (2)

19-Feb-1998 17:02:26.65 tcp_local    l            E 1
 service@siroe.com rfc822;adam@sesta.com adam
 THOR.SIROE.COM (THOR.SIROE.COM [192.160.253.66]) (3)

19-Feb-1998 17:02:27.05 tcp_local    +            C    (4)
 TCP|206.184.139.12|25|192.160.253.66|1244 SMTP

19-Feb-1998 17:02:31.73 l                         D 1
 service@siroe.com rfc822;adam@sesta.com adam
```

1 リモートシステムが接続を開きます。「O」は、このエントリが接続開始に対応したものであることを示しています。また、「+」は、このエントリが受信接続であることを示しています。

2 IP 番号とポートが示されています。このエントリから、受信システム （ログファイルエントリを記録しているシステム）の IP アドレスは 206.184.139.12 で、接続ポートは 25 であることが分かります。また、送信システムの IP アドレスは 192.160.253.66 で、ポートは 1244 です。

3 このエントリは、受信 TCP/IP チャネル （tcp_local）からチャネル l の受信者へ送られるメッセージがキューに入ったことを示しています。LOG_CONNECTION=3 が有効になっているため、デフォルト以外の情報も含まれています。特に、送信システムが HELO/EHLO 行に示す名前、接続 IP 番号に関する DNS 逆検索で見つかった送信システムの名前、および送信システムの IP アドレスなどがすべて記録されています。このアクションに影響するチャネルキーワードの詳細については、第 8 章 「チャネル定義を設定する」を参照してください。

4 受信接続が閉じました。「C」は、このエントリが接続終了に対応したものであることを示しています。また、「+」は、このエントリが受信接続であることを示しています。

付録 A

SNMP サポート

iPlanet Messaging Server では、SNMP (Simple Network Management Protocol) を利用したシステムモニタ機能がサポートされています。Sun Net Manager や HP OpenView (本製品には含まれていません) などの SNMP クライアント (*ネットワークマネージャ*とも呼ばれる) を使用すると、iPlanet Messaging Server の特定の部分をモニタできます。

この章では、Messaging Server に対する SNMP サポートを有効にする方法について説明します。また、SNMP から得られる情報の種類についても簡単に説明します。ただし、この章では、それらの情報を表示する方法については取り上げていません。SNMP クライアントを使って SNMP ベースの情報を表示する方法については、SNMP クライアントのマニュアルを参照してください。このマニュアルには、Messaging Server の SNMP 実装で使用できるデータの一部も紹介されています。MIB の詳細については、RFC 2788 および RFC 2789 を参照してください。

この章には、以下の項目があります。

- SNMP の実装
- Solaris 8 で iPlanet Messaging Server 用の SNMP サポートを設定する
- SNMP クライアントからモニタする
- UNIX 上での他の iPlanet 製品との共存
- Messaging Server からの SNMP 情報

SNMP の実装

iPlanet Messaging Server には、Network Services Monitoring MIB (RFC 2788) と Mail Monitoring MIB (RFC 2789) という 2 つの標準化された MIB が実装されています。Network Services Monitoring MIB は POP、IMAP、HTTP、SMTP などのサーバのネットワークサービスをモニタし、Mail Monitoring MIB は MTA をモニタします。Mail Monitoring MIB では、各 MTA チャネルのアクティブ状態と、その履歴をモニタできます。アクティブ状態のモニタでは、現在キューにあるメッセージと開かれているネットワーク接続の情報が収集されます。たとえば、キューにあるメッセージの数や、開かれているネットワーク接続のソース IP アドレスなどです。一方、履歴のモニタからは、累積による統計情報が得られます。たとえば、処理したメッセージの合計数や、受信接続の合計数などです。

注	Messaging Server SNMP モニタ機能の詳細については、RFC 2788 および RFC 2789 を参照してください。

SNMP は Solaris 8 プラットフォームでのみサポートされています。今後のリリースでは、このほかのプラットフォームでもサポートされる予定です。Solaris の SNMP サポートには、ネイティブ Solaris SNMP テクノロジーである Solstice Enterprise Agents (SEA) が利用されています。SEA を Solaris 8 システムにインストールする必要はありません。Solaris 8 には、SEA に必要な実行時ライブラリがあらかじめ含まれています。

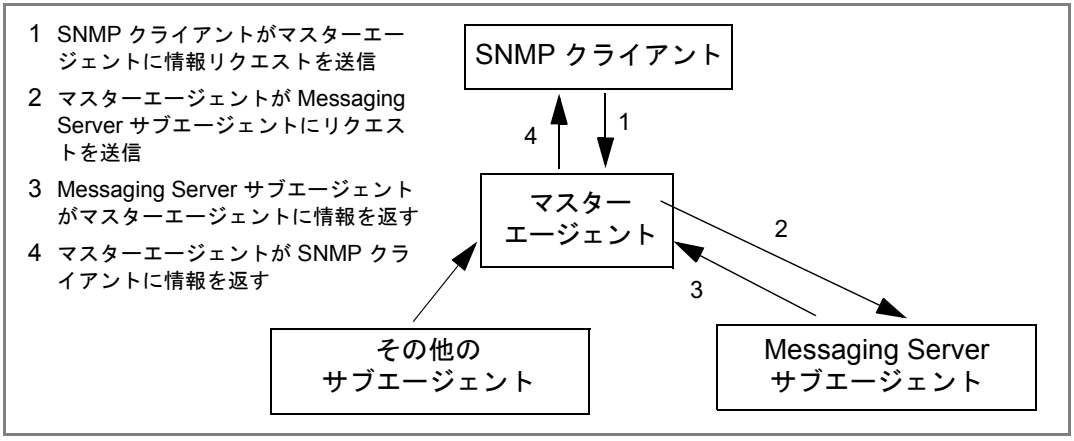
Messaging Server SNMP サポートには、次のような制限があります。

- SNMP を介してモニタできる Messaging Server のインスタンスは、ホストコンピュータ当たり 1 つのみである。
- サポートされている機能は、SNMP モニタ機能のみである。SNMP 管理機能はサポートされていない。
- SNMP トラップは実装されていない (RFC 2788 に、トラップを使用せずに同様の機能を実装する方法が記述されています)。

Messaging Server での SNMP の動作

Solaris プラットフォームでは、Messaging Server SNMP プロセスは SNMP サブエージェントであり、起動時にプラットフォームのネイティブ SNMP マスターエージェントに自動的に登録されます。クライアントからの SNMP リクエストは、マスターエージェントに送られます。マスターエージェントは、Messaging Server 宛てのすべてのリクエストを Messaging Server サブエージェントプロセスに転送します。最後に Messaging Server サブエージェントプロセスがリクエストを処理して、マスターエージェントを介してクライアントに応答を返します。図 A-1 に、このプロセスを示します。

図 A-1　　SNMP の情報フロー



Solaris 8 で iPlanet Messaging Server 用の SNMP サポートを設定する

SNMP モニタ機能によって発生するオーバーヘッドは非常に小さなものですが、Messaging Server は SNMP サポートを無効にした状態で出荷されています。SNMP サポートを有効にするには、次のコマンドを実行します。

```
# su user-id-for-ims
# configutil -o local.snmp.enable -v 1
# start-msg snmp
```

SNMP を有効にすると、パラメータを指定せずに `start-msg` コマンドを実行するだけで、SNMP サブエージェントプロセスがその他の Messaging Server プロセスとともに自動的に起動するようになります。

Messaging Server SNMP サブエージェントが機能するには、Solaris のネイティブ SNMP マスターエージェントが稼動している必要があります。Solaris のネイティブ SNMP マスターエージェントは snmpdx デーモンであり、通常これは Solaris の起動プロセスの一部として起動されます。

リクエストを受信する UDP ポートは、SNMP サブエージェントによって自動的に選択されます。必要であれば、次のコマンドを使ってサブエージェントに固定の UDP ポートを割り当てることもできます。

```
# configutil -o local.snmp.port -v ポート番号
```

この設定は、後でポート番号にゼロを指定することで取り消すことができます。ゼロ (デフォルト設定) を指定すると、Messaging Server は、使用可能な任意の UDP ポートを自動的にサブエージェントに選択させます。

/etc/snmp/conf ディレクトリには、2 つの SNMP サブエージェント設定ファイルがあります。1 つは SNMP アクセスコントロール情報を含む ims.acl で、もう 1 つは SNMP MIB OID 登録情報を含む ims.reg です。

通常は、この 2 つのファイルを編集する必要はありません。Messaging Server によって提供される MIB は読み取り専用なので、ims.reg ファイルにポート番号を指定する必要はありません。このファイルにポート番号を指定した場合は、configutil ユーティリティでポート番号を設定した場合を除き、その番号が使用されます。configutil でポート番号を設定した場合は、そのポート番号がサブエージェントで使用されます。ファイルを編集した場合は、変更を反映させるために SNMP サブエージェントをいったん停止してから再起動する必要があります。

```
# stop-msg snmp
# start-msg snmp
```

SNMP クライアントからモニタする

RFC 2788 および RFC 2789 のベース OID は次のとおりです。

mib-2.27 = 1.3.6.1.2.1.27

mib-2.28 = 1.3.6.1.2.1.28

SNMP クライアントに上記の OID をポイントして、SNMP コミュニティに「パブリック」としてアクセスします。

使用中の SNMP クライアントに MIB のコピーを読み込みたい場合は、<*server-root*>/plugins/snmp ディレクトリにある ASCII 形式の MIB を利用できます。ファイル名は rfc2788.mib と rfc2789.mib です。これらの MIB を SNMP クライアントソフトウェアに読み込む方法については、SNMP クライアントソフトウェアのマニュアルを参照してください。これらの MIB で使用される SnmpAdminString データのタイプは、古いバージョンの SNMP クライアントでは認識されないことがあります。その場合には、同じディレクトリにある rfc2248.mib と rfc2249.mib を使用してください。

UNIX 上での他の iPlanet 製品との共存

Messaging Server を実行している UNIX プラットフォーム上で、SNMP をサポートしている他の Netscape 製品または iPlanet 製品を使用する場合は、そのプラットフォームのネイティブマスターエージェントを無効にする必要があります。これらの iPlanet 製品を Messaging Server と同じホストで実行し、両者を SNMP でモニタする場合は、『Managing Servers with Netscape Console』の第 7 章 (`http://docs.iplanet.com/docs/manuals/console/42/html/7_snmp.htm#1024620`) の説明に従って iPlanet Proxy SNMP Agent を設定します。これにより、Messaging Server SNMP サブエージェント (ネイティブ SNMP エージェント) が他の iPlanet 製品のネイティブでない iPlanet SNMP サブエージェントと共存できるようになります。

Messaging Server からの SNMP 情報

この節では、SNMP を介して提供される Messaging Server 情報について簡単に説明します。詳細については、RFC 2788 および RFC 2789 で個々の MIB テーブルを参照してください。RFC および MIB の用語では、メッセージングサービス (MTA、HTTP など) が「*アプリケーション* (`appl`)」、Messaging Server ネットワーク接続が「*アソシエーション* (`assoc`)」、MTA チャネルが「*MTA グループ* (`mtaGroups`)」と呼ばれていることに注意してください。

Messaging Server の複数のインスタンスを同時にモニタできるプラットフォームでは、`applTable` には複数の MTA とサーバのセットが存在し、その他のテーブルには複数の MTA が存在する場合があります。

注　MIB でレポートされる累積値 (配信済みメッセージの合計数や、IMAP 接続の合計数など) は、再起動時、ゼロにリセットされます。

SNMP 情報によって、サイト固有のしきい値と監視の有効数値が得られます。優れた SNMP クライアントであれば、それらの値の傾向を分析し、過去の傾向から急にそれた場合に警告を出すことができます。

applTable

applTable には、サーバ情報があります。これは 1 次元のテーブルであり、MTA の行が 1 つと、WebMail HTTP、IMAP、POP、SMTP、SMTP Submit が有効である場合は、これらに対応する行がそれぞれ 1 つずつ含まれています。このテーブルには、バージョン情報、稼動時間、現在の動作のステータス (up、down、congested)、現在の接続数、接続の累積合計数、およびその他の関連するデータがあります。

以下に、applTable (mib-2.27.1.1) のデータ例を示します。

