

プロビジョニングガイド

iPlanet™ Messaging Server

Release 5.2

816-5021-01
2002年2月

Copyright © 2002, Sun Microsystems, Inc. All rights reserved.

Sun、Sun Microsystems、Sun のロゴマークは、米国およびその他の国における米国 Sun Microsystems, Inc.(以下、米国 Sun Microsystems 社とします)の商標もしくは登録商標です。

Netscape は、米国およびその他の国における Netscape Communications Corporation 社の登録商標です。

UNIX は、X/Open Company, Ltd が独占的にライセンスしている米国およびその他の国における登録商標です。

Legato Networker は、Legato Systems, Inc. の登録商標です。

Federal Acquisitions: Commercial Software—Government Users Subject to Standard License Terms and Conditions.

本書で説明されている製品は著作権法により保護されており、その使用、複製、頒布および逆コンパイルを制限するライセンスのもとにおいて頒布されます。Sun および Sun のライセンサーの書面による事前の許可なく、本製品および関連する文書のいかなる部分も、いかなる方法によっても複製することが禁じられます。

本書は、「現状のまま」をベースとして提供され、商品性、特定目的への適合性または第三者の権利の非侵害の黙示の保証を含みそれに限定されない、明示的であるか黙示的であるかを問わない、なんらの保証も行われないものとします。

目次

図目次	7
表目次	9
コード例一覧	11
このマニュアルについて	15
対象読者	15
お読みになる前に	16
内容の紹介	16
表記上の規則	17
コマンドラインプロンプト	17
関連マニュアル	18
第1章 プロビジョニングの概念とテクノロジー	19
iPlanet Messaging Server のプロビジョニング	19
iPlanet Messaging Server ネームスペース	20
二重ツリーネームスペース機構の仕組み	20
2つのディレクトリ情報ツリーが必要な理由	22
既存の DIT を iPlanet Messaging Server にマッピングする	22
アクセス制御のためのデータのパーティション化	23
サブドメイン用の個別のネームスペースの提供	24
iPlanet Messaging Server データモデル	24
ACI アーキテクチャ	25
サービスクラス	28
iPlanet Messaging Server のサービスクラスの設定	28
サービスクラスの例	29

第2章 ドメインのプロビジョニング	33
ドメイン ACI	34
DC ツリーの作成	35
DC ツリーのルートドメインエントリの作成	36
DC ツリーのルートエントリ属性とオブジェクトクラス	36
DC ツリーのトップレベルのドメインエントリの作成	37
DC ツリーのトップレベルノード属性とオブジェクトクラス	38
DC ツリーのホストドメインエントリの作成	38
DC ツリーのホストドメイン属性とオブジェクトクラス	39
ドメイン属性	40
inetDomain Attributes	40
mailDomain 属性	40
組織ツリーの作成	41
組織ツリーのルートドメインエントリの作成	42
組織ツリー内のホストドメインエントリの作成	42
組織ツリーのホストドメイン属性とオブジェクトクラス	43
organization 属性	43
nsManagedDomain 属性	43
ホストドメインに必要なコンテナの作成	44
組織ツリーのホストドメインコンテナ属性とオブジェクトクラス	45
ドメイン組織の作成	45
ドメイン組織の削除	46
バニティドメインの作成	47
ドメインタスク	48
使用可能なドメインメールサービスの追加と削除	49
ドメインのエリアスの作成	50
ドメインのスマートルーティングホストの追加	50
ドメインの新しいルーティングホストの追加	51
Messenger Express クライアントの添付ファイル数の制限	52
ドメインの状態の設定	52
ドメインのポストマスターの設定	54
受信メッセージサイズの制限の設定	55
ドメインの catch-all アドレスの指定	56
第3章 ファミリーアカウントのプロビジョニング	57
ファミリーアカウントの作成	57
ファミリーグループ管理者の作成	60
第4章 ユーザのプロビジョニング	63
ユーザエントリの作成	64
ユーザエントリオブジェクトクラスと属性	65
inetOrgPerson	65
inetUser	66

ipUser	66
inetMailUser	66
inetLocalMailRecipient	67
userPresenceProfile	67
nsManagedPerson	67
メールユーザのタスク	68
ユーザのアクティブ化と非アクティブ化	68
ユーザパスワードの変更	69
ユーザの Vacation メッセージの設定	70
使用可能なメールサービスの追加と削除	72
受信メール配信オプションの追加と変更	73
ユーザメッセージフィルタの設定	74
メールとメッセージの制限	76
メールの転送	77
新しいメールエイリアス	78
ユーザのメールサーバの変更	79
メーリングリストの作成権限の追加	80
受信メッセージサイズの制限	81
第 5 章 メーリングリストのプロビジョニング	83
メーリングリストエントリの作成	84
メールリストの属性	84
groupOfUniqueNames	85
inetMailGroup	85
inetLocalMailRecipient	86
nsManagedMailList	86
属性値の形式	86
メーリングリストのタスク	87
メーリングリスト所有者の割り当て	87
メンバーの追加	88
メーリングリストへの投稿の制限の作成	89
優先規則	90
メーリングリストのモデレータ	93
メーリングリストの有効化、無効化、削除	94
メッセージのファイルへのアーカイブ	94
リクエストアドレス	95
メーリングリストメンバーの表示	96
メーリングリストの参加可能者	97
動的なメーリングリストの作成	98
受信メッセージサイズの制限	99

第 6 章 Messaging Server 管理者のプロビジョニング	101
管理者のタイプ	102
構成管理者の作成	104
メッセージストア管理者の作成	104
特定の Messaging Server のメッセージストア管理者の作成	105
メールシステムトポロジ全体のメッセージストア管理者の作成	105
特定ドメインのメッセージストア管理者の作成	107
トップレベル管理者の作成	109
ドメイン管理者の作成	110
ドメイン組織管理者の作成	112
付録 A ルートとドメインの ACI の例	117
ACI の例内の変数の定義	117
組織ツリールートノード ACI	118
DC ツリールートノード ACI	121
ホストドメイン ACI	126
ドメイン組織 ACI	128
用語集	129
索引	159

図目次

図 1-1	iPlanet Messaging Server ディレクトリ構造の例	21
図 1-2	既存の DIT の iPlanet Messaging Server へのマッピングの例	23
図 1-3	TEST アクセス制御のためのデータのパーティション化の例	23
図 1-4	ACI の例	27
図 5-1	アクセス制御プロセス	91
図 6-1	ドメイン組織管理者の作成	113

表目次

表 1	マニュアルの表記規則	17
表 1-1	エントリタイプと対応するオブジェクトクラス	24
表 1-2	iPlanet Messaging Server サービスクラスのパラメータ値	29
表 6-1	Messaging Server 管理者と権限	102

コード例一覧

DC ツリールート of LDIF レコード	36
トップレベルノード of LDIF レコード	37
DC ツリー内のホストドメインノードを作成するための LDIF レコード	38
組織ツリールート of LDIF レコード	42
組織ツリー内のホストドメインを作成するための LDIF レコードの例	43
ホストドメインコンテナ of LDIF コード	44
組織ツリー内のドメイン組織 of LDIF レコード	46
バニティドメインを指定したユーザエントリの例	47
ドメインメールサービスを追加するための変更文	49
スマートルーティングホストを含むホストドメイン of LDIF レコード	49
ドメインのエイリアスの作成	50
スマートルーティングホストを追加するための変更文	50
スマートルーティングホストを含むホストドメイン of LDIF レコード	50
ルーティングホストを追加するための変更文	51
ルーティングホストを含むホストドメイン of LDIF レコード	51
Messenger Express の添付ファイル数を各メッセージで 2 つまでに制限するための変更文	52
Messenger Express の添付ファイル数を各メッセージで 2 つまでに制限するための LDIF レコード	52
ドメインの状態を Hold に設定するための変更文	53
Hold 状態のホストドメイン of LDIF レコード	53
ドメインのポストマスターを作成するための変更文	54
ドメインのポストマスターを作成するための LDIF レコード	54
ドメインのメッセージサイズの制限を設定するための変更文	55
ドメインのメッセージサイズの制限を設定するための LDIF レコード	55
catch-all アドレスを指定するための変更文	56
catch-all アドレスを指定するための LDIF レコード	56
ファミリーアカウントエントリ	58

ファミリーグループのメンバーの LDIF レコード	59
ファミリー管理者グループのエントリ	60
ファミリーグループ管理者のエントリ	60
ユーザエントリの例	64
ユーザのパスワード変更後の LDIF レコード	69
ユーザの自動応答 Vacation メッセージを設定して有効にした後の LDIF レコード	71
ユーザのメールサービス変更後の LDIF レコード	72
ユーザのメール配信オプションを変更するための LDIF レコード	73
ユーザのメッセージフィルタを設定した後の LDIF レコード (ldapsearch に -o フラグを指定して表示)	75
ユーザのメールボックスとメッセージ数の制限を設定するための LDIF レコード	77
ユーザのメール転送アドレスを追加するための LDIF レコード	78
ユーザのメールアドレスエイリアスを追加するための LDIF レコード	79
ユーザのメールサーバを変更するための LDIF レコード	79
ユーザのメールサーバを変更するための LDIF レコード	80
ユーザのメールサーバを変更するための LDIF レコード	81
メーリングリスト用の LDIF レコード	84
所有者を指定したメーリングリストの LDIF レコード	88
メンバーを追加したメーリングリストの LDIF レコード	88
配信制限を指定したメーリングリストの LDIF レコード	92
モデレータを指定したメーリングリストの LDIF レコード	93
メーリングリストを無効化した LDIF レコード	94
アーカイブ属性を指定したメーリングリストの LDIF レコード	95
購読リクエスト属性を指定したメーリングリストの LDIF レコード	95
表示属性を指定したメーリングリストの LDIF レコード	96
参加可能者を指定したメーリングリストの LDIF レコード	97
動的なメーリングリスト用の LDIF レコード	98
参加可能者を指定したメーリングリストの LDIF レコード	99
システム全体のメッセージストア管理者グループの作成	106
システム全体のメッセージストア管理者のユーザエントリの例	106
ストア管理者グループの作成	107
ドメイン管理者のユーザエントリの例	108
トップレベル管理者グループ	109
トップレベル管理者のユーザエントリの例	109
ドメイン管理者グループの作成	110
ドメイン管理者のユーザエントリの例	111
組織管理者グループの作成	113

ドメイン管理者のユーザエントリの例	114
組織ツリールートノード ACI	118
DC ツリールートノード ACI	121
ホストドメイン ACI	126
ドメイン組織 ACI	128

このマニュアルについて

このマニュアルでは、LDAP を使用して、ユーザ、メーリングリスト、ドメイン、管理者に関する iPlanet Messaging Server のプロビジョニングを行う方法について説明します。このマニュアルは、『iPlanet Schema Reference Manual』と共に使用する必要があります。

この章は、次の節から構成されています。

- 対象読者
- お読みになる前に
- 内容の紹介
- 表記上の規則
- 関連マニュアル

対象読者

このマニュアルは、LDAP を使用して iPlanet Messaging Server のプロビジョニングを行う場合にお読みください。このマニュアルの対象読者は次のとおりです。

- iPlanet LDAP ディレクトリ内の Messaging Server エントリと既存の情報ソースを連動させるようなプロビジョニングツールを開発するメッセージングシステムアーキテクト。既存の情報ソースとは、企業データベースや課金システムなどのユーザ、グループ、ドメイン情報を指す
- LDAP を使用したドメイン、ユーザ、グループ、管理者のエントリの作成方法を
知る必要があるサイト管理者

読者は、LDAP、iPlanet Directory Server、および電子メールの概念についての基本的な知識を持っている必要があります。

お読みになる前に

このマニュアルは、読者が次の一般的な知識を持っていることを前提としています。

- 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
- 電子メールとその概念
- Netscape Console

内容の紹介

このマニュアルには、次の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 (この章)
- 第1章「プロビジョニングの概念とテクノロジー」
- 第2章「ドメインのプロビジョニング」
- 第3章「ファミリーアカウントのプロビジョニング」
- 第4章「ユーザのプロビジョニング」
- 第5章「メーリングリストのプロビジョニング」
- 第6章「Messaging Server 管理者のプロビジョニング」
- 付録 A 「ルートとドメインの ACI の例」

表記上の規則

表 1 マニュアルの表記規則

書体または記号	意味	例
AaBbCc123	コマンド名、ファイル名、コード、ディレクトリ名、ホスト名、識別名、およびコンピュータ画面に表示されるテキストを示します。	msg.conf ファイルを編集します。 すべてのファイルを一覧表示するには、ls -a を使用します。 Error:illegal port #
AaBbCc123	ユーザが入力したテキストを示します。	% cd madonna
<i>the_variable</i>	コマンドラインのプレースホルダや変数を示します。実際の名前または値で置き換えます。	# instance_root/start-msg
<i>AaBbCc123</i>	新しい言葉や用語、強調する言葉を示します。	iPlanet Messaging Server プロビジョニングガイド

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、コマンドはこのマニュアルで示すとおりに入力してください。

関連マニュアル

iPlanet Messaging Server には、このマニュアルの他に、管理者用の補足情報およびエンドユーザやディベロッパ用のマニュアルもあります。次の URL を使用すると、Messaging Server のすべてのマニュアルを参照できます。

<http://docs.iplanet.com/docs/manuals/messaging.html>

利用できる関連マニュアルは次のとおりです。

- 『iPlanet Messaging Server 管理者ガイド』
- 『iPlanet Messaging Server インストールガイド』
- 『iPlanet Messaging Server リファレンスマニュアル』
- 『iPlanet Messaging Server スキーマリファレンス』
- 『iPlanet Messaging Server プロビジョニングガイド』
- 『iPlanet Delegated Administrator for Messaging and Collaboration インストールおよび管理ガイド』

プロビジョニングの概念とテクノロジー

この章では、iPlanet Messaging Server のプロビジョニングに関する概念とテクノロジーを説明します。この章には、以下の節があります。

- 20 ページの「iPlanet Messaging Server ネームスペース」
- 24 ページの「iPlanet Messaging Server データモデル」
- 25 ページの「ACI アーキテクチャ」
- 28 ページの「サービスクラス」

iPlanet Messaging Server のプロビジョニング

プロビジョニングとは、Directory Server 内の iPlanet Messaging Server ユーザ、メーリングリスト、システム管理者、ドメインの各エントリに関する追加、変更、削除を行うことです。Messaging Server は、必要に応じてディレクトリを照会することにより、これらの要素に関する情報を取得します。

iPlanet Messaging Server には、次の 4 つのプロビジョニングインタフェースがあります。

- iPlanet Delegated Administrator for Messaging コンソール
- iPlanet Delegated Administrator for Messaging コマンドラインユーティリティ
- iPlanet Messaging Server 管理コンソール
- Messaging Server LDAP ディレクトリ

このマニュアルでは、LDAP を使用してプロビジョニングを行う方法について説明します。他のプロビジョニング方法に触れる場合がありますが、このマニュアルでは、LDAP を使用したプロビジョニングを中心に説明します。

iPlanet Messaging Server ネームスペース

インストール後の iPlanet Messaging Server ネームスペースは、「組織ツリー」および「ドメインコンポーネントツリー (DC ツリー)」の 2 つのディレクトリ情報ツリー (DIT) で構成されます。組織ツリーは、ユーザおよびグループの各エントリを含んでいます。DC ツリーは、ローカル DNS 構造をミラー化したものであり、データエントリを含む組織ツリーへのインデックスとしてシステムにより使用されます (図 1-2 を参照)。DC ツリーはさらに、スマートホスト、ルーティングホスト、ドメインディスク容量制限などの、ドメインの操作パラメータを含んでいます。

この後の節では、組織ツリーと DC ツリーからなる「二重ツリー機構」の仕組みと、この機構が選択された理由について説明します。既存の DIT を iPlanet Messaging Server の二重ツリー機構へ移植する方法の詳細については、『iPlanet Messaging Server 移行ガイド』を参照してください。

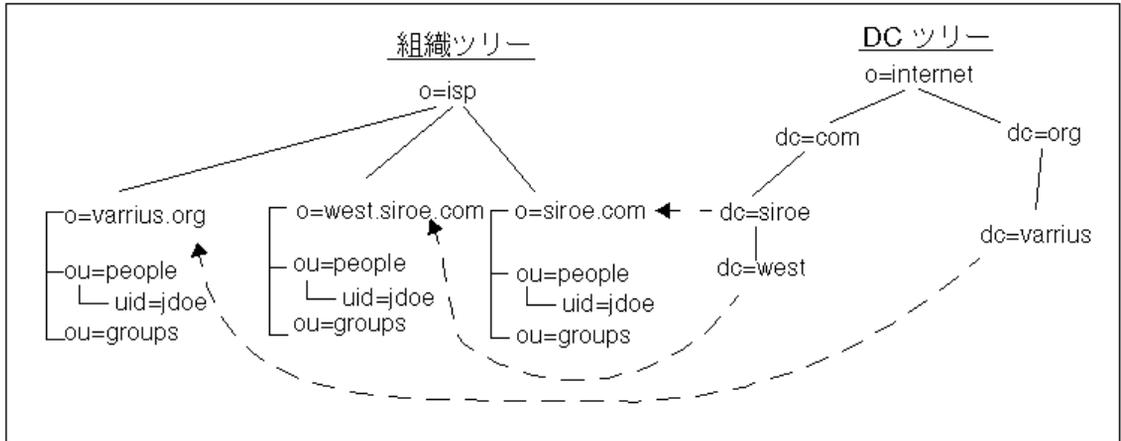
二重ツリーネームスペース機構の仕組み

この節では、iPlanet Messaging Server が 2 つの DIT 機構をどのように利用しているかを説明します。

iPlanet Messaging Server がユーザまたはグループのエントリを検索する場合、初めに DC ツリー内でユーザまたはグループのドメインノードを検索し、`inetDomainBaseDN` 属性の値を展開します。この属性には、実際のユーザまたはグループのエントリを含む組織サブツリーへの DN 参照が格納されています。

このモデルを使用することで、iPlanet Messaging Server は任意のタイプのディレクトリツリー内に格納されたエントリをサポートできます。ただし条件として、DC ツリー内のドメインコンポーネントノードが、そのドメインのユーザが見つかる組織ツリー内のノードを指している必要があります。この関係を、図 1-1 の例に示します。この図の点線は `inetDomainBaseDN` の値を示しています。組織ツリー内のノード名は、DC ツリー内のノード名と一致している必要はありません。

図 1-1 iPlanet Messaging Server ディレクトリ構造の例



この例では、データエントリが組織ツリーの下で追加および変更されていますが、実際にはメッセージサーバは DC ツリーを参照します。次の 3 人のユーザについて考えてみます。

	ユーザ 1	ユーザ 2	ユーザ 3
名前 :	John Doe	John Doe	Jane Doe
ドメイン :	siroe.com	west.siroe.com	varrius.org
UID :	jdoe	jdoe	jdoe
ログイン :	jdoe@siroe.com	jdoe@west.siroe.com	jdoe@varrius.org

ログイン名は UID とドメインで構成されます。どのユーザの場合にも、サーバはログインのドメイン部分 (@ マークの後の値) を探し、対応する DC ノードの `inetdomainbasedn` 属性から DN を取得します。次に、ログイン名のローカル部分 (@ マークの前の値) と等しい UID を持つユーザエントリを、DN によって指定されたサブツリーから検索します。

たとえば `west.siroe.com` に属する John Doe は、ログイン名 `jdoe@west.siroe.com` を使用して、サーバにログインします。サーバは、DC ノード内の `west.siroe.com` に対する DN 参照 (`inetdomainbasedn`) を `o=west.siroe.com`, `o=isp` までたどります。

インストール時に、iPlanet Messaging Server は、既存の DNS にマップされるデフォルトの DC ツリーと組織ツリーを作成します。Delegated Administrator コマンド `imadmin domain create` を使用してディレクトリドメインノードを追加すると、対応するノードが DC ツリーと組織ツリーの両方に作成されます。LDAP インタフェースを使用してノードを作成する場合は、そのドメインに対応するノードを DC ツリー内に作成し、データに対応するドメインを組織ツリー内に作成する必要があります。この手順は、『iPlanet Messaging Server 移行ガイド』に記載されています。

注 特定のドメインにメールを配信するには、そのドメインの MX レコードを DNS 内に含める必要があります。

2 つのディレクトリ情報ツリーが必要な理由

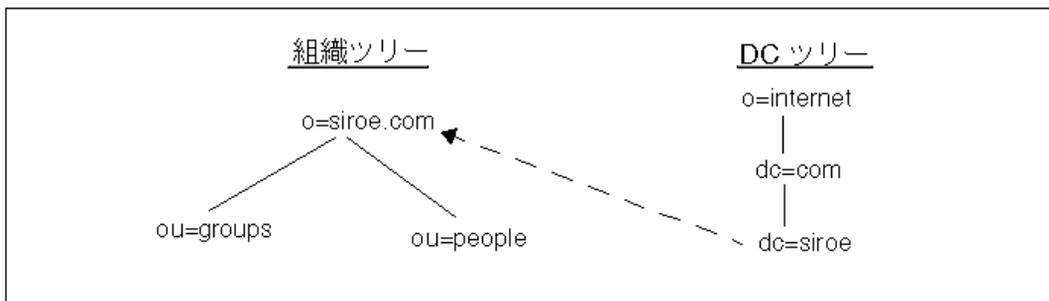
iPlanet Messaging Server は、構成情報およびユーザやグループのデータを含む単一の DC ツリーをサポートします。しかし、インストール時には、iPlanet Messaging Server は、DC ツリーと組織ツリーの両方を作成します。この二重ツリー機構は次の拡張機能を提供します。

- 既存の DIT にマップする DC ツリーを作成することによって、iPlanet Messaging Server が既存のディレクトリを利用できる
- 組織に特有のアクセス制御を行うために、データをパーティション化できる。つまり各組織は、ユーザとグループのエントリが置かれた DIT 内に個別のサブツリーを持つことができます。データにアクセスできるユーザを、そのサブツリーに含まれるユーザに制限できます。これにより、iPlanet Delegated Administrator for Messaging のようなローカライズされたアプリケーションを安全に稼働できる
- サブドメイン用の個別のネームスペースを持つことができる。たとえば、`west.siroe.com` と `siroe.com` は、別々の組織サブツリーにマップされます。これにより、各サブツリー内に同じ UID を持つユーザエントリを作成できる

既存の DIT を iPlanet Messaging Server にマッピングする

二重ツリー機構を使うと、既存の DIT を iPlanet Messaging Server にマッピングできません。次の図にこの様子を示します。この図は、iPlanet Messaging Server 内の DC ツリーにマップされた既存の NMS DIT (`o=siroe.com`) を示しています。このプロセスの詳細は、『iPlanet Messaging Server 移行ガイド』に記載されています。

図 1-2 既存の DIT の iPlanet Messaging Server へのマッピングの例

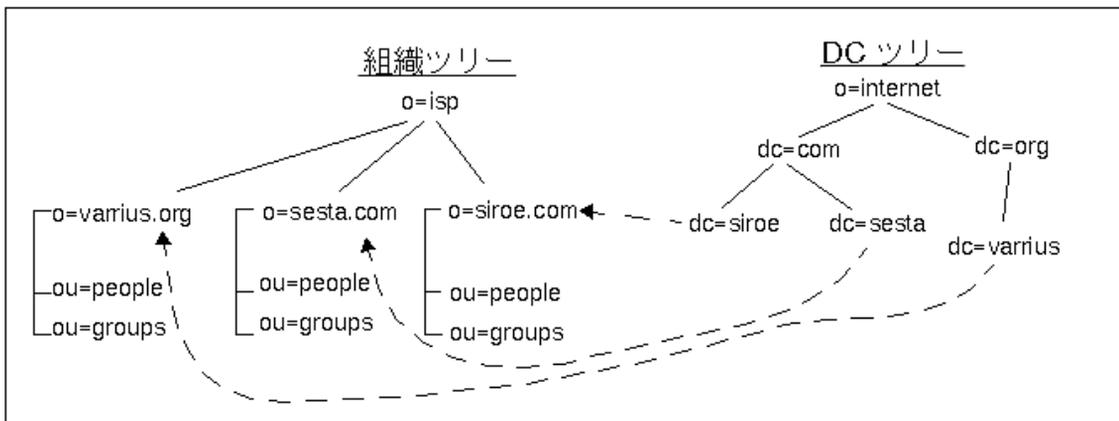


アクセス制御のためのデータのパーティション化

二重ツリー機構は、各パーティション内でのデータのパーティション化とアクセス制御を提供します。この機能は、あるカスタマが同じディレクトリツリー内に格納された他のカスタマに関するデータにアクセスできないという厳しい要件に対応できるため、マルチテナントディレクトリにおいて重要です。データのパーティション化とアクセス制御により、個々のカスタマ組織に安全な方法でアプリケーションのアウトソーシングを提供することができます。その際、各組織のユーザやグループのデータを、他の組織のデータと分けて格納できます。iPlanet Delegated Administrator for Messaging は、このタイプのアプリケーションの一例です。

そのため、アウトソーシングを受けるメッセージングカスタマは、1つの大きな DIT の中にある適切に定義されたサブツリー（一般的にはドメイン）内に表現されます。このサブツリーは、そのカスタマに属するすべてのサービスデータを格納するために使用されます。図 1-3 に、この概念を示します。

図 1-3 TEST アクセス制御のためのデータのパーティション化の例



サブドメイン用の個別のネームスペースの提供

二重ツリー機構は、サブドメイン用に個別のネームスペースを提供します。これにより、サブドメイン内で同じログイン名を使用することができます。たとえば、jdoe@siroe.com と jdoe@west.siroe.com を、2つの独立した有効な電子メールアドレスにすることができます。図 1-1 にこのことを示しています。

iPlanet Messaging Server データモデル

iPlanet Messaging Server オブジェクトクラスの基本データモデルは、コアオブジェクトクラスによって作成された LDAP エントリタイプ (ユーザ、グループ、ドメインなど) を共有クラス (複数のサービスで共有できるオブジェクトクラス) およびサービス固有のオブジェクトクラス (特定のタイプのサーバに固有のクラス) でオーバーレイすることによって LDAP エントリタイプを拡張します。この関係を次の表に示します。

表 1-1 エントリタイプと対応するオブジェクトクラス

タイプ \ クラス	コアクラス	共有クラス	Messaging Server のクラス
DC ツリーのドメイン	domain、inetdomain		mailDomain、nsManagedDomain、icsCalendarDomain
組織ツリードメイン	organization		nsManagedDomain
電子メールユーザ	person、inetUser、organizationalPerson、inetOrgPerson	ipUser、userPresenceProfile	inetMailUser、inetLocalMailRecipient、nsManagedPerson
グループ	groupOfUniqueNames		inetMailGroup、inetLocalRecipient、inetMailGroupManagement、nsManagedMailList
ファミリーアカウント	inetManagedGroup		nsManagedDept

たとえば電子メールユーザタイプを使う場合、各オブジェクトクラスは、それぞれ次の属性を提供します。

Person は、ユーザを説明するための属性を提供します。

organizationalPerson は、組織に属するユーザを説明するための属性を提供します。

`inetOrgPerson` は、基本的なインターネットユーザの属性を提供します。

`ipUser` は、個人アドレス帳属性、サービスクラステンプレート、さらに該当する場合はファミリーアカウントの DN を保持します。

`inetUser` はユーザアカウントを表します。このクラスは、`inetMailUser` や `ipUser` と共にメールアカウントを作成するために使用されます。

`inetSubscriber` は、加入者アカウントを表すオプションのオブジェクトクラスです。このクラスは、アカウント ID および `challenge/response` 属性を提供します。

`inetMailUser` は、メールアカウントを表し、ユーザ固有のメールアカウント属性の大半を提供します。

`inetLocalMailRecipient` は、ローカル(組織内)の電子メール受信者を表します。このクラスは、受信者の電子メールアドレスを指定し、受信者に関するルーティング情報を提供します。

ACI アーキテクチャ

アクセスコントロール情報指示 (Access Control Information instructions、AIC) は、ディレクトリに対するユーザのアクセスを制御します。Messaging Server のユーザにはいくつかタイプがあり、必要とするディレクトリアクセスのレベルはタイプごとに異なります。これらのユーザタイプの一部を次に示します。

- 通常の電子メールユーザ: このタイプのユーザは、単に電子メールを送受信し、パスワードの変更や Vacation モードの開始のための権限を必要とします。
- トップレベル管理者: ディレクトリ内のすべてのエントリに対してすべての処理を実行する権限を持ちます。
- メッセージストア管理者: システムまたはドメインのメールボックスの表示や、メッセージストアの管理を実行する権限を持ちます。
- ドメイン管理者: ドメイン内のメールユーザ、メーリングリスト、およびファミリーアカウントのエントリの作成、変更、削除を行うことができます。
- ドメイン組織管理者: ドメイン組織内のメールユーザとメーリングリストのエントリの作成、変更、削除を行うことができます。
- ファミリーグループ管理者: ファミリーグループエントリ内のファミリーメンバーを追加または削除する権限を持ちます。

これらの各ユーザタイプには、DC ツリーおよび組織ツリーのルートまたはドメインレベルで特定の ACI が割り当てられます (図 1-4 を参照)。各ユーザに対してではなく、ルートやドメインエントリ内で ACI を割り当てることにより、アクセス範囲をドメインまたはシステム全体に設定できます。ルートノード上で指定された ACI は、システム全体のエントリに適用されます。ドメイン内で指定された ACI は、そのドメイン内のエントリにのみ適用されます。(ACI 情報の詳細については、『iPlanet Directory Server 管理ガイド』を参照)。

さまざまな管理者用の ACI は、特定のグループ上で与えられます。管理者を作成するには、単にユーザをグループに追加し、そのユーザエントリにグループバックポインタ属性 (memberof) を追加します。たとえば、インストール時には、cn=Domain Administrators, ou=groups, <ドメインの DN> というグループが特定の ACI 権限を使って作成されます。ドメイン管理者を作成するには、単にユーザをそのグループに追加し、そのユーザのエントリに memberof 属性を追加します。

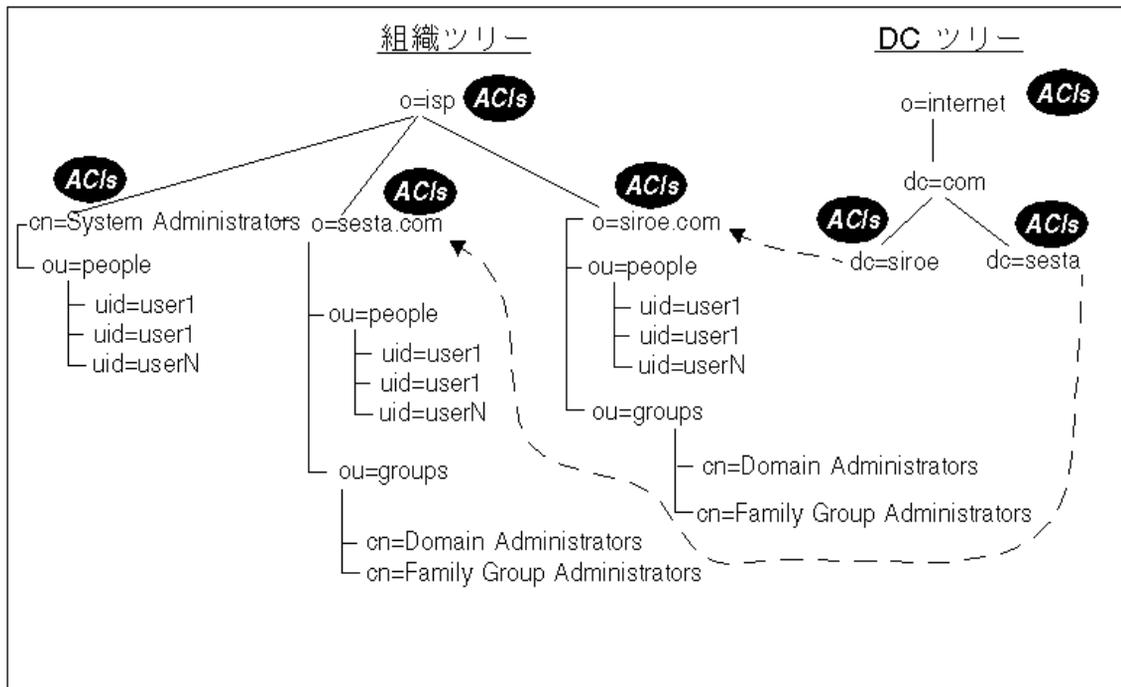
ファミリーグループ管理者を作成するには、ユーザをメーリングリスト cn=Family Group Administrators, ou=groups, <ドメインの DN> に追加します。詳しい管理者の作成手順については、第 6 章「Messaging Server 管理者のプロビジョニング」を参照してください。

たとえば、以下に示す構成内では、次のエントリ内で ACI が指定されます。

```
o=isp
o=sesta.com,o=isp
o=siroe.com,o=isp
o=internet
dc=siroe, dc=com, o=internet
dc=sesta, dc=com, o=internet
```

図 1-4 に、ドメインとルートエントリノード用にインストールされる ACI を示します。

図 1-4 ACI の例



サービスクラス

サービスクラス (COS) 機能を使用すると、指定したユーザに適用できる固定された機能と属性のセットを名前付きで作成できます。さらに、単一の属性を持つユーザエンタリに与えることができる属性のテンプレートを作成できます。たとえば、ISP を運用している場合、Hall of Fame および All-Star という名前で、2 つのレベルのメールサービスを作成することが考えられます。この場合、Hall of Fame サービスクラスでは、IMAP、セキュア IMAP、POP3、および HTTP (Web メール) メールサービスに加え、5G バイトのメッセージストアのディスク容量をユーザに提供できます。All-Star サービスクラスでは、POP3 メールサービスと 5G バイトのメッセージストアのディスク容量を提供できます。

注 サービスクラスで定義された属性を参照するフィルタを含む LDAP 検索要求は実行されません。たとえば、mailquota がサービスクラステンプレート内だけに定義され、ユーザエンタリ内に定義されていない場合は、属性 mailquota に関する検索は正常に実行できません。サーバは、そのような要求が出されると、「実行されません」エラーメッセージを返します。

iPlanet Messaging Server のサービスクラスの設定

サービスクラス機能を追加するための基本的な手順は次のとおりです。

1. slapd.ldbm.conf に COS プラグインを追加します。
2. COS メールスキーマのエントリを作成します。COS メールスキーマは次の項目を定義します。
 - ディレクトリ内の cos テンプレート定義の場所
 - サービスクラスを適用できるユーザエンタリを含むディレクトリ
 - ユーザエンタリに適用されるサービスクラステンプレートを指定するために使用する属性 (inetCOS) の名前
 - テンプレート内で使用する属性のリスト
3. サービスクラステンプレートのエントリを作成します。
4. サービスクラスをユーザエンタリに割り当てます。