```
applTable:

    applName.1[1] = mailsrv-1[2] MTA on mailsrv-1.west.sesta.com
    applVersion.1 = 5.1
    applUptime.1 = 7322[3]
    applOperStatus.1 = up[4]
    applLastChange.1 = 7422[3]
    applInboundAssociations.1 = 5
    applOutboundAssociations.1 = 2
    applAccumulatedInboundAssociations.1 = 873
    applAccumulatedOutboundAssociations.1 = 234
    applLastInboundActivity.1 = 1054822[3]
    applLastOutboundActivity.1 = 1054222[3]
    applRejectedInboundAssociations.1 = 0[5]
    applFailedOutboundAssociations.1 = 17
    applDescription.1 = iPlanet Messaging Server 5.1
    applName.2[1] = mailsrv-1 HTTP WebMail server on mailsrv-1.west.sesta.com
    ...
    applName.3 = mailsrv-1 IMAP server on mailsrv-1.west.sesta.com
    ...
    applName.4 = mailsrv-1 POP server on mailsrv-1.west.sesta.com
    ...
    applName.5 = mailsrv-1 SMTP server on mailsrv-1.west.sesta.com
    ...
    applName.6 = mailsrv-1 SMTP Submit server on mailsrv-1.west.sesta.com
    ...
```

注 :

1. 上の例の .1、.2 などの接尾辞は行番号 (applIndex) です。applIndex の値は、MTA に対しては値 1、HTTP サーバに対しては値 2 というように決められています。したがって、上の例で言うと、テーブルの最初の行は MTA のデータを、接尾辞を持つ 2 つ目の行 は HTTP サーバのデータを示しています。
2. 監視している Messaging Server インスタンスの名前です。上の例の場合、インスタンス名は「mailsrv-1」です。
3. これらは SNMP TimeStamp 値で、イベント発生時の sysUpTime の値です。一方 sysUpTime は、SNMP マスターエージェントが起動してから経過した時間で、100 分の 1 秒を単位とする値です。

4 HTTP、IMAP、POP、SMTP、および SMTP 送信サーバの動作ステータスを判別するために Messaging Server は、各サーバに設定された TCP ポートを介して実際にこれらのサーバに接続し、適切なプロトコル (たとえば、HTTP では HEAD リクエストと応答、SMTP では HELO コマンドと応答など) を使用して簡単な処理を行います。これによって、各サーバのステータス (up (1)、down (2)、または congested (4)) が決定されます。

この接続処理は、サーバに対する通常の受信接続として認識され、各サーバの applAccumulatedInboundAssociations MIB 変数に影響を与えます。

MTA の場合、動作ステータスはジョブコントローラのステータスとなります。MTA が稼動中 (up) として表示された場合は、ジョブコントローラが稼動していることを意味します。また、MTA が停止中 (down) として表示された場合は、ジョブコントローラが停止していることを意味します。この MTA の動作ステータスは、MTA のサービスディスパッチャのステータスには左右されません。MTA の動作ステータスは、up または down の値だけをとります。ジョブコントローラに「congested (混雑)」という概念がありますが、MTA のステータスにこの状態が表示されることはありません。

5 HTTP、IMAP、および POP サーバの場合、applRejectedInboundAssociations MIB 変数は、拒否された受信接続の数ではなく、失敗したログイン試行の回数を示します。

applTable の使用法

各サーバを監視するときには、リストされているアプリケーションのそれぞれについてサーバステータス (applOperStatus) を監視することが重要です。

applLastInboundActivity に示されている最後の受信アクティビティから長い時間が経過している場合は、何らかの問題が発生して接続が切断されている可能性があります。applOperStatus=2 (down) の場合は、監視中のサービスが稼動していません。applOperStatus=1 (up) の場合は、他に問題があることが考えられます。

assocTable

このテーブルには、MTA に対するネットワーク接続情報が表示されます。これは 2 次元のテーブルで、アクティブな各ネットワーク接続に関する情報があります。他のサーバに関する接続情報は提供されません。

以下に、applTable (mib-2.27.2.1) のデータ例を示します。

```
assocTable:

    assocRemoteApplication.1.1[1] = 129.146.198.167[2]
    assocApplicationProtocol.1.1[1] = applTCPProtoID.25[3]
    assocApplicationType.1.1 = peerinitiator(3)[4]
    assocDuration.1.1 = 400[5]
...
```

注 :

1 *.x.y* という形式の接尾辞のうち、*x* の部分はアプリケーションインデックス (applIndex) であり、applTable のどのアプリケーションがレポートされているのかを示しています。この場合は MTA です。*y* の部分は、レポートされているアプリケーションの各接続を調べる際に使用されます。

2 リモート SMTP クライアントのソース IP アドレスです。

3 ネットワーク接続で使用されているプロトコルを示す OID です。aplTCPProtoID は TCP プロトコルを意味します。*.n* は使用中の TCP ポートを表す接尾辞で、.25 は TCP ポート 25 で使用されているプロトコルである SMTP を示しています。

4 リモート SMTP クライアントがユーザエージェント (UA) であるか、またはその他の MTA であるかを判別することはできません。このため、サブエージェントは常に peer-initiator をレポートします。ua-initiator がレポートされることはありません。

5 これは SNMP TimeInterval で、単位は 100 分の 1 秒です。上の例では、接続を開始してから 4 秒が経過しています。

assocTable の使用法

このテーブルは、現在発生している問題を診断するために使用されます。たとえば、急に 200,000 個の受信接続が発生した場合には、このテーブルで接続元を確認できます。

mtaTable

これは 1 次元のテーブルで、applTable の各 MTA に対してそれぞれ 1 つの行があります。各行には、mtaGroupTable で選択した変数に対して、その MTA 内のすべてのチャネル (グループと呼ばれる) の合計が示されます。

以下に、applTable (mib-2,28.1.1) のデータ例を示します。

```
mtaTable:

    mtaReceivedMessages.1[1] = 172778
    mtaStoredMessages.1 = 19
    mtaTransmittedMessages.1 = 172815
    mtaReceivedVolume.1 = 3817744
    mtaStoredVolume.1 = 34
    mtaTransmittedVolume.1 = 3791155
    mtaReceivedRecipients.1 = 190055
    mtaStoredRecipients.1 = 21
    mtaTransmittedRecipients.1 = 3791134
    mtaSuccessfulConvertedMessages.1 = 0[2]
    mtaFailedConvertedMessages.1 = 0
    mtaLoopsDetected.1 = 0[3]
```

注 :

1 *.x* という形式の接尾辞は、アプリケーションに対応する applTable 内の行の番号を示します。上の例の .1 は、このデータが applTable 内にある最初のアプリケーションのものであることを意味しています。つまり、このデータは MTA に関するものです。

2 変換チャネルは、ゼロ以外の値しかとりません。

3 現在 MTA のメッセージキューに保管されている .HELD メッセージファイルの数です。

mtaTable の使用法

mtaLoopsDetected がゼロでない場合は、メールのループ問題があります。問題を解決するためには、MTA キューの .HELD ファイルを見つけて診断してください。

システムが変換チャネルを使ってウィルススキャンを行い、ウィルスに感染したメッセージを拒否した場合は、mtaSuccessfulConvertedMessages に、変換失敗の数と、感染したメッセージの数が記録されます。

mtaGroupTable

この 2 次元のテーブルには、applTable 内の各 MTA に対するチャネル情報があります。この情報には、保存された (キュー内にある) メッセージ数や、配信されたメールメッセージ数などのデータが含まれています。各チャネルに対して保存されたメッセージの数 (mtaGroupStoredMessages) を監視することは、とても重要です。この値が通常の範囲を超えて大きくなった場合は、メールがキュー内にたまっています。

以下に、mtaGroupTable (mib-2.28.2.1) のデータ例を示します。

```
mtaGroupTable:

mtaGroupName.1.1[1] = autoreply[2]
    ...
mtaGroupName.1.2[1] = ims-ms
    ...
mtaGroupName.1.3[1] = tcp_local
    mtaGroupDescription.1.3 = mailsrv-1 MTA tcp_local channel
    mtaGroupReceivedMessages.1.3 = 12154
    mtaGroupRejectedMessages.1.3 = 0
    mtaGroupStoredMessages.1.3 = 2
    mtaGroupTransmittedMessages.1.3 = 12148
    mtaGroupReceivedVolume.1.3 = 622135
    mtaGroupStoredVolume.1.3 = 7
    mtaGroupTransmittedVolume.1.3 = 619853
    mtaGroupReceivedRecipients.1.3 = 33087
    mtaGroupStoredRecipients.1.3 = 2
    mtaGroupTransmittedRecipients.1.3 = 32817
    mtaGroupOldestMessageStored.1.3 = 1103
    mtaGroupInboundAssociations.1.3 = 5
    mtaGroupOutboundAssociations.1.3 = 2
    mtaGroupAccumulatedInboundAssociations.1.3 = 150262
    mtaGroupAccumulatedOutboundAssociations.1.3 = 10970
    mtaGroupLastInboundActivity.1.3 = 1054822
    mtaGroupLastOutboundActivity.1.3 = 1054222
```

```
mtaGroupRejectedInboundAssociations.1.3 = 0
mtaGroupFailedOutboundAssociations.1.3 = 0
mtaGroupInboundRejectionReason.1.3 =
mtaGroupOutboundConnectFailureReason.1.3 =
mtaGroupScheduledRetry.1.3 = 0
mtaGroupMailProtocol.1.3 = applTCPProtoID.25
mtaGroupSuccessfulConvertedMessages.1.3 = 0[3]
mtaGroupFailedConvertedMessages.1.3 = 0
mtaGroupCreationTime.1.3 = 0
mtaGroupHierarchy.1.3 = 0
mtaGroupOldestMessageId.1.3 = <01IFBV8AT8HYB4T6UA@red.iplanet.com>
mtaGroupLoopsDetected.1.3 = 0[4]
mtaGroupLastOutboundAssociationAttempt.1.3 = 1054222
```

注 :

1 *.x.y* という形式の接尾辞のうち、*x* の部分はアプリケーションインデックス (applIndex) であり、applTable のどのアプリケーションがレポートされているのかを示しています。この場合は MTA です。*y* の部分は、レポートされているアプリケーションの各接続を調べる際に使用されます。この列挙型のインデックス (mtaGroupIndex) は、mtaGroupAssociationTable テーブルと mtaGroupErrorTable テーブルでも使われています。

2 レポート対象のチャネルの名前で、この場合は autoreply チャネルです。

3 変換チャネルは、ゼロ以外の値しかとりません。

4 現在チャネルのメッセージキューに保管されている .HELD メッセージファイルの数です。

mtaGroupTable の使用法

Rejected と *Failed* の傾向分析を行うと、チャネルの潜在的な問題を発見できる場合があります。

mtaGroupStoredVolume と mtaGroupStoredMessages の比が突然変化した場合は、キューに大きなジャンクメールがある可能性があります。

mtaGroupStoredMessages が急激に変化した合は、大量の迷惑メールが送信されているか、何らかの理由で配信に失敗している可能性があります。

mtaGroupOldestMessageStored の値が、配信不能メッセージの通知時間 (notices チャネルキーワード) に使用されている値よりも大きい場合は、差出人に戻すという処理でも対処できないメッセージがある可能性があります。差出人に戻す処理は毎晩夜間に行われるため、テストには mtaGroupOldestMessageStored > (最大時間 + 24 時間) を使用してください。

mtaGroupLoopsDetected がゼロよりも大きい場合は、メールループが発生しています。

mtaGroupAssociationTable

これは 3 次元のテーブルで、各エントリは assocTable に対するインデックスを表しています。このテーブルには、applTable 内の各 MTA に対して、2 次元のサブテーブルが 1 つずつ用意されています。この 2 次元のサブテーブルには、対応する MTA の各チャネルに対して 1 つの行があります。また、各チャネルに対し、そのチャネルが現在使用しているアクティブなネットワーク接続ごとにエントリが 1 つずつあります。エントリの値は assocTable へのインデックスです (エントリの値と、参照されている MTA の applIndex によってインデックスが付けられています)。この assocTable 内のエントリは、そのチャネルが保持しているネットワーク接続です。

簡単に言うと、mtaGroupAssociationTable テーブルは assocTable に示されているネットワーク接続を、mtaGroupTable の対応するチャネルに関連付けているものです。

以下に、mtaGroupAssociationTable (mib-2.28.3.1) のデータ例を示します。