これらの手順の詳細は、次の Web サイトに記載されています。

http://docs.iplanet.com/docs/manuals/deladmin/45/html/06_cos.htm#25217

次の節では、iPlanet Messaging Server サービスクラスに関する具体的な問題と例について説明します。サービスクラス機能をシステムに実装する際の「COS スキーマの管理」の手順では、次のパラメータ値を使用してください。

表 1-2 iPlanet Messaging Server サービスクラスのパラメータ値

パラメータ	値
サービスクラスのスキーマおよびテンプレート用のコンテナの DN	ou=COS, <ドメインの DN>
メールスキーマエントリの DN	cn=mail scheme, ou=COS, <ドメインの DN>
サービスクラスコンテナの DN (cosTemplateDn)	ou=MailSchemeTemplates, ou=COS, <ドメインの DN>
サービスクラスをエントリに割り当てるための属性 (cosSpecifier)	inetCOS

サービスクラスの例

前の節で説明した例を使用し、sesta.com というホストドメイン用に、*Hall of Fame* および *All-Star* という名前を持つメールサービス用のサービスクラスを作成します。Hall of Fame サービスクラスでは、IMAP、セキュア IMAP、POP3、および HTTP (Web メール) メールサービスに加え、5G バイトのメッセージストアのディスク容量をユーザに提供します。All-Star サービスクラスでは、POP3 メールサービスと 5G バイトのメッセージストアのディスク容量を提供できます。

1. Directory Server に COS プラグインをインストールします Directory Server 4.1 の場合は、次のサイトを参照してください。

<http://home.netscape.com/eng/server/directory/DSRK/4.1/cos.htm>

Directory Server 5.0 の場合は、次のサイトを参照してください。

<http://docs.iplanet.com/docs/manuals/directory/51/html/cli/plugconf.htm#16608>

2. COS のクラスと定義用のコンテナを作成します。

```
dn: ou=COS,o=sesta.com, o=isp
objectclass: top
objectclass: organizationalUnit
ou: COS
```

3. 次の LDIF エントリの例を使用して、メールスキーマエントリを作成します。

```
dn: uid=mail scheme,ou=COS,o=sesta.com, o=isp
objectclass: top
objectclass: cosDefinition
cosTemplateDn: ou=MailSchemeTemplates,ou=COS,o=sesta.com, o=isp
cosTargetTree: o=sesta.com, o=isp
cosSpecifier: inetCOS
cosAttribute: mailQuota
cosAttribute: mailAllowedServiceAccess
```

- dn: uid=mail scheme,ou=COS,o=sesta.com, o=isp
COS メールスキーマエントリの DN
- objectclass: cosDefinition
サービスクラススキーマのエントリを定義するオブジェクトクラス
- cosTemplateDn: ou=MailSchemeTemplates,ou=COS,o=sesta.com, o=isp
このスキーマの COS テンプレートエントリが格納されるサブツリーを含む複数値の属性
- cosTargetTree: ou=People,o=sesta.com, o=isp
COS スキーマが適用されるサブツリーを含む複数値の属性
- cosSpecifier: inetCOS
ユーザエントリに適用されるサービスクラステンプレートを指定するために使用する属性の名前
- cosAttribute: mailQuota
cosAttribute: mailAllowedServiceAccess
テンプレートエントリ内で使用される属性

4. クラス用のコンテナを作成します。

Hall of Fame および All-Star テンプレートのそれぞれに対応する 2 つのテンプレートエントリ用の LDIF を以下に示します。

```
dn: ou=MailSchemeClasses,ou=COS,o=sesta.com, o=isp
objectclass: top
objectclass: organizationalunit
ou: MailSchemeClasses
```

5. COS テンプレートエントリを作成します。

Hall of Fame および All-Star テンプレートのそれぞれに対応する、2つのテンプレートエントリ用の LDIF を以下に示します。

```
dn: cn=All-Star,ou=MailSchemeClasses,ou=COS,o=sesta.com, o=isp
objectclass: top
objectclass: inetUser
objectclass: inetMailUser
mailQuota: 5000000
mailAllowedServiceAccess: +pop3:*
```

```
dn: cn=Hall of Fame,ou=MailSchemeClasses,ou=COS,o=sesta.com, o=isp
objectclass: top
objectclass: inetUser
objectclass: inetMailUser
mailQuota: 5000000000
mailAllowedServiceAccess: +imap, imaps, pop3, http:*
```

- dn: cn=All-Star,ou=MailSchemeClasses,ou=COS,o=sesta.com, o=isp
dn: cn=Hall of Fame,ou=MailSchemeClasses,ou=COS,o=sesta.com, o=isp

COS テンプレートの DN

- objectclass: top
objectclass: inetUser
objectclass: inetMailUser
mailQuota: 5000000
mailAllowedServiceAccess: +pop3:*

All-Star テンプレート内の属性とオブジェクトクラス

- objectclass: top
objectclass: inetUser
objectclass: inetMailUser
mailQuota: 5000000
mailAllowedServiceAccess: +imap, imaps, pop3:*

Hall of Fame テンプレート内の属性とオブジェクトクラス

6. サービスクラステンプレートをユーザに追加します。

```
dn: uid=Havlicek,ou=People,o=sesta.com, o=isp
objectClass: top
objectClass: person
objectClass: organizationalPerson
```

```
objectClass: inetOrgPerson
objectClass: inetUser
objectClass: ipUser
objectClass: userPresenceProfile
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
cn: John Havlicek
sn: Havlicek
initials: JH
givenName: John
mail: john.havlicek@sesta.com
mailAlternateAddress: Havlicek@sesta.com
mailHost: mail.siroe.com
uid: Havlicek
dataSource: iPlanet Messaging Server
userPassword: secret
inetUserStatus: active
mailUserStatus: active
mailMsgQuota: 100
inetCos: Hall of Fame

dn: uid=Hornicek,ou=People,o=sesta.com, o=isp
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: inetUser
objectClass: ipUser
objectClass: userPresenceProfile
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
cn: Jeff Hornicek
sn: Hornicek
initials: JH
givenName: Jeff
mail: jeff.hornicek@sesta.com
mailAlternateAddress: Hornicek@sesta.com
mailDeliveryOption: mailbox
mailHost: mail.siroe.com
uid: Hornicek
dataSource: iPlanet Messaging Server 5.0
userPassword: secret
inetUserStatus: active
mailUserStatus: active
mailMsgQuota: 100
inetCos: All-Star
```

ドメインのプロビジョニング

この章では、iPlanet Messaging Server のプロビジョニングを行うために必要なドメインと組織ユニットの作成方法について説明します。これらのユニットの一部は、インストール時または Delegated Administrator の使用時に作成されますが、ここでは説明のために、これらのユニットの作成手順を示します。また、このマニュアルでは、属性の概要を説明します。属性の詳細は、『iPlanet Messaging and Collaboration スキーマリファレンスマニュアル』に記載されています。この章には、以下の節があります。

- 34 ページの「ドメイン ACI」
- 35 ページの「DC ツリーの作成」
 - 36 ページの「DC ツリーのルートドメインエントリの作成」
 - 37 ページの「DC ツリーのトップレベルのドメインエントリの作成」
 - 38 ページの「DC ツリーのホストドメインエントリの作成」
- 41 ページの「組織ツリーの作成」
 - 42 ページの「組織ツリーのルートドメインエントリの作成」
 - 42 ページの「組織ツリー内のホストドメインエントリの作成」
 - 44 ページの「ホストドメインに必要なコンテナの作成」
- 45 ページの「ドメイン組織の作成」
 - 46 ページの「ドメイン組織の削除」
- 47 ページの「バニティドメインの作成」
- 48 ページの「ドメインタスク」
 - 49 ページの「使用可能なドメインメールサービスの追加と削除」
 - 50 ページの「ドメインのエイリアスの作成」
 - 50 ページの「ドメインのスマートルーティングホストの追加」
 - 51 ページの「ドメインの新しいルーティングホストの追加」

- 52 ページの「Messenger Express クライアントの添付ファイル数の制限」
- 52 ページの「ドメインの状態の設定」
- 54 ページの「ドメインのポストマスターの設定」
- 55 ページの「受信メッセージサイズの制限の設定」
- 56 ページの「ドメインの catch-all アドレスの指定」

ドメイン ACI

ACI は、DC ツリーおよび組織ツリーのすべてのルートエン트리とドメインエントリに必要です。ACI は、さまざまなタイプのユーザや管理者によるディレクトリへのアクセスを制御するだけでなく、iPlanet Delegated Administrator for Messaging ツールによるディレクトリへのアクセスも制御します。ユーザアクセスを制御するための Messaging Server ACI の設計については、25 ページの「ACI アーキテクチャ」を参照してください。

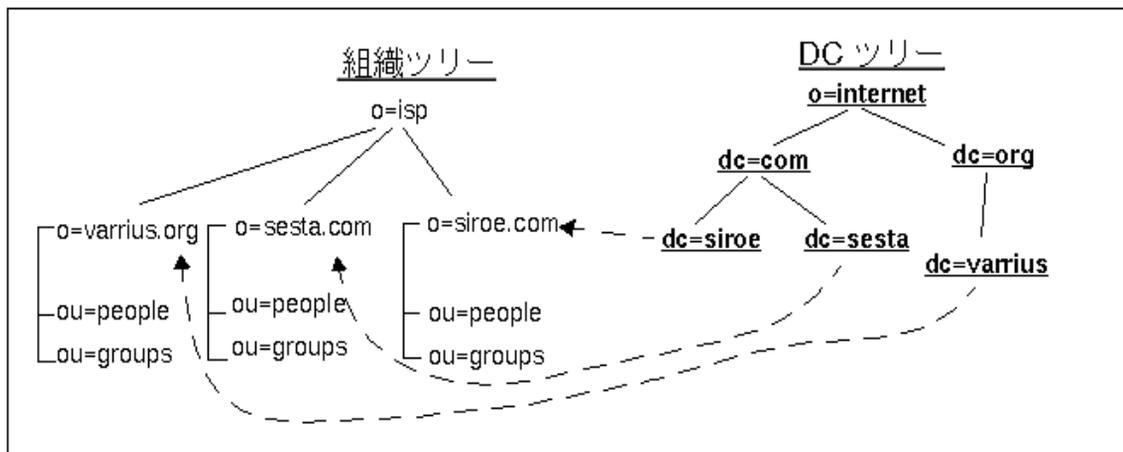
インストール時には、DC ツリーおよび組織ツリーの両方のルートレベルと、組織ツリーのトップレベルドメイン用に ACI がインストールされます (付録 A 「ルートとドメインの ACI の例」を参照)。これらの ACI は、ノードとすべてのサブノードに適用されます。したがって、ルートノード上に作成された ACI は、ルートの下にあるすべてのドメインに適用されます。ACI 規則は、特定のドメインに対して `ldapsearch` を実行することによって表示できます。ACI 規則は、ドメインエントリの属性の後に次の形式で表示されます。

```
# 匿名アクセス制御
#
# ユーザエントリに対する匿名の読み取りと検索のアクセスを許可
#
aci: (targetattr != "userPassword")
  (targetfilter=(objectClass=nsManagedPerson))
  (version 3.0; acl "Anonymous access to User entries";
  allow (read,search)
  userdn="ldap:///anyone");
#
```

この ACI 規則は、すべてのユーザが、オブジェクトクラス `nsManagedPerson` を含む任意のエントリ内の `userPassword` を除くすべてを検索して読み取ることを許可しています。ポンド記号 (#) は実行不能のコメントを示します。targetattr は、動作対象の属性を指定します。targetfilter は、検索対象のオブジェクトクラスです。version は、ユーザが定義するバージョン番号とコメントです。allow は、許可されている権限 (読み取り、書き込み、検索、削除、変更) を一覧表示します。userdn は、これらの属性に対して処理を行うユーザを指定します。

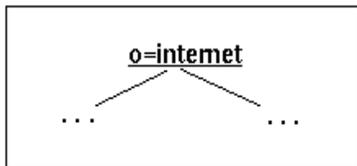
ディレクトリ ACI の詳細については、『iPlanet Directory Server 4.1 管理者ガイド』を参照してください。

DC ツリーの作成



DC ツリーノードは、特定のドメインの操作パラメータ（ルーティングホスト、ディスク容量制限など）と、ドメインのユーザとメーリングリストのエントリを含むサブツリーへのポインタを含みます。DC ツリーは、DNS 構造をミラー化します。また、インストール時にデフォルトの DC ツリーが作成されます。新しいホストドメインまたはドメイン組織が作成された場合は、DC ツリーと組織ツリー内に新しいドメインとドメイン組織ノードを作成する必要があります。この処理は、iPlanet Delegated Administrator for Messaging コマンド `imadmin domain create`（コマンドの詳細については『iPlanet Messaging Server リファレンスマニュアル』を参照）または iPlanet Delegated Administrator for Messaging コンソール（『iPlanet Delegated 管理者ガイド』を参照）を使用して実行できます。この節では、LDAP を使用して DC ツリーを作成する方法だけを説明します。なお、新しいドメインには MX レコードも追加する必要がありますことに注意してください。

DC ツリーのルートドメインエントリの作成



ルートエントリは、ディレクトリツリーのトップレベルノードです。DC ツリーでは、ルートは `o=internet` に設定する慣例になっています。ルートを `o=internet` 以外に設定する場合は、Messaging Server 構成内の `service.dccroot` が、DC ツリールートの DN に一致していることを確認します。コード例 2-1 に DC ルートを作成するための LDIF レコードを示します。DC ツリーと組織ツリーのルートノードはインストール時に作成されますが、ここでは説明のために LDIF を示します。デフォルトの ACI は、付録 A 「ルートとドメインの ACI の例」に記載しています。

注 通常、特定の共通属性にはエイリアスを指定します。エイリアスは、Directory Server の構成ディレクトリ内の定義ファイル (`*.at.conf`) で指定します。一般的に使用されるエイリアスには、`cn` (commonname)、`ou` (organizationalUnit)、`o` (organization)、`sn` (surname)、`dn` (distinguishedName) があります。

コード例 2-1 DC ツリールートの LDIF レコード

```
dn: o=internet
objectClass: organization
o: internet
description: Root level node in the Domain Component (DC) tree
```

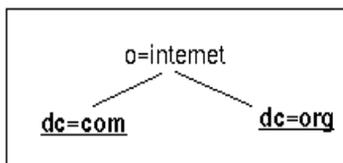
DC ツリーのルートエントリ属性とオブジェクトクラス

- `dn: o=internet`
識別名 (dn) は、ツリー内のディレクトリエントリを一意に識別します。DC ツリー内のデフォルトのルートノードは、`o=internet` です。
- `objectClass: organization`

DC ツリーのルートノードは、オブジェクトクラス `organization` によって定義されます。このオブジェクトクラスでは、別の属性をエントリに追加できますが、`"o"` だけは必須です。`o` は、このエントリの `dn` 内に設定されている値と同じ値にする必要があります。

注 全てのオブジェクトクラスは、`top` オブジェクトクラスを継承するため、エントリを作成する際には LDIF コード内に `objectClass: top` 行を含める必要はありません。

DC ツリーのトップレベルのドメインエントリの作成



トップレベルドメインエントリは、ルートのすぐ下にあり、DNS ドメインのドメインコンポーネントをミラー化する必要があります。コード例 2-2 に、トップレベルノードを作成するための LDIF レコードを示します。ルートノード、トップレベルノード、およびデフォルトドメインノードはインストール時に作成されます。ここでは、説明のために LDIF を示します。ACI も作成されます (付録 A 「ルートとドメインの ACI の例」を参照)。

コード例 2-2 トップレベルノードの LDIF レコード

```

dn: dc=com, o=internet
objectClass: domain
dc: com
description: top level .com domain in the DC Tree

dn: dc=org, o=internet
objectClass: domain
dc: org
description: top level .org domain in the DC Tree
  
```

DC ツリーのトップレベルノード属性とオブジェクトクラス

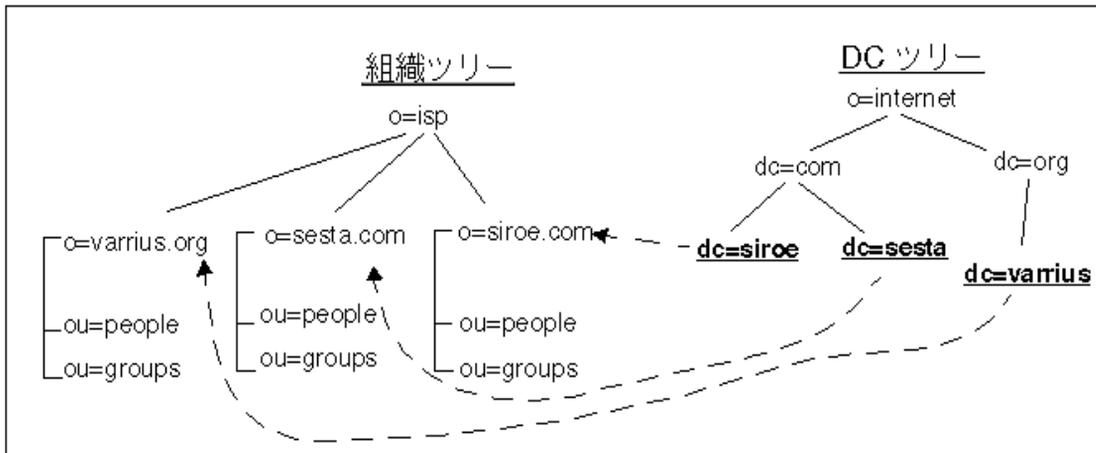
- dn: dc=com,o=internet
dn: dc=org,o=internet

dn はトップレベルドメインノードエントリを指定します。

- objectClass: domain

domain オブジェクトクラスは、DC ツリー内のすべてのコンテナエントリ (ルートエントリ以外) を作成するために使用されます。

DC ツリーのホストドメインエントリの作成



組織ツリー内の各ホストドメインについては、対応するホストドメインノードも DC ツリー内に作成する必要があります。DC ツリー内にホストドメインを作成するための LDIF コードを次に示します。ACI については、付録 A 「ルートとドメインの ACI の例」を参照してください。

コード例 2-3

DC ツリー内のホストドメインノードを作成するための LDIF レコード

```
dn: dc=sesta,dc=com,o=internet
objectClass: domain
objectClass: inetDomain
objectClass: mailDomain
objectClass: nsManagedDomain
objectClass: icsCalendarDomain
description: DC node for sesta.com hosted domain
```

コード例 2-3

DC ツリー内のホストドメインノードを作成するための LDIF レコード (続き)

```
dc: sesta
inetDomainBaseDN: o=sesta.com,o=isp
inetDomainStatus: active
mailDomainStatus: active
mailDomainAllowedServiceAccess: +imap, pop3, http:*
mailRoutingHosts: manatee.siroe.com
preferredMailHost: manatee.siroe.com
mailDomainDiskQuota: 100000000
mailDomainMsgQuota: -1
mailClientAttachmentQuota: 5
```

DC ツリーのホストドメイン属性とオブジェクトクラス

- dn: dc=sesta, dc=com, o=internet

dn は、ツリー内のドメインエントリを一意に識別します。各ホストドメインコンポーネントは、ホストドメインの DNS ノードと一致している必要があります。

- objectClass: domain
objectClass: inetDomain
objectClass: mailDomain
objectClass: nsManagedDomain
objectClass: icsCalendarDomain

これらの行は、dc=sesta エントリを DIT 内に作成するために必要なオブジェクトクラスを指定します。domain は、コアオブジェクトクラスで、DC ツリーのドメインコンポーネントノードを説明するために役立つ属性を提供します。

inetDomain は、ホストドメインのその他のプロパティを説明する属性を提供します。このオブジェクトクラスは、DNS ドメインに対応するディレクトリエントリに関連付けられています。

mailDomain はホストドメインアカウントを表します。このオブジェクトクラスを mailDomain (およびオプションで inetDomainAuthInfo) と組み合わせて使用することで、ホスト組織のメールサービスに適したホストドメインノードを作成できます。このオブジェクトクラスは、すべてのホストドメインエントリで使用する必要があります。

nsManagedDomain は、iPlanet Delegated Administrator for Messaging 用の情報を格納します。

注

ユーザデータとグループデータが DC ツリー内に格納され、組織ツリー内に格納されていない場合は、nsManagedDomain オブジェクトクラスと関連属性を含める必要があります。42 ページの「組織ツリー内のホストドメインエントリの作成」を参照してください。

ドメイン属性

- `description`: DC node for sesta.com hosted domain
自由な形式のテキスト記述。通常は、このエントリの属性 `organizationName` の値に関連付けられている組織の完全な名前です。
- `dc`: sesta
必須の属性。dc は、このノードに関連付けられている DNS ドメインコンポーネントです。

inetDomain Attributes

- `inetDomainBaseDN`: o=sesta.com,o=isp
単一値の属性です。このホストドメインのすべてのユーザとグループのエントリが含まれるサブツリーの DN です。
- `inetDomainStatus`: active
ホストドメインの現在の状態。有効な値は、`active`、`inactive`、`deleted` です。この属性はグローバルドメインの状態を示します。値がない場合は、状態が `active` であることを示します。不正な値は、`inactive` として扱われます。メールドメインの場合は、他の状態属性として `mailDomainStatus` があります。

mailDomain 属性

- `mailDomainStatus`: active
メールドメインの現在の状態。次のいずれかの値になります。有効な値は、`active`、`inactive`、`deleted`、`hold` です。
- `mailDomainAllowedServiceAccess`: +imap, pop3, http:*
サービスアクセスフィルタを格納します。フィルタを指定しない場合、ユーザがすべてのクライアントからすべてのサービスにアクセスできるようになります。
- `mailRoutingHosts`: manatee.siroe.com
このドメインおよびそのすべてのサブドメインのユーザに対するルーティングを決定する MTA の完全修飾ホスト名。この名前が空白かまたは見つからない場合、すべての MTA は、このドメインおよびそのサブドメインのユーザやグループのメッセージをルーティングする必要があります。
- `preferredMailHost`: manatee.siroe.com
iPlanet Delegated Administrator for Messaging とコンソールで、このメールドメイン内のユーザとグループの `mailHost` 属性を設定するために使用されます。
- `mailDomainDiskQuota`: 100000000

このドメイン内のすべてのユーザに許可されているメッセージの割当量 (バイト単位)。-1 は、制限がないことを示します。Delegated Administrator によりプロビジョニングが行われますが、この値は強制されません。ただし、レポートに役立つ場合があります。

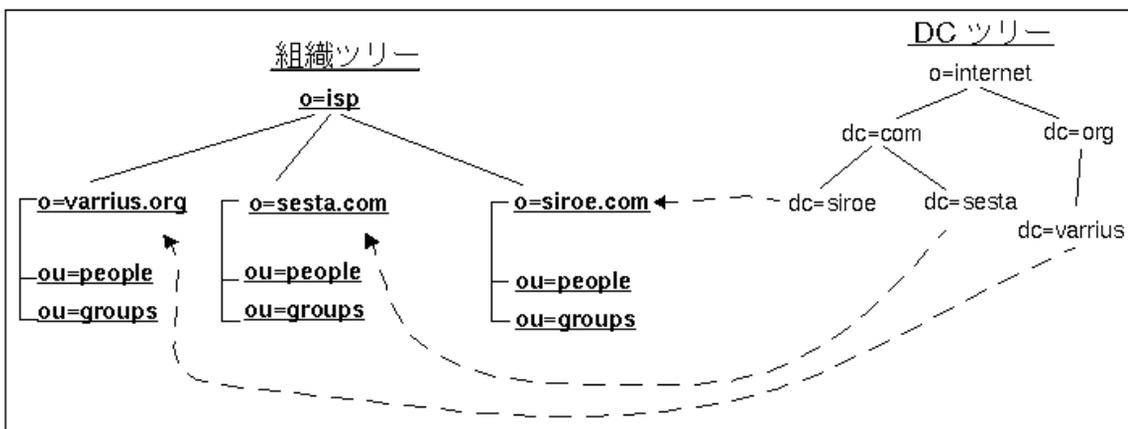
- mailDomainMsgQuota: -1

このドメイン内のすべてのユーザに許可されているメッセージ数の制限。-1 は、制限がないことを示します。Delegated Administrator によりプロビジョニングが行われますが、この値は強制されません。ただし、レポートに役立つ場合があります。

- mailClientAttachmentQuota: 5

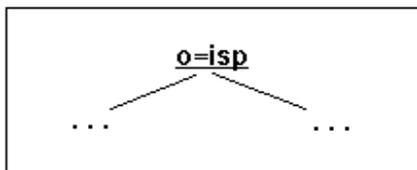
Messenger Express クライアントがこのドメインで使用できる添付ファイルの数。-1 は添付ファイルの制限がないことを意味します。

組織ツリーの作成



組織ツリーは、ユーザとグループのエントリを含んでいます。サーバは、組織ツリーを指す DC ツリーを参照します。新しいホストドメインを作成すると、DC ツリーと組織ツリー内に新しいドメインノードが作成されます。この処理は、iPlanet Delegated Administrator for Messaging コマンド `imadmin domain create` または iPlanet Delegated Administrator for Messaging GUI ツールを使用して実行できます。

組織ツリーのルートドメインエントリの作成



組織ツリーのルートエントリは、DC ツリーのルートエントリと同じようにインストール時に作成されます。組織ツリーのルート名はインストーラで指定できます。このノードはインストール時に作成されますが、ここでは説明のために LDIF を示します。

コード例 2-4 組織ツリールートの LDIF レコード

```
dn: o=isp
objectClass: organization
o: internet
description: Root level node in the Organizational tree
```

この例では、ルートエントリ DN として `o=isp` を使用します。属性の説明については、36 ページの「DC ツリーのルートドメインエントリの作成」を参照してください。ACI については、付録 A 「ルートとドメインの ACI の例」を参照してください。

組織ツリー内のホストドメインエントリの作成



組織ツリー内のホストドメインは、ルート (`o=isp`) の下に作成されます。ホストドメインの DN は、任意の名前を使用することができ、DC ツリー内で使用されている名前に合わせる必要はありません。ただし、DC ツリーのドメインノード内の `inetDomainBaseDN` 属性が、組織ツリー内の対応するノードを指している必要があります。コード例 2-5 に、組織ツリー内のホストドメインを作成するための LDIF コードの例を示します。

コード例 2-5 組織ツリー内のホストドメインを作成するための LDIF レコードの例

```
dn: o=sesta.com,o=isp
objectclass: organization
objectclass: nsManagedDomain
o: sesta.com
nsNumMailLists: 5
nsMaxMailLists: 1000
nsNumUsers: 20
nsMaxUsers: 1000
```

組織ツリーのホストドメイン属性とオブジェクトクラス

この節では、ホストドメイン属性について簡単に説明します。属性の詳細については、『iPlanet Messaging and Collaboration スキーマリファレンスマニュアル』を参照してください。

- `dn: o=sesta.com, o=isp`
`dn` は、ツリー内のホストドメインエントリを一意に識別します。
- `objectClass: organization`
`objectclass: nsManagedDomain`
 これらは、組織ツリー内のホストドメインエントリに必要なオブジェクトクラスです。`organization` は、コアオブジェクトクラスで、組織を説明するために使用されます。`nsManagedDomain` は、iPlanet Delegated Administrator for Messaging 用の情報を格納します。

organization 属性

- `o: sesta.com`
`o` は、`organizationName` のエイリアスで、必須の属性です。

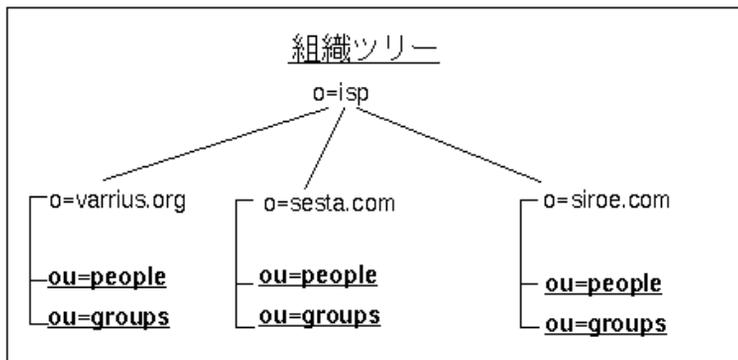
nsManagedDomain 属性

- `nsNumMailLists: 5`

ドメイン内のユーザによって作成されたメールリストの数を示します。この数は、すべてのネストされたサブドメインを累計したものです。Delegated Administrator は、このカウンタを保持し、その値を強制します。

- **nsMaxMailLists: 1000**
このドメイン内のユーザが作成できるメールリストの最大数を示します。この制限は、すべてのネストされたサブドメインに適用されます。
- **nsNumUsers: 20**
Delegated Administrator で使用中のユーザアカウントの数を示します。
- **nsMaxUsers: 1000**
作成可能なユーザアカウントの最大数を示します。

ホストドメインに必要なコンテナの作成



各ホストドメインは、ユーザエンタリ用の *people* という名前のコンテナと、メールリストエンタリ用の *groups* という名前のコンテナを持っている必要があります。次にコードの例を示します。

コード例 2-6 ホストドメインコンテナの LDIF コード

```

dn: ou=People,o=sesta.com,o=isp
objectClass: organizationalUnit
ou: People

dn: ou=Groups,o=sesta.com,o=isp
objectClass: organizationalUnit
ou: Groups
    
```

組織ツリーのホストドメインコンテナ属性とオブジェクトクラス

- dn: ou=People,o=sesta.com,o=isp
dn: ou=Groups,o=sesta.com,o=isp

これらは、すべてのホストドメインに必要なコンテナの識別名です。ou=People は、ホストドメインのすべてのユーザエントリを含んでいます。ou=Groups は、ホストドメインのすべてのメーリングリストエントリを含んでいます。

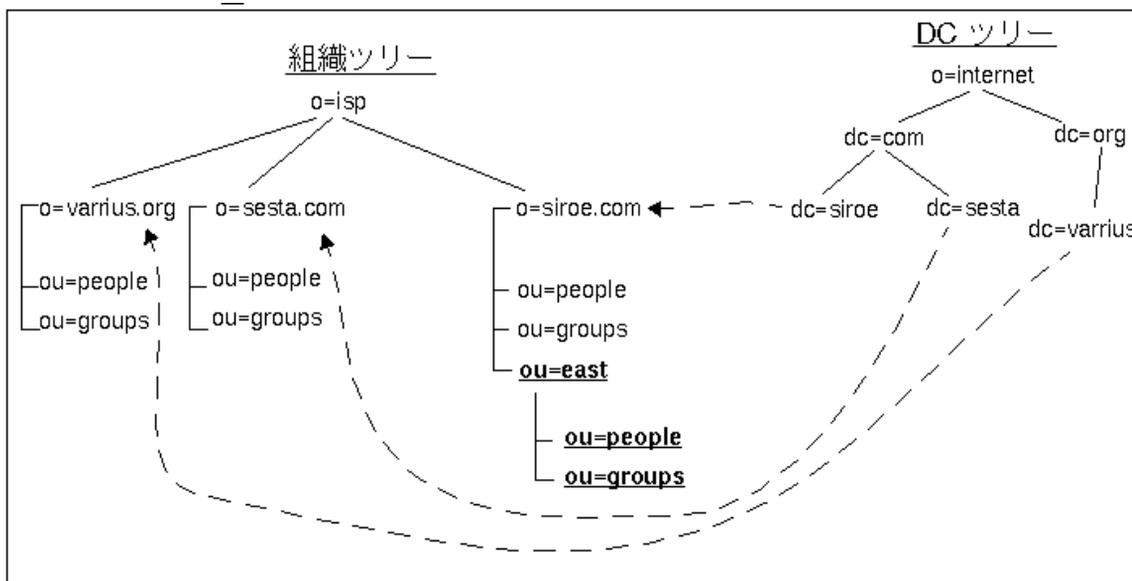
- objectClass: organizationalUnit

organizationalUnit オブジェクトクラスは、この例では、ホストドメインのコンテナエントリを作成するために使用されます。

- ou: People
ou: Groups

これらは、必須の organizationalUnit エントリです。

ドメイン組織の作成



ドメイン組織は、ドメインノード(上記を参照)内のユーザとグループを含むノードです。Delegated Administrator for Messaging から見ると、ドメイン組織は別の組織ノードのように見えます。ドメイン組織は、部門や機能ラインを基準として、ユーザとグループのエントリの編成と委任を行う必要がある企業にとって有効です。ユーザエントリをドメイン組織に入れた場合、そのユーザは以前と同じ電子メールアドレスを保持します。

ドメイン組織を作成するには、LDAP を使用する必要があります。現在、iPlanet Console や iPlanet Delegated Administrator for Messaging 内には、組織を作成するメカニズムはありません。ただし、Delegated Administrator コンソールは、既存のドメイン組織内のユーザやグループの作成、削除、変更をサポートしています。

ACI が指定されていないドメイン組織エントリを次に示します (ACI については、付録 A 「ルートとドメインの ACI の例」を参照)。ドメイン組織用のコンテナを作成する手順については、前の 44 ページの「ホストドメインに必要なコンテナの作成」を参照してください。

コード例 2-7 組織ツリー内のドメイン組織の LDIF レコード

```
dn: ou=east,o=siroe.com,o=isp
objectclass: nsManagedOrgUnit
objectclass: organizationalUnit
objectclass: inetdomainOrg
ou: east
nsdamodifiableby: cn=Domain Organization Administrators,ou=east,
o=siroe.com,o=isp
domOrgMaxUsers: 1000
domOrgNumUsers: 3
```

ドメイン組織の削除

ドメイン組織は次の手順で削除します。

1. `imadmin delete` コマンドを使用して、すべてのユーザとグループを削除します。
2. `imadmin purge` コマンドを使用して、すべてのユーザとグループをバージします。
3. `ou=users` や `ou=groups` など、残りのすべてのコンテナを削除します。

バニティドメインの作成

バニティドメインまたはカスタムドメインは、ドメインエントリにはなく、個々のユーザエントリに付けられるドメイン名です。バニティドメインは、カスタマイズされたドメイン名を希望し、かつホストドメインをサポートするための管理作業を行わない個人または小さな組織に有効です。たとえば、従業員 6 人の小さな会社 Florizel が Siroe ISP に電子メールアカウントを持っているとします。同社の社員は、florizel.com で電子メールを受信することを希望しています。この場合、ホストドメインを作成する代わりに、Florizel の各メンバーが `username@florizel.com` でメールを受信できるようにバニティドメインを登録して設定することができます。

バニティドメインはドメイン名の LDAP エントリを持ちません。代わりに、`MailAlternateAddress` 属性 (オブジェクトクラス `inetLocalMailRecipient`) と `msgVanityDomain` 属性 (オブジェクトクラス `msgVanityDomainUser`) をユーザエントリ内に追加することによって、ユーザごとに指定されます。次にコード例を示します。

コード例 2-8 バニティドメインを指定したユーザエントリの例

```
dn: uid=kong,ou=people,o=siroe.com,o=isp
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: inetUser
objectClass: ipUser
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: nsManagedPerson
objectClass: userPresenceProfile
objectClass: msgVanityDomainUser
cn: Kelly Kong
sn: Kong
initials: KK
givenName: Kelly
mail: Kelly.Kong@siroe.com
mailAlternateAddress: kelly.kong@florizel.com
mailAlternateAddress: @florizel.com
msgVanityDomain: florizel.com
mailDeliveryOption: mailbox
mailHost: manatee.siroe.com
uid: kong
dataSource: iMS 5.0 @(#)ims50users.sh 1.5a 02/3/00
userPassword: password
mailAllowedServiceAccess: +imap, imaps, pop3, http:*
inetUserStatus: active
mailUserStatus: active
mailQuota: -1
mailMsgQuota: 100
```

この例では、msgVanityDomain は、MTA によってルーティングのために使用されるドメイン名を指定します。kelly.kong@siroe.com または kelly.kong@florizel.com 宛てのメールは、Kelly Kong のメッセージストアに送信されます。

「mailAlternateAddress: @florizel.com」という行により、kelly.kong@florizel.com が catch-all ドメインアドレスになります。catch-all ドメインアドレスとは、MTA が正確に一致するアドレスを見つけることができなかった場合に、ドメイン florizel.com 宛てのメールを受信するアドレスです。ダイレクト LDAP 参照を使用するシステムの場合は、mailDomainCatchAllAddress 属性 (56 ページの「ドメインの catch-all アドレスの指定」を参照) を使用する必要があります。

-
- 注**
- 1) バニティドメインを使用するユーザは、実ドメイン名を使用して Messaging Server にログインする必要があります。上の例では、Kelly Kong は、ドメイン florizel.com ではなく、siroe.com を使用して自分のメールにアクセスする必要があります。
 - 2) バニティドメイン名には、一意の登録済みインターネットドメイン名を使用する必要があります。また、MX レコードも、それらの名前に登録する必要があります。
-

ドメインタスク

この節では、一般的なドメインタスクを実行する方法について説明します。各タスクについて LDIF レコード全体が示されていますが、ほとんどのタスクでは、1 つまたは複数の属性を既存のドメインに追加するだけで済みます。これらの属性は、LDIF の更新文内に示されています。また、LDIF レコード全体の中では、これらの属性は太字で示されています。この節には、以下の項があります。

- 49 ページの「使用可能なドメインメールサービスの追加と削除」
- 50 ページの「ドメインのエイリアスの作成」
- 50 ページの「ドメインのスマートルーティングホストの追加」
- 51 ページの「ドメインの新しいルーティングホストの追加」
- 52 ページの「Messenger Express クライアントの添付ファイル数の制限」
- 52 ページの「ドメインの状態の設定」
- 54 ページの「ドメインのポストマスターの設定」
- 55 ページの「受信メッセージサイズの制限の設定」
- 56 ページの「ドメインの catch-all アドレスの指定」

使用可能なドメインメールサービスの追加と削除

使用可能なドメインメールサービスは、`mailDomainAllowedServiceAccess` 属性で設定します。形式は次のとおりです。

```
mailAllowedDomainServiceAccess: filter_syntax
```

(使用可能なサービスのシンタックスについては、『iPlanet Message Server 管理者ガイド』の「フィルタの構文」の節を参照してください。) 次の LDIF 変更コードは、`sesta.com` 用の IMAP、POP3、および HTTP (Messenger Express) サポートを追加します。

コード例 2-9 ドメインメールサービスを追加するための変更文

```
dn: dc=sesta, dc=com, o=internet
changetype: modify
add: mailDomainAllowedServiceAccess
mailDomainAllowedServiceAccess: +imap:ALL$+pop:ALL$+http:ALL
```

コード例 2-10 スマートルーティングホストを含むホストドメインの LDIF レコード

```
dn: dc=sesta,dc=com,o=internet
objectClass: domain
objectClass: inetDomain
objectClass: mailDomain
description: DC node for sesta.com hosted domain
dc: sesta
inetDomainBaseDN: o=sesta.com,o=isp
inetDomainStatus: active
mailDomainStatus: active
mailDomainAllowedServiceAccess: +imap, pop3, http:*
mailRoutingHosts: manatee.sesta.com
preferredMailHost: manatee.sesta.com
mailDomainDiskQuota: 100000000
mailDomainMsgQuota: -1
mailClientAttachmentQuota: 5
mailDomainAllowedServiceAccess: +imap:ALL$+pop:ALL$+http:ALL
```

ドメインのエイリアスの作成

ドメインのエイリアスとは、別のドメインを指すドメインエントリのことです。ドメインのエイリアスは、DC ツリー内で作成されます。ドメインのエイリアスには、登録済みの一意のインターネットドメイン名を使用する必要があります。ドメインでメールを受信するには、MX レコードもドメインに登録する必要があります。次の LDIF の例では、ドメイン florizel.com を sesta.com のエイリアスにすることができます。

コード例 2-11 ドメインのエイリアスの作成

```
dn: dc=sesta, dc=com, o=internet
objectclass: alias
objectclass: inetDomainAlias
aliasedObjectName: dc=sesta, dc=com, o=internet
dc: florizel
```

ドメインのスマートルーティングホストの追加

スマートルーティングホストまたはスマートホストは、ドメイン内のすべてのユーザーのルーティング情報の正式なソースと見なされる MTA ホストです。ローカル MTA は、ローカルディレクトリ内でユーザを検出できない場合に、メッセージをスマートホストに転送します。ルーティングホストの完全修飾ホスト名をドメインエントリの mailRoutingSmartHost 属性に追加することによって、スマートホストを指定します。次の LDIF レコードでは、smarthost1.siroe.com をドメイン sesta.com のルーティングホストとして設定します。

コード例 2-12 スマートルーティングホストを追加するための変更文

```
dn: dc=sesta, dc=com, o=internet
changetype: modify
add: mailRoutingSmartHost
mailRoutingSmartHostsmarthost1.siroe.com
```

コード例 2-13 スマートルーティングホストを含むホストドメインの LDIF レコード

```
dn: dc=sesta, dc=com, o=internet
objectClass: domain
objectClass: inetDomain
objectClass: mailDomain
description: DC node for sesta.com hosted domain
```

コード例 2-13 スマートルーティングホストを含むホストドメインの LDIF レコード

```
dc: sesta
inetDomainBaseDN: o=sesta.com,o=isp
inetDomainStatus: active
mailDomainStatus: active
mailDomainAllowedServiceAccess: +imap, pop3, http:*
mailRoutingHosts: manatee.sesta.com
preferredMailHost: manatee.sesta.com
mailDomainDiskQuota: 100000000
mailDomainMsgQuota: -1
mailClientAttachmentQuota: 5
mailRoutingSmartHost: smarthost1.siroe.com
```

ドメインの新しいルーティングホストの追加

ルーティングホストとは、特定のドメインおよびそのサブドメイン内のアドレスにメールをルーティングすることになっている MTA ホストです。ドメインレコード内に `mailRoutingHosts` 属性が含まれていない場合は、システム内でそのディレクトリにアクセスするすべての MTA がそのドメインのメールのルーティングを行う必要があります。次の LDIF レコードの例は、ドメインのメールルーティングを行う複数の MTA を指定する方法を示しています。

コード例 2-14 ルーティングホストを追加するための変更文

```
dn: dc=sesta, dc=com, o=internet
changetype: modify
add: mailRoutingHosts
mailRoutingHosts: sestarouter1.siroe.com
mailRoutingHosts: sestarouter2.siroe.com
```

コード例 2-15 ルーティングホストを含むホストドメインの LDIF レコード

```
dn: dc=sesta,dc=com,o=internet
objectClass: domain
objectClass: inetDomain
objectClass: mailDomain
description: DC node for sesta.com hosted domain
dc: sesta
inetDomainBaseDN: o=sesta.com,o=isp
inetDomainStatus: active
mailDomainStatus: active
mailDomainAllowedServiceAccess: +imap, pop3, http:*
mailRoutingHosts: manatee.sesta.com
mailRoutingHosts: sestarouter1.siroe.com
mailRoutingHosts: sestarouter2.siroe.com
```

コード例 2-15 ルーティングホストを含むホストドメインの LDIF レコード

```
preferredMailHost: manatee.sesta.com
mailDomainDiskQuota: 100000000
mailDomainMsgQuota: -1
mailClientAttachmentQuota: 5
```

Messenger Express クライアントの添付ファイル数の制限

Messenger Express クライアントが1つのメッセージで送信できる添付ファイルの数を制限するには、次のように mailClientAttachmentQuota 属性を設定します。

コード例 2-16 Messenger Express の添付ファイル数を各メッセージで2つまでに制限するための変更文

```
dn: dc=sesta, dc=com, o=internet
changetype: modify
replace: mailClientAttachmentQuota
mailClientAttachmentQuota: 2
```

コード例 2-17 Messenger Express の添付ファイル数を各メッセージで2つまでに制限するための LDIF レコード

```
dn: dc=sesta, dc=com, o=internet
objectClass: domain
objectClass: inetDomain
objectClass: mailDomain
description: DC node for sesta.com hosted domain
dc: sesta
inetDomainBaseDN: o=sesta.com, o=isp
inetDomainStatus: active
mailDomainStatus: active
mailRoutingHosts: manatee.siroe.com
preferredMailHost: manatee.siroe.com
mailDomainDiskQuota: 100000000
mailDomainMsgQuota: -1
mailClientAttachmentQuota: 2
```

ドメインの状態の設定

メールアドレスの状態は、次のいずれかになります。

- active - ドメイン内のメールサービスが完全に機能している
- inactive - メールサービスが一時停止している
- deleted - メールサービスが一時停止中で、`imadmin domain purge` コマンド (『iPlanet Messaging Server リファレンスマニュアル』を参照) によってドメインに削除用のマークが付けられている
- hold - そのドメイン内のユーザへのすべてのメッセージを宛先メールサーバの HOLD キュー内に保持するように MTA が指示されている。これは、ユーザを 1 つのサーバから別のサーバに移すときに、ユーザの移動中にメッセージを保持する場合などに使用します。

これらの状態は、属性 `mailDomainStatus` 内に設定されます。状態は 1 つの値から別の値に変化する場合があります。値がない場合は、状態が `active` であることを示します。不正な値は、`inactive` として扱われます。次の LDIF は、状態を `hold` に設定します。

コード例 2-18 ドメインの状態を Hold に設定するための変更文

```
dn: dc=sesta, dc=com, o=internet
changetype: modify
replace: mailDomainStatus
mailDomainStatus: hold
```

コード例 2-19 Hold 状態のホストドメインの LDIF レコード

```
dn: dc=sesta,dc=com,o=internet
objectClass: domain
objectClass: inetDomain
objectClass: mailDomain
description: DC node for sesta.com hosted domain
dc: sesta
inetDomainBaseDN: o=sesta.com,o=isp
inetDomainStatus: active
mailDomainStatus: active
mailRoutingHosts: manatee.sesta.com
mailDomainDiskQuota: 100000000
mailDomainMsgQuota: -1
mailClientAttachmentQuota: 5
mailDomainStatus: hold
```

ドメインのポストマスターの設定

ポストマスターは各ドメインの特別なユーザです。ポストマスターのアドレスは、エラーメッセージや配信ステータスの通知に使用されます。ポストマスターを明示的に指定していない場合は、デフォルトの「postmaster@ドメイン」に設定されます。

注 この手順は、ダイレクト LDAP を使用してメールのルーティングを行うシステムだけで使用できます。dirsync を使用するシステムでは、次の手順は使用できません。

コード例 2-20 ドメインのポストマスターを作成するための変更文

```
dn: dc=sesta, dc=com, o=internet
changetype: modify
add: mailDomainReportAddress
mailDomainReportAddress: rfc822_Address
```

コード例 2-21 ドメインのポストマスターを作成するための LDIF レコード

```
dn: dc=sesta, dc=com, o=internet
objectClass: domain
objectClass: inetDomain
objectClass: mailDomain
description: DC node for sesta.com hosted domain
dc: sesta
inetDomainBaseDN: o=sesta.com, o=isp
inetDomainStatus: active
mailDomainStatus: active
mailRoutingHosts: manatee.sesta.com
mailDomainDiskQuota: 100000000
mailDomainMsgQuota: -1
mailClientAttachmentQuota: 5
mailDomainReportAddress: rfc822_Address
```

受信メッセージサイズの制限の設定

mailDomainMsgMaxBlocks 属性を使用すると、ドメイン内のユーザ宛てに送信されるメッセージサイズの制限を設定できます。メッセージサイズは、MTA ブロックサイズ (デフォルトは 1024 バイト) 単位で設定します。ユーザのブロック制限属性 mailMsgMaxBlocks が設定されている場合は、mailDomainMsgMaxBlocks は無視されます。次の例では、ブロックサイズが 1K バイトであると仮定して、制限を 1M バイトに設定しています。

注 この手順は、ダイレクト LDAP を使用してメールのルーティングを行うシステムだけで使用できます。dirsync を使用するシステムでは、次の手順は使用できません。

コード例 2-22 ドメインのメッセージサイズの制限を設定するための変更文

```
dn: dc=sesta, dc=com, o=internet
changetype: modify
add: mailDomainMsgMaxBlocks
mailDomainMsgMaxBlocks: 1000
```

コード例 2-23 ドメインのメッセージサイズの制限を設定するための LDIF レコード

```
dn: dc=sesta,dc=com,o=internet
objectClass: domain
objectClass: inetDomain
objectClass: mailDomain
description: DC node for sesta.com hosted domain
dc: sesta
inetDomainBaseDN: o=sesta.com,o=isp
inetDomainStatus: active
mailDomainStatus: active
mailRoutingHosts: manatee.sesta.com
mailDomainDiskQuota: 100000000
mailDomainMsgQuota: -1
mailClientAttachmentQuota: 5
mailDomainMsgMaxBlocks: 1000
```

ドメインの catch-all アドレスの指定

ドメインにメッセージが送信され、その受取人アドレスと一致するユーザまたはグループがない場合は、通常メッセージは差出人に返されます。しかし、そのようなメッセージをすべて受信するアドレスを指定することができます。これは **catch-all** アドレスと呼ばれます。catch-all アドレスは、`mailDomainCatchAllAddress` 属性を使用して指定します。

注 この手順は、ダイレクト LDAP を使用してメールのルーティングを行うシステムだけで使用できます。dirsync を使用するシステムでは、次の手順は使用できません。

コード例 2-24 catch-all アドレスを指定するための変更文

```
dn: dc=sesta,dc=com,o=internet
changetype: modify
add: mailDomainCatchAllAddress
mailDomainCatchAllAddress:rfc822_Address
```

コード例 2-25 catch-all アドレスを指定するための LDIF レコード

```
dn: dc=sesta,dc=com,o=internet
objectClass: domain
objectClass: inetDomain
objectClass: mailDomain
description: DC node for sesta.com hosted domain
dc: sesta
inetDomainBaseDN: o=sesta.com,o=isp
inetDomainStatus: active
mailDomainStatus: active
mailRoutingHosts: manatee.sesta.com
mailDomainDiskQuota: 100000000
mailDomainMsgQuota: -1
mailClientAttachmentQuota: 5
mailDomainCatchAllAddress: rfc822_Address
```

ファミリーアカウントのプロビジョニング

ファミリーアカウントは、同一ドメイン内の電子メールユーザのグループです。ファミリーアカウントは、ファミリーグループ管理者によって管理され、1人のユーザが請求対象ユーザとして指定されます。請求対象ユーザとは、このユーザグループの電子メールアカウントに対する請求の支払いを担当するユーザです。ファミリーグループ管理者は、グループのユーザの作成や削除、および新しく別のユーザをファミリー管理者にすることを担当するユーザです。メンバーとは、ファミリーグループ管理者の管理下にあるユーザのことで、メンバーの電子メール料金は請求対象ユーザにより支払われます。ファミリーアカウントとなるのは、通常は家族ですが、管理責任や請求責任をローカルで持つ必要がある部門組織がファミリーアカウントになる場合もあります。この章には、以下の節があります。

- 57 ページの「ファミリーアカウントの作成」
- 60 ページの「ファミリーグループ管理者の作成」

ファミリーアカウントの作成

ファミリーアカウントの管理と作成は、`imadmin` コマンドラインインタフェース (『iPlanet Messaging Server リファレンスマニュアル』を参照)、iPlanet Delegated Administrator for Messaging、または LDAP を使用して行うことができます。このマニュアルでは、LDAP を使用してプロビジョニングを行う方法について説明します。

LDAP を使用してファミリーアカウントのユーザのプロビジョニングを行うには、次の2つの手順を実行する必要があります。

1. ファミリーアカウントエントリを作成します (コード例 3-1)。
2. 「`memberOfManagedGroup: <FamilyGroupDN>`」という属性行をファミリーアカウント内の各ユーザのエントリに追加します (コード例 3-2)。

コード例 3-1 に、ファミリーアカウントエントリの例を示します。

コード例 3-1 ファミリーアカウントエントリ

```
dn: cn=gsWarriors, ou=groups, o=sesta.com, o=ISP
objectclass: inetManagedGroup
objectclass: nsManagedDept
mnggrpbillableuser: uid=attles, ou=People, o=sesta.com, o=ISP
mnggrpmailquota: 1024000
mnggrpcurrentusers: 0
mnggrpdeletionpolicy: delete
cn: gsWarriors
mnggrpstatus: active
mnggrpmaxusers: 1000
nsdamodifiableby: cn=Family Group
Administrators, cn=gsWarriors, ou=groups, o=sesta.com, o=ISP
```

- dn: cn=gsWarriors, ou=groups, o=sesta.com, o=ISP
ファミリーアカウントの識別名
- objectclass: inetManagedGroup
objectclass: nsManagedDept
inetManagedGroup は、ファミリーアカウントを表します。nsManagedDept は、iPlanet Delegated Administrator for Messaging によって使用される情報を格納します。
- mnggrpbillableuser: uid=attles, ou=People, o=sesta.com, o=ISP
このユーザグループに対する請求の支払いを担当するユーザの DN
- mnggrpmailquota: 1024000
グループ内のすべてのユーザに対する累積ディスク容量制限
- mnggrpcurrentusers: 0
グループ内の現在のユーザ数
- cn: gswarriors
ファミリーアカウントの共通名
- mnggrpstatus: active
グループの現在の状態。有効な値は、active、inactive、deleted のどれか1つです。inactive は、動作を一時停止します。deleted は、エントリに削除用のマークを付けます。ただし、ユーザには削除用のマークは付きません。値がない場合は、状態が active であることを示します。不正な値は、inactive として扱われます。
- mnggrpmaxusers: 1000
グループ内に許可されるユーザ数

- nsdamodifiableby: cn=Domain Organization Administrators, cn=gsWarriors,ou=groups,o=sesta.com,o=ISP

このファミリーグループを管理できるメンバーを含むグループを指定します。60ページの「ファミリーグループ管理者の作成」を参照してください。

ファミリーアカウントのエントリを作成したら、ユーザエントリ内の `memberOfManagedGroup` 属性をファミリーアカウントの DN に設定することによって、メンバーを追加します。次にコードの例を示します。

コード例 3-2 ファミリーグループのメンバーの LDIF レコード

```
dn: uid=Antwan,ou=people,o=sesta.com,o=ISP
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: inetUser
objectClass: ipUser
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: nsManagedPerson
objectClass: userPresenceProfile
cn: Antwan
sn: James
initials: AJ
givenName: Ant
mail: aj@sesta.com
mailAlternateAddress: ant@sesta.com
mailDeliveryOption: mailbox
mailHost: manatee.siroe.com
uid: Antwan
dataSource: iMS 5.0 @(#)ims50users.sh 1.5a 02/3/00
userPassword: {SHA}aluWfd0LYY9ImsJb3h4afrI4AXk=
mailAllowedServiceAccess: +imap, imaps, pop3, smtp, http:*
inetUserStatus: active
mailUserStatus: active
mailQuota: -1
mailMsgQuota: 100
memberOfManagedGroup: cn=gsWarriors, ou=groups,o=sesta.com,o=ISP
```

ファミリーグループ管理者の作成

Delegated Admin タスクユーティリティ: `imadmin family-admin add`

タスクの権限: トップレベル管理者、ドメイン管理者、またはファミリーグループ管理者

ファミリーグループ管理者は、ユーザの作成やファミリーグループからのユーザの削除を担当します。Delegated Administrator を使用してファミリーグループを作成した場合は、Family Group Administrators という別のグループがそのファミリーグループエントリの DN の下に作成されます。たとえば、次のファミリーグループを作成した場合、

```
cn=gsWarriors,ou=groups,o=sesta.com,o=isp
```

ファミリー管理者のグループも作成されます。その DN は次のようになります。

```
cn=Family Group Administrators,cn=gsWarriors,ou=groups,o=sesta.com,o=isp
```

このグループのメンバーは、ファミリーグループの管理権限を持ちます。次の例は、ファミリーグループ管理者のプロビジョニングを行う方法を示しています。

1. Family Group Administrators というグループが、ファミリーグループエントリの DN の下に作成されていることを確認し、ファミリーグループ管理者の DN を追加します。Delegated Administrator を使用してファミリーグループを作成した場合は、これは自動的に作成されます。

コード例 3-3 ファミリー管理者グループのエントリ

```
dn: cn=Family Group Administrators,cn=gsWarriors,ou=groups,o=sesta.com,o=isp
objectclass: groupOfUniqueNames
objectclass: nsManagedDept
cn: Organization Administrators
nsNumUsers: 1
nsMaxUsers: Unlimited
uniqueMember: uid=Dave,ou=people,ou=sesta.com,o=isp
```

2. 新しいファミリーグループ管理者のエントリに `memberof` 属性を追加します。

コード例 3-4 ファミリーグループ管理者のエントリ

```
dn: uid=Dave,ou=people,o=sesta.com,o=isp
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: inetUser
objectClass: ipUser
```

コード例 3-4 ファミリーグループ管理者のエントリ (続き)

```
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: nsManagedPerson
objectClass: userPresenceProfile
cn: Dave Cowins
sn: cowins
initials: DC
givenName: Dave
mail: Dave.Cowins@sesta.com
mailAlternateAddress: dcowins@florizel.com
mailDeliveryOption: mailbox
mailHost: manatee.siroe.com
uid: Dave
dataSource: iMS 5.0 @(#)ims50users.sh 1.5a 02/3/00
userPassword: {SHA}aluWfd0LYY9ImsJb3h4afrI4AXk=
mailAllowedServiceAccess: +imap, imaps, pop3, http:*
inetUserStatus: active
mailUserStatus: active
mailQuota: -1
mailMsgQuota: 100
memberOf: cn=Family Group Administrators,cn=gsWarriors,ou=groups,o=sesta.com,o=isp
```

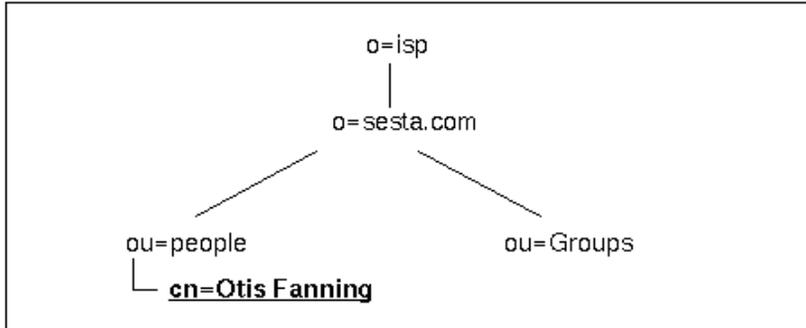
3. ACIはルートノードでトップレベルに設定されます。付録A「ルートとドメインのACIの例」を参照してください。

ユーザのプロビジョニング

この節では、iPlanet Messaging Server のユーザエントリを作成する方法について説明します。インストールを行うと、複数のユーザエントリが組織ツリー内に作成されます。ここで紹介する例では、これらのインストール時に作成されるユーザエントリを取り上げます。また、このマニュアルでは、属性の概要を説明します。属性の詳細は、『iPlanet スキーマリファレンスマニュアル』に記載されています。この章には、以下の節があります。

- 64 ページの「ユーザエントリの作成」
- 68 ページの「メールユーザのタスク」
 - 68 ページの「ユーザのアクティブ化と非アクティブ化」
 - 69 ページの「ユーザパスワードの変更」
 - 70 ページの「ユーザの Vacation メッセージの設定」
 - 72 ページの「使用可能なメールサービスの追加と削除」
 - 73 ページの「受信メール配信オプションの追加と変更」
 - 74 ページの「ユーザメッセージフィルタの設定」
 - 76 ページの「メールとメッセージの制限」
 - 77 ページの「メールの転送」
 - 78 ページの「新しいメールエイリアス」
 - 79 ページの「ユーザのメールサーバの変更」
 - 80 ページの「メーリングリストの作成権限の追加」
 - 81 ページの「受信メッセージサイズの制限」

ユーザエントリの作成



sesta.com の電子メールユーザは、組織ツリーの ou=people, o=sesta.com, o=isp 内に含まれています。各エントリはそのユーザの属性情報を含んでいます。次に LDIF の例を示します。

コード例 4-1 ユーザエントリの例

```
dn: uid=fanning,ou=people,o=sesta.com,o=ISP
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: inetUser
objectClass: ipUser
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: nsManagedPerson
objectClass: userPresenceProfile
cn: Otis Fanning
sn: fanning
initials: OTF
givenName: Otis
pabURI: ldap://ldap.siroe.com:389/ou=fanning,ou=people,o=sesta.com,o=isp,o=pab
mail: Otis.Fanning@sesta.com
mailAlternateAddress: ofanning@sesta.com
mailDeliveryOption: mailbox
mailHost: manatee.siroe.com
uid: fanning
dataSource: iMS 5.0 @(#)ims50users.sh 1.5a 02/3/00
userPassword: password
inetUserStatus: active
mailUserStatus: active
mailQuota: -1
mailMsgQuota: 100
```

ユーザエントリオブジェクトクラスと属性

- `dn: uid=fanning,ou=people,o=sesta.com,o=ISP`

ユーザ Otis Fanning の識別名です。uid に使用できない文字があることに注意してください。使用できない文字は、\$ ~ = # * + % ! @ , { } () / ¥ < > ; : " ' [] & ? DEL TAB、および最上位ビットが設定された文字とすべての制御文字です。

- `objectClass: person`
`objectClass: organizationalPerson`
`objectClass: inetOrgPerson`
`objectClass: inetUser`
`objectClass: ipUser`
`objectClass: inetMailUser`
`objectClass: inetLocalMailRecipient`
`objectClass: nsManagedPerson`
`objectClass: userPresenceProfile`

これらは、ユーザエントリオブジェクトクラスです。inetOrgPerson は、コアオブジェクトクラスで、organizationalPerson および person を継承します(プロビジョニングを実行する際、これらの2つのクラスを LDAP 追加 (add) 文に含める必要はありませんが、ここでは明確に説明するためにこれらのクラスを示しています)。

inetUser、inetMailUser、および ipUser は、メールユーザアカウントを作成するための属性を提供します。これらは、UID、ユーザパスワード、公開アドレス帳情報、メール配信情報などの属性を提供します。

inetLocalMailRecipient は、ローカルルーティング情報を提供します。

userPresenceProfile は、Vacation 属性をサポートします。

nsManagedPerson は、iPlanet Delegated Administrator for Messaging のサポート属性を提供します。

inetOrgPerson

- `cn: Otis Fanning`
`cn` (commonname) は、ユーザのフルネームを示します。これは、person オブジェクトクラスから継承されます。
- `sn: Fanning`
`sn` (surname) は、ユーザの姓 (ラストネーム) を示します。これは、person オブジェクトクラスから継承されます。
- `initials: OTF`
`initials` は、個人の名前のイニシャルの一部またはすべてを含んでいます。この例では、OTF は Otis Tiberus Fanning を意味します。

- `givenName: Otis`
`givenName` は、ユーザの名 (ファーストネーム) です。
- `mail: Otis.Fanning@sesta.com`
アドバタイズされたユーザの電子メールアドレス (RFC 822 形式) です。

inetUser

- `uid: fanning`
`uid` は、ユーザのログイン識別子です。この属性は、ドメイン内で一意にする必要があります。
- `userPassword: secret`
`userPassword` は、ユーザがアカウントにアクセスしてメールの送受信を行うためのユーザのパスワードを表す文字列です。
- `inetUserStatus: active`
すべてのディレクトリ使用可能サーバに対するユーザのグローバルステータスです。有効な値は、`active`、`inactive`、`deleted` です。値がない場合は、状態が `active` であることを示します。不正な値は、`inactive` として扱われます。

ipUser

このコアオブジェクトクラスは、メールやカレンダーなどのインターネットサービスをサポートします。このクラスは、個人アドレス帳やサービスクラス機能の属性を提供します。

- `pabURI: ldap://ldap.siroe.com:389/ou=fanning,ou=people,o=sesta.com,o=isp,o=pab`
このユーザ用の個人アドレスブックのエントリのコンテナを指定する LDAP URI。この URI は、通常、ユーザが個人アドレス帳エントリを作成するときにサーバによって設定されます。ただし、アドレス帳用に別の LDAP サーバを使用するようにサーバに強制する場合は、この属性を使用して適切な値をプロビジョニングします。

inetMailUser

- `dataSource: iPlanet Messaging Server 5.0 @(#)ims50users.sh`
タグまたは識別子を格納するテキストフィールドです。
- `mailDeliveryOption: mailbox`
受信者用に使用されるメール配信オプションです。`mailDeliveryOption` には複数の値を指定できます。使用可能な値は、`mailbox`、`native|unix`、`autoreply`、`program`、および `forward` です。
- `mailUserStatus: active`

単一値の属性です。メールユーザの状態を格納します。有効な値は、active、inactive、deleted、holdです。holdは、ユーザのInbox宛てのメールをすべて保留キューに送信し、IMAPとPOPによるメールボックスアクセスをすべて拒否することを示します。値がない場合は、状態がactiveであることを示します。不正な値は、inactiveとして扱われます。

- mailQuota: -1

ユーザのメールボックス用に使用できるディスク容量(バイト単位)です。0の値(または指定されていない場合)は、システムのデフォルト容量制限(iPlanet Consoleで指定)を意味します。-1は、使用容量に制限がないことを意味します。

- mailMsgQuota: 100

ユーザが使用できるメッセージの最大数です。この数は、ストア内のすべてのフォルダのメッセージの累計です。0の値(または指定されていない場合)は、システムのデフォルトの制限を意味します。-1(iPlanet ConsoleまたはiPlanet Delegated Administrator for Messagingで指定)は、メッセージ数に制限がないことを意味します。

inetLocalMailRecipient

- mailHost: manatee.siroe.com

このグループ宛てのメッセージの最終的なSMTP宛先となるMTAの完全修飾ホスト名です。

- mailAlternateAddress: ofanning@sesta.com

このユーザの別のRFC 822電子メールアドレスです。

userPresenceProfile

Vacation属性をサポートします。詳細は、『iPlanet スキーマリファレンスマニュアル』を参照してください。

nsManagedPerson

iPlanet Delegated Administrator for Messagingの属性をサポートします。

メールユーザのタスク

この節には、以下の項があります。

- 68 ページの「ユーザのアクティブ化と非アクティブ化」
- 69 ページの「ユーザパスワードの変更」
- 70 ページの「ユーザの Vacation メッセージの設定」
- 72 ページの「使用可能なメールサービスの追加と削除」
- 73 ページの「受信メール配信オプションの追加と変更」
- 74 ページの「ユーザメッセージフィルタの設定」
- 76 ページの「メールとメッセージの制限」
- 77 ページの「メールの転送」
- 78 ページの「新しいメールエイリアス」
- 79 ページの「ユーザのメールサーバの変更」
- 80 ページの「メーリングリストの作成権限の追加」
- 81 ページの「受信メッセージサイズの制限」

ユーザのアクティブ化と非アクティブ化

iPlanet Messaging Server は、ユーザのアクティブ化と非アクティブ化に使用できる `inetUserStatus` と `mailUserStatus` という 2 つの異なる状態属性を提供します。`inetUserStatus` 属性は、すべてのサービス (メール、カレンダーなど) のグローバルユーザ状態を保持し、`mailUserStatus` に設定された状態を無効にします。`mailUserStatus` は、メールサービスの状態だけを設定します。有効な値は、`active`、`inactive`、`deleted` です。`inetUserStatus` を `deleted` に設定すると、次のページサイクル中にエントリに削除用のマークが付きます。

`mailUserStatus` では、メールユーザの状態 (`active`、`inactive`、`deleted`、`hold` のどれか) を使用して各ユーザの状態を設定します。`mailUserStatus=hold` は、ユーザの **Inbox** 宛てのメールをすべて保留キューに送信し、**IMAP** と **POP** によるメールボックスアクセスをすべて拒否することを意味します。`mailUserStatus` を `delete` に設定すると、エントリに削除用のマークが付けられます。

次の LDIF 更新文は、ユーザがすべてのサービスを使用できないようにします。アクティブになっていないユーザ宛てにメールが送信されると、送信元の MTA に一時的なエラーが返されます。

```
dn: uid=fanning,ou=people,o=sesta.com,o=ISP
changetype: modify
replace: inetUserStatus
inetUserStatus: inactive
```

次の LDIF 更新文は、そのユーザのメールサービスだけを無効にします。カレンダーなどのそのユーザの他のサービスをプロビジョニングした場合、それらのサービスはアクティブのままになります。

```
dn: uid=fanning,ou=people,o=sesta.com,o=ISP
changetype: modify
replace: mailUserStatus
mailUserStatus: inactive
```

次の更新文は、そのユーザ宛てのメッセージを保留キューにリダイレクトします。この更新文は、あるメールサーバから別のサーバにユーザを移動するときを使用する場合があります。ユーザ宛ての受信メッセージは、保留キューにリダイレクトされます。そのユーザに対するメール配信を再び開始するには、mailUserStatus の設定を active に戻す必要があります。

```
dn: uid=fanning,ou=people,o=sesta.com,o=ISP
changetype: modify
replace: mailUserStatus
mailUserStatus: hold
```

ユーザパスワードの変更

userPassword 属性を変更することによって、ユーザのパスワードを変更できます。次の LDIF を使用してパスワードを変更できます。

```
dn: uid=fanning,ou=people,o=sesta.com,o=ISP
changetype: modify
replace: userPassword
userPassword: PAssWoRd
```

コード例 4-2 ユーザのパスワード変更後の LDIF レコード

```
dn: uid=fanning,ou=people,o=sesta.com,o=ISP
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: inetUser
objectClass: ipUser
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: nsManagedPerson
objectClass: userPresenceProfile
```

コード例 4-2 ユーザのパスワード変更後の LDIF レコード (続き)

```

cn: Otis Fanning
sn: fanning
initials: OTF
givenName: Otis
mail: Otis.Fanning@sesta.com
mailAlternateAddress: ofanning@sesta.com
mailDeliveryOption: mailbox
mailHost: manatee.siroe.com
uid: fanning
dataSource: iMS 5.0 @(#)ims50users.sh 1.5a 02/3/00
userPassword: PAssWoRd
inetUserStatus: active
mailUserStatus: active
mailQuota: -1
mailMsgQuota: 100

```

ユーザの Vacation メッセージの設定

Vacation メッセージは、オブジェクトクラス `userPresenceProfile` (`vacationStartDate`、`vacationEndDate` 属性) および `inetMailUser` (`mailAutoreplyMode`、`mailAutoreplyTimeout`、`mailAutoreplySubject`、`mailAutoreplyText`、`mailAutoreplyTextInternal`、`mailDeliveryOption` 属性) を使用して設定します。

各属性の意味の詳細については、『iPlanet スキーマリファレンスマニュアル』を参照してください。

次の LDIF ファイルの例は、2001 年 2 月 15 日から始まり、2001 年 2 月 20 日に終わるユーザの Vacation メッセージを設定します。自動応答のタイムアウトは 2 日です。

Vacation メッセージの件名は、「I am on vacation」です。メッセージの本文は、「Please contact me later」です。本文は、同一ドメイン向けの内部用の場合も、その他のユーザ向けの外部用の場合も、同じものを使用します。

```

dn: uid=fanning,ou=people,o=sesta.com,o=ISP
changetype: modify
add: mailDeliveryOption:
mailDeliveryOption: autoreply
-
replace: mailAutoreplyMode
mailAutoreplyMode: reply
-
replace: vacationStartDate
vacationStartDate: 20010215000000Z
-
replace: vacationEndDate

```

```

vacationEndDate: 20010220000000Z
-
replace: mailAutoreplyTimeout
mailAutoreplyTimeout: 48
-
replace: mailAutoreplySubject
mailAutoreplySubject: I am on vacation
-
replace: mailAutoreplyTextInternal
mailAutoreplyTextInternal: Please contact me later.
-
replace: mailAutoreplyText
mailAutoreplyText: Please contact me later.