```
mtaGroupAssociationTable:

    mtaGroupAssociationIndex.1.3.1[1] = 1[2]
    mtaGroupAssociationIndex.1.3.2 = 2
    mtaGroupAssociationIndex.1.3.3 = 3
    mtaGroupAssociationIndex.1.3.4 = 4
    mtaGroupAssociationIndex.1.3.5 = 5
    mtaGroupAssociationIndex.1.3.6 = 6
    mtaGroupAssociationIndex.1.3.7 = 7
```

注 :

1 *.x.y.z* という形式の接尾辞のうち、*x* の部分はアプリケーションインデックス (applIndex) であり、applTable 内のどのアプリケーションがレポートされているかを示します。この場合は MTA です。*y* の部分は mtaGroupTable 内のどのチャネルがレポートされているかどうかを示します。上の例で、3 は tcp_local チャネルを表しています。*z* の部分は、チャネルに対して開かれている、またはチャネルから開かれているアソシエーションを調べる際に使用されます。

2 この値は assocTable へのインデックスです。特に、接尾辞の *x* の部分とこの値は、それぞれ applIndex の値と、assocTable への assocIndex インデックスになります。言い換えると、applIndex を無視した場合、assocTable の最初の行は tcp_local チャネルによって制御されているネットワーク接続を表していることになります。

mtaGroupErrorTable

これも 3 次元のテーブルで、メッセージの配信中に各 MTA の各チャネルで発生した一時的および永続的なエラーの数を示します。インデックス値が 4000000 のエントリは一時的なエラー、5000000 のエントリは永続的なエラーです。一時的なエラーの場合は、メッセージが再度キューに入れられ、後で再び配信が試みられます。永続的なエラーの場合は、メッセージが拒否されるか、配信不能として戻されます。

以下に、`mtaGroupErrorTable` (mib-2.28.5.1) のデータ例を示します。

```
mtaGroupErrorTable:

    mtaGroupInboundErrorCount.1.1.4000000[1] = 0
    mtaGroupInboundErrorCount.1.1.5000000 = 0
    mtaGroupInternalErrorCount.1.1.4000000 = 0
    mtaGroupInternalErrorCount.1.1.5000000 = 0
    mtaGroupOutboundErrorCount.1.1.4000000 = 0
    mtaGroupOutboundErrorCount.1.1.5000000 = 0

    mtaGroupInboundErrorCount.1.2.4000000[1] = 0
    ...