```

日付は、世界協定時刻 (UTC) で設定します。これは、以前はグリニッジ標準時 (GMT) として知られていた国際標準時間です。異なる時間帯を使用している場合は、対応する UTC 時間に設定する必要があります。たとえば、Vacation を太平洋標準時の 2001 年 2 月 15 日の深夜に設定する場合は、8 時間引きます。

コード例 4-3 ユーザの自動応答 Vacation メッセージを設定して有効にした後の LDIF レコード

```

dn: uid=fanning,ou=people,o=sesta.com,o=ISP
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: inetUser
objectClass: ipUser
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: nsManagedPerson
objectClass: userPresenceProfile
cn: Otis Fanning
sn: fanning
initials: OTF
givenName: Otis
mail: Otis.Fanning@sesta.com
mailAlternateAddress: ofanning@sesta.com
mailDeliveryOption: mailbox
mailHost: manatee.siroe.com
uid: fanning
dataSource: iMS 5.0 @(#)ims50users.sh 1.5a 02/3/00
userPassword: password
inetUserStatus: active
mailUserStatus: active
mailQuota: -1
mailMsgQuota: 100
mailDeliveryOption: autoreply
mailAutoreplyMode: reply
vacationStartDate: 20010215000000Z

```

コード例 4-3 ユーザの自動応答 Vacation メッセージを設定して有効にした後の LDIF レコード (続き)

```
vacationEndDate: 20010220000000Z
mailAutoreplyTimeout: 48
mailAutoreplySubject: I am on vacation
mailAutoreplyTextInternal: Please contact me later.
mailAutoreplyText: Please contact me later.
```

使用可能なメールサービスの追加と削除

使用可能なメールサービスは、mailAllowedServiceAccess 属性で設定します。使用可能な値は、imap、imaps、pop3、http です。形式は次のとおりです。

```
mailAllowedServiceAccess: +<Allowed Services>:*
```

使用可能なサービスのシンタックスについては、iPlanet Message Server 管理者ガイドの「フィルタの構文」の節を参照してください。次の LDIF 変更コードは、Otis Fanning 用のサービスに IMAP、POP3、および HTTP (Messenger Express) サポートを追加します。

```
dn: uid=fanning,ou=people,o=sesta.com,o=ISP
changetype: modify
replace: mailAllowedServiceAccess
mailAllowedServiceAccess: +smtp:ALL$+imap:ALL$+pop:ALL$+http:ALL
```

コード例 4-4 ユーザのメールサービス変更後の LDIF レコード

```
dn: uid=fanning,ou=people,o=sesta.com,o=ISP
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: inetUser
objectClass: ipUser
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: nsManagedPerson
objectClass: userPresenceProfile
cn: Otis Fanning
sn: fanning
initials: OTF
givenName: Otis
mail: Otis.Fanning@sesta.com
mailAlternateAddress: ofanning@sesta.com
mailDeliveryOption: mailbox
mailHost: manatee.siroe.com
uid: fanning
dataSource: iMS 5.0 @(#)ims50users.sh 1.5a 02/3/00
userPassword: password
```

コード例 4-4 ユーザのメールサービス変更後の LDIF レコード (続き)

```

mailAllowedServiceAccess: +smtp:ALL$+imap:ALL$+pop:ALL$+http:ALL
inetUserStatus: active
mailUserStatus: active
mailQuota: -1
mailMsgQuota: 100

```

受信メール配信オプションの追加と変更

mailDeliveryOption 属性は、受信メッセージの送信先を制御します。送信先としては、メッセージストア (mailbox)、/var/mail (native)、自動応答機能 (autoreply)、別のメールアドレスへの転送 (forward)、承認されたメール処理プログラム (program) を選択できます。この属性には、複数の値を指定できます。mailDeliveryOption を program に設定する場合は、mailProgramDeliveryInfo を設定する必要があります (プログラム配信の詳細は『iPlanet Message Server 管理者ガイド』を参照)。

次の LDIF データは、メッセージストアと /var/mail にメッセージを送信します。

```

dn: uid=fanning,ou=people,o=sesta.com,o=ISP
changetype: modify
add: mailDeliveryOption:
mailDeliveryOption: native

```

コード例 4-5 ユーザのメール配信オプションを変更するための LDIF レコード

```

dn: uid=fanning,ou=people,o=sesta.com,o=ISP
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: inetUser
objectClass: ipUser
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: nsManagedPerson
objectClass: userPresenceProfile
cn: Otis Fanning
sn: fanning
initials: OTF
givenName: Otis
mail: Otis.Fanning@sesta.com
mailAlternateAddress: ofanning@sesta.com
mailDeliveryOption: native
mailDeliveryOption: mailbox
mailHost: manatee.siroe.com
uid: fanning
dataSource: iMS 5.0 @(#)ims50users.sh 1.5a 02/3/00

```

コード例 4-5 ユーザのメール配信オプションを変更するための LDIF レコード (続き)

```
userPassword: password
inetUserStatus: active
mailUserStatus: active
mailQuota: -1
mailMsgQuota: 100
```

ユーザメッセージフィルタの設定

iPlanet Messaging Server は、SIEVE メールフィルタリング言語をサポートします。この言語を使用して、指定した文字列を含むメッセージや指定した長さを超えるメッセージのブロック、保管、リダイレクトを行うメッセージフィルタを作成することができます。ユーザは、フィルタリングの規則と処理を iPlanet Delegated Administrator for Messaging を使用するか、または LDAP の mailSieveRuleSource 属性を使用して指定できます。ただし、LDAP で mailSieveRuleSource 属性を追加することによって作成したメッセージフィルタを、iPlanet Delegated Administrator for Messaging を使用して変更することはできません。iPlanet Delegated Administrator for Messaging では、LDAP で作成したメッセージフィルタの表示と削除はできますが、編集はできません。iPlanet Messaging Server は、インターネット草案 "Sieve: A Mail Filtering Language"、T. Showalter、draft 9 (<http://docs.iplanet.com/docs/sieve>) に記載された SIEVE 規則をサポートします。次に SIEVE を使用したメールフィルタリングの例を示します。

注 iPlanet Delegated Administrator for Messaging には、最も一般的に使用するメールフィルタのテンプレートが用意されています。iPlanet Delegated Administrator for Messaging メールフィルタおよびテンプレートの作成と変更の方法については、『iPlanet Message Server 管理者ガイド』を参照してください。

この例では、mailSieveRuleSource の値はファイルに格納され、その値は、ldapmodify コマンドで -b フラグを入力することによってエンコードされます。

- 変更エントリファイル modfanning.ldif は次のコードを含みます。

```
dn: uid=fanning,ou=people,o=sesta.com,o=ISP
changetype: modify
add: mailSieveRuleSource
mailSieveRuleSource: /export/example/maillsievesource.txt
```
- maillsievesource.txt は次のコードを含みます。

```

require ["fileinto", "reject"];
if header :contains "Subject" "New Rules Suggestion"
    {redirect "rules@sesta.com" # Forward message }
elsif header :contains "Sender" "porn.com"
    {discard text:
Your message has been rejected.Please remove this address from
your mailing list.# メッセージを拒否し、応答メッセージを送信します
.
    ;}
elsif size :over 1M
    { reject text:
Please do not send me large attachments.
Put your file on a server and send me the URL.
Thank you.# メッセージを破棄し、応答メッセージを送信します
.
    ;}
elsif header :contains "Sender" "barkley@sesta.com"
    { fileinto "complaints.refs"; # file message}

```

- 変更コマンドは次のとおりです。

```

ldapmodify -D "cn=Directory Manager" -w password -b -f
modfanning.ldif

```

コード例 4-6 ユーザのメッセージフィルタを設定した後の LDIF レコード (ldapsearch に -o フラグを指定して表示)

```

dn: uid=fanning,ou=people,o=sesta.com,o=ISP
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: inetUser
objectClass: ipUser
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: nsManagedPerson
objectClass: userPresenceProfile
cn: Otis Fanning
sn: fanning
initials: OTF
givenName: Otis
mail: Otis.Fanning@sesta.com
mailAlternateAddress: ofanning@sesta.com
mailDeliveryOption: mailbox
mailHost: manatee.siroe.com
uid: fanning
dataSource: iMS 5.0 @(#)ims50users.sh 1.5a 02/3/00
userPassword: password
inetUserStatus: active
mailUserStatus: active

```

コード例 4-6 ユーザのメッセージフィルタを設定した後の LDIF レコード (ldapsearch に -o フラグを指定して表示) (続き)

```

mailQuota: -1
mailMsgQuota: 100
mailSieveRuleSource:
require ["fileinto", "reject"];
if header :contains "Subject" "New Rules Suggestion"
    { redirect "rules@sesta.com" # Forward message }
elseif header :contains "Sender" "porn.com"
    { discard text:
Your message has been rejected.Please remove this address from
your mailing list.# メッセージを拒否し、応答メッセージを送信します
.
    ; }
elseif size :over 1M
    { reject text:
Please do not send me large attachments.
Put your file on a server and send me the URL.
Thank you.# メッセージを破棄し、応答メッセージを送信します
.
    ; }
elseif header :contains "Sender" "barkley@sesta.com"
    { fileinto "complaints.refs"; #file message}

```

メールとメッセージの制限

ユーザのメールボックスのディスク容量制限を設定するには、mailQuota 属性 (バイト単位) を指定します。ユーザが使用できるメールストア内のメッセージの最大数を設定するには、mailMsgQuota を使用します。mailQuota=-2 の値の場合、または属性を定義していない場合は、システムのデフォルトの容量 (iPlanet Console または変数 store.defaultmessagequota で指定) が使用されます。mailQuota=-1 の値は、メッセージ数に制限がないことを意味します。mailQuota=0 の値は、メッセージは一切保存されないことを意味します。

次の LDIF 変更コードは、このユーザのメール容量制限を無制限に設定し、メッセージ数の制限を 2000 に設定します。

```

dn: uid=fanning,ou=people,o=sesta.com,o=ISP
changetype: modify
replace: mailQuota
mailQuota: -1
-
replace: mailMsgQuota
mailMsgQuota: 2000

```

コード例 4-7 ユーザのメールボックスとメッセージ数の制限を設定するための LDIF レコード

```
dn: uid=fanning,ou=people,o=sesta.com,o=ISP
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: inetUser
objectClass: ipUser
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: nsManagedPerson
objectClass: userPresenceProfile
cn: Otis Fanning
sn: fanning
initials: OTF
givenName: Otis
mail: Otis.Fanning@sesta.com
mailAlternateAddress: ofanning@sesta.com
mailDeliveryOption: mailbox
mailHost: manatee.siroe.com
uid: fanning
dataSource: ims 5.0 @(#)ims50users.sh 1.5a 02/3/00
userPassword: password
inetUserStatus: active
mailUserStatus: active
mailQuota: -1
mailMsgQuota: 2000
```

メールの転送

メールを転送するには、`mailDeliveryOption` を `forward` に設定し、`mailForwardingAddress` を転送先の電子メールアドレスに設定します。`mailForwardingAddress` には複数の値を指定できます。次の例では、メールをユーザのメールボックスに送信し、さらにそのメールを `fastjonny@varrius.com` と `John@florizel.net` に転送します。`mailDeliveryOption` を `mailbox` に設定しているため、メッセージはそのユーザの `Inbox` にも配信されることに注意してください。

```
dn: uid=fanning,ou=people,o=sesta.com,o=ISP
changetype: modify
add: mailDeliveryOption:
mailDeliveryOption: forward
-
replace: mailForwardingAddress
mailForwardingAddress: fastjonny@varrius.com
mailForwardingAddress: John@florizel.net
```

コード例 4-8 ユーザのメール転送アドレスを追加するための LDIF レコード

```

dn: uid=fanning,ou=people,o=sesta.com,o=ISP
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: inetUser
objectClass: ipUser
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: nsManagedPerson
objectClass: userPresenceProfile
cn: Otis Fanning
sn: fanning
initials: OTF
givenName: Otis
mail: Otis.Fanning@sesta.com
mailAlternateAddress: ofanning@sesta.com
mailDeliveryOption: mailbox
mailDeliveryOption: forward
mailForwardingAddress: fastjonny@varrius.com
mailForwardingAddress: john@florizel.com
mailHost: manatee.siroe.com
uid: fanning
dataSource: ims 5.0 @(#)ims50users.sh 1.5a 02/3/00
userPassword: password
inetUserStatus: active
mailUserStatus: active
mailQuota: -1
mailMsgQuota: 100

```

新しいメールエイリアス

ユーザは、1つのメールアカウントで複数の別の電子メールアドレスを使用できます。これを行うには、使いたい別のアドレスを `mailAlternateAddress` に設定します。この属性を `@<domain_name>` に設定すると、catch-all アドレス (MTA が正確に一致するアドレスを見つけない場合に、ドメイン内の特定のアドレス宛てのすべてのメッセージを受信するアドレス) を作成できます。

次の変更文は、Otis Fanning 用のその他のアドレスを追加します。

```

dn: uid=fanning,ou=people,o=sesta.com,o=ISP
changetype: modify
replace: mailAlternateAddress
mailAlternateAddress: ofanning@sesta.com

```

コード例 4-9 ユーザのメールアドレスエイリアスを追加するための LDIF レコード

```
dn: uid=fanning,ou=people,o=sesta.com,o=ISP
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: inetUser
objectClass: ipUser
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: nsManagedPerson
objectClass: userPresenceProfile
cn: Otis Fanning
sn: fanning
initials: OTF
givenName: Otis
mail: Otis.Fanning@sesta.com
mailAlternateAddress: ofanning@sesta.com
mailDeliveryOption: mailbox
mailHost: manatee.siroe.com
uid: fanning
dataSource: ims 5.0 @(#)ims50users.sh 1.5a 02/3/00
userPassword: password
inetUserStatus: active
mailUserStatus: active
mailQuota: -1
mailMsgQuota: 100
```

ユーザのメールサーバの変更

ユーザのメールサーバ(この受信者宛てのメッセージの最終的な SMTP 宛先となる MTA の完全修飾ホスト名)を変更するには、mailhost に新しいサーバを指定します。

```
dn: uid=fanning,ou=people,o=sesta.com,o=ISP
changetype: modify
replace: mailhost
mailhost: buffalo.siroe.com
```

コード例 4-10 ユーザのメールサーバを変更するための LDIF レコード

```
dn: uid=fanning,ou=people,o=sesta.com,o=ISP
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: inetUser
objectClass: ipUser
```

コード例 4-10 ユーザのメールサーバを変更するための LDIF レコード (続き)

```
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: nsManagedPerson
objectClass: userPresenceProfile
cn: Otis Fanning
sn: fanning
initials: OTF
givenName: Otis
mail: Otis.Fanning@sesta.com
mailAlternateAddress: ofanning@sesta.com
mailDeliveryOption: mailbox
mailHost: buffalo.siroe.com
uid: fanning
dataSource: iMS 5.0 @(#)ims50users.sh 1.5a 02/3/00
userPassword: password
inetUserStatus: active
mailUserStatus: active
mailQuota: -1
mailMsgQuota: 100
```

メーリングリストの作成権限の追加

メーリングリストの作成を許可するには、属性値のペア `nsDACapability: mailListCreate` をユーザのエントリに追加します。

```
dn: uid=fanning,ou=people,o=sesta.com,o=ISP
changetype: modify
add: nsDACapability
nsDACapability: yes
```

コード例 4-11 ユーザのメールサーバを変更するための LDIF レコード

```
dn: uid=fanning,ou=people,o=sesta.com,o=ISP
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: inetUser
objectClass: ipUser
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: nsManagedPerson
objectClass: userPresenceProfile
cn: Otis Fanning
sn: fanning
initials: OTF
givenName: Otis
mail: Otis.Fanning@sesta.com
mailAlternateAddress: ofanning@sesta.com
```

コード例 4-11 ユーザのメールサーバを変更するための LDIF レコード (続き)

```

mailDeliveryOption: mailbox
mailHost: manatee.siroe.com
nsDACapability: mailListCreate
uid: fanning
dataSource: iMS 5.0 @(#)ims50users.sh 1.5a 02/3/00
userPassword: password
inetUserStatus: active
mailUserStatus: active
mailQuota: -1
mailMsgQuota: 100

```

受信メッセージサイズの制限

ユーザやグループが受信できるメッセージのサイズを制限するには、属性 `mailMsgMaxBlocks` を使用します。メッセージサイズは、MTA ブロックサイズ (デフォルトは 1024 バイト) 単位で設定します。この属性は、`mailDomainMsgMaxBlocks` よりも優先されます。次の例では、制限を 1M バイトに設定します。

```

dn: uid=fanning,ou=people,o=sesta.com,o=ISP
changetype: modify
add: mailMsgMaxBlocks
mailMsgMaxBlocks: 1000

```

コード例 4-12 ユーザのメールサーバを変更するための LDIF レコード

```

dn: uid=fanning,ou=people,o=sesta.com,o=ISP
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: inetUser
objectClass: ipUser
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: nsManagedPerson
objectClass: userPresenceProfile
cn: Otis Fanning
sn: fanning
initials: OTF
givenName: Otis
mail: Otis.Fanning@sesta.com
mailAlternateAddress: ofanning@sesta.com
mailDeliveryOption: mailbox
mailHost: manatee.siroe.com
mailMsgMaxBlocks: 1000
uid: fanning
dataSource: iMS 5.0 @(#)ims50users.sh 1.5a 02/3/00

```

コード例 4-12 ユーザのメールサーバを変更するための LDIF レコード (続き)

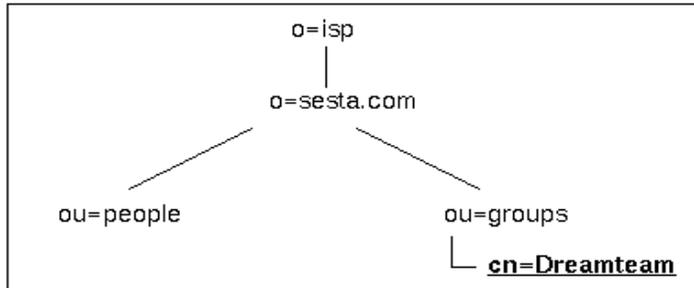
```
userPassword: password
inetUserStatus: active
mailUserStatus: active
mailQuota: -1
mailMsgQuota: 100
```

メーリングリストのプロビジョニング

この節では、iPlanet Messaging Server でメーリングリストエントリを作成する方法について説明します。インストールを行うと、メーリングリストエントリが組織ツリー内に作成されます。SIMS DC ツリーを使用しているシステムの場合は、メーリングリストエントリは DC ツリー内に作成されます。このマニュアルでは、属性の概要を説明します。属性の詳細は、『iPlanet スキーマリファレンスマニュアル』に記載されています。

- 84 ページの「メーリングリストエントリの作成」
- 87 ページの「メーリングリストのタスク」
 - 86 ページの「属性値の形式」
 - 87 ページの「メーリングリスト所有者の割り当て」
 - 88 ページの「メンバーの追加」
 - 89 ページの「メーリングリストへの投稿の制限の作成」
 - 93 ページの「メーリングリストのモデレータ」
 - 94 ページの「メーリングリストの有効化、無効化、削除」
 - 94 ページの「メッセージのファイルへのアーカイブ」
 - 95 ページの「リクエストアドレス」
 - 96 ページの「メーリングリストメンバーの表示」
 - 97 ページの「メーリングリストの参加可能者」
 - 98 ページの「動的なメーリングリストの作成」
 - 99 ページの「受信メッセージサイズの制限」

メーリングリストエントリの作成



メーリングリストエントリは、組織ツリーの ou=group コンテナ内に作成されます。次にメーリングリスト用の LDIF レコードの例を示します。

コード例 5-1 メーリングリスト用の LDIF レコード

```
dn: cn=Dreamteam,ou=groups,o=sesta.com,o=isp
cn: Dreamteam
objectClass: groupOfUniqueNames
objectClass: inetMailGroup
objectClass: inetLocalMailRecipient
objectClass: inetMailGroupManagement
objectClass: nsManagedMailList
uniqueMember: uid=baylor,ou=People,o=sesta.com,o=isp
uniqueMember: uid=bird,ou=People,o=sesta.com,o=isp
uniqueMember: uid=jordan,ou=People,o=sesta.com,o=isp
uniqueMember: uid=jabbar,ou=People,o=sesta.com,o=isp
uniqueMember: uid=magic,ou=People,o=sesta.com,o=isp
mgrpRFC822MailMember: west@florizel.com
mgrpRFC822MailMember: robertson@florizel.com
mail: dreamteam@sesta.com
mailAlternateAddress: thegreatest@sesta.com
mailHost: manatee.siroe.com
dataSource: @(#)ims50users.sh 1.5a 02/3/00
inetMailGroupStatus: active
nsNumUsers: 7
nsMaxUsers: 1000
```

メールリストの属性

- dn: cn=Dreamteam,ou=groups,o=sesta.com,o=isp
メーリングリストの識別名です。

- `objectClass: groupOfUniqueNames`
`objectClass: inetMailGroup`
`objectClass: inetLocalMailRecipient`
`objectClass: inetMailGroupManagement`
`objectClass: nsManagedMailList`

`groupOfUniqueNames` は、すべてのメーリングリストエントリ用のコアオブジェクトクラスです。メールサービスオブジェクトクラス `inetMailGroup` および `inetLocalMailRecipient` と、**Delegated Administrator** サービスオブジェクトクラス `inetMailGroupManagement` をオーバーレイすると、そのエントリがメッセージングサーバで使用されるメーリングリストになります。

`inetMailGroup` は、メーリングリストの属性を指定します。

`inetLocalMailRecipient` は、内部ルーティング属性を提供します。このオブジェクトクラスは、プライベートエンタープライズ内に限定した RFC 822 ベースの電子メールをルーティングする SMTP メッセージ転送エージェントをサポートすることを目的としており、公共のインターネット上で電子メールをルーティングするプロセスでは使用されません。

`inetMailGroupManagement` は、メーリングリストを管理するための属性を指定します。

`nsManagedMailList` は、メーリングリストに関する iPlanet Delegated Administrator for Messaging のサポート属性を提供します。

groupOfUniqueNames

- `cn: Dreamteam`
`cn` (commonname) はメーリングリストの名前です。
- `uniqueMember: uid=baylor,ou=People,o=sesta.com,o=isp`
`uniqueMember: uid=bird,ou=People,o=sesta.com,o=isp`
`uniqueMember: uid=jordan,ou=People,o=sesta.com,o=isp`
`uniqueMember: uid=jabbar,ou=People,o=sesta.com,o=isp`
`uniqueMember: uid=magic,ou=People,o=sesta.com,o=isp`

これらは、このディレクトリ内のユーザとして解決されるメーリングリストのメンバーです。

inetMailGroup

- `inetMailGroupStatus: active`

メーリングリストの現在の状態を示します。有効な値は、`active`、`inactive`、`deleted` です。値がない場合は、状態が `active` であることを示します。不正な値は、`inactive` として扱われます。

- `dataSource: @(#) ims50users.sh 1.5a 02/3/00`
タグまたは識別子を格納するテキストフィールドです。
- `mgrpRFC822MailMember: west@florizel.com`
`mgrpRFC822MailMember: robertson@florizel.com`
メーリングリストの外部メンバーです。

inetLocalMailRecipient

- `mail: dreamteam@sesta.com`
アドパタイズされたメーリングリストの電子メールアドレス (RFC 822 形式) です。
- `mailAlternateAddress: thegreatest@sesta.com`
このメーリングリストのその他の RFC 822 電子メールアドレスです。
- `mailHost: manatee.siroe.com`
このメーリングリスト宛でのメッセージの最終的な SMTP 宛先となる MTA サーバの完全修飾ホスト名です。

nsManagedMailList

- `nsNumUsers: 7`
現在のユーザエントリの数です。
- `nsMaxUsers: 1000`
ユーザエントリの最大数です。

属性値の形式

`moderator` や `mailDeliveryURL` など、ユーザアドレスや URL として指定されたファイル名を必要とする属性がいくつかあります。エントリの前に `ldap:///` が付いている場合、そのエントリは LDAP エントリとして扱われ、残りの値はエントリの識別名として扱われます。たとえば、以下のように記述します。

```
moderator: ldap:///uid=cox,ou=people,o=sesta,o=isp
```

属性と値のペアが 2 行にわたる場合は、2 行目の先頭に空白を置く必要があります。

mailto: ofanning@sesta.com のようにエントリの前に mailto: が付いている場合、そのエントリはメールアドレスとして解釈されます。

エントリの前に file:/// が付いている場合、そのエントリはファイルとして解釈されます。例:

```
mailDeliveryURL:file:///home/dogboy/dr_j/mail_archive.htm
```

メーリングリストのタスク

- 86 ページの「属性値の形式」
- 87 ページの「メーリングリスト所有者の割り当て」
- 88 ページの「メンバーの追加」
- 89 ページの「メーリングリストへの投稿の制限の作成」
- 93 ページの「メーリングリストのモデレータ」
- 94 ページの「メーリングリストの有効化、無効化、削除」
- 94 ページの「メッセージのファイルへのアーカイブ」
- 95 ページの「リクエストアドレス」
- 96 ページの「メーリングリストメンバーの表示」
- 97 ページの「メーリングリストの参加可能者」
- 98 ページの「動的なメーリングリストの作成」
- 99 ページの「受信メッセージサイズの制限」

メーリングリスト所有者の割り当て

メーリングリスト所有者は、リストのメンバーの追加や削除を実行できます。メーリングリストの所有者を変更するには、DN を owner 属性に割り当てます。メーリングリストの所有者は複数指定できますが、各所有者はメーリングリストと同じディレクトリ内に DN を持っている必要があります。次に変更文と LDIF レコードの例を示します。

```
dn: cn=Dreamteam,ou=groups,o=sesta.com,o=isp
changetype: modify
add: owner
owner: uid=baylor,ou=People,o=sesta.com,o=isp
```

コード例 5-2 所有者を指定したメーリングリストの LDIF レコード

```
dn: cn=Dreamteam,ou=groups,o=sesta.com,o=isp
cn: Dreamteam
objectClass: groupOfUniqueNames
objectClass: inetMailGroup
objectClass: inetLocalMailRecipient
objectClass: inetMailGroupManagement
objectClass: nsManagedMailList
uniqueMember: uid=baylor,ou=People,o=sesta.com,o=isp
uniqueMember: uid=bird,ou=People,o=sesta.com,o=isp
uniqueMember: uid=jordan,ou=People,o=sesta.com,o=isp
uniqueMember: uid=jabbar,ou=People,o=sesta.com,o=isp
uniqueMember: uid=magic,ou=People,o=sesta.com,o=isp
mgrpRFC822MailMember: west@florizel.com
mgrpRFC822MailMember: robertson@florizel.com
mail: dreamteam@sesta.com
mailAlternateAddress: thegreatest@sesta.com
mailHost: manatee.siroe.com
dataSource: @(#)ims50users.sh 1.5a 02/3/00
inetMailGroupStatus: active
nsNumUsers: 7
nsMaxUsers: 1000
owner: uid=baylor,ou=People,o=sesta.com,o=isp
```

メンバーの追加

内部メンバー (解決可能 DN を持つメンバー) を追加するには、そのメンバーの DN を uniqueMember 属性に割り当てます。外部メンバーを追加するには、それらのメンバーの電子メールアドレスを mgrpRFC822MailMember 属性に割り当てます。次の LDIF コードの例は、内部ユーザと外部ユーザを追加する方法を示しています。

```
dn: cn=Dreamteam,ou=groups,o=sesta.com,o=isp
changetype: modify
add: uniqueMember
uniqueMember: uid=russell,ou=People,o=sesta.com,o=isp
-
add: mgrpRFC822MailMember
mgrpRFC822MailMember: chamberlain@varrius.com
```

コード例 5-3 メンバーを追加したメーリングリストの LDIF レコード

```
dn: cn=Dreamteam,ou=groups,o=sesta.com,o=isp
cn: Dreamteam
objectClass: groupOfUniqueNames
```

コード例 5-3 メンバーを追加したメーリングリストの LDIF レコード (続き)

```
objectClass: inetMailGroup
objectClass: inetLocalMailRecipient
objectClass: inetMailGroupManagement
objectClass: nsManagedMailList
uniqueMember: uid=baylor,ou=People,o=sesta.com,o=isp
uniqueMember: uid=bird,ou=People,o=sesta.com,o=isp
uniqueMember: uid=jordan,ou=People,o=sesta.com,o=isp
uniqueMember: uid=jabbar,ou=People,o=sesta.com,o=isp
uniqueMember: uid=magic,ou=People,o=sesta.com,o=isp
mgrpRFC822MailMember: west@florizel.com
mgrpRFC822MailMember: robertson@florizel.com
uniqueMember: uid=russell,ou=People,o=sesta.com,o=isp
mgrpRFC822MailMember: chamberlain@varrius.com
mail: dreamteam@sesta.com
mailAlternateAddress: thegreatest@sesta.com
mailHost: manatee.siroe.com
dataSource: @(#)ims50users.sh 1.5a 02/3/00
inetMailGroupStatus: active
nsNumUsers: 7
nsMaxUsers: 1000
owner: uid=baylor,ou=People,o=sesta.com,o=isp
```

メーリングリストへの投稿の制限の作成

メーリングリストへの受信メールは、ドメインまたはユーザごとに制限できます。制限の属性は以下のとおりです。

- `mgrpAllowedBroadcaster` は、メーリングリストへのメッセージ送信を許可するアドレスを指定します。この属性が LDIF レコードに含まれていない場合は、そのリストは制限されず、すべてのユーザがメッセージを送信できます。MTA がメッセージをメンバーのリストにルーティングするには、エンベロープの `From:` アドレスが、許可されているリスト内のいずれかのアドレスと一致している必要があります。
- `mgrpDisallowedBroadcaster` は、メーリングリストへのメッセージ投稿を許可しないアドレスを指定します。差出人のアドレスは、この属性内のアドレスと比較されます。一致するアドレスがある場合、メッセージは拒否されます。

`mgrpAllowedBroadcaster` または `mgrpDisallowedBroadcaster` は静的なグループのアドレスに設定できますが、入れ子のグループ (グループ内に含まれるグループ) はサポートされません。特定の投稿者について設定する場合は、これらの属性を特定の許可された投稿者のアドレスに設定するか、または動的なグループ (URL 基準を使用した LDAP 検索) として指定します。

- `mgrpAllowedDomain` は、メーリングリストへのメッセージ投稿を許可するユーザドメイン名を指定します。ワイルドカード文字は「*」です。オプションで、ワイルドカード文字を使用してサブドメインを置き換えることにより、特定のトップドメインまたはサブドメインの下の DNS 階層全体を承認することができます。

注 `mgrpAllowedBroadcaster` または `mgrpDisallowedBroadcaster` は静的なグループのアドレスに設定できますが、入れ子のグループ (グループ内に含まれるグループ) はサポートされません。特定の投稿者について設定する場合は、これらの属性を特定の投稿者のアドレスに設定します。

- `mgrpDisallowedDomain` は、メーリングリストへのメッセージ投稿を拒否するユーザドメイン名を定義します。

注 `mgrpAllowedBroadcaster`、`mgrpDisallowedBroadcaster` の DN 値には、`ldap:///` または `mailto:` のプレフィックスを付ける必要があります。86 ページの「属性値の形式」を参照してください。