    mtaGroupInboundErrorCount.1.3.4000000[1] = 0
    ...
```

注 :

1 *.x.y.z* という形式の接尾辞のうち、*x* の部分はアプリケーションインデックス (`applIndex`) であり、`applTable` 内のどのアプリケーションがレポートされているかを示します。この場合は MTA です。*y* の部分は `mtaGroupTable` 内のどのチャネルがレポートされているかを示します。上の例では、1 は autoreply チャネルを、2 は ims-ms チャネルを、3 は tcp_local チャネルを指定しています。*z* の部分は 4000000 または 5000000 の値をとり、そのチャネルのメッセージ配信中に発生した一時的エラーと永続的なエラーの数を示します。

mtaGroupErrorTable の使用法

エラー数が急激に増加した場合は、配信に問題が発生している可能性があります。たとえば、tcp_ channel の値が急激に増加した場合は、DNS またはネットワークの問題が考えられます。ims_ms チャネルの値が急激に増加した場合は、メッセージストアへの配信の問題が考えられます。たとえば、パーティションに空き容量がない、または `stored` に問題があるなどです。

用語集

/var/mail 新しいメールメッセージが単一のフラットテキストファイルとして逐次保存される、Berkeley スタイルの Inbox を指すときによく使用される名前。

A レコード ホスト名とその関連 IP アドレスを含む一種の DNS レコード。レコードは、インターネットのメッセージングサーバで電子メールをルーティングするために使用されます。参照 : **Domain Name System（DNS）**、**MX レコード**

admin 管理者または管理を指す用語。

ALLOW フィルタ 次のサービスへのアクセスを許可されているクライアントを識別するための Messaging Server のアクセス制御規則 : POP、IMAP、または HTTP。比較 : **DENY フィルタ**

APOP Authenticated Post Office Protocol の略。POP（Post Office Protocol）に似ていますが、認証には、プレーンテキストによるパスワードではなく、暗号化したパスワードとチャレンジ文字列を一緒に使用します。

AUTH SMTP クライアントが、サーバの認証メソッドを指定し、認証プロトコル交換を処理し、必要に応じて後続のプロトコル相互対話のセキュリティ層を交渉するための SMTP コマンド。

Berkeley DB 読み取り / 書き込み処理の同時実行が多く、およびトランザクション / 修復可能性が要求されるアプリケーションのための、トランザクション用データベースストア。iPlanet Messaging Server は、数々の目的で Berkeley データベースを使用します。

CA 認証局。デジタル証明書（デジタルの識別子）を発行したり、公開鍵を作成して対象ユーザがそれを利用できるようにする機関です。

cipher 暗号化で使用されるアルゴリズム。

ciphertext（暗号文） 暗号化されたテキスト。対語 : **cleartext（平文）**

cleartext（平文） 暗号化されていないテキスト。

CLI コマンドラインインターフェース。

cn 共通の名前を表す LDAP エイリアス。

CNAME レコード ドメイン名エイリアスをドメイン名にマップする DNS レコードの一種。

config Configuration (設定) の略。

Configuration Directory Server (構成ディレクトリサーバ)
: 1 つまたは複数のサーバの構成情報を管理している Directory Server。

configutil
: Directory Server またはローカルの設定ファイル `configdb` に格納されているさまざまな設定パラメータを変更するためのコマンドラインユーティリティ。

cookie
: 特定の Web サイトに接続するとき、ブラウザのメモリに自動的に入力されるテキストのみの文字列。cookie は、Web ページの作成者によってプログラムされます。ユーザは cookie を承諾または拒否できます。cookie を承諾すると、より高速に Web ページがロードされます。ユーザのマシンのセキュリティを脅かすものではありません。

counterutil
: カウンタオブジェクト内のすべてのカウンタを表示するためのコマンドラインユーティリティ。

CRAM-MD5
: RFC 2195 に記載されている軽量の標準トラック認証方法。ネットワーク上でユーザのログインパスワードを保護する必要がある場合に、TLS (SSL) の代替として素早く利用できます (やや強度が落ちます)。

cronjob
: UNIX 専用。設定時に cron デーモンによって自動的に実行されるタスク。参照 : **crontab ファイル**

crontab ファイル
: UNIX 専用。指定時に実行されるコマンドのリスト。1 行にコマンドが 1 つずつ記述されています。

DC ツリー
: ドメインコンポーネント（Domain Compornent）ツリー。DNS ネットワーク構造をミラーしているディレクトリ情報ツリー。DC ツリー内の識別名の例 : `cn=billbob`、`dc=bridge`、`dc=net`、`o=internet`

Delegated Administrator Console
: ドメイン管理者が、ホストドメインのユーザやグループを変更または追加するために使用する Web ブラウザベースのソフトウェアコンソール。エンドユーザが、各自のパスワードの変更、メッセージ転送規則の設定、Vacation 規則の設定、配信リスト / 購読リストの作成に使用することもできます。

Delegated Administrator for Messaging
: ドメイン管理者が、ホストドメインのユーザやグループを変更または追加するために使用するインタフェース（GUI および CLI）。

deliver
: POP、IMAP、または HTTP メールクライアントからアクセスできるメッセージストアにメールを直接配信するためのコマンドラインユーティリティ。

DENY フィルタ
: 次のサービスへのアクセスを拒否されているクライアントを識別するための、Messaging Server アクセス制御規則 : POP、IMAP、または HTTP。比較 : **ALLOW フィルタ**

DIGEST-MD5
: CRAM-MD5 より安全な軽量の標準トラック認証方法。TLS (SSL) の設定オーバーヘッドなしで接続全体を保護するためのオプションとともに、RFC 2831 に記述されています。

Directory Server
: LDAP ベースの iPlanet ディレクトリサービス。参照 : **ディレクトリサービス**、**Lightweight Directory Access Protocol (LDAP)**、**Configuration Directory Server (構成ディレクトリサーバ)**、**ユーザ / グループ Directory Server**

DIT
: **「ディレクトリ情報ツリー」**を参照。

DN 「**識別名**」を参照。

dn 識別名の LDAP エイリアス。参照：**識別名**

DNS 「**Domain Name System（DNS）**」を参照。

DNS エイリアス DNS サーバが、別のホスト（DNS CNAME レコード）へのポインティングとして認識するホスト名。マシンの本当の名前は 1 つだけですが、1 つまたは複数のエイリアスを割り当てることができます。たとえば、`www.siroe.domain` は、実際には現在サーバが存在しているマシン `realthing.siroe.domain` をポインティングするエイリアスであることも考えられます。

DNS スプーフィング DNS サーバが不正情報を提供するネットワークアタックの一種。

DNS データベース ドメイン名（ホスト名）および対応する IP アドレスのデータベース。

Domain Name System（DNS） コンピュータが、ネットワークまたはインターネット上の他のコンピュータを探し出せるようにするための分散型名前解決ソフトウェア。システムは、標準の IP アドレスとホスト名（例：`www.siroe.com`）を関連付けます。通常、マシンはこの情報を DNS サーバから取得します。DNS サーバは、ホスト名をインターネットアドレスに変換するために、レプリケートによる分散型のデータクエリサービスを提供します。参照：**A レコード**、**MX レコード**、**CNAME レコード**

DSN 「**配信ステータス通知**」を参照。

dsservd ディレクトリ情報を格納しているデータベースファイルにアクセスし、LDAP プロトコルを使用してディレクトリクライアントと直接通信するデーモン。

dssetup 既存の Directory Server を iPlanet Messaging Server 対応にするための Directory Server 準備ツール。

EHLO コマンド サーバが拡張 SMTP コマンドをサポートするかどうかをサーバに照会するための SMTP コマンド。RFC 1869 で定義されています。

ESMTP 「**Extended Simple Mail Transfer Protocol（ESMTP）**」を参照。

ESP Enterprise Service Provider の略。

ETRN サーバーでクライアントマシンを待機しているメッセージのメールキュー処理が開始されるように要求する SMTP コマンド。RFC 1985 で定義されています。

EXPN メーリングリストを展開する SMTP コマンド。RFC 821 で定義されています。

Extended Simple Mail Transfer Protocol（ESMTP） インターネットメッセージトランスポートプロトコル。ESMTP は、SMTP コマンドセットにオプションのコマンドを追加し、リモートサイトでどのコマンドが実行されたのかを ESMTP サーバが検出できるようにするなどの機能を補足します。

FQDN 「**完全なドメイン名（FQDN）**」を参照。

GUI グラフィカルユーザインターフェース。

HA 「**High Availability**」を参照。

hashdir　特定ユーザに対するメッセージストアがどのディレクトリに含まれているかを判断するためのコマンドラインユーティリティ。

High Availability　サービスの中断を検出し、システム障害やプロセス失敗の場合には復旧メカニズムを提供することが可能。または故障の処理を可能にすること。さらに、プライマリシステム障害の場合には、バックアップシステムを稼動してサービスを継続することもできます。

HTTP　「**HyperText Transfer Protocol**」を参照。

HyperText Transfer Protocol　Web 上でハイパーテキストドキュメントの転送を可能にするための標準プロトコル。iPlanet Messaging Server は、Web ベースの電子メールをサポートするために HTTP サービスを提供しています。参照 : **Messenger Express**

iDA　iPlanet Delegated Administrator for Messaging。

IDENT　「**Identification Protocol**」を参照。

Identification Protocol　特定の TCP 接続におけるリモート端末を制御しているリモートプロセスを識別するための手段を提供するプロトコル。RFC 1413 で定義されています。

IMAP4　「**Internet Message Access Protocol Version 4 (IMAP4)**」を参照。

imsadmin　ドメイン管理者、ユーザ、およびグループを管理するためのコマンドラインユーティリティセット。

imsasm　ユーザメールボックスの保存や回復を処理するためのユーティリティ。`imsasm` ユーティリティは、`imsbackup` および `imsrestore` ユーティリティを呼び出し、データストリームを作成および解釈します。

imsbackup　メッセージストアをバックアップするためのコマンドラインユーティリティ。

imscripter　IMAP サーバと交信するためのコマンドラインユーティリティ。このユーティリティは、IMAP フォルダで 1 つのコマンドを実行したり、複数のコマンドを一括して実行するときに使用できます。

imsimta コマンド　MTA（Message Transfer Agent）の各種のメンテナンス、テスト、管理タスクを行うためのコマンドラインユーティリティセット。

imsrestore　メッセージストアをリストアするためのコマンドラインユーティリティ。

INBOX　メール配信用のユーザのデフォルトメールボックスの予約。INBOX は、大文字と小文字が区別されない唯一のフォルダ名です。たとえば、INBOX、Inbox、および inbox は、いずれもユーザのデフォルトメールボックス名として有効です。

Internet Message Access Protocol Version 4 (IMAP4)　ユーザがメインのメッセージシステムから切断されてもメールを処理することができるようにする標準プロトコル。IMAP 仕様により、切断されたユーザの管理制御が可能になるとともに、それらのユーザがメッセージシステムに再接続したときに、ユーザのメッセージストアの同期化が可能になります。

Internet Protocol (IP)　インターネットとイントラネットのベースとなる基本的なネットワーク層プロトコル。

IP　「**Internet Protocol (IP)**」を参照。

iPlanet Setup すべての iPlanet サーバおよび iPlanet Console に使われるインストールプログラム。

IP アドレス インターネットまたはインターネットにおけるマシンの実際の場所を特定する番号。198.93.93.10 などのように、ドット(ピリオド)によって区切られています。TCP/IP を利用するホストには、32 ビットアドレスが割り当てられます。

ISP インターネットサービスプロバイダ。電子メール、電子カレンダー、WWW アクセス、Web ホスティングなどのインターネットサービスを顧客に提供する会社。

LDAP 「**Lightweight Directory Access Protocol (LDAP)**」を参照。

LDAP 検索文字列 ディレクトリの検索に使用される属性を定義するための、代替可能なパラメータ文字列。たとえば、LDAP 検索文字列 "uid=%s" は、ユーザ ID 属性に基づく検索を意味します。

LDAP サーバ LDAP ディレクトリを管理し、そのディレクトリクエリサービスを提供するソフトウェアサーバ。iPlanet Directory Services は LDAP サーバの実装です。

LDAP サーバフェイルオーバー LDAP サーバのバックアップ機能。LDAP サーバの 1 つに故障が発生した場合に、システムは別の LDAP サーバに切り替えることができます。

LDAP 参照 別の LDAP エントリへのシンボリック リンク（参照）から成る LDAP エントリ。LDAP 参照は、LDAP ホストと識別名で構成されています。LDAP 参照は、データを複製せずに、既存の LDAP データを参照するのに使用されます。また、移動された特定のエントリに依存するプログラムの互換性を維持するためにも使用されます。

LDAP データ交換方式 (LDIF) Directory Server エントリをテキスト形式で表すために使用されるフォーマット。

LDAP フィルタ 特定の属性または属性値に基づいて、一連のエントリを指定する方法。

LDBM LDAP Data Base Manager の略。

LDIF 「**LDAP データ交換方式 (LDIF)**」を参照。

Legato Networker Legato から配布されているサードパーティバックアップユーティリティ。

Lightweight Directory Access Protocol (LDAP) TCP/IP を介して複数のプラットフォーム上で実行するように設計されたディレクトリサービスプロトコル。X.500 Directory Access Protocol (DAP) を簡素化したもので、ユーザプロファイル、配信リスト、iPlanet サーバ上の設定データなどの情報の格納、検索、および配布の管理に単一のポイントを提供します。iPlanet Directory Server は、LDAP プロトコルを使用します。

mboxutil メールフォルダを管理するためのコマンドラインユーティリティ。このユーティリティを使うと、メールボックス（フォルダ）をリスト、作成、削除、名前変更、または移動できます。また、制限容量情報を報告するためにも使用できます。

MD5 RSA Data Security によるメッセージダイジェストアルゴリズム。MD5 は、高確率で固有なものとなる短いダイジェストデータを生成するときに使用できます。数学的には、同一のメッセージダイジェスト電子メールを作成するデータを生成することは非常に困難です。

Message Handling System (MHS)
接続されている MTA、それらのユーザエージェント、およびメッセージストアのグループ。

Message Transfer Agent (MTA)
メッセージのルーティングおよび配信専用のプログラム。MTA は相互に機能してメッセージを転送し、目的の受信者に配信します。MTA は、メッセージをローカルのメッセージストアに配信するのか、またはリモート配信として別の MTA にルーティングするのかを決定します。

Messaging Multiplexor
複数のメールサーバの単一接続ポイントとして機能し、複数のメールボックスホストを利用する膨大な数のユーザへの配信を容易にする特別な iPlanet Messaging Server。

Messaging Server 管理者
iPlanet Messaging Server のインストールおよび管理を行う権限を持つ管理者。

Messenger Express
ユーザが、ブラウザ ベース（HTTP）のインターフェースを使ってメールボックスにアクセスできるようにするメールクライアント。メッセージ、フォルダ、およびその他のメールボックス情報を、HTML 形式でブラウザウィンドウに表示できます。参照：**Web メール**

MHS
「**Message Handling System (MHS)**」を参照。

MIME
「**Multipurpose Internet Mail Extension (MIME)**」を参照。

mkbackupdir
メッセージストア内の情報にあわせてバックアップディレクトリを作成、同期化するためのユーティリティ。Legato Networker と併用します。

MMP
「**Messaging Multiplexor**」を参照。

MoveUser
ユーザのメールフォルダ内にあるメッセージを Messaging Server 間で移動するためのコマンドラインユーティリティ。

MTA
「**Message Transfer Agent (MTA)**」を参照。

MTA 設定ファイル
Messaging Server のすべてのチャネル定義、およびルーティング用にアドレスを書き換えるための書き換え規則を含むファイル（`imta.cnf`）。参照：**チャネル**、**書き換え規則**

MTA ディレクトリ キャッシュ
MTA がメッセージを処理する際に必要とする、ユーザおよびグループに関するディレクトリサービス情報のスナップショット。参照：**ディレクトリ同期**

MTA ホップ
MTA 間でメッセージをルーティングする処理。

MUA
「**ユーザエージェント（UA）**」を参照。

Multiplexor
「**Messaging Multiplexor**」を参照。

Multipurpose Internet Mail Extension (MIME)
メッセージ内にマルチメディアファイルを追加するために使用されるプロトコル。

MX レコード
メール交換レコード（Mail Exchange Record）。あるホスト名から別のホスト名にマップする DNS レコードの一種。

NDN
「**未配信通知**」を参照。

next-hop リスト　メールルーティングがメッセージの転送先を判断するときに使用する隣接システムのリスト。next-hop リストに記述されているシステムの順序が、メールルーティングがメッセージを転送するときの順序となります。

NIS　ネットワーク上のシステムおよびユーザに関する主要情報を含む分散ネットワーク情報サービス。NIS データベースは、マスターサーバおよびすべての複製（スレーブ）サーバ上に保存されます。

NIS+　ネットワーク上のシステムとユーザの階層的な情報を含む分散ネットワーク情報サービス。NIS+ データベースは、マスターサーバおよびすべての複製サーバ上に保存されます。

NMS　Netscape Messaging Server の略。

NOTARY メッセージ　RFC 1892 の NOTARY 仕様に準拠する未配信通知（NDN）および配信ステータス通知（DSN）。

OSI ツリー　Open Systems Interconnect ネットワーク構文を反映するディレクトリ情報ツリー。OSI ツリーにおける識別名の例：`cn=billt,o=bridge,c=us`

POP3　「**Post Office Protocol Version 3 (POP3)**」を参照。

postmaster アカウント　システムが生成する Messaging Server のメッセージを受信する、電子メールグループおよび電子メールアドレスのエイリアス。postmaster アカウントは、1 つまたは複数の有効なメールボックスをポイントしていなければなりません。

Post Office Protocol Version 3 (POP3)　標準の配信メソッドを提供するプロトコルで、メッセージ転送エージェントは、ユーザのメール フォルダへのアクセス権を持っている必要はありません。そのため、メールクライアントとメッセージ転送エージェントが別のコンピュータに置かれるようなネットワーク環境で、その有用性を発揮します。

RC2　RSA Data Security による可変鍵サイズブロック暗号。

RC4　RSA Data Security によるストリーム暗号。RC2 よりも高速に処理されます。

RDN　相対的な識別名 (Relative Distinguished Name)。実際のエントリの名前で、これにエントリの祖先の名前を付加すると完全な識別名になります。

readership　共有メールフォルダに関する読み取りユーザ情報を収集するためのコマンドラインユーティリティ。

reconstruct　メールフォルダを修復するためのコマンドラインユーティリティ。

RFC　Request For Comments の略。インターネットで使用するプロトコルやそれに関連する実験を記述したもの（1969 年に開始）。インターネット標準はすべて RFC として公開されていますが、それは RFC の全体量に比べると僅かなものです。`http://www.imc.org/rfcs.html` を参照。

SASL　「**Simple Authentication and Security Layer (SASL)**」を参照。

SCM　「**Service Control Manager**」を参照。

Secure Sockets Layer (SSL)　2 点間（クライアントとサーバ）の安全な接続を確立するソフトウェアライブラリ。

sendmail — UNIX マシンで使用される一般的な MTA。ほとんどのアプリケーションでは、iPlanet Messaging Server を sendmail に代わるものとして使用できます。

Server Side Rules (SSR) — サーバ側のメールフィルタリングに関する規則セット。Sieve メールフィルタリング言語に基づいています。

Service Control Manager — サービスを管理する Windows NT 管理プログラム。

Sieve — メールフィルタリング言語。

Simple Authentication and Security Layer (SASL) — POP、IMAP、または SMTP クライアントがサーバに対して識別されるようにするためのメカニズムを制御する手段。iPlanet Messaging Server は、RFC 2554 (ESMTP AUTH) に準拠する SMTP SASL の使用をサポートします。SASL は、RFC 2222 で定義されています。

Simple Mail Transfer Protocol (SMTP) — インターネットで最も一般的に使用されており、iPlanet Messaging Server でもサポートされている電子メールプロトコル。RFC 821 で定義されています。RFC 822 には関連するメッセージフォーマットの記述があります。

SIMS — Sun Internet Mail Server の略。

SIZE — クライアントが特定のメッセージのサイズをサーバに宣言できるようにする SMTP 拡張。サーバは宣言されたメッセージサイズに基づいて、メッセージの受信を承諾するかどうかをクライアントに示すことができます。サーバは、承諾可能な最大メッセージサイズをクライアントに宣言できます。RFC 1870 で定義されています。

SMTP — 「**Simple Mail Transfer Protocol (SMTP)**」を参照。

SMTP AUTH — 「**AUTH**」を参照。

sn — surname を表すディレクトリ属性エイリアス。

SSL — 「**Secure Sockets Layer**」を参照。

SSR — 「**Server Side Rules**」を参照。

stored — メッセージストアに毎日のメンテナンスタスクを実行するコマンドラインユーティリティ。このユーティリティを使って、ディスク上に保存されたメッセージを永久に消去することもできます。

TCP — 「**Transmission Control Protocol (TCP)**」を参照。

TCP/IP — 「**Transmission Control Protocol/Internet Protocol (TCP/IP)**」を参照。

TLS — 「**Transport Layer Security (TLS)**」を参照。

Transmission Control Protocol (TCP) — 2 台のホスト間において、信頼性が高く、接続指向のストリームサービスを提供するインターネットプロトコルの 1 つ。基本的なトランスポートプロトコルです。

Transmission Control Protocol/Internet Protocol (TCP/IP)
: インターネットプロトコルとして使用される一連のネットワークプロトコルに付けられた名前。2 つの主要なネットワークプロトコルを表しています。TCP (Transmission Control Protocol) はトランスポート層のプロトコル、IP (Internet Protocol) はネットワーク層のプロトコルです。

Transport Layer Security (TLS)
: SSL を標準化したもの。参照 : **Secure Sockets Layer (SSL)**

UA
: **「ユーザエージェント（UA）」**を参照。

UBE
: **「Unsolicited Bulk Email (UBE)」**を参照。

UID
: (1) ユーザ識別子。システムでユーザを識別するための固有文字列。「ユーザ ID」とも呼ばれます。(2) ユーザ ID（ログイン名）のディレクトリ属性エイリアス。

Unsolicited Bulk Email (UBE)
: 通常、商業目的のためにダイレクトメール配信業者などから送信される不特定多数の電子メール。

UUCP
: UNIX to UNIX Copy Program の略。UNIX システム間で通信に使用されるプロトコル。

Veritas Cluster Server
: iPlanet Messaging Server と組み合わせて使用できる Veritas Software の High Availability クラスタリングソフトウェア。

VRFY
: ユーザ名を確認するための SMTP コマンド。RFC 821 で定義されています。

Web メール
: ブラウザベースの電子メールサービスを指す一般的な用語。ブラウザベースのクライアント。サーバ上でより多くのプロセスが処理されるため「thin」クライアントとも呼ばれます。常にサーバ上に保存されているメールにアクセスします。参照 : **Messenger Express**

X.400
: メッセージ処理システムの標準。

アカウント
: 特定のユーザやユーザグループを定義する情報。ユーザ名やグループ名、有効な電子メールアドレス（1 つまたは複数のアドレス）、および電子メールの配信方法 / 場所などに関する情報が含まれます。

アクセス制御
: サーバ、あるいはサーバ上のフォルダやファイルへのアクセスを制御するためのメソッド。

アクセス制御規則
: 特定のディレクトリエントリまたは属性に対するユーザアクセス権を指定する規則。

アクセス制御情報
: ACI (Access Control Information)。アクセス制御リスト内の一項目。

アクセス制御リスト
: ACL（Access Control List）。ユーザやグループのディレクトリアクセス許可を定義するデータのセット。

アクセスドメイン
: 指定されたドメイン内における特定の Messaging Server の操作に関するアクセスを制限します。たとえば、アクセスドメインは、アカウントのメールが収集される場所を制限するときに使用できます。