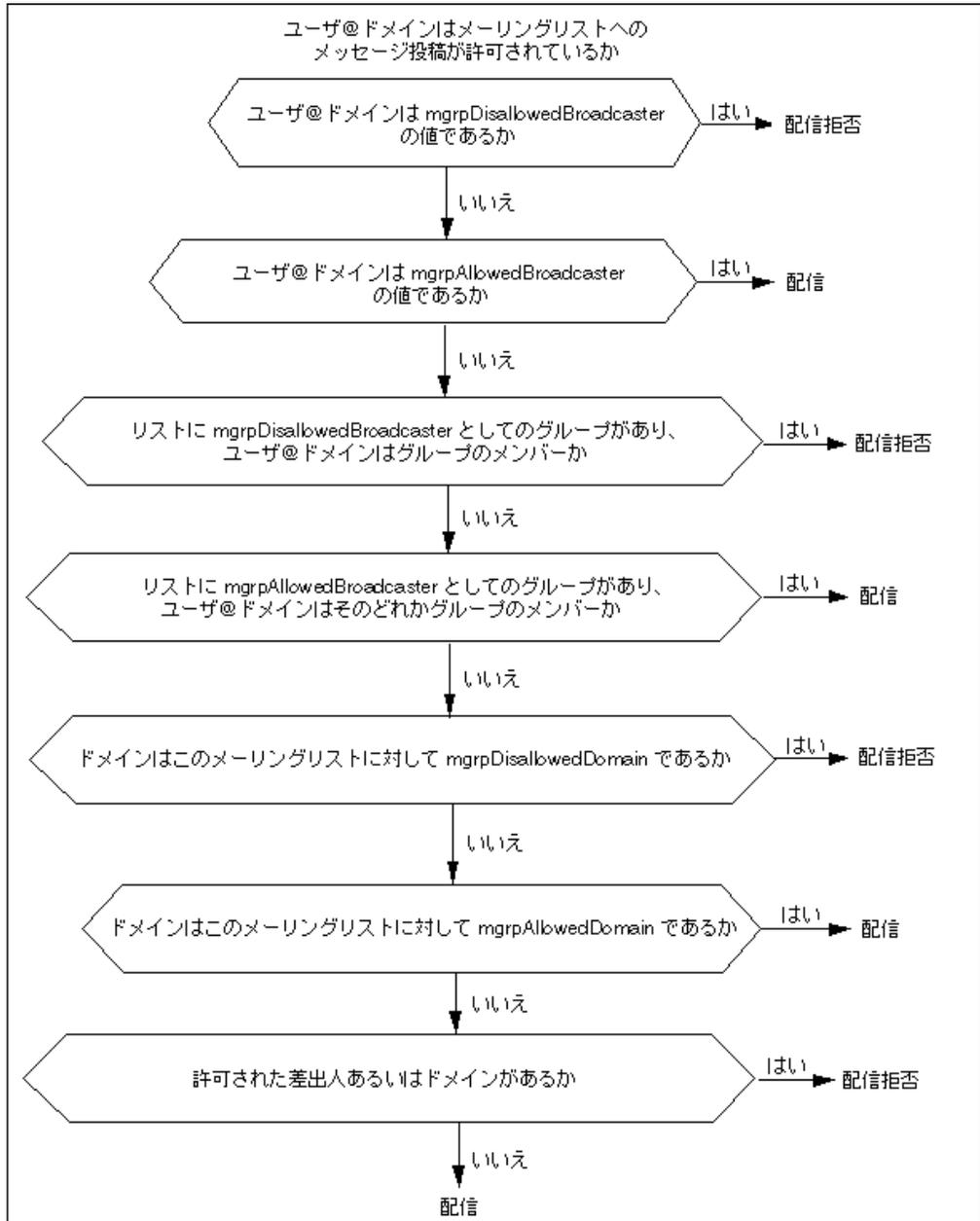
優先規則

MTA はメッセージを受信してさらに処理を行うかどうかを判断する際に、次の優先規則に従います (一致するものを探す場合には、エンベロープの「From:」アドレスがすべての規則で使用されます)。

1. `mgrpDisallowedBroadcaster` が設定されている場合は、この値が差出人の `mail` 属性と一致するか、または差出人が `ldap:///<DN>` の形式でリストに記載されている DN の `mailAlternateAddress` 属性と一致しているか、または `mailto: <RFC-822>` アドレスの形式でリストに記載されている RFC-822 アドレスと一致すると拒否されます。
2. `mgrpAllowedBroadcaster` 属性が LDAP エントリ内にある場合は、差出人のアドレスが、`mail` 属性または `ldap:///<DN>` アドレスの形式でリストに記載されている DN の `mailAlternateAddress` 属性のどれかと一致するか、または `mailto: <RFC-822>` アドレスの形式でリストに記載されている RFC-822 アドレスと一致する必要があります。
3. `mgrpDisallowedDomain` が LDAP エントリ内にある場合は、差出人のドメインが `mgrpDisallowedDomain` 属性内のリストに記載されているドメインと一致すると拒否されます。
4. `mgrpAllowedDomain` 属性が LDAP エントリ内にある場合は、差出人のドメインが `mgrpAllowedDomain` 属性内のリストに記載されているドメインと一致する必要があります。

次の図に、アクセス制御プロセスを示します。

図 5-1 アクセス制御プロセス



次の LDIF コードを使用すると、ドメイン `sesta.com` のユーザはメーリングリストにメッセージを送信できますが、その他すべてのドメインのユーザが送信したメッセージは拒否されます。また、`barry@sesta.com` からの内部メールは拒否されますが、`barkley@florizel.com` からのメールは許可されます。

```
dn: cn=Dreamteam,ou=groups,o=sesta.com,o=isp
changetype: modify
add: mgrpAllowedDomain
mgrpAllowedDomain: sesta.com
-
dn: cn=Dreamteam,ou=groups,o=sesta.com,o=isp
changetype: modify
add: mgrpAllowedBroadcaster
mgrpAllowedBroadcaster: mailto:barkley@florizel.com
-
dn: cn=Dreamteam,ou=groups,o=sesta.com,o=isp
changetype: modify
add: mgrpDisallowedBroadcaster
mgrpDisallowedBroadcaster:
    ldap:///cn=barry,ou=people,o=sesta.com,o=isp
```

コード例 5-4 配信制限を指定したメーリングリストの LDIF レコード

```
dn: cn=Dreamteam,ou=groups,o=sesta.com,o=isp
cn: Dreamteam
objectClass: groupOfUniqueNames
objectClass: inetMailGroup
objectClass: inetLocalMailRecipient
objectClass: inetMailGroupManagement
objectClass: nsManagedMailList
uniqueMember: uid=baylor,ou=People,o=sesta.com,o=isp
uniqueMember: uid=bird,ou=People,o=sesta.com,o=isp
uniqueMember: uid=jordan,ou=People,o=sesta.com,o=isp
uniqueMember: uid=jabbar,ou=People,o=sesta.com,o=isp
uniqueMember: uid=magic,ou=People,o=sesta.com,o=isp
mgrpRFC822MailMember: west@florizel.com
mgrpRFC822MailMember: robertson@florizel.com
mail: dreamteam@sesta.com
mailAlternateAddress: thegreatest@sesta.com
mailHost: manatee.siroe.com
dataSource: @(#)ims50users.sh 1.5a 02/3/00
inetMailGroupStatus: active
nsNumUsers: 7
nsMaxUsers: 1000
mgrpAllowedDomain: sesta.com
mgrpAllowedBroadcaster: mailto:barkley@florizel.com
mgrpDisallowedBroadcaster: ldap:///cn=barry,ou=people,o=sesta.com,o=isp
```

メーリングリストのモデレータ

メーリングリストのモデレータとは、メーリングリストへのメッセージを他のすべてのメンバーより前に受信し、必要に応じて他のメンバーに転送するユーザです。メーリングリストに送信されたすべてのメッセージは、メーリングリストメンバーではなくモデレータに送信されます。有効な DN または電子メールアドレスを `moderator` 属性に設定します。複数のモデレータを指定できます。

モデレータを作成するには、`mgrpModerator` を RFC 822 電子メールアドレスまたは URL 形式の DN に設定します。

```
dn: cn=Dreamteam,ou=groups,o=sesta.com,o=isp
changetype: modify
add: mgrpModerator
mgrpModerator: ldap:///uid=baylor,ou=People,o=sesta.com,o=isp
```

コード例 5-5 モデレータを指定したメーリングリストの LDIF レコード

```
dn: cn=Dreamteam,ou=groups,o=sesta.com,o=isp
cn: Dreamteam
objectClass: groupOfUniqueNames
objectClass: inetMailGroup
objectClass: inetLocalMailRecipient
objectClass: inetMailGroupManagement
objectClass: nsManagedMailList
uniqueMember: uid=baylor,ou=People,o=sesta.com,o=isp
uniqueMember: uid=bird,ou=People,o=sesta.com,o=isp
uniqueMember: uid=jordan,ou=People,o=sesta.com,o=isp
uniqueMember: uid=jabbar,ou=People,o=sesta.com,o=isp
uniqueMember: uid=magic,ou=People,o=sesta.com,o=isp
mgrpRFC822MailMember: west@florizel.com
mgrpRFC822MailMember: robertson@florizel.com
mail: dreamteam@sesta.com
mailAlternateAddress: thegreatest@sesta.com
mailHost: manatee.siroe.com
dataSource: @(#)ims50users.sh 1.5a 02/3/00
inetMailGroupStatus: active
nsNumUsers: 7
nsMaxUsers: 1000
mgrpModerator: ldap:///uid=baylor,ou=People,o=sesta.com,o=isp
```

メーリングリストの有効化、無効化、削除

`inetMailGroupStatus` を `active`、`inactive`、または `deleted` に設定することによって、メーリングリストを有効化、一時的に無効化、または削除することができます。無効化されたメーリングリストは、`inetMailGroupStatus` を `active` に再設定することによって有効化できます。値がない場合は、状態が `active` であることを示します。不正な値は、`inactive` として扱われます。

次の LDIF コードは、メーリングリストを無効にします。

```
dn: cn=Dreamteam,ou=groups,o=sesta.com,o=isp
changetype: modify
add: inetMailGroupStatus
inetMailGroupStatus: inactive
```

コード例 5-6 メーリングリストを無効化した LDIF レコード

```
dn: cn=Dreamteam,ou=groups,o=sesta.com,o=isp
cn: Dreamteam
objectClass: groupOfUniqueNames
objectClass: inetMailGroup
objectClass: inetLocalMailRecipient
objectClass: inetMailGroupManagement
objectClass: nsManagedMailList
uniqueMember: uid=baylor,ou=People,o=sesta.com,o=isp
uniqueMember: uid=bird,ou=People,o=sesta.com,o=isp
uniqueMember: uid=jordan,ou=People,o=sesta.com,o=isp
uniqueMember: uid=jabbar,ou=People,o=sesta.com,o=isp
uniqueMember: uid=magic,ou=People,o=sesta.com,o=isp
mgrpRFC822MailMember: west@florizel.com
mgrpRFC822MailMember: robertson@florizel.com
mail: dreamteam@sesta.com
mailAlternateAddress: thegreatest@sesta.com
mailHost: manatee.siroe.com
dataSource: @(#)ims50users.sh 1.5a 02/3/00
nsNumUsers: 7
nsMaxUsers: 1000
inetMailGroupStatus: inactive
```

メッセージのファイルへのアーカイブ

メーリングリストのメッセージをアーカイブするには、`mailDeliveryFileURL` を URL ファイルに設定します。次の例では、`dreamteam@sesta.com` に送信されたメッセージを `/home/dreamteam/mail_archive.log` に保存します。

```
dn: cn=Dreamteam,ou=groups,o=sesta.com,o=isp
changetype: modify
add: mailDeliveryFileURL
mailDeliveryFileURL: file:///home/dreamteam/mail_archive.log
```

コード例 5-7 アーカイブ属性を指定したメーリングリストの LDIF レコード

```
dn: cn=Dreamteam,ou=groups,o=sesta.com,o=isp
cn: Dreamteam
objectClass: groupOfUniqueNames
objectClass: inetMailGroup
objectClass: inetLocalMailRecipient
objectClass: inetMailGroupManagement
objectClass: nsManagedMailList
uniqueMember: uid=baylor,ou=People,o=sesta.com,o=isp
uniqueMember: uid=bird,ou=People,o=sesta.com,o=isp
uniqueMember: uid=jordan,ou=People,o=sesta.com,o=isp
uniqueMember: uid=jabbar,ou=People,o=sesta.com,o=isp
uniqueMember: uid=magic,ou=People,o=sesta.com,o=isp
mgrpRFC822MailMember: west@florizel.com
mgrpRFC822MailMember: robertson@florizel.com
mail: dreamteam@sesta.com
mailAlternateAddress: thegreatest@sesta.com
mailHost: manatee.siroe.com
dataSource: @(#)ims50users.sh 1.5a 02/3/00
inetMailGroupStatus: active
nsNumUsers: 7
nsMaxUsers: 1000
mailDeliveryFileURL: file:///home/dreamteam/mail_archive.log
```

リクエストアドレス

メーリングリストの購読リクエストアドレスを指定するには、mgrpRequestsTo 属性を使用します。購読リクエストの例として、dreamteam-request@sesta.com があります。この属性には、内部アドレスだけを指定できます。アドレスは URL 形式で指定する必要があります。

```
dn: cn=Dreamteam,ou=groups,o=sesta.com,o=isp
changetype: modify
add: mgrpRequestsTo
mgrpRequestsTo: uid=baylor,ou=People,o=sesta.com,o=isp
```

コード例 5-8 購読リクエスト属性を指定したメーリングリストの LDIF レコード

```
dn: cn=Dreamteam,ou=groups,o=sesta.com,o=isp
cn: Dreamteam
objectClass: groupOfUniqueNames
```

コード例 5-8 購読リクエスト属性を指定したメーリングリストの LDIF レコード (続き)

```
objectClass: inetMailGroup
objectClass: inetLocalMailRecipient
objectClass: inetMailGroupManagement
objectClass: nsManagedMailList
uniqueMember: uid=baylor,ou=People,o=sesta.com,o=isp
uniqueMember: uid=bird,ou=People,o=sesta.com,o=isp
uniqueMember: uid=jordan,ou=People,o=sesta.com,o=isp
uniqueMember: uid=jabbar,ou=People,o=sesta.com,o=isp
uniqueMember: uid=magic,ou=People,o=sesta.com,o=isp
mgrpRFC822MailMember: west@florizel.com
mgrpRFC822MailMember: robertson@florizel.com
mail: dreamteam@sesta.com
mailAlternateAddress: thegreatest@sesta.com
mailHost: manatee.siroe.com
dataSource: @(#)ims50users.sh 1.5a 02/3/00
inetMailGroupStatus: active
nsNumUsers: 7
nsMaxUsers: 1000
mgrpRequestsTo: uid=baylor,ou=People,o=sesta.com,o=isp
```

メーリングリストメンバーの表示

メーリングリストのメンバーは、一般的に iPlanet Console、iPlanet Delegated Administrator for Messaging、または SMTP の EXPN コマンドを使用します。mgmanMemberVisibility を ANYONE (すべてのユーザが表示可能)、ALL (ディレクトリ内のすべてのユーザが表示可能)、NONE (所有者だけが表示可能) に設定することによって表示可能なユーザを制限できます。

```
dn: cn=Dreamteam,ou=groups,o=sesta.com,o=isp
changetype: modify
add: mgmanMemberVisibility
mgmanMemberVisibility: ALL
```

コード例 5-9 表示属性を指定したメーリングリストの LDIF レコード

```
dn: cn=Dreamteam,ou=groups,o=sesta.com,o=isp
cn: Dreamteam
objectClass: groupOfUniqueNames
objectClass: inetMailGroup
objectClass: inetLocalMailRecipient
objectClass: inetMailGroupManagement
objectClass: nsManagedMailList
uniqueMember: uid=baylor,ou=People,o=sesta.com,o=isp
uniqueMember: uid=bird,ou=People,o=sesta.com,o=isp
uniqueMember: uid=jordan,ou=People,o=sesta.com,o=isp
uniqueMember: uid=jabbar,ou=People,o=sesta.com,o=isp
uniqueMember: uid=magic,ou=People,o=sesta.com,o=isp
```

コード例 5-9 表示属性を指定したメーリングリストの LDIF レコード (続き)

```
mgrpRFC822MailMember: west@florizel.com
mgrpRFC822MailMember: robertson@florizel.com
mail: dreamteam@sesta.com
mailAlternateAddress: thegreatest@sesta.com
mailHost: manatee.siroe.com
dataSource: @(#)ims50users.sh 1.5a 02/3/00
inetMailGroupStatus: active
nsNumUsers: 7
nsMaxUsers: 1000
mgmanMemberVisibility: ALL
```

メーリングリストの参加可能者

`mgmanJoinability` 属性を設定することによって、メーリングリストに参加できるユーザを指定できます。このタスクで使用可能な値は、`ANYONE` (すべてのユーザが参加可能)、`ALL` (ディレクトリ内のすべてのユーザが参加可能)、`NONE` (メンバーの追加不能) のいずれかです。

```
dn: cn=dreamteam,ou=groups,o=sesta.com,o=isp
changetype: modify
add: mgmanJoinability
mgmanJoinability: ALL
```

コード例 5-10 参加可能者を指定したメーリングリストの LDIF レコード

```
dn: cn=Dreamteam,ou=groups,o=sesta.com,o=isp
cn: Dreamteam
objectClass: groupOfUniqueNames
objectClass: inetMailGroup
objectClass: inetLocalMailRecipient
objectClass: inetMailGroupManagement
objectClass: nsManagedMailList
uniqueMember: uid=baylor,ou=People,o=sesta.com,o=isp
uniqueMember: uid=bird,ou=People,o=sesta.com,o=isp
uniqueMember: uid=jordan,ou=People,o=sesta.com,o=isp
uniqueMember: uid=jabbar,ou=People,o=sesta.com,o=isp
uniqueMember: uid=magic,ou=People,o=sesta.com,o=isp
mgrpRFC822MailMember: west@florizel.com
mgrpRFC822MailMember: robertson@florizel.com
mail: dreamteam@sesta.com
mailAlternateAddress: thegreatest@sesta.com
mailHost: manatee.siroe.com
dataSource: @(#)ims50users.sh 1.5a 02/3/00
inetMailGroupStatus: active
nsNumUsers: 7
nsMaxUsers: 1000
mgmanJoinability: ALL
```

動的なメーリングリストの作成

iPlanet Messaging Server は、静的メーリングリストと動的メーリングリストの両方をサポートします。静的なメーリングリストのメンバーは、`uniquemember` 属性と `mgrpRFC822mailmember` 属性を使用して指定します。一方、動的なメーリングリストのメンバーは、LDAP 検索フィルタ (RFC-2254) を使用して指定します。LDAP フィルタは、`inetMailGroup` オブジェクトクラスの `mgrpDeliverTo` 属性で設定します。

次の例は、静的メンバーと、LDAP 検索フィルタで動的に決定されるメンバーとの両方で構成されるメーリングリストを示しています。次に示すフィルタは、`o=sesta.com,o=isp` のメンバーで、かつ属性値のペア `city=tokyo` を持つメンバーをメーリングリストに含めます。LDAP 検索フィルタ内で使用される属性にインデックスが付いていることを確認する必要があります。インデックスが付いていないと、動的リストのメンバーシップの評価に時間がかかり、ディレクトリサーバの負荷が大きくなります。

コード例 5-11 動的なメーリングリスト用の LDIF レコード

```
dn: cn=Dreamteam,ou=groups,o=sesta.com,o=isp
cn: Dreamteam
objectClass: groupOfUniqueNames
objectClass: inetMailGroup
objectClass: inetLocalMailRecipient
objectClass: inetMailGroupManagement
objectClass: nsManagedMailList
uniqueMember: uid=baylor,ou=People,o=sesta.com,o=isp
uniqueMember: uid=bird,ou=People,o=sesta.com,o=isp
uniqueMember: uid=jordan,ou=People,o=sesta.com,o=isp
uniqueMember: uid=jabbar,ou=People,o=sesta.com,o=isp
uniqueMember: uid=magic,ou=People,o=sesta.com,o=isp
mgrpRFC822MailMember: west@florizel.com
mgrpRFC822MailMember: robertson@florizel.com
mail: dreamteam@sesta.com
mailAlternateAddress: thegreatest@sesta.com
mgrpDeliverTo: ldap:///o=sesta.com,o=isp??sub?
  (&(objectclass=inetMailUser)(city=tokyo))
mailHost: manatee.siroe.com
dataSource: @(#)ims50users.sh 1.5a 02/3/00
inetMailGroupStatus: active
nsNumUsers: 7
nsMaxUsers: 1000
mgmanJoinability: ALL
```

注 iPlanet Messaging Server はさらに、オブジェクトクラス `groupofurls` の `memberURL` 属性に基づく動的リストをサポートします。Netscape Directory Server 4.x では、この属性を使用して動的なグループを作成できます。Messaging Server では `memberURL` を使用してすでに定義されているすべてのグループを利用できます。

受信メッセージサイズの制限

ユーザやグループが受信できるメッセージのサイズを制限するには、属性 `mailMsgMaxBlocks` を使用します。メッセージサイズは、MTA ブロックサイズ (デフォルトは 1024 バイト) 単位で設定します。この属性は、`mailDomainMsgMaxBlocks` よりも優先されます。

次の例では、制限を 1M バイトに設定します。

```
dn: cn=dreamteam,ou=groups,o=sesta.com,o=isp
changetype: modify
add: mailMsgMaxBlocks
mailMsgMaxBlocks: 1000
```

コード例 5-12 参加可能者を指定したメーリングリストの LDIF レコード

```
dn: cn=Dreamteam,ou=groups,o=sesta.com,o=isp
cn: Dreamteam
objectClass: groupOfUniqueNames
objectClass: inetMailGroup
objectClass: inetLocalMailRecipient
objectClass: inetMailGroupManagement
objectClass: nsManagedMailList
uniqueMember: uid=baylor,ou=People,o=sesta.com,o=isp
uniqueMember: uid=bird,ou=People,o=sesta.com,o=isp
uniqueMember: uid=jordan,ou=People,o=sesta.com,o=isp
uniqueMember: uid=jabbar,ou=People,o=sesta.com,o=isp
uniqueMember: uid=magic,ou=People,o=sesta.com,o=isp
mgrprRFC822MailMember: west@florizel.com
mgrprRFC822MailMember: robertson@florizel.com
mail: dreamteam@sesta.com
mailAlternateAddress: thegreatest@sesta.com
mailHost: manatee.siroe.com
dataSource: @(#)ims50users.sh 1.5a 02/3/00
inetMailGroupStatus: active
nsNumUsers: 7
nsMaxUsers: 1000
mailMsgMaxBlocks: 1000
```

メーリングリストのタスク

Messaging Server 管理者のプロビジョニング

この章では、さまざまなタイプの Messaging Server 管理者 (表 6-1) のプロビジョニングを行う方法について説明します。この章には、以下の節があります。

- 102 ページの「管理者のタイプ」
- 104 ページの「構成管理者の作成」
- 104 ページの「メッセージストア管理者の作成」
 - 105 ページの「特定の Messaging Server のメッセージストア管理者の作成」
 - 105 ページの「メールシステムトポロジ全体のメッセージストア管理者の作成」
 - 107 ページの「特定ドメインのメッセージストア管理者の作成」
- 109 ページの「トップレベル管理者の作成」
- 110 ページの「ドメイン管理者の作成」
- 112 ページの「ドメイン組織管理者の作成」

管理者のタイプ

iPlanet Messaging Server 管理者は、次の2つの権限のセットによって分類されます。

- Messaging Server を構成する権限 (サーバ管理者)
- システム内のユーザやグループを追加、変更、削除する権限 (メッセージングディレクトリ管理者)

表 6-1 Messaging Server 管理者と権限

管理者	説明と権限の適用範囲	権限付与と作成
サーバ管理者		
構成管理者	<p>すべてのサーバを構成し、トポロジ全体のすべてのディレクトリデータを変更できる。MTA を変更するためのシステムレベルのアクセス権を持つ。</p> <p>Console 内のすべてのリソースへの無制限のアクセス権を持つ。他の管理者にサーバアクセスを提供できる</p>	<p>構成管理者のユーザ ID は、Messaging Server が最初に起動されたときに自動的に作成される。詳細は、『Managing Servers with Netscape Console』を参照。</p> <p>ACI により付与される権限 : o=NetscapeRoot</p> <p>管理アカウント : uid=admin、ou=administrators、ou=topologymanagement、o=NetscapeRoot)</p> <p>グループ DN : cn=configuration administrators、ou=groups、ou=topologymanagment、o=NetscapeRoot</p>
Directory Manager	<p>ディレクトリ内のすべてのものを変更できる。ディレクトリを構成できる。</p> <p>セキュリティ上の理由から、構成管理者とディレクトリマネージャは異なるユーザにする</p>	<p>ディレクトリマネージャのユーザ ID は、Directory Server のインストール時に作成される。</p> <p>ディレクトリマネージャの証明書は、Directory Server の構成ファイル slapd.conf に格納される。一般的なアカウント : cn = Directory Manager</p>
メッセージストア管理者	<p>システムレベルの管理者は、メールボックスを表示し、アクセス制御を指定できる。プロキシ認証権限を使用して、任意のユーザとしてログインできるメールボックスのパーティションを指定し、メッセージストアユーティリティを実行できる。</p> <p>ドメインレベルの管理者は、パーティションを指定できない。メッセージストアユーティリティへのアクセスは制限される</p>	<p>この管理者は、Messaging Server Console またはコマンドラインユーティリティを使って作成される。</p> <p>System-wide MS Admin Group DN: store.serviceAdminGroupDN で指定される。</p> <p>ドメインメッセージストア管理グループの DN : cn=Store Administrators、ou=Groups、<組織ツリードメインのサフィックス></p> <p>サーバメッセージストア管理者は、サーバ構成変数 store.admin で指定される</p>

表 6-1 Messaging Server 管理者と権限 (続き)

管理者	説明と権限の適用範囲	権限付与と作成
メッセージングディレクトリ管理者		
トップレベル管理者 (サービス管理者とも呼ばれる)	<p>DA GUI または CLI を使用して、Messaging Server ネームスペース全体のメールユーザ、メーリングリスト、ファミリーアカウント、ドメインを作成、変更、削除する。</p> <p>トポロジ内のすべてのサーバのすべてのメッセージストア権限を自動的に取得する</p>	<p>トップレベル管理者は、インストール時に自動的に作成される。</p> <p>ルートノードに格納された ACI。</p> <p>グループ DN : cn = Service Administrators、ou=groups、<組織ツリールート></p>
ドメイン管理者	<p>DA 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、ファミリーアカウントを作成、変更、削除する。</p> <p>デフォルトでは、ホストドメインのメッセージストア管理者が割り当てられる</p>	<p>トップレベル管理者がドメイン管理者を作成できる。</p> <p>組織ツリールート、DC ルート、組織ツリードメインノードの ACI。</p> <p>グループ DN : cn = Domain Administrators、ou=groups、<組織ツリードメイン></p>
ドメイン組織管理者	<p>DA GUI または CLI を使用して、ドメイン組織内のメールユーザとメーリングリストを作成、変更、削除する</p>	<p>トップレベルの管理者またはドメイン管理者が、ドメイン組織管理者を作成できる。</p> <p>ルートおよびドメイン組織ノードの ACI。</p> <p>グループ DN : cn = Organization Administrator、<ドメイン組織 DN></p>
ファミリーグループ管理者	<p>ファミリーグループ内のファミリーメンバーの追加と削除を行う。グループの他のメンバーに管理アクセス権を与えることができる。60 ページの「ファミリーグループ管理者の作成」を参照</p>	<p>トップレベル管理者とドメイン管理者が、ファミリーグループ管理者を作成できる。</p> <p>LDAP に格納された権限。</p> <p>グループ DN : cn=Family Group Administrators、<ファミリーグループ DN></p>
メールリストの所有者	<p>作成権限と、メーリングリストのメンバーの追加や削除を行う権限の 2 つの権限セットを持つ</p>	<p>トップレベル管理者、ドメイン管理者、ドメイン組織管理者は、メーリングリスト所有者に権限を与えることができる。</p> <p>nsDACapability は作成権限を与える (80 ページの「メーリングリストの作成権限の追加」を参照)。owner は、管理権限を与える (87 ページの「メーリングリスト所有者の割り当て」を参照)</p>

注 Netscape Console の使用方法の詳細は、
<http://docs.iplanet.com/docs/manuals/console.html> にある
Netscape Console のマニュアルを参照してください。

構成管理者の作成

構成管理者は、インストール時に自動的に作成されます。構成管理者は、Console を使用して追加の構成管理者を作成できます。詳細は、
<http://docs.iplanet.com/docs/manuals/console.html> にある Netscape Console のマニュアルを参照してください。

メッセージストア管理者の作成

メッセージストア管理者は権限を持ち、権限には適用範囲があります。次のような権限があります。

- IMAP を使用してユーザのメールボックスの表示と監視を行う
- IMAP を使用してメッセージストアのアクセス制御を指定する
- プロキシ認証を必要とするメッセージストアコマンドラインユーティリティ (MoveUser など) を実行する
- プロキシ認証権限を使用して、任意のユーザとしてログインできる
- メールボックスのパーティションを指定する

管理者権限の適用範囲は次のように設定できます。

- 単一ドメイン (さらに、ドメインレベル管理者の場合は、パーティションを指定できず、特定のメッセージストアコマンドへのアクセスが制限されます)
- 単一のメッセージストア (つまり、1 つの Messaging Server のメッセージストア)
- メールシステムトポロジ内のすべてのメッセージストア
- トップレベル管理者には、システム全体のメッセージストア権限が自動的に与えられる
- インストール時に作成された Messaging Server 管理者には、インストール先のサーバのメッセージストア権限が自動的に与えられる
- インストール時に作成されたか、または Console で作成されたトップレベル管理者には、トポロジ全体のメッセージストア権限が自動的に与えられる
- iPlanet Delegated Administrator for Messaging で作成されたドメイン管理者には、インストール先のドメインのユーザのメッセージストア権限が自動的に与えられる

特定の Messaging Server のメッセージストア管理者の作成

必要な権限: 構成管理者または Messaging Server マシン上の mailsrv アカウントへのアクセス権

構成管理者には、インストール先のサーバのメッセージストア権限が自動的に与えられます。サーバ固有のメッセージストア管理者を作成するには、**Console** (『iPlanet Message Server 管理者ガイド』を参照) または次のコマンドラインを使用します。

```
configutil -o store.admin -v "adminlist"
```

ここでの configutil は設定オプションを変更できるユーティリティです。store.admins はメッセージストア管理者のパラメータです。adminlist は、完全修飾 UID (デフォルトのドメインの場合) または <uid>@<ドメイン> (ホストドメインの場合) の空白で区切られたリストです。詳細は、『iPlanet Messaging Server リファレンスマニュアル』を参照してください。

メールシステムトポロジ全体のメッセージストア管理者の作成

必要な権限: トップレベル管理者または Messaging Server マシン上の mailsrv アカウントへのアクセス権

「メールシステムトポロジ全体」とは、共通のユーザおよびグループのディレクトリのルート下にあるすべての Messaging Server のすべてのメッセージストアを意味します。デフォルトでは、トポロジ全体のメッセージストアの管理権限は、グループ `cn=Service Administrators,ou=groups,<組織ツリーのルート>` のメンバーだけに与えられます。ただし、構成値 `store.serviceAdminGroupDN` を再設定することによって、これらのメッセージストア権限を別のグループに変更できます。変更した場合、`cn=Service Administrators,ou=groups,<組織ツリールート>` のメンバーを新しいグループに追加しない限り、それらのメンバーのメッセージストア権限はなくなります。

次の例では、システム全体のメッセージストア管理者グループを `cn=Service Administrators,ou=groups,o=isp` から `cn=System-wide Store Administrators,ou=groups,o=isp` に変更し、さらに管理者として `Biff` を追加します。

1. システム全体のストア管理者グループを作成し、メンバーを追加します。

初めに、`System-wide Store Administrators` というグループを作り、`uniqueMember` 属性を使用してメンバーを追加します。

コード例 6-1 システム全体のメッセージストア管理者グループの作成

```
dn: cn=System-wide Store Administrators,ou=groups,o=isp
objectclass: groupOfUniqueNames
cn: System-wide Store Administrators
uniqueMember: uid=Biff,ou=people,o=sesta.com,o=isp
```

2. store.serviceAdminGroupDN をシステム全体のメッセージストア管理者グループ (System-wide Message Store Administrators Group) の DN に設定します。

```
configutil -o store.serviceAdminGroupDN -v "cn=System-wide Store
Administrators,ou=groups,o=isp"
```

この設定は、システム内の各サーバで行う必要があります。

3. ユーザエントリ内の memberof 属性を設定します。

コード例 6-2 システム全体のメッセージストア管理者のユーザエントリの例

```
dn: uid=Biff,ou=people,o=sesta.com,o=isp
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: inetUser
objectClass: ipUser
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: nsManagedPerson
objectClass: userPresenceProfile
cn: Biff Fanning
sn: fanning
initials: BTF
givenName: Biff
mail: Biff.Fanning@sesta.com
mailAlternateAddress: bfanning@florizel.com
mailDeliveryOption: mailbox
mailHost: manatee.siroe.com
uid: biff
dataSource: iMS 5.0 @(#)ims50users.sh 1.5a 02/3/00
userPassword: {SHA}aluWfd0LYY9ImsJb3h4afrI4AXk=
mailAllowedServiceAccess: +imap, imaps, pop3, smtp, http:*
inetUserStatus: active
mailUserStatus: active
mailQuota: -1
mailMsgQuota: 100
memberOf: cn=System-wide Store Administrators,ou=groups o=sesta.com,o=isp
```

特定ドメインのメッセージストア管理者の作成

必要な権限：ドメイン管理者またはトップレベル管理者

ドメインメッセージストア管理者は、次の手順で作成できます。

- iPlanet Delegated Administrator for Messaging GUI を使用して、ユーザを委任管理者に変更する
- LDAP を使用してプロビジョニングを行う

次の例では、LDAP を使用して、ユーザ Biff に sesta.com のメッセージストアに対する権限を与えます。

1. ストア管理者グループを作成し、メンバーを追加します。

組織ツリーのドメインノード内に **Store Administrators** というグループを作成します。inetMailAdministrator オブジェクトクラスを追加し、グループエントリに対する mailAdminRole 属性を storeadmin に設定します。uniqueMember 属性を使用してメンバーを追加します。以下の LDIF データを参照してください。

ACI はインストール時に自動的に作成されます。また、このグループは、Delegated Administrator または Console を使用してドメインを作成すると必ず作成されます。

コード例 6-3 ストア管理者グループの作成

```
dn: cn=Store Administrators,ou=Groups,o=sesta.com,o=isp
objectclass: groupOfUniqueNames
objectclass: inetMailAdministrator
cn: Store Administrators
mailAdminRole: storeadmin
uniqueMember: uid=Biff,ou=People,o=sesta.com,o=isp
```