アドレス 電子メールメッセージの配信先と配信方法を示す情報。アドレスは、メッセージヘッダおよびメッセージエンベロープの両方に示されています。エンベロープアドレスはメッセージのルーティングと配信方法を示しますが、ヘッダアドレスは単に表示目的で使われます。

アドレス処理 アドレスのエラーを検出し、必要に応じてアドレスを書き直し、受信者アドレスと照合する MTA の操作。

アドレストークン 書き換え規則パターンのアドレス要素。

アドレスプロトコル 電子メールの利用を可能にするアドレス規則。RFC 822 は、インターネットで最も幅広く使用されているプロトコルで、iPlanet Messaging Server でサポートされています。その他のプロトコルには、X.400、UUCP（UNIX to UNIX Copy Protocol）などがあります。

暗号化 符号キーを所有する特定の受信者以外の人には解読できないように情報を変装させるプロセス。

安全なファイル システム システムがクラッシュした際に、クラッシュ発生以前の状態にデータをロールバックし、すべてのデータをリストアすることができるファイルシステム。セーフファイルシステムの一例として、Veritas File System の VxFS などが挙げられます。

委託管理サーバ ホストドメインによってディレクトリのアクセス制御を処理するデーモンプログラム。

一時的なエラー メッセージ処理中に発生するエラーの状態。リモート MTA は、配信時にメッセージを処理できませんが、後で処理できます。ローカル MTA は、メッセージをキューに戻し、後に送信するようにスケジュールします。

インスタンス 別々に実行可能なサーバの設定、または特定のホスト上にあるその他のソフトウェアエンティティ（構成要素）。インストールされたバイナリファイルの 1 セットから個別に実行およびアクセスできる、iPlanet サーバの複数のインスタンスを作成できます。

インスタンスディレクトリ サーバの特定インスタンスを定義するファイルを含むディレクトリ。Messaging Server の場合は、サーバルートのサブディレクトリです (*serverRoot*/msg-*インスタンス名*/)。この場合の、*インスタンス名* はインストール時に指定された名前です。比較：**インストールディレクトリ**、**サーバルート**

インストールディレクトリ サーバのバイナリ（実行可能）ファイルがインストールされるディレクトリ。Messaging Server の場合は、サーバルートのサブディレクトリです (*ServerRoot*/bin/msg/)。比較：**インスタンスディレクトリ**、**サーバルート**

インターネット TCP/IP プロトコルを使用する世界規模のネットワーク。

インターネットプロトコル アドレス **「IP アドレス」**を参照。

イントラネット 企業や組織内における TCP/IP ネットワークのネットワーク。イントラネットでは、World Wide Web で使われているのと同種のサーバやクライアントソフトウェアを、企業 LAN 上で企業の社内アプリケーションとして使用できます。インターネットを介するイントラネットでは、通常、機密情報はファイアウォールによって保護されます。参照：**ファイアウォール**、**エクストラネット**

永続的なエラー メッセージ処理時に発生するエラー状態。このエラーが発生すると、メッセージストアはその電子メールメッセージを削除します。MTA はそのメッセージを送信者に戻し、そのメッセージのコピーを削除します。

エイリアス 電子メールアドレスの別名。

エイリアスの参照解除 バインドまたは検索処理において、ディレクトリ サービスがエイリアス識別名をエントリの実際の識別名に翻訳するように指定すること。

エイリアスファイル ディレクトリ内以外の場所にエイリアスを設定するために使用されるファイル (Postmaster エイリアスなど)。

エクストラネット 企業イントラネットで、顧客や供給業者がアクセスできる部分。参照 : **イントラネット**

エクスパンション（展開） 配信リストの MTA 処理に使用される用語。1 つのメッセージアドレスを配信リスト内の各メンバーに変換する操作のことです。

エクスパンダ メッセージを受信者リストに配信できるようにする電子メール配信システムの一部分。メールエクスパンダは、メーリングリストを実装するために使用されます。ユーザが単一のアドレス（例 : `hacks@somehost.edu`）にメッセージを送信すると、エクスパンダによって、リスト内に指定されている各メールボックスへの配信が処理されます。「メールエクスプローダ」とも呼ばれます。参照 : **EXPN**

エラーハンドラ エラーを処理するプログラム。Messaging Server では、エラーメッセージを発行し、postmaster によって書かれたエラーアクションフォームを処理します。

エラーハンドラアクションフォーム Messaging Server が処理できない受信メッセージといっしょに postmaster アカウントに送信されるフォーム。postmaster は、メッセージ処理方法をフォームに記入し、サーバに指示します。

エラーメッセージ エラーやその他の状況を報告するメッセージ。iPlanet Messaging Server は、処理できない電子メールを受信したときなど、数々の状況においてメッセージを生成します。通知エラーと呼ばれるその他のメッセージは、情報伝達を目的とするものです。

エンベロープ 電子メールメッセージの送信者と受信者に関する転送情報を含むコンテナ。この情報はメッセージヘッダの一部分ではありません。エンベロープは、メッセージが別の場所へ移動するときに、さまざまな電子メールプログラムによって使用されます。ユーザが見るのは、メッセージのヘッダと本文だけです。

エンベロープフィールド メッセージエンベロープ中の `RCPT TO` などの既定情報項目。

オブジェクトクラス エントリが記述するオブジェクトの種類、およびそのオブジェクトに含まれる属性を指定するテンプレート。たとえば、iPlanet Directory Server で、`commonname`、`mail` (電子メールアドレス)、`mailHost`、`mailQuota` などの属性を持つ `emailPerson` というオブジェクトクラスを指定することが可能です。

オフライン状態 メールクライアントがサーバシステムからクライアントシステムにメッセージをダウンロードし、メッセージを表示したり、返信することができる状態。サーバ上のメッセージは、削除される場合と削除されない場合があります。

オンライン状態 メッセージをサーバ上に残したまま、メールクライアントによってリモートから返信する状態。

下位参照 ディレクトリサーバのネーミングコンテクストの子を指すネーミングコンテクスト。参照：**知識情報**

書き換え規則 「ドメイン書き換え規則」とも呼ばれます。MTA が配信メッセージを正しいホストにルーティングするために使用するツール。書き換え規則には、以下の機能があります。(1) 受信メッセージのアドレスからホスト / ドメイン仕様を抽出する。(2) ホスト / ドメイン仕様を書き換え規則のパターンと照合する。(3) ドメインテンプレートに基づいてホスト / ドメイン仕様を書き換える。(4) メッセージを配置すべきチャネルキューを決定する。

仮想ドメイン (1) ISP ホストドメイン。参照：**ホストドメイン**。(2) Messaging Multiplexor によってクライアントのユーザ ID に追加されたドメイン名。LDAP 検索やメールボックスサーバへのログインを可能にします。

完全なドメイン名（FQDN） インターネットホストを識別するための固有の名前。参照：**ドメイン名**

管理権限 ユーザの管理に関する役割を定義する権限のセット。

管理コンソール 参照：**コンソール**

管理サーバ管理者 Directory Server に接続されていないときでもサーバの起動と停止を実行するための管理権限を持つユーザ。管理サーバ管理者は、ローカルサーバグループ内のすべてのサーバに対する制限されたサーバタスク（通常はサーバの再起動とサーバの停止のみ）を実行できます。管理サーバがインストールされているときには、この管理者エントリはローカルで自動的に作成されます（この管理者はユーザディレクトリのユーザではありません）。

管理者 管理権限として定義された権利セットを持つユーザ。参照：**設定管理者**、**ディレクトリマネージャ**、**管理サーバ管理者**、**サーバ管理者**、**メッセージストア管理者**、**トップレベル管理者**、**ドメイン管理者**、**組織管理者**、**ファミリグループ管理者**、**メーリングリストの所有者**

管理対象オブジェクト ディレクトリサービスに関する一連の属性のように、設定可能な属性の集合体。

企業ネットワーク 地理的に分散している場所を相互に接続する数々のネットワークで構成されるネットワーク。企業ネットワークは、広範囲に分散された会社のニーズを満たすことができ、会社のミッションクリティカルな用途にも利用されています。

キーデータベース サーバ証明書用のキーの組み合せデータを含むファイル。「キーファイル」とも呼ばれます。

機能 (capability) クライアントに与えられる文字列で、特定の IMAP サービスで利用できる機能を定義するもの。

機能 (facility) Messaging Server ログファイルエントリにおいて、ログエントリを生成したソフトウェアサブシステム（Network や Account など）のこと。

キュー **「メッセージキュー」**を参照。

共有フォルダ 複数の人が読むことのできるフォルダ。共有フォルダの所有者は、誰にフォルダの読み取りアクセスを許可するのか、または誰が共有フォルダからメッセージを削除できるのかなどを指定できます。また、共有フォルダには、受信メッセージの編集、ブロック、転送を行うことができるモデレータもいます。共有できるのは、IMAP フォルダだけです。比較：**個人フォルダ**

クライアント サーバにサービスまたは情報を要求するソフトウェアエンティティ。

クライアント/サーバモデル ネットワークに接続されたコンピュータが他のクライアントコンピュータに特定のサービスを提供するコンピューティングモデル。例：DNS の ネームサーバ / ネームリゾルバプログラム、NFS やディスクレスホストなどの file-server/file-client の関係など。

グリーティングフォーム アカウントが新たに作成されたときに、ユーザに送信するメッセージ。このフォームは、新規アカウントの確認とその内容の検証としての役割を果します。

グループ 1 つの識別名でまとめられた LDAP メールエントリのグループ。通常、これは配信リストとして使用されますが、グループのメンバーに特定の管理特権を与える場合にも使用されることがあります。参照：**ダイナミックグループ**、**スタティックグループ**

グループフォルダ 共有フォルダやグループフォルダを含むフォルダ。参照：**共有フォルダ**

ゲートウェイ あるネイティブ形式を別の形式に変換するシステムおよびそのアプリケーション。一例として、X.400 / RFC 822 間の電子メールゲートウェイなどが挙げられます。2 つ以上の電子メールシステム（特に、2 つのネットワーク上にある異種メールシステムなど）を接続して、メッセージを相互に転送するマシンもゲートウェイと呼ばれます。場合によってはマッピングや変換処理が複雑になるため、いったんシステムから完全にメッセージを受信してから、変換処理を行い、次のシステムに転送するという格納 / 転送方式が必要となります。

検索ベース 「**ベース DN**」を参照。

検索（ルックアップ） 検索（サーチ）と同じ機能で、特定のパラメータを使ってデータを並べ替えます。

公開鍵暗号方式 公開コンポーネントと非公開コンポーネントの 2 つの部分から成る鍵（コード）を使用する暗号方式。メッセージの暗号化には、受信者の公開鍵が使われます。メッセージの暗号を解読する受信者は、他人には公開されていない非公開の鍵を使用します。

個人フォルダ 所有者だけが読み取ることのできるフォルダ。参照：**共有フォルダ**

コメント文字 行の頭に配置することで、その行を実行不可能なコメント行に変える文字。

コンソール 数多い iPlanet コンポーネントの設定、監視、メンテナンス、トラブルシューティングを行うことができる GUI（グラフィカルユーザインターフェース）。

サーバインスタンス 特定のサーバを表すディレクトリ、プログラム、およびユーティリティ。

サーバ管理者 サーバ管理タスクを実行する人物。サーバ管理者は、タスク ACI に基づき、特定のサーバのタスクに対する制限付きアクセスを提供します。サーバへのアクセス権は設定管理者によって割り当てられなければなりません。サーバへのアクセス権を得たユーザは、他のユーザにサーバアクセス権を与えることができるサーバ管理者となります。

サーバルート 指定のホスト上にある Administration Server に関連付けられたすべての iPlanet サーバがインストールされているディレクトリ。通常、このディレクトリは *サーバ_ルート* に指定されます。比較 : **インストールディレクトリ , インスタンスディレクトリ**

サービス (1) サーバにより提供される機能。たとえば、iPlanet Messaging Server は、SMTP、POP、IMAP、および HTTP サービスを提供します。(2) ユーザインターフェースを持たない Windows NT のバックグラウンドプロセス。Windows NT プラットフォーム上での iPlanet サーバは、サービスとして実行されます。「デーモン」の同義語。

サービス拒否攻撃 ある個人が、故意的であるかどうかに関わらず、膨大な数のメッセージを送信してメールサーバを圧倒する状況。サーバのスループットにかなりの影響が出たり、過重負荷によってサーバ自体が機能しなくなることがあります。

サブドメイン ドメインの一部分。たとえば、ドメイン名 `corp.siroe.com` の場合、`corp` はドメイン `siroe.com` のサブドメインです。参照 : **ホスト名**、**完全なドメイン名 (FQDN)**

サブネット ホスト ID のブロックを識別する IP アドレスの一部分。

参照 Directory Server がクライアントに対し、アクセスすべき DSA (Directory Service Agent) に関する情報とともに情報要求を返すプロセス。参照 : **知識情報**

識別名 ディレクトリ情報ツリー内におけるエントリの固有の位置を指定する属性と値をカンマで区切ったシーケンス。「DN」と呼ばれる場合もあります。

自動返信オプションファイル Vacation 通知ファイルなどの自動返信オプションを設定するために使用するファイル。

自動返信ユーティリティ 自動返信機能が有効になっているアカウント宛に送信されたメッセージに対し、自動的にメッセージを返信するためのユーティリティ。iPlanet Messaging Server 内の各アカウントは、受信メッセージに自動返信するように設定できます。

上位参照 ディレクトリ情報ツリー（DIT）において、ディレクトリサーバのネーミングコンテクストの上にあるディレクトリサーバを示すネーミングコンテクスト。

証明書データベース サーバのデジタル証明書（1 つまたは複数の証明書）が含まれているファイル。「証明書ファイル」とも呼ばれます。

証明書に基づく認証 クライアントによって提出されたデジタル証明書によるユーザの認証。比較 : **パスワード認証**

証明書名 証明書とその所有者を識別するための名前。

ジョブコントローラ さまざまな MTA コンポーネントの要求によってタスクをスケジュールしたり実行したりする MTA コンポーネント。

シングルサインオン 一度認証されたユーザが複数のサービス（メール、ディレクトリ、ファイルサービスなど）へアクセスできる機能。

スキーマ iPlanet Directory Server 内にエントリとして格納できる情報タイプの定義（構造と構文）。スキーマに一致しない情報がディレクトリに格納されている場合は、ディレクトリにアクセスしようとするクライアントは適切な結果を表示できない可能性があります。

スタティックグループ それぞれのグループメンバーを列挙することによって静的に定義されるメールグループ。参照 : **ダイナミックグループ**

スプーフ クライアントが、不正なホスト名のサーバにアクセス、またはメッセージ送信しようとする一種のネットワークアタック。

スマートホスト 受信者を認識できない場合に別のメールサーバがメッセージをを転送する、ドメイン内の宛先メールサーバ。

スレッド プロセス内の軽量実行インスタンス。

スレーブチャネルプログラム リモートシステムで開始された転送を受け入れるチャネルプログラム。参照：**マスターチャネルプログラム**

正規表現 パターンマッチングの目的で、文字の範囲またはクラスを表す特殊文字を使った文字列。

セキュリティモジュールデータベース SSL 暗号用のハードウェアアクセラレータを記述する情報が含まれているファイル。「secmod」とも呼ばれます。

セッション クライアント / サーバ接続のインスタンス。

切断状態 メールクライアントが、サーバに接続し、選択したメッセージのキャッシュコピーを作成してから、サーバとの接続を切断すること。

設定管理者 iPlanet トポロジ全体におけるサーバ管理とディレクトリデータ設定の管理権限を持つ人物。設定管理者は、iPlanet トポロジ内のあらゆるリソースに自由にアクセスできます。サーバアクセスを他の管理者に割り当てることができる唯一の管理者です。設定管理者は、管理者グループやメンバーが確立されるまでの間、最初に管理設定を担当します。

設定ファイル iPlanet Messaging システムの特定コンポーネントに対する設定パラメータが含まれているファイル。

相対識別名 属性と値を列挙した識別名の表記 (シーケンス) の中の、最終的な属性とその値を指す。参照：**識別名**

組織管理者 Delegated Administrator for Messaging の GUI または CLI を使用して、組織またはサブ組織内のメールユーザおよびメールリストの作成、変更、および削除を行う管理権限を持つユーザ。

その他のアドレス アカウントの補助的なアドレス（通常プライマリアドレスのバリエーション）。単一のアカウントに複数のアドレスがあると便利な場合があります。

ダイナミックグループ LDAP 検索 URL によって定義されたメールグループ。通常、ユーザは、それらのディレクトリエントリ内に LDAP 属性を設定することによって、グループに加わります。

単一フィールド置換文字列 書き換え規則において、ホスト / ドメインアドレスの指定アドレストークンをダイアナミックに書き換えるドメインテンプレートの一部分。参照：**ドメインテンプレート**

知識情報 ディレクトリサービスインフラストラクチャ情報の一部分。ディレクトリサーバは、別のサーバに情報要求を渡すときに知識情報を使用します。

チャネル メッセージを処理する基本的な MTA コンポーネント。チャネルは、別のコンピュータシステムまたはシステムグループとの接続を表すものです。各チャネルは、1 つまたは複数のチャネルプログラムとメッセージ（そのチャネルに関連する 1 つまたは複数のシステムに送信されるメッセージ）を格納する送信メッセージキューから構成されています。参照：**チャネルブロック**、**チャネルホストテーブル**、**チャネルプログラム**

チャネルプログラム 以下の機能を実行するチャネルの一部分：(1) リモートシステムにメッセージを送信し、送信後にそのメッセージをキューから削除する。(2) リモートシステムからメッセージを受信し、適切なチャネルキューに配置する。参照：**マスターチャネルプログラム**、**スレーブチャネルプログラム**

チャネルブロック 単一のチャネル定義。参照：**チャネルホストテーブル**

チャネルホストテーブル 複数のチャネル定義を 1 つにまとめたもの。

通知メッセージ メッセージ配信処理のステータス、および配信問題や障害の理由などを知らせる一種のメッセージで、Messaging Server によって送信されます。これは、情報の提供を目的とするもので、postmaster による対処を要求するものではありません。参照：**配信ステータス通知**

ディスパッチャ 定義された TCP ポートへの接続要求を処理する MTA コンポーネント。ディスパッチャは、複数のマルチスレッドサーバが指定されたサービスにおける責任を共有することを許可する、マルチスレッド接続ディスパッチエージェントです。ディスパッチャを使用すると、複数のマルチスレッド SMTP サーバの同時実行が可能になります。

ディレクトリエントリ 識別名によって確認されるディレクトリ属性とその値のセット。各エントリには、エントリが記述するオブジェクトの種類を指定し、そのオブジェクトの属性のセットを定義する、オブジェクトクラス属性が含まれています。

ディレクトリ検索 ユーザやリソースの名前またはその他の特性に基づいて、特定のユーザまたはリソースに関する情報を見つけるためにディレクトリを検索するプロセス。

ディレクトリコンテクスト メッセージストアへアクセスするために、ユーザとパスワードの認証に使用するエントリの検索の検索を開始するディレクトリツリー情報内のポイント。参照：**ベース DN**

ディレクトリサービス 組織内の人材やリソースに関する情報を論理的に集めたリポジトリ。参照：**Lightweight Directory Access Protocol (LDAP)**

ディレクトリ情報ツリー ディレクトリエントリを組み立てる階層構造。「DIT」とも呼ばれます。DIT は、DNS（DC ツリー）または Open Systems Interconnect ネットワーク（OSI ツリー）に沿って組織構成できます。

ディレクトリスキーマ ディレクトリに保存できるデータを定義した一連の規則。

ディレクトリ同期 ディレクトリサービスに保存された現在のディレクトリ情報がある MTA ディレクトリキャッシュを更新（同期）するプロセス。参照：**MTA ディレクトリ キャッシュ**

ディレクトリマネージャ ディレクトリサーバデータベースの管理権限を持つユーザ。アクセス制御は、このユーザには適用されません。ディレクトリマネージャは「ディレクトリのスーパーユーザ」として捉えることもできます。

データストア ディレクトリ情報（通常は、ディレクトリ情報ツリー全体）を含むストア。

デフラグメンテーション 分割された大きなメッセージを再現できるようにする MIME（Multipurpose Internet Mail Extensions）機能。各分割データに表示される Message Partial Content-Type のヘッダフィールドには、それらの分割データを 1 つのメッセージとして再現するのを補助する情報が入っています。参照：**分割**

デーモン 端末から独立してバックグラウンドで動作し、必要に応じて機能を実行する UNIX プログラム。デーモンプログラムの一般的な例として、メールハンドラ、ライセンスサーバ、および印刷デーモンなどがあります。Windows NT マシンの場合、この種のプログラムはサービスと呼ばれます。参照：**サービス**

転送 **「メッセージ転送」**を参照。

同期 (1) マスターディレクトリサーバをレプリカ（複製）ディレクトリサーバのデータに合わせて更新すること。(2) MTA ディレクトリキャッシュの更新。

トップレベル管理者 Delegated Administrator for Messaging の GUI または CLI を使用して、Message Server namespace 全体のメールユーザ、メーリングリスト、ファミリアカウント、ドメインの作成、変更、および削除を行うための管理権限を持つユーザ。デフォルトでは、このユーザがトポロジ内のすべてのメッセージサーバに対するメッセージストア管理者となります。

ドメイン (1) ホスト名が共通のサフィックス（ドメイン名）を持つコンピュータのグループ。構文としては、ピリオド（ドット）で区切られた名前（ラベル）のシーケンスが含まれるインターネットドメイン名です。例：corp.mktng.siroe.com。(2) 管理制御の範囲。

ドメインエイリアス 別のドメインを指すドメインエントリ。エイリアスを使用することによって、ホストドメインで複数のドメイン名を持つことができます。

ドメイン書き換え規則 **「書き換え規則」**を参照。

ドメイン管理者 Delegated Administrator for Messaging の GUI または CLI を使用して、ホストドメイン内のメールユーザ、メーリングリスト、およびファミリアカウントの作成、変更、および削除を行うための管理権限を有するユーザ。デフォルトでは、このユーザは、トポロジにおけるすべてのメッセージサーバのメッセージストア管理者として作業を行うことができます。

ドメイン制限容量 電子メールメッセージ用にドメインに割り当てられる容量で、システム管理者によって設定されます。

ドメイン組織 組織ツリー内でホストドメインの下にあるサブドメイン。ドメイン組織は、組織の部門別にユーザやグループのエントリを整理する場合に便利です。

ドメインテンプレート アドレスのホスト / ドメイン部分をどのように書き換えるのかを定義する書き換え規則の一部分。完全なスタティックホスト / ドメインアドレスまたは単一のフィールド置換文字列のいずれか、あるいはその両方を含むことができます。

ドメイン名 (1) 電子メールアドレスに使用されるホスト名。(2) 管理組織を定義する固有の名前。ドメインは他のドメインを含むことができます。ドメイン名は右から左の方向に解釈されます。たとえば、siroe.com は、Siroe Company のドメイン名であり、かつ、最上位である com ドメインのサブドメインです。また、ドメイン siroe.com をさらに別のドメインに分割し、corp.siroe.com などとすることもできます。参照：**ホスト名、完全なドメイン名（FQDN）**

ドメイン部分 電子メールアドレスで @ 記号の右側にある部分。たとえば、siroe.com は、電子メールアドレス dan@siroe.com のドメイン部分です。

ドメインホスティング 共有メッセージングサーバ上で 1 つまたは複数のドメインをホストする機能。たとえば、siroe.com および sesta.org というドメイン名がいずれも siroe.net というメールサーバ上でホストされていることも考えられます。ユーザは、ホストドメインにメールを送信し、そのホストドメインからメールを受信します。メールサーバの名前は、電子メールアドレスには表示されません。

トランスポートプロトコル MTA 間におけるメッセージ転送手段（SMTP、X.400 など）を提供します。

名前の変換 IP アドレスを対応する名前にマップするプロセス。参照 : **DNS**

認証 (1) iPlanet Messaging Server に対し、クライアントユーザであることを立証するプロセス。(2) クライアント、または別のサーバに対し、iPlanet Messaging Server であることを立証するプロセス。

認証局 **「CA」**を参照。

認証証明書 相手を検証・認証するためにサーバからクライアント、またはクライアントからサーバに送信されるデジタルファイル。証明書の所有者（クライアントまたはサーバ）は確実に認証されます。証明書を譲渡することはできません。

ネーミングコンテクスト DN によって識別されるディレクトリ情報ツリーの特定のサブツリー。iPlanet Directory Server では、特定の種類のディレクトリ情報がネーミングコンテクスト内に保存されます。たとえば、Siroe Corporation のボストンオフィスに勤務するマーケティング従業員に関するすべてのエントリを保存するネーミングコンテクストの場合は、次のようになります。ou=mktg, ou=Boston, o=Siroe, c=US

ネーミング属性 ディレクトリ情報ツリーの識別名における最終的な属性。参照 : **相対識別名**

ネームスペース LDAP ディレクトリのツリー構造。参照 : **ディレクトリ情報ツリー**

ネットワークマネージャ SNMP データの読み取り、フォーマット、および表示を行うプログラム。SNMP クライアントとも呼ばれます。

ノード DIT 内のドメインエントリ。

配信 **「メッセージの配信」**を参照。

配信ステータス通知 配信されたメッセージのステータス情報。たとえば、ネットワークが停止したために配信が遅延していることなどを示します。

配信リスト 電子メールのアドレスを 1 つ指定することによってメッセージを一度に送信できる電子メールアドレス（ユーザ）のリスト。「メーリングリスト」または「グループ」とも呼ばれます。参照 : **エクスパンション（展開）**、**メンバー**、**モデレータ**、**エイリアス**

配布リストの所有者 配信リストの責任者である個人。所有者は、配信リストのメンバーを追加したり削除することができます。参照 : **配信リスト**、**エクスパンション（展開）**、**メンバー**、**モデレータ**

バインド DN Directory Server への認証に使用される識別名。

パスワード認証 ユーザ名およびパスワードによるユーザの識別。比較 : **証明書に基づく認証**

パターン ALLOW フィルタや DENY フィルタなどのように、マッチングを目的として使用する文字列表現。

バックアップ フォルダの内容をメッセージストアからバックアップデバイスにバックアップするプロセス。参照：**リストア**

バックエンドサーバ 電子メールメッセージの保管と取り出しのみを行う電子メールサーバ。メッセージストアサーバとも呼ばれます。

バックボーン 分散システムの主要コネクティビティメカニズム。バックボーン上にある中間的なシステムへのコネクティビティを持ったシステムはすべて互いに接続されています。これによって、コスト、性能、またはセキュリティの理由でバックボーンを迂回するようなシステムをセットアップする際に、妨げられることはありません。

パーティション **「メッセージストア パーティション」**を参照。

バニティドメイン 特定のサーバやホストドメインではなく、個々のユーザに関連付けられたドメイン。バニティドメインは、`MailAlternateAddress` 属性を使って指定されます。バニティドメインにはドメイン名の LDAP エントリはありません。バニティドメインは、個人や小規模の組織が、独自のホストドメインを管理することなく、カスタマイズしたドメイン名を使いたい場合に便利です。「カスタムドメイン」とも呼ばれます。