- objectclass: groupOfUniqueNames
- objectclass: inetMailAdministrator

groupOfUniqueNames オブジェクトクラスには、ディレクトリエントリ (つまり、ユーザや他のグループ) のコレクションを記述するための属性が含まれます。

inetMailAdministrator は、管理権限をこのグループに与える属性を指定します。

- cn: Store Administrators

これは、メッセージストア管理者が所属している必要があるグループの共通名です。

- mailAdminRole: storeadmin

このグループに与えられた管理権限のタイプです。

- `uniqueMember: uid=Biff,ou=People,o=sesta.com,o=isp`

メンバーの DN です。この例では、このグループのメンバーは 1 人だけです。

2. ユーザのエントリ内の `memberOf` 属性を次のように指定します。
`cn=Store Administrators,ou=Groups,o=sesta.com,o=isp`

コード例 6-4 ドメイン管理者のユーザエントリの例

```
dn: uid=Biff,ou=people,o=sesta.com,o=isp
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: inetUser
objectClass: ipUser
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: nsManagedPerson
objectClass: userPresenceProfile
cn: Biff Fanning
sn: fanning
initials: BTF
givenName: Biff
mail: Biff.Fanning@sesta.com
mailAlternateAddress: bfanning@florizel.com
mailDeliveryOption: mailbox
mailHost: manatee.siroe.com
uid: biff
dataSource: iMS 5.0 @(#)ims50users.sh 1.5a 02/3/00
userPassword: {SHA}aluWfd0LYY9ImsJb3h4afrI4AXk=
mailAllowedServiceAccess: +imap, imaps, pop3, smtp, http:*
inetUserStatus: active
mailUserStatus: active
mailQuota: -1
mailMsgQuota: 100
memberOf: cn=Store Administrators,ou=groups o=sesta.com,o=isp
```

- `dn: uid=Biff,ou=People,o=sesta.com,o=isp`
このグループのメッセージストア管理者に指名されたユーザの DN です。
- `memberOf: cn=Store Administrators,ou=groups,o=sesta.com,o=isp`
Biff が所属するグループの DN です。

トップレベル管理者の作成

タスクの権限：トップレベル管理者

トップレベル管理者は、メッセージシステム全体のディレクトリおよびメッセージストアに対する権限を持ちます。デフォルトのトップレベル管理者はインストール時に作成されますが、以下のグループにユーザを追加することによって、複数のトップレベル管理者を作成できます。

```
cn=Service Administrators,ou=Groups,o=<組織ツリールート>
```

さらに、ユーザのエントリ内の `memberOf` 属性を次のように指定します。

```
cn=Service Administrators,o=groups,o=<組織ツリールート>
```

次の例では、**Biff Fanning** をトップレベル管理者にします。インストーラによって、このエントリ用の適切な **ACI** が作成されます。ディレクトリを最初から作成する場合は、付録 A 「ルートとドメインの **ACI** の例」を参照してください。

コード例 6-5 トップレベル管理者グループ

```
dn: cn=Service Administrators,ou=Groups,o=isp
objectclass: groupOfUniqueNames
objectclass: nsManagedDept
cn: Service Administrators
nsNumUsers: 1
nsMaxUsers: Unlimited
uniqueMember: uid=Biff,ou=People,o=sesta.com,o=isp
```

コード例 6-6 トップレベル管理者のユーザエントリの例

```
dn: uid=Biff,ou=people,o=sesta.com,o=isp
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: inetUser
objectClass: ipUser
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: nsManagedPerson
objectClass: userPresenceProfile
cn: Biff Fanning
sn: fanning
initials: BTF
givenName: Biff
mail: Biff.Fanning@sesta.com
mailAlternateAddress: bfanning@florizel.com
```

コード例 6-6 トップレベル管理者のユーザエントリの例 (続き)

```

mailDeliveryOption: mailbox
mailHost: manatee.siroe.com
uid: biff
dataSource: iMS 5.0 @(#)ims50users.sh 1.5a 02/3/00
userPassword: {SHA}aluWfd0LYY9ImsJb3h4afrI4AXk=
mailAllowedServiceAccess: +imap, imaps, pop3, http:*
inetUserStatus: active
mailUserStatus: active
mailQuota: -1
mailMsgQuota: 100
memberOf: cn=Service Administrators,ou=groups,o=isp

```

ドメイン管理者の作成

Delegated Admin ユーティリティ: `imadmin admin add`
 プロビジョニングのためのタスク権限: トップレベル管理者

ドメイン管理者は、Delegated Administrator またはコマンドラインユーティリティを使用して、特定ドメイン内のユーザやグループの追加、削除、変更を行う権限を持ったユーザです。トップレベル管理者だけがホストドメインの管理者を作成できます。

ドメイン管理者のグループの作成と ACI 規則の設定を一度実行すれば、その作業を再び実行する必要はありません。新規管理者を作成するには、単にそれらをグループに追加します。次の LDIF の例では、ドメイン管理者グループを作成し、このグループのメンバーとして Biff を追加します。

1. ドメイン管理者グループを作成し、このグループにユーザを追加します。

組織ツリーのホストドメインノードに **Domain Administrators** というグループを作成し、ドメイン管理者に指名するユーザの DN をこのグループに追加します。さらに、オブジェクトクラス `inetMailAdministrator` と属性値のペア `mailadminrole: storeadmin` を追加します (Delegated Administrator を使用してドメインを作成した場合は、自動的にこのグループが作成され、ACI が設定されます)。ドメイン管理者グループの `uniqueMember` 属性を、新しいドメイン管理者の DN に指定します。以下にこの例を示します。

コード例 6-7 ドメイン管理者グループの作成

```

dn: cn=Domain Administrators,ou=groups,o=sesta.com,o=isp
objectclass: groupOfUniqueNames
objectClass: nsManagedDept
objectClass: inetMailAdministrator
mailadminrole: storeadmin
cn: Domain Administrators
uniqueMember: uid=Biff,ou=People,o=sesta.com,o=isp

```

- `objectclass: groupOfUniqueNames`
`objectClass: nsManagedDept`
`objectClass: inetMailAdministrator`
`groupOfUniqueNames` オブジェクトクラスには、ディレクトリエントリ (つまり、ユーザや他のグループ) のコレクションを記述するための属性が含まれます。
 - `cn: Domain Administrators`
これは、ドメイン管理者が所属している必要があるグループの共通名です。
 - `mailadminrole: storeadmin`
メッセージストア管理者権限をこのグループのメンバーに与えます。
 - `uniqueMember: uid=Biff,ou=People,o=sesta.com,o=isp`
`uniqueMember` は、このリストのメンバーの識別名を指定します。この例では、このグループのメンバーは 1 人だけです。
2. ドメイン管理者 ACI 規則を検証します。
ドメイン管理者 ACI 規則は、`Delegated Administrator` または `imadmin domain create` などのコマンドラインユーティリティを使用して、ホストドメインを作成すると、自動的に作成されます。LDAP を使用してホストドメインをプロビジョニングした場合は、ACI 規則を追加する必要があります。この例は、付録 A 「ルートとドメインの ACI の例」に記載されています。
 3. ユーザエンタリに `memberOf` を追加します。
ユーザエンタリ内の `memberOf` 属性を
`cn=Domain Administrators,o=groups,o=sesta.com,o=isp` に指定します。

コード例 6-8 ドメイン管理者のユーザエンタリの例

```
dn: uid=Biff,ou=people,o=sesta.com,o=isp
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: inetUser
objectClass: ipUser
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: nsManagedPerson
objectClass: userPresenceProfile
cn: Biff Fanning
sn: fanning
initials: BTF
givenName: Biff
mail: Biff.Fanning@sesta.com
mailAlternateAddress: bfanning@florizel.com
mailDeliveryOption: mailbox
mailHost: manatee.siroe.com
uid: fanning
```

コード例 6-8 ドメイン管理者のユーザエントリの例(続き)

```
dataSource: iMS 5.0 @(#)ims50users.sh 1.5a 02/3/00
userPassword: password
mailAllowedServiceAccess: +imap, imaps, pop3, http:*
inetUserStatus: active
mailUserStatus: active
mailQuota: -1
mailMsgQuota: 100
memberOf: cn=Domain Administrators,o=groups,o=sesta.com,o=isp
```

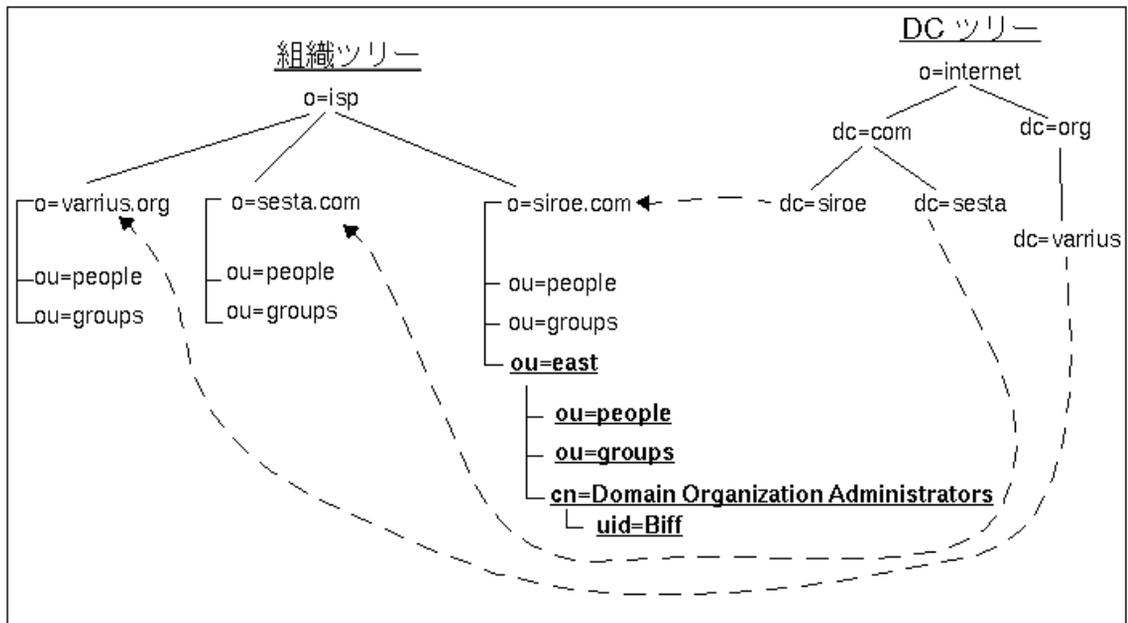
- dn: uid=Biff,ou=People,o=sesta.com,o=isp
このドメインのドメイン管理者に指名されたユーザの DN です。
- memberOf: cn=Domain Administrators,o=sesta.com,o=isp
このユーザが属するグループの DN です。

ドメイン組織管理者の作成

ドメイン組織管理者は、Delegated Administrator またはコマンドラインユーティリティを使用して、特定組織内のユーザやグループの追加、削除、変更を行う権限を持った組織のユーザです。複数のドメイン組織管理者を、1つのホストドメインに含めることができます。また、ドメイン組織管理者は入れ子にすることができます。トップレベル管理者だけが組織管理者を作成できます。

組織管理者のグループの作成と ACI 規則の設定を一度実行すれば、その作業を再び実行する必要はありません。新規管理者を作成するには、単にそれらをグループに追加します。次の例は、ou=east、o=siroe.com、o=isp に対する組織管理者 Biff の作成方法を示しています。

図 6-1 ドメイン組織管理者の作成



ドメイン組織の作成方法については、45 ページの「ドメイン組織の作成」を参照してください。

1. 組織ツリーのドメイン組織ノード内に Domain Organization Administrators というグループを作成し、このグループのドメイン組織管理者の DN を追加します。

コード例 6-9 組織管理者グループの作成

```
dn: cn=Domain Organization Administrators,ou=east,o=siroe.com,o=isp
objectclass: nsManagedDept
objectclass: inetAdmin
objectclass: groupOfUniqueNames
cn: Domain Organization Administrators
uniqueMember: uid=Biff,ou=people,ou=east,o=siroe.com,o=isp
```

- dn: cn=Organization Administrators,ou=groups,ou=east,o=siroe.com,o=isp
組織管理者のグループの名前です。
- objectclass: nsManagedDept
objectclass: inetAdmin
objectclass: groupOfUniqueNames

nsManagedDept は、Delegated Administrator をサポートするための属性を提供します。inetAdmin は、管理をサポートするための属性を提供します。groupOfUniqueNames オブジェクトクラスには、ディレクトリエントリ (つまり、ユーザや他のグループ) のコレクションを記述するための属性が含まれます。

- cn: Organization Administrators

これは、組織管理者が所属している必要があるグループの共通名です。

- uniqueMember: uid=Biff,ou=People,o=east.siroe.com,o=isp

uniqueMember は、このリストのメンバーの識別名を指定します。この例では、このグループのメンバーは 1 人だけです。

2. ドメイン組織管理者 ACI 規則を追加します。

適切な ACI 規則をドメイン組織に追加して変更する必要があります。この例では、ou=east,o=siroe.com,o=isp です。この例は、付録 A「ルートとドメインの ACI の例」に記載されています。

3. ドメイン組織管理者のエントリ内の memberOf 属性を指定します。

memberOf 属性を、uid=Biff,ou=people,o=sesta.com,o=isp 内の cn=Domain Organization Administrators,o=east.siroe.com,o=isp に指定します。

コード例 6-10

ドメイン管理者のユーザエントリの例

```
dn: uid=Biff,ou=people,o=sesta.com,o=isp
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: inetUser
objectClass: ipUser
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: nsManagedPerson
objectClass: userPresenceProfile
cn: Otis Fanning
sn: fanning
initials: BTF
givenName: Biff
mail: Biff.Fanning@sesta.com
mailAlternateAddress: bfanning@florizel.com
mailDeliveryOption: mailbox
mailHost: manatee.siroe.com
uid: fanning
dataSource: iMS 5.0 @(#)ims50users.sh 1.5a 02/3/00
userPassword: {SHA}aluWfd0LYY9ImsJb3h4afrI4AXk=
mailAllowedServiceAccess: +imap, imaps, pop3, http:*
inetUserStatus: active
mailUserStatus: active
```

コード例 6-10 ドメイン管理者のユーザエントリの例 (続き)

```
mailQuota: -1
mailMsgQuota: 100
memberOf: cn=Domain Organization Administrators,ou=east,o=siroe.com,o=isp
```

- dn: uid=Biff,ou=People,o=eng.siroe.com,o=isp
このグループのドメイン組織管理者に指名されたユーザの DN です。
- memberOf: cn=Organization Administrators,ou=groups,ou=east,o=siroe.com,o=isp
このユーザが所属するグループの DN です。

ルートとドメインの ACI の例

この付録に記載した ACI は、ディレクトリ情報ツリーでドメインまたはルートノードを作成したときにインストールされるデフォルトの ACI です。これらの ACI は、システムの要件に応じて変更できます。さらに、ルートやドメインのエントリで LDAP 検索を行うことによって、これらの ACI をオンラインで表示できます。ドメイン組織 ACI は、ドメイン組織を作成したときに、LDAP を使用して追加する必要があることに注意してください。この付録には、以下の節があります。

- 118 ページの「組織ツリールートノード ACI」
- 121 ページの「DC ツリールートノード ACI」
- 126 ページの「ホストドメイン ACI」
- 128 ページの「ドメイン組織 ACI」

注 ドメイン、ユーザ、グループのエントリ用に DC ツリーを使用している場合 (つまり、組織ツリーがない場合)、この付録に記載した組織ツリー用の ACI はすべて不要です。その場合は、DC ツリーの ACI 内に記載されている「<OrgRoot>」を <DCRoot> の値に変更します。

ACI の例内の変数の定義

<OrgRoot> - 組織ツリーのルート。デフォルトのインストールでユーザとグループのエントリが作成される場所

<DCRoot> - ドメインコンポーネントツリーのルート。ドメインエントリが作成される場所

<OrgNodeDN> - 組織ツリー内のドメインノード。ドメインのユーザとグループのエントリが置かれる場所

<DCNodeDN> - DC ツリー内のドメインノード。ドメインのユーザとグループのエントリが置かれる場所

<DomainOrgNodeDN> - ドメインコンポーネントツリーのルート。ドメインエントリが作成される場所

組織ツリールートノード ACI

次の ACI は、トップレベル管理者、ドメイン管理者、ドメイン組織管理者、ファミリーグループ管理者、メールリスト所有者、エンドユーザに必要なアクセス権を与えます。必要な場合は、ツリー内の下位のドメインノードやドメイン組織ノードで、追加の ACI を設定します。ネームスペースのセットアップを最初から手動で実行する場合（つまり、ネームスペースの作成に **iPlanet Messaging Server** インストーラを使用しない場合）、組織ツリールートノードで ACI を設定する必要があります。

コード例 A-1

組織ツリールートノード ACI

```
dn: <OrgRoot>
changetype: modify
add: aci:
#
#-----
# iDA ユーザのアクセス制御
#
# すべてのエントリ内のすべての属性に対する読み取りと検索のアクセスを許可する
#
aci: (targetattr="*") (version 3.0; acl "NDAUser access -
  product=ims5.0,class=nda,num=1,version=1"; allow (read,search)
  userdn="ldap:///uid=NDAUser,ou=config,<OrgRoot>");)
#
# すべてのドメインエントリの nsNum* 属性に対する書き込みアクセスを許可する
#
aci: (targetattr="nsNumUsers|nsNumDepts|nsNumMailLists|nsNumDomains")
  (version 3.0; acl "NDAUser access - product=ims5.0, class=nda,num=2,
  version=1"; allow (write) userdn="ldap:///uid=NDAUser,ou=config,
  <OrgRoot>");)
#
#-----
# サービス管理者のアクセス制御
#
# すべての DCROOT ノードに対する読み取りと検索のアクセスを許可する
#
aci: (targetattr="*") (version 3.0; acl "SA root node access -
  product=ims5.0,class=nda,num=3,version=1"; allow (all)
  groupdn="ldap:///cn=Service Administrators,ou=Groups,<OrgRoot>");)
#
#-----
# ドメイン管理者の制御
```

コード例 A-1 組織ツリールートノード ACI (続き)

```

#
# すべてのドメインコンテナノードに対する書き込みと削除のアクセスを拒否する
#
aci: (targetfilter="objectclass=nsManagedDomain") (version 3.0; acl
  "Domain Admin domain container access -
  product=ims5.0,class=nda,num=5,version=1"; deny (delete,write)
  userdn="ldap:///<DCRoot>??sub?(memberOf=cn=Domain Administrators*)" or
  userdn="ldap:///<OrgRoot>??sub?(memberOf=cn=Domain Administrators*");)
#
#-----
# ユーザのアクセス制御
#
# self に対して、読み取りと検索のアクセスを許可する
#
aci: (targetattr="*") (targetfilter=(objectClass=inetOrgPerson)) (version
  3.0; acl "User self search and read - product=ims5.0,class=nda,num=6,
  version=1"; allow (read,search) userdn="ldap:///self");)
#
# self に対して、書き込みアクセスを許可する
#
aci: (targetattr="*") (version 3.0; acl "Allow self entry modification -
  product=ims5.0,class=nda,num=7,version=1";
  allow (write) userdn = "ldap:///self");)
#
# uid、ou、owner、nsDAModifiableBy、nsDACapability、
# mail、mailAlternateAddress、memberOf、および nsDADomain 属性の
# self に対して、書き込みアクセスを拒否する
#
aci: (targetattr="uid||ou||owner||nsDAModifiableBy||nsDACapability||
  mail||mailAlternateAddress||memberOf||nsDADomain||inetuserstatus||
  mailuserstatus||memberOfManagedGroup||mailQuota||mailMsgQuota||
  inetSubscriberAccountId||dataSource||mailhost||mailAllowedServiceAccess
  ||pabURI||inetCOS") (targetfilter=(objectClass=nsManagedPerson))
  (version 3.0; acl "User self modification - product=ims5.0,class=nda,
  num=8,version=1"; deny (write) userdn = "ldap:///self" and
  userdn != "ldap:///<OrgRoot>??sub?(memberOf=cn=Domain Administrators*)"
  and userdn !=
  "ldap:///<DCRoot>??sub?(memberOf=cn=Domain Administrators*)"
  and groupdn != "ldap:///cn=Service Administrators,ou=groups,<OrgRoot>");)
#
# self に対して、削除アクセスを拒否する
#
aci: (targetfilter=(objectClass=inetOrgPerson)) (version 3.0; acl
  "User self deletion - product=ims5.0,class=nda,num=9,version=1";
  deny (delete) userdn="ldap:///self");)
#
#-----
# メールリストのアクセス制御
#
# 指定したユーザによるメールリストの作成を許可する
#
aci: (targetattr="*") (targetfilter=(objectClass=inetMailGroupManagement))
  (version 3.0; acl "Mail list create access - product=ims5.0,class=nda,
  num=10,version=1"; allow (add)
  userdn="ldap:///<OrgRoot>??sub?(nsDACapability=mailListCreate)");)

```

コード例 A-1

組織ツリールートノード ACI (続き)

```

#
# nsMaxUsers 属性を除き、メールリスト所有者が所有するメールリストへの
# 読み取り、検索、書き込み、削除のアクセスを許可する
#
aci: (targetattr="*)(targetfilter=(objectClass=inetMailGroupManagement))
  version 3.0; acl "Mail list owner access - product=ims5.0,class=nda,num=11,
  version=1"; allow (read,search,write,delete)
  groupdnattr="ldap:///<OrgRoot>?owner";)
#
#-----
# ファミリーグループ管理者のアクセス制御
#
# ファミリーグループの読み取りアクセス権
#
aci: (targetattr="*)(targetfilter=(objectClass=inetManagedGroup))
  (version 3.0; acl "Family Group Adm group read & search access -
  product=ims5.0,class=nda,num=12,version=1"; allow (read,search)
  userdn="ldap:///<OrgRoot>??sub?(memberOf=cn=Family Group
  Administrators*)" and groupdnattr="ldap:///<OrgRoot>?nsDAModifiableBy";)
#
# ファミリーグループの description 属性に対する書き込みアクセス権
#
aci: (targetattr="description")
  (targetfilter=(objectClass=inetManagedGroup))
  (version 3.0; acl "Family Group Adm description write access -
  product=ims5.0,class=nda,num=13,version=1"; allow (write)
  userdn="ldap:///<OrgRoot>??sub?(memberOf=cn=Family Group
  Administrators*)" and groupdnattr="ldap:///<OrgRoot>?nsDAModifiableBy";)
#
# ファミリーグループの mnggrpCurrentUsers 属性に対する書き込みアクセス権
#
aci: (targetattr="mnggrpCurrentUsers")
  (targetfilter=(objectClass=inetManagedGroup)) (version 3.0; acl "Family
  Group Adm description write access - product=ims5.0,class=nda,num=14,
  version=1"; allow (write)
  userdn="ldap:///<OrgRoot>??sub?(memberOf=cn=Family Group
  Administrators*)" and groupdnattr="ldap:///<OrgRoot>?nsDAModifiableBy";)
#
# ファミリーグループメンバーの作成、削除、変更に関する許可
#
aci: (targetattr="*)(targetfilter=(objectClass=nsManagedPerson))
  (version 3.0;acl "Family Group Adm member access - product=ims5.0,
  class=nda, num=15,version=1"; allow (add,read,search,write,delete)
  userdn="ldap:///<OrgRoot>??sub?(memberOf=cn=Family Group
  Administrators*)" and groupdnattr="ldap:///<OrgRoot>?nsDAModifiableBy";)
#
# 同一管理グループのファミリー管理者の追加と削除を行うためのアクセス権
#
aci: (targetattr="uniquemember")
  (targetfilter=(&(|(objectClass=nsManagedDept)
  (objectClass=nsManagedDeptAdminGroup))(cn=Family Group
  Administrators*))) (version 3.0;acl "Family Group Adm admin write
  access - product=ims5.0,class=nda,num=16,version=1"; allow (write)
  userdn="ldap:///<OrgRoot>??sub?(memberOf=cn=Family Group

```

コード例 A-1 組織ツリールートノード ACI (続き)

```

Administrators*)" and groupdnattr="ldap:///<OrgRoot>?uniquemember");)
#
#memberof 属性の追加と削除を行うためのアクセス権
#
aci: (targetattr="memberOf") (targetfilter=(objectClass=nsManagedPerson))
(version 3.0;acl "Family Adm user access -
product=ims5.0,class=nda,num=17,version=1"; allow (write)
userdn="ldap:///<OrgRoot>??sub?(memberOf=cn=Family Group
Administrators*)" and groupdnattr="ldap:///<OrgRoot>?nsDAModifiableBy");)
#
#-----
#ドメイン組織管理者
#
#ドメイン組織ノードに対するアクセス権
#
aci: (targetattr="*") (targetfilter=(objectClass=inetdomainorg)) (version
3.0; acl "Domain Organization Administrator - Dom Org node read & search
access - product=ims5.0,class=nda,num=21,version=1"; allow (read,search)
groupdnattr="ldap:///<OrgRoot>?nsDAModifiableBy");)
#
#選択した属性に対する書き込みアクセス権
#
aci: (targetattr="description||domOrgMaxUsers")
(targetfilter=(objectClass=inetdomainorg)) (version 3.0; acl "Domain
Organization Administrator - Dom Org node write access -
product=ims5.0,class=nda,num=22,version=1"; allow (write)
groupdnattr="ldap:///<OrgRoot>?nsDAModifiableBy");)

```

DC ツリールートノード ACI

次に示す ACI は、トップレベル管理者、ドメイン管理者、ドメイン組織管理者、ファミリーグループ管理者、メールリスト所有者、エンドユーザに必要なアクセス権を与えます。必要な場合は、ツリー内の下位のドメインノードやドメイン組織ノードで、追加の ACI を設定します。ネームスペースのセットアップを最初から手動で行う場合（つまり、ネームスペースの作成に iPlanet Messaging Server インストーラを使用しない場合）、DC ツリーノードで ACI を設定する必要があります。

コード例 A-2 DC ツリールートノード ACI

```

dn: <DCRoot>
changetype: modify
add: aci:
#-----
#
#iDA ユーザのアクセス制御
#
#すべてのエントリ内のすべての属性に対する読み取りと検索のアクセスを許可する

```

```

#
aci: (targetattr="*") (version 3.0; acl "NDAUser access -
product=ims5.0,class=nda,num=1,version=1"; allow (read,search)
userdn="ldap:///uid=NDAUser,ou=config,<OrgRoot>");)
#
# すべてのドメインエントリの nsNum* 属性に対する書き込みアクセスを許可する
#
aci: (targetattr="nsNumUsers|nsNumDepts|nsNumMailLists|nsNumDomains")
(version 3.0; acl "NDAUser access - product=ims5.0,class=nda,num=2,
version=1"; allow (write) userdn="ldap:///uid=NDAUser,
ou=config,<OrgRoot>");)
#
#-----
# サービス管理者のアクセス制御
#
# すべての DCROOT ノードに対する読み取りと検索のアクセスを許可する
#
aci: (targetattr="*") (version 3.0; acl "SA root node access -
product=ims5.0,class=nda,num=3,version =1"; allow (all)
groupdn="ldap:///cn=Service Administrators,ou=Groups,<OrgRoot>");)
#
#-----
# ドメイン管理者の制御
#
# ドメインコンポーネントを検索するための dcroot に対するアクセス権
#
aci: (targetattr="*") (version 3.0; acl "Domain Admin dc root access -
product=ims5.0,class=nda,num=4 ,version=1"; allow (read,search)
userdn="ldap:///<DCRoot>??sub?(memberOf=cn=Domain Administrators*)" or
userdn="ldap:///<OrgRoot>??sub?(memberOf=cn=Domain Administrators*");)
#
# すべてのドメインコンテナノードに対する書き込みと削除のアクセスを拒否する
#
aci: (targetfilter="objectclass=nsManagedDomain") (version 3.0; acl
"Domain Admin domain container access -
product=ims5.0,class=nda,num=5,version=1"; deny (delete,write)
userdn="ldap:///<DCRoot>??sub?(memberOf=cn=Domain Administrators*)" or
userdn="ldap:///<OrgRoot>??sub?(memberOf=cn=Domain Administrators*");)
#
#-----
# ユーザのアクセス制御
#
# self に対して、読み取りと検索のアクセスを許可する
#
aci: (targetattr="*") (targetfilter=(objectClass=inetOrgPerson)) (version
3.0; acl "User self search and read - product=ims5.0,class=nda, num=6,
version=1"; allow (read,search) userdn="ldap:///self");)
#
# self に対して、書き込みアクセスを許可する
#
aci: (targetattr = "*") (version 3.0; acl "Allow self entry modification
- product=ims5.0,class=nda,num=7,version=1"; allow (write) userdn =
"ldap:///self");)
#

```

コード例 A-2

DC ツリールートノード ACI (続き)

```

# uid, ou, owner, nsDAModifiableBy, nsDACapability,
# mail, mailAlternateAddress, memberOf, および nsDADomain 属性の
# self に対して、書き込みアクセスを拒否する
#
aci: (targetattr="uid|ou|owner|nsDAModifiableBy|nsDACapability|
mail|mailAlternateAddress|memberOf|nsDADomain|inetuserstatus|
mailuserstatus|memberOfManagedGroup|mailQuota|mailMsgQuota|
inetSubscriberAccountId|dataSource|mailhost|mailAllowedServiceAccess
|pabURI|inetCOS") (targetfilter=(objectClass=nsManagedPerson))
(version 3.0; acl "User self modification - product=ims5.0,class=nda,
num=8, version=1"; deny (write) userdn = "ldap:///self" and userdn
!= "ldap:///<DCRoot>??sub?(memberOf=cn=Domain Administrators*)" and
userdn != "ldap:///<OrgRoot>??sub?(memberOf=cn=Domain Administrators*)"
and groupdn != "ldap:///cn=Service Administrators,ou=groups,<OrgRoot>");)
#
# self に対して、削除アクセスを拒否する
#
aci: (targetfilter=(objectClass=inetOrgPerson)) (version 3.0; acl "User
self deletion - product=ims5.0,class=nda,num=9,version=1"; deny (delete)
userdn="ldap:///self");)
#
#-----
# メールリストのアクセス制御
#
# 指定したユーザによるメールリストの作成を許可する
#
aci: (targetattr="*") (targetfilter=(objectClass=inetMailGroupManagement))
(version 3.0; acl "Mail list create access - product=ims5.0,class=nda,
num=10, version=1"; allow (add)
userdn="ldap:///<DCRoot>??sub?(nsDACapability=mailListCreate)");)
#
# nsMaxUsers 属性を除き、メールリスト所有者が所有するメールリストへの
# 読み取り、検索、書き込み、削除のアクセスを許可する
#
aci: (targetattr="*") (targetfilter=(objectClass=inetMailGroupManagement))
(version 3.0; acl "Mail list owner access -
product=ims5.0,class=nda,num=11,version=1"; allow (read,search,write,delete)
groupdnattr="ldap:///<DCRoot>?owner");)
#
#-----
# ファミリーグループ管理者のアクセス制御
#
# ファミリーグループの読み取りアクセス権
#
aci: (targetattr="*") (targetfilter=(objectClass=inetManagedGroup))
(version 3.0; acl "Family Group Adm group read & search access -
product=ims5.0 ,class=nda,num=12,version=1"; allow (read,search)
userdn="ldap:///<DCRoot>??sub?(memberOf=cn=Family Group
Administrators*)" and groupdnattr="ldap:///<DCRoot>?nsDAModifiableBy");)
#
# ファミリーグループの description 属性に対する書き込みアクセス権
#
aci: (targetattr="description")

```

コード例 A-2

DC ツリールートノード ACI (続き)

```

(targetfilter=(objectClass=inetManagedGroup)) (version 3.0; acl "Family
Group Adm description write access -
product=ims5.0,class=nda,num=13,version=1"; allow (write)
userdn="ldap:///<DCRoot>??sub?(memberOf=cn=Family Group
Administrators*)" and groupdnattr="ldap:///<DCRoot>?nsDAModifiableBy";)
#
# ファミリーグループの mnggrpCurrentUsers 属性に対する書き込みアクセス権
#
aci: (targetattr="mnggrpCurrentUsers")
(targetfilter=(objectClass=inetManagedGroup)) (version 3.0; acl "Family
Group Adm description write access -
product=ims5.0,class=nda,num=14,version=1"; allow (write)
userdn="ldap:///<DCRoot>??sub?(memberOf=cn=Family Group
Administrators*)" and groupdnattr="ldap:///<DCRoot>?nsDAModifiableBy";)
#
# ファミリーグループメンバーの作成、削除、変更に関する許可
#
aci: (targetattr="*") (targetfilter=(objectClass=nsManagedPerson))
(version 3.0;acl "Family Group Adm member access -
product=ims5.0,class=nda,num=15,version=1"; allow
(add,read,search,write,delete)
userdn="ldap:///<DCRoot>??sub?(memberOf=cn=Family Group
Administrators*)" and groupdnattr="ldap:///<DCRoot>?nsDAModifiableBy";)
#
# 同一管理グループのファミリー管理者の追加と削除を行うためのアクセス権
#
aci: (targetattr="uniquemember")
(targetfilter=(&(|(objectClass=nsManagedDept)(objectClass=nsManagedDept
AdminGroup))(cn=Family Group Administrators*))) (version 3.0;acl "Family
Group Adm admin write access - product=ims5.0,class=nda,num=16,
version=1"; allow (write) userdn="ldap:///<DCRoot>??sub?(memberOf=cn=
Family Group Administrators*)" and
groupdnattr="ldap:///<DCRoot>?uniquemember";)
#
# memberof 属性の追加と削除を行うためのアクセス権
#
aci: (targetattr="memberOf") (targetfilter=(objectClass=nsManagedPerson))
(version 3.0;acl "Family Adm user access - product=ims5.0,class=nda,
num=17,version=1"; allow (write)
userdn="ldap:///<DCRoot>??sub?(memberOf=cn=Family Group
Administrators*)" and groupdnattr="ldap:///<DCRoot>?nsDAModifiableBy";)
#
# ファミリー管理者は、dn を取得するためにドメインを読み取る必要がある
#
aci: (targetattr="objectclass|preferredmailhost||
preferredmailmessagestore") (targetfilter=(objectClass=domain)) (version
3.0;acl "Family Adm domain access - product=ims5.0,class=nda,num=18,
version=1"; allow (read,search)
userdn="ldap:///<OrgRoot>??sub?(memberOf=cn=Family Group
Administrators*)" or userdn="ldap:///<DCRoot>??sub?(memberOf=cn=Family
Group Administrators*");)
#
# -----
# ドメイン組織管理者
#

```

コード例 A-2 DC ツリールートノード ACI (続き)

```
# ドメイン組織管理者による
# dc ツリーからの属性読み取りを許可する
#
aci: (targetattr="objectclass||preferredmailhost||
preferredmailmessagestore||dc") (targetfilter=(objectClass=domain))
(version 3.0;acl "Domain Organization Admin domain access -
product=ims5.0,class=nda,num=20,version=1"; allow (read,search)
userdn="ldap:///<DCRoot>??sub?(memberOf=cn=Domain Organization
Administrators*)" or userdn="ldap:///<OrgRoot>??sub?(memberOf=cn=Domain
Organization Administrators*)" );)
#
# ドメイン組織ノードに対するアクセス権
#
aci: (targetattr="*") (targetfilter=(objectClass=inetdomainorg)) (version
3.0; acl "Domain Organization Administrator - Dom Org node read & search
access - product=ims5.0,class=nda,num=21,version=1"; allow (read,search)
groupdnattr="ldap:///<DCRoot>?nsDAModifiableBy";)
#
# 選択した属性に対する書き込みアクセス権
#
aci: (targetattr="description||domOrgMaxUsers")
(targetfilter=(objectClass=inetdomainorg)) (version 3.0; acl "Domain
Organization Administrator - Dom Org node write access -
product=ims5.0,class=nda,num=22,version=1"; allow (write)
groupdnattr="ldap:///<DCRoot>?nsDAModifiableBy";)
```

ホストドメイン ACI

次に示す ACI は、ドメイン管理者、メールリスト所有者、エンドユーザに必要なアクセス権を与えます。これらの 6 つの ACI は、標準の二重ツリーネームスペースで使用します。5 つの規則は組織ツリーで設定し、1 つの規則は DC ツリーで設定します。1 つの DC ツリーだけを含むネームスペースを使用している場合は、6 つの規則はすべてホストドメインノードで設定します。これらの ACI は、プロビジョニングを行うすべてのドメインで設定する必要があります。

コード例 A-3 ホストドメイン ACI

```
dn: <OrgNodeDN>
changetype: modify
add: aci:
#
#-----
# ドメイン管理者のアクセス制御
#
# ドメインのユーザおよびグループのサブツリーに対するフルアクセスを許可する
#
aci: (targetattr="*") (version 3.0; acl "Domain Admin Domain access -
product=ims5.0,class=nda,num=18,version=1"; allow (all)
groupdn="ldap:///cn=Domain Administrators,ou=Groups,<OrgNodeDN>";)
#
#-----
# エンドユーザのアクセス制御
# ユーザによるドメイン内のすべてのユーザの読み取りと検索を許可する
#
aci: (targetattr!="userPassword")
(targetfilter=(|(objectClass=inetOrgPerson)(objectclass=nsManagedDomain
))) (version 3.0; acl "User access to all users in domain -
product=ims5.0,class=nda,num=19,version=1"; allow (read,search)
userdn="ldap:///<OrgNodeDN>??sub?(objectclass=inetOrgPerson)";)
#
# ユーザによる自己登録制メールリストへのユーザ自身の追加を許可する
#
aci: (targetattr="uniqueMember")
(targetfilter=(&(objectClass=nsManagedMailList)
(|(mgmanJoinability=anyone)(mgmanJoinability=all))))
(version 3.0; acl "User mail list self subscribe access -
product=ims5.0,class=nda,num=20,version=1"; allow (selfwrite)
userdn="ldap:///<OrgNodeDN>??sub?(objectclass=inetOrgPerson)";)
#
# 非表示のマークが付けられたグループメンバーを隠す
#
aci: (targetattr!="uniqueMember||mgrpRfc822MailMember")
(targetfilter=(&(objectClass=inetMailGroupManagement)
(mgmanHidden=false))) (version 3.0; acl "User mail list access when
visible - product=ims5.0,class=nda,num=21,version=1"; allow
(read,search)
userdn="ldap:///<OrgNodeDN>??sub?(objectclass=inetOrgPerson)";)
#
```

コード例 A-3 ホストドメイン ACI (続き)

```
# 非表示のマークが付けられたグループメンバーを隠す
#
aci: (targetattr="uniqueMember||mgrpRfc822MailMember")
      (targetfilter=(amp(objectClass=inetMailGroupManagement)
                       (|(mgmanMemberVisibility=anyone)(mgmanMemberVisibility=all)))) (version
3.0; acl "User mail list member access -
product=ims5.0,class=nda,num=22,version=1"; allow (read,search)
userdn="ldap:///<OrgNodeDN>??sub?(objectclass=inetOrgPerson)");)

dn: <DCNodeDN>
changetype: modify
add: aci:
#
#-----
# ドメイン管理者の ics 属性に対するアクセス権
#
aci: (targetattr="icsTimeZone||icsMandatorySubscribed||
icsMandatoryView||icsDefaultAccess||icsRecurrenceBound||
icsRecurrenceDate||icsAnonymousLogin||icsAnonymousAllowWrite||
icsAnonymousCalendar||icsAnonymousSet||icsAnonymousDefaultSet||
icsSessionTimeout||icsAllowRights||icsExtended||
icsExtendedDomainPrefs") (targetfilter=(objectClass=icsCalendarDomain))
(version 3.0; acl "Domain Adm calendar access - product=ims5.0,
class=nda,num=16,version=1"; allow (all) groupdn="ldap:///cn=Domain
Administrators,ou=Groups,<OrgNodeDN>");)
```

ドメイン組織 ACI

次に示す ACI は、プロビジョニングを行うすべてのドメイン組織に追加する必要があります。

コード例 A-4

ドメイン組織 ACI

```
dn: <DomainOrgNodeDN>
changetype: modify
add: aci:
#
# ユーザの変更、追加、削除を行う権限
#
aci: (target="ldap:///uid=*,ou=people,<DomainOrgNodeDN>")
      (targetattr ="*")
      (targetfilter=(objectclass=organizationalPerson))
      (version 3.0; acl "Domain Organization Admin User add,delete,write -
product=ims5.0,class=nda,num=201,version=1";
allow (add,write,delete)
groupdn="ldap:///cn=Domain Organization
Administrators,<DomainOrgNodeDN>";)
#
# メールングリストの変更、追加、削除を行う権限
#
aci: (target="ldap:///cn=*,ou=groups,<DomainOrgNodeDN>")
      (targetattr ="*")
      (targetfilter=(objectclass=inetMailGroup))
      (version 3.0; acl "Domain Organization Admin User add,delete,write -
product=ims5.0,class=nda,num=202,version=1";
allow (add,write,delete)
groupdn="ldap:///cn=Domain Organization
Administrators,<DomainOrgNodeDN>";)
```

用語集

/var/mail 新しいメールメッセージを順番に単一のフラットテキストファイル内に格納する Berkeley 方式の受信箱を示すために使用される名前。

A レコード (A record) ホスト名および関連付けられた IP アドレスを含む DNS レコードの一種。A レコードは、Messaging Server がインターネット上で電子メールをルーティングするために使用します。ドメインネームシステム (DNS)、MX レコードも参照してください。

Administration Server 管理者 (administration server administrator) Directory Server に接続していない場合でも、サーバの起動および停止を行う管理権限を持つユーザ。Administration Server 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停止のみ) を実行できます。Administration Server をインストールすると、この管理者のエントリが自動的にローカルに作成されます (この管理者はユーザディレクトリ内のユーザではありません)。

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使用します。

AUTH SMTP コマンドの 1 つ。SMTP クライアントがサーバに対して認証方法を指定したり、認証プロトコル交換を実行したり、必要に応じて後続プロトコルの相互対話で使用するセキュリティ層をネゴシエートしたりできるようにします。

Berkeley DB トランザクション用のデータベースストアで、読み取りと書き込みの同時実行の負荷が大きく、さらにトランザクションと回復可能性が要求されるアプリケーションで使用します。

CA 認証局。デジタル証明書 (デジタルの識別子) を発行し、その公開鍵を対象者が広く利用できるようにする組織。

capability クライアントに提供され、特定の IMAP サービスで利用可能な機能を定義する文字列。

cipher 暗号化で使用するアルゴリズム。

ciphertext (暗号文) 暗号化されたテキスト。**cleartext (平文)** の対語です。

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フェースを参照してください。

cn 共通名を表す LDAP エイリアス。

CNAME レコード (CNAME record) ドメイン名の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。

Configuration Directory Server 単一サーバまたはサーバのセットの構成情報を保持する Directory Server。

cookie 特定の Web サイトを訪れたときに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 ページ作成者によってプログラムされます。ユーザは、**cookie** を受け入れることも、拒否することもできます。**cookie** を受け入れると、Web ページを高速に読み込むことができます。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。

CRAM-MD5 RFC 2195 に記述されている軽量な標準化過程の認証方法。ネットワークでユーザのログインパスワードだけを保護する場合に、TLS (SSL) の代わりに使用できます。TLS より高速ですが、やや強度が落ちます。

cronjob UNIX 専用。指定した時間に cron デーモンによって自動的に実行されるタスク。**crontab ファイル** も参照してください。

crontab ファイル (crontab file) UNIX 専用。指定した時間に自動的に実行されるコマンドのリスト。1 行に 1 つずつ記述されています。

DC ツリー (DC Tree) ドメインコンポーネント (Domain Component) ツリー。DNS ネットワーク構造を反映するディレクトリ情報ツリー。DC ツリー内の識別名は、**cn=billbob,dc=bridge,dc=net,o=internet** のようになります。

Delegated Administration Server ホストドメインによるディレクトリへのアクセス制御を処理するデーモンプログラム。

Delegated Administrator Console Web ブラウザベースのソフトウェアコンソール。ドメイン管理者はこれを使用して、ホストドメインに対してユーザやグループの追加または変更を行うことができます。また、エンドユーザは、これを使用して、自分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、メールリスト購読の一覧表示などを行うことができます。

Delegated Administrator for Messaging and Collaboration ドメイン管理者がホストドメインに対してユーザやグループの追加または変更を行うために使用する一連のインタフェース (GUI とユーティリティ)。

DIGEST-MD5 CRAM-MD5 より安全で軽量な標準化過程の認証方法。RFC 2831 に記述されています。RFC 2831 には、TLS (SSL) のような設定の手間をかけずに接続全体を保護するオプションも記述されています。

Directory Manager 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。Directory Manager はディレクトリのスーパーユーザと考えることができます。

Directory Server LDAP に基づく iPlanet のディレクトリサービス。**ディレクトリサービス**、**Lightweight Directory Access Protocol**、**Configuration Directory Server**、**Users and Groups Directory Server** も参照してください。

DIT **ディレクトリ情報ツリー**を参照してください。

DN **識別名**を参照してください。

dn 識別名のための LDAP エイリアス。**識別名**も参照してください。

DNS **ドメインネームシステム**を参照してください。

DNS エイリアス (DNS alias) DNS サーバが、別のホスト (DNS CNAME レコード) へのポインタとして認識するホスト名。マシンの実際の名前は 1 つだけですが、1 つまたは複数のエイリアスを持つことができます。たとえば、**www.siroe.domain** を現在サーバが置かれている **realthing.siroe.domain** という実際のマシンをポイントするエイリアスとすることができます。

DNS スプーフィング (DNS spoofing) DNS サーバが不正情報を提供するように仕向けるネットワーク攻撃の形態。

DNS データベース (DNS database) 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。

DNS ドメイン (DNS domain) 共通の接尾辞 (ドメイン名) の付いたホスト名を持つコンピュータのグループ。構文的には、ピリオド (ドット) で区切られた一連の名前 (ラベル) から成るインターネットドメイン名です。たとえば **corp.mktng.siroe.com** などです。**ドメイン**も参照してください。

DSN **配信ステータス通知**を参照してください。

dsservd ディレクトリ情報が格納されたデータベースにアクセスし、LDAP プロトコルを使用してディレクトリクライアントと通信するデーモン。

dssetup 既存の Directory Server を iPlanet Messaging Server で使用できるように準備する Directory Server 準備ツール。

EHLO コマンド (EHLO command) 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 に定義されています。

ESMTP **Extended Simple Mail Transfer Protocol** を参照してください。

ESP Enterprise Service Provider (エンタープライズサービスプロバイダ) の略。

ETRN クライアントからサーバに対して、サーバ上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の処理を開始するように要求する SMTP コマンド。RFC 1985 に定義されています。

EXPN メールリストを展開するための SMTP コマンド。RFC 821 に定義されています。

Extended Simple Mail Transfer Protocol (ESMTP) インターネットメッセージ転送プロトコルの一種。ESMTP では、SMTP コマンドセットにオプションのコマンドを追加することで、その機能が拡張されています。ESMTP サーバが、リモートサイトで実装されているコマンドを検出する機能などが含まれます。

facility (機能) Messaging Server ログファイルエントリ内での、ログエントリを生成したソフトウェアサブシステム (ネットワークやアカウントなど) の指定。

FQDN **完全指定ドメイン名**を参照してください。

GUI グラフィカルユーザインタフェース。

HA **高可用性**を参照してください。

hashdir 特定ユーザのメッセージストアが含まれるディレクトリを調べるためのコマンドラインユーティリティ。

HTTP **HyperText Transfer Protocol** を参照してください。

HyperText Transfer Protocol (HTTP) 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。**Messenger Express** も参照してください。

IDENT **Identification Protocol** を参照してください。

Identification Protocol 特定の TCP 接続のリモート端末を制御するリモートプロセスを識別できるようにするプロトコル。RFC 1413 に定義されています。

IMAP4 **Internet Message Access Protocol Version 4** を参照してください。

imsadmin コマンド (imsadmin commands) 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のセット。

imsimta コマンド (imsimta commands) MTA (Message Transfer Agent) の各種の保守、テスト、管理を行うためのコマンドラインユーティリティのセット。

INBOX メール配信用のユーザのデフォルトメールボックス用に予約されている名前。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、以下のように記述します。INBOX、Inbox、inbox は、すべてユーザのデフォルトのメールボックスとして有効な名前です。

Internet Message Access Protocol Version 4 (IMAP4) ユーザがメインのメッセージ送信システムから切断された場合でもメールを処理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、メッセージング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。

IP インターネットプロトコルを参照してください。

IP アドレス (IP address) 198.93.93.10 のような、ドットで区切られた一連の数値で、イントラネットまたはインターネット上でのマシンの実際の場所を示します。TCP/IP を使用するホストには、32 ビットのアドレスが割り当てられます。

iPlanet Setup すべての iPlanet サーバおよび iPlanet Console 用のインストールプログラム。

ISP Internet Service Provider (インターネットサービスプロバイダ) の略。電子メール、電子カレンダー、World Wide Web へのアクセス、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です。

LDAP Lightweight Directory Access Protocol を参照してください。

LDAP Data Interchange Format (LDIF) Directory Server エントリをテキスト形式で表すために使用する形式。

LDAP 検索文字列 (LDAP search string) ディレクトリ検索に使用される属性を定義する、置換可能なパラメータを含む文字列。たとえば、「uid=%s」という LDAP 検索文字列は、検索の基準がユーザ ID 属性であることを意味します。

LDAP サーバ (LDAP Server) LDAP ディレクトリを管理し、そのディレクトリに対する照会サービスを提供するソフトウェアサーバ。iPlanet ディレクトリサービスは LDAP サーバの実装です。

LDAP サーバフェイルオーバー (LDAP server failover) LDAP サーバのバックアップ機能。1 つの LDAP サーバに障害が発生した場合、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 転送 (LDAP referrals) 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 転送は、LDAP ホストと識別名から構成されます。通常、LDAP 転送は、データをレプリケートしないで、既存の LDAP データを参照するために使用されます。また、移動された特定のエンタ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 フィルタ (LDAP filter) 特定の属性または属性値の有無に基づいて一連のエンタリを指定する方法。

LDBM LDAP Data Base Manager の略。

LDIF LDAP Data Interchange Format を参照してください。

Legato Networker Legato® が提供するサードパーティ製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でき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、メールリスト、複数の iPlanet サーバ上の設定データなどの情報の格納、検索、および配布を単一の場所で管理できるようにします。iPlanet Directory Server は、LDAP プロトコルを使用します。

mailbox メッセージの格納と表示を行う場所。**フォルダ**も参照してください。

MD5 RSA Data Security によって提供されるメッセージダイジェストアルゴリズム。MD5 を使用すると、一意になる確率が高い短い形式のダイジェストデータを生成できます。同一のメッセージダイジェスト電子メールが生成されるようなデータを作成することは数学的に非常に困難です。

Message Handling System (MHS) 接続されている MTA、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と配信専用のプログラム。複数の MTA が連携してメッセージを転送し、目的の受取人に配信します。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、リモート配信のために別の MTA にルーティングするのかを決定します。

Messaging Multiplexor (MMP) 複数のメールサーバに対する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多数のユーザへの配信を円滑に行うための特別な iPlanet Messaging Server。

Messaging Server 管理者 (Messaging Server administrator) iPlanet Messaging Server インスタンスのインストールや管理などの権限を持つ管理者。

Messenger Express ユーザがブラウザベース (HTTP) のインタフェースを介し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、その他のメールボックス情報は、HTML 形式でブラウザのウィンドウに表示されます。**Web メール**も参照してください。

Messenger Express Multiplexor マルチプレクサとして機能するメッセージングプロキシサーバで、ユーザが iPlanet Messaging Server の HTTP サービス (Messenger Express) に接続できるようにします。Messenger Express Multiplexor を使用すると、複数のサーバマシンにユーザを分散できるようになります。

MHS Message Handling System を参照してください。

MIME Multipurpose Internet Mail Extension を参照してください。

MMP Messaging Multiplexor を参照してください。

MTA Message Transfer Agent を参照してください。

MTA 設定ファイル (MTA configuration file) Messaging Server のすべてのチャンネル定義と、ルーティングのためのアドレス書き換え規則を含むファイル (imta.cnf)。**チャンネル、書き換え規則**も参照してください。

MTA ディレクトリキャッシュ (MTA directory cache) 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で、MTA がメッセージを処理するために必要とします。**ディレクトリの同期**も参照してください。

MTA ホップ (MTA hop) 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を参照してください。

Multiplexor Messaging Multiplexor を参照してください。

Multipurpose Internet Mail Extension (MIME) 電子メールメッセージ内にマルチメディアファイルを追加できるようにするために使用されるプロトコル。

MX レコード (MX record) メール交換レコード。ホスト名を別のホスト名にマップする、DNS レコードの一種。

NDN 非配信通知を参照してください。

NOTARY メッセージ (notary messages) RFC 1892 の NOTARY 仕様に準拠した非配信通知 (NDN) および配信ステータス通知 (DSN)。

OSI ツリー (OSI tree) Open Systems Interconnect ネットワーク構造を反映するディレクトリ情報ツリー。OSI ツリー内の識別名は、cn=billt,o=bridge,c=us のようになります。

POP3 **Post Office Protocol Version 3** を参照してください。

Post Office Protocol Version 3 (POP3) 標準の配信方法を提供するプロトコル。このプロトコルを使用する場合、MTA (Message Transfer Agent) 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。アクセス権が不要なことは、メールクライアントと MTA が別のコンピュータに置かれることが多いネットワーク環境で利点となります。

RC2 RSA Data Security によって提供される可変鍵サイズによるブロック暗号化方式。

RC4 RSA Data Security によって提供されるストリーム暗号化方式。RC2 よりも高速に処理できます。

RDN 相対識別名。実際のエントリ自体の名前。この文字列にエントリの祖先を付加すると完全な識別名になります。

RFC Request For Comments の略。1969 年に開始されたドキュメントシリーズで、インターネットの一連のプロトコルと、関連する実験について記述されています。インターネット標準について記述した RFC の数はわずかですが、すべてのインターネット標準が RFC として公開されています。<http://www.imc.org/rfc.html> を参照してください。

SASL **Simple Authentication and Security Layer** を参照してください。

SCM **Service Control Manager** を参照してください。

Secure Sockets Layer (SSL) クライアントとサーバの間で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、sendmail の代わりに iPlanet Messaging Server を使用できます。

Service Control Manager サービスを管理するための Windows NT の管理プログラム。

Sieve メールの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から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 での SMTP SASL の使用は、RFC 2554 (ESMTP AUTH) に準拠しています。SASL は、RFC 2222 に定義されています。

Simple Mail Transfer Protocol (SMTP) インターネットでもっとも一般的に使用される電子メールプロトコルで、iPlanet Messaging Server でもサポートされています。RFC 821 に定義されています。関連するメッセージ形式は RFC 822 に記述されています。

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対して宣言できるようにする SMTP 拡張機能。サーバは、宣言されたメッセージサイズに基づいて、メッセージ受信の可否をクライアントに示すことができます。サーバは、受信可能なメッセージの最大サイズをクライアントに宣言できます。RFC 1870 に定義されています。

SMTP Simple Mail Transfer Protocol を参照してください。

SMTP AUTH AUTH を参照してください。

sn 苗字を表すエイリアスディレクトリ属性。

SSL Secure Sockets Layer を参照してください。

SSR サーバ側規則を参照してください。

TCP Transmission Control Protocol を参照してください。

TCP/IP Transmission Control Protocol/Internet Protocol を参照してください。

TLS Transport Layer Security を参照してください。

Transmission Control Protocol (TCP) 2つのホスト間での信頼性の高い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群内の基本転送プロトコル。

Transmission Control Protocol/Internet Protocol (TCP/IP) インターネットプロトコルで 사용되는複数のネットワークプロトコルの総称。この名前は、トランスポート層のプロトコルである TCP (Transmission Control Protocol) とネットワーク層のプロトコルである IP (Internet Protocol) の2つの主要ネットワークプロトコルを指します。

Transport Layer Security (TLS) SSL を標準化したもの。**Secure Sockets Layer** も参照してください。

UA ユーザエージェントを参照してください。

UBE Unsolicited Bulk Email を参照してください。

UID (1) ユーザ識別子。システムでユーザを識別するための一意の文字列。ユーザ ID とも呼ばれます。(2) ユーザ ID (ログイン名) のエイリアスディレクトリ属性。

Unsolicited Bulk Email (UBE) 一般に宣伝目的でメール送信業者から大量に送信される迷惑メール。

Users and Groups Directory Server (User/Groups Directory Server) 組織内のユーザおよびグループに関する情報を保持する Directory Server。

UUCP UNIX to UNIX Copy Program (UNIX から UNIX へのコピープログラム) の略。UNIX システム間での通信に使用されるプロトコルです。

Veritas Cluster Server iPlanet Messaging Server と統合できる Veritas Software 製の高可用性クラスタリングソフトウェア。

VERFY ユーザ名を確認するための SMTP コマンド。RFC 821 に定義されています。

Web サーバ (Web server) World Wide Web アクセスを提供するために導入されるソフトウェアプログラムまたはサーバコンピュータ。Web サーバは、ユーザからの要求を受け取り、要求されたファイルやアプリケーションを検索し、さらにエラーメッセージを発行します。

Web メール (webmail) ブラウザベースの電子メールサービスを示す一般的な用語。ブラウザベースのクライアントは、多くの処理をサーバに任せるので、「シンクライアント」とも呼ばれ、常にサーバ上に格納されるメールにアクセスします。**Messenger Express** も参照してください。

X.400 メッセージ処理システムの標準。

アカウント (account) 特定のユーザまたはユーザグループを定義する情報。この情報には、ユーザやグループの名前、1 つまたは複数の有効な電子メールアドレス、および電子メールの配信方法と配信先が含まれます。

アクセス制御 (access control) サーバ、また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方法。

アクセス制御規則 (access control rules) 特定のディレクトリエントリまたは属性のセットに対するユーザの権限を指定する規則。

アクセス制御情報 (access control information) ACI。アクセス制御リストの単一の情報項目。

アクセス制御リスト (access control list) ACL。ディレクトリに対するユーザやグループのアクセス権を定義するためにディレクトリに関連付けられた一連のデータ。

アクセスドメイン (access domain) 指定したドメイン内から利用できる Messaging Server 操作を制限します。たとえば、アクセスドメインを使用すると、特定のアカウント宛てのメールを収集できる場所を制限できます。

アドレス (address) 電子メールメッセージの送信先と送信方法を決定するメッセージ内の情報。アドレスはメッセージヘッダーとメッセージエンベロープの両方に表示されます。エンベロープアドレスは、メッセージのルーティング方法と配信方法を決定します。ヘッダーアドレスは表示専用です。

アドレス指定プロトコル (addressing protocol) 電子メールの利用を可能にするアドレス指定規則。RFC 822 は、インターネット上でもっと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 や UUCP (UNIX to UNIX Copy Protocol) などがあります。

アドレス処理 (address handling) アドレス指定のエラーを検出し、必要に応じてアドレスを書き換え、アドレスと受取人の照合を行うために MTA によって実行される処理。

アドレストークン (address token) 書き換え規則パターン of アドレス要素。

暗号化 コードキーを持つ特定の受取人以外には解読できないように情報を隠すプロセス。

安全なファイルシステム (safe file system) システムがクラッシュした場合に、データをクラッシュ前の状態にロールバックし、すべてのデータをリストアできるようにログを記録しているファイルシステム。安全なファイルシステムの例として、Veritas File System (VxFS) などがあります。

一時的な失敗 (transient failure) メッセージ処理中に発生するエラー状態。リモート MTA が、配信時にメッセージを処理できない場合でも、あとで処理可能になることがあります。ローカル MTA は、メッセージをキューに戻し、あとで再転送されるようにスケジューリングします。

インスタンス (instance) 個別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。インストール済みの 1 組のバイナリファイルから、独立して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 (instance directory) サーバの特定の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 (*server-root/msg-instance/*) です。*instance* は、インストール時に指定したサーバの名前です。**インスタンスディレクトリ**、**サーバルート**も参照してください。

インストールディレクトリ (installation directory) 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 (*server-root/bin/msg/*) です。**インスタンスディレクトリ**、**サーバルート**も参照してください。

インターネット (Internet) 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 (IP) (Internet Protocol) インターネットおよびイントラネットの基礎となる基本ネットワークレイヤープロトコル。

インターネットプロトコルアドレス (internet protocol address) IP アドレスを参照してください。

イントラネット (intranet) 企業や組織内における複数の TCP/IP ネットワークからなるネットワーク。イントラネットでは、World Wide Web で使われているものと同種のサーバおよびクライアントソフトウェアを、企業 LAN 上で提供される社内アプリケーションとして使用できます。インターネットと通信するイントラネット上の機密情報は、通常はファイアウォールで保護されます。**ファイアウォール**、**エクストラネット**も参照してください。

永続的な失敗 (permanent failure) メッセージ処理中に発生するエラー状態。この状態が発生すると、メッセージストアは電子メールメッセージのコピーを削除します。MTA はメッセージを差出人に戻し、メッセージのコピーを削除します。

エイリアス (alias) 電子メールアドレスの別名。

エイリアスの参照解除 (dereferencing an alias) バインドまたは検索で、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変換するように指定すること。

エイリアスファイル (alias file) ポストマスターエイリアスなど、ディレクトリ内に設定されていないエイリアスを設定するために使用されるファイル。

エクストラネット (extranet) 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。**イントラネット**も参照してください。

エクспанダ (expander) メッセージをアドレスの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。メールエクспан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1つのアドレス (hacks@somehost.edu など) にメッセージを送信すると、メールエクспанダがリスト内のメールボックスへの配信を行います。メールエクプロダとも呼ばれます。**EXPN**も参照してください。

エクスパンド (expansion) この用語は、MTA によるメールリストの処理で使用されます。メールリスト宛てのメッセージを、各メールリストのメンバーに必要な数のコピーに変換することです。

エラーハンドラ (error handler) 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、ポストマスターが入力し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 (Error-Handler Action form) Messaging Server が処理できない受信メッセージとともにポストマスターアカウントに送信されるフォーム。ポストマスターは、フォームに入力して、メッセージの処理方法をサーバに指示します。

エラーメッセージ (error message) エラーやその他の状況をレポートするメッセージ。iPlanet Messaging Server は、処理できない電子メールメッセージを受け取った場合など、さまざまな状況でメッセージを生成します。また、情報の通知だけを目的とする通知エラーと呼ばれるメッセージもあります。

エンタープライズネットワーク (enterprise network) 地理的に分散している相互接続されたネットワークの集合で構成されるネットワーク。エンタープライズネットワークは、広範囲に分散している企業のニーズを満たすもので、企業のミッションクリティカルなアプリケーションで使用されます。

エンベロープ (envelope) 電子メールメッセージの差出人と受取人に関する情報を転送するためのコンテナ。これらの情報は、メッセージヘッダーには含まれません。エンベロープは、さまざまな電子メールプログラムで、メッセージを別の場所に移動するときに使用します。ユーザには、メッセージのヘッダーと本文だけが表示されます。

エンベロープフィールド (envelope field) メッセージエンベロープ内の名前付きの情報項目。RCPT TO などがあります。

オブジェクトクラス (object class) エントリが記述するオブジェクトの種類と、そのエントリに含まれる属性のセットを指定するテンプレート。たとえば、iPlanet Directory Server では、commonname、mail (電子メールアドレス)、mailHost、mailQuota などの属性を持つ emailPerson オブジェクトクラスが指定されます。

オフライン状態 (off-line state) 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て、メッセージの表示や返信の作成ができる状態。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 (online state) 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がリモートから返信する状態。

書き換え規則 (rewrite rules) 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です。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またはドメインの仕様を抽出する。(2) ホストまたは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またはドメイン仕様を書き換える。(4) メッセージを置くチャネルキューを決定する。

鍵データベース (key database) サーバの証明書用の鍵のペアを含むファイル。鍵ファイルとも呼ばれます。

仮想ドメイン (virtual domain) (1) ISP 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 に追加されるドメイン名。LDAP 検索やメールボックスサーバへのログインで使用します。**ドメイン**、**ホストドメイン**も参照してください。

完全指定ドメイン名 (FQDN) (fully-qualified domain name) 特定のインターネットホストを識別する一意の名前。**ドメイン名**も参照してください。

管理権限 (administration privileges) ユーザ管理の役割を定義する一連の権限。

管理コンソール (administration console) **コンソール**を参照してください。

管理者 (administrator) 定義済みの一連の管理権限を持つユーザ。**構成管理者**、**Directory Manager**、**Administration Server 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**、**ファミリーグループ管理者**、**メールリスト所有者**も参照してください。

管理対象オブジェクト (managed object) 設定可能な属性の集まり。たとえば、ディレクトリサービスの属性の集まりです。

管理ドメイン (administration domain) 管理制御の対象範囲。**ドメイン**も参照してください。

キュー (queue) **メッセージキュー**を参照してください。

共有フォルダ (shared folder) 複数のユーザが読み取り可能なフォルダ。共有フォルダに対しては所有者が指定されます。所有者は、フォルダに対する読み取りアクセス権を指定したり、共有フォルダからメッセージを削除したりできます。共有フォルダにはモデレータを指定することもできます。モデレータは、受信メッセージの編集、ブロック、転送などを行うことができます。共有できるのは IMAP フォルダだけです。**個人用フォルダ**も参照してください。

許可フィルタ (Allow filter) 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。**拒否フィルタ**も参照してください。

拒否フィルタ (Deny filter) 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。**許可フィルタ**も参照してください。

クライアント (client) 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 (client-server model) ネットワーク接続されたコンピュータがほか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処理モデル。例として、DNS のネームサーバとネームリゾルバのパラダイム、NFS やディスクレスホストなどのファイルサーバとファイルクライアントの関係などがあります。

クラスパス (class path) サブレットエンジンとサブレットテンプレートを実行するために必要なディレクトリおよび .jar ファイルへのパス。

グリーティングフォーム (greeting form) ユーザのアカウントが作成されたときにユーザに送信されるメッセージ。このフォームは、新しいアカウントを確認し、その内容を検証するために使用されます。

グループ (group) 識別名によって編成された LDAP メールエントリのグループ。通常は、メール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権限を与えるために使用される場合もあります。**動的グループ**、**静的グループ**も参照してください。

グループフォルダ (group folders) これらのフォルダには、共有フォルダとグループフォルダが含まれます。**共有フォルダ**も参照してください。

ゲートウェイ (gateway) ゲートウェイおよびアプリケーションゲートウェイという用語は、1つのネイティブフォーマットから別のフォーマットへの変換を行うシステムを指します。例として、X.400とRFC 822間の送受信を行う電子メールゲートウェイがあります。複数の電子メールシステム(特に、2つの異なるネットワーク上の類似性のないメールシステム)を接続し、その間でメッセージを転送するマシンです。マッピングと変換は複雑になることもあり、一般的に、あるシステムからメッセージを完全に受け取ってから適切な変換を行なって次のシステムに送信するようなストアアンドフォワードのしくみが必要です。

検索ベース (search base) ベース DN を参照してください。

公開鍵暗号化 (public key encryption) 公開コンポーネントと非公開コンポーネントの2つの部分から構成される鍵(コード)を使用する暗号化方式。メッセージの暗号化には、受取人の公開鍵が使われます。メッセージを解読するには、受取人だけが知っている受取人の非公開の鍵を使用します。

高可用性 (High Availability) サービスの中断を検出できるようにし、システム障害やプロセス失敗時の回復メカニズムを提供します。さらに、一次システムに障害が発生した場合には、バックアップシステムがサービスを引き継ぐことができるようにします。

構成管理者 (configuration administrator) iPlanet トポロジ全体のサーバおよび構成ディレクトリデータの管理権限を持つユーザ。構成管理者は、iPlanet トポロジ内のすべてのリソースに無制限にアクセスできます。ほかの管理者にサーバアクセス権を割り当てることができる唯一の管理者です。構成管理者は、管理者グループとそのメンバーが配置されるまで初期の管理構成を管理します。

個人用フォルダ (personal folder) 所有者だけが読み取り可能なフォルダ。**共有フォルダ**も参照してください。

コマンドラインインタフェース (command line interface) コマンドラインから実行できるコマンド。ユーティリティとも呼ばれます。

コメント文字 (comment character) 行の最初に配置することで、その行を実行されないコメントに変換する文字。

コンソール (Console) 多くの iPlanet コンポーネントの設定、監視、管理、および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フェース)。

サーバインスタンス (server instance) インストールされた特定のサーバソフトウェアを表す、ディレクトリ、プログラム、およびユーティリティ。

サーバ側規則 (SSR) (server side rules) サーバ側でメールをフィルタリングできるようにする規則のセット。Sieve メールフィルタリング言語に基づいています。

サーバ管理者 (server administrator) サーバ管理タスクを実行するユーザ。サーバ管理者は、タスク ACI に基づいて、特定のサーバのタスクに制限付きのアクセス権を提供します。構成管理者が、ユーザにサーバへのアクセス権を割り当てる必要があります。サーバへのアクセス権を与えられたユーザは、サーバ管理者となり、サーバへのアクセス権をほかのユーザに与えることができます。

サーバルート (server root) 特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、*server-root* と記述します。インストールディレクトリ、インスタンスディレクトリも参照してください。