ハブ システムの単一の接続ポイントとして機能するホスト。2 つのネットワークがファイアウォールによって分離されている場合は、ファイアウォールコンピュータをメールハブとして機能させることがよくあります。

ファイアウォール 組織内のネットワーク上にあるコンピュータと組織外のコンピュータの間にバリアを形成するネットワーク構成（通常は、ハードウェアとソフトウェアの両方を指す）。一般に、ファイアウォールは、物理的なビル内または組織内ネットワーク上の電子メール、ディスカッショングループ、データファイルなどの情報を保護するために使用されます。

ファミリグループ管理者 ファミリグループのファミリメンバーを追加したり削除する管理権限を持つユーザ。このユーザは、グループ内の別のメンバーにファミリグループ管理アクセスを許可できます。

フェールオーバー 冗長バックアップを提供するために、あるシステムから別のシステムにコンピュータサービスを自動転送すること。

フォルダ メッセージを収納する場所（固有の名前を付けることができる）。フォルダ内に別のフォルダを含めることもできます。「メールボックス」とも呼ばれます。参照：**個人フォルダ**、**共有フォルダ**、**INBOX**

輻輳しきい値 システム管理者が設定できるディスク容量の限界。システムリソースが不足しているときに新しい操作を制限することによって、データベースへの過重負荷を防ぐことができます。

プレーンテキスト データを送信するためのメソッド。その定義はコンテクストに依存します。たとえば、SSL の場合、プレーンテキストパスワードは暗号化されるため、平文（cleartext）として送信されることはありません。SASL の場合、プレーンテキストパスワードはハッシュされるため、パスワードのハッシュだけがテキストとして送信されます。参照：**SSL**、**SASL**

プレーンテキスト認証 **「パスワード認証」**を参照。

プロキシ プロトコルの要求に応答する際、1 つのシステムが別のシステムの「フロント」として機能するメカニズム。プロキシシステムは、モデムなどの単純なデバイスで完全なプロトコルスタックを実装しなくてもよいように、ネットワーク管理で使用されます。

プロトコル 2 台以上のシステムで情報を交換するために従わなければならない規則と、メッセージの交換に関する正式な説明。

プロビジョン iPlanet Directory Server 内でエントリを追加、修正、削除するプロセス。これらのエントリには、ユーザやグループ、およびドメイン情報が含まれます。

プロセス オペレーティングシステムにより作り出される自己充足的で完全機能的な実行環境。アプリケーションの各インスタンスは、通常、別々のプロセスとして実行されます。比較：**スレッド**

分割 大きなメッセージを小さく分割できるようにする MIME（Multipurpose Internet Mail Extensions）機能。参照：**デフラグメンテーション**

ベース DN 検索の対象となるディレクトリの識別名エントリ。「検索ベース」とも呼ばれます。例：`ou=people,o=siroe.com`

ヘッダ 電子メールメッセージにおいてメッセージの本文に先行する部分。ヘッダは、フィールド名、コロン、値の順に構成されています。ヘッダは、電子メールプログラムとユーザがメッセージの内容を理解するのに役立つ情報を含んでいます。たとえば、ヘッダには配信情報、内容のまとめ、トレース、MIME 情報などが含まれています。すなわち、ヘッダを見ると、メッセージの宛先、送信者、配信日、用件などがわかります。ヘッダは、電子メールプログラムで読み取ることができるように、RFC 822 に準じて書かれていなければなりません。

ヘッダフィールド `From:` や `To:` などのように、メッセージヘッダで固有の名前が付けられている情報。「ヘッダ行」と呼ばれる場合もあります。

ホスト 1 つまたは複数のサーバが存在するマシン。

ホストドメイン ISP がアウトソースする電子メールドメイン。ISP は、組織の電子メールドメインホスティングを提供し、その組織の電子メールサービスの運営および管理を行います。ホストドメインは、その他のホストドメインと共に同一の Messaging Server ホストを共有します。初期の LDAP ベースの電子メールシステムでは、1 つのドメインが 1 つまたは複数の電子メールサーバホストでサポートされていました。Messaging Server では、複数のドメインを単一のサーバでホストできます。各ホスト ドメインには、それぞれのドメインのユーザおよびグループコンテナをポイントする LDAP エントリがあります。ホストドメインは、「仮想ホストドメイン」や「仮想ドメイン」とも呼ばれます。

ホスト名 ドメイン内の特定マシンの名前。ホスト名は、IP ホスト名（電子メールなどの短縮形のホスト名、または完全なホスト名のいずれか）です。完全なホスト名は、ホスト名とドメイン名の 2 つの部分からなっています。たとえば、`mail.siroe.com` は、ドメイン `siroe.com` 内のマシン `mail` です。ホスト名は、そのドメイン内で固有の名前でなければなりません。組織内では、異なるサブドメイン内にある限り、複数の `mail` という名前のマシンを使用できます。例：`mail.corp.siroe.com`、`mail.field.siroe.com`。ホスト名は、常に、特定の IP アドレスをマップします。参照：**ドメイン名**、**完全なドメイン名（FQDN）**、**IP アドレス**

ホスト名の非表示 特定の内部ホスト名を含まないドメインベースの電子メールのアドレスを持つこと。

ホップ 2 台のコンピュータ間における送信。

ポート番号 ホストマシン上にある個々の TCP/IP アプリケーション（データの転送先）を指定する番号。

本文 電子メールメッセージの一部分。ヘッダとエンベロープは標準書式に従う必要がありますが、メッセージの本文は、テキスト、グラフィックス、またはマルチメディアなどを使って、送信者が自由に作成できます。作成された本文は MIME 標準規格に従います。

マスターチャネルプログラム リモートシステムへの転送を開始するチャネルプログラム。参照：**スレーブチャネルプログラム**

マスターディレクトリサーバ 複製されるデータを含むディレクトリサーバ。

見出し クライアントが最初に IMAP などのサービスに接続したときに、そのサービスによって表示されるテキスト文字列。

未配信通知 メッセージの転送中に、アドレスパターンとその書き換え規則の間で一致が見つからない場合に、MTA が元のメッセージと未配信報告を送信者に戻すこと。

無効ユーザ メッセージ処理時に発生するエラー状態。このエラーが発生すると、メッセージストアは MTA にその旨を通知し、メッセージストアからそのメッセージのコピーを削除します。MTA はそのメッセージを送信者に戻し、そのメッセージのコピーを削除します。

メッセージ 電子メールの基本単位。メッセージは、ヘッダと本文から構成されており、送信者から受信者に渡されるまでの間はエンベロープも含んでいます。

メッセージアクセスサービス Messaging Server メッセージストアへのクライアントアクセスをサポートする、プロトコルサービス、ソフトウェアドライバ、およびライブラリ。

メッセージキュー クライアントやその他のメールサーバから受け取ったメッセージが配信（即時または遅延）されるまで待機するディレクトリ。

メッセージストア Messaging Server のインスタンスがローカルに配信したすべてのメッセージを含むデータベース。メッセージは、単一または複数の物理ディスクに格納できます。

メッセージストア管理者 Messaging Server のメッセージストアを管理する権限を持つユーザ。このユーザは、メールボックスの表示や監視、およびストアへのアクセス制御を指定できます。また、プロキシ承認権を使用して、ストアを管理するための特定のユーティリティを実行できます。

メッセージストアパーティション 単一の物理ファイルシステムパーティション上の、メッセージストアまたはそのサブセット。

メッセージ制限容量 特定のフォルダが使用可能なディスク容量を定義する上限。

メッセージ転送 MTA が特定のアカウントに配信されたメッセージを、アカウントの属性に示された 1 つまたは複数の新しい宛先に送信する処理。転送先はユーザが設定できます。参照：**メッセージの配信**、**メッセージルーティング**

メッセージの送信 クライアントユーザエージェント (UA) が、メッセージをメールサーバに転送し、配信を要求すること。

メッセージの統一化 電子メール、ボイスメール、ファックス、その他の通信手段に単一のメッセージストアを使用する概念。iPlanet Messaging Server は、統一されたメッセージングソリューションを実現するための基礎を提供します。

メッセージの配信 MTA がメッセージをローカルの受信者（メールフォルダまたはプログラム）に配信するときの処理。

メッセージルーティング 最初の MTA が、受信者がローカルのアカウント以外の場所に存在するかもしれないと判断したときに、別の MTA にメッセージを転送する処理。通常、ルーティングを設定できるのはネットワーク管理者だけです。参照：**メッセージ転送**

メッセージを削除 削除するメッセージに印を付ける操作。削除済みメッセージは、別のユーザ操作で消去（パージ）されるまで、メッセージストアに残っています。参照：**メッセージをパージ**、**メッセージを消去**

メッセージを消去 メッセージに削除の印を付け、INBOX から永久的に削除する操作。参照：**メッセージを削除**、**メッセージをパージ**

メッセージをパージ ユーザグループフォルダでは既に削除済みとなり、参照されていないメッセージを永久的に削除し、そのスペースをメッセージファイルシステムに戻すプロセス。参照：**メッセージを削除**、**メッセージを消去**

メーリングリスト メッセージを送信する場合の宛先となる電子メールアドレスのリスト。「グループ」とも呼ばれます。

メーリングリストの所有者 メーリングリストにメンバーの追加や削除を行うための管理権限を持つユーザ。

メールクライアント ユーザの電子メール送受信を支援するプログラム。さまざまなネットワークおよびメールプログラムの一部分であり、ユーザが最も頻繁に利用する部分です。メールクライアントは、配信するメッセージを作成し、提出します。また、新たに受信したメールを確認し、受理し、整理します。

メール交換レコード **「MX レコード」**を参照。

メールボックス メッセージを保存したり表示するための場所。参照：**フォルダ**

メールリレー MUA または MTA からのメールを受け入れ、それをメール受信者のメッセージストアや別のルータに中継するメールサーバ。

メールルータ 参照：**メールリレー**

メンバー 配信リスト宛に送信された電子メールのコピーを受信するユーザまたはグループ。参照：**配信リスト**、**エクスパンション（展開）**、**モデレータ**、**配布リストの所有者**

モデレータ 配信リストに送られた電子メールを最初に受信する人物。この人物は、電子メールを受信した後、(A) 配信リストにメッセージを転送するか (B) メッセージを編集し、配信リストに転送することができます。または (C) 配信リストにメッセージを転送しない場合もあります。参照：**配信リスト**、**エクスパンション（展開）**、**メンバー**

ユーザアカウント サーバにアクセスするためのアカウント。Directory Server でのエントリとして管理されます。

ユーザエージェント（UA） ユーザが電子メールを作成、送信、受信できるようにするためのクライアントコンポーネント（Netscape Communicator など）。

ユーザエントリ（ユーザ プロファイル） 各ユーザに関する情報を記述するフィールド（必須の場合とオプションの場合とがあります）。例：識別名、氏名、役職、電話番号、ポケットベル番号、ログイン名、パスワード、ホームディレクトリなど。

ユーザ / グループ Directory Server 組織内のユーザおよびグループを管理する Directory Server。

ユーザ制限容量 システム管理者によって、ユーザの電子メールメッセージ用に割り当てられた容量。

ユーザフォルダ ユーザの電子メールメールボックス。

リストア バックアップデバイスからメッセージストアにフォルダの内容を復元するプロセス。参照：**バックアップ**

リッスンポート サーバが、クライアントやその他のサーバとの通信に使用するポート。

リバース DNS 検索 数値 IP アドレスから完全なドメイン名に変換するよう DNS に要求するプロセス。

リレー メッセージサーバ間でメッセージを渡すプロセス。

ルータ いくつかのネットワークトラフィック経路の中から経路を決定するシステム。ネットワークに関する情報を得るためのルーティングプロトコル、および「ルーティングマトリクス」として知られるシステム条件に基づいて最善のルーティングを決定するアルゴリズムを使います。OSI では、ルータは「ネットワークレイヤ中間システム」といいます。参照：**ゲートウェイ**

ルーティング **「メッセージルーティング」**を参照。

ルートエントリ ディレクトリ情報ツリー（DIT）階層の最初のエントリ。

レプリカ（複製）ディレクトリサーバ すべてまたは一部分のデータのコピーを受信するディレクトリ。

レベル ログの詳細度の指定（ログファイルに記録されるイベントの種類の相対的な数）。たとえば、Emergency レベルではほとんどのイベントがログに記録されませんが、Informational レベルでは数多くのイベントがログに記録されます。

ローカライズ、ローカライゼーション 翻訳のプロセス。

ローカル部分 電子メールアドレスの受信者を識別する部分。参照：**ドメイン部分**

ログディレクトリ サービスのすべてのログファイルが保存されているディレクトリ。

ログ有効期限 指定された期限に達したときにログディレクトリからログファイルを削除すること。

ログローテーション 現在のログファイルとして新しいログファイルを作成すること。それ以降のログイベントは、新しいログファイルに書き込まれます。前のログファイルはそのままログディレクトリに残りますが、ログが書き込まれることはありません。

ワイルドカード 検索文字列で、1 つまたは複数の文字、あるいは文字範囲を表すために使用する特殊文字。

ワークグループ ローカルのワークグループ環境。この環境において、サーバはローカルのオフィスまたはワークグループ内でルーティングと配信を実行します。部署内のメールは、バックボーンサーバにルーティングされます。参照：**バックボーン**

索引

シンボル

数字

A

B

C

D

E

F

H

I

J

L

M

N

O

P

R

S

T

U

V

W

あ

そ

た

ち

て

と

な

に

ね

は

ふ

へ

ほ

ま

み

め

も

ゆ

よ

り

ろ