サービス (service) (1) サーバが提供する機能。たとえば、iPlanet Messaging Server は、SMTP、POP、IMAP、HTTP などのサービスを提供します。(2) ユーザインタフェースを持たない Windows NT 上のバックグラウンドプロセス。iPlanet サーバは、Windows NT プラットフォーム上ではサービスとして稼働します。UNIX プラットフォーム上の **デーモン** と同じです。

サービス拒否攻撃 (denial of service attack) 個人が意図的にまたは誤ってメッセージを大量に送信したために、メールサーバが処理不能になる状態。サーバのスループットに著しい悪影響を与えたり、サーバ自体が過負荷状態になって機能しなくなることがあります。

サーブレット (servlet) Web サーバがクライアントの要求に応じてコンテンツを生成するために実行するサーバ側の Java プログラム。サーブレットは、サーバ側で実行されますが、ユーザインタフェースを使用しないという点でアプレットに似ています。

再組立 (defragmentation) MIME (Multipurpose Internet Mail Extension) の機能で、大きいサイズのメッセージが小さなメッセージ (断片) に分割された場合に、そのメッセージを再現します。各断片の Message Partial Content-Type ヘッダーフィールドには、断片を 1 つのメッセージに再組立するために使用する情報が含まれています。断片化も参照してください。

サブドメイン (subdomain) ドメインの一部。たとえば、corp.siroe.com というドメイン名では、corp は、ドメイン siroe.com のサブドメインを示します。ホスト名、完全指定ドメイン名も参照してください。

サブネット (subnet) 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 (referral) Directory Server が、情報要求を送信したクライアントに対し、そのクライアントが通信する必要がある 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。知識情報も参照してください。

識別名 (distinguished name) ディレクトリ情報ツリー内のエントリの位置を一意に指定する、カンマで区切られた一連の属性と値。通常、DN と略記されます。

自動返信オプションファイル (autoreply option file) 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 (AutoReply utility) 自動返信機能が有効になっているアカウント宛てに送信されたメッセージに対し、自動的に返信するためのユーティリティ。iPlanet Messaging Server 内のすべてのアカウントは、受信メッセージに対して自動的に返信するように設定できます。

従属参照 (subordinate reference) ディレクトリサーバによって保持される名前付きコンテキストの子の名前付きコンテキスト。**知識情報**も参照してください。

上位参照 (upper reference) ディレクトリ情報ツリー (DIT) 内で、ディレクトリサーバの名前付きコンテキストの上位にある名前付きコンテキストを保持するディレクトリサーバを示します。

使用可能な属性 (allowed attributes) 特定のオブジェクトクラスを使用するエントリについて指定できるが、必須ではない属性。**属性、必須の属性**も参照してください。

証明書データベース (certificate database) サーバのデジタル証明書 (1 つまたは複数) 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 (certificate-based authentication) クライアントが提供したデジタル証明書によるユーザの識別。**パスワード認証**も参照してください。

証明書名 (certificate name) 証明書とその所有者を特定する名前。

ジョブコントローラ (Job Controller) ほかのさまざまな MTA コンポーネントの要求に応じてタスクをスケジュールおよび実行する MTA コンポーネント。

シングルサインオン (single sign-on) ユーザを一度認証するだけで、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) にアクセスできるようにする機能。

スキーマ iPlanet Directory Server 内にエントリとして格納できる情報のタイプの定義 (構造と構文を含む)。スキーマと一致しない情報がディレクトリに格納されていると、ディレクトリにアクセスするクライアントが適切な結果を表示できない場合があります。

スプーフィング (spoofing) ネットワーク攻撃の形態の 1 つで、サーバにアクセスまたはメッセージを送信しようとしているクライアントに、不正なホスト名を使用させること。

スマートホスト (smart host) ほかのメールサーバが受取人を認識できない場合に、メッセージの転送先となる、ドメイン内のメールサーバ。

スレーブチャネルプログラム (slave channel program) リモートシステムによって開始された転送を受け入れるチャネルプログラム。**マスターチャネルプログラム**も参照してください。

スレッド (thread) プロセス内の小さな実行インスタンス。

正規表現 (regular expression) パターンマッチングのために、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。

静的グループ (static group) 各グループメンバーを列挙することにより静的に定義されたメールグループ。**動的グループ**も参照してください。

セキュリティモジュールデータベース (security-module database) SSL 暗号化方式用のハードウェアアクセラレータを記述する情報を含むファイル。secmod と呼ばれます。

セッション (session) クライアントサーバ接続のインスタンス。

切断状態 (disconnected state) メールクライアントはサーバに接続し、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します。

設定ファイル (configuration file) iPlanet Messaging システムの特定の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 (relative distinguished name) RDN を参照してください。

属性 (attributes) LDAP データは、属性と値のペアとして表されます。個々の情報は、記述属性に関連付けられています。**使用可能な属性**、**必須の属性**も参照してください。

組織管理者 (organization administrator) Delegated Administrator for Messaging and Collaboration 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と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。

代替アドレス (alternate address) アカウントの二次的なアドレス。通常はプライマリアドレスを変化させたものです。1つ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。

単一フィールド置換文字列 (single field substitution string) 書き換え規則において、ホストまたはドメインアドレスの指定アドレστοークンを動的に書き換えるドメインテンプレートの一部分。**ドメインテンプレート**も参照してください。

断片化 (fragmentation) 大きなメッセージを複数の小さなメッセージに分割できるようにする Multiple Internet Mail Extensions (MIME) 機能。**再組立**も参照してください。

知識情報 (knowledge information) 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。Directory Server は、知識情報を使用して、情報要求をほかのサーバに渡します。

チャンネル (channel) メッセージを処理する基本的な MTA コンポーネント。チャンネルは、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。各チャンネルは、1つまたは複数のチャンネルプログラムと1つの送信メッセージキューから構成されます。送信メッセージキューには、そのチャンネルに関連付けられている1つまたは複数のシステム宛てのメッセージが格納されます。**チャンネルブロック**、**チャンネルホストテーブル**、**チャンネルプログラム**も参照してください。

チャンネルプログラム (channel program) 次の機能を実行するチャンネルの一部。(1) メッセージをリモートシステムに送信し、送信後に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て適切なチャンネルキューに置く。**マスターチャンネルプログラム**、**スレーブチャンネルプログラム**も参照してください。

チャンネルブロック (channel block) 単一のチャンネル定義。**チャンネルホストテーブル**も参照してください。

チャンネルホストテーブル (channel host table) チャンネル定義のセット。

通知メッセージ (notification message) Messaging Server によって送信されるメッセージの一種で、メッセージ配信処理のステータスと、配信に関する問題や障害の理由などを知らせます。このメッセージは、情報提供を目的とし、ポストマスターに対してアクションを要求するものではありません。**配信ステータス通知**も参照してください。

次のホップリスト (next-hop list) メール経路で、メッセージの転送先を判別するために使用される近接システムのリスト。次のホップリスト内のシステムの順序によって、メール経路内でシステムにメッセージが転送される順序が決まります。

データストア (data store) ディレクトリ情報の保存場所。通常はディレクトリ情報ツリー全体の情報が含まれます。

デーモン (daemon) 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、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。**サービス**も参照してください。

ディスパッチャ (Dispatcher) 定義済み 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特定のサービスを分担できるように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 サーバプロセスを同時に実行できるようになります。

ディレクトリエントリ (directory entry) 識別名で特定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、エントリに含まれる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 (directory lookup) ユーザやリソースの名前またはその他の特性を基準として、ディレクトリ内で特定のユーザやリソースに関する情報を検索するプロセス。

ディレクトリコンテキスト (directory context) メッセージストアへのアクセスに対して、ユーザとパスワードの認証に使用するエントリ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。**ベース DN**も参照してください。

ディレクトリサービス (directory service) 組織内の人材とリソースに関する、論理的に集中化された情報のリポジトリ。**Lightweight Directory Access Protocol** も参照してください。

ディレクトリ情報ツリー (directory information tree) ディレクトリエントリを編成する、ツリー状の階層構造。DIT と呼ばれます。DIT は DNS (DC ツリー) または Open Systems Interconnect ネットワーク (OSI ツリー) に従って編成できます。

ディレクトリスキーマ (directory schema) ディレクトリに保存できるデータを定義する一連の規則。

ディレクトリ同期 (directory synchronization) MTA ディレクトリキャッシュを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で更新 (同期化) するプロセス。**MTA ディレクトリキャッシュ** も参照してください。

転送 (forwarding) メッセージの転送を参照してください。

転送プロトコル (transport protocols) SMTP や X.400 など、MTA 間でのメッセージ転送手段を提供するプロトコル。

統一メッセージング (unified messaging) 電子メール、ボイスメール、FAX、およびその他の通信形態に関して単一のメッセージストアを使用するという概念。**iPlanet Messaging Server** では、完全な統一メッセージングソリューションの基盤を提供します。

同期 (synchronization) (1) マスターディレクトリサーバのデータによる複製ディレクトリサーバのデータの更新。(2) MTA ディレクトリキャッシュの更新。

動的グループ (dynamic group) LDAP 検索 URL で定義されるメールグループ。通常、ユーザはディレクトリエントリ内で LDAP 属性を設定することによってグループに参加します。

ドキュメントルート (document root) iPlanet Web Server にアクセスするユーザに対して表示されるファイル、イメージ、データを含むサーバマシン上のディレクトリ。

トップレベル管理者 (top-level administrator) Delegated Administrator for Messaging and Collaboration の GUI または CLI を使用して、Messaging Server ネームスペース全体のメールユーザ、メールリスト、ファミリーアカウント、およびドメインの作成、変更、および削除を行う管理権限を持つユーザ。デフォルトでは、このユーザは、トポロジ内のすべての Messaging Server のメッセージストア管理者として作業することができます。

ドメイン (domain) 単一のコンピュータシステムの制御下にあるリソース。**管理ドメイン**、DNS ドメイン、ホストドメイン、**仮想ドメイン**も参照してください。

ドメインエイリアス (domain alias) 別のドメインを指すドメインエントリ。ホストドメインはエイリアスを使用することにより、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 (domain rewrite rules) **書き換え規則**を参照してください。

ドメイン管理者 (domain administrator) Delegated Administrator for Messaging and Collaboration 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、メールリスト、およびファミリーアカウントの作成、変更、および削除を行うための管理権限を持つユーザ。デフォルトでは、このユーザは、トポロジ内のすべての Messaging Server のメッセージストア管理者として作業することができます。

ドメイン制限容量 (domain quota) 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 (domain organization) 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、企業内でユーザとグループのエントリを部門別に編成する場合に有用です。

ドメインテンプレート (domain template) 書き換え規則の一部で、アドレスのホスト部分とドメイン部分の書き換え方法を定義します。テンプレートは、完全に静的なホストアドレスおよびドメインアドレス、または単一フィールド置換文字列、あるいはその両方を含む場合があります。

ドメインネームシステム (DNS) (Domain Name System) 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ほかのコンピュータをドメイン名で見つけることができるようにする分散型名前解決ソフトウェア。システムは、標準 IP アドレスをホスト名 (www.siroe.com など) に関連付けます。通常、各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の、複製された分散型のデータ照会サービスを提供します。**A レコード**、**MX レコード**、**CNAME レコード**も参照してください。

ドメイン部分 (domain part) 電子メールアドレスの @ 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 (domain hosting) 共有 Messaging Server 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 と sesta.org の両方のドメインを siroe.net メールサーバ上でホストできます。ユーザは、ホストドメインとの間でメールの送受信を行います。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。

ドメイン名 (domain name) (1) 電子メールアドレス内で使用されるホスト名。(2) 管理組織を定義する一意の名前。ドメインにはほかのドメインを含めることができます。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、かつトップレベルの com ドメインのサブドメインです。siroe.com ドメインをさらに corp.siroe.com などのサブドメインに分割することもできます。**ホスト名**、**完全指定ドメイン名**も参照してください。

名前解決 (name resolution) IP アドレスを対応する名前にマップするプロセス。DNS も参照してください。

名前付きコンテキスト (naming context) 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接尾辞。iPlanet Directory Serverでは、特定のタイプのディレクトリ情報が名前付きコンテキストに格納されます。たとえば、Siroe CorporationのBostonオフィスのマーケティング部門の社員すべてのエントリを格納する名前付きコンテキストは、ou=mktg, ou=Boston, o=siroe, c=USのようになります。

名前付き属性 (naming attribute) ディレクトリ情報ツリーの識別名の最後の属性。相対識別名も参照してください。

認証 (authentication) (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 (Certificate Authority) CA を参照してください。

認証証明書 (authentication certificate) 相手を検証および認証するために、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。証明書は、その所有者(クライアントまたはサーバ)の信頼性を保証します。証明書は譲渡できません。

ネームスペース (name space) LDAP ディレクトリのツリー構造。ディレクトリ情報ツリーも参照してください。

ネットワークマネージャ (network manager) 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 (node) DIT 内のエントリ。

パーティション (partition) メッセージストアパーティションを参照してください。

配信 (delivery) メッセージの配信を参照してください。

配信ステータス通知 (delivery status notification) 受取人に配信中のメッセージに関するステータス情報を示すメッセージ。たとえば、ネットワークが停止したために配信が遅れていることを知らせるメッセージなどがあります。

配布リスト (distribution list) メールリストを参照してください。

配布リスト所有者 (distribution list owner) メールリスト所有者を参照してください。

バインド DN (bind DN) 操作実行時に Directory Server に対する認証に使用される識別名。

パスワード認証 (password authentication) ユーザ名とパスワードによるユーザの識別。証明書に基づく認証も参照してください。

パターン (pattern) 許可フィルタや拒否フィルタなどで、マッチングのために使用される文字列表現。

バックアップ (backup) メッセージストアのフォルダの内容をバックアップデバイスにバックアップするプロセス。リストアも参照してください。

バックエンドサーバ (backend server) 電子メールメッセージの保管と取り出しの機能だけを持つ電子メールサーバ。メッセージストアサーバとも呼ばれます。

バックボーン (backbone) 分散システムの主要な接続メカニズム。バックボーン上の中間システムに接続するすべてのシステムは、相互に接続されます。バックボーンがある場合でも、コスト、パフォーマンス、セキュリティなどの理由から、バックボーンを迂回するようにシステムを設定することができます。

バニティドメイン (vanity domain) 特定のサーバまたはホストドメインではなく、個別のユーザに関連付けられているドメイン名。MailAlternateAddress 属性を使用して指定されます。バニティドメインのドメイン名には LDAP エントリが含まれません。バニティドメインは、個人または小さな組織が、独自のホストドメインを持つための管理負荷をかけずに、カスタマイズしたドメイン名を使用する場合に便利です。カスタムドメインとも呼ばれます。

ハブ (hub) システムの単一接続ポイントとして機能するホスト。たとえば、2つのネットワークがファイアウォールで分離されている場合は、しばしばファイアウォールコンピュータがメールハブとして機能します。

必須の属性 (required attributes) 特定のオブジェクトクラスを使用するエントリ内に存在する必要がある属性。使用可能な属性、属性も参照してください。

非配信通知 (nondelivery notification) メッセージ転送中に、アドレスパターンと書き換え規則の間に一致するものが見つからない場合、MTA は、オリジナルのメッセージとともに非配信レポートを差出人に返します。

ファイアウォール (firewall) ネットワーク構成の1つで、通常はハードウェアおよびソフトウェアの両方を使用して、組織内のネットワーク接続されたコンピュータと組織外のコンピュータの間の防護壁を構成します。一般に、ファイアウォールは物理的な建物または組織のサイト内にある、ネットワークの電子メール、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。

ファミリーグループ管理者 (family group administrator) ファミリーグループ内のファミリーメンバーの追加と削除を行う管理権限を持つユーザ。このユーザは、グループのほかのメンバーに管理アクセス権を与えることができます。

フェイルオーバー (failover) 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 (folder) メッセージの名前付きのコレクション。フォルダにはほかのフォルダを含めることができます。メールボックスとも呼ばれます。**個人用フォルダ**、**共有フォルダ**、**INBOX** も参照してください。

複製ディレクトリサーバ (replica directory server) データのすべてまたは一部のコピーを受信するディレクトリ。

輻輳しきい値 (congestion thresholds) システム管理者が設定できるディスク容量の上限。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 (plaintext) データの転送方法を表します。意味は状況によって異なります。たとえば、SSL のプレーンテキストパスワードは暗号化され、**cleartext** (平文) としては送信されません。SASL では、プレーンテキストパスワードはハッシュされ、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。**SSL**、**SASL** も参照してください。

プレーンテキスト認証 (plaintext authentication) **パスワード認証**を参照してください。

プロキシ (proxy) 1 つのシステムが別のシステムの代理でプロトコルの要求に応答するメカニズム。プロキシシステムをネットワーク管理で使用すると、モデムなどの単純なデバイスに完全なプロトコルスタックを実装する必要がなくなります。

プロセス (process) オペレーティングシステムによって設定される、独立して完全に機能する実行環境。通常、アプリケーションの各インスタンスは個別のプロセスで実行されません。**スレッド**も参照してください。

プロトコル (protocol) 情報を交換する 2 つ以上のシステムが従う必要がある規則と、交換されるメッセージに関する公式の記述。

プロビジョニング (provisioning) iPlanet Directory Server のエントリを追加、変更、または削除するプロセス。これらのエントリには、ユーザ、グループ、およびドメイン情報が含まれます。

ベース DN (base DN) 検索が開始されるディレクトリ内の識別名エントリ。検索ベースとも呼ばれます。例: `ou=people, o=siroe.com`

ヘッダー (header) 電子メールメッセージで本文の前にある部分。ヘッダー内では、フィールド名のあとにコロンと値が続きます。ヘッダーには、電子メールプログラムとユーザにとって、メッセージが意味をなすようにするために有用な情報が含まれます。たとえば、配信情報、内容の概要、トレース、MIME 情報などが含まれます。これらは、メッセージの受取人、差出人、送信日時、内容を示します。ヘッダーは、電子メールプログラムが読み取れるように RFC 822 に従って記述されている必要があります。

ヘッダーフィールド (header field) メッセージヘッダー内の名前付きの情報項目。From:、To: などが 있습니다。ヘッダー行と呼ばれることもあります。

ポート番号 (port number) ホストマシン上の個々の TCP/IP アプリケーションを指定する番号。転送されたデータの宛先を提供します。

ホスト (host) 1つ以上のサーバが置かれているマシン。

ホストドメイン (hosted domain) ISP にアウトソースされた電子メールドメイン。ISP は、企業の電子メールドメインのホスティングを提供し、その企業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、ほかのホストドメインと同一の 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によって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上でホストできます。各ホストドメインには、そのドメインのユーザとグループのコンテナを指す 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または仮想ドメインとも呼ばれます。**ドメイン**、**仮想ドメイン** も参照してください。

ポストマスターアカウント (postmaster account) Messaging Server からのシステム生成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。ポストマスターアカウントには、1つ以上の有効なメールボックスを指定する必要があります。

ホスト名 (host name) ドメイン内の特定マシンの名前。ホスト名は、IP ホスト名です。IP ホスト名としては、「短縮形」のホスト名 (mail など) または完全指定ホスト名が使用されます。完全指定ホスト名は、ホスト名とドメイン名の2つの部分から構成されます。たとえば mail.siroe.com は、ドメイン siroe.com 内のマシン mail を表します。ホスト名は、ドメイン内で一意にする必要があります。組織内の異なるサブドメイン内にある場合は、複数のマシンに mail という名前を付けることができます。たとえば、mail.corp.siroe.com と mail.field.siroe.com を使用できます。ホスト名は、常に、特定の IP アドレスにマップされます。**ドメイン名**、**完全指定ドメイン名**、**IP アドレス** も参照してください。

ホスト名の非表示 (host name hiding) 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使用すること。

ホップ (hop) 2台のコンピュータ間での転送。

本文 (body) 電子メールメッセージの一部分。ヘッダー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、マルチメディアなどを使って差出人が自由に作成できます。構造化された本文は MIME 標準に従う必要があります。

マスターチャネルプログラム (master channel program) 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。**スレーブチャネルプログラム**も参照してください。

マスターディレクトリサーバ (master directory server) 複製されるデータを含むディレクトリサーバ。

見出し (banner) クライアントがはじめて接続したときに IMAP などのサービスによって表示されるテキスト文字列。

無効なユーザ (invalid user) メッセージ処理中に発生するエラー状態。この状態が発生すると、メッセージストアは、MTA と通信して、メッセージのコピーを削除します。MTA はメッセージを差出人に戻し、メッセージのコピーを削除します。

メーリングリスト メールリストを参照してください。

メーリングリスト所有者 (mailing list owner) メールリスト所有者を参照してください。

メールクライアント (mail client) ユーザが電子メールを送受信する際に利用するプログラム。さまざまなネットワークやメールプログラムの一部で、ユーザがもっとも頻繁に使用する部分です。メールクライアントは、配信するメッセージを作成して送信し、新たに受信したメールを確認し、受信メールを受理して整理します。

メール交換レコード (mail exchange record) MX レコードを参照してください。

メールリスト (mail list) 電子メールアドレスのリスト。メールリストのアドレスを指定することによってそれらの電子メールアドレス宛てにメッセージを送信できます。グループと呼ばれることもあります。

メールリスト所有者 (mail list owner) メールリストのメンバーの追加と削除を行う管理権限を持つユーザ。

メールリレー (mail relay) MUA または MTA からのメールを受け取り、そのメールを受取人のメッセージストアや別のルーターに中継するメールサーバ。

メールルーター (mail router) メールリレーを参照してください。

メッセージ (message) 電子メールの基本単位。メッセージは、ヘッダーと本文で構成され、多くの場合、差出人から受取人に転送される間はエンベロープに格納されます。

メッセージアクセスサービス (message access services) 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バ、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 (message queue) クライアントやほかのメールサーバから受け取ったメッセージを (即時または指定日に) 配信するために保管するディレクトリ。

メッセージストア (message store) Messaging Server インスタンスに対してローカルに配信されたすべてのメッセージのデータベース。メッセージは、単一の物理ディスクに格納することも、複数の物理ディスクに格納することもできます。

メッセージストア管理者 (message store administrator) Message Server のメッセージストアを管理する管理権限を持つユーザ。このユーザは、メールボックスの表示と監視、およびストアへのアクセス制御の指定を行うことができます。プロキシ認証の権限を使用して、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 (message store partition) 単一の物理ファイルシステムパーティション上に置かれたメッセージストアまたはメッセージストアのサブセット。

メッセージ制限容量 (message quota) 特定のフォルダが消費できるディスク容量を定義する制限。

メッセージの削除 (delete message) 削除するメッセージにマークを付けること。削除したメッセージは、別の処理で消去 (パージ) するまで、メッセージストアからは削除されません。**メッセージのパージ**、**メッセージの消去**も参照してください。

メッセージの消去 (expunge message) メッセージに削除マークを付け、その後 INBOX から永久に削除すること。**メッセージの削除**、**メッセージのパージ**も参照してください。

メッセージの送信 (message submission) クライアントのユーザエージェント (UA) は、メールサーバにメッセージを転送し、配信を要求します。

メッセージの転送 (message forwarding) MTA が、特定のアカウントに配信されたメッセージを、アカウントの属性で指定された 1 つまたは複数の新しい宛先に送信するときの処理。転送は、ユーザが設定できます。**メッセージの配信**、**メッセージのルーティング**も参照してください。

メッセージのパージ (purge message) ユーザおよびグループフォルダ内で削除マークを付け、参照することのなくなったメッセージを永久に削除し、使用していた領域をメッセージストアのファイルシステムに戻すプロセス。**メッセージの削除**、**メッセージの消去**も参照してください。

メッセージの配信 (message delivery) MTA がメッセージをローカルの受取人 (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。

メッセージのルーティング (message routing) 最初の MTA が、受取人がローカルアカウントではなくほかの場所にいると判断したときに、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。**メッセージの転送**も参照してください。

メンバー (member) メールリスト宛ての電子メールのコピーを受け取るユーザまたはグループ。**メールリスト**、**エクスパンド**、**モデレータ**、**所有者**も参照してください。

モデレータ (moderator) メールリスト宛てのすべての電子メールを最初に受信して、以下の処理を選択実行するユーザ。(A) 配布リストにメッセージを転送する。(B) メッセージを編集してからメールリストに転送する。(C) メッセージをメールリストに転送しない。**メールリスト**、**エクスパンド**、**メンバー**も参照してください。

ユーザアカウント (user account) サーバにアクセスするためのアカウント。ディレクトリサーバ上のエン트리として管理されます。

ユーザエージェント (UA) (user agent) ユーザがメールメッセージを作成、送信、受信できるようにするクライアントコンポーネント。Netscape Communicator などがあります。

ユーザエン트리またはユーザプロフィール (user entry or user profile) 各ユーザに関する必須および任意の情報を記述するフィールド。識別名、氏名、役職、電話番号、ポケットベルの番号、ログイン名、パスワード、ホームディレクトリなどがあります。

ユーザ制限容量 (user quota) 電子メールメッセージ用にユーザ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。

ユーザフォルダ (user folders) ユーザの電子メールのメールボックス。

リストア (restore) フォルダの内容をバックアップデバイスからメッセージストアに復元するプロセス。バックアップも参照してください。

リスンポート (listen port) サーバがクライアントやその他のサーバと通信するために使用するポート。

リバース DNS 検索 (reverse DNS lookup) 数値 IP アドレスを対応する完全指定ドメイン名に解釈するために DNS に照会するプロセス。

リレー (relaying) メッセージサーバ間でメッセージを渡すプロセス。

ルーター (router) 複数のネットワークトラフィック経路から利用する経路を決定するシステム。ルーターは、ネットワークに関する情報を取得するためのルーティングプロトコルを使用し、さらに、「ルーティングマトリクス」と呼ばれるいくつかの条件に基づいて最善の経路を決定するアルゴリズムを使用します。OSI の用語では、ルーターはネットワークレイヤーの中間システムになります。ゲートウェイも参照してください。

ルーティング (routing) メッセージのルーティングを参照してください。

ルートエン트리 (root entry) ディレクトリ情報ツリー (DIT) 階層のトップレベルのエン트리。

ルックアップ (lookup) 検索の同義語。特定のパラメータを使ってデータを並べ替えます。

レベル (level) ログの詳細度の指定。ログファイルに記録するイベントの種類の相対的な数を意味します。たとえば、Emergency レベルでは、ログに記録されるイベントはわずかですが、Informational レベルでは数多くのイベントがログに記録されます。

ローカル部分 (local part) 電子メールアドレス内の受取人を識別する部分。ドメイン部分も参照してください。

ログディレクトリ (log directory) 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 (log expiration) 有効期間が過ぎたログファイルは、ログディレクトリから削除されます。

ログローテーション (log rotation) 現在のログファイルとして使用する新しいログファイルを作成すること。以後のログイベントは、新しいログファイルに書き込まれます。以前のログファイルはログディレクトリ内に残りますが、ログが書き込まれることはありません。

ワークグループ (workgroup) ローカルワークグループ環境。サーバは、ローカルオフィスまたはワークグループ内で、独自のルーティングおよび配信を実行します。部門間のメールは、バックボーンサーバにルーティングされます。**バックボーン**も参照してください。

ワイルドカード (wildcard) 1つまたは複数のほかの文字または文字範囲を表すことができる検索文字列内の特殊文字。

索引

記号

/var/mail, 73

A

ACI

アーキテクチャ, 25

ドメイン (domain), 34

ACI の例, 117

C

catch-all ドメインアドレス, 48, 56, 78

cn, 36, 65

Console のマニュアル, 104

D

dataSource, 66, 86

dc, 40

DC ツリー, 20

DC ツリー (DC Tree)

トップレベルドメインエントリ、作成, 37

ホストドメインエントリ、作成, 38

ルートドメインエントリ、作成, 36

DC ツリー、作成, 35

description, 40

Directory Manager, 102

DIT、iPlanet Messaging Server へのマッピング, 22

dn, 36

E

EXPN コマンド, 96

G

givenName, 66

groupOfUniqueNames, 85

I

icsCalendarDomain, 39

inetDomain, 39, 40

inetDomain attributes, 40

inetDomainBaseDN, 20, 40

- inetDomainStatus, 40
- inetLocalMailRecipient, 47, 65, 85
- inetMailGroup, 85
- inetMailGroupManagement, 85
- inetMailGroupStatus, 85
- inetMailUser, 65
- inetManagedGroup, 58
- inetOrgPerson, 65
- inetUser, 65
- inetUserStatus, 66
- initials, 65
- ipUser, 65

L

- ldap:///, 86

M

- mail, 66, 86
- mailAlternateAddress, 47, 67, 86
- mailClientAttachmentQuota, 41, 52
- mailDeliveryURL
 - 属性値の形式, 86
- mailDomain, 40
- mailDomainAllowedServiceAccess, 40
- mailDomainDiskQuota, 40
- mailDomainMsgQuota, 41
- mailDomainStatus, 40, 53
- mailHost, 67, 86
- mailMsgQuota, 67
- mailProgramDeliveryInfo, 73
- mailQuota, 67
- mailRoutingHosts, 40, 51
- mailRoutingSmartHost, 50
- mailUserStatus, 66
- memberOfManagedGroup, 57
- Messaging Server 管理者、「管理者」を参照
- mgmanJoinability, 97

- mgrpAllowedBroadcaster, 89
- mgrpAllowedDomain, 90
- mgrpDisallowedBroadcaster, 89
- mgrpDisallowedDomain, 90
- mgrpRequestsTo, 95
- mgrpRFC822MailMember, 88
- mnggrpbillableuser:, 58
- mnggrpcurrentusers, 58
- mnggrpmailquota, 58
- mnggrpmaxusers, 58
- mnggrpstatus, 58
- msgVanityDomain, 47
- msgVanityDomainUser, 47

N

- Netscape Console のマニュアル, 104
- nsdamodifiableby, 59
- nsManagedDept, 58
- nsManagedDomain, 39, 43
- nsManagedMailList, 85
- nsManagedPerson, 65, 67
- nsMaxMailLists, 44
- nsMaxUsers, 44, 86
- nsNumMailLists, 43
- nsNumUsers, 44, 86

O

- o, 36
- objectClass
 - inetDomain, 39
 - mailDomain, 39
 - ドメイン (domain), 39
- objectClass domain attributes
 - dc, 40
 - description, 40
- organizationalPerson, 65
- organizationalUnit, 45
- organizationName, 40

ou, 36
 People, 45
owner, 87

P

person, 65
preferredMailHost, 40

S

SIEVE 規則, 74
sn, 36, 65

T

top オブジェクトクラス, 37

U

uid, 66
uniqueMember, 85, 88
userPassword, 66
userPresenceProfile, 65, 67

あ

暗号化
 定義, 139

お

オブジェクトクラス、設計, 24

か

管理者
 構成管理者、作成, 104
 サーバのメッセージストア管理者, 105
 作成, 102
 特定ドメインのメッセージストア, 107
 トップレベル, 109
 トップレベル管理者、作成, 109
 ドメイン, 110
 ドメイン組織管理者, 112
 ドメインユーティリティ
 imadmin_domain_create, 111
 ファミリーグループ, 60
 メッセージストア, 104
 メッセージストア管理者、作成, 104
 メッセージストア管理者、トポロジ全体, 105
管理対象のグループアカウント、「ファミリーア
 カウント」を参照

き

行の折り返し, 86
共有クラス, 24

く

グループ
 メールの制限, 89
グループ、「メーリングリスト」を参照

こ

構成管理者, 102
コンテナ, 44

さ

サービス管理者, 109

サービスクラス, 28
サービスクラス、設定, 28
サービスクラス、例, 29
サービス固有のオブジェクトクラス, 24
作成
 ホストドメイン, 38, 43
 ルートエントリ (root entry), 36

し

システム管理者, 102
省略名
 属性 (attributes), 36
所有者, 87

す

スキーマ, 24
スマートルーティングホスト, 50

せ

請求対象ユーザ, 57

そ

属性 (attributes)
 ホストドメイン (hosted domain), 43
属性のエイリアス, 36
属性の省略名, 36
組織, 43
組織管理者, 112
組織ツリー, 20, 41
 ホストドメインエントリ, 43
 ルートエントリ (root entry), 42

た

対象読者, 15

ち

チャプタの単一テンプレート, 117

つ

追加の行, 86

て

ディレクトリツリー
 「ネームスペース」も参照, 20
データモデル, 24
添付ファイル数の制限, 52
添付ファイル、制限, 52

と

動的なメーリングリスト, 98
トップレベル管理者, 103
ドメイン (domain)
 ACI, 34
 作成, 33
 ステータス, 52
 メールサービス, 49
ドメイン (domain), 39
ドメイン管理者, 103
ドメイン管理者グループ, 110
ドメイン組織
 削除, 46
ドメイン組織 (domain organization)
 作成, 46
ドメイン組織管理者, 103, 112

ドメインタスク, 48
ドメインのエイリアス、作成, 50

ね

ネームスペース, 20
2つのDITが必要な理由, 22
既存のDITのマッピング, 22
サブドメイン用の個別のネームスペース, 24
データのパーティション化とアクセス制御, 23
二重ツリー機構, 20

は

パスワード, 69
バニティドメイン (vanity domain), 47

ふ

ファミリーアカウント, 57
作成, 57
メンバーの追加, 57
ファミリーグループ
管理者の作成, 60
請求対象ユーザ, 57
ファミリーグループ管理者, 60, 103
プログラム, 73
プロビジョニング、定義, 19

ほ

ホスト、定義, 153
ホストドメイン
作成, 38, 43
ホストドメイン (hosted domain)
属性 (attributes), 43
ホストドメインコンテナ, 44

ま

マニュアルの表記規則, 17

め

メーリングリスト, 83, 87
アクティブ化と非アクティブ化, 94
購読リクエスト, 95
作成, 84
参加可能, 97
受信メールのフィルタリング, 89
ステータス, 94
制限、メッセージサイズ, 99
属性値の形式, 86
動的, 98
メールフィルタリングの優先規則, 90
メッセージのアーカイブ, 94
メンバーの追加, 88
メンバーの表示, 96
モデレータ, 93
メールリストの所有者, 103
メッセージストア管理者, 102
作成, 107

も

モデレータ, 93
属性値の形式, 86

ゆ

ユーザ
Vacation メッセージ, 70
アクティブ化と非アクティブ化, 68
ステータス, 68
その他の電子メールアドレス, 78
パスワード, 69
メーリングリストの作成, 80
メールサーバ, 79
メールサーバ、72

- メールの転送, 77
- メール配信オプション, 73
- メッセージサイズの制限, 81
- メッセージの制限, 76
- メッセージフィルタ, 74

- ユーザエン트리
 - 作成, 63, 64

る

- ルーティングホスト, 51
- ルートエン트리 (root entry)
 - 作成, 